DOCTOR OF PHILOSOPHY

Quantum communication with continuous variables

van Loock, Peter

Award date:
2001

Awarding institution:
Bangor University

Quantum Communication

with

Continuous Variables

by Peter van Loock

PhD thesis, University of Wales, Bangor

to my son
Julian

Contents

Summary

Many quantum communication schemes rely on the resource of entanglement. For example, quantum teleportation is the transfer of arbitrary quantum states through a classical communication channel using shared entanglement. Entanglement, however, is in general not easy to produce. The bottom line of this thesis is that a particular kind of entanglement, namely that based on continuous quantum variables, can be created relatively easily. Only squeezers and beam splitters are required to entangle arbitrarily many electromagnetic modes.

In the first two chapters of the thesis, some basics of quantum optics and quantum information theory are presented. These results are then needed in chapter III, where we characterize continuous-variable entanglement and show how to make it. The members of a family of multi-mode states are found to be truly multi-party entangled with respect to all their modes. These states also violate multi-party inequalities imposed by local realism, as we demonstrate for some members of the family. Various quantum communication protocols based on the continuous-variable entangled states are discussed and developed in chapter IV. These include the teleportation of entanglement (entanglement swapping) as a test for genuine quantum teleportation. It is shown how to optimize the performance of continuous-variable entanglement swapping. We highlight the similarities and differences between continuous-variable entanglement swapping and entanglement swapping with discrete variables. For this purpose, we examine the infinite-dimensional limit of the latter. Chapter IV also contains a review of quantum cryptographic schemes based on continuous variables.

Finally, in chapter V, we consider a multi-party generalization of quantum teleportation. This so-called telecloning means that arbitrary quantum states are transferred not only to a single receiver, but to several. However, due to the quantum mechanical no-cloning theorem, arbitrary quantum states cannot be perfectly copied. We present a protocol that enables telecloning of arbitrary coherent states with the optimal quality allowed by quantum theory. The entangled states needed in this scheme are again producible with squeezed light and beam splitters. Although the telecloning scheme may also be used for "local" cloning of coherent states, we show that cloning coherent states locally can be achieved in an optimal fashion without entanglement. It only requires a phase-insensitive amplifier and beam splitters.

Acknowledgements

I would like to thank Professor Samuel L. Braunstein for his great supervision. I am also grateful to my colleagues Pieter Kok, Arun Pati, and Kae Nemoto for their support and the pleasant atmosphere we have had in our group. Special thanks to Pieter for his help with the format of this thesis. Thanks to all the other people who made my time in Bangor an unforgettable experience (my Spanish friends, let alone the Welsh), and to my parents.

Peter van Loock, September 2001

Introduction

The field of 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 not only lead to a deeper understanding of quantum theory. In addition, the exploitation of quantum effects proves beneficial for various kinds of information processing and communication. Many of the schemes based on this idea refer to one particular quantum system: light. Propagating with the maximum speed allowed for the transfer of information, light is an ideal medium for communication (though less suitable for storing information). This applies to communication both in the classical and in the quantum realm where the quantum effects of light are utilized. We will here develop various protocols for quantum communication with light. For this purpose, the quantum features of light we are mainly interested in are those expressed by continuous quantum variables such as the quadratures of an electromagnetic mode.

When we study *quantum communication with continuous variables*, our investigations rely on many results of quantum optics and quantum information theory. In order to be self-contained, we will therefore first discuss several results from these two fields. This also enables us to introduce the notations and conventions that we use throughout the thesis. We will not deal with quantum computation here, although the efficient quantum optical manipulation of continuous quadrature amplitudes may be useful for that purpose as well (see for example Ref. [129]). Probably the most important result of this thesis is that entanglement, the essential ingredient of many quantum communication schemes, can be relatively easily produced for continuous quantum variables. Continuous-variable entanglement is extraordinarily "cheap". Its generation requires only a resource of "squeezed light" and beam splitters.

The thesis is organized as follows: in chapter I, we will study some basics

of quantum optics. This includes the quantisation of the electromagnetic field and various representations of the quantised field. The active optical elements required for our quantum circuits are squeezers. Hence we discuss different methods for producing squeezed light. At the end of chapter I, we will then examine how the quantised light field can be manipulated by linear optics using passive optical elements such as beam splitters. The basics of quantum information presented in chapter II contain some tools useful for later and some fundamental results such as the no-cloning theorem and the definition of different kinds of entanglement. We will also consider quantum teleportation with discrete variables in chapter II.

As a resource for quantum communication we need entanglement. We will extensively describe and characterize entanglement based on continuous quantum variables in chapter III. This includes inseparability criteria and quantum circuits for generating continuous-variable entanglement. We will find a family of multi-mode states whose members are genuinely multi-party entangled with respect to all their modes. This is shown using a multi-party inseparability criterion that relies on the states' purity and total symmetry. In addition, the presence of multi-mode entanglement is verified by revealing the states' nonlocality: we demonstrate that these states violate multi-party inequalities imposed by local realism. A broadband description of entanglement will be given at the end of chapter III.

In chapter IV, we will then develop quantum communication protocols using the continuous-variable entanglement. These protocols enable in principle the reliable transfer of arbitrary quantum states. We describe quantum teleportation in various representations and analyze when the transfer of quantum states through a classical communication channel deserves to be called quantum teleportation. These teleportation criteria are applied to the teleportation of coherent or squeezed states and to that of one half of an entangled state (so-called entanglement swapping). We will investigate both discrete-variable and

continuous-variable entanglement swapping. The differences and similarities of these two schemes are highlighted when we examine the infinite-dimensional limit of entanglement swapping with discrete variables. The "gain" for transforming the classical measurement results (photocurrents) into optical fields will prove crucial for the optimality of continuous-variable entanglement swapping. We will then use the multi-party entangled states within a quantum communication (teleportation) network. This will confirm their multi-party entanglement in an operational way. Again, only the right choice of the "gain" ensures an optimal performance of the multi-party scheme. We will then also give a broadband treatment of teleportation and entanglement swapping. Finally, we discuss schemes such as quantum cryptography for the secure transmission of classical information exploiting quantum effects.

Chapter V is devoted to quantum cloning with continuous variables. We will study both "local" cloning and "cloning at a distance" (telecloning). A circuit for the optimal local cloning of coherent states will be presented. It requires only a linear amplifier and beam splitters. No entanglement is needed. By contrast, for telecloning coherent states, entanglement is essential. But again the entangled states turn out to be producible in a relatively simple way using squeezed light and beam splitters. Since the squeezing needed is *finite*, optimal telecloning can not only be approached like perfect one-to-one quantum teleportation in the limit of *infinite* squeezing; optimal telecloning can be achieved in principle. This might be a surprising result, because existing qubit telecloning schemes are based on maximum entanglement. However, maximum entanglement for continuous variables corresponds to infinitely squeezed, unphysical states. Nonetheless, we will show that finite squeezing suffices. We also present a numerical analysis confirming that our telecloning protocol exploits *minimal* squeezing resources. In contrast to the existing qubit schemes, an experimental realization of our telecloning scheme is thus possible with current technology.

I

Basics of quantum optics

Modern communication technology increasingly relies on classical optics. Photons are faster than electrons and bits of classical information encoded, for instance, in the temporal position of a light pulse in an optical fiber, can be conveyed at a wide range of frequencies. Convenient and efficient communication via the internet utilizes *classical* optics, namely optical-fiber technology. For these purposes, *quantum* properties of light are not relevant. In fact, quantum effects are unwanted, because they might degrade the performance of the optical communication system (for example, timing jitter of fiber-solitons due to quantum noise [96], photon number fluctuations and others).

In quantum communication, one explicitly wants to exploit quantum features such as superposition and entanglement, as we will see in the next chapter. The quantum counterpart of optical communication, quantum optical communication, therefore must rely on sophisticated quantum properties of light. Indeed most of the experimental proposals for demonstrating quantum communication protocols originate from the field of quantum optics. The distinct quantum features of light have been known much longer than the relatively new ideas of quantum information theory. The famous papers by Glauber from 1963 [93, 94, 95], based on a rigorous quantum formulation of optical coherence, represent milestones of a quantum theory of light. Thanks to the invention of the laser, a lot of progress has been made in experimental quantum optics as well.

What are the consequences of a quantum description of light? Put in simple terms, not only must the position and momentum of massive particles such

as electrons obey the Heisenberg uncertainty relation, but also electromagnetic field observables such as the "quadrature amplitudes". Light fields emitted from a laser source not only exhibit thermal fluctuations that in principle might be entirely suppressed, but also intrinsic unavoidable quantum fluctuations. The quantum state of the electromagnetic field closest to a well determined classical state is the so-called coherent state, with minimum uncertainty symmetrically distributed in phase space. Any decrease of say the amplitude uncertainty ("amplitude squeezing") must be accompanied by an increase of the phase uncertainty ("phase antisqueezing"), because otherwise the Heisenberg uncertainty relation is violated. Among the nonclassical features of light, "squeezing" will turn out to be the effect we are most interested in. Originally, squeezing was considered as a means to enhance the sensitivity of optical measurements near the standard quantum limit (for example, in the interferometric detection of gravitational radiation [52] or for low-noise communications [211]). In this thesis, we will see that squeezed light represents a relatively simple tool to produce entanglement.

At the heart of quantum uncertainty is the superposition principle. In fact, coherent states can be written as a superposition of states with definite photon number (Fock states) weighted according to the Poisson distribution. Appropriate superpositions of more than one so-called electromagnetic mode (involving the effect of squeezing) may then lead to entangled states of light. Before we can turn to these, first we have to clarify: what is a single mode of the electromagnetic field? What does it mean quantum mechanically?

Thus, in this chapter, we will first deal with the quantisation of the electromagnetic field. Among the field observables, particular emphasis will be put on the continuous quadrature amplitudes. We will then turn to various representations of single-mode states of the quantised electromagnetic field. Next, we will deal with nonlinear interactions that lead to squeezed states of light. Finally, we will show how to treat linear optics within the framework of quantum theory.

1 QUANTISATION OF THE ELECTROMAGNETIC FIELD

In quantum optics textbooks, the electromagnetic field is ususally quantized without a rigorous quantum field theoretical approach, based on a more heuristic substitution of operators for c numbers. This approach is sufficient to identify modes of the electromagnetic field as quantum mechanical harmonic oscillators. It ultimately reveals that the number of photons in a mode corresponds to the degree of excitation of the quantum oscillator. Thus, in this sense, photons have a much more abstract and mathematical meaning than the "light particles" that Einstein 1905 referred to for interpreting the photoelectric effect.

The starting point now shall be the Maxwell equations of classical electrodynamics,

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} , \tag{I.1}$$

$$\nabla \times \mathbf{H} = \mathbf{j} + \frac{\partial \mathbf{D}}{\partial t} , \tag{I.2}$$

$$\nabla \cdot \mathbf{D} = \rho , \tag{I.3}$$

$$\nabla \cdot \mathbf{B} = 0 , \tag{I.4}$$

with $\mathbf{D} = \varepsilon_0 \mathbf{E} + \mathbf{P}$ and $\mathbf{B} = \mu_0 \mathbf{H} + \mathbf{M}$. Here, ε_0 is the electric permittivity of free space and μ_0 is the magnetic permeability (with $\varepsilon_0 \mu_0 = c^{-2}$, c the vacuum speed of light). Considering the free electromagnetic field allows us to remove all charges and currents ($\rho = 0$, $\mathbf{j} = 0$), and also any electric polarisation and magnetisation ($\mathbf{P} = 0$, $\mathbf{M} = 0$).

By inserting Eq. (I.2) with $\mathbf{H} = \mathbf{B}/\mu_0$ into Eq. (I.1), with $\mathbf{D} = \varepsilon_0 \mathbf{E}$, and with $\nabla \times \nabla \times \mathbf{E} = \nabla(\nabla \cdot \mathbf{E}) - \nabla^2 \mathbf{E}$ and Eq. (I.3), one obtains the wave equation for the electric field

$$\nabla^2 \mathbf{E} - \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} = 0 , \tag{I.5}$$

and likewise for the magnetic field.

In his quantum treatment of optical coherence, Glauber regarded the electric and magnetic field as a pair of Hermitian operators, $\hat{\mathbf{E}}(\mathbf{r},t)$ and $\hat{\mathbf{B}}(\mathbf{r},t)$, both obeying the wave equation [94]. Written as a Fourier integral, Hermiticity of the electric field operator,

$$\hat{\mathbf{E}}(\mathbf{r},t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} d\omega\, \hat{\mathcal{E}}(\mathbf{r},\omega)\, e^{-i\omega t}\,, \tag{I.6}$$

is ensured through $\hat{\mathcal{E}}(\mathbf{r},-\omega) = \hat{\mathcal{E}}^{\dagger}(\mathbf{r},\omega)$. The positive-frequency part,

$$\hat{\mathbf{E}}^{(+)}(\mathbf{r},t) = \frac{1}{\sqrt{2\pi}} \int_{0}^{\infty} d\omega\, \hat{\mathcal{E}}(\mathbf{r},\omega)\, e^{-i\omega t}\,, \tag{I.7}$$

and the negative-frequency part,

$$\begin{aligned} \hat{\mathbf{E}}^{(-)}(\mathbf{r},t) &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{0} d\omega\, \hat{\mathcal{E}}(\mathbf{r},\omega)\, e^{-i\omega t} \\ &= \frac{1}{\sqrt{2\pi}} \int_{0}^{\infty} d\omega\, \hat{\mathcal{E}}^{\dagger}(\mathbf{r},\omega)\, e^{+i\omega t}\,, \end{aligned} \tag{I.8}$$

regarded separately, are non-Hermitian operators, with $\hat{\mathbf{E}}(\mathbf{r},t) = \hat{\mathbf{E}}^{(+)}(\mathbf{r},t) + \hat{\mathbf{E}}^{(-)}(\mathbf{r},t)$. They are mutually adjoint, $\hat{\mathbf{E}}^{(-)}(\mathbf{r},t) = \hat{\mathbf{E}}^{(+)\dagger}(\mathbf{r},t)$. In fact, Glauber realized that $\hat{\mathbf{E}}^{(-)}(\mathbf{r},t)$ and $\hat{\mathbf{E}}^{(+)}(\mathbf{r},t)$ must represent photon creation and annihilation operators, respectively [94]. However, we will find it more convenient to describe the electromagnetic field by a discrete set of "mode variables" rather than the whole continuum of frequencies. We will now deal with this discretization according to Walls and Milburn [200] whose approach is based on Glauber [95].

a *Discrete single modes*

The free electromagnetic field vectors may both be determined from a vector potential $\mathbf{A}(\mathbf{r},t)$ as

$$\mathbf{B} = \nabla \times \mathbf{A}\,, \qquad \mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}\,, \tag{I.9}$$

where we have taken the Coulomb gauge condition $\nabla \cdot \mathbf{A} = 0$. Using these equations for the vector potential and the free Maxwell equations, we can also derive the wave equation for $\mathbf{A}(\mathbf{r}, t)$,

$$\nabla^2 \mathbf{A} - \frac{1}{c^2} \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0 \, . \tag{I.10}$$

The vector potential can also be written as $\mathbf{A}(\mathbf{r}, t) = \mathbf{A}^{(+)}(\mathbf{r}, t) + \mathbf{A}^{(-)}(\mathbf{r}, t)$, where again $\mathbf{A}^{(+)}(\mathbf{r}, t)$ contains all amplitudes which vary as $e^{-i\omega t}$ for $\omega > 0$ and $\mathbf{A}^{(-)}(\mathbf{r}, t)$ contains all amplitudes which vary as $e^{+i\omega t}$ [the positive and negative frequency parts here are still c numbers, $\mathbf{A}^{(-)} = (\mathbf{A}^{(+)})^*$]. In order to discretize the field variables we assume that the field is confined within a spatial volume of finite size. Now we can expand the vector potential in terms of a discrete set of orthogonal mode functions,

$$\mathbf{A}^{(+)}(\mathbf{r}, t) = \sum_k c_k \, \mathbf{u}_k(\mathbf{r}) \, e^{-i\omega_k t} . \tag{I.11}$$

The Fourier coefficients c_k are constant, because the field is free. If the volume contains no refracting materials, every vector mode function $\mathbf{u}_k(\mathbf{r})$ corresponding to the frequency ω_k satisfies the wave equation [as the mode functions must independently satisfy Eq. (I.10)]

$$\left(\nabla^2 + \frac{\omega_k^2}{c^2} \right) \mathbf{u}_k(\mathbf{r}) = 0 \, . \tag{I.12}$$

More generally, the mode functions are required to obey the transversality condition,

$$\nabla \cdot \mathbf{u}_k(\mathbf{r}) = 0 \, , \tag{I.13}$$

and they shall form a complete orthonormal set,

$$\int \mathbf{u}_k^*(\mathbf{r}) \, \mathbf{u}_{k'}(\mathbf{r}) \, d^3 r = \delta_{kk'} \, . \tag{I.14}$$

The plane wave mode functions appropriate to a cubical volume of side L may now be written as

$$\mathbf{u}_k(\mathbf{r}) = L^{-3/2} \, \mathbf{e}^{(\lambda)} \, e^{i\mathbf{k}\cdot\mathbf{r}} \, , \tag{I.15}$$

with $\mathbf{e}^{(\lambda)}$ being a unit polarisation vector [perpendicular to $\mathbf{k}$ due to transversality Eq. (I.13)]. We can verify that this choice leads with the wave equation Eq. (I.12) to the correct linear dispersion relation $|\mathbf{k}| = \omega_k/c$. The polarisation index ($\lambda = 1, 2$) and the three components of the wave vector $\mathbf{k}$ are all labelled by the mode index k. The permissible values of the components of $\mathbf{k}$ are determined in a familiar way by means of periodic boundary conditions,

$$k_x = \frac{2\pi\, n_x}{L}\,, \qquad k_y = \frac{2\pi\, n_y}{L}\,, \qquad k_z = \frac{2\pi\, n_z}{L}\,, \qquad n_x, n_y, n_z = 0, \pm 1, \pm 2, \ldots \tag{I.16}$$

The vector potential then takes the quantized form [200, 95, 140]

$$\begin{aligned} \hat{\mathbf{A}}(\mathbf{r},t) &= \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0}\right)^{1/2} [\hat{a}_k\, \mathbf{u}_k(\mathbf{r})\, e^{-i\omega_k t} + \hat{a}_k^\dagger\, \mathbf{u}_k^*(\mathbf{r})\, e^{+i\omega_k t}] \\ &= \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0 L^3}\right)^{1/2} \mathbf{e}^{(\lambda)} [\hat{a}_k\, e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}_k^\dagger\, e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}], \end{aligned} \tag{I.17}$$

where now the Fourier amplitudes c_k from Eq. (I.11) (complex numbers in the classical theory) are replaced by the operators $\hat{a}_k$ times a normalization factor. Quantisation of the electromagnetic field is accomplished by choosing $\hat{a}_k$ and $\hat{a}_k^\dagger$ to be mutually adjoint operators. The normalization factor renders dimensionless the pair of operators $\hat{a}_k$ and $\hat{a}_k^\dagger$. According to Eq. (I.9), the electric field operator becomes

$$\hat{\mathbf{E}}(\mathbf{r},t) = i \sum_k \left(\frac{\hbar\omega_k}{2\varepsilon_0}\right)^{1/2} [\hat{a}_k\, \mathbf{u}_k(\mathbf{r})\, e^{-i\omega_k t} - \hat{a}_k^\dagger\, \mathbf{u}_k^*(\mathbf{r})\, e^{+i\omega_k t}]\,, \tag{I.18}$$

and likewise the magnetic field operator

$$\hat{\mathbf{B}}(\mathbf{r},t) = i \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0}\right)^{1/2} [\hat{a}_k\, \mathbf{k} \times \mathbf{u}_k(\mathbf{r})\, e^{-i\omega_k t} - \hat{a}_k^\dagger\, \mathbf{k} \times \mathbf{u}_k^*(\mathbf{r})\, e^{+i\omega_k t}]\,. \tag{I.19}$$

Inserting these field operators into the Hamiltonian of the electromagnetic field,

$$\hat{H} = \frac{1}{2} \int \left(\varepsilon_0\, \hat{\mathbf{E}}^2 + \mu_0^{-1} \hat{\mathbf{B}}^2\right) d^3 r\,, \tag{I.20}$$

using Eq. (I.13) and Eq. (I.14), the Hamiltonian may be reduced to

$$\hat{H} = \frac{1}{2} \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \hat{a}_k \hat{a}_k^\dagger \right) . \tag{I.21}$$

With the appropriate commutation relations for the operators $\hat{a}_k$ and $\hat{a}_k^\dagger$, the bosonic commutation relations

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0 , \qquad [\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'} , \tag{I.22}$$

we recognize the Hamiltonian of an ensemble of independent quantum harmonic oscillators

$$\hat{H} = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right) . \tag{I.23}$$

The entire electromagnetic field therefore may be described by the tensor product state of all these quantum harmonic oscillators of which each represents a *single electromagnetic mode*. The operator $\hat{a}_k^\dagger \hat{a}_k$ stands for the excitation number (photon number) of mode k, $\hat{a}_k$ itself is a photon annihilation, $\hat{a}_k^\dagger$ a photon creation operator of mode k. For most quantum optical calculations, in particular with regard to a compact description of protocols in quantum information theory, it is very convenient to use this discrete single-mode picture. However, we will also encounter the situation where we are explicitly interested in the continuous frequency spectrum of "modes" that are distinct from each other in a discrete sense only with respect to spatial separation and/or polarization. Let us briefly consider such a decomposition of the electromagnetic field into a continuous set of frequency "modes".

b *Continuous set of modes*

It seems in some ways more natural to describe the electromagnetic field vectors by Fourier integrals rather than by Fourier series, although the continuous

formalism is less compact. The discrete mode expansion of the electric field in Eq. (I.18) becomes in the continuous limit [140]

$$\hat{\mathbf{E}}(\mathbf{r},t) = \frac{i}{(2\pi)^{3/2}} \sum_{\lambda} \int d^3k \left(\frac{\hbar\omega}{2\varepsilon_0}\right)^{1/2} \mathbf{e}^{(\lambda)} \times \left[\hat{a}(\mathbf{k},\lambda)\, e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} - \hat{a}^{\dagger}(\mathbf{k},\lambda)\, e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega t)}\right], \tag{I.24}$$

where the mode index k has been replaced by the discrete polarisation index λ and the three continuous wave vector components. This corresponds to the limit of a very large cube of size $L \to \infty$. The discrete expansion of the magnetic field from Eq. (I.19) becomes now [140]

$$\hat{\mathbf{B}}(\mathbf{r},t) = \frac{i}{(2\pi)^{3/2}} \sum_{\lambda} \int d^3k \left(\frac{\hbar}{2\omega\varepsilon_0}\right)^{1/2} \mathbf{k} \times \mathbf{e}^{(\lambda)} \times \left[\hat{a}(\mathbf{k},\lambda)\, e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} - \hat{a}^{\dagger}(\mathbf{k},\lambda)\, e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega t)}\right]. \tag{I.25}$$

The commutation relations in this continuous representation take the form

$$[\hat{a}(\mathbf{k},\lambda), \hat{a}(\mathbf{k}',\lambda')] = [\hat{a}^{\dagger}(\mathbf{k},\lambda), \hat{a}^{\dagger}(\mathbf{k}',\lambda')] = 0\,, \tag{I.26}$$

$$[\hat{a}(\mathbf{k},\lambda), \hat{a}^{\dagger}(\mathbf{k}',\lambda')] = \delta^3(\mathbf{k}-\mathbf{k}')\,\delta_{\lambda\lambda'}\,. \tag{I.27}$$

Note that now the photon number operator must be defined within a finite wave vector range, $\hat{a}^{\dagger}(\mathbf{k})\hat{a}(\mathbf{k})d^3k$, which means the operator $\hat{a}(\mathbf{k})$ has the dimension of $L^{3/2}$.

Finally, in terms of Glauber's continuous Fourier integral representation from Eq. (I.7), we can also write for example the electric field as [56]

$$\hat{E}^{(+)}(z,t) = [\hat{E}^{(-)}(z,t)]^{\dagger} = \frac{1}{\sqrt{2\pi}} \int_0^{\infty} d\omega \left(\frac{u\hbar\omega}{2cA_{\mathrm{tr}}}\right)^{1/2} \hat{a}(\omega)\, e^{-i\omega(t-z/c)}, \tag{I.28}$$

with $\hat{E}(z,t) = \hat{E}^{(+)}(z,t) + \hat{E}^{(-)}(z,t)$, traveling here in the positive-z direction ($|\mathbf{k}| = \omega/c$) and describing a single unspecified polarisation. The parameter A_{tr}

represents the transverse structure of the field (dimension of L^2) and u is a units-dependent constant [for the units we have used in the Maxwell equations (SI units), $u = \varepsilon_0^{-1}$, for Gaussian units, $u = 4\pi$]. Here, the photon number operator must be defined within a finite frequency range, $\hat{a}^\dagger(\omega)\hat{a}(\omega)d\omega$, which means the operator $\hat{a}(\omega)$ has the dimension of time$^{1/2}$. Compared to the discrete expansion, a phase shift of $\exp(i\pi/2)$ has been absorbed by the amplitude operator $\hat{a}(\omega)$. The correct commutation relations are now

$$[\hat{a}(\omega), \hat{a}(\omega')] = [\hat{a}^\dagger(\omega), \hat{a}^\dagger(\omega')] = 0 \,, \qquad [\hat{a}(\omega), \hat{a}^\dagger(\omega')] = \delta(\omega - \omega') \,. \tag{I.29}$$

Later, we will also make use of this finite-bandwidth quantum description of the electromagnetic field. However, in most parts of this thesis, we consider unitary transformations of discrete single modes of the *free* quantised electromagnetic field based on additional nonlinear (squeezers) and linear (beam splitters) interactions. This simplified approach will lead to interesting quantum information theoretical results, e.g., we will learn how to entangle two or more of these modes. However, one has to bear in mind that a realistic quantum description must rely on a broadband operator formalism.

c *The quantum harmonic oscillator and number states*

According to Eq. (I.23), every single mode of the electromagnetic field is described by the Hamiltonian of a quantum harmonic oscillator, $\hbar\omega_k(\hat{n}_k + \frac{1}{2})$, with the number operator $\hat{n}_k \equiv \hat{a}_k^\dagger \hat{a}_k$. The eigenstates of the number operator are the number or Fock states $|n_k\rangle$,

$$\hat{n}_k|n_k\rangle = n_k|n_k\rangle \,, \tag{I.30}$$

where $n_k = 0, 1, 2, ..., \infty$ is the excitation number of the oscillator or the photon number of the mode. Thus, the energy eigenvalues of each mode are given by the energy of the photons in that mode, $\hbar\omega_k$, times the number of photons in that mode, n_k, plus an amount of $\hbar\omega_k/2$, corresponding to the energy of the vacuum

fluctuations of that mode. The ground state of the oscillator or the vacuum state of the field mode is defined by

$$\hat{a}_k|0\rangle = 0 \; . \tag{I.31}$$

As already mentioned, $\hat{a}_k$ and $\hat{a}_k^\dagger$ are photon number annihilation and creation operators, i.e., for the harmonic oscillator's ladder of eigenstates, they play the roles of lowering and raising operators, respectively,

$$\hat{a}_k|n_k\rangle = \sqrt{n_k}\,|n_k - 1\rangle \; , \qquad \hat{a}_k^\dagger|n_k\rangle = \sqrt{n_k + 1}\,|n_k + 1\rangle \; . \tag{I.32}$$

By successive application of the creation operator, all number states may be obtained from the vacuum state

$$|n_k\rangle = \frac{\left(\hat{a}_k^\dagger\right)^{n_k}}{\sqrt{n_k!}}\,|0\rangle \; . \tag{I.33}$$

Since the number states are orthonormal [proper normalisation is ensured by the prefactors in Eq. (I.32)],

$$\langle n_k|m_k\rangle = \delta_{n_k\, m_k} \; , \tag{I.34}$$

and complete,

$$\sum_{n_k=0}^{\infty} |n_k\rangle\langle n_k| = \mathbb{1}_k \; , \tag{I.35}$$

they form a complete set of basis states ("Fock basis") for the mode's Hilbert space. From a theoretical point of view, the Fock basis is a very convenient basis and it is often used to describe single-mode quantum states for quantum information purposes. This is because the discrete Fock basis is in some sense the natural infinite-dimensional extension of the discrete-variable bases which are commonly used in quantum information theory with *finite-dimensional* Hilbert spaces (an example for this "natural" transition can be found in chapter IV where the infinite-dimensional limit of discrete-variable entanglement swapping

is considered). However, in quantum optics, the coherent-state basis is more commonly used to describe optical fields of large photon number. Coherent states (see later) symmetrically distribute their minimum uncertainty among the photon number and phase [1]. Fock states must have a completely random phase due to their certain photon number.

From an experimental point of view, dealing with Fock states is difficult. They are particularly hard to generate for large photon numbers. Detectors capable of resolving the number of absorbed photons are not available yet [2]. "Photon number displacements", i.e., adding or subtracting a certain number of photons in a mode, do not lie within the capabilities of current technology either. All these manipulations, however, are required in quantum communication protocols. This is exactly the motivation for dealing with continuous quantum variables such as the quadratures of a single mode, introduced in the next section. As opposed to the discrete photon number, those continuous quadratures can be easily and

[1] Though there is no rigorous formulation of phase in terms of Hermitian operators [195].

[2] An even greater challenge are so-called quantum non-demolition (QND) measurements that have attracted a lot of interest in the quantum optics community. In general, a QND detection aims at indirectly measuring a "QND-variable" $\hat{Q}$ of a signal through direct measurement of a probe observable after a signal-probe interaction. Ideally, the QND-variable $\hat{Q}$ is not changed by the whole process, neither by the interaction ($[\hat{Q}, \hat{H}_{\text{int}}] = 0$) nor by the free evolution ($[\hat{Q}, \hat{H}_0] = 0$). The latter makes an observable a QND-variable by guaranteeing that the increased uncertainty of the conjugate variable due to the measurement-induced collapse does not affect the subsequent evolution of the QND-variable. Applied to the photon number, an ideal QND measurement corresponds to a completely transparent detector capable of determining the photon number without absorbing any photons. In the ideal case, the outgoing state would be a Fock state with known photon number (more realistically, it would have to exhibit sub-Poissonian statistics). The resulting phase uncertainty is tolerated, because in a QND scenario, only the QND variable is of interest, whereas the conjugate variable is not relevant. By contrast, in quantum communication, often the whole quantum state is important rather than only a single observable. Hence the concept of QND measurements [54] and QND criteria [108] play just a minor role in this thesis.

efficiently manipulated in the desired way via homodyne detection and feed-forward techniques. This compensates for the mathematical complications such as singularities when dealing with continuous variables.

d Quadratures as continuous quantum variables

From the Hamiltonian of a quantum harmonic oscillator expressed in terms of 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 expressed in terms of 'position' and 'momentum' operators (unit mass),

$$\hat{H}_k = \frac{1}{2}\left(\hat{p}_k^2 + \omega_k^2 \hat{x}_k^2\right), \tag{I.36}$$

with

$$\hat{a}_k = \frac{1}{\sqrt{2\hbar\omega_k}}\left(\omega_k \hat{x}_k + i\hat{p}_k\right), \tag{I.37}$$

$$\hat{a}_k^\dagger = \frac{1}{\sqrt{2\hbar\omega_k}}\left(\omega_k \hat{x}_k - i\hat{p}_k\right), \tag{I.38}$$

or, conversely,

$$\hat{x}_k = \sqrt{\frac{\hbar}{2\omega_k}}\left(\hat{a}_k + \hat{a}_k^\dagger\right), \tag{I.39}$$

$$\hat{p}_k = -i\sqrt{\frac{\hbar\omega_k}{2}}\left(\hat{a}_k - \hat{a}_k^\dagger\right). \tag{I.40}$$

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

$$[\hat{x}_k, \hat{p}_{k'}] = i\hbar\,\delta_{kk'}, \tag{I.41}$$

which is consistent with the bosonic commutation relation $[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}$. In Eq. (I.37), 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,

$$\hat{X}_k \equiv \sqrt{\frac{\omega_k}{2\hbar}}\,\hat{x}_k = \mathrm{Re}\,\hat{a}_k, \qquad \hat{P}_k \equiv \frac{1}{\sqrt{2\hbar\omega_k}}\,\hat{p}_k = \mathrm{Im}\,\hat{a}_k. \tag{I.42}$$

Their commutation relation is then

$$[\hat{X}_k, \hat{P}_{k'}] = \frac{i}{2}\,\delta_{kk'} \,. \tag{I.43}$$

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 will always refer to these dimensionless quadratures playing the roles of 'position' and 'momentum'. Hence also* $(\hat{x}, \hat{p})$ *shall stand for a conjugate pair of dimensionsless quadratures.*

The Heisenberg uncertainty relation, expressed in terms of the variances of two arbitrary non-commuting observables $\hat{A}$ and $\hat{B}$ in an arbitrary given quantum state ($\hat{A}$ and $\hat{B}$ shall no longer be associated with the vector potential and the magnetic field),

$$\begin{aligned} \langle(\Delta\hat{A})^2\rangle &\equiv \langle(\hat{A} - \langle\hat{A}\rangle)^2\rangle = \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2 \,, \\ \langle(\Delta\hat{B})^2\rangle &\equiv \langle(\hat{B} - \langle\hat{B}\rangle)^2\rangle = \langle\hat{B}^2\rangle - \langle\hat{B}\rangle^2 \,, \end{aligned} \tag{I.44}$$

becomes [153]

$$\langle(\Delta\hat{A})^2\rangle\langle(\Delta\hat{B})^2\rangle \geq \frac{1}{4}\,|\langle[\hat{A}, \hat{B}]\rangle|^2 \,. \tag{I.45}$$

Inserting Eq. (I.43) into Eq. (I.45) yields the uncertainty relation for a pair of conjugate quadrature observables of a single mode k,

$$\hat{x}_k = (\hat{a}_k + \hat{a}_k^\dagger)/2 \,, \qquad \hat{p}_k = (\hat{a}_k - \hat{a}_k^\dagger)/2i \,, \tag{I.46}$$

namely,

$$\langle(\Delta\hat{x}_k)^2\rangle\langle(\Delta\hat{p}_k)^2\rangle \geq \frac{1}{4}\,|\langle[\hat{x}_k, \hat{p}_k]\rangle|^2 = \frac{1}{16} \,. \tag{I.47}$$

Let us further illuminate the meaning of the quadratures by looking at a single mode taken from the electric field in Eq. (I.18) for a single polarisation [phase

shift of $\exp(i\pi/2)$ absorbed by $\hat{a}_k$],

$$\hat{E}_k(\mathbf{r},t) = E_0\,[\hat{a}_k\, e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \hat{a}_k^\dagger\, e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}]\,. \tag{I.48}$$

The constant E_0 contains all the dimensional prefactors. By using Eq. (I.46), we can rewrite the mode as

$$\hat{E}_k(\mathbf{r},t) = 2E_0\,[\hat{x}_k\,\cos(\omega_k t - \mathbf{k}\cdot\mathbf{r}) + \hat{p}_k\,\sin(\omega_k t - \mathbf{k}\cdot\mathbf{r})]\,. \tag{I.49}$$

Apparently, the "position" and "momentum" operators $\hat{x}_k$ and $\hat{p}_k$ represent the in-phase and the 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

$$\hat{E}_k(\mathbf{r},t) = 2E_0\,[\hat{x}_k^{(\Theta)}\,\cos(\omega_k t - \mathbf{k}\cdot\mathbf{r} - \Theta) + \hat{p}_k^{(\Theta)}\,\sin(\omega_k t - \mathbf{k}\cdot\mathbf{r} - \Theta)]\,, \tag{I.50}$$

with the "more general" quadratures

$$\hat{x}_k^{(\Theta)} = (\hat{a}_k e^{-i\Theta} + \hat{a}_k^\dagger e^{+i\Theta})/2\,, \qquad \hat{p}_k^{(\Theta)} = (\hat{a}_k e^{-i\Theta} - \hat{a}_k^\dagger e^{+i\Theta})/2i\,. \tag{I.51}$$

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

$$\begin{pmatrix} \hat{x}_k^{(\Theta)} \\ \hat{p}_k^{(\Theta)} \end{pmatrix} = \begin{pmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{pmatrix} \begin{pmatrix} \hat{x}_k \\ \hat{p}_k \end{pmatrix}\,. \tag{I.52}$$

Since this is a unitary transformation, we again end up with a pair of conjugate observables fufilling the commutation relation Eq. (I.43). 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, as we will see in the next section. For simplicity, however, we will mostly refer 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

$$\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k = \hat{x}_k^2 + \hat{p}_k^2 - \frac{1}{2}\,, \tag{I.53}$$

using Eq. (I.43).

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

$$\hat{x}|x\rangle = x|x\rangle \ , \qquad \hat{p}|p\rangle = p|p\rangle \ , \tag{I.54}$$

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

$$\langle x|x'\rangle = \delta(x-x') \ , \qquad \langle p|p'\rangle = \delta(p-p') \ , \tag{I.55}$$

and complete,

$$\int_{-\infty}^{\infty} |x\rangle\langle x| \, dx = \mathbb{1} \ , \qquad \int_{-\infty}^{\infty} |p\rangle\langle p| \, dp = \mathbb{1} \ . \tag{I.56}$$

As it is known for position and momentum eigenstates, the quadrature eigenstates are mutually related to each other by Fourier transformation,

$$|x\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-2ixp}|p\rangle \, dp \ , \qquad |p\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{+2ixp}|x\rangle \, dx \ . \tag{I.57}$$

Remember that in our scales, these quadrature eigenstates can be obtained from the "real" position and momentum eigenstates [64] with $\hbar = 1/2$. 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 (see later) 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.

The quadrature observables introduced in this section are the principal actors and the exploitation and manipulation of their quantum properties for quantum communication purposes make the plot of this thesis.

2 Representations of the quantised electromagnetic field

In the previous sections, we have already introduced several representations for the electromagnetic field. For example, the *dynamics* of the free electromagnetic field was described in Eq. (I.18) and Eq. (I.19) by time-dependent operators, corresponding to the *Heisenberg picture*. Any change of this dynamics due to additional interactions of the single modes can be expressed in different ways. We can, for example, stick with the Heisenberg representation and unitarily transform the single modes' creation and annihilation operators, $\hat{a}^\dagger$ and $\hat{a}$. The modes' state vectors remain unchanged in this case. Alternatively, the unitary transformation may act upon the state vector (for example expanded in the number or the quadrature basis) leaving the Heisenberg operators $\hat{a}^\dagger$ and $\hat{a}$ invariant. This description is called the *Schrödinger picture*. The Heisenberg and the Schrödinger representations lead to equivalent results and which one is chosen for a particular calculation only depends on convenience. However, the evolution of the quantum states is more clearly revealed in the Schrödinger picture, whereas the evolution of particular observables is very well expressed in the Heisenberg picture.

In this section, we will give a few examples for dealing with these two representations. In addition, we will introduce a representation based on quasi-probability distributions, in particular we introduce the Wigner function. The *Wigner representation* is another alternative to describe discrete-mode quantum states, as a matter of fact a very convenient one when the continuous quadratures are the relevant observables. Furthermore, we will collect some facts about pure and mixed states in general, and coherent states and Gaussian states in particular.

a *The Heisenberg and the Schrödinger representations*

Before turning to the dynamics of quantum states and observables, let us first review some quantum mechanical postulates involving quantum states and ob-

servables independent of their evolution. A *pure* quantum state is given by a vector in Hilbert space $|\psi\rangle$, and the vector may be expanded in an arbitrary basis,

$$|\psi\rangle = \sum_m \langle m|\psi\rangle \, |m\rangle \; . \tag{I.58}$$

The basis is by definition complete,

$$\sum_m |m\rangle\langle m| = \mathbb{1} \; , \tag{I.59}$$

and by choice orthonormal,

$$\langle m|m'\rangle = \delta_{mm'} \; . \tag{I.60}$$

The complex numbers $\langle m|\psi\rangle$ are the components of the Hilbert space vector $|\psi\rangle$. When measuring an observable $\hat{M}$, the probability for obtaining the measurement result m (a *real* eigenvalue of $\hat{M}$ with eigenstate $|m\rangle$) is determined by the size of the component of $|\psi\rangle$ in direction of $|m\rangle$,

$$p_m = \frac{|\langle m|\psi\rangle|^2}{\langle\psi|\psi\rangle} \; . \tag{I.61}$$

Here,

$$\langle\psi|\psi\rangle = \sum_m \sum_{m'} \langle\psi|m\rangle \, \langle m|\langle m'|\psi\rangle \, |m'\rangle = \sum_m |\langle m|\psi\rangle|^2 \tag{I.62}$$

ensures the proper normalization, with $\langle m|\psi\rangle^* = \langle\psi|m\rangle$. Once the measurement result m has been obtained, the state vector $|\psi\rangle$ *is reduced* ("collapses") onto the corresponding eigenstate $|m\rangle$. The *overlap* $\langle\psi|\psi'\rangle$ is the scalar product of the vector space. Written in this form, its independence of a particular choice of basis [a particular decomposition as in Eq. (I.58)] becomes obvious. In fact, we might choose a particular expansion as in Eq. (I.58) for convenience, for example, because of a particular experimental setting that aims at measuring the

observable $\hat{M}$. The mean value of this observable $\hat{M}$ in the state $|\psi\rangle$ is then given by (we now assume $\langle\psi|\psi\rangle = 1$)

$$\langle\hat{M}\rangle = \sum_m p_m\, m = \sum_m m\langle\psi|m\rangle\langle m|\psi\rangle = \langle\psi|\sum_m m|m\rangle\langle m|\psi\rangle = \langle\psi|\hat{M}|\psi\rangle\ . \tag{I.63}$$

This equation reveals the *spectral decomposition* of the observable $\hat{M}$,

$$\hat{M} = \sum_m m|m\rangle\langle m|\ , \tag{I.64}$$

which is obviously a *Hermitian operator* since the eigenvalues m are real.

In contrast to pure states, *mixed states* cannot be described by Hilbert space vectors due to incomplete knowledge about the state preparation. A mixed state is a statistical mixture of pure states expressing that at least statistical information about the state preparation may exist. Such an ensemble of pure states is given by the density operator

$$\hat{\rho} = \sum_k \rho_k|\psi_k\rangle\langle\psi_k|\ . \tag{I.65}$$

As opposed to the coherent superposition in Eq. (I.58), a mixed state is sometimes called an incoherent superposition. The actual (pure) quantum state $|\psi_k\rangle$ in which the system is prepared occurs with probability ρ_k. According to this definition, we find for the overall mean value of the observable $\hat{M}$,

$$\begin{aligned}\langle\hat{M}\rangle &= \sum_k \rho_k\langle\psi_k|\hat{M}|\psi_k\rangle = \sum_m\sum_k \rho_k\langle\psi_k|\hat{M}|m\rangle\langle m|\psi_k\rangle \\ &= \sum_m \langle m|\sum_k \rho_k|\psi_k\rangle\langle\psi_k|\hat{M}|m\rangle = \mathrm{Tr}(\hat{\rho}\hat{M})\ ,\end{aligned} \tag{I.66}$$

where we have introduced the trace operation $\mathrm{Tr}(\cdots) = \sum_m \langle m|\cdots|m\rangle$ with an arbitrary basis $\{|m\rangle\}$. In the most general case, mean values of observables are given by $\mathrm{Tr}(\hat{\rho}\hat{M})$. This also applies to the uncertainty relation Eq. (I.45). What can we say about the density operator itself? It is a normalized Hermitian

operator, $\mathrm{Tr}(\hat{\rho}) = 1$, and it is nonnegative (has only nonnegative eigenvalues), because

$$\langle\phi|\hat{\rho}|\phi\rangle = \sum_k \rho_k |\langle\phi|\psi_k\rangle|^2 \geq 0 \tag{I.67}$$

for any $|\phi\rangle$.

Note that the states $|\psi_k\rangle$ in the mixture $\hat{\rho}$ need not be orthogonal to each other. Further, the mixed-state decomposition is not unique. The entanglement swapping protocol in chapter IV will be a nice example that demonstrates the subjective character of the notion of mixed states. In general, we will encounter quantum communication protocols, where the pure input states are turned into mixed output states due to imperfect resources (an imperfect resource can be either a mixed entangled state or a pure nonmaximally entangled state) or due to in principle limitations (as for instance in quantum cloning). In the Schrödinger representation, this state conversion from pure to mixed is very transparent. However, it becomes less obvious in the Heisenberg representation, where output mean values and variances are still calculated with respect to the pure input states. In the Heisenberg picture, the mixedness of the output "states" is inherent in the Heisenberg operators that change during the protocol and emerge noisier at the output.

Let us briefly discuss the unitary evolution of quantum systems [3] in the Schrödinger and the Heisenberg representation and give an example for the equivalence of both descriptions. Assuming the pure state $|\psi(t_0)\rangle$ has been prepared at time t_0, the unitarily evolved state at time $t > t_0$ can be written in the

[3] Unitary transformations of single modes due to linear-optics and nonlinear-optics interactions play a major role in this thesis. In addition, most quantum communication protocols also require nonunitary operations such as measurements (resulting in a state reduction or collapse).

Schrödinger representation as [4]

$$|\psi(t)\rangle = \hat{U}(t,t_0)\,|\psi(t_0)\rangle\ . \tag{I.68}$$

For a closed conservative system (where the Hamiltonian is time independent, $\partial\hat{H}/\partial t = 0$), the unitary operator $\hat{U}(t,t_0)$ takes on the simple form [153]

$$\hat{U}(t,t_0) = \exp\left[-\frac{i}{\hbar}\,\hat{H}\,(t-t_0)\right]\ . \tag{I.69}$$

The unitary evolution of a mixed state is easily found to be

$$\hat{\rho}(t) = \hat{U}(t,t_0)\,\hat{\rho}(t_0)\,\hat{U}^\dagger(t,t_0)\ , \tag{I.70}$$

because the probabilities ρ_k in Eq. (I.65) are time independent.

In the Heisenberg picture, the states remain unchanged during the evolution, $|\psi_H(t)\rangle \equiv |\psi_H\rangle = |\psi(t_0)\rangle$. It follows $|\psi_H\rangle = \hat{U}^\dagger(t,t_0)\,|\psi(t)\rangle$. Since we require equivalence of mean values in both representations,

$$\begin{aligned}\langle\psi_H|\hat{M}_H(t)|\psi_H\rangle &= \langle\psi(t)|\hat{U}(t,t_0)\hat{U}^\dagger(t,t_0)\hat{M}\hat{U}(t,t_0)\hat{U}^\dagger(t,t_0)|\psi(t)\rangle \\ &= \langle\psi(t)|\hat{M}|\psi(t)\rangle\ ,\end{aligned} \tag{I.71}$$

for arbitrary $|\psi_H\rangle$, we obtain

$$\hat{M}_H(t) = \hat{U}^\dagger(t,t_0)\hat{M}\hat{U}(t,t_0)\ . \tag{I.72}$$

Using this relation, one can derive the equation of motion [153]

$$\frac{d}{dt}\hat{M}_H(t) = \frac{1}{i\hbar}\,\hat{U}^\dagger[\hat{M},\hat{H}]\hat{U} + \hat{U}^\dagger\frac{\partial\hat{M}}{\partial t}\hat{U}\ , \tag{I.73}$$

or

$$i\hbar\frac{d}{dt}\hat{M}_H(t) = [\hat{M}_H,\hat{H}_H] + i\hbar\frac{\partial\hat{M}_H}{\partial t}\ . \tag{I.74}$$

[4] We always use hats on observables and unitary transformations to emphasize their operator character. When a particular matrix representation of these operators or a matrix equation equivalent to their action becomes relevant, we may drop the hats.

In general, a unitary transformation does not necessarily involve a time dependence. Especially in quantum information theory, *arbitrary* unitary transformations often are considered. The action of an arbitrary unitary operator $\hat{U}$ is then described by either $\hat{M} \to \hat{U}^\dagger \hat{M} \hat{U}$ (Heisenberg) or $\hat{\rho} \to \hat{U} \hat{\rho} \hat{U}^\dagger$ (Schrödinger). A simple example for this is a phase shift operation acting on a single mode with annihilation operator $\hat{a}$. In the Heisenberg picture, we have

$$\hat{a} \to \hat{U}^\dagger(\Theta) \hat{a} \hat{U}(\Theta) = \hat{a} \exp(-i\Theta) \,, \tag{I.75}$$

where the phase-shifting operator $\hat{U}(\Theta)$ can be expressed in terms of the photon number operator, $\hat{U}(\Theta) = \exp(-i\Theta\hat{n})$ [125]. The mean value of any observable depending on $\hat{a}$, $\hat{M} \equiv f(\hat{a})$, then becomes after the phase shift according to Eq. (I.66) [125]

$$\begin{aligned} \mathrm{Tr}\{\hat{\rho}\, f[\hat{a}\exp(-i\Theta)]\} &= \mathrm{Tr}\{\hat{\rho}\, f[\hat{U}^\dagger(\Theta)\hat{a}\hat{U}(\Theta)]\} \\ &= \mathrm{Tr}\{\hat{U}(\Theta)\hat{\rho}\hat{U}^\dagger(\Theta)\, f(\hat{a})\} \,. \end{aligned} \tag{I.76}$$

That the last equality holds can be seen by expanding the function f in powers of $\hat{a}$. The last expression in Eq. (I.76) incorporates the phase shift via the Schrödinger picture, where the state goes from $\hat{\rho}$ to $\hat{U}(\Theta)\hat{\rho}\hat{U}^\dagger(\Theta)$ and the observable $f(\hat{a})$ remains unchanged. In terms of the quadrature operators, the unitary phase shift operation reads [see Eq. (I.75) with $\hat{a} = \hat{x} + i\hat{p}$]

$$\begin{aligned} \hat{U}^\dagger(\Theta)\hat{x}\hat{U}(\Theta) = \hat{x}\cos\Theta + \hat{p}\sin\Theta &\equiv \hat{x}^{(\Theta)} \,, \\ \hat{U}^\dagger(\Theta)\hat{p}\hat{U}(\Theta) = -\hat{x}\sin\Theta + \hat{p}\cos\Theta &\equiv \hat{p}^{(\Theta)} \,, \end{aligned} \tag{I.77}$$

just as the general quadrature operators in Eq. (I.52). Later, when we treat quantum communication protocols in the Heisenberg picture, we may formulate the unitary transformations either by a matrix equation as in Eq. (I.52) or by an operator equation $\hat{x} \to \hat{x}' = \hat{U}^\dagger \hat{x} \hat{U}$ etc.

b Coherent states

We have seen that the single modes of the electromagnetic field can be expressed by Fock states describing the photon or excitation number of the corresponding quantum harmonic oscillator. However, the Fock states are not very realistic states, since they represent a perfectly determined photon number with complete quantum uncertainty of the phase. A more appropriate basis for most optical fields are the coherent states. As opposed to the Fock states, the coherent states' photon number and phase are both uncertain, but by no more than the Heisenberg uncertainty principle requires. Coherent states provide a compromise by symmetrically distributing minimum uncertainty among conjugate observables such as photon number and phase or "position" and "momentum". They are the quantum states closest to a classical description of the field. The importance of coherent states also stems from the fact that they are (ideally) the output states produced from lasers.

Coherent states are the eigenstates of the annihilation operator $\hat{a}$,

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\ . \tag{I.78}$$

Their mean photon number is given by

$$\langle\alpha|\hat{n}|\alpha\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2\ . \tag{I.79}$$

The following unitary displacement operator is very convenient, when coherent states are considered,

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}) = \exp(2ip_\alpha\hat{x} - 2ix_\alpha\hat{p})\ , \tag{I.80}$$

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

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha\ . \tag{I.81}$$

This statement can be proven by dividing the displacement α into infinitesimal steps $\delta\alpha$ and keeping only first order terms [125, 95]. For the creation operator, $\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*$ holds. Coherent states are now displaced vacuum states,

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\ , \tag{I.82}$$

which can be verified with Eq. (I.81) and Eq. (I.78),

$$\hat{a}\hat{D}(-\alpha)|\alpha\rangle = \hat{D}(-\alpha)\hat{D}^\dagger(-\alpha)\hat{a}\hat{D}(-\alpha)|\alpha\rangle = \hat{D}(-\alpha)(\hat{a}-\alpha)|\alpha\rangle = 0\ , \tag{I.83}$$

implying $\hat{D}(-\alpha)|\alpha\rangle = |0\rangle$ [with $\hat{D}(-\alpha) = D^\dagger(\alpha)$].

In order to obtain the coherent-state wave function in the position basis, $\psi_\alpha(x) \equiv \langle x|\alpha\rangle$ with $|\alpha\rangle = \int dx\langle x|\alpha\rangle|x\rangle$, we decompose the displacement operator from Eq. (I.80) into [125]

$$\hat{D}(\alpha) = \exp(-ix_\alpha p_\alpha)\exp(2ip_\alpha\hat{x})\exp(-2ix_\alpha\hat{p})\ , \tag{I.84}$$

by using a standard form of the Baker-Campbell-Hausdorff (BCH) formula [162],

$$\exp(\hat{A}+\hat{B}) = \exp(\hat{A})\exp(\hat{B})\exp(-[\hat{A},\hat{B}]/2)\ . \tag{I.85}$$

This BCH formula only requires that the two operators commute with their commutator, $[\hat{A},[\hat{A},\hat{B}]] = [\hat{B},[\hat{A},\hat{B}]] = 0$. In the position representation, the momentum operator is given by $\hat{p} = -(i/2)\partial/\partial x$. The exponential $\exp(-2ix_\alpha\hat{p}) = \exp(-x_\alpha\partial/\partial x)$ when acting on a position wave function has the effect of a displacement by x_α,

$$\exp\left(-x_\alpha\frac{\partial}{\partial x}\right)\psi(x) = \psi(x-x_\alpha)\ . \tag{I.86}$$

This can be checked by differentiating both sides with respect to x_α [125]. Since the exponential $\exp(2ip_\alpha\hat{x})$ becomes $\exp(2ip_\alpha x)$ in the position representation, and since coherent states are displaced vacua, the position wave function for coherent states reads according to Eq. (I.84)

$$\psi_\alpha(x) = \psi_0(x-x_\alpha)\exp(2ip_\alpha x - ix_\alpha p_\alpha)\ . \tag{I.87}$$

Here, $\psi_0(x)$ is the position wave function of the vacuum state. What is the vacuum wave function? We know that the annihilation operator acting on the vacuum state $|0\rangle$ yields zero. Thus, we have to solve the following differential equation [125],

$$\hat{a}\,\psi_0(x) = \left(x + \frac{1}{2}\frac{\partial}{\partial x}\right)\psi_0(x) = 0\,, \tag{I.88}$$

derived with $\hat{a} = \hat{x} + i\hat{p}$ and $\hat{p} = -(i/2)\partial/\partial x$, $\hat{x} = x$ for the position representation. The solution is

$$\psi_0(x) = \left(\frac{2}{\pi}\right)^{1/4} \exp(-x^2)\,. \tag{I.89}$$

Here, proper normalization has been taken into account, $\int |\psi_0(x)|^2 dx = 1$. The vacuum state's probability density is a Gaussian distribution,

$$|\psi_0(x)|^2 = \frac{1}{\sqrt{2\pi\sigma_x}} \exp\left(-\frac{x^2}{2\sigma_x}\right)\,, \tag{I.90}$$

with the variance σ_x. In our scales, we have

$$|\psi_0(x)|^2 = \sqrt{\frac{2}{\pi}} \exp(-2x^2)\,, \tag{I.91}$$

i.e., $\sigma_x = \int x^2 |\psi_0(x)|^2 dx = \langle 0|\hat{x}^2|0\rangle = 1/4$. Now, using Eq. (I.87), we can also write down the coherent-state position wave function,

$$\psi_\alpha(x) = \left(\frac{2}{\pi}\right)^{1/4} \exp[-(x - x_\alpha)^2 + 2ip_\alpha x - ix_\alpha p_\alpha]\,. \tag{I.92}$$

For nonzero mean values, the additional phase factors and the displacement by x_α do not affect the shape of the probability density $|\psi_\alpha(x)|^2$ compared to the vacuum state. We still have $\sigma_x = 1/4$. Analogous results are obtained in the momentum representation, with the momentum variance $\sigma_p = 1/4$. This clearly confirms that any coherent state is a minimum uncertainty state with symmetric fluctuations in $\hat{x}$ and $\hat{p}$, according to the uncertainty relation Eq. (I.47). This result holds for any pair of quadratures $\hat{x}^{(\Theta)}$ and $\hat{p}^{(\Theta)}$.

By using the BCH formula Eq. (I.85) and decomposing the creation/annihilation operator form of the displacement operator in Eq. (I.80) into

$$\hat{D}(\alpha) = \exp(-|\alpha|^2/2)\exp(\alpha\hat{a}^\dagger)\exp(-\alpha^*\hat{a}) \;, \tag{I.93}$$

we find the Fock basis expansion for coherent states,

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle \;. \tag{I.94}$$

Here, we have used the polynomial expansion of $\exp(\alpha\hat{a}^\dagger)$ with Eq. (I.33) and the fact that $\exp(-\alpha^*\hat{a})$ leaves the vacuum state $|0\rangle$ unchanged. Apparently, the photon statistics of coherent states obeys a Poisson distribution (with mean photon number $|\alpha|^2$, as we know already),

$$|\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!}\exp(-|\alpha|^2) \;. \tag{I.95}$$

Coherent states represent a very useful basis for expanding optical fields, although they are not exactly orthogonal to each other (since they are not eigenstates of a Hermitian operator). Using the Fock basis expansion from Eq. (I.94), we obtain

$$\langle\alpha|\beta\rangle = \exp(-|\alpha|^2/2 - |\beta|^2/2 + \alpha^*\beta) \;, \tag{I.96}$$

and thus

$$|\langle\alpha|\beta\rangle|^2 = \exp(-|\alpha-\beta|^2) \;. \tag{I.97}$$

Only for sufficiently large $|\alpha-\beta|$, i.e., for sufficiently different amplitudes α and β, do coherent states become approximately orthogonal. Though in general nonorthogonal, coherent states are complete [where the integration is over the whole complex plane with $d^2\alpha \equiv d(\mathrm{Re}\,\alpha)d(\mathrm{Im}\,\alpha) \equiv dx_\alpha dp_\alpha$],

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\,d^2\alpha = \mathbb{1} \;, \tag{I.98}$$

which can be proven by using Eq. (I.94) and polar coordinates in the complex plane [200]. In fact, coherent states are actually overcomplete (a consequence of their lack of orthogonality), because any coherent state can be expanded in terms of the others [179],

$$|\alpha\rangle = \frac{1}{\pi}\int d^2\beta|\beta\rangle\langle\beta|\alpha\rangle = \frac{1}{\pi}\int d^2\beta|\beta\rangle \exp(-|\alpha|^2/2 - |\beta|^2/2 + \alpha\beta^*). \quad \text{(I.99)}$$

Always when we consider a coherent state of the electromagnetic field as a whole (e.g., of a broadband field), we mean the tensor product of coherent states for the individual modes $|\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \cdots$. Let us now turn to a quantum mechanical description of the electromagnetic field that relies on "quasiprobability distributions" behaving almost but not entirely like distributions in classical probability theory.

c *Quasiprobability distributions: the Wigner representation*

In this section, we will introduce another possible way to describe the quantised electromagnetic field, the Wigner representation. Besides the Heisenberg and the Schrödinger representations, it is the third representation we will make use of to a great extent in this thesis. The Wigner function as a "quantum phase-space distribution" is particularly suitable to describe the effects on the quadrature observables which may arise from quantum theory and classical statistics. It partly behaves like a classical probability distribution thus enabling to calculate measurable quantities such as mean values and variances of the quadratures in a classical-like fashion. On the other hand, as opposed to a classical probability distribution, the Wigner function can become negative. This is one of the odd properties we have to accept when attempting to give quantum mechanics a classical interpretation.

Furthermore, such a classical-like formulation of quantum optics in terms of quasiprobability distributions is not unique. Apart from the Wigner function, there are other quasiprobability distributions. These are more suited to provide

mean values of quantities that are not as symmetric in $\hat{a}$ and $\hat{a}^\dagger$ as the quadratures. In fact, examples such as the P function and the Q function turn out to be useful tools to calculate expectation values of particular ordering in $\hat{a}$ and $\hat{a}^\dagger$.

The Wigner function was originally proposed by Wigner in his 1932 paper "On the quantum correction for thermodynamic equilibrium" [206]. 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 $\hbar = 1/2$) [206]

$$W(x,p) = \frac{2}{\pi} \int dy\, e^{+4iyp} \langle x - y|\hat{\rho}|x + y\rangle \,. \tag{I.100}$$

Here and throughout the thesis, unless otherwise specified, the integration shall 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 original equation was in N-particle form [206]), because it simplifies the understanding of the concept behind the Wigner function approach. The extension to N modes is straightforward, and later we will extensively deal with N-mode Wigner functions.

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

$$\int W(\alpha)\, d^2\alpha = 1 \,, \tag{I.101}$$

the property of yielding the correct marginal distributions,

$$\int W(x,p)\, dx = \langle p|\hat{\rho}|p\rangle \,, \qquad \int W(x,p)\, dp = \langle x|\hat{\rho}|x\rangle \,, \tag{I.102}$$

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,

$$\langle \hat{A}\rangle = \mathrm{Tr}(\hat{\rho}\hat{A}) = \int W(\alpha)\, A(\alpha)\, d^2\alpha \,, \tag{I.103}$$

with a function $A(\alpha)$ related to the operator $\hat{A}$. The measure of integration is in our case $d^2\alpha = d(\mathrm{Re}\,\alpha)d(\mathrm{Im}\,\alpha) = dx\, dp$ with $W(\alpha = x + ip) \equiv W(x,p)$, and we

will use $d^2\alpha$ and $dx\,dp$ 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. (I.57), that for x, $\langle x|\hat{\rho}|x\rangle$, by using $\int \exp(+4iyp)dp = (\pi/2)\delta(y)$. The normalisation of the Wigner function then follows from $\mathrm{Tr}(\hat{\rho}) = 1$. In order to derive an equation of the form of Eq. (I.103), we can write the Wigner function from Eq. (I.100) as [5]

$$\begin{aligned} W(x,p) &= \frac{2}{\pi}\int dy\,dx'\,e^{+4iyp}\,\delta(x-x')\,\langle x'-y|\hat{\rho}|x'+y\rangle \\ &= \frac{1}{\pi^2}\int dx'du\,dv\,e^{+2iu(x-x')+2ivp}\,\left\langle x'-\frac{v}{2}\right|\hat{\rho}\left|x'+\frac{v}{2}\right\rangle \\ &= \frac{1}{\pi^2}\int \chi_s(u,v)\,e^{+2iux+2ivp}\,du\,dv\,, \end{aligned} \tag{I.104}$$

with the Fourier transform of the Wigner function, called the characteristic function,

$$\chi_s(u,v) = \int W(x,p)\,e^{-2iux-2ivp}\,dx\,dp \tag{I.105}$$

$$= \int e^{-2iux'}\,\left\langle x'-\frac{v}{2}\right|\hat{\rho}\left|x'+\frac{v}{2}\right\rangle\,dx'\,. \tag{I.106}$$

With the substitution $x = x' - v/2$ in Eq. (I.106), we obtain now

$$\begin{aligned} \chi_s(u,v) &= \exp(-iuv)\int \exp(-2iux)\,\langle x|\hat{\rho}|x+v\rangle\,dx \\ &= \int \langle x|\hat{\rho}\,\exp(-2iu\hat{x}-2iv\hat{p})|x\rangle\,dx\,, \end{aligned} \tag{I.107}$$

where in the last line we have used the BCH formula,

$$\exp(-2iu\hat{x}-2iv\hat{p}) = \exp(+iuv)\exp(-2iu\hat{x})\exp(-2iv\hat{p})\,, \tag{I.108}$$

and according to Eq. (I.57), $\exp(-2iv\hat{p})|x\rangle = |x+v\rangle$, and $\exp(-2iu\hat{x})|x+v\rangle = \exp[-2iu(x+v)]|x+v\rangle$. With Eq. (I.107), we have found a compact formula for

[5] Throughout the thesis, we will indicate integration over more than one variable only by the multiple differentials and we will omit the multiple integrals. For example, in Eq. (I.104), $\int dx'du\,dv \equiv \int\int\int dx'du\,dv$.

the characteristic function,

$$\chi_s(u,v) = \mathrm{Tr}[\hat{\rho}\,\exp(-2iu\hat{x} - 2iv\hat{p})]\,. \tag{I.109}$$

Let us now calculate the following expectation value [125],

$$\begin{aligned}\mathrm{Tr}[\hat{\rho}\,(\lambda\hat{x}+\mu\hat{p})^k] &= \left(\frac{i}{2}\right)^k \frac{\partial^k}{\partial\xi^k}\,\chi_s(\lambda\xi,\mu\xi)\Big|_{\xi=0} \\ &= \int W(x,p)\,(\lambda x+\mu p)^k\,dx\,dp\,,\end{aligned} \tag{I.110}$$

according to Eq. (I.109) (in the first line) and Eq. (I.105) (in the second line). By comparison of the powers of λ and μ, we find [125]

$$\mathrm{Tr}[\hat{\rho}\,\mathcal{S}(\hat{x}^n\hat{p}^m)] = \int W(x,p)\,x^n p^m\,dx\,dp\,, \tag{I.111}$$

where $\mathcal{S}(\hat{x}^n\hat{p}^m)$ 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 [125]. This is the so-called Weyl correspondence [205]. It provides a rule how to calculate quantum mechanical expectation values in a classical-like fashion as in Eq. (I.103). Apparently, any symmetrized operator belongs to the particular class of operators $\hat{A}$ in Eq. (I.103) for which the classical-like averaging procedure works. In terms of creation and annihilation operators, we have

$$\mathrm{Tr}[\hat{\rho}\,\mathcal{S}(\hat{a}^{\dagger n}\hat{a}^m)] = \int W(\alpha)\,\alpha^{*n}\alpha^m\,d^2\alpha\,. \tag{I.112}$$

This correspondence can be similarly derived as above by expressing the characteristic function in terms of complex variables [6],

$$\begin{aligned}\chi_s(\beta) &= \int W(\alpha)\,\exp(-i\beta\alpha^* - i\beta^*\alpha)\,d^2\alpha \\ &= \mathrm{Tr}[\hat{\rho}\,\exp(-i\beta\hat{a}^\dagger - i\beta^*\hat{a})]\,,\end{aligned} \tag{I.113}$$

[6] Some authors use a different Fourier transformation, $\chi_s(\beta) = \int W(\alpha)\exp(\beta\alpha^* - \beta^*\alpha)d^2\alpha = \int W(x,p)\exp(2ivx - 2iup)dx\,dp$, and correspondingly $\chi_s(\beta) = \mathrm{Tr}[\hat{\rho}\hat{D}(\beta)] = \mathrm{Tr}[\hat{\rho}\exp(2iv\hat{x} - 2iu\hat{p})]$, with the displacement operator from Eq. (I.80) [200].

with $\beta = u + iv$.

Are there possibly any other quasiprobability distributions that provide quantum mechanical expectation values of nonsymmetrized operators in a classical-like fashion? Indeed, the mean values of operators normally and antinormally ordered in $\hat{a}$ and $\hat{a}^\dagger$ can be calculated via the so-called P function and Q function, respectively. Normal ordering refers to operators of the form $\hat{a}^{\dagger n}\hat{a}^m$ and the expectation values become

$$\begin{aligned} \mathrm{Tr}(\hat{\rho}\,\hat{a}^{\dagger n}\hat{a}^m) &= i^{n+m}\frac{\partial^n}{\partial\beta^n}\frac{\partial^m}{\partial\beta^{*m}}\,\chi_n\Big|_{\beta=\beta^*=0} \\ &= \int P(\alpha)\,\alpha^{*n}\alpha^m\,d^2\alpha\,, \end{aligned} \tag{I.114}$$

with a normally ordered characteristic function,

$$\begin{aligned} \chi_n(\beta) &= \int P(\alpha)\,\exp(-i\beta\alpha^* - i\beta^*\alpha)\,d^2\alpha \\ &= \mathrm{Tr}[\hat{\rho}\,\exp(-i\beta\hat{a}^\dagger)\exp(-i\beta^*\hat{a})]\,. \end{aligned} \tag{I.115}$$

Consequently, antinormal ordering means operators such as $\hat{a}^n\hat{a}^{\dagger m}$, where

$$\begin{aligned} \mathrm{Tr}(\hat{\rho}\,\hat{a}^n\hat{a}^{\dagger m}) &= i^{n+m}\frac{\partial^n}{\partial\beta^{*n}}\frac{\partial^m}{\partial\beta^m}\,\chi_a\Big|_{\beta=\beta^*=0} \\ &= \int Q(\alpha)\,\alpha^n\alpha^{*m}\,d^2\alpha\,, \end{aligned} \tag{I.116}$$

with an antinormally ordered characteristic function,

$$\begin{aligned} \chi_a(\beta) &= \int Q(\alpha)\,\exp(-i\beta\alpha^* - i\beta^*\alpha)\,d^2\alpha \\ &= \mathrm{Tr}[\hat{\rho}\,\exp(-i\beta^*\hat{a})\exp(-i\beta\hat{a}^\dagger)]\,. \end{aligned} \tag{I.117}$$

The Wigner characteristic function $\chi_s(\beta)$ is correspondingly a symmetrized characteristic function [see Eq. (I.113)].

By applying the BCH formula to the characteristic functions, and utilizing the fact that the Fourier transform of a product of functions is the convolution of the Fourier-transformed functions (and that a Fourier-transformed Gaussian

is a Gaussian with inverse width), we find the following relations:

$$W(\alpha) = \frac{2}{\pi}\int d^2\beta\, P(\beta)\, e^{-2|\alpha-\beta|^2}\,, \tag{I.118}$$

$$\begin{aligned} Q(\alpha) &= \frac{2}{\pi}\int d^2\beta\, W(\beta)\, e^{-2|\alpha-\beta|^2} \\ &= \frac{1}{\pi}\int d^2\beta\, P(\beta)\, e^{-|\alpha-\beta|^2}\,. \end{aligned} \tag{I.119}$$

We see that the Wigner function is a convolution of the P function with a Gaussian of one vacuum unit. The Q function is a convolution of the Wigner function with a Gaussian of one vacuum unit, or consequently a convolution of the P function with a Gaussian of two vacuum units. This may explain why the Q function is the most regular and the P function the most singular quasiprobability distribution.

Historically, the P function was first proposed independently by Glauber and Sudarshan [93, 194] (that is why the P function is sometimes called Glauber-Sudarshan function) in the form

$$\hat{\rho} = \int P(\alpha)\, |\alpha\rangle\langle\alpha|\, d^2\alpha\,. \tag{I.120}$$

In this form, $P(\alpha)$ seems to perfectly resemble a classical distribution over coherent states. However, $P(\alpha)$ can become negative and hence nonclassical. The P function of a coherent state $|\alpha_0\rangle$ becomes highly singular, $P(\alpha) = \delta(\alpha - \alpha_0)$. According to Eq. (I.119), Eq. (I.97), and Eq. (I.120), the Q function can be written in a very convenient form,

$$\begin{aligned} Q(\alpha) &= \frac{1}{\pi}\int d^2\beta\, P(\beta)\, e^{-|\alpha-\beta|^2} \\ &= \frac{1}{\pi}\int d^2\beta\, P(\beta)\, |\langle\alpha|\beta\rangle|^2 = \frac{1}{\pi}\,\langle\alpha|\hat{\rho}|\alpha\rangle\,. \end{aligned} \tag{I.121}$$

The Q function is nonnegative, because $\hat{\rho}$ is a nonnegative operator. Later, we will use the above form of $Q(\alpha)$ to calculate the quality of quantum teleportation (given by the "fidelity"). Furthermore, the Q function quantifies the attempt of

determining a quantum state through a measurement, for example through the simultaneous detection of the x and the p quadrature of a single mode [5, 125]. The distribution of the measurement results in this case does not reproduce the actual quantum state (given by the Wigner function), but rather a randomized version of the state (given by the Q function, i.e., the Wigner function convoluted with a one-vacuum Gaussian). This issue will be relevant to "classical teleportation".

Wigner called $W(x,p)$ "the probability-function of the simultaneous values of x $[x_1, x_2, ...]$ for the coordinates and p $[p_1, p_2, ...]$ for the momenta" [206]. Since position and momentum cannot simultaneously take on precise values, we anticipate that $W(x,p)$ reveals some odd properties. In fact, the overlap formula [125]

$$|\langle\psi_1|\psi_2\rangle|^2 = \pi \int W_1(x,p)\, W_2(x.p)\, dx\, dp \tag{I.122}$$

shows that either $W_1(x,p)$ or $W_2(x,p)$ must become negative for orthogonal states $\langle\psi_1|\psi_2\rangle = 0$. For example, Wigner functions of Fock states are negative [200]. In fact, the only pure states with nonnegative Wigner functions are Gaussian states (see next section) [172]. Later, we may use Eq. (I.122) (in a more general form, $\langle\psi_1|\hat{\rho}_2|\psi_1\rangle$) to calculate teleportation fidelities.

Finally, by inserting the vacuum wave function Eq. (I.89) into Wigner's formula Eq. (I.100), we obtain the Wigner function for the vacuum state,

$$W(x,p) = \frac{2}{\pi} \exp(-2x^2 - 2p^2)\ , \tag{I.123}$$

a Gaussian probability distribution with variances $\sigma_x = \sigma_p = 1/4$ (or complex variance $\sigma = 1/2$). We have seen that the coherent-state wave function is not simply the displaced vacuum wave function, but the coherent-state probability density is indeed the displaced vacuum probability density. The latter also applies to the coherent-state Wigner function. In general, displaced quantum states, $\hat{D}(\alpha_0)\hat{\rho}\hat{D}^\dagger(\alpha_0)$ with $\alpha_0 = x_0 + ip_0$, turn out to be described by displaced Wigner functions according to Wigner's formula, $W(x,p) \to W(x - x_0, p - p_0)$. Thus,

the coherent-state Wigner function is the displaced vacuum Wigner function,

$$W(x,p) = \frac{2}{\pi} \exp[-2(x-x_0)^2 - 2(p-p_0)^2] \,. \tag{I.124}$$

The Wigner function, though not always positive definite, appears to be a good compromise to describe quantum states in terms of quantum phase-space variables such as the single-mode quadratures. We will 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 they are posititve definite. In fact, they belong to the class of Gaussian states which we consider next.

d Gaussian states

The Gaussian states relevant to the following investigations in quantum communication are "multipartite" (multi-mode) states with zero mean. The corresponding Wigner function is then a normalized Gaussian distribution of the form

$$W(\boldsymbol{\xi}) = \frac{1}{(2\pi)^N \sqrt{\det \mathbf{V}^{(\mathbf{N})}}} \exp\left\{ -\frac{1}{2} \boldsymbol{\xi} \left[\mathbf{V}^{(\mathbf{N})}\right]^{-1} \boldsymbol{\xi}^T \right\} \,, \tag{I.125}$$

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

$$\boldsymbol{\xi} = (x_1, p_1, x_2, p_2, ..., x_N, p_N) \,, \qquad \hat{\boldsymbol{\xi}} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, ..., \hat{x}_N, \hat{p}_N) \,, \tag{I.126}$$

and with the $2N \times 2N$ correlation matrix $\mathbf{V}^{(\mathbf{N})}$ having as its elements the second moments symmetrized according to the Weyl correspondence Eq. (I.111),

$$\begin{aligned} \mathrm{Tr}[\hat{\rho}\,(\Delta\hat{\xi}_i \Delta\hat{\xi}_j + \Delta\hat{\xi}_j \Delta\hat{\xi}_i)/2] &= \langle (\hat{\xi}_i \hat{\xi}_j + \hat{\xi}_j \hat{\xi}_i)/2 \rangle \\ &= \int W(\boldsymbol{\xi})\, \xi_i \xi_j \, d^{2N}\xi = V_{ij}^{(N)} \,, \end{aligned} \tag{I.127}$$

where $\Delta\hat{\xi}_i = \hat{\xi}_i - \langle \hat{\xi}_i \rangle = \hat{\xi}_i$ for zero mean values. The last equality defines the correlation matrix for any quantum state, but for Gaussian states of the

form Eq. (I.125), the Wigner function is completely determined by the second-moment correlation matrix. Conversely, given a Gaussian Wigner function, we may directly extract the correlation matrix. The simplest example is of course the vacuum Wigner function of a single mode from Eq. (I.123) with $V_{11}^{(1)} = \sigma_x = 1/4$, $V_{22}^{(1)} = \sigma_p = 1/4$, and $V_{12}^{(1)} = V_{21}^{(1)} = 0$.

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. (I.43) [188, 204],

$$[\hat{\xi}_k, \hat{\xi}_l] = \frac{i}{2}\Lambda_{kl}\,, \qquad k,l = 1,2,3,...,2N\,, \tag{I.128}$$

with the $2N \times 2N$ matrix Λ having the 2×2 matrix J as diagonal entry for each quadrature pair, for example for $N = 2$, [7]

$$\Lambda = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}\,, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\,. \tag{I.129}$$

A direct consequence of this commutation relation and the non-negativity of the density operator $\hat{\rho}$ is the following N-mode uncertainty relation [188, 204],

$$V^{(N)} + \frac{i}{4}\Lambda \geq 0\,. \tag{I.130}$$

This matrix equation means that the matrix sum on the left-hand-side has only nonnegative 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 it is also sufficient to ensure the positivity of $\hat{\rho}$ [204]. In the simplest case $N = 1$, Eq. (I.130) is

[7] In general, we do not indicate matrices by bold print, unless their matrix character is not obvious or needs to be emphasized.

reduced to the statement $\det V^{(1)} \geq 1/16$, which is a more precise and complete version of the Heisenberg uncertainty relation in Eq. (I.47). For any N, Eq. (I.130) becomes exactly the Heisenberg uncertainty relation of Eq. (I.47) for each individual mode, if $V^{(N)}$ is diagonal.

e *Distinction of pure and mixed states*

In a previous section, we introduced pure states as vectors in Hilbert space and mixed states as statistical ensembles of pure states. How can we generally discriminate between purity and mixedness, given an arbitrary density operator or Wigner function?

By writing the density operator of Eq. (I.65) in its eigenbasis, we find

$$\mathrm{Tr}(\hat{\rho}^2) = \sum_k \rho_k^2 \leq \sum_k \rho_k = 1 \; . \tag{I.131}$$

Equality, $\mathrm{Tr}(\hat{\rho}^2) = 1$, holds only for pure states. Therefore, any state that satisfies $\mathrm{Tr}(\hat{\rho}^2) < 1$ reveals its mixedness. This condition can be translated into the Wigner representation, and for one mode it reads [125],

$$\mathrm{Tr}(\hat{\rho}^2) = \pi \int W^2(x,p)\, dxdp \leq 1 \; , \tag{I.132}$$

where $W(x,p)$ is the Wigner function corresponding to $\hat{\rho}$. Another option is to calculate the von Neumann entropy,

$$E_{\mathrm{v.N.}} = -\mathrm{Tr}\hat{\rho}\log\hat{\rho} \; . \tag{I.133}$$

It becomes nonzero for any mixed state and vanishes for pure states. Later, the von Neumann entropy will be particularly relevant as an entanglement measure.

For Gaussian Wigner functions, a very useful way to distinguish between pure and mixed states relies on their correlation matrix. Minimum uncertainty states, namely coherent states and squeezed states (see next section), are pure. Intuitively, we expect that equality in the Heisenberg uncertainty relation of

Eq. (I.47) is necessary for a state to be pure. But only for simple Gaussian states such as coherent or squeezed states is this requirement also sufficient for purity. In fact, for Gaussian N-mode states, a necessary and sufficient purity condition is that the matrix sum in Eq. (I.130), $V^{(N)} + (i/4)\Lambda$, has a maximal number of null eigenvectors or, in other words, the null space $\{\mathbf{e}|[V^{(N)} + (i/4)\Lambda]\mathbf{e} = 0\}$ has dimension N [204]. Let us recast this statement for a particular form of the correlation matrix (of a zero-mean Gaussian state) that will be relevant later, namely

$$V^{(N)} = \frac{1}{4}\begin{pmatrix} a_1 & 0 & c & 0 & c & 0 & \cdots \\ 0 & b_1 & 0 & d & 0 & d & \cdots \\ c & 0 & a_2 & 0 & c & 0 & \cdots \\ 0 & d & 0 & b_2 & 0 & d & \cdots \\ c & 0 & c & 0 & a_3 & 0 & \cdots \\ 0 & d & 0 & d & 0 & b_3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} . \tag{I.134}$$

By rearranging this matrix into a form $\tilde{V}^{(N)}$ satisfying

$$\langle(\hat{\xi}'_i\hat{\xi}'_j + \hat{\xi}'_j\hat{\xi}'_i)/2\rangle = \int W(\boldsymbol{\xi}')\,\xi'_i\xi'_j\,d^{2N}\xi' = \tilde{V}^{(N)}_{ij} , \tag{I.135}$$

with

$$\boldsymbol{\xi}' = (x_1, x_2, ..., x_N, p_1, p_2, ..., p_N),\ \hat{\boldsymbol{\xi}}' = (\hat{x}_1, \hat{x}_2, ..., \hat{x}_N, \hat{p}_1, \hat{p}_2, ..., \hat{p}_N), \tag{I.136}$$

we obtain for $\tilde{V}^{(N)}$ the block form

$$\tilde{V}^{(N)} = \frac{1}{4}\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} , \tag{I.137}$$

with the $N \times N$ matrices

$$A = \begin{pmatrix} a_1 & c & c & \cdots \\ c & a_2 & c & \cdots \\ c & c & a_3 & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} , \quad B = \begin{pmatrix} b_1 & d & d & \cdots \\ d & b_2 & d & \cdots \\ d & d & b_3 & \cdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix} , \tag{I.138}$$

for which the purity condition reads $A\,B = \mathbb{1}$ [189]. For example, for $a = a_1 = a_2 = \cdots$, and $b = b_1 = b_2 = \cdots$, we have

$$ab + (N-1)\,cd = 1\,, \qquad ad + bc + (N-2)\,cd = 0\,. \tag{I.139}$$

After having discussed various representations for the quantum states of the electromagnetic field, let us now in the remaining sections of this chapter turn to the manipulation of quantised light fields via nonlinear and linear optics.

3 Nonlinear optics with the quantised field

An important ingredient of most 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, one needs nonlinear optics. The subject of this section is therefore: what kind of nonlinear processes lead to squeezed light? What are the differences between the "squeezed states" that emerge from different processes? What do they have in common?

The relevant nonlinear processes are accomplished via the interaction of electromagnetic modes in a nonlinear medium. In classical nonlinear optics, the response of a nonmagnetic medium to an external light field may be described by a nonzero polarisation $\mathbf{P}$ in the Maxwell equations Eq. (I.2) and Eq. (I.3) (with again $\rho = 0$, $\mathbf{j} = 0$, and $\mathbf{M} = 0$, where ρ must not be confused with a quantum density matrix). By inserting Eq. (I.2) with $\mathbf{H} = \mathbf{B}/\mu_0$ into Eq. (I.1), with $\mathbf{D} = \varepsilon_0\mathbf{E} + \mathbf{P}$, and with $\nabla \times \nabla \times \mathbf{E} = \nabla(\nabla \cdot \mathbf{E}) - \nabla^2\mathbf{E}$, one obtains instead of the free wave equation Eq. (I.5) now

$$\nabla^2\mathbf{E} - \nabla(\nabla \cdot \mathbf{E}) - \frac{1}{c^2}\frac{\partial^2\mathbf{E}}{\partial t^2} = \mu_0\frac{\partial^2\mathbf{P}}{\partial t^2}\,. \tag{I.140}$$

The components of $\mathbf{P}$, P_i with $i = x, y, z$, can be expressed in terms of the

external electric field components E_i via the phenomenological relation [145]

$$\begin{aligned} P_i(\mathbf{r},t) &= P_i^{(0)} + \sum_j \chi_{ij}^{(1)} E_j(\mathbf{r},t) + \sum_{jk} \chi_{ijk}^{(2)} E_j(\mathbf{r},t) E_k(\mathbf{r},t) \\ &\quad + \sum_{jkl} \chi_{ijkl}^{(3)} E_j(\mathbf{r},t) E_k(\mathbf{r},t) E_l(\mathbf{r},t) + \cdots , \end{aligned} \tag{I.141}$$

or assuming $P_i^{(0)} = 0$ simply

$$\mathbf{P} = \varepsilon_0(\boldsymbol{\chi}^{(1)} \cdot \mathbf{E} + \boldsymbol{\chi}^{(2)} : \mathbf{EE} + \boldsymbol{\chi}^{(3)} \vdots \mathbf{EEE} + \cdots) . \tag{I.142}$$

Here, the nth order susceptibilities $\boldsymbol{\chi}^{(n)}$ are given by tensors of rank $n+1$. The linear susceptibility $\boldsymbol{\chi}^{(1)}$ is the dominant term in Eq. (I.142). If the electric field is linearly polarised, say in x direction, and the induced polarisation of the medium has only one nonzero component P_x, the susceptibility tensors can be replaced by scalars, $\chi_{xx}^{(1)} \equiv \chi^{(1)}$, $\chi_{xxx}^{(2)} \equiv \chi^{(2)}$, etc.

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. The various schemes for the generation of squeezed light rely on different kinds of nonlinearity and these schemes may differ in other aspects as well. We will briefly discuss their characteristics, first for the schemes involving a $\chi^{(2)}$ interaction, and then for those based on a $\chi^{(3)}$ nonlinearity (for a review on squeezing experiments, in particular those using the $\chi^{(3)}$ nonlinearity in an optical fiber, see Sizmann [191]).

a *Squeezing via the* $\boldsymbol{\chi}^{(2)}$ *interaction*

In an optical parametric amplifier (OPA), a pump beam produces signal and idler beams by interacting with a $\chi^{(2)}$ nonlinearity. We will later in chapter III focus on the nondegenerate optical parametric amplifier (NOPA), where the two outgoing beams emerge at two sidebands around half the pump frequency ($\omega_{\text{pump}} = \omega_{\text{signal}} + \omega_{\text{idler}}$) and have different polarisation. This leads to two-mode

squeezing, later desribed in a more realistic broadband picture. The output state of degenerate parametric amplification, where the signal and idler frequencies both equal half the pump frequency ($\omega_{\text{signal}} = \omega_{\text{idler}}$), 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,

$$\hat{H}_{\text{int}} = i\hbar\frac{\kappa}{2}\left(\hat{a}^{\dagger 2}e^{i\Theta} - \hat{a}^2 e^{-i\Theta}\right) . \tag{I.143}$$

It 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, $\kappa \propto \chi^{(2)}|\alpha_{\text{pump}}|$. [8]

In the interaction picture, we can insert $\hat{H}_{\text{int}}$ into the Heisenberg equation of motion Eq. (I.74) for the annihilation operator, and obtain (taking zero pump phase $\Theta = 0$)

$$\frac{d}{dt}\hat{a}(t) = \frac{1}{i\hbar}\left[\hat{a}(t), \hat{H}_{\text{int}}\right] = \kappa\,\hat{a}^{\dagger}(t) . \tag{I.144}$$

This equation is solved by

$$\hat{a}(t) = \hat{a}(0)\,\cosh(\kappa t) + \hat{a}^{\dagger}(0)\,\sinh(\kappa t) . \tag{I.145}$$

The quadrature operators evolve correspondingly into

$$\hat{x}(t) = e^{+\kappa t}\,\hat{x}(0) , \qquad \hat{p}(t) = e^{-\kappa t}\,\hat{p}(0) . \tag{I.146}$$

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:

$$\langle[\Delta\hat{x}(t)]^2\rangle = e^{+2\kappa t}\,\langle[\Delta\hat{x}^{(0)}]^2\rangle , \qquad \langle[\Delta\hat{p}(t)]^2\rangle = e^{-2\kappa t}\,\langle[\Delta\hat{p}^{(0)}]^2\rangle . \tag{I.147}$$

[8] The fully quantum mechanical Hamiltonian is $\hat{H}_{\text{int}} \propto \hat{a}^{\dagger 2}\hat{a}_{\text{pump}} - \hat{a}^2\hat{a}^{\dagger}_{\text{pump}}$, and with the parametric approximation we assume $\hat{a}_{\text{pump}} \to \alpha_{\text{pump}} = |\alpha_{\text{pump}}|e^{i\Theta}$ [179].

Here we have chosen coherent-state or vacuum-state inputs and replaced the initial quadratures by those of the vacuum, labelled by a superscript '(0)'. These 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 Eq. (I.69) with the Hamiltonian from Eq. (I.143) and $t_0 = 0$, let us now introduce the unitary squeezing 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, the minus sign is the usual convention),

$$\begin{aligned} \hat{U}(t,0) &= \exp\left[\frac{\kappa}{2}\left(\hat{a}^{\dagger 2} e^{i\Theta} - \hat{a}^2 e^{-i\Theta}\right) t\right] \\ &\equiv \hat{S}(\zeta) = \exp\left(\frac{\zeta^*}{2}\,\hat{a}^2 - \frac{\zeta}{2}\,\hat{a}^{\dagger 2}\right) . \end{aligned} \tag{I.148}$$

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 [Eq. (I.72)]

$$\begin{aligned} \hat{S}^\dagger(\zeta)\hat{a}\hat{S}(\zeta) &= \hat{a}\cosh r - \hat{a}^\dagger e^{i\Theta}\sinh r\,, \\ \hat{S}^\dagger(\zeta)\hat{a}^\dagger\hat{S}(\zeta) &= \hat{a}^\dagger\cosh r - \hat{a}e^{-i\Theta}\sinh r\,. \end{aligned} \tag{I.149}$$

For the rotated mode

$$\hat{x}^{(\Theta/2)} + i\hat{p}^{(\Theta/2)} = (\hat{x} + i\hat{p})\, e^{-i\Theta/2} = \hat{a}\, e^{-i\Theta/2}\,, \tag{I.150}$$

the squeezing transformation results in

$$\begin{aligned} \hat{S}^\dagger(\zeta)[\hat{x}^{(\Theta/2)} + i\hat{p}^{(\Theta/2)}]\hat{S}(\zeta) &= \hat{a}\, e^{-i\Theta/2}\cosh r - \hat{a}^\dagger\, e^{+i\Theta/2}\sinh r \\ &= e^{-r}\,\hat{x}^{(\Theta/2)} + i\, e^{+r}\,\hat{p}^{(\Theta/2)}\,. \end{aligned} \tag{I.151}$$

Thus, the effect of the squeezing operator on an arbitrary pair of quadratures, as generally defined in Eq. (I.51), 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 OPA Hamiltonian. The corresponding

expressions for the resulting Heisenberg quadrature operators (with $\Theta = 0$ and *vacuum inputs*),

$$\hat{x}(r) = e^{-r}\,\hat{x}^{(0)}\,, \qquad \hat{p}(r) = e^{+r}\,\hat{p}^{(0)}\,, \tag{I.152}$$

will prove extremely useful for the following investigations. Comparing Eq. (I.146) with Eq. (I.152), note that the time reversal due to the sign convention in $r \equiv -\kappa t$ just swaps the squeezed and the antisqueezed quadrature. The quadrature squeezing, mathematically defined through the squeezing operator $\hat{S}(\zeta)$ and physically associated with the OPA interaction, is commonly referred to as "ordinary" squeezing. Other sorts of squeezing will be briefly mentioned in the next section. The Heisenberg equations Eq. (I.152) 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,

$$|\alpha, \zeta\rangle = \hat{D}(\alpha)\hat{S}(\zeta)|0\rangle\,, \tag{I.153}$$

for which the position wave function becomes

$$\psi(x) = \left(\frac{2}{\pi}\right)^{1/4} e^{r/2} \exp[-e^{2r}(x - x_\alpha)^2 + 2ip_\alpha x - ix_\alpha p_\alpha]\,. \tag{I.154}$$

The corresponding Wigner function is

$$W(x,p) = \frac{2}{\pi} \exp[-2e^{+2r}(x - x_\alpha)^2 - 2e^{-2r}(p - p_\alpha)^2]. \tag{I.155}$$

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, $|\psi(x)|^2 = \sqrt{2/\pi}\,e^r \times \exp[-2e^{2r}(x - x_\alpha)^2]$ beomes a delta function $\lim_{\epsilon\to 0} \exp[-(x - x_\alpha)^2/\epsilon^2]/\epsilon\sqrt{\pi} = \delta(x - x_\alpha)$ with $\epsilon = e^{-r}/\sqrt{2}$. For example, the squeezed vacuum wave function in that limit, $\psi(x) \propto \delta(x)$, describes a zero position eigenstate, $\int \psi(x)|x\rangle \propto |0\rangle$. Infinite-squeezing eigenstates may be useful for quantum communication protocols in an idealized approach. The mean photon number of an infinitely

squeezed state becomes infinite, because for the displaced squeezed vacuum we have

$$\langle \hat{n} \rangle = \langle \hat{x}^2 \rangle + \langle \hat{p}^2 \rangle - \frac{1}{2} = |\alpha|^2 + \sinh^2 r \ , \tag{I.156}$$

using Eq. (I.53).

Later, we will 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, nondegenerate optical parametric amplification, is a generalization of the nonlinear interaction involved in degenerate optical parametric amplification. The NOPA interaction relies on the Hamiltonian

$$\hat{H}_{\rm int} = i\hbar\kappa \left(\hat{a}_1^\dagger \hat{a}_2^\dagger e^{i\Theta} - \hat{a}_1 \hat{a}_2 e^{-i\Theta} \right) , \tag{I.157}$$

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

$$\begin{aligned} \hat{U}(t,0) &= \exp\left[\kappa \left(\hat{a}_1^\dagger \hat{a}_2^\dagger e^{i\Theta} - \hat{a}_1 \hat{a}_2 e^{-i\Theta} \right) t \right] \\ &\equiv \hat{S}(\zeta) = \exp\left(\zeta^* \, \hat{a}_1 \hat{a}_2 - \zeta \, \hat{a}_1^\dagger \hat{a}_2^\dagger \right) \ , \end{aligned} \tag{I.158}$$

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

$$\begin{aligned} \hat{a}_1(r) &= \hat{a}_1 \cosh r - \hat{a}_2^\dagger \sinh r \ , \\ \hat{a}_2(r) &= \hat{a}_2 \cosh r - \hat{a}_1^\dagger \sinh r \ . \end{aligned} \tag{I.159}$$

These output modes are entangled and exhibit quantum correlations between the quadratures. Since these correlations cover a finite range of sideband frequencies, we will later consider "broadband two-mode squeezing" in more detail. We will

also demonstrate later that a two-mode squeezed state, produced by the NOPA interaction, is equivalent to two single-mode squeezed states (with perpendicular squeezing directions and produced via the degenerate OPA interaction or alternatively via a $\chi^{(3)}$ interaction, see next section) combined at a beam splitter. Moreover, other representations of the two-mode squeezed state will be given. As opposed to the textbook convention used for defining the single-mode and two-mode squeezing operators, $r \equiv -\kappa t$ [179, 200, 125], we will mostly use $r \equiv \kappa t \geq 0$ in the following.

b Squeezing via the $\chi^{(3)}$ interaction

Another important nonlinear process that gives rise to squeezing is four-wave mixing. It also involves the production of photon pairs (signal and idler), but it is based on a $\chi^{(3)}$ interaction. Furthermore, two pump beams are necessary for four-wave mixing ($2\omega_{\rm pump} = \omega_{\rm signal} + \omega_{\rm idler}$) rather than just one as for the parametric amplifier. In order to describe (degenerate) four-wave mixing quantum mechanically, however, the same quadratic interaction Hamiltonian as for the OPA [Eq. (I.143)] can be used, provided the "parametric approximation" with classical pump modes applies, $\kappa \propto \chi^{(3)}|\alpha_{\rm pump}|^2$ [210]. Consequently, the squeezed states producible by four-wave mixing have the same "ordinary" form as those for the OPA. The generation of squeezed light via four-wave mixing was achieved by Slusher *et al.* [192] (published in 1985 as the first light-squeezing experiment).

Initially, the main conceptual difficulty in creating a detectable squeezing effect was that a $\chi^{(3)}$ process is very weak in all transparent media. In particular, in order to achieve measurable quantum noise reduction against addititonal 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 [126]. The proposal referred to a dispersionless *cw* type of four-wave mixing. Describing the response of the fiber material to an external field by Eq. (I.142), the dominant nonlinear term contains $\chi^{(3)}$ ("Kerr

effect"), because the $\chi^{(2)}$ susceptibility vanishes in a glass fiber [1]. This Kerr effect is equivalent to an intensity dependent refraction index. A squeezing experiment confirming the *cw* theory of four-wave mixing in a single-mode fiber [126] was successfully conducted by Shelby *et al.* [180]. 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 [51]. In the corresponding classical theory, using several approximations and assumptions, Eq. (I.140) can be turned into a suitably scaled propagation equation of a (complex) light pulse envelope [1] [9],

$$i\,\frac{\partial\phi}{\partial\tau} + \frac{1}{2}\,\frac{\partial^2\phi}{\partial\xi^2} + |\phi|^2\,\phi = 0, \tag{I.160}$$

where τ is a normalized dimensionless propagation distance and ξ is a normalized dimensionless time in a co-moving reference frame. Just as for the free electromagnetic field, quantisation can now also be applied to the more complicated system of a light pulse in a fiber. After Fourier transforming the whole propagation equation Eq. (I.160) according to

$$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} a(\sigma,\tau)\,e^{-i\sigma\xi}\,d\sigma = \phi(\xi,\tau)\;, \tag{I.161}$$

[9] This equation correctly describes the effects of anomalous dispersion ($k'' = \partial^2 k/\partial\omega^2 < 0$) and $\chi^{(3)}$ nonlinearity on the propagation of a (not too short) light pulse in an optical fiber, where the envelope $\phi(\xi,\tau)$ is a normalized version of $B(z,t)$ in $\mathbf{E}(\mathbf{r},t) = \mathbf{e}_x\,A(x,y)\,B(z,t)\,\exp[i(k_0 z - \omega_0 t)]$ + complex conj. It is called the "nonlinear Schrödinger equation", because of its similarity to the well-known quantum Schrödinger equation. Yet the "nonlinear Schrödinger equation" is an entirely *classical* equation. There are so-called soliton solutions of this equation. The envelope of the fundamental soliton solution does not change its shape through propagation. This reflects the full compensation of group-velocity dispersion [the second term in Eq. (I.160)] and so-called self-phase modulation [the third term in Eq. (I.160) representing the Kerr effect] for optical fiber solitons. Because of this stability, optical solitons are very useful in classical optical communication. More information on *classical* nonlinear fiber optics, light pulse and soliton propagation in fibers, can be found in the book by Agrawal [1].

again the complex Fourier amplitudes $a(\sigma,\tau)$ and $a^*(\sigma,\tau)$ are replaced by the operators $\hat{a}(\sigma,\tau)$ and $\hat{a}^\dagger(\sigma,\tau)$ respectively, yielding

$$i\frac{\partial}{\partial\tau}\hat{a}(\sigma,\tau) - \frac{\sigma^2}{2}\hat{a}(\sigma,\tau) + \int_{-\infty}^{\infty} d\sigma_1 d\sigma_2\, \hat{a}^\dagger(\sigma_1,\tau)\hat{a}(\sigma_2,\tau)\hat{a}(\sigma+\sigma_1-\sigma_2,\tau) = 0\,. \tag{I.162}$$

With the normalized dimensionless frequency σ, the corresponding "broadband" commutation relations are given by

$$[\hat{a}(\sigma,\tau),\hat{a}(\sigma',\tau)] = [\hat{a}^\dagger(\sigma,\tau),\hat{a}^\dagger(\sigma',\tau)] = 0\,,\ [\hat{a}(\sigma,\tau),\hat{a}^\dagger(\sigma',\tau)] = \delta(\sigma-\sigma')/\bar{n}\,. \tag{I.163}$$

Here, $\bar{n}$ is a scaling factor that contains the group-velocity dispersion and nonlinearity parameters. An inverse Fourier transform finally yields the quantised spatial-temporal propagation equation [10]

$$i\frac{\partial\hat{\phi}}{\partial\tau} + \frac{1}{2}\frac{\partial^2\hat{\phi}}{\partial\xi^2} + \hat{\phi}^\dagger\,\hat{\phi}\,\hat{\phi} = 0\,, \tag{I.164}$$

with

$$[\hat{\phi}(\xi,\tau),\hat{\phi}(\xi',\tau)] = [\hat{\phi}^\dagger(\xi,\tau),\hat{\phi}^\dagger(\xi',\tau)] = 0\,,\ [\hat{\phi}(\xi,\tau),\hat{\phi}^\dagger(\xi',\tau)] = \delta(\xi-\xi')/\bar{n}\,. \tag{I.165}$$

[10] This equation is called the "quantum nonlinear Schrödinger equation", the quantised version of the classical nonlinear Schrödinger equation. The operators $\hat{\phi}(\xi,\tau)$ and $\hat{\phi}^\dagger(\xi,\tau)$ are scaled annihilation and creation operators depending on time and distance. They change with propagation, i.e., equation Eq. (I.164) is formulated in the Heisenberg picture, $i\hbar\, d\hat{\phi}(\xi,\tau)/d\tau = [\hat{\phi}(\xi,\tau),\hat{H}]$ with $\hat{H} = (\hbar\bar{n}/2)\int d\xi(:|\partial\hat{\phi}/\partial\xi|^2 - |\hat{\phi}|^4:)$ and the colons indicating normal ordering [124]. The propagation of quantised light pulses in optical fibers, in particular the propagation of "quantum solitons" can be recast in the Schrödinger representation [124] and in phase-space representations such as the Wigner function [50]. Via the so-called positive-P representation [73], a stochastic nonlinear Schrödinger equation can be derived which contains the deterministic classical evolution and additional quantum noise in terms of stochastic functions [51]. It was shown by Fini *et al.* that the stochastic soliton formalism agrees with the Heisenberg operator and phase-space approaches [85]. More information about the quantum theory of optical solitons in fibers, squeezing of quantum solitons and photon number QND measurements via soliton collisions, can be found in the review article by Drummond *et al.* [72].

By using a stochastic equation instead of the operator equation Eq. (I.164) for describing the classical propagation plus the evolution of the quantum noise in the fiber, Carter *et al.* proposed the squeezing of quantum fiber-solitons [51]. This theory was then experimentally confirmed by Rosenbluh and Shelby [174].

What is the potential advantage of using optical fibers and light pulses with respect to applications in quantum communication? In classical optical communication, light pulses represent classical bits that are sent over large distances to many receivers through a fiber network. At the communication wavelength of 1.55 μm, glass fibers have an absorption minimum with very low losses and negative dispersion which enables the use of stable soliton pulses. All this would also apply to the transfer of quantum information, provided the fragile quantum states survive the propagation in the fiber (pure superposition states might evolve into mixed states due to "decoherence" caused by unwanted noise sources such as guided acoustic wave Brillouin scattering [181]). The issue of protection against decoherence, however, is not specific to the use of an optical fiber, but the issue is crucial and requires further investigations (possible remedies are entanglement purification [17, 42] or quantum error correction [165]).

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. Furthermore, with regard to continuous-variable quantum communication, an optical fiber offers not only the possibility of generating squeezed light and building entanglement from it, but also directly a way to distribute the entanglement. A fiber-based quantum communication system can be potentially integrated into existing fiber-optics communication networks. Recently, bipartite continuous-variable entanglement was created in an optical fiber with optical pulses squeezed via the Kerr $\chi^{(3)}$ nonlinearity [186].

The actual interaction Hamiltonian that accounts for the Kerr effect is quartic

(see footnote 10) rather than quadratic as for the OPA or for conventional four-wave mixing. In terms of discrete single modes, it reads

$$\hat{H}_{\text{int}} = \hbar\kappa\, \hat{a}^{\dagger 2}\hat{a}^2 = \hbar\kappa\, \hat{n}(\hat{n} - 1)\ . \tag{I.166}$$

Here, κ is proportional to $\chi^{(3)}$. 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 [116]. This state correponds to a photon number squeezed state with sub-Poissonian statistics, as opposed to the ordinary quadrature squeezed state. It 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 distance [113]) 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" is by far larger than its length. The difference between such a state and an ordinary squeezed state with an "elliptic" phase-space distribution is negligible. Similarly, the observation of Kerr-induced superpositions of coherent states ("Schrödinger cat states") at an effective interaction time of $\kappa t = \pi/2$ requires extremely large interaction lengths [200, 88].

For sufficiently small effective interaction times κt and large photon number, however, a coherent-state input first evolves into an amplitude squeezed state with Poisson statistics [200]. Apart from this short time behaviour ($\kappa t \ll 1$) and the unrealistic long time behaviour ($\kappa t > 1$), Kerr-induced squeezing resembles ordinary squeezing. Of course, Kerr-induced squeezing relies on nonzero input intensity. The initial coherent states are then to a good approximation turned into ordinary displaced squeezed vacua.

The continuous-variable quantum communication protocols in this thesis are based on entanglement built from ordinary squeezed states using linear optics. The proposed entanglement generation directly applies to *cw* light with zero mean amplitude (squeezed vacua), as producible for example via parametric amplification. As discussed in this section, bright-light pulses squeezed via the Kerr nonlinearity exhibit similar quantum features. Our goal is to find interesting quantum communication protocols using relatively simple systems. These protocols may be translated to technologically more promising but more complicated systems.

4 Linear optics with the quantised field

The quantum description of a simple optical beam splitter is very fundamental, both from a conceptual and a practical point of view. The quantum effects of almost all passive optical devices can be understood assuming appropriate beam-splitter models [125]. Later, we will also find it useful to describe detector inefficiencies via simple beam splitters. More important, however, will be that the entanglement-generating circuits and the entire protocols including quadrature measurements and phase-space displacements are realizable through linear optics with squeezed and coherent light. Let us here briefly discuss how single-mode quantum states are unitarily transformed by beam splitters, how single-mode quadratures are measured through homodyne detection, and how single modes are displaced in phase space.

a Beam splitter transformations

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

$$(\hat{a}_1' \ \hat{a}_2')^T = U(2)\,(\hat{a}_1 \ \hat{a}_2)^T\,. \tag{I.167}$$

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

$$[\hat{a}'_i, \hat{a}'_j] = [(\hat{a}'_i)^{\dagger}, (\hat{a}'_j)^{\dagger}] = 0 \; , \qquad [\hat{a}'_i, (\hat{a}'_j)^{\dagger}] = \delta_{ij} \; , \tag{I.168}$$

or for the elements of $U(2)$,

$$\begin{aligned} |U_{11}(2)|^2 + |U_{12}(2)|^2 = |U_{21}(2)|^2 + |U_{22}(2)|^2 &= 1 \; , \\ U_{11}(2)U^*_{21}(2) + U_{12}(2)U^*_{22}(2) &= 0 \; . \end{aligned} \tag{I.169}$$

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 [67, 19]

$$U(2) = \begin{pmatrix} e^{-i(\phi+\delta)} \sin\theta & e^{-i\delta} \cos\theta \\ e^{-i(\phi+\delta')} \cos\theta & -e^{-i\delta'} \sin\theta \end{pmatrix} \; . \tag{I.170}$$

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

$$\begin{pmatrix} \hat{a}'_1 \\ \hat{a}'_2 \end{pmatrix} = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \; , \tag{I.171}$$

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",

$$U(2) = \begin{pmatrix} e^{-i\delta} & 0 \\ 0 & e^{-i\delta'} \end{pmatrix} \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & 1 \end{pmatrix} \; . \tag{I.172}$$

Let us at this point mention the following very useful result by Reck *et al.* [171]. Not only the above 2×2 matrix can be decomposed into phase shifting and beam splitting operations. Any $N \times N$ unitary matrix may be expressed by a sequence of phase shifters and beam splitters [171],

$$\begin{aligned} U(N) \;=\; & (B_{N-1\,N} B_{N-2\,N} \cdots B_{1\,N} \\ & \times B_{N-2\,N-1} B_{N-3\,N-1} \cdots B_{12} D)^{-1} \; . \end{aligned} \tag{I.173}$$

The $N(N-1)/2$ beam splitter operations each depend on two parameters, the reflectivity/transmittance parameter and one phase, $B_{kl} \equiv B_{kl}(\theta_{kl}, \phi_{kl})$. The B_{kl} do not represent matrix elements, but N-dimensional identity matrices with the entries I_{kk}, I_{kl}, I_{lk}, and I_{ll} replaced by

$$e^{i\phi_{kl}} \sin\theta_{kl}\,, \qquad e^{i\phi_{kl}} \cos\theta_{kl}\,, \qquad \cos\theta_{kl}\,, \qquad \text{and} \quad -\sin\theta_{kl}\,, \tag{I.174}$$

respectively. Extra phase shifts are included by matrix D having diagonal elements $e^{i\delta_1}, e^{i\delta_2}, ..., e^{i\delta_N}$ and off-diagonal terms zero. For example, the unitary 2×2 matrix in Eq. (I.170) corresponds to $U(2) = (B_{12}D)^{-1}$, with $\phi \equiv \phi_{12}$, $\theta \equiv \theta_{12}$, $\delta \equiv \delta_1$, and $\delta' \equiv \delta_2$.

The action of an ideal phase-free beam splitter operation on two modes can be expressed in the Heisenberg picture by the linear transformation Eq. (I.171). The input operators are changed, whereas the input states remain invariant. The corresponding unitary operator must satisfy

$$\begin{pmatrix} \hat{a}_1' \\ \hat{a}_2' \end{pmatrix} = \hat{B}_{12}^{\dagger}(\theta) \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \hat{B}_{12}(\theta)\,. \tag{I.175}$$

Note that this operator equation and the matrix equation Eq. (I.171) are equivalent, but the matrix in Eq. (I.171), $B_{12}(\theta_{12} = \theta, \phi_{12} = 0)$ according to the definitions above, is not a particular matrix representation of the unitary operator $\hat{B}_{12}(\theta)$ [we had a similar relation between Eq. (I.77) and Eq. (I.52)]. In the Schrödinger representation, we have correspondingly $\hat{\rho}' = \hat{B}_{12}(\theta)\hat{\rho}\hat{B}_{12}^{\dagger}(\theta)$ or for pure states, $|\psi'\rangle = \hat{B}_{12}(\theta)|\psi\rangle$. Rather than deriving the unitary operator $\hat{B}_{12}(\theta)$ and the beam-splitter Hamiltonian (see Ref. [125] for that), we may only note that $\hat{B}_{12}(\theta)$ acts on the position eigenstates as

$$\hat{B}_{12}(\theta)|x_1, x_2\rangle = |x_1 \sin\theta + x_2 \cos\theta, x_1 \cos\theta - x_2 \sin\theta\rangle = |x_1', x_2'\rangle\,. \tag{I.176}$$

This appears obvious when the reality of the matrix in Eq. (I.171) is taken into account for input modes infinitely squeezed in $\hat{x}$. In Eq. (I.176), $|x_1, x_2\rangle \equiv$

$|x_1\rangle|x_2\rangle \equiv |x_1\rangle_1 \otimes |x_2\rangle_2$ which we will use interchangeably throughout the thesis. The position wave function is transformed according to

$$\psi(x_1, x_2) \to \psi'(x_1', x_2') = \psi(x_1' \sin\theta + x_2' \cos\theta, x_1' \cos\theta - x_2' \sin\theta) \; . \quad \text{(I.177)}$$

Such a simple rule applies to an arbitrary number of modes that are subject to a linear transformation,

$$\begin{aligned} &(\hat{x}_1' \; \hat{x}_2' \; \cdots \; \hat{x}_N')^T + i\,(\hat{p}_1' \; \hat{p}_2' \; \cdots \; \hat{p}_N')^T = \\ &\qquad U(N)\,(\hat{x}_1 \; \hat{x}_2 \; \cdots \; \hat{x}_N)^T + i\,U(N)\,(\hat{p}_1 \; \hat{p}_2 \; \cdots \; \hat{p}_N)^T \; , \end{aligned} \quad \text{(I.178)}$$

with a real unitary $N \times N$ matrix $U(N)$ (reality of this matrix ensures that there is no mixing of $\hat{x}_i$ and $\hat{p}_i$ in the output positions $\hat{x}_i'$, so that the $\hat{x}_i'$ only depend on the input $\hat{x}_i$). The corresponding evolution operator $\hat{U}(N)$ [again, $U(N)$ is not a particular matrix representation of $\hat{U}(N)$] acting on an arbitrary state $|\psi\rangle$ has the effect

$$\begin{aligned} |\psi'\rangle &= \hat{U}(N)|\psi\rangle = \hat{U}(N) \int dx_1 dx_2 \cdots dx_N \, \langle x_1, x_2, ..., x_N|\psi\rangle |x_1, x_2, ..., x_N\rangle \\ &= \int dx_1 dx_2 \cdots dx_N \, \langle x_1, x_2, ..., x_N|\psi\rangle \, \hat{U}(N)|x_1, x_2, ..., x_N\rangle \\ &= \int dx_1 dx_2 \cdots dx_N \, \langle x_1, x_2, ..., x_N|\psi\rangle \\ &\quad \times |x_1'(x_1, x_2, ..., x_N), x_2'(x_1, x_2, ..., x_N), ..., x_N'(x_1, x_2, ..., x_N)\rangle \; , \end{aligned} \quad \text{(I.179)}$$

where the functions $x_i'(x_1, x_2, ..., x_N)$ are determined by the matrix equation Eq. (I.178). With the variable substitution $x_i' = x_i'(x_1, x_2, ..., x_N)$, we obtain

$$\begin{aligned} |\psi'\rangle = &\int dx_1' dx_2' \cdots dx_N' \\ &\times \langle x_1(x_1', x_2', ..., x_N'), x_2(x_1', x_2', ..., x_N'), ..., x_N(x_1', x_2', ..., x_N')|\psi\rangle |x_1', x_2', ..., x_N'\rangle \; , \end{aligned} \quad \text{(I.180)}$$

where the functions $x_i(x_1', x_2', ..., x_N')$ are determined by the inverse matrix equation of Eq. (I.178). Note that the linearity of the transformation Eq. (I.178) ensures that the Jacobian J for the variable substitution is constant. Due to

the unitarity, we also have $|\det J| = 1$. From Eq. (I.180), we can derive the transformation rule for the position wave function that yields the new state $|\psi'\rangle = \int dx'_1 dx'_2 \cdots dx'_N \langle x'_1, x'_2, ..., x'_N|\psi'\rangle |x'_1, x'_2, ..., x'_N\rangle$,

$$\psi(x_1, x_2, ..., x_N) \to \psi'(x'_1, x'_2, ..., x'_N) = \\ \psi[x_1(x'_1, x'_2, ..., x'_N), x_2(x'_1, x'_2, ..., x'_N), ..., x_N(x'_1, x'_2, ..., x'_N)] \,. \qquad \text{(I.181)}$$

The 2×2 beam splitter transformation in Eq. (I.177) is a special case of the general rule in Eq. (I.181) (in this special case, the transformation matrix is its own inverse). An even simpler example was the position displacement in Eq. (I.86). A transformation rule equivalent to that in Eq. (I.181) applies also to the momentum wave function, the probability densities, and the Wigner function.

b Homodyne detection

In this section, we will show how to measure the quadrature observables. 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 $\hat{i} = q\,\hat{a}^\dagger \hat{a}$ with q a constant [160]. 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, $|\alpha_{\rm LO}\rangle$. It is therefore reasonable to describe this oscillator by a classical complex amplitude $\alpha_{\rm LO}$ rather than by an annihilation operator $\hat{a}_{\rm LO}$. The two output modes of the beam splitter, $(\hat{a}_{\rm LO} + \hat{a})/\sqrt{2}$ and $(\hat{a}_{\rm LO} - \hat{a})/\sqrt{2}$, may then be approximated by

$$\hat{a}_1 = (\alpha_{\rm LO} + \hat{a})/\sqrt{2} \,, \qquad \hat{a}_2 = (\alpha_{\rm LO} - \hat{a})/\sqrt{2} \,. \qquad \text{(I.182)}$$

This yields the photocurrents

$$\begin{aligned} \hat{i}_1 &= q\,\hat{a}_1^\dagger \hat{a}_1 = q\,(\alpha_{\rm LO}^* + \hat{a}^\dagger)(\alpha_{\rm LO} + \hat{a})/2 \,, \\ \hat{i}_2 &= q\,\hat{a}_2^\dagger \hat{a}_2 = q\,(\alpha_{\rm LO}^* - \hat{a}^\dagger)(\alpha_{\rm LO} - \hat{a})/2 \,. \end{aligned} \qquad \text{(I.183)}$$

The actual quantity to be measured shall be the difference photocurrent

$$\delta\hat{i} \equiv \hat{i}_1 - \hat{i}_2 = q\left(\alpha_{\mathrm{LO}}^{*}\hat{a} + \alpha_{\mathrm{LO}}\hat{a}^{\dagger}\right) . \tag{I.184}$$

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. (I.51) is measured (without mode index k). Now adjustment of the local oscillator's phase $\Theta \in [0, \pi]$ enables the detection of any quadrature from the whole continuum of quadratures $\hat{x}^{(\Theta)}$. A possible way to realize quantum tomography [125], 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, which we will need later, can be found in Ref. [31]. In addition, the influence of a quantized local oscillator is investigated there.

We have seen now that it is not too hard to measure the quadratures of an electromagnetic mode. Also unitary transformations such as quadrature displacements (phase-space displacements) can be relatively easily performed via so-called feed-forward technique, as opposed to for example "photon number displacements". This will be shown next.

c *Coherent displacement of a single mode*

Let us assume we would like to displace a mode $\hat{a}_1$ by a c number β,

$$\hat{a}_1 \to \hat{a}_1' = \hat{a}_1 + \beta . \tag{I.185}$$

What we need now is a highly reflective beam splitter. According to the beam splitter transformation Eq. (I.171), we have

$$\hat{a}_1' = \hat{a}_1 \sin\theta + \hat{a}_2 \cos\theta , \tag{I.186}$$

where mode $\hat{a}_2$ shall be in a highly excited coherent state $|\alpha_2\rangle$ with $|\alpha_2| \gg 1$. Thus, we can write $\hat{a}_2 = \alpha_2 + \hat{x}_2^{(0)} + i\hat{p}_2^{(0)}$ with vacuum quadratures $\hat{x}_2^{(0)}$ and $\hat{p}_2^{(0)}$.

Since $\sin\theta \to 1$ (high reflectivity), the vacuum contribution of mode 2 approaches zero, $\cos\theta\,\hat{x}_2^{(0)} \to 0$ and $\cos\theta\,\hat{p}_2^{(0)} \to 0$, whereas $\cos\theta\,\alpha_2 = \beta$ for sufficiently large $|\alpha_2| \gg 1$. Eventually, mode 1 is displaced by some c number β (depending on the fine adjustment of α_2 and θ), as in Eq. (I.185) or in

$$\hat{a}_1' = \hat{D}^\dagger(\beta)\,\hat{a}_1\,\hat{D}(\beta)\ , \tag{I.187}$$

with the unitary displacement operator $\hat{D}(\beta) = \exp(\beta\hat{a}_1^\dagger - \beta^*\hat{a}_1)$ as defind in Eq. (I.80). Apparently, we can conclude that operations such as quadrature measurements or quadrature displacements acting on continuous-variable quantum states are relatively easy and efficiently to perform (as for the efficiency, see chapter IV). These operations will prove extremely useful for continuous-variable quantum communication.

In this chapter, we have collected some tools and results from quantum optics that will be needed for the analysis of optical quantum communication. The quantum optics textbooks used in this chapter are those by Leonhardt [125], Walls and Milburn [200], Scully and Zubairy [179], Mandel and Wolf [140], Paul [160], and Loudon [137]. 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 represent the building components of the following quantum communication protocols. Let us now gather some useful results of quantum information theory.

II

Basics of quantum information

What is the meaning of quantum information in comparison to classical information? Classical information, as we all know, may be quantified by how many bits are required to encode it. A single bit contains the information whether a " zero" or a "one" has been chosen between only those two options (for example, depending on the electrical current in a computer wire exceeding a certain value or not). Quantum information is encoded in quantum mechanical superpositions such as a "qubit" [1], an arbitrary superposition of "zero" and "one". Because there is an infinite number of possible superpositions, each giving the "zero" and the "one" particular weights within a continuous range, even a single qubit requires a vast amount of information to describe it. A qubit contains far more than the modest information about either "zero" or "one" in a classical bit. We also know that classical information is not necessarily encoded in bits. Bits may be tailor-made for handling by a computer. However, when we perform calculations ourselves, we prefer the decimal to the binary system. In the decimal system, a single digit informs us about a particular choice between ten discrete options rather than only between two as in the binary system. Similarly, quantum information may also be encoded in higher-dimensional sytems rather than in states defined in two-dimensional Hilbert spaces. In fact, as potential superpositions of an infinite number of choices, continuous quantum variables carry maximal quantum information, just as real numbers contain maximal classical information.

A very distinct and fundamental feature of quantum information encoded in

[1] The term qubit was coined by Schumacher [178].

an arbitrary quantum state is that it cannot be copied with perfect accuracy. This rule is expressed by the famous no-cloning theorem [70, 207]. It has no classical counterpart, because no fundamental principle prevents us from making arbitrarily many copies of classical information. The no-cloning theorem was one of the first results on the more general concepts of quantum theory that had the flavour of today's quantum information theory. Deutsch's work on universal quantum computation [69], based on earlier ideas of Feynman [84], also belongs to the forerunners of this rapidly advancing field.

By processing quantum information encoded in a superposition of all possible classical inputs, a quantum computer is capable of simultaneously computing each output value for every possible input. Initially, quantum algorithms were only of interest to specialists in the field. However, when Shor discovered how to factorize numbers into prime numbers significantly faster than classically (in polynomial rather than exponential time) by using a quantum algortihm [183], the quantum computer became a security issue. Codes considered effectively secure, just because breaking them would take a classical computer the age of the universe, were suddenly vulnerable not only in principle. Ironically, the solution to this problem was also offered by quantum theory in form of quantum cryptography [13], a solution that promised in principle unconditional security. Since we are not concerned about quantum computation with continuous variables in this thesis, we will not deal with the basics of general quantum computation.

Another milestone of quantum information theory was the proposal of quantum teleportation by Bennett *et al.* in 1993 [15]. *Entanglement*, though dispensable in quantum cryptography and possibly even in quantum computation [2], was for the first time clearly identified as a resource that allowed one to achieve par-

[2]Whether entanglement is the essential ingredient of a quantum computer is still an issue of debate, see for example Refs. [128, 33]. Quantum cryptography does not necessarily rely on entanglement and the original proposals in fact do not [13]. However, Ekert suggested a quantum cryptographic scheme based on entanglement [83].

ticular communication tasks otherwise impossible. In quantum teleportation, the corresponding task is the reliable transfer of quantum information via a classical communication channel.

Continuous-variable entanglement and entanglement-assisted quantum teleportation protocols with continuous variables are the main subject of this thesis. In this section, we will therefore present only a limited selection of the basics of quantum information theory. The emphasis will be primarily on various sorts of entanglement originally defined for finite-dimensional Hilbert spaces. In addition, by considering mainly discrete-variable systems, we will deal also with the no-cloning theorem, Positive Operator-Valued Measures (POVM's) and quantum teleportation. There are already several monographs available to study quantum information theory. Among them are the book by Nielsen and Chuang [151], Preskill's lecture notes [165], and Peres' book on quantum theory [162] (which presents quantum mechanics in an unconventional manner).

1 Tools and fundamental results

a No-cloning

One of the earliest fundamental results relevant to what we consider today quantum information theory is the so-called no-cloning theorem. It was published more or less at the same time in 1982 by Dieks [70] and by Wootters and Zurek [207]. Both of their motivations were to demonstrate that linearity in quantum mechanical evolution negates the possibility of superluminal communication by means of entanglement. Without their analysis, one might be tempted to speculate that two parties, "Alice" and "Bob", sharing an entangled state such as

$$\begin{aligned}\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) &= \frac{1}{2\sqrt{2}}[(|0\rangle_A + |1\rangle_A) \otimes (|0\rangle_B + |1\rangle_B) \\ &\quad +(|0\rangle_A - |1\rangle_A) \otimes (|0\rangle_B - |1\rangle_B)] \qquad \text{(II.1)}\end{aligned}$$

can communicate faster than the speed of light. For example, one might argue along the lines that Alice could measure her half of the entangled state in either the basis $\{|0\rangle, |1\rangle\}$ (e.g., two eigenstates for electron spin in x direction or for orthogonal photon polarizations) or in the basis $\{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$ (e.g., two eigenstates for electron spin in z direction or for orthogonal photon polarizations rotated by 45 degrees). In the former case, Bob's half ends up in the corresponding eigenstate $|0\rangle$ or $|1\rangle$ and so would *all* copies generated from his half. In the latter case, copies of Bob's half would all be in the corresponding state $(|0\rangle + |1\rangle)/\sqrt{2}$ or $(|0\rangle - |1\rangle)/\sqrt{2}$, and measurements in the basis $\{|0\rangle, |1\rangle\}$ would yield on average half of the copies in the state $|0\rangle$ and likewise half of them in the state $|1\rangle$. Therefore, the statistics of measurements on copies of Bob's half might enable him to find out which measurement basis Alice had chosen. Such a scheme could be exploited for superluminal information transfer from Alice to Bob. However, quantum mechanics does not allow this possibility due to no-cloning as we now describe.

The crucial ingredient of the entanglement-assisted superluminal communication scenario above is the copying device that may be represented by an (initial) state $|A\rangle$. It must be capable of copying *arbitrary* quantum states $|s\rangle$ as

$$|s\rangle|A\rangle \longrightarrow |s\rangle|s\rangle|A'\rangle \; . \tag{II.2}$$

The final state of the copying apparatus is described by $|A'\rangle$. More accurately, the transformation should read

$$|s\rangle_a|0\rangle_b|A\rangle_c \longrightarrow |s\rangle_a|s\rangle_b|A'\rangle_c \; , \tag{II.3}$$

where the original input a to be cloned is described by $|s\rangle_a$ and a second particle or mode b is initially in the "blank" state $|0\rangle_b$. After the copying process both particles or modes are in the original quantum state $|s\rangle$.

Wootters and Zurek [207] (and similarly Dieks for his "multiplier" [70]) then consider a device that in fact copies the basis states $\{|0\rangle, |1\rangle\}$ in the appropriate

way according to Eq. (II.2),

$$\begin{aligned} |0\rangle|A\rangle &\longrightarrow |0\rangle|0\rangle|A_0\rangle \,, \\ |1\rangle|A\rangle &\longrightarrow |1\rangle|1\rangle|A_1\rangle \,. \end{aligned} \tag{II.4}$$

Since this transformation must be unitary (and hence linear), its application to an input in the superposition state $|s\rangle = \alpha|0\rangle + \beta|1\rangle$ ("qubit") leads to

$$|s\rangle|A\rangle \longrightarrow \alpha|0\rangle|0\rangle|A_0\rangle + \beta|1\rangle|1\rangle|A_1\rangle \,. \tag{II.5}$$

For identical output states of the copying apparatus, $|A_0\rangle = |A_1\rangle$, a and b are in the pure state $\alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$ which is not the desired output state $|s\rangle|s\rangle$. With a distinction between the apparatus states, i.e., taking them to be orthonormal, $\langle A_0|A_0\rangle = \langle A_1|A_1\rangle = 1$, $\langle A_0|A_1\rangle = 0$, we obtain from the density operator of the whole output system (assuming for simplicity real α and β),

$$\begin{aligned} \hat{\rho}_{abc} \;=\; & \alpha^2 |00A_0\rangle_{abc\,abc}\langle 00A_0| + \beta^2 |11A_1\rangle_{abc\,abc}\langle 11A_1| \\ & + \alpha\beta |00A_0\rangle_{abc\,abc}\langle 11A_1| + \alpha\beta |11A_1\rangle_{abc\,abc}\langle 00A_0| \,, \end{aligned} \tag{II.6}$$

that of the original-copy system ab by tracing out the apparatus,

$$\mathrm{Tr}_c \hat{\rho}_{abc} = \alpha^2 |00\rangle_{ab\,ab}\langle 00| + \beta^2 |11\rangle_{ab\,ab}\langle 11| \equiv \hat{\rho}_{ab} \,. \tag{II.7}$$

Finally, we can calculate the individual density operators of a and b,

$$\begin{aligned} \mathrm{Tr}_b \hat{\rho}_{ab} &= \alpha^2 |0\rangle_{a\,a}\langle 0| + \beta^2 |1\rangle_{a\,a}\langle 1| \equiv \hat{\rho}_a \,, \\ \mathrm{Tr}_a \hat{\rho}_{ab} &= \alpha^2 |0\rangle_{b\,b}\langle 0| + \beta^2 |1\rangle_{b\,b}\langle 1| \equiv \hat{\rho}_b \,. \end{aligned} \tag{II.8}$$

The two outgoing states are identical, but significantly different from the desired original density operator,

$$|s\rangle_{a\,a}\langle s| = \alpha^2 |0\rangle_{a\,a}\langle 0| + \alpha\beta |0\rangle_{a\,a}\langle 1| + \alpha\beta |1\rangle_{a\,a}\langle 0| + \beta^2 |1\rangle_{a\,a}\langle 1| \,. \tag{II.9}$$

In fact, any information about quantum coherence encoded in the off-diagonal terms is eliminated in the output states of Eq. (II.8). Note that the degree of

similarity between the actual output states and the original state, expressed by their overlap, the so-called fidelity [178],

$$F = {}_a\langle s|\hat{\rho}_a|s\rangle_a = {}_b\langle s|\hat{\rho}_b|s\rangle_b = \alpha^4 + \beta^4 = \alpha^4 + (1-\alpha^2)^2 \,, \tag{II.10}$$

depends on the original input state. The basis states $|0\rangle$ or $|1\rangle$ are perfectly copied with unit fidelity ($\alpha = 1$ or $\alpha = 0$), as we know from Eq. (II.4). However, coherent superpositions are copied with non-unit fidelity, where the worst result is obtained for the symmetric superposition $\alpha = 1/\sqrt{2}$ with $F = 1/2$.

Is it inevitable to obtain such a bad result when copying a symmetric superposition? Of course, only when we insist on perfectly copying certain basis states $\{|0\rangle, |1\rangle\}$. A universal copying machine that "treats all input states equally well" can in fact be found. For any input state $|s\rangle = \alpha|0\rangle + \beta|1\rangle$, it always yields the same optimum non-unit fidelity independent of α, namely $F = 5/6$ [47]. Later we will consider such cloning transformations, in particular for states decribed by continuous quantum variables.

b *Bipartite entanglement*

Probably the most commonly discussed entangled system is a pair of qubits maximally entangled in one of the four "Bell states" [41],

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \,, \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \,. \end{aligned} \tag{II.11}$$

The entanglement of pure states is mathematically associated with the non-factorizability of the total state vector. In fact, it is obvious that none of the Bell states can be written in the tensor product form $|\chi\rangle_1 \otimes |\chi\rangle_2$. They are maximally entangled in the sense that measuring either qubit in the basis $\{|0\rangle, |1\rangle\}$ leaves the other qubit in a particular basis state with certainty, while their individual states before the measurement are completely uncertain. Conversely, not

having any information about either half (i.e., tracing out either qubit) leaves the other half in the maximally mixed state $\mathbb{1}/2$.

A rigorous definition of maximum bipartite entanglement in arbitrary finite dimensions can be given in terms of the so-called Schmidt decomposition [177]. 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 as

$$|\psi\rangle = \sum_n c_n |u_n\rangle |v_n\rangle \ , \tag{II.12}$$

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

$$|\psi\rangle = \sum_{mk} a_{mk} |m\rangle |k\rangle = \sum_{nmk} u_{mn} c_{nn} v_{kn} |m\rangle |k\rangle = \sum_n c_n |u_n\rangle |v_n\rangle \ , \tag{II.13}$$

with $c_{nn} \equiv c_n$. In the first step, the matrix a with complex elements a_{mk} is diagonalised, $a = ucv^T$, where u and v are unitary matrices and c is a diagonal matrix with non-negative elements. In the second step, we defined $|u_n\rangle \equiv \sum_m u_{mn} |m\rangle$ and $|v_n\rangle \equiv \sum_k v_{kn} |k\rangle$ which form orthonormal sets due to the unitarity of u and v and the orthonormality of $|m\rangle$ and $|k\rangle$.

Now we can give the following definition: a pure state of two d-level systems (of two "qu*d*its") is maximally entangled when the Schmidt coefficients of its total state vector are all equal; thus we may write the state as

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{i\phi_n} |u_n\rangle |v_n\rangle \ , \tag{II.14}$$

with arbitrary phases ϕ_n [the Schmidt form Eq. (II.12) absorbs these phases into the bases].

The Schmidt decomposition in Eq. (II.12) makes it transparent that the "majority" of pure bipartite states are nonmaximally (partially) entangled, whereas

the class of factorizable (separable) states ($c_n = \delta_{nn_0}$ with $n_0 = 0, 1, ..., d-1$) and that of maximally entangled states ($c_n = 1/\sqrt{d}$) are only two limiting cases. For pure bipartite states, there is also a unique measure of entanglement. This measure is given by the partial von Neumann entropy, the von Neumann entropy [Eq. (I.133)] after tracing out either subsystem [16]. It can be directly inferred from the Schmidt decomposition that $E_{\text{v.N.}} = -\sum_n c_n^2 \log_d c_n^2$ ranges between zero and one.

We have seen that two systems in a *pure* state are always Schmidt decomposable and how their entanglement can be quantified [3]. Mixed states are more subtle, even for only two parties. As for the quantification of mixed-state entanglement, there are various measures available such as the entanglement of formation introduced in Ref. [18]. We do not further discuss mixed-state entanglement quantification here. Instead, we will now turn to the question how to find out whether a bipartite state described by an arbitrary density operator is entangled or not.

c *how to witness bipartite entanglement*

The definition of pure-state entanglement via the non-factorizability of the total state vector is generalized to mixed states through non-separability (or inseparability) of the total density operator. A general quantum state of a two-party system is separable if and only if its total density operator is a convex sum of

[3] This statement is not restricted to finite-dimensional systems. For example, the Schmidt basis of a two-mode squeezed state, defined in an infinite-dimensional Hilbert space, is the Fock basis [see later, Eq. (III.24)]. In a continuous-variable basis such as the position basis, the two-mode squeezed state is not in Schmidt decomposition form [see later, Eq. (III.26)].

product states [4] [202],

$$\hat{\rho} = \sum_i p_i \, \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \; . \tag{II.15}$$

Otherwise, it is inseparable. In general, it is non-trivial whether a given density operator is separable or inseparable. Nonetheless, a very convenient method to test for inseparability is Peres' partial transpose criterion [163]. For a separable state as in Eq. (II.15), transposition of either density matrix yields again a legitimate non-negative density operator with unit trace,

$$\hat{\rho}' = \sum_i p_i \, (\hat{\rho}_{i1})^T \otimes \hat{\rho}_{i2} \; , \tag{II.16}$$

since $(\hat{\rho}_{i1})^T = (\hat{\rho}_{i1})^*$ corresponds to a legitimate density matrix. This is a necessary condition for a separable state, and hence a single negative eigenvalue of the partially transposed density matrix is a sufficient condition for inseparability. In the (2×2)- and (2×3)-dimensional cases, this condition is both necessary and sufficient. For any other dimension, negative partial transpose is only sufficient for inseparability [109]. Inseparable states with positive partial transpose cannot be distilled to a maximally entangled state via local operations and classical communication. They are so-called "bound entangled" [111]. The converse, however, does not hold. An explicit example of a bound entangled state with negative partial transpose was given in Ref. [71]. In other words, not all entangled states that reveal their inseparability through negative partial transpose are distillable or "free entangled".

Other sufficient inseparability criteria include violations of inequalities imposed by local realistic theories (see chapter III), an entropic inequality [namely

[4] In quantum information theory, the notion of inseparability has a purely mathematical meaning as expressed by the convex-sum definition. This mathematical inseparability has the consequence that even when the two systems are spatially separated from each other there is no well-defined physical state of the subsystems alone. The "physical inseparability" may manifest in "nonlocal" correlations that cannot be explained by a local realistic theory (see chapter III).

$E_{\text{v.N.}}(\hat{\rho}_1) > E_{\text{v.N.}}(\hat{\rho}_{12})$ with $\hat{\rho}_1 = \text{Tr}_2\hat{\rho}_{12}$] [110], and a condition based on the theory of majorization [152].

d Multipartite entanglement

A more complex issue than bipartite entanglement is the entanglement shared by more than two parties. In fact, even the entanglement of *pure* multi-party states is much more subtle than that of pure two-party states. The latter is easy to handle by means of the Schmidt decomposition. For pure multi-party states, a Schmidt decomposition does not exist in general. The total state vector then cannot be written as a single sum over orthonormal basis states. There is, however, one very important representative of multipartite entanglement that does have the form of a multi-party Schmidt decomposition. It is the Greenberger-Horne-Zeilinger (GHZ) state [101]

$$|\text{GHZ}^{(N,2)}\rangle = \frac{1}{\sqrt{2}}\left(|000\cdots000\rangle + |111\cdots111\rangle\right) , \tag{II.17}$$

or, more generally, the GHZ-like state

$$|\text{GHZ}^{(N,d)}\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}|nn\cdots n\rangle . \tag{II.18}$$

Here, the superscript (N, d) denotes the number of parties N and the dimension d of each subsystem. Although there is no rigorous definition of maximally entangled multi-party states due to the lack of a general Schmidt decomposition, the form of the GHZ and the GHZ-like state with all "Schmidt coefficients" equal *suggests* that these states exhibit maximum multipartite entanglement. In fact, there are various reasons for assigning the attribute "maximally entangled" to those states. For example, they yield the maximum violations of multi-party inequalities imposed by local realistic theories [117]. 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 $|\mathrm{GHZ}^{(3,2)}\rangle$ or the so-called W state,

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right) , \tag{II.19}$$

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

$$\mathrm{Tr}_1|\mathrm{W}\rangle\langle\mathrm{W}| = \frac{1}{3}\left(|00\rangle\langle 00| + |10\rangle\langle 10| + |01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01|\right) , \tag{II.20}$$

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

$$\begin{aligned} \mathrm{Tr}_1|\mathrm{GHZ}^{(3,2)}\rangle\langle\mathrm{GHZ}^{(3,2)}| &= \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) \\ &= \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right) . \end{aligned} \tag{II.21}$$

Note that this is not the maximally mixed state of two qubits, $\mathbb{1}^{\otimes 2}/4$. The maximally mixed state of one qubit, however, is obtained after tracing out two parties of the GHZ state. Bipartite entanglement is only available from the GHZ state through some local operation such as a measurement on the conjugate basis $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$,

$$\frac{\frac{1}{2}\left(|0\rangle_1 \pm |1\rangle_1\right)\left({}_1\langle 0| \pm {}_1\langle 1|\right)|\mathrm{GHZ}^{(3,2)}\rangle}{\left\|\frac{1}{2}\left(|0\rangle_1 \pm |1\rangle_1\right)\left({}_1\langle 0| \pm {}_1\langle 1|\right)|\mathrm{GHZ}^{(3,2)}\rangle\right\|} = \frac{1}{\sqrt{2}}(|0\rangle_1 \pm |1\rangle_1) \otimes |\Phi^{\pm}\rangle . \tag{II.22}$$

Here, $\| |\chi\rangle \|$ means the norm $\sqrt{\langle\chi|\chi\rangle}$ and $|\Phi^{\pm}\rangle$ are two of the four Bell states in Eq. (II.11).

What can be said about arbitrary *mixed* entangled states of more than two parties? There is of course an immense variety of inequivalent classes of multi-party mixed states [for example, five classes of three-qubit states of which the extreme cases are the fully separable ($\hat{\rho} = \sum_i p_i \ \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3}$) and the fully (genuinely) inseparable states [79]]. In general, multi-party inseparability criteria cannot be formulated in such a compact form as the two-party partial transpose criterion (see for example, Ref. [209]). Similarly, the quantification of multipartite entanglement, even for pure states, is still subject of current research [82]. Existing multi-party entanglement measures do not appear to be unique as is the partial von Neumann entropy for pure two-party states.

e *Werner states*

In this section, we will introduce a certain class of mixed states, the so-called Werner states. They are mixtures of a maximally entangled and a maximally mixed state. The separability properties of Werner states depend on the respective weight of the quantum correlated and the random fraction.

The two-qubit mixed state originally proposed by Werner was [202]

$$\hat{\rho}_{\mathrm{W}} = p|\Psi^-\rangle\langle\Psi^-| + (1-p)\mathbb{1}^{\otimes 2}/4 \,, \tag{II.23}$$

where $|\Psi^-\rangle$ is one of the four Bell states in Eq. (II.11) (the "singlet" state) and the "singlet fraction" is $p = 1/2$. Werner's original intention was to demonstrate that quantum states exist which are inseparable according to the convex-sum definition and yet admit a local realistic description [202]. In fact, any separable state satisfies the inequalities imposed by local realism (see chapter III). Conversely, pure entangled states always lead to violations of some local-realism inequality [92], but there are inseparable (mixed entangled) states that do not, as shown by Werner by giving the explicit example $\hat{\rho}_{\mathrm{W}}$ with $p = 1/2$. The Werner states in

Eq. (II.23) are indeed inseparable for any singlet fraction $p > 1/3$ and separable otherwise. This can be seen through partial transpose [163] [remember that this criterion is necessary and sufficient for the (2×2)-case].

A generalized version of the Werner state was investigated by Deuar *et al.* [68]. Their generalized Werner state is a decomposition of the maximally mixed state and the GHZ-type entangled state $|\mathrm{GHZ}^{(N,d)}\rangle$ for N qu*d*its [68],

$$\hat{\rho}_{\mathrm{W}}^{(N,d)} = p|\mathrm{GHZ}^{(N,d)}\rangle\langle\mathrm{GHZ}^{(N,d)}| + (1-p)\mathbb{1}^{\otimes N}/d^N, \tag{II.24}$$

with $|\mathrm{GHZ}^{(N,d)}\rangle$ from Eq. (II.18) and

$$\mathbb{1}^{\otimes N} = \sum_{n_1,n_2,\ldots,n_N=0}^{d-1} |n_1 n_2 \cdots n_N\rangle\langle n_1 n_2 \cdots n_N| \,. \tag{II.25}$$

We will get back to these states in chapter III, where we focus on the infinite-dimensional limit $d \to \infty$ of the results obtained for the N-qu*d*it Werner states.

f Quantum circuits to generate qubit entanglement

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

Let us consider the generation of entanglement between arbitrarily many qubits. The quantum circuit shall turn N independent qubits into an N-partite entangled state. Initially, the N qubits shall be in the eigenstate $|0\rangle$. All we need now is a circuit with the following two elementary gates: the Hadamard gate (or Hadamard transformation) acting on a single qubit as [151]

$$|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \,, \quad |1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \,, \tag{II.26}$$

and the controlled-NOT (C-NOT) gate, a two-qubit operation acting as [151]

$$|00\rangle \longrightarrow |00\rangle \,, \quad |01\rangle \longrightarrow |01\rangle \,, \quad |10\rangle \longrightarrow |11\rangle \,, \quad |11\rangle \longrightarrow |10\rangle \,. \tag{II.27}$$

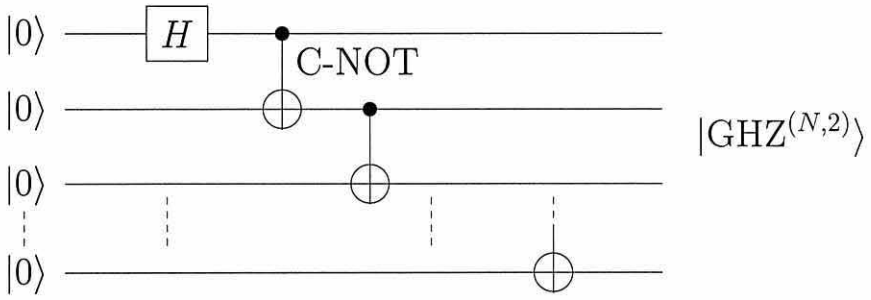

Figure II.1: Quantum circuit for generating the GHZ state. The gates (elementary unitary transformations) are a Hadamard transformation ("H") and pairwise acting C-NOT gates.

The first qubit (control qubit) remains unchanged under the C-NOT. The second qubit (target qubit) is flipped if the control qubit is set to 1, and is left unchanged otherwise. Equivalently, we can describe the action of the C-NOT gate by $|y_1, y_2\rangle \rightarrow |y_1, y_2 \oplus y_1\rangle$ with $y_1, y_2 = 0, 1$ and the addition modulo two $\oplus$. The N-partite entangled output state of the circuit (see Fig. II.1) is the GHZ state from Eq. (II.17).

Later, we will translate the quantum circuit here to continuous variables. This analogy will deliver a recipe for how to produce continuous-variable entanglement between arbitrarily many parties. We will then also be able to deduce a physical (optical) realization from the idealized circuit.

g POVM's

In the preceding chapter, we have seen how the measurement of an observable, a Hermitian operator with real eigenvalues, affects the quantum state of a system: the state is reduced to an eigenstate of the observable and the corresponding eigenvalue is the measurement result. Let us now bring this "projection measurement" into a more general context by identifying it as a special case of a generalized measurement called Positive Operator-Valued Measure (POVM).

In order to describe a general measurement, we first define a collection of measurement operators $\{\hat{M}_m\}$ [151]. The index m refers to the measurement outcomes. If the quantum system is in the normalized state $|\psi\rangle$ (we consider pure states which is sufficient for our purposes) before the measurement, the probability for obtaining the result m is given by

$$p_m = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle \ . \tag{II.28}$$

The state after the measurement is

$$\frac{\hat{M}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle}} = \frac{\hat{M}_m|\psi\rangle}{\|\hat{M}_m|\psi\rangle\|} \ . \tag{II.29}$$

The completeness,

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = \mathbb{1} \ , \tag{II.30}$$

ensures that the probabilities sum to one,

$$\sum_m p_m = \sum_m \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle = 1 \ . \tag{II.31}$$

A projective measurement is now expressed by an Hermitian operator $\hat{M}$ with spectral decomposition

$$\hat{M} = \sum_m m\hat{P}_m \ , \tag{II.32}$$

where $\hat{P}_m \equiv |m\rangle\langle m|$ is the projector onto the eigenspace of $\hat{M}$ with eigenvalues m [see the spectral decomposition in Eq. (I.64)]. The measurement probabilities are now given by [see Eq. (I.61)]

$$p_m = \langle\psi|\hat{P}_m|\psi\rangle \ , \tag{II.33}$$

and the state after the measurement becomes

$$\frac{\hat{P}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_m^\dagger \hat{P}_m|\psi\rangle}} = \frac{\hat{P}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_m|\psi\rangle}} \ . \tag{II.34}$$

The last statement was used for example in Eq. (II.22) to describe a projection measurement on the basis $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$. Comparing the equations for a projection measurement with those above for a general measurement, we see that the former is a special case of the latter, $\hat{M}_m \equiv \hat{P}_m$, under the additional assumptions $\hat{M}_m^\dagger = \hat{M}_m$ and $\hat{M}_m \hat{M}_{m'} = \delta_{mm'} \hat{M}_m$. The last assumption reflects the orthonormality of the eigenbasis $\{|m\rangle\}$. The completeness relation Eq. (II.30) for a projection measurement reduces to the completeness relation of the eigenbasis $\{|m\rangle\}$, $\sum_m \hat{M}_m = \mathbb{1}$. For historical reasons, a projection measurement is often called a "von Neumann measurement".

Let us now define the positive operator

$$\hat{E}_m \equiv \hat{M}_m^\dagger \hat{M}_m \,, \tag{II.35}$$

with the measurement operators $\hat{M}_m$ from above. Then, obviously $\sum_m \hat{E}_m = \mathbb{1}$ and $p_m = \langle\psi|\hat{E}_m|\psi\rangle$ hold. The probabilities of the measurement outcomes are completely determined by the set $\{\hat{E}_m\}$, known as a Positive Operator-Valued Measure (POVM). Note that the definition of the POVM does not contain any statements about the quantum state after the measurement associated with the POVM. By definition, *any* complete set of positive operators $\{\hat{E}_m\}$ is a POVM. It can then be shown that there is a set of measurement operators $\{\hat{M}_m\}$ defined by $\hat{M}_m^\dagger \hat{M}_m \equiv \hat{E}_m$ [151]. With $p_m = \langle\psi|\hat{E}_m|\psi\rangle$, the POVM is a complete description of the corresponding measurement. Throughout the thesis, it will be clear from the context whether the operators $\hat{E}_m$ refer to elements of a POVM or components of the quantized electric field. The POVM elements and the measurement operators coincide, $\hat{E}_m \equiv \hat{M}_m^\dagger \hat{M}_m = \hat{M}_m$, if and only if the measurement is a projection measurement, $\hat{M}_m \equiv \hat{P}_m$ [151]. In this sense, a projection measurement is described by a special POVM.

After this purely mathematical definition of a POVM, we may ask what the advantage is of describing measurements in a more general fashion through POVM's. We will proceed to give two examples to answer this question. The

first one is taken from Ref. [151] and it is based on discrete-variable qubits. The second example is for an electromagnetic mode defined by continuous quantum variables.

Let us suppose that someone called "Victor" prepares a qubit in one of two states, $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ [151]. He gives the qubit to "Alice" and it is Alice's task to decide whether she was given the state $|\psi_1\rangle$ or $|\psi_2\rangle$. Alice cannot fulfil this task with perfect reliability, because $|\psi_1\rangle$ and $|\psi_2\rangle$ are non-orthogonal to each other. The POVM $\{\hat{E}_1, \hat{E}_2\}$ for distinguishing two arbitrary non-orthogonal states with perfect reliability, $\langle\psi_j|\hat{E}_i|\psi_j\rangle = \delta_{ij}$, does not exist (for a proof, see Ref. [151]). Is there possibly a measurement that sometimes yields a reliable distinction at the price that the other times no information at all is obtained? A projection measurement onto the basis $\{|0\rangle, |1\rangle\}$ is obviously not the choice for this. It can never conclusively identify $|\psi_1\rangle$ and only sometimes $|\psi_2\rangle$ [5]. Instead, let us define the following POVM:

$$\begin{aligned} \hat{E}_1 &\equiv \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2} , \\ \hat{E}_2 &\equiv \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1| , \\ \hat{E}_3 &\equiv \mathbb{1} - \hat{E}_1 - \hat{E}_2 . \end{aligned} \tag{II.36}$$

These three operators are positive and form a complete set as required. Now if either of the first two measurement results occur, $\hat{E}_1$ or $\hat{E}_2$, Alice can reliably identify the state, since

$$\langle\psi_j|\hat{E}_i|\psi_j\rangle \propto \delta_{ij} \qquad \text{for} \quad i,j = 1,2 . \tag{II.37}$$

[5] "Never" and "sometimes" here refer to a sequence of trials where Victor draws either state from his two-state "alphabet" with equal probability in each trial. Of course, if Alice had an ensemble of identical copies of the state she received from Victor in a single trial, she could make a statistical distinction by measuring in the basis $\{|0\rangle, |1\rangle\}$. The copies in the state $|\psi_1\rangle$ would all yield the same result, whereas for those in the state $|\psi_2\rangle$, about half of the results would be "0", the other half "1". Alice, however, cannot produce exact copies of the unknown state due to the no-cloning theorem.

The measurement result $\hat{E}_3$, however, contains no information about the identity of the state. Knowing that the conclusive results $\hat{E}_1$ and $\hat{E}_2$ are perfectly reliable and that the inconclusive result $\hat{E}_3$ is useless, Alice can sometimes identify both $|\psi_1\rangle$ and $|\psi_2\rangle$ and she never draws a faulty conclusion.

Our second example for a POVM involves continuous quantum variables. The POVM is defined by

$$\hat{E}_\alpha = \frac{1}{\pi}|\alpha\rangle\langle\alpha| \,. \tag{II.38}$$

The complex amplitude α labels the measurement results. Completeness is satisfied, because coherent states form an (over-)complete set, $\int d^2\alpha\, \hat{E}_\alpha = \mathbb{1}$ (see the previous chapter). Due to the lack of orthogonality of coherent states, this POVM is clearly not a projection measurement. Yet it represents the optimal measurement in the following situation. Victor prepares an arbitrary coherent state $|\beta\rangle$ and gives it to Alice. Alice's task is to identify the unknown amplitude β as reliably as possible (perfect reliability in a single shot is impossible again due to the nonorthogonality of the states $|\beta\rangle$). The detection of individual quadratures such as position or momentum measurements is certainly not the optimal choice. In fact, the optimal measurement for estimating the unknown amplitude β is the POVM given by the "coherent-state projectors". However, in contrast to the above qubit POVM, a single shot of the coherent-state POVM never yields a perfectly conclusive result, because

$$\langle\beta|\hat{E}_\alpha|\beta\rangle = \frac{1}{\pi}\,|\langle\alpha|\beta\rangle|^2 \,. \tag{II.39}$$

There is no distinction between conclusive and inconclusive results. Any single shot α occurs with non-zero probability for a whole range of β's. Hence it contains only approximate information about the actual state $|\beta\rangle$ drawn by Victor. In this case, Alice may rely on a distribution over subsequent measurements of an ensemble of identically prepared states $|\beta\rangle$ (assuming Victor's laser source produces the same coherent state every inverse bandwidth time). The "noisy" information

obtained about the actual state $|\beta\rangle$ is then described by the probability distribution in Eq. (II.39). According to Eq. (I.121), this probability distribution is the Q function of the state $|\beta\rangle$,

$$Q_\beta(\alpha) = \frac{1}{\pi}\langle\alpha|\hat{\rho}_\beta|\alpha\rangle = \frac{1}{\pi}\langle\alpha|\beta\rangle\langle\beta|\alpha\rangle\,. \tag{II.40}$$

Thus, Alice's distribution of measurement results shows the actual quantum state described by the Wigner function of the state $|\beta\rangle$ [see Eq. (I.124) with $\beta \equiv x_0+ip_0$] convoluted with a Gaussian of one unit of vacuum [see Eq. (I.119)]. This is the optimal state estimation available to Alice. Using it Alice can achieve the best possible performance when "teleporting" an arbitrary coherent state without sharing entanglement with the reciever (this so-called "classical teleportation" of coherent states will be discussed in chapter IV).

The optimal measurement for coherent-state estimation, the POVM defined in Eq. (II.38), is equivalent to an Arthurs-Kelly measurement [5]. Such an Arthurs-Kelly measurement is effectively an attempt to simultaneously detect position and momentum. Optically, it is realized by means of a beam splitter: the mode of interest is split at a 50:50 beam splitter, and the position of one output mode and the momentum of the other output mode are detected. The simplest way to quantify the imperfect (but optimal) information gain through an Arthurs-Kelly measurement is in the Heisenberg representation and this will be shown in chapter IV.

Now we turn to the following question: how can an Arthurs-Kelly measurement involving the detection of *two* modes be equivalent to the *single-mode* POVM in Eq. (II.38)? In fact, here we encounter a general feature of POVM's. *Any* POVM-measurement corresponds to a projection measurement of a larger system consisting of the system for which the POVM is defined and a sufficiently large auxiliary system. In other words, any POVM is effectively a von Neumann measurement in a higher-dimensional Hilbert space. For discrete variables, this

equivalence is expressed by [162]

$$(\hat{E}_m)_{kl} = \sum_{ij} (\hat{P}_m)_{ki,lj} (\hat{\rho}_{\rm aux})_{ji} \ , \tag{II.41}$$

where the matrix element indices kl refer to the system that is subject to the POVM and the indices ij refer to the auxiliary system. The operators $\hat{P}_m$ are projectors in the extended Hilbert space. Translating this rule to continuous variables, we obtain for example in the position basis

$$\langle x|\hat{E}_\alpha|x'\rangle = \int dy\, dy' \, \langle x,y|\hat{P}_\alpha|x',y'\rangle\langle y'|\hat{\rho}_{\rm aux}|y\rangle \ , \tag{II.42}$$

where x, x' are the positions of the POVM-system and y, y' are those of the auxiliary system. This formula applies to any continuous-variable POVM, but here we shall use it for the coherent-state POVM of a single mode from Eq. (II.38). The left-hand-side of Eq. (II.42) then becomes

$$\frac{1}{\pi}\,\langle x|\alpha\rangle\langle\alpha|x'\rangle = \sqrt{\frac{2}{\pi^3}}\; e^{-(x-u)^2-(x'-u)^2+2iv(x-x')} \ , \tag{II.43}$$

according to Eq. (I.92) with $\alpha \equiv u + iv$. Equation (II.42) is now satisfied with the projector [6]

$$\begin{aligned} \hat{P}_\alpha &= |\Psi(u,v)\rangle\langle\Psi(u,v)| \\ &= \frac{1}{\pi}\int dx\, dx'\, e^{2iv(x-x')}|x\rangle\langle x'| \otimes |x-u\rangle\langle x'-u| \ , \end{aligned} \tag{II.45}$$

and the auxiliary mode

$$\hat{\rho}_{\rm aux} = \sqrt{\frac{2}{\pi}}\int dy\, dy'\, e^{-y^2-y'^2}\,|y\rangle\langle y'| \ . \tag{II.46}$$

In fact, the states $|\Psi(u,v)\rangle$ form a complete orthogonal set [see Eq. (IV.11)]. The auxiliary mode is a vacuum mode according to Eq. (I.89). The projectors

[6] In order to ensure $\hat{P}_\alpha^2 = \hat{P}_\alpha$, we have more precisely

$$\hat{P}_\alpha = \lim_{\epsilon\to 0}\int_{u-\epsilon}^{u+\epsilon}\int_{v-\epsilon}^{v+\epsilon} du'\, dv'\, |\Psi(u',v')\rangle\langle\Psi(u',v')| \ . \tag{II.44}$$

$|\Psi(u,v)\rangle\langle\Psi(u,v)|$ represent a projection on the "continuous-variable Bell basis", corresponding to a measurement of the relative position u and the total momentum v of the POVM-mode and the auxiliary vacuum mode. Interpreting this as an Arthurs-Kelly measurement, the vacuum mode is the input mode of the "unused port" of the beam splitter at which the POVM-mode (the coherent state to be estimated) is split. The position u of one beam splitter output mode and the momentum v of the other output mode are then detected. We will get back to this scheme in chapter IV.

2 Discrete-variable quantum teleportation

As an example of quantum communication with discrete variables, we consider now the entanglement-assisted transfer of quantum information: quantum teleportation with qu*d*its. The original quantum teleportation proposal by Bennett *et al.* referred to this finite-dimensional case [15]. Other quantum communication schemes originally proposed for discrete variables include dense coding [14] and quantum cryptrography [13]. An introduction to various discrete-variable, and in particular, qubit quantum communication schemes can be found for example in Ref. [165]. In the remainder of this chapter, we will consider qu*d*it quantum teleportation in order to provide the basis for a comparison with continuous-variable teleportation. Later, we will highlight the analogies and differences between these finite and infinite dimensional cases.

a The original teleportation proposal

How the original quantum teleportation protocol works can be seen with the following decomposition:

$$|\phi\rangle_{\rm in}\otimes|\Psi_{0,0}\rangle_{12} \;=\; \frac{1}{d}\sum_{\alpha,\beta=0}^{d-1}|\Psi_{\alpha,\beta}\rangle_{{\rm in},1}\hat{U}_2^\dagger(\alpha,\beta)|\phi\rangle_2\;. \tag{II.47}$$

Note that we use α and β here as *discrete* indices. The initial total state vector is a product of an arbitrary quantum state $|\phi\rangle_{\rm in}$ for the input qu*d*it and a particular maximally entangled state $|\Psi_{0,0}\rangle_{12}$ for qu*d*its 1 and 2. A projection measurement of the input qu*d*it and qu*d*it 1 onto the maximally entangled basis

$$|\Psi_{\alpha,\beta}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp(2\pi i k\beta/d)|k\rangle|k \oplus \alpha\rangle \tag{II.48}$$

reduces the above decomposition according to the measurement result. Applying the appropriate unitary transformation that corresponds to this measurement result to qu*d*it 2 leaves qu*d*it 2 exactly in the input state (the initial state of qu*d*it "in"). The unitary transformations are defined as

$$\hat{U}(\alpha,\beta) = \sum_{k=0}^{d-1} \exp(2\pi i k\beta/d)|k\rangle\langle k \oplus \alpha| \,, \tag{II.49}$$

and $\oplus$ means addition modulo d. The maximally entangled "qu*d*it Bell states" are indeed complete and orthonormal,

$$\begin{aligned} \sum_{\alpha,\beta=0}^{d-1} |\Psi_{\alpha,\beta}\rangle\langle\Psi_{\alpha,\beta}| &= \mathbb{1} \otimes \mathbb{1}, \\ \langle\Psi_{\alpha,\beta}|\Psi_{\alpha',\beta'}\rangle &= \delta_{\alpha\alpha'}\,\delta_{\beta\beta'} \,. \end{aligned} \tag{II.50}$$

The crucial point is that the quantum teleportation of an arbitrary quantum state from qu*d*it "in" to qu*d*it 2 is, in principle, not subject to any spatial limitations. Suppose a sender "Alice" and a receiver "Bob" initially share the maximally entangled state of qu*d*its 1 and 2 [7]. Alice is then capable of transferring an

[7] Of course, in reality, it is anything but trivial to distribute a maximally entangled state between two distant locations. When the entangled halves are sent through a "quantum channel", they are normally subject to various noise sources degrading the entanglement (the same noise sources prevent Alice reliably sending the input qu*d*it directly to Bob). A scheme called "entanglement purification" is known as a possible remedy. It uses classical communication and local operations and, in principle, enables Alice and Bob to retrieve the undegraded pure entangled state [17].

arbitrary and even unknown quantum state from her location to Bob's. All she has to do is jointly measure the qu*d*its "in" and 1 ("Bell measurement") and convey the measurement result to Bob via a classical communication channel. Finally, Bob has to apply an appropriate unitary transformation to qu*d*it 2. 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. Thus, to provide a test for quantum theory we henceforth assume neither parties know the identity of the state to be teleported. In this case, the state remains completely unknown to both throughout the entire quantum teleportation process [8].

2. The input qu*d*it does not remain in its initial state because of the Bell measurement. This fact ensures that no-cloning 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.

For qubits ($d = 2$), the maximally entangled states $|\Psi_{\alpha,\beta}\rangle$ become the four Bell states from Eq. (II.11). The unitary transformations are in this case given by the identiy, $\hat{U}(0,0) = |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}$, and the three Pauli operators [165],

$$\begin{aligned} \hat{U}(1,0) = |0\rangle\langle 1| + |1\rangle\langle 0| &\equiv \hat{\sigma}_x \equiv \hat{\sigma}_1 \ , \\ \hat{U}(1,1) = |0\rangle\langle 1| - |1\rangle\langle 0| &\equiv i\hat{\sigma}_y \equiv i\hat{\sigma}_2 \ , \\ \hat{U}(0,1) = |0\rangle\langle 0| - |1\rangle\langle 1| &\equiv \hat{\sigma}_z \equiv \hat{\sigma}_3 \ . \end{aligned} \tag{II.51}$$

Therefore, Bob accomplishes quantum teleporation by either flipping his qubit ($\hat{\sigma}_1$), flipping its relative phase ($\hat{\sigma}_3$), doing both ($\hat{\sigma}_2$), or doing nothing.

[8] In fact, the success of quantum teleportation crucially depends on the fact that Alice does not gain any information about the input state through her measurement, as we will see later.

b Imperfect and conclusive teleportation

In the original teleportation protocol, shared *maximum* entanglement is used to perfectly teleport a quantum state. What about using a pure nonmaximally entangled state? Let us study this case and write the entangled state in the Schmidt decomposition,

$$|\psi\rangle = \sum_{n=0}^{d-1} c_n |n\rangle|n\rangle \ . \tag{II.52}$$

We now consider the decomposition

$$|\phi\rangle_{\rm in} \otimes |\psi\rangle_{12} = \frac{1}{\sqrt{d}} \sum_{\alpha,\beta=0}^{d-1} |\Psi_{\alpha,\beta}\rangle_{{\rm in},1} \hat{U}_2^\dagger(\alpha,\beta) \sum_{n=0}^{d-1} c_{n\oplus\alpha} |n\rangle_2 \, {}_2\langle n|\phi\rangle_2 \ . \tag{II.53}$$

Apparently, a Bell measurement performed by Alice reduces Bob's qu*d*it 2 to a state which is no longer unitarily related to the *exact* input state $|\phi\rangle$, but only to an *approximate* version of it. In particular, this imperfect replica still depends on the measurement result α (later, for continuous variables, the analogous observation will prove crucial in the teleportation of entanglement). Connected with the imperfection of the teleported state is the fact that now Alice actually does gain some information about the input state through the Bell measurement (in contrast to point 1 in the previous section). We can conclude that a nonmaximally entangled state enables quantum teleportation of only limited quality. Nonetheless, this protocol still deserves to be called quantum teleportation, because the teleported state resembles the input state more than in any 'classical' scheme without entanglement. This can be shown using teleportation criteria such as those for qubits which we derive at the end of this chapter.

Finally, we shall discuss an alternative teleportation scheme using nonmaximally entangled states. It can be understood using the following decomposition [different from that of Eq. (II.53)],

$$|\phi\rangle_{\rm in} \otimes |\psi\rangle_{12} \ = \ \frac{1}{d} \sum_{\alpha,\beta=0}^{d-1} |\psi_{\alpha,\beta}\rangle_{{\rm in},1} \hat{U}_2^\dagger(\alpha,\beta) |\phi\rangle_2 \ , \tag{II.54}$$

where the nonmaximally entangled states $|\psi_{\alpha,\beta}\rangle$ are related to the state $|\psi\rangle \equiv |\psi_{0,0}\rangle$ in Eq. (II.52) through local unitary transformations,

$$|\psi_{\alpha,\beta}\rangle = \hat{U}(\alpha,\beta) \otimes \mathbb{1} \, |\psi\rangle \; . \tag{II.55}$$

These states are identical to the orthonormal complete Bell basis only when $c_n = 1/\sqrt{d}$. However, if Alice were able to distinguish between the nonorthogonal states $|\psi_{\alpha,\beta}\rangle$ and provide Bob with the corresponding information, Bob could exactly reconstruct the unknown input state. A reliable distinction of the states $|\psi_{\alpha,\beta}\rangle$ is, as we know, impossible. Notwithstanding this, Alice may use an appropriate POVM $\{\hat{E}_{\alpha,\beta}, \hat{E}_d\}$ in order to identify the state $|\psi_{\alpha,\beta}\rangle$ of qu*d*it "in" and 1 at least sometimes,

$$\begin{aligned} \langle\psi_{\alpha',\beta'}|\hat{E}_{\alpha,\beta}|\psi_{\alpha',\beta'}\rangle &\propto \delta_{\alpha\alpha'}\delta_{\beta\beta'} \; , \\ \hat{E}_d &\equiv \mathbb{1}^{\otimes 2} - \sum_{\alpha,\beta=0}^{d-1} \hat{E}_{\alpha,\beta} \; . \end{aligned} \tag{II.56}$$

For all other measurement outcomes she would obtain inconclusive results $\hat{E}_d$. Thus, at least sometimes, the input state is perfectly teleported to Bob despite the imperfect entanglement. This protocol is termed "conclusive teleportation" [146]. Son *et al.* showed how the appropriate POVM with $\hat{E}_{\alpha,\beta} \propto |\tilde{\psi}_{\alpha,\beta}\rangle\langle\tilde{\psi}_{\alpha,\beta}|$ and $\langle\tilde{\psi}_{\alpha,\beta}|\psi_{\alpha',\beta'}\rangle = \delta_{\alpha\alpha'}\delta_{\beta\beta'}$ can be constructed [193].

c *Universal teleportation with a twist*

A particularly striking feature of the quantum teleportation protocol presented in this chapter is that it can be formulated in a very compact universal fashion. The universal formalism relies on the observation that the entire protocol is describable by a "twist". Alice projects the input qu*d*it and qu*d*it 1 onto an arbitrary maximally entangled state and Bob "twists" the entangled state that he shares with Alice in accordance with her measurement result [34].

Let us explain this using equations. In any Hilbert space dimension, an arbitrary maximally entangled (basis) state can be written as [34] [9]

$$\hat{U}(\gamma) \otimes \mathbb{1} |\Psi\rangle\!\rangle = \mathbb{1} \otimes \hat{U}(\gamma') |\Psi\rangle\!\rangle \,, \tag{II.57}$$

with γ labelling a particular measurement result, $\hat{U}(\gamma') = \hat{U}^T(\gamma)$, for $|\Psi\rangle\!\rangle$ being any (other) maximally entangled state ("$|\cdots\rangle\!\rangle$" is used to emphasize that the state is bipartite). For example, for the above discrete-variable realization, the qu*d*it Bell states $|\Psi_{\alpha,\beta}\rangle$ from Eq. (II.48) may be written

$$\hat{U}(\gamma) \otimes \mathbb{1} \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle|n\rangle = \mathbb{1} \otimes \hat{U}(\gamma') \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle|n\rangle \,, \tag{II.58}$$

with $\hat{U}(\gamma) \equiv \hat{U}(\alpha, \beta)$ from Eq. (II.49). We now suppose that Alice's measurement yields the result

$$|\overrightarrow{\Psi}(\gamma)\rangle\!\rangle_{\text{in},1} \equiv \hat{U}(\gamma) \otimes \mathbb{1} \; |\Psi\rangle\!\rangle_{\text{in},1} \,. \tag{II.59}$$

Bob's task is then simply to 'twist' the entangled state he shares with Alice according to the result γ,

$$|\overleftarrow{\psi}(\gamma)\rangle\!\rangle_{1,2} \equiv \mathbb{1} \otimes \hat{U}(\gamma) \; |\psi\rangle\!\rangle_{1,2} \,. \tag{II.60}$$

The arrows here indicate which subsystem the unitary transformation acts upon. For the finite-dimensional case, the entire process is then described by

$$\begin{aligned} {}_{\text{in},1}\langle\langle \overrightarrow{\Psi}(\gamma)|\phi\rangle_{\text{in}} \otimes |\overleftarrow{\psi}(\gamma)\rangle\!\rangle_{1,2} &= \frac{1}{\sqrt{d}} \hat{U}(\gamma) \hat{\mathcal{D}} \hat{U}^\dagger(\gamma) \hat{\tau}_{2,\text{in}} |\phi\rangle_{\text{in}} \\ &= \frac{1}{\sqrt{d}} \hat{U}(\gamma) \hat{\mathcal{D}} \hat{U}^\dagger(\gamma) |\phi\rangle_2 \,, \end{aligned} \tag{II.61}$$

with the "transfer operator" defined

$$\hat{\tau}_{2,\text{in}} = \sum_{n=0}^{d-1} |n\rangle_{2\,\text{in}}\langle n| \,, \tag{II.62}$$

[9] This property is quite remarkable. The whole bipartite Hilbert space can be manipulated by applying just local unitary transformations to either of the two subsytems. A quantum communication protocol that exploits this feature is for example dense coding [14].

and the "distortion operator"

$$\hat{\mathcal{D}} = \sum_{n=0}^{d-1} c_n |n\rangle\langle n| \,, \tag{II.63}$$

which expresses the effect of the nonmaximally entangled channel [Eq. (II.52)]. It is proportional to the identity only for a maximally entangled channel. Only in this case does the right-hand-side of Eq. (II.61), i.e., the unnormalized teleported state, become exactly the input state. More generally, the (normalized) teleported state is a distorted version of the input state:

$$\frac{\hat{U}_2(\gamma)\hat{\mathcal{D}}_2\hat{U}_2^\dagger(\gamma)|\phi\rangle_2}{\|\hat{U}_2(\gamma)\hat{\mathcal{D}}_2\hat{U}_2^\dagger(\gamma)|\phi\rangle_2\|} \,. \tag{II.64}$$

The twist formalism described here is universal. Hence we shall make use of it later for continuous variables. We will then find out that under certain circumstances, twisting the shared entangled state according to Alice's measurement result is not necessarily the optimal operation for Bob.

d Criteria for qubit teleportation

When we later consider (imperfect) continuous-variable teleportation, it will be important to quantify the distinction between classical teleportation (quantum state transfer without using entanglement) and quantum teleportation (enhanced quantum state transfer using entanglement). We will then extensively discuss teleportation criteria. However, at this point, it shall be sufficient to answer the following question: What is the best overlap between Alice's input qubit state $\hat{\rho}_{\rm in}$ and Bob's output qubit state $\hat{\rho}_{\rm out}$ achievable without the use of entanglement? The overlap shall be described by the so-called fidelity $F \equiv \langle\psi_{\rm in}|\hat{\rho}_{\rm out}|\psi_{\rm in}\rangle$ [178], with the pure input state $\hat{\rho}_{\rm in} = |\psi_{\rm in}\rangle\langle\psi_{\rm in}|$. This input state shall be assumed to be an arbitrary qubit state, here written as [165]

$$|\psi_{\rm in}\rangle \equiv |\psi_{\theta_0,\phi_0}\rangle = \cos\frac{\theta_0}{2}\, e^{-i\phi_0/2}|0\rangle + \sin\frac{\theta_0}{2}\, e^{+i\phi_0/2}|1\rangle \,. \tag{II.65}$$

The parameters θ_0 and ϕ_0 are unknown to Alice and Bob as previously discussed. Without sharing entanglement with Bob, the best Alice can do is estimate θ_0 and ϕ_0 and inform Bob about her estimation via a classical communication channel. The optimal measurement that enables this estimation can be described by the POVM

$$\hat{E}_{\theta,\phi} = 2\pi |\psi_{\theta,\phi}\rangle\langle\psi_{\theta,\phi}| \,, \tag{II.66}$$

with

$$\int \frac{d\Omega}{4\pi}\, \hat{E}_{\theta,\phi} = \frac{1}{4\pi} \int_0^{2\pi} d\phi \int_0^{\pi} d\theta \, \sin\theta \, \hat{E}_{\theta,\phi} = \mathbb{1} \,. \tag{II.67}$$

The probabilities for obtaining the corresponding results of the POVM,

$$p(\theta,\phi)\,\frac{d\Omega}{4\pi} = \langle\psi_{\theta_0,\phi_0}|\hat{E}_{\theta,\phi}|\psi_{\theta_0,\phi_0}\rangle\,\frac{d\Omega}{4\pi} = |\langle\psi_{\theta,\phi}|\psi_{\theta_0,\phi_0}\rangle|^2\,\frac{d\Omega}{2\pi} \,, \tag{II.68}$$

and the overlap for the corresponding states $|\psi_{\theta,\phi}\rangle$ generated by Bob based on these results, $|\langle\psi_{\theta,\phi}|\psi_{\theta_0,\phi_0}\rangle|^2$, yield the overall fidelity

$$F = \int \frac{d\Omega}{4\pi}\, p(\theta,\phi)\, |\langle\psi_{\theta,\phi}|\psi_{\theta_0,\phi_0}\rangle|^2 = \int \frac{d\Omega}{2\pi}\, |\langle\psi_{\theta,\phi}|\psi_{\theta_0,\phi_0}\rangle|^4 = 2/3 \,. \tag{II.69}$$

Note that this fidelity does not depend on the parameters θ_0 and ϕ_0 of the particular input state. Any input state is "teleported" (through classical teleportation) with the same fidelity $F = 2/3$. This fidelity value represents the boundary between classical and quantum teleportation when unknown qubit states are to be transmitted. It was derived by Massar and Popescu [142] using a more general and complete approach than ours here, by taking arbitrary measurements into account. Massar and Popescu's aim thereby was to determine the maximum amount of information that can be extracted from a qubit state and how this maximum may be gained. This maximum information gain increases when not just a single qubit but N identical qubits are available. For this generalization, Massar and Popescu found the optimum fidelities $F = (N+1)/(N+2)$ [142].

We have seen that the overlap of the output state with the input state after optimal classical teleportation does not depend on the input state (for arbitrary qubit input states) and is always given by the fidelity $F = 2/3$. This fact can be expressed in terms of the Bloch vector representation [165] in which the output state of optimal classical teleportation looks like

$$\hat{\rho}_{\text{out}} = \frac{1}{2}[\mathbb{1} + \bar{\eta}_{\text{meas}}(1)\vec{s}_{\text{in}} \cdot \vec{\sigma}] \,, \tag{II.70}$$

for an input state of the form

$$\hat{\rho}_{\text{in}} = \frac{1}{2}\begin{pmatrix} 1 + s_{\text{in},3} & s_{\text{in},1} - is_{\text{in},2} \\ s_{\text{in},1} + is_{\text{in},2} & 1 - s_{\text{in},3} \end{pmatrix} = \frac{1}{2}(\mathbb{1} + \vec{s}_{\text{in}} \cdot \vec{\sigma}) \,, \tag{II.71}$$

where $\bar{\eta}_{\text{meas}}(1) = 1/3$, and $\vec{\sigma} = (\sigma_1 \;\; \sigma_2 \;\; \sigma_3)^T$ with the Pauli matrices [165]

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \,, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \,, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \,. \tag{II.72}$$

The input state $\hat{\rho}_{\text{in}} = |\psi_{\theta_0,\phi_0}\rangle\langle\psi_{\theta_0,\phi_0}|$ has a density matrix

$$\hat{\rho}_{\text{in}} = \frac{1}{2}\mathbb{1} + \frac{1}{2}\begin{pmatrix} \cos\theta_0 & \sin\theta_0 e^{-i\phi_0} \\ \sin\theta_0 e^{+i\phi_0} & -\cos\theta_0 \end{pmatrix} \,, \tag{II.73}$$

which is identical to the density matrix in Eq. (II.71) when

$$\vec{s}_{\text{in}} = (s_{\text{in},1} \;\; s_{\text{in},2} \;\; s_{\text{in},3})^T = (\sin\theta_0\cos\phi_0 \;\; \sin\theta_0\sin\phi_0 \;\; \cos\theta_0)^T \,. \tag{II.74}$$

The Bloch vector $\vec{s}_{\text{in}}$ fully describes the input qubit state. In the Bloch sphere, it points into the direction specified by the spherical coordinates θ_0 and ϕ_0. The vector's tip lies on the surface of the Bloch sphere, representing a pure state with $|\vec{s}_{\text{in}}| = 1$. For mixed states, we would have $|\vec{s}| < 1$. Therefore, according to Eq. (II.70) and Eq. (II.71), the effect of optimal classical teleportation can be interpreted as a process that shrinks the input Bloch vector and hence turns the pure input state into a mixed output state without changing the Bloch vector's orientation. Optimal classical teleportation based on the optimal measurement

for state estimation attains the maximum shrinking factor $\bar{\eta}_{\rm meas}(1) = 1/3$, corresponding to a fidelity $F = \langle\psi_{\theta_0,\phi_0}|\hat{\rho}_{\rm out}|\psi_{\theta_0,\phi_0}\rangle = 2/3$. If Alice had access to more than just a single copy of the input qubit state, say, an ensemble of N identical qubits, the optimal (maximum) shrinking factor would be enhanced, $\bar{\eta}_{\rm meas}(N) = N/(N+2)$, and so would the fidelity when $\bar{\eta}_{\rm meas}(1)$ is replaced by $\bar{\eta}_{\rm meas}(N)$ in Eq. (II.70),

$$F = \langle\psi_{\theta_0,\phi_0}|\hat{\rho}_{\rm out}|\psi_{\theta_0,\phi_0}\rangle = \frac{1}{2} + \frac{\bar{\eta}_{\rm meas}(N)}{2} = \frac{N+1}{N+2}\,. \tag{II.75}$$

This is Massar and Popescu's previously mentioned result for the maximal information gain from N qubits. The corresponding optimal measurement, however, must treat the N qubits as an entity (as a single composite system), whereas separate measurements on each qubit never provide the optimum result [142].

In this chapter, we have presented some basics of quantum information theory that we may either directly apply to continuous quantum variables or with an appropriate "translation". The original results on discrete-variable quantum information and communication will also serve as a comparison for developing continuous-variable protocols. Let us now enter the realm of quantum information with continuous variables.

III

The Resource: Continuous-Variable Entanglement

Entanglement is the essential ingredient in many quantum communication protocols. In the preceding chapter, quantum teleportation was presented as an example for entanglement-based quantum communication. There, we considered quantum teleportation of quantum states defined in a finite-dimensional Hilbert space (described by discrete variables). Among those, the two-dimensional qubit states play the most important role. Most quantum communication protocols were first proposed for qubits. From a conceptual point of view, qubit states represent the simplest manifestation of the quantum mechanical superposition principle, and they are most appropriate for quantum computation purposes being the natural extension of classical bits to the quantum realm.

Generating qubit entanglement experimentally, however, is a difficult task. It can be done in a quantum optical setting via weak down-conversion producing polarization-entangled single photons, but the resulting maximum entanglement is 'polluted' by a large vacuum contribution. The consequence of this is that the entanglement never emerges from the device in an event-ready fashion. Any verification of the presence of entanglement and also any exploitation of it for quantum communication must therefore rely on post-selection [38, 121, 120]. Since successful post-selected events occur very rarely, one has to cope with very low efficiency in these single-photon schemes [1]. Furthermore, if the goal is to create

[1] The issue of post-selection not only affects the efficiency, but also the quality of the perfor-

entanglement between more than two qubits (multipartite rather than bipartite entanglement), these difficulties accumulate. Nevertheless, great progress has been made in generating single-photon entanglement in a post-selected manner, both for the case of two qubits [23] and three qubits [24].

Interestingly, from a historial perspective, the notion of quantum entanglement appeared in the literature first in 1935, long before the dawn of the relatively young field of quantum information, and without any reference to qubit states. In fact, the entangled states treated in that paper by Einstein, Podolsky, and Rosen [81] were two-particle states quantum mechanically correlated with respect to the continuous variables position and momentum. Although important milestones in quantum information theory have been derived and expressed in terms of qubits or discrete variables (e.g., the no-cloning theorem [207] or the proposal of quantum teleportation [15], as shown in the previous chapter), the notion of quantum entanglement itself first came to light in a continuous-variable setting.

Despite the conceptual complications when dealing with continuous variables and superposition states in infinite-dimensional Hilbert spaces, are there possibly any advantages by considering continuous-variable entanglement as a resource for quantum communication? In fact, we will see that the entanglement between the continuous quadrature amplitudes of single-mode light fields (or of broadband light fields in a more realistic description) can be produced in a very efficient way without the need of post-selection. An important (and new) result will be that this statement applies not only to bipartite entanglement, but also to multipartite entanglement shared by an arbitrary number of parties. Continuous-variable entanglement turns out to be extraordinarily cheap. The building ingredients will be simple state-of-the-art elements from nonlinear quantum optics (squeezers) and from linear optics (beam splitters). It will depend on the quality of the

mance when using this single-photon entanglement for quantum communication. This is also discussed in Refs. [38, 121, 120]. Recently, new ideas in that direction were proposed by Knill *et al.* [119].

squeezers how much entanglement is generated every inverse bandwidth time.

In this chapter, we will first review inseparability criteria for bipartite continuous-variable systems, as proposed in Refs. [188, 74, 196]. We will also analyze the inseparability of qu*d*it Werner states in the infinite-dimensional limit. Some of these considerations concerning bipartite systems will then be extended to multipartite systems. A simple and very useful universal inseparability criterion for multi-party states of any dimension will be derived. We will then give quantum circuits for generating continuous-variable entanglement, first for the known two-party case, and then in a general multi-party setting, as proposed by van Loock and Braunstein [132]. Moreover, we will discuss properties of the multipartite entangled continuous-variable states, including their ability to violate multi-party Bell-type inequalitites imposed by local realism (based on van Loock and Braunstein [133]). Finally, we will present a realistic broadband description for the continuous-variable entangled states and their generation [155, 136].

1 Inseparability of continuous-variable systems

In this section, we are investigating the inseparability of continuous-variable systems. First, we focus on inseparability criteria applicable to general bipartite systems and in particular Gaussian states, before we turn to bipartite Werner-like states in infinite dimensions. Based on this, we are able to consider possible extensions of these results to more than two parties.

a *Criteria for bipartite entanglement*

In the previous chapter, it was pointed out that the majority of pure bipartite states is entangled rather than factorizable, which can be seen from the Schmidt decomposition. For the more subtle case of mixed states, inseparability is revealed when the density operator cannot be written as a convex sum of products of density operators. A simple (generally only sufficient) criterion to recognize

bipartite entanglement in the case of arbitrary mixed quantum states of two discrete-variable systems is the partial transpose criterion [163]: if the state is separable, its density matrix must remain legitimate with non-negative eigenvalues after either subsystem's density matrix has been transposed. Negative eigenvalues indicate an inseparable state. In general, if the bipartite states are pure, their degree of entanglement can be quantified by the partial entropy, i.e., by tracing out either subsystem and calculating the von Neumann entropy of the remaining system [16]. This partial trace for pure states and the partial transpose for arbitrary states are theoretical means to "witness" entanglement. Measuring violations of Bell inequalitites is an example of an experimental method for witnessing entanglement.

From a theoretical point of view, it was only recently that some light was cast on the bipartite entanglement of continuous-variable systems [188, 74, 196]. At first sight it is anything but clear whether inseparability criteria developed for discrete-variable systems such as the partial transpose can be directly translated and applied to continuous-variable systems. Moreover, the partial transpose criterion turns out to be only a sufficient condition for the inseparability of two discrete systems, except for the (2×2)- and (2×3)-dimensional cases, for which it then provides both a sufficient and a necessary condition. Bearing this in mind, one might expect that a possible infinite-dimensional, continuous-variable version of the partial transpose criterion yields at best a sufficient and not a necessary condition, as it does for higher-dimensional discrete systems. In fact, Simon showed that for the general case of *arbitrary continuous-variable states*, this assumption proves correct [188]. However, Simon also demonstrated that for *Gaussian states*, the partial transpose criterion represents not only a sufficient, but also a necessary inseparability condition [188] [2]. Simon's approach is based

[2]However, this result of Simon only applies to the simplest bipartite systems with a single oscillator (mode) at each side. It was shown by Werner and Wolf [204] that for more degrees of freedom, e.g., two oscillators at each side, inseparable Gaussian states having positive partial

on the identification of the partial transpose as a mirror reflection in phase space. A similar inseparability criterion, applicable to continuous-variable systems and expressed in terms of an inequality for certain variances involving position and momentum operators, was derived by Duan *et al.* using a strategy independent of the partial transpose [74]. This criterion also turns out to be a necessary and sufficient condition for inseparability, when Gaussian states are considered.

The criteria of Simon and Duan et al.: According to the definition of the N-mode correlation matrix $V^{(N)}$ in Eq.(I.127), let us write the correlation matrix of an arbitrary bipartite two-mode system (mean values can always be eliminated through local unitary transformations) in block form,

$$V^{(2)} = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} , \tag{III.1}$$

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 [188],

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

where J is the 2×2 matrix

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} . \tag{III.3}$$

Note that as opposed to Simon's convention with $[\hat{x}, \hat{p}] = i$ ($\hbar = 1$), we stick with those introduced in chapter I, $[\hat{x}, \hat{p}] = i/2$ ($\hbar = 1/2$). Any separable bipartite state satisfies the inequality of Eq. (III.2), so that it represents a necessary condition for separability, and hence its violation is a sufficient condition for inseparability. We note that this condition is invariant under local unitary transformations of the subsystems. The inequality Eq. (III.2) is a consequence of the fact that the two-mode uncertainty relation, Eq. (I.130) with

transpose ("bound entangled Gaussian states") exist.

$N = 2$, is preserved under partial transpose [mirror reflection in phase space: $W(x_1, p_1, x_2, p_2) \to W(x_1, p_1, x_2, -p_2)$], provided the state is separable. The uncertainty relation itself, Eq. (I.130) with $N = 2$, satisfied by any physical bipartite state before possible partial transpose, is almost identical to Eq. (III.2), with $\det C$ instead of $|\det C|$. It follows that states with $\det C \geq 0$, whether separable or not, definitely obey Eq. (III.2). Therefore, in general, inseparability can only (but need not necessarily) be witnessed for those inseparable states with $\det C < 0$.

Let us now define the following two standard forms for the correlation matrix:

$$V_I^{(2)} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & c' \\ c & 0 & b & 0 \\ 0 & c' & 0 & b \end{pmatrix}, \tag{III.4}$$

and

$$V_{II}^{(2)} = \begin{pmatrix} a_1 & 0 & c_1 & 0 \\ 0 & a_2 & 0 & c_2 \\ c_1 & 0 & b_1 & 0 \\ 0 & c_2 & 0 & b_2 \end{pmatrix}, \tag{III.5}$$

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

$$\begin{aligned} \frac{a_1 - 1/4}{b_1 - 1/4} &= \frac{a_2 - 1/4}{b_2 - 1/4}, \\ |c_1| - |c_2| &= \sqrt{(a_1 - 1/4)(b_1 - 1/4)} - \sqrt{(a_2 - 1/4)(b_2 - 1/4)}. \end{aligned} \tag{III.6}$$

Any correlation matrix can be transformed into the first standard form $V_I^{(2)}$ via appropriate local canonical transformations [188] (or local linear unitary Bogoliubov operations, LLUBO's [74, 28]). From the first standard form $V_I^{(2)}$, two appropriate local squeezing operations can always lead to the second standard form $V_{II}^{(2)}$ [74]. Note here that according to our definition of the correlation

matrix, its elements each contain a vacuum scale factor of 1/4 (corresponding to $\hbar = 1/2$), differing from Duan *et al.*'s convention where matrix elements are normalized to the vacuum.

For the standard form $V_I^{(2)}$, the necessary separability condition of Eq. (III.2) simplifies to

$$16(ab - c^2)(ab - c'^2) \geq (a^2 + b^2) + 2|cc'| - \frac{1}{16}. \tag{III.7}$$

Simon's criterion does not rely on that specific standard form and can, in fact, be applied to an arbitrary state (even non-Gaussian states) using Eq. (III.2). For Gaussian states, however, Eq. (III.2) turns out to be both a necessary and a sufficient condition for separability. This important result can still be directly applied to any Gaussian state as no specific standard form is required. In order to prove this result, Simon used the fact that Gaussian states with

$$\det C \geq 0 \tag{III.8}$$

are separable, which is by itself a useful result [188]. By contrast, the criterion proposed by Duan *et al.* [74] requires the standard form $V_{II}^{(2)}$ to follow through as a necessary and sufficient condition for Gaussian states. Its application therefore depends on that standard form $V_{II}^{(2)}$. Expressed in terms of the elements of $V_{II}^{(2)}$, this criterion reads

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq \frac{a_0^2}{2} + \frac{1}{2a_0^2}, \tag{III.9}$$

where

$$\begin{aligned} \hat{u} &= a_0\hat{x}_1 - \frac{c_1}{|c_1|a_0}\hat{x}_2, \\ \hat{v} &= a_0\hat{p}_1 - \frac{c_2}{|c_2|a_0}\hat{p}_2, \\ a_0^2 &= \sqrt{\frac{b_1 - 1/4}{a_1 - 1/4}} = \sqrt{\frac{b_2 - 1/4}{a_2 - 1/4}}, \end{aligned} \tag{III.10}$$

and the bipartite state of interest $\hat{\rho}$ has been labeled ρ. Without the assumption of Gaussian states and without the need of any standard form for the correlation matrix, an alternative approach leads to an inequality similar to Eq. (III.9), representing a necessary condition for separability (a sufficient condition for inseparability through its violation) for arbitrary states,

$$\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho \geq \frac{\bar{a}^2}{2} + \frac{1}{2\bar{a}^2}, \tag{III.11}$$

with

$$\begin{aligned} \hat{u} &= |\bar{a}|\hat{x}_1 - \frac{1}{\bar{a}}\hat{x}_2, \\ \hat{v} &= |\bar{a}|\hat{p}_1 + \frac{1}{\bar{a}}\hat{p}_2. \end{aligned} \tag{III.12}$$

Here, $\bar{a}$ is an arbitrary nonzero real parameter. One can use Eq. (III.11), satisfied by *any* separable state, in order to reveal that Eq. (III.9) is a necessary separability condition for the special case of Gaussian states. However, only for this special case does Eq. (III.9) also represent a sufficient separability condition.

Let us also mention at this point that a similar (but weaker) inseparability criterion was derived by Tan [196], namely the necessary condition for any separable state

$$\langle(\Delta\hat{u})^2\rangle_\rho\langle(\Delta\hat{v})^2\rangle_\rho \geq \frac{1}{4}, \tag{III.13}$$

with $\bar{a} = 1$ in Eq. (III.12). It is simply the product version of the sum condition in Eq. (III.11) (with $\bar{a} = 1$). In the next chapter, we will encounter inseparable states that do not violate Duan *et al.*'s condititon Eq. (III.11) (with $\bar{a} = 1$), but do violate Tan's condition Eq. (III.13), thereby revealing their inseparability. Finally, we emphasize that the sufficient inseparability criteria of Eq. (III.11) (with $\bar{a} = 1$) and Eq. (III.13) are useful for witnessing entanglement not only theoretically, but also experimentally. An indirect experimental confirmation of the presence of entanglement then relies 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 beamsplitter [196].

b Bipartite Werner-like states in infinite dimensions

In this section, we gain some insight about the inseparability of quantum states defined in an infinite-dimensional Hilbert space by examining the d-level Werner states and taking the limit $d \to \infty$.

It is important to have practically applicable inseparability criteria especially for the case of mixed states, where even bipartite inseparability is less obvious. Discrete-variable inseparability criteria applied to the generalized two-party Werner states [mixtures of the maximally mixed state $\mathbb{1}^{\otimes 2}/d^2$ and a d^2-dimensional maximally entangled state, Eq. (II.24) with $N = 2$] show that these states are separable if and only if $p \leq 1/(1+d)$ [77, 176]. For example, this condition can be derived using criteria based on the theory of majorization [152]. For qubits ($d = 2$), the condition $p \leq 1/3$ had been found already by Peres [163], with the help of his partial transpose criterion (see chapter II). With respect to the continuous variables, it is illuminating to look at the infinite-dimensional limit $d \to \infty$ for these results. This limit implies that the corresponding Werner-like states $\hat{\rho}_{\mathrm{W}}^{(2,\infty)}$ are separable if and only if $p = 0$.

We obtain an analogous result when we analyze the separability of (d^2-dimensional) bipartite states near the maximally mixed state, $(1 - \epsilon)\mathbb{1}^{\otimes 2}/d^2 + \epsilon\hat{\rho}$, with $\hat{\rho}$ being an arbitrary bipartite state. For qu*d*its, we know that all states with $\epsilon \leq 1/(1 + d^3)$ are separable, and that there are inseparable states for $\epsilon > 1/(1 + d)$ [176] (which are the generalizations of the previous results for qubits [33] and qutrits [55]). The infinite-dimensional limit yields an arbitrarily small ϵ-neighbourhood around the maximally mixed state which is completely inseparable. Using a more elementary approach, the same result was obtained by Clifton and Halvorson with respect to inseparability [62], and by Clifton, Halvorson, and Kent also with regard to nonlocality, i.e., violation of Bell inequalitites (see section 4 of this chapter) [63]: bipartite states in an infinite-dimensional Hilbert space can be arbitrarily close to the maximally mixed state, and yet be

inseparable and nonlocal. Apparently, it is hard to eliminate entanglement in an infinite-dimensional Hilbert space by adding arbitrarily large classical noise in a Werner-like state [3]. The quality of the entanglement may deteriorate, but the inseparability does not vanish. We will encounter a similar behaviour for continuous-variable entanglement later in the context of entanglement swapping.

We introduced the continuous-variable inseparability criteria in all their various appearances, because we will make extensive use of them. Using the approach for deriving the necessary separability condition Eq. (III.11) in the case of arbitrary bipartite states [74], we will now investigate whether that condition can be generalized to arbitrary multipartite states. Further inseparability criteria for bipartite continuous-variable systems will be discussed in chapter IV. There we will introduce an operational inseparability criterion. It relies on the fact that quantum states that enable quantum teleporation with fidelity better than classical must be inseparable. For qubits, we have already presented such an operational criterion in chapter II, by deriving the classical-quantum fidelity boundary of qubit teleportation of $F = 2/3$.

c *Criteria for multipartite entanglement*

In chapter II, we pointed out that multipartite entanglement is a more complex and subtle matter than bipartite entanglement. Multipartite entanglement is of

[3] Recently, Nielsen *et al.* [148] suggested to consider infinite-dimensional Werner-like states from the outset, rather than simply taking the qu*d*it results for $d \to \infty$. These bipartite Werner-like states are $\hat{\rho}_{\mathrm{W}}^{(2,\infty)} = p|\psi^{(2)}(\lambda)\rangle\langle\psi^{(2)}(\lambda)| + (1-p)\hat{\rho}_{\mathrm{th}} \otimes \hat{\rho}_{\mathrm{th}}$ [148], where $|\psi^{(2)}(\lambda)\rangle$ is a two-mode squeezed state [as introduced later in Eq. (III.24)]. The single-mode thermal state $\hat{\rho}_{\mathrm{th}} = \mathrm{Tr}_1|\psi^{(2)}(\lambda)\rangle\langle\psi^{(2)}(\lambda)| = \mathrm{Tr}_2|\psi^{(2)}(\lambda)\rangle\langle\psi^{(2)}(\lambda)|$ mimicks a maximally mixed state [with the Wigner function in Eq. (III.31)], although it is truly maximally mixed only for infinite squeezing, when the two-mode squeezed state becomes maximally entangled. Preliminary results using the majorization-based inseparability criterion [152] do not verify that $\hat{\rho}_{\mathrm{W}}^{(2,\infty)}$ is inseparable for any $p > 0$ and any nonzero squeezing [148]. However, the reason for this may be the weakness of the only sufficient inseparability criterion based on majorization.

great importance for many quantum information processing and communication protocols, but, in particular, its quantification turns out to be rather difficult for any Hilbert space dimensions, even when the states in question are pure. Therefore, in the case of continuous variables, we may focus on the following questions: How can we generate and recognize multipartite entangled states? How do they compare to their discrete-variable, and in particular qubit counterparts with respect to various properties? For three qubits for example, we know from chapter II that there are two classes of pure tripartite entanglement, which are inequivalent under SLOCC. These are represented by the "maximally entangled" GHZ state

$$|\mathrm{GHZ}^{(3,2)}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) , \tag{III.14}$$

and the "non-maximally entangled" W state

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right) . \tag{III.15}$$

Before we investigate the continuous-variable analogues and how they might be produced, let us first see how their entanglement may be witnessed.

A sufficient inseparability criterion á la Duan et al.: The inseparability criterion for continuous-variable two-party states of Eq. (III.11) is expressed in terms of variances of quadrature combinations such as $\hat{x}_1 - \hat{x}_2$ and $\hat{p}_1 + \hat{p}_2$. It is motivated by the fact that the maximally entangled bipartite state $\int dx\, |x, x\rangle$ is a simultaneous zero-eigenstate of these two combinations [74]. In a similar way, motivated by the fact that the tripartite entangled state $\int dx\, |x, x, x\rangle$ is an eigenstate with total momentum zero and relative positions $x_i - x_j = 0$ $(i, j = 1, 2, 3)$, let us now assume three parties or three modes described by continuous variables and derive an inequality in terms of variances of the combinations

$$\hat{u} = \hat{x}_1 - \hat{x}_2 , \quad \hat{v} = \hat{x}_1 - \hat{x}_3 , \quad \hat{w} = \hat{x}_2 - \hat{x}_3 , \quad \hat{t} = \sqrt{2}(\hat{p}_1 + \hat{p}_2 + \hat{p}_3) . \tag{III.16}$$

Let us further assume that the three-party state $\hat{\rho}$ is fully separable and can be written as

$$\hat{\rho} = \sum_i p_i \, \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3} \, . \tag{III.17}$$

Using this state, we can calculate the total variance of the operators in Eq. (III.16):

$$\begin{aligned}
& \langle (\Delta\hat{u})^2 \rangle_\rho + \langle (\Delta\hat{v})^2 \rangle_\rho + \langle (\Delta\hat{w})^2 \rangle_\rho + \langle (\Delta\hat{t})^2 \rangle_\rho \\
= & \sum_i p_i \, \left(\langle \hat{u}^2 \rangle_i + \langle \hat{v}^2 \rangle_i + \langle \hat{w}^2 \rangle_i + \langle \hat{t}^2 \rangle_i \right) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 - \langle \hat{w} \rangle_\rho^2 - \langle \hat{t} \rangle_\rho^2 \\
= & \sum_i p_i \, 2 \, \left(\langle \hat{x}_1^2 \rangle_i + \langle \hat{x}_2^2 \rangle_i + \langle \hat{x}_3^2 \rangle_i + \langle \hat{p}_1^2 \rangle_i + \langle \hat{p}_2^2 \rangle_i + \langle \hat{p}_3^2 \rangle_i \right) \\
- & \sum_i p_i \, 2 \Big(\langle \hat{x}_1 \rangle_i \langle \hat{x}_2 \rangle_i + \langle \hat{x}_1 \rangle_i \langle \hat{x}_3 \rangle_i + \langle \hat{x}_2 \rangle_i \langle \hat{x}_3 \rangle_i - 2 \langle \hat{p}_1 \rangle_i \langle \hat{p}_2 \rangle_i \\
& \qquad - 2 \langle \hat{p}_1 \rangle_i \langle \hat{p}_3 \rangle_i - 2 \langle \hat{p}_2 \rangle_i \langle \hat{p}_3 \rangle_i \Big) - \langle \hat{u} \rangle_\rho^2 - \langle \hat{v} \rangle_\rho^2 - \langle \hat{w} \rangle_\rho^2 - \langle \hat{t} \rangle_\rho^2 \\
= & \sum_i p_i \, 2 \Big(\langle (\Delta\hat{x}_1)^2 \rangle_i + \langle (\Delta\hat{x}_2)^2 \rangle_i + \langle (\Delta\hat{x}_3)^2 \rangle_i \\
& \qquad + \langle (\Delta\hat{p}_1)^2 \rangle_i + \langle (\Delta\hat{p}_2)^2 \rangle_i + \langle (\Delta\hat{p}_3)^2 \rangle_i \Big) \\
+ & \sum_i p_i \, \langle \hat{u} \rangle_i^2 - \left(\sum_i p_i \, \langle \hat{u} \rangle_i \right)^2 + \sum_i p_i \, \langle \hat{v} \rangle_i^2 - \left(\sum_i p_i \, \langle \hat{v} \rangle_i \right)^2 \\
+ & \sum_i p_i \, \langle \hat{w} \rangle_i^2 - \left(\sum_i p_i \, \langle \hat{w} \rangle_i \right)^2 + \sum_i p_i \, \langle \hat{t} \rangle_i^2 - \left(\sum_i p_i \, \langle \hat{t} \rangle_i \right)^2 \, ,
\end{aligned} \tag{III.18}$$

where $\langle \cdots \rangle_i$ means the average in the product state $\hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \hat{\rho}_{i3}$. Similar to Ref. [74], we can apply the Cauchy-Schwarz inequality $\sum_i p_i \langle \hat{u} \rangle_i^2 \geq (\sum_i p_i |\langle \hat{u} \rangle_i|)^2$, and see that the last two lines in Eq. (III.18) are bounded below by zero. Also taking into account the sum uncertainty relation $\langle (\Delta\hat{x}_j)^2 \rangle_i + \langle (\Delta\hat{p}_j)^2 \rangle_i \geq |[\hat{x}_j, \hat{p}_j]| = 1/2$ $(j = 1, 2, 3)$, we find that the total variance itself [the first line in Eq. (III.18)] is bounded below by 3. Any total variance smaller than this boundary of 3 would imply that the quantum state concerned is not *fully separable* as in Eq. (III.17) and that it hence contains some kind of entanglement. But would this also imply that the quantum state is genuinely tripartite entangled in the sense that none of the parties can be separated from the others (as in the pure qubit states

$|\mathrm{GHZ}^{(3,2)}\rangle$ and $|\mathrm{W}\rangle$)? Unfortunately, a total variance below 3 does not rule out the possibility of *partial separability*. The quantum state might still not be a true tripartite entangled state, since it might be written in one or more of the following forms [4] [79]:

$$\hat{\rho} = \sum_i p_i \, \hat{\rho}_{i12} \otimes \hat{\rho}_{i3}, \quad \hat{\rho} = \sum_i p_i' \, \hat{\rho}_{i13} \otimes \hat{\rho}_{i2}, \quad \hat{\rho} = \sum_i p_i'' \, \hat{\rho}_{i23} \otimes \hat{\rho}_{i1}. \tag{III.19}$$

Thus, in general, a violation of $\langle(\Delta\hat{u})^2\rangle_\rho + \langle(\Delta\hat{v})^2\rangle_\rho + \langle(\Delta\hat{w})^2\rangle_\rho + \langle(\Delta\hat{t})^2\rangle_\rho \geq 3$ does not necessarily witness true tripartite entanglement. However, it will whenever the quantum state in question is pure and totally symmetric with respect to all three subsystems (this argument will be discussed in more detail in section 3 of this chapter). In that case, a possible separation of any individual subsystem,

$$\hat{\rho} = \hat{\rho}_{12} \otimes \hat{\rho}_3, \quad \hat{\rho} = \hat{\rho}_{13} \otimes \hat{\rho}_2, \quad \hat{\rho} = \hat{\rho}_{23} \otimes \hat{\rho}_1, \tag{III.20}$$

implies full separability, $\hat{\rho} = \hat{\rho}_1 \otimes \hat{\rho}_2 \otimes \hat{\rho}_3$. Hence a total variance below 3 negates the possibility of any form of separability in this case.

By extending the combinations in Eq. (III.16) from 3 to N parties and performing a similar calculation as for $N = 3$, we find that any *fully separable* state $\hat{\rho} = \sum_i p_i \, \hat{\rho}_{i1} \otimes \hat{\rho}_{i2} \otimes \cdots \otimes \hat{\rho}_{iN}$ obeys the inequality

$$\mathcal{V}(N) \equiv \frac{1}{2} \sum_{i,j}^{N} \langle[\Delta(\hat{x}_i - \hat{x}_j)]^2\rangle_\rho + (N-1) \left\langle \left[\Delta \left(\sum_{i=1}^{N} \hat{p}_i \right)\right]^2 \right\rangle_\rho \geq \frac{N(N-1)}{2} \, . \tag{III.21}$$

Here, we have defined the total variance $\mathcal{V}(N)$ of possible quadrature combinations for N-party states in a suitable manner. In the special case $N = 2$, the inequality Eq. (III.21) becomes the necessary separability condition for arbitrary bipartite states from Eq. (III.11) with $\bar{a} = 1$. A violation of inequaltiy Eq. (III.21)

[4] A full classification of tripartite Gaussian states is given in Ref. [89] in analogy to that for qubits from Ref. [79]. In addition, sufficient and necessary three-party inseparability criteria for Gaussians are proposed in Ref. [89].

for arbitrary N is a sufficient criterion for some kind of inseparability of any continuous-variable N-party state (pure or mixed, Gaussian or non-Gaussian), but the state might still be partially separable. However, for a completely symmetric pure state (Gaussian or non-Gaussian), a violation of Eq. (III.21) would reveal genuine N-partite inseparability. This observation applies to the regularized version of the maximally entangled, but unphysical (unnormalizable) state $\int dx\, |x, x, \ldots, x\rangle$, which we will examine after the next section.

d Multipartite Werner-like states in infinite dimensions

In this section, we will gather more information about N-party quantum states defined in an infinite-dimensional Hilbert space. We will briefly discuss the inseparability of the generalized N-party qu*d*it Werner states in the infinite-dimensional limit.

Deuar *et al.* proved that $\hat{\rho}_{\mathrm{W}}^{(N,d)}$ from Eq. (II.24) is inseparable for $p > 1/(1 + d^{N-1})$ and gave an explicit decomposition into product states for qubits ($d = 2$) at the boundary $p = 1/(1 + 2^{N-1})$ [68]. However, the bound is not known to be strong for arbitrary dimension $d \neq 2$, so that $\hat{\rho}_{\mathrm{W}}^{(N,d)}$ might be inseparable even for $p \leq 1/(1 + d^{N-1})$. Nevertheless, the infinite-dimensional limit $d \to \infty$ again tells us that p can become arbitrarily small, and yet $\hat{\rho}_{\mathrm{W}}^{(N,\infty)}$ remains inseparable [5].

In their analysis, Deuar *et al.* do not explicitly examine whether the inseparability of $\hat{\rho}_{\mathrm{W}}^{(N,d)}$ is genuine or only partial. The state is obviously totally symmetric, but not pure. Thus, partial inseparability does not imply full inseparability. Of course, the special form of $\hat{\rho}_{\mathrm{W}}^{(N,d)}$ with the genuinely N-party entangled fraction $|\mathrm{GHZ}^{(N,d)}\rangle$ indicates full inseparability.

[5] Of course, the boundary above which entanglement is guaranteed also becomes arbitrarily small in the limit of an infinite number of parties $N \to \infty$. In fact, Deuar *et al.* found that "increasing the number of subsystems rather than increasing their Hilbert space dimension is a more effective way of increasing entanglement" [68].

2 QUANTUM CIRCUITS FOR GENERATING ENTANGLEMENT

How "expensive" is it to generate continuous-variable entanglement? In this section, we will see that the entanglement-creating quantum circuits consist only of squeezers and beam splitters. We will first derive circuits for two-party and then multi-party entanglement. Finally, we will discuss some properties of the multipartite entangled states.

a Generating bipartite entanglement

In chapter II, we have seen that a qubit based Bell state can be created in a quantum circuit that contains a Hadamard transformation acting on the first qubit in the state $|0\rangle$, and a C-NOT gate acting on the resulting qubit and the second qubit in the state $|0\rangle$. In order to construct an analogous curcuit for continuous variables, we may replace the Hadamard by a Fourier transformation and the C-NOT gate by a beam splitter operation [6]. The input states may be two zero-position eigenstates $|x = 0\rangle$. The 50:50 beam splitter is then effectively applied to a zero-momentum eigenstate (the Fourier-transformed zero-position eigenstate) $|p = 0\rangle \propto \int dx\, |x\rangle$ of mode 1 and a zero-position eigenstate $|x = 0\rangle$ of mode 2, which yields according to Eq. (I.176)

$$\hat{B}_{12}(\pi/4) \int dx\, |x, 0\rangle \propto \int dx\, |x, x\rangle \; . \tag{III.22}$$

We obtain a maximally entangled state, a two-mode momentum eigenstate with total momentum $p_1 + p_2 = 0$ and relative position $x_1 - x_2 = 0$. In order to describe the generation of a finitely correlated state, the beam splitter operation is applied to a momentum-squeezed and a position-squeezed vacuum mode. Using

[6] A possible continuous-variable generalization of the C-NOT gate is $|x_1, x_2\rangle \to |x_1, x_2 + x_1\rangle$, where the addition modulo two of the qubit C-NOT, $|y_1, y_2\rangle \to |y_1, y_2 \oplus y_1\rangle$ with $y_1, y_2 = 0, 1$, has been replaced by the normal addition. However, for the quantum circuit here, a 50:50 beam splitter acting as $|x_1, x_2\rangle \to |(x_1 + x_2)/\sqrt{2}, (x_1 - x_2)/\sqrt{2}\rangle$ is a suitable substitute for the generalized C-NOT gate.

Eq. (I.152) and Eq. (I.171), the Heisenberg operators of the outgoing modes become

$$\begin{aligned}
\hat{x}_1 &= (e^{+r_1}\hat{x}_1^{(0)} + e^{-r_2}\hat{x}_2^{(0)})/\sqrt{2}, \\
\hat{p}_1 &= (e^{-r_1}\hat{p}_1^{(0)} + e^{+r_2}\hat{p}_2^{(0)})/\sqrt{2}, \\
\hat{x}_2 &= (e^{+r_1}\hat{x}_1^{(0)} - e^{-r_2}\hat{x}_2^{(0)})/\sqrt{2}, \\
\hat{p}_2 &= (e^{-r_1}\hat{p}_1^{(0)} - e^{+r_2}\hat{p}_2^{(0)})/\sqrt{2}\,. \qquad \text{(III.23)}
\end{aligned}$$

Throughout, a superscript '(0)' denotes initial vacuum modes and r_1, r_2 are the squeezing parameters. We can easily check that the total variance of the operators defined in Eq. (III.12) (with $\bar{a} = 1$), $\langle(\Delta\hat{u})^2\rangle + \langle(\Delta\hat{v})^2\rangle = e^{-2r_1}/2 + e^{-2r_2}/2$, drops below the boundary of 1 for any squeezing $r > 0$ with equal initial squeezing $r = r_1 = r_2$, but also for any $r_1 > 0$ with $r_2 = 0$ or for any $r_2 > 0$ with $r_1 = 0$. This is an important observation. In order to produce entanglement between two modes, just *one* single-mode squeezed state split at a beam splitter suffices for any nonzero squeezing [7].

Under the assumption of equal initial squeezing $r = r_1 = r_2$, the above state in the Heisenberg picture exactly corresponds to the well-known two-mode squeezed state ("twin-beam state"). Using the unitary evolution involving a two-mode squeezing operator (see chapter I), this state can be written in the Schrödinger picture as

$$|\psi^{(2)}(\lambda)\rangle = e^{r(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1\hat{a}_2)}|00\rangle = \sqrt{1-\lambda}\sum_{n=0}^{\infty}\lambda^{n/2}|n\rangle|n\rangle\,, \qquad \text{(III.24)}$$

with $\lambda = \tanh^2 r$, now expanded in the discrete number basis with the squeezing parameter r corresponding to a scaled interaction time (see chapter I). The

[7] The result that a single squeezed state suffices to produce entanglement is not new. It was obtained in Refs. [2, 158] using different approaches. The new result will be later that a single squeezed state also suffices to generate multipartite entanglement between arbitrarily many parties.

state $|00\rangle$ is the two-mode vacuum. In this Schmidt form, we can quantify the entanglement of the twin-beam state via the partial von Neumann entropy $E_{\text{v.N.}} = -\text{Tr}\hat{\rho}_1 \log \hat{\rho}_1 = -\text{Tr}\hat{\rho}_2 \log \hat{\rho}_2$ with $\text{Tr}_2\hat{\rho}_{12} = \hat{\rho}_1$, $\text{Tr}_1\hat{\rho}_{12} = \hat{\rho}_2$, and $\hat{\rho}_{12} = |\psi^{(2)}(\lambda)\rangle\langle\psi^{(2)}(\lambda)|$:

$$\begin{aligned} E_{\text{v.N.}} &= -\log(1-\lambda) - \lambda \log \lambda/(1-\lambda) \\ &= \cosh^2 r \log(\cosh^2 r) - \sinh^2 r \log(\sinh^2 r) \, . \end{aligned} \tag{III.25}$$

The wave functions for the two-mode squeezed state are well-known [125],

$$\begin{aligned} \psi^{(\lambda)}(x_1, x_2) &= \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(x_1+x_2)^2/2 - e^{+2r}(x_1-x_2)^2/2] \\ &= \langle x_1, x_2|\psi^{(2)}(\lambda)\rangle \, , \end{aligned} \tag{III.26}$$

$$\begin{aligned} \bar{\psi}^{(\lambda)}(p_1, p_2) &= \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(p_1-p_2)^2/2 - e^{+2r}(p_1+p_2)^2/2] \\ &= \langle p_1, p_2|\psi^{(2)}(\lambda)\rangle \, , \end{aligned} \tag{III.27}$$

with the corresponding Wigner function [125, 10, 37]

$$\begin{aligned} W^{(\lambda)}(x_1, p_1, x_2, p_2) = \frac{4}{\pi^2} \exp\{&-e^{-2r}[(x_1+x_2)^2 + (p_1-p_2)^2] \\ &-e^{+2r}[(x_1-x_2)^2 + (p_1+p_2)^2]\} \, . \end{aligned} \tag{III.28}$$

From this Wigner function, the marginal distributions for the two positions or the two momenta according to Eqs. (III.26) and (III.27) may be obtained by integration over the two momenta or the two positions, respectively,

$$\begin{aligned} \int dp_1\, dp_2\, W^{(\lambda)}(x_1, p_1, x_2, p_2) &= |\psi^{(\lambda)}(x_1, x_2)|^2 \\ &= \frac{2}{\pi} \exp[-e^{-2r}(x_1+x_2)^2 - e^{+2r}(x_1-x_2)^2], \end{aligned} \tag{III.29}$$

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

Since the Wigner function in Eq. (III.28) is Gaussian, we can extract the corre-

lation matrix of the two-mode squeezed state:

$$V^{(2)} = \frac{1}{4} \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix} . \tag{III.30}$$

This matrix is already in Duan *et al.*'s standard form $V_{II}^{(2)}$. Hence one can easily verify that both Duan *et al.*'s and Simon's necessary and sufficient conditions for inseparability of Gaussian states are fulfilled for any $r > 0$. Tracing out either party of the Wigner function in Eq. (III.28) yields a thermal state,

$$\int dx_1\, dp_1\, W^{(\lambda)}(x_1, p_1, x_2, p_2) = \frac{2}{\pi(1+2\bar{n})} \exp\left[-\frac{2(x_2^2+p_2^2)}{1+2\bar{n}}\right] , \tag{III.31}$$

with mean excitation number $\bar{n} = \sinh^2 r$. In the limit of infinite squeezing $r \to \infty$, i.e., $\lambda \to 1$, we obtain the perfect correlations of the original Einstein, Podolsky, and Rosen (EPR) state [81],

$$\begin{aligned} W^{(\lambda)}(x_1, p_1, x_2, p_2) &\propto \delta(x_1 - x_2)\delta(p_1 + p_2), \\ \psi^{(\lambda)}(x_1, x_2) \propto \delta(x_1 - x_2), \quad \tilde{\psi}^{(\lambda)}(p_1, p_2) &\propto \delta(p_1 + p_2). \end{aligned} \tag{III.32}$$

In the following section, we will explicitly derive more general multipartite entangled states described by continuous variables, of which the two-mode squeezed state is the simplest special case.

b *Generating multipartite entanglement*

The circuit that produces the qubit GHZ state contains a Hadamard transformation of the first qubit followed by a sequence of C-NOT gates pairwise acting on the remaining qubits (see Fig. II.1), where all qubits are initially in the state $|0\rangle$. As in the two-party case, let us replace the Hadamard by a Fourier transformation and the C-NOT gates by appropriate beam splitter operations in order to construct an analogous circuit for continuous variables. In the ideal case, the input

states are again 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 [Eq. (I.176)]. Now we apply this sequence of beam splitters (making an "N-splitter"),

$$\hat{B}_{N-1\,N}(\pi/4)\hat{B}_{N-2\,N-1}\left(\sin^{-1}1/\sqrt{3}\right)\times\cdots\times\hat{B}_{12}\left(\sin^{-1}1/\sqrt{N}\right), \quad \text{(III.33)}$$

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 analogue to the qubit GHZ state with perfect correlations among the quadratures. However, it is an unphysical (unnormalizable) state. Instead of referring to a perfectly correlated multi-party state, again we proceed to a regularized, physical state with only finite correlations. In order to verify its inseparability, we may apply the previously derived variance inequality. Rather than sending (infinitely squeezed) position eigenstates through the entanglement-generating circuit, we will now use finitely squeezed states. The above N-splitter with $N = 3$ applied to a single momentum-squeezed vacuum mode and two position-squeezed vacuum modes yields the following output quadratures,

$$\begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \hat{x}_2 \\ \hat{p}_2 \\ \hat{x}_3 \\ \hat{p}_3 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} e^{+r_1}\hat{x}_1^{(0)} \\ e^{-r_1}\hat{p}_1^{(0)} \\ e^{-r_2}\hat{x}_2^{(0)} \\ e^{+r_2}\hat{p}_2^{(0)} \\ e^{-r_3}\hat{x}_3^{(0)} \\ e^{+r_3}\hat{p}_3^{(0)} \end{pmatrix}. \quad \text{(III.34)}$$

It is easily checked that the total variance of the operators defined in Eq. (III.16), $\mathcal{V}(3) = \langle(\Delta\hat{u})^2\rangle + \langle(\Delta\hat{v})^2\rangle + \langle(\Delta\hat{w})^2\rangle + \langle(\Delta\hat{t})^2\rangle = 3e^{-2r}$, drops below the boundary

of 3 for any $r > 0$ (with equal squeezing $r = r_1 = r_2 = r_3$). Moreover, just *one* single-mode squeezed state for any nonzero squeezing $r_1 > 0$ symmetrically split at two beam splitters (each with one vacuum input $r_2 = r_3 = 0$) is sufficient to violate the necessary separability condition Eq. (III.21) for $N = 3$.

The N-mode circuit now applied to N position-squeezed vacuum modes, i.e., the N-splitter applied to one momentum-squeezed and $N-1$ position-squeezed vacuum modes yields quadrature operators correlated as ($r = r_1 = r_2 = \cdots = r_N$)

$$\langle(\hat{x}_k - \hat{x}_l)^2\rangle = e^{-2r}/2\,, \quad \langle(\hat{p}_1 + \hat{p}_2 + \cdots + \hat{p}_N)^2\rangle = Ne^{-2r}/4\,, \tag{III.35}$$

where $k \neq l$. With only one momentum-squeezed ($r_1 > 0$) and $N-1$ vacuum modes ($r_2 = r_3 = \cdots = r_N = 0$) as the N-splitter input, the output modes obey

$$\langle(\hat{x}_k - \hat{x}_l)^2\rangle = 1/2\,, \quad \langle(\hat{p}_1 + \hat{p}_2 + \cdots + \hat{p}_N)^2\rangle = Ne^{-2r_1}/4\,. \tag{III.36}$$

Note that all modes involved have zero mean values, thus the variances and the second moments are identical. One can verify these results by means of the following matrix equation for our N-mode circuit,

$$\begin{aligned}
&(\hat{x}_1\ \hat{p}_1\ \hat{x}_2\ \hat{p}_2\ \hat{x}_3\ \hat{p}_3\ \cdots\ \hat{x}_N\ \hat{p}_N)^T \\
&= \begin{pmatrix}
\frac{1}{\sqrt{N}} & 0 & \sqrt{\frac{N-1}{N}} & 0 & 0 & 0 & \cdots \\
0 & \frac{1}{\sqrt{N}} & 0 & \sqrt{\frac{N-1}{N}} & 0 & 0 & \cdots \\
\frac{1}{\sqrt{N}} & 0 & \frac{-1}{\sqrt{N(N-1)}} & 0 & \sqrt{\frac{N-2}{N-1}} & 0 & \cdots \\
0 & \frac{1}{\sqrt{N}} & 0 & \frac{-1}{\sqrt{N(N-1)}} & 0 & \sqrt{\frac{N-2}{N-1}} & \cdots \\
\frac{1}{\sqrt{N}} & 0 & \frac{-1}{\sqrt{N(N-1)}} & 0 & \frac{-1}{\sqrt{(N-1)(N-2)}} & 0 & \cdots \\
0 & \frac{1}{\sqrt{N}} & 0 & \frac{-1}{\sqrt{N(N-1)}} & 0 & \frac{-1}{\sqrt{(N-1)(N-2)}} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{pmatrix} \\
&\times (e^{+r_1}\hat{x}_1^{(0)}\ e^{-r_1}\hat{p}_1^{(0)}\ e^{-r_2}\hat{x}_2^{(0)}\ e^{+r_2}\hat{p}_2^{(0)}\ e^{-r_3}\hat{x}_3^{(0)}\ e^{+r_3}\hat{p}_3^{(0)} \cdots\ e^{-r_N}\hat{x}_N^{(0)}\ e^{+r_N}\hat{p}_N^{(0)})^T.
\end{aligned} \tag{III.37}$$

For the N-mode output state with $r = r_1 = r_2 = \cdots = r_N$, inequality Eq. (III.21) is violated for any $r > 0$,

$$\mathcal{V}(N) = \binom{N}{2}\frac{e^{-2r}}{2} + (N-1)N\frac{e^{-2r}}{4} = \frac{N(N-1)}{2}e^{-2r}. \tag{III.38}$$

Furthermore, the N-mode output state with only one squeezed input ($r_1 > 0$) and $N-1$ vacuum inputs ($r_2 = r_3 = \cdots = r_N = 0$) turns out to be inseparable for any nonzero squeezing $r_1 > 0$,

$$\mathcal{V}(N) = \binom{N}{2}\frac{1}{2} + (N-1)N\frac{e^{-2r_1}}{4} = \frac{N(N-1)}{2}\left(\frac{1}{2} + \frac{e^{-2r_1}}{2}\right). \tag{III.39}$$

The states emerging from our circuit are therefore truly N-partite entangled for any $r > 0$ or $r_1 > 0$, taking into account their symmetry and purity. The symmetry of these *states* will become more transparent when we look at them in the Schrödinger and in the Wigner representation. For the remainder of this discussion, we will henceforth focus on those multipartite states with equal squeezing in the input modes ($r = r_1 = r_2 = \cdots = r_N$).

In chapter I, we have analyzed how arbitrary states are transformed by phase-free beam splitters in three different representations (Heisenberg, Schrödinger, Wigner). The Heisenberg operator equation Eq. (III.37) describes the output quadratures in terms of the input quadratures and has the structure $\boldsymbol{\xi}_{\text{out}}^T = \mathbf{A}\boldsymbol{\xi}_{\text{in}}^T$, where $\boldsymbol{\xi}_{\text{in}} = (x_1', p_1', x_2', p_2', ..., x_N', p_N')$ is the vector of the input quadratures and $\boldsymbol{\xi}_{\text{out}} = (x_1, p_1, x_2, p_2, ..., x_N, p_N)$ is the vector of the output quadratures. Recalling that at phase-free beam splitters the transformation properties of the Wigner function is

$$\begin{aligned} W_{\text{out}}(x_1, p_1, x_2, p_2, ..., x_N, p_N) = W_{\text{in}}[&x_1'(x_1, x_2, ..., x_N), p_1'(p_1, p_2, ..., p_N), \\ &x_2'(x_1, x_2, ..., x_N), p_2'(p_1, p_2, ..., p_N), ..., x_N'(x_1, x_2, ..., x_N), p_N'(p_1, p_2, ..., p_N)], \end{aligned} \tag{III.40}$$

and the wave function is

$$\psi_{\rm out}(x_1, x_2, ..., x_N) = \psi_{\rm in}[x_1'(x_1, x_2, ..., x_N), \quad x_2'(x_1, x_2, ..., x_N), ..., x_N'(x_1, x_2, ..., x_N)], \tag{III.41}$$

we see that in order to obtain the input quadratures in terms of the output quadratures, we must invert the $2N \times 2N$ matrix $\mathbf{A}$ in Eq. (III.37). With the help of this matrix inverse, where $\mathbf{A}^{-1} = \mathbf{A}^\dagger = \mathbf{A}^T$ due to the unitarity and reality of the N-splitter, and with the appropriate input Wigner function to the N-splitter (one momentum-squeezed mode and $N-1$ position-squeezed modes),

$$W_{\rm in}(\mathbf{x}', \mathbf{p}') = \left(\frac{2}{\pi}\right)^N \exp(-2e^{-2r}x_1'^2 - 2e^{+2r}p_1'^2) \exp(-2e^{+2r}x_2'^2 - 2e^{-2r}p_2'^2) \times \exp(-2e^{+2r}x_3'^2 - 2e^{-2r}p_3'^2) \times \cdots \times \exp(-2e^{+2r}x_N'^2 - 2e^{-2r}p_N'^2), \tag{III.42}$$

we can determine the output Wigner function to be

$$W_{\rm out}(\mathbf{x}, \mathbf{p}) = \left(\frac{2}{\pi}\right)^N \exp\left\{ - e^{-2r}\left[\frac{2}{N}\left(\sum_{i=1}^N x_i\right)^2 + \frac{1}{N}\sum_{i,j}^N (p_i - p_j)^2\right] - e^{+2r}\left[\frac{2}{N}\left(\sum_{i=1}^N p_i\right)^2 + \frac{1}{N}\sum_{i,j}^N (x_i - x_j)^2\right]\right\}. \tag{III.43}$$

Here we have used $\mathbf{x} = (x_1, x_2, ..., x_N)$, $\mathbf{p} = (p_1, p_2, ..., p_N)$, etc. The pure-state Wigner function $W_{\rm out}(\mathbf{x}, \mathbf{p})$ is always positive, *symmetric* among the N modes, and becomes peaked at $x_i - x_j = 0$ $(i, j = 1, 2, ..., N)$ and $p_1 + p_2 + \cdots + p_N = 0$ for large squeezing r. For $N = 2$, it exactly equals the two-mode squeezd state Wigner function from Eq. (III.28), which is proportional to $\delta(x_1 - x_2)\delta(p_1 + p_2)$ in the limit of infinite squeezing. The state $W_{\rm out}(\mathbf{x}, \mathbf{p})$ is genuinely N-partite entangled for any squeezing $r > 0$, taking into account its symmetry, its purity,

and its violation of the total variance inequality for fully separable states [8]. The quantum nature of the cross correlations $x_i x_j$ and $p_i p_j$ appearing in $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ for any $r > 0$ is also confirmed by the purity of this state, without reference to the total variance. This purity is guaranteed, since beam splitters turn pure states into pure states. In addition, we can verify the purity by means of the correlation matrix, which can be extracted from the Gaussian Wigner function $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (III.43) according to Eq. (I.125):

$$V^{(N)} = \frac{1}{4} \begin{pmatrix} a & 0 & c & 0 & c & 0 & \cdots \\ 0 & b & 0 & d & 0 & d & \cdots \\ c & 0 & a & 0 & c & 0 & \cdots \\ 0 & d & 0 & b & 0 & d & \cdots \\ c & 0 & c & 0 & a & 0 & \cdots \\ 0 & d & 0 & d & 0 & b & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} , \tag{III.44}$$

where

$$a = \frac{1}{N} e^{+2r} + \frac{N-1}{N} e^{-2r}, \quad b = \frac{1}{N} e^{-2r} + \frac{N-1}{N} e^{+2r}, \\ c = \frac{2}{N} \sinh 2r, \quad d = -c \, , \tag{III.45}$$

are the only coefficients needed. First, we can convince ourselves that for $N = 2$, the matrix $V^{(N)}$ reduces to that of the two-mode squeezed state in Eq. (III.30). Furthermore, one can now easily apply the purity check discussed in chapter I [see Eq. (I.139)].

The Schrödinger representation for the N-partite entangled output state of our circuit may be similarly derived giving

$$|\psi_{\text{out}}\rangle = \int dx_1 \, dx_2 \cdots dx_N \; \psi_{\text{out}}(\mathbf{x}) \; |x_1\rangle |x_2\rangle \cdots |x_N\rangle \equiv |\psi^{(N)}(\lambda)\rangle \, , \tag{III.46}$$

[8] Recently, this result was confirmed for three modes using criteria solely applicable to Gaussian states: the pure state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (III.43) with $N = 3$ belongs to the fully inseparable class of the five classes of (arbitrary pure or mixed) three-mode Gaussian states [89].

where the position wave function is

$$\psi_{\text{out}}(\mathbf{x}) = \left(\frac{2}{\pi}\right)^{N/4} \exp\left[-e^{-2r}\frac{1}{N}\left(\sum_{i=1}^{N} x_i\right)^2 - e^{+2r}\frac{1}{2N}\sum_{i,j}^{N}(x_i - x_j)^2\right] . \tag{III.47}$$

The two-mode squeezed state wave function of Eq. (III.26) is seen as the special case $N = 2$.

We will now discuss various properties of the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in comparison with its multipartite entangled qubit analogues. This will further illustrate the character of $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ as a nonmaximally entangled multi-party state.

c *Properties of the multipartite entangled states*

In chapter II, we discussed some properties of pure tripartite entangled states of three qubits. An important feature of these states is that a distinction can be made between two inequivalent classes: states from the first class can be converted into the state $|\text{GHZ}^{(3,2)}\rangle$ [Eq. (III.14)] via SLOCC, but not into the state $|\text{W}\rangle$ [Eq. (III.15)] (not even with arbitrarily small probability). For the second class, exactly the opposite holds. In several senses, the representative $|\text{GHZ}^{(3,2)}\rangle$ of the former class would be best described as a maximally entangled state, whereas the representative $|\text{W}\rangle$ of the latter class is nonmaximally entangled. A distinct feature of the maximum entanglement of $|\text{GHZ}^{(3,2)}\rangle$ is that after tracing out one qubit, the remaining qubit pair is in a separable mixed state [9]. Apparently, the entanglement of $|\text{GHZ}^{(3,2)}\rangle$ heavily relies on all three parties. By contrast, the entanglement of the state $|\text{W}\rangle$ is robust to some extent against disposal of one qubit. When tracing out one qubit of $|\text{W}\rangle$, the remaining pair shares a mixed entangled state. Mixed-state bipartite entanglement between any pair is "readily available" for the state $|\text{W}\rangle$, but not for $|\text{GHZ}^{(3,2)}\rangle$. In the continuous-variable

[9] However, remember that this is not the maximally mixed state for two qubits. Only when tracing out two parties, do we end up having the maximally mixed one-qubit state (chapter II).

context we can derive analogous results. By interpreting the state $\int dx\,|x,x,x\rangle$ as the analogue of $|\mathrm{GHZ}^{(3,2)}\rangle$, we see that

$$\mathrm{Tr}_1 \int dx\,dx'\,|x,x,x\rangle\langle x',x',x'| = \int dx\,|x\rangle_{2\,2}\langle x| \otimes |x\rangle_{3\,3}\langle x|\,, \tag{III.48}$$

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

$$\mathrm{Tr}_1 W_{\mathrm{out}}(\mathbf{x},\mathbf{p}) = \int dx_1\,dp_1\,W_{\mathrm{out}}(\mathbf{x},\mathbf{p}) \tag{III.49}$$

$$\propto \exp\Bigg[-2e^{+2r}\frac{e^{+2r}+2e^{-2r}}{e^{-2r}+2e^{+2r}}\left(x_2^2+x_3^2\right) - 2e^{-2r}\frac{e^{-2r}+2e^{+2r}}{e^{+2r}+2e^{-2r}}\left(p_2^2+p_3^2\right) + 4e^{+2r}\frac{e^{+2r}-e^{-2r}}{e^{-2r}+2e^{+2r}}x_2x_3 + 4e^{-2r}\frac{e^{-2r}-e^{+2r}}{e^{+2r}+2e^{-2r}}p_2p_3\Bigg]\,.$$

From the resulting Gaussian two-mode Wigner function, we first extract the inverse correlation matrix, and then calculate the bipartite correlation matrix

$$V^{(2)} = \frac{1}{12}\begin{pmatrix} e^{+2r}+2e^{-2r} & 0 & 2\sinh 2r & 0 \\ 0 & e^{-2r}+2e^{+2r} & 0 & -2\sinh 2r \\ 2\sinh 2r & 0 & e^{+2r}+2e^{-2r} & 0 \\ 0 & -2\sinh 2r & 0 & e^{-2r}+2e^{+2r} \end{pmatrix}. \tag{III.50}$$

We could have also obtained this correlation matrix by taking the N-mode correlation matrix $V^{(N)}$ from Eq. (III.44) with $N=3$ and ignoring all entries involving mode 1 [or equivalently by explicitly calculating the correlations between modes 2 and 3 with the Heisenberg operators in Eq. (III.34) for $r = r_1 = r_2 = r_3$].

There are now two important observations about the *Gaussian* state described by $V^{(2)}$ in Eq. (III.50): it does not always violate the necessary separability condition Eq. (III.11) (with $\bar{a}=1$), and yet it is a (mixed) inseparable state

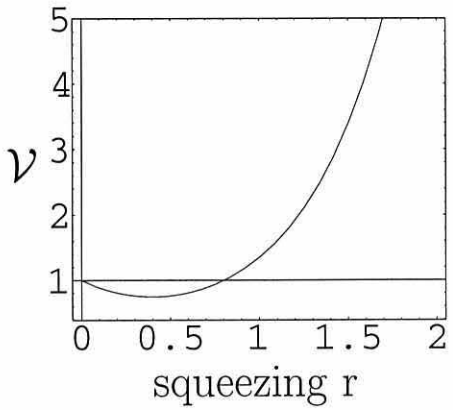

Figure III.1: The total variance $\mathcal{V}(2)$ of the bipartite state after tracing out one mode of the tripartite state $W_{\rm out}(\mathbf{x},\mathbf{p})$ as a function of the dimensionless squeezing parameter r. Only for sufficiently small nonzero squeezing, the necessary separability condition is violated ($\mathcal{V}<1$).

for any nonzero squeezing $r>0$ (see below). The total variance in Eq. (III.11) becomes for this state $\mathcal{V}(2)=\langle(\Delta\hat{u})^2\rangle+\langle(\Delta\hat{v})^2\rangle=(5e^{-2r}+e^{+2r})/6$, which drops below the boundary of 1 only for sufficiently small nonzero squeezing, but approaches infinity as the squeezing increases (see Fig. III.1).

We can easily verify the state's inseparability for any $r>0$ by looking at the necessary separability condition in product form in Eq. (III.13). We find $\langle(\Delta\hat{u})^2\rangle\langle(\Delta\hat{v})^2\rangle=(2e^{-4r}+1)/12$, which drops below the boundary of $1/4$ for any $r>0$. As for the necessary and sufficient inseparabiliy criteria for Gaussian states, we see from Eq. (III.50) that $V^{(2)}$ is not in standard form $V_{II}^{(2)}$ of Eq. (III.5). Let us therefore directly apply Simon's condition for a general bipartite correlation matrix as in Eq. (III.1). After some algebra, the separability condition of Eq. (III.2) with $V^{(2)}$ from Eq. (III.50) can be turned into $\sinh^2 2r\leq 0$, which is violated for any $r>0$. Let us emphasize again that even as $r\rightarrow\infty$, yielding $\mathcal{V}(2)\rightarrow\infty$, the state remains inseparable according to the product criterion $\langle(\Delta\hat{u})^2\rangle\langle(\Delta\hat{v})^2\rangle<1/4$ and also according to Simon's condition. Recall that by first taking the infinite-squeezing limit and then tracing out one mode, we had

obtained a separable state [Eq. (III.48)]. That was what we expected according to the result for the maximally entangled qubit state $|\mathrm{GHZ}^{(3,2)}\rangle$. Apparently, it makes a difference, whether we first trace out one mode and then take the limit or vice versa. One could say that these two operations "do not commute" [189].

These results tell us that, though the tripartite state $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ may be the analogue of the qubit state $|\mathrm{GHZ}^{(3,2)}\rangle$ in the limit of infinite squeezing, when tracing out one party, $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ behaves more like $|\mathrm{W}\rangle$ than like $|\mathrm{GHZ}^{(3,2)}\rangle$. The remaining two-mode state is inseparable and mixed. Its mixedness can be verified by rearranging the correlation matrix $V^{(2)}$ from Eq. (III.50) into the form $\tilde{V}^{(2)}$ in Eq. (I.137) and applying the purity test presented in chapter I: the purity conditions are not fulfilled. So after all, we confirm what we had intuitively expected: the tripartite state $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ *for finite squeezing* is a nonmaximally entangled state like the qubit state $|\mathrm{W}\rangle$. Only for infinite squeezing does it approach the maximally entangled state $\int dx\,|x,x,x\rangle$, the analogue of $|\mathrm{GHZ}^{(3,2)}\rangle$. This result reflects what is known for two parties. The two-mode squeezed state $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ with $N=2$ becomes a maximally entangled state $\int dx\,|x,x\rangle$, such as the Bell state $(|00\rangle+|11\rangle)/\sqrt{2}$, only for infinite squeezing. For finite squeezing, it is known to be nonmaximally entangled [see its Schmidt decomposition in Eq. (III.24)].

In the current section, we have examined the bipartite state of any pair of modes of the tripartite state $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ when no information at all is obtainable about the third mode. What about the situation when information is indeed gained about one mode by measuring it? What kind of state shares the remaining pair of modes in this case? We will turn to this question in chapter IV where this scenario will be part of a quantum communication protocol within a network of more than two participants.

3 A UNIVERSAL MULTI-PARTY INSEPARABILITY CRITERION

In section 2, continuous-variable N-mode quantum states were shown to be fully inseparable: first, we proved that these states are at least partially inseparable, and then we referred to their purity and symmetry. We will formulate and prove this argument now in a universal fashion for quantum states defined in an arbitrary Hilbert space.

a The theorem

Theorem: Any pure entangled multi-party state which is symmetric under interchange of parties is genuinely inseparable.

Proof: Let us write the N-partite quantum state as

$$|\psi\rangle_{1\ldots j} \otimes |\phi\rangle_{j+1\ldots N} \,. \tag{III.51}$$

Parties 1 through j ($j = 2\ldots N-1$) shall be entangled with each other in the state $|\psi\rangle_{1\ldots j}$. The remaining parties are in an arbitrary state $|\phi\rangle_{j+1\ldots N}$. Tracing out parties 1 through j now yields a pure state. Due to symmetry, swapping party j from $|\psi\rangle_{1\ldots j}$ for party $j+1$ from $|\phi\rangle_{j+1\ldots N}$ should leave the state unchanged. However, tracing out parties 1 through j after that swapping yields a mixed state due to the entanglement of the parties 1 through $j-1$ with $j+1$. The N-party state therefore cannot be only partially inseparable, it must be fully inseparable. Such a conclusion is not possible for mixed states. For example, the symmetric three-qubit state

$$\hat{\rho} = \frac{1}{3}\hat{\rho}^{-}_{12} \otimes |0\rangle_{3\,3}\langle 0| + \frac{1}{3}\hat{\rho}^{-}_{13} \otimes |0\rangle_{2\,2}\langle 0| + \frac{1}{3}\hat{\rho}^{-}_{23} \otimes |0\rangle_{1\,1}\langle 0| \,, \tag{III.52}$$

with the singlet state $\hat{\rho}^{-} = |\Psi^{-}\rangle\langle\Psi^{-}|$ [Eq. (II.11)], is neither fully inseparable nor fully separable. It is generated by randomly distributing the two halves of the singlet and the eigenstate $|0\rangle$ among three parties.

At first sight, the above theorem does not appear to be of great importance, in particular, because it is only applicable to pure states. However, especially for

large numbers of parties, it may prove a useful tool to find out whether multi-party quantum states of arbitrary dimension are fully inseparable or not. For example, as yet pure multi-qubit states have been classified only for the simplest tripartite case, as discussed in chapter II.

*b The **N**-mode continuous-variable states*

In the case of the continuous-variable states, the theorem has proven its usefulness already in section 2. There, we applied it to the pure symmetric N-mode states built from one squeezed state and those built from N equally squeezed states with the quadrature correlations in Eq. (III.36) and Eq. (III.35), respectively. These two classes of states represent only the extreme cases of a larger family of pure symmetric N-mode states generated with squeezers and beam splitters. This family consists of all states that emerge from the N-splitter when the first vacuum input mode is momentum-squeezed with r_1 and the remaining $N-1$ vacuum input modes are all equally position-squeezed with $r_2 = r_3 = \cdots = r_N$. The quadrature correlations are then for any N given by

$$\langle(\hat{x}_k - \hat{x}_l)^2\rangle = e^{-2r_2}/2\,, \quad \langle(\hat{p}_1 + \hat{p}_2 + \cdots + \hat{p}_N)^2\rangle = Ne^{-2r_1}/4\,. \qquad \text{(III.53)}$$

The two extreme cases we had considered correspond to $r_2 = 0$ and $r = r_1 = r_2$. Now in general, for any $r_1 > 0$ *or* $r_2 > 0$, the total variance inequality Eq. (III.21) is violated. Applying the theorem, we see that the family of pure symmetric states with the correlations in Eq. (III.53) are genuinely inseparable for any $r_1 > 0$ *or* $r_2 > 0$. Note that violations of the total variance inequality also occur with input states to the N-splitter for example squeezed as $r_1 = 0$, $r_2 > 0$, and $r_3 = r_4 = \cdots = r_N = 0$. However, the N-mode output states are not completely symmetric in this case. Full symmetry requires $r_2 = r_3 = \cdots = r_N$. Independent of the total variance inequality Eq. (III.21), using the theorem there are also other ways to prove the continuous-variable states' genuine inseparability. One simply has to find some form of entanglement in these states. For example, just look at

mode 1 in Eq. (III.37). For any N, its correlation matrix satisfies $\det V^{(1)} > 1/16$ if $r_1 > 0$ *or* $r_2 > 0$. As discussed in chapter I, this shows that mode 1 alone (which is equivalent to tracing out modes 2 through N) is in a mixed state. Thus, the pure N-mode state is entangled and hence fully inseparable due to the theorem.

From a conceptual point of view, it is very illuminating to analyze which states of the above family of N-mode states can be transformed into each other via local squeezing operations. This was done recently by Bowen *et al.* [25]. Let us briefly recast their analysis using our formalism and giving our own interpretation.

By applying local squeezers with squeezing s_1 and s_2 to the two modes of the bipartite state generated with only one squeezer [Eq. (III.23) with $r_2 = 0$], we obtain

$$\begin{aligned}
\hat{x}_1' &= e^{-s_1}\hat{x}_1 = (e^{+r_1-s_1}\hat{x}_1^{(0)} + e^{-s_1}\hat{x}_2^{(0)})/\sqrt{2}, \\
\hat{p}_1' &= e^{+s_1}\hat{p}_1 = (e^{+s_1-r_1}\hat{p}_1^{(0)} + e^{+s_1}\hat{p}_2^{(0)})/\sqrt{2}, \\
\hat{x}_2' &= e^{-s_2}\hat{x}_2 = (e^{+r_1-s_2}\hat{x}_1^{(0)} - e^{-s_2}\hat{x}_2^{(0)})/\sqrt{2}, \\
\hat{p}_2' &= e^{+s_2}\hat{p}_2 = (e^{+s_2-r_1}\hat{p}_1^{(0)} - e^{+s_2}\hat{p}_2^{(0)})/\sqrt{2}\,. \qquad \text{(III.54)}
\end{aligned}$$

With the choice of $s_1 = s_2 = r_1/2 \equiv r$, the state in Eq. (III.54) is identical to a two-mode squeezed state built from two equally squeezed states [Eq. (III.23) with $r_1 \equiv r$, $r_2 \equiv r$]. The latter and the state of Eq. (III.23) with $r_1 = 2r$ and $r_2 = 0$ are equivalent under local squeezing operations. This means that Alice and Bob sharing the state of Eq. (III.23) with $r_2 = 0$ have access to the same amount of entanglement as in the "canonical" two-mode squeezed state with squeezing $r = r_1/2$, $E_{\text{v.N.}} = [\cosh(r_1/2)]^2 \log[\cosh(r_1/2)]^2 - [\sinh(r_1/2)]^2 \log[\sinh(r_1/2)]^2$ [see Eq. (III.25)]. For a given amount of entanglement, however, the canonical two-mode squeezed state has the least mean photon number [10]. Conversely, for a given mean energy, the canonical two-mode squeezed state contains the maximum

[10] Bowen *et al.* interpret the *deterministic* transformation described by Eq. (III.54) as an "entanglement concentration" scheme in the sense that the amount of entanglement per photon increases. This interpretation differs from the common use of the term "entanglement concen-

amount of entanglement possible.

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

$$e^{\pm 2r_1} = (N-1)\sinh 2r_2 \left[\sqrt{1+\frac{1}{(N-1)^2\sinh^2 2r_2}} \pm 1\right] . \qquad \text{(III.55)}$$

This relation is obtained by requiring each mode of the N-mode states to be symmetric or "unbiased" in the x and p variances [25]. Only for $N = 2$, we obtain $r_1 = r_2$. Otherwise, the first squeezer with r_1 and the $N-1$ remaining squeezers with r_2 have different squeezing. In the limit of large squeezing, we may use $\sinh 2r_2 \approx e^{+2r_2}/2$ and approximate e^{+2r_1} of Eq. (III.55) by

$$e^{+2r_1} \approx (N-1)e^{+2r_2} . \qquad \text{(III.56)}$$

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

In the next section, where we deal with the nonlocality of the continuous-variable multipartite entangled states, we will focus on the N-mode states generated with N equally squeezed states.

---

tration" in quantum information theory. In chapter IV, we will study the *probabilistic* effect of entanglement concentration via entanglement swapping.

4 Revealing nonlocality of continuous-variable entangled states

We will now uncover another important property of the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (III.43). Despite having an always positive Wigner function, for any squeezing $r > 0$, it violates N-party Bell-type [10] (or Mermin-type [143]) inequalities imposed by local realism [133]. We will find that, just as for the qubit states $|\text{GHZ}^{(N,2)}\rangle$ of Eq.(II.17) [143], the violations increase as the number of parties N grows. However, this increase becomes steadily smaller for larger N, as opposed to the exponential increase for $|\text{GHZ}^{(N,2)}\rangle$ [143]. This discrepancy may be explained by the fact that the violations are exposed only for finite squeezing where the state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ is a *nonmaximally* entangled multi-party state.

There are 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. We will use the term nonlocality here in just this way.

It was John Bell who showed that nonlocality can be revealed via the constraints that local realism imposes on the statistics of two physically separated systems [10]. These constraints, expressed in terms of the Bell inequalities, can be violated by quantum mechanics. Entanglement does not automatically imply nonlocality. The qubit Werner states are mixed states which can be inseparable (see chapter II) without violating any (non-collective) Bell inequality [202]. Also pure entangled states, if associated with a positive Wigner function, can directly reveal a local hidden-variable description in terms of their continuous variables [10]. Thus, for the two-mode squeezed state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ with $N = 2$, attempts to derive violations of Bell inequalities based on homodyne measurements of the quadratures failed [156]. However, whether nonlocality is uncovered depends on the observables and the measurements considered in a specific Bell inequality and

not only on the quantum state itself. For example, it was shown by Banaszek and Wodkiewicz [7] how to demonstrate the nonlocality of the two-mode squeezed vacuum state: it violates a Clauser-Horne-Shimony-Holt (CHSH) inequality [61] when measurements of photon number parity are considered.

The nonlocality of the multipartite entangled qubit states $|\mathrm{GHZ}^{(N,2)}\rangle$ can *in principle* be manifest in a single measurement (corresponding to an impossibly ideal scenario) and need not be statistical [101] as is a violation of a Bell inequality that relies on expectation values. Despite this, however, Mermin and others [143, 117] have derived Bell-CHSH inequalities for such N-particle systems. We will now apply these N-party inequalities to the continuous-variable states $W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$ and thereby prove their nonlocality. Since these states have a positive Wigner function for any N, we shall follow the strategy of Banaszek and Wodkiewicz [7] who exploited the fact that the Wigner function is connected to the expectation value of the photon number parity operator. Relying on this connection, we will demonstrate N-party nonlocality using mean-value inequalities [117], and thus we do not follow the original GHZ program based on a contradiction to local realism in a single measurement.

In order to prove the nonlocality exhibited by the state $W(\mathbf{x},\mathbf{p}) \equiv W_{\mathrm{out}}(\mathbf{x},\mathbf{p})$, let us now use the fact that the Wigner function is proportional to the quantum expectation value of a displaced parity operator [175, 7]:

$$W(\boldsymbol{\alpha}) = \left(\frac{2}{\pi}\right)^N \left\langle \hat{\Pi}(\boldsymbol{\alpha}) \right\rangle = \left(\frac{2}{\pi}\right)^N \Pi(\boldsymbol{\alpha}) \,, \tag{III.57}$$

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

$$\hat{\Pi}(\boldsymbol{\alpha}) = \bigotimes_{i=1}^{N} \hat{\Pi}_i(\alpha_i) = \bigotimes_{i=1}^{N} \hat{D}_i(\alpha_i)(-1)^{\hat{n}_i}\hat{D}_i^{\dagger}(\alpha_i) \,. \tag{III.58}$$

The operators $\hat{D}_i(\alpha_i)$ are the displacement operators acting on mode i [Eq. (I.80)]. Thus, $\hat{\Pi}(\boldsymbol{\alpha})$ is a product of displaced parity operators given by

$$\hat{\Pi}_i(\alpha_i) = \hat{\Pi}_i^{(+)}(\alpha_i) - \hat{\Pi}_i^{(-)}(\alpha_i) \,, \tag{III.59}$$

with the projection operators

$$\hat{\Pi}_i^{(+)}(\alpha_i) = \hat{D}_i(\alpha_i) \sum_{k=0}^{\infty} |2k\rangle\langle 2k| \hat{D}_i^{\dagger}(\alpha_i), \tag{III.60}$$

$$\hat{\Pi}_i^{(-)}(\alpha_i) = \hat{D}_i(\alpha_i) \sum_{k=0}^{\infty} |2k+1\rangle\langle 2k+1| \hat{D}_i^{\dagger}(\alpha_i) \, , \tag{III.61}$$

corresponding to the measurement of an even (parity $+1$) or an odd (parity -1) number of photons in mode i. This means that each mode is now characterized by a dichotomic variable similar to the spin of a spin-1/2 particle or the single-photon polarization. Different spin or polarizer orientations from the original qubit based Bell inequality are replaced by different displacements in phase space. This set of two-valued measurements for each setting is just what we need for the nonlocality test.

In the case of N-particle systems, such a nonlocality test is possible using the N-particle generalization of the two-particle Bell-CHSH inequality [117]. This inequality is based on the following recursively defined linear combination of joint measurement results (in this section, the symbol B does not refer to a beam splitter operation)

$$\begin{aligned} B_N &\equiv \frac{1}{2}[\sigma(a_N) + \sigma(a'_N)]B_{N-1} \\ &+ \frac{1}{2}[\sigma(a_N) - \sigma(a'_N)]B'_{N-1} = \pm 2 \, , \end{aligned} \tag{III.62}$$

where $\sigma(a_N) = \pm 1$ and $\sigma(a'_N) = \pm 1$ describe two possible outcomes for two possible measurement settings (denoted by a_N and a'_N) of measurements on the Nth particle. Note, the expressions B'_N are equivalent to B_N but with all the a_i and a'_i swapped. Provided that $B_{N-1} = \pm 2$ and $B'_{N-1} = \pm 2$, Equation (III.62) is trivially true for a single run of measurements where $\sigma(a_N)$ is either $+1$ or -1 and similarly for $\sigma(a'_N)$. Induction proves Eq. (III.62) for any N when we take

$$\begin{aligned} B_2 &\equiv [\sigma(a_1) + \sigma(a'_1)]\sigma(a_2) \\ &+ [\sigma(a_1) - \sigma(a'_1)]\sigma(a'_2) = \pm 2 \, . \end{aligned} \tag{III.63}$$

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

$$\left| \int d\lambda_1 d\lambda_2 ... d\lambda_N P(\boldsymbol{\lambda}) B_N(\boldsymbol{\lambda}) \right| \leq 2 \, . \tag{III.64}$$

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

$$|C(a_1, a_2) + C(a_1, a_2') + C(a_1', a_2) - C(a_1', a_2')| \leq 2, \tag{III.65}$$

with the correlation functions

$$C(a_1, a_2) = \int d\lambda_1 d\lambda_2 P(\lambda_1, \lambda_2) \sigma(a_1, \lambda_1) \sigma(a_2, \lambda_2) \, . \tag{III.66}$$

Following Bell [10], an always positive Wigner function can serve as the hidden-variable probability distribution with respect to measurements corresponding to any linear combination of $\hat{x}$ and $\hat{p}$. In this sense, the finitely squeezed EPR-state Wigner function could prevent the CHSH inequality from being violated when restricted to such measurements: $W(x_1, p_1, x_2, p_2) \equiv P(\lambda_1, \lambda_2)$. The same applies to the Wigner function in Eq. (III.43): $W(\mathbf{x}, \mathbf{p}) \equiv P(\boldsymbol{\lambda})$ could be used to construct correlation functions

$$\begin{aligned} C(\mathbf{a}) \; &= \; \int d\lambda_1 d\lambda_2 ... d\lambda_N P(\boldsymbol{\lambda}) \\ &\quad \times \sigma(a_1, \lambda_1) \sigma(a_2, \lambda_2) \cdots \sigma(a_N, \lambda_N), \end{aligned} \tag{III.67}$$

where $\mathbf{a} = (a_1, a_2, ..., a_N)$. However, for parity measurements on each mode with possible results ± 1 for each differing displacement, this would require unbounded δ-functions for the local objective quantities $\sigma(a_i, \lambda_i)$ [7], as in this case we have

$$C(\mathbf{a}) \equiv \Pi(\boldsymbol{\alpha}) = (\pi/2)^N W(\boldsymbol{\alpha}) \, . \tag{III.68}$$

This relation directly relates the correlation function to the Wigner function and is indeed crucial for the nonlocality proof of the continuous-variable states in Eq. (III.43).

a Nonlocal correlations between two parties

Let us begin by analyzing the nonlocal correlations exhibited by the entangled two-party state. For this state, the finitely squeezed EPR state $W_{\rm out}(\mathbf{x},\mathbf{p})$ with $N=2$, we may investigate the combination [7]

$$\mathcal{B}_2 = \Pi(0,0) + \Pi(0,\beta) + \Pi(\alpha,0) - \Pi(\alpha,\beta)\ , \tag{III.69}$$

which according to Eq. (III.65) satisfies $|\mathcal{B}_2| \leq 2$ for local realistic theories. Here, we have chosen the displacement settings $\alpha_1 = \alpha_2 = 0$ and $\alpha_1' = \alpha$, $\alpha_2' = \beta$.

Writing the states in Eq. (III.43) as

$$\begin{aligned}\Pi(\boldsymbol{\alpha}) \;=\; \exp\Bigg\{ &-2\cosh 2r \sum_{i=1}^{N} |\alpha_i|^2 \\ &+\sinh 2r \left[\frac{2}{N}\sum_{i,j}^{N}(\alpha_i\alpha_j + \alpha_i^*\alpha_j^*) - \sum_{i=1}^{N}(\alpha_i^2 + \alpha_i^{*2})\right]\Bigg\}\ ,\end{aligned} \tag{III.70}$$

for $N=2$ and $\alpha = \beta = i\sqrt{\mathcal{J}}$ with the real displacement parameter $\mathcal{J} \geq 0$ [11], we obtain $\mathcal{B}_2 = 1 + 2\exp(-2\mathcal{J}\cosh 2r) - \exp(-4\mathcal{J}e^{+2r})$. In the limit of large r (so $\cosh 2r \approx e^{+2r}/2$) and small $\mathcal{J}$, $\mathcal{B}_2$ is maximized for $\mathcal{J}e^{+2r} = (\ln 2)/3$, yielding $\mathcal{B}_2^{\max} \approx 2.19$ [7], which is a clear violation of the inequality $|\mathcal{B}_2| \leq 2$. Smaller violations also occur for smaller squeezing and larger $\mathcal{J}$. Indeed, for any nonzero squeezing, some violation takes place (see Fig. III.2).

b Nonlocal correlations between many parties

We will now consider more than two parties. Let us first examine the three-mode state by setting $N=3$ in Eq. (III.43). According to the inequality of the correlation functions derived from Eq. (III.62)-(III.64), we have

$$\begin{aligned}&|C(a_1,a_2,a_3') + C(a_1,a_2',a_3) \\ &\quad + C(a_1',a_2,a_3) - C(a_1',a_2',a_3')| \leq 2\ .\end{aligned} \tag{III.71}$$

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

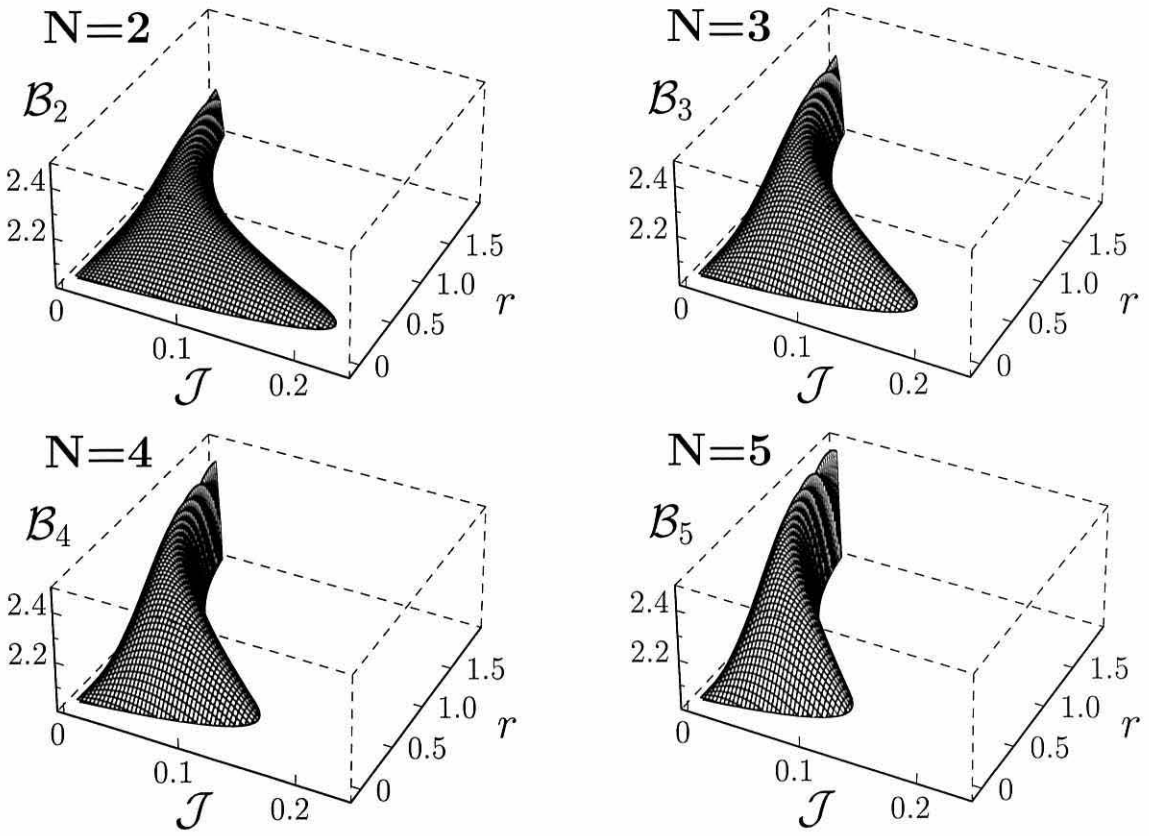

Figure III.2: Violations of the inequality $|\mathcal{B}_N| \leq 2$ imposed by local realistic theories with the entangled two-mode ($N = 2$, as in Ref. [7]), three-mode ($N = 3$), four-mode ($N = 4$), and five-mode ($N = 5$) states.

Thus, for the combination

$$\mathcal{B}_3 = \Pi(0,0,\gamma) + \Pi(0,\beta,0) + \Pi(\alpha,0,0) - \Pi(\alpha,\beta,\gamma), \tag{III.72}$$

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

$$\begin{aligned}\mathcal{B}_3 &= \sum_{i=1}^{3} \exp(-2\mathcal{J}\cosh 2r - \frac{2}{3}\mathcal{J}\sinh 2r\cos 2\phi_i) \\ &- \exp\left\{-6\mathcal{J}\cosh 2r - \frac{1}{3}\mathcal{J}\sinh 2r \sum_{i\neq j}^{3}[\cos 2\phi_i - 4\cos(\phi_i+\phi_j)]\right\}.\end{aligned} \tag{III.73}$$

Apparently, because of the symmetry of the entangled three-mode state, equal phases ϕ_i should also be chosen in order to maximize $\mathcal{B}_3$. The best choice is $\phi_1 = \phi_2 = \phi_3 = \pi/2$, which ensures that the positive terms in Eq. (III.73) become maximal and the contribution of the negative term minimal. Therefore, we again use equal settings $\alpha = \beta = \gamma = i\sqrt{\mathcal{J}}$ and obtain

$$\mathcal{B}_3 = 3\exp(-2\mathcal{J}\cosh 2r + 2\mathcal{J}\sinh 2r/3) - \exp(-6\mathcal{J}e^{+2r})\ . \tag{III.74}$$

The violations of $|\mathcal{B}_3| \leq 2$ that occur with this result are similar to the violations of $|\mathcal{B}_2| \leq 2$ obtained for the EPR state, but the $N = 3$ violations are even more significant than the $N = 2$ violations (see Fig. III.2). In the limit of large r (and small $\mathcal{J}$), we may use $\cosh 2r \approx \sinh 2r \approx e^{+2r}/2$ in Eq. (III.74). Then $\mathcal{B}_3$ is maximized for $\mathcal{J}e^{+2r} = 3(\ln 3)/16$: $\mathcal{B}_3^{\max} \approx 2.32$. This optimal choice requires smaller displacements $\mathcal{J}$ than those of the $N = 2$ case for the same squeezing.

Let us now investigate the cases $N = 4$ and $N = 5$. From Eq. (III.62)-(III.64)

with $N = 4$, the following inequality for the correlation functions can be derived:

$$\begin{aligned}\frac{1}{2}|&C(a_1,a_2,a_3,a_4')+C(a_1,a_2,a_3',a_4)+C(a_1,a_2',a_3,a_4)\\&+C(a_1',a_2,a_3,a_4)+C(a_1,a_2,a_3',a_4')+C(a_1,a_2',a_3,a_4')\\&+C(a_1',a_2,a_3,a_4')+C(a_1,a_2',a_3',a_4)+C(a_1',a_2,a_3',a_4)\\&+C(a_1',a_2',a_3,a_4)-C(a_1',a_2',a_3',a_4)-C(a_1',a_2',a_3,a_4')\\&-C(a_1',a_2,a_3',a_4')-C(a_1,a_2',a_3',a_4')-C(a_1,a_2,a_3,a_4)\\&-C(a_1',a_2',a_3',a_4')|\leq 2\,. \end{aligned}\tag{III.75}$$

It is symmetric among all four parties as any inequality derived from Eq. (III.62)-(III.64) is symmetric among all parties. For the settings $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$ and $\alpha_1' = \alpha$, $\alpha_2' = \beta$, $\alpha_3' = \gamma$, $\alpha_4' = \delta$, complying with local realism implies $|\mathcal{B}_4| \leq 2$ where

$$\begin{aligned}\mathcal{B}_4 \;=\; \frac{1}{2}[&\Pi(0,0,0,\delta)+\Pi(0,0,\gamma,0)+\Pi(0,\beta,0,0)\\&+\Pi(\alpha,0,0,0)+\Pi(0,0,\gamma,\delta)+\Pi(0,\beta,0,\delta)\\&+\Pi(\alpha,0,0,\delta)+\Pi(0,\beta,\gamma,0)+\Pi(\alpha,0,\gamma,0)\\&+\Pi(\alpha,\beta,0,0)-\Pi(\alpha,\beta,\gamma,0)-\Pi(\alpha,\beta,0,\delta)\\&-\Pi(\alpha,0,\gamma,\delta)-\Pi(0,\beta,\gamma,\delta)-\Pi(0,0,0,0)\\&-\Pi(\alpha,\beta,\gamma,\delta)]\,. \end{aligned}\tag{III.76}$$

Similarly, for $N = 5$ one finds

$$\begin{aligned}\mathcal{B}_5 \;=\; \frac{1}{2}[&\Pi(0,0,0,\delta,\epsilon)+\Pi(0,0,\gamma,0,\epsilon)+\Pi(0,\beta,0,0,\epsilon)\\&+\Pi(\alpha,0,0,0,\epsilon)+\Pi(0,0,\gamma,\delta,0)+\Pi(0,\beta,0,\delta,0)\\&+\Pi(\alpha,0,0,\delta,0)+\Pi(0,\beta,\gamma,0,0)+\Pi(\alpha,0,\gamma,0,0)\\&+\Pi(\alpha,\beta,0,0,0)-\Pi(\alpha,\beta,\gamma,\delta,0)-\Pi(\alpha,\beta,\gamma,0,\epsilon)\\&-\Pi(\alpha,\beta,0,\delta,\epsilon)-\Pi(\alpha,0,\gamma,\delta,\epsilon)-\Pi(0,\beta,\gamma,\delta,\epsilon)\\&-\Pi(0,0,0,0,0)]\,, \end{aligned}\tag{III.77}$$

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

We can now use the entangled states of Eq. (III.70) with $N = 4$ and $N = 5$ and apply these inequalities to them. For the same reason as for $N = 3$ (symmetry among all modes in the states and in the inequalities), the choice $\alpha = \beta = \gamma = \delta = \epsilon = i\sqrt{\mathcal{J}}$ appears to be optimal (maximizes positive terms and minimizes negative contributions).

With this choice, we obtain

$$\begin{aligned}
\mathcal{B}_4 &= 2\exp(-2\mathcal{J}\cosh 2r + \mathcal{J}\sinh 2r) \\
&\quad -2\exp(-6\mathcal{J}\cosh 2r - 3\mathcal{J}\sinh 2r) \\
&\quad +3\exp(-4\mathcal{J}\cosh 2r) - \frac{1}{2}\exp(-8\mathcal{J}e^{+2r}) - \frac{1}{2}\,, \\
\mathcal{B}_5 &= 5\exp(-4\mathcal{J}\cosh 2r + 4\mathcal{J}\sinh 2r/5) \\
&\quad -\frac{5}{2}\exp(-8\mathcal{J}\cosh 2r - 24\mathcal{J}\sinh 2r/5) - \frac{1}{2}\,. \qquad \text{(III.78)}
\end{aligned}$$

As shown in Fig. III.2, the maximum violation of $|\mathcal{B}_N| \leq 2$ (for our particular choice of settings) grows with increasing number of parties N. The asymptotic analysis (large r and small $\mathcal{J}$) yields for $N = 5$: $\mathcal{B}_5^{\max} \approx 2.48$ with $\mathcal{J}e^{+2r} = 5(\ln 2)/24$. For a given amount of squeezing, smaller displacements $\mathcal{J}$ than those for $N \leq 4$ (at the same squeezing) are needed to approach this maximum violation. Another interesting observation is that in all four cases ($N = 2, 3, 4, 5$), violations occur for any nonzero squeezing. This implies the presence of N-partite entanglement for any nonzero squeezing, which is indeed what we found in section 2. Moreover, we see also for modest finite squeezing, the size of the violations (at optimal displacement $\mathcal{J}$) grows with increasing N.

We will now examine the general case of N parties. How does the maximum violation of the Bell-type inequalities derived with the continuous-variable states evolve with increasing number of parties, in particular when compared to the exponential growth for the qubit GHZ states [143, 117]? At least for $N \leq 5$,

the maximum observed violation grows, and this growth does not appear to be exponentially large, but rather seems to decrease. The validity of this observation is not clear since we have not considered all possible combinations of α_i and α_i'. Nonetheless, there are hints that our choice of $\alpha_i = 0$ and $\alpha_i' = i\sqrt{\mathcal{J}}$ is indeed optimal. In particular, since the nonlocality is revealed for arbitrarily small squeezing, our choice appears appropriate. In the remainder of this section, we will use the same settings for a larger number of parties.

Considering an odd number of parties N, $\mathcal{B}_N$ may be written

$$\begin{aligned}\mathcal{B}_N &= \frac{1}{2^{(N-3)/2}} \sum_{k=0}^{\frac{N-1}{2}} (-1)^k \binom{N}{2k+1} \\ &\quad \times \Pi(\alpha_1', \alpha_2', ..., \alpha_{2k+1}', \alpha_{2k+2}, \alpha_{2k+3}, ..., \alpha_N), \quad \text{with } N = 3 + 8M,\end{aligned} \tag{III.79}$$

for $M = 0, 1, 2, 3, ...$, where the first $2k+1$ arguments of Π are $\alpha_1' = \alpha_2' = \cdots = \alpha_{2k+1}' = i\sqrt{\mathcal{J}}$ and the remainder are $\alpha_{2k+2} = \alpha_{2k+3} = \cdots = \alpha_N = 0$. Because of the symmetry of the states $\Pi(\boldsymbol{\alpha})$ in Eq. (III.70), all possible permutations of the $(2k+1)$ α_i''s with $\alpha_i' = i\sqrt{\mathcal{J}}$ and the $[N-(2k+1)]$ α_i's with $\alpha_i = 0$ can be described by the same function $\Pi(\alpha_1', \alpha_2', ..., \alpha_{2k+1}', \alpha_{2k+2}, \alpha_{2k+3}, ..., \alpha_N)$.

Similarly, with the same settings $\alpha_i' = i\sqrt{\mathcal{J}}$ and $\alpha_i = 0$, and again exploiting symmetry we obtain

$$\begin{aligned}\text{for } N = 5 + 8M: \quad \mathcal{B}_N &= \frac{1}{2^{(N-3)/2}} \sum_{k=0}^{\frac{N-1}{2}} (-1)^{k+1} \binom{N}{2k} \\ &\quad \times \Pi(\alpha_1', \alpha_2', ..., \alpha_{2k}', \alpha_{2k+1}, \alpha_{2k+2}, ..., \alpha_N),\end{aligned} \tag{III.80}$$

$$\begin{aligned}\text{for } N = 7 + 8M: \quad \mathcal{B}_N &= \frac{1}{2^{(N-3)/2}} \sum_{k=0}^{\frac{N-1}{2}} (-1)^{k+1} \binom{N}{2k+1} \\ &\quad \times \Pi(\alpha_1', \alpha_2', ..., \alpha_{2k+1}', \alpha_{2k+2}, \alpha_{2k+3}, ..., \alpha_N),\end{aligned} \tag{III.81}$$

$$\begin{aligned}\text{for } N = 9 + 8M: \quad \mathcal{B}_N &= \frac{1}{2^{(N-3)/2}} \sum_{k=0}^{\frac{N-1}{2}} (-1)^{k} \binom{N}{2k} \\ &\quad \times \Pi(\alpha_1', \alpha_2', ..., \alpha_{2k}', \alpha_{2k+1}, \alpha_{2k+2}, ..., \alpha_N).\end{aligned} \tag{III.82}$$

The functions concerned in these formulas are explicitly given by [see Eq. (III.70)]

$$\Pi(\alpha_1', \alpha_2', ..., \alpha_{2k}', \alpha_{2k+1}, \alpha_{2k+2}, ..., \alpha_N) = \exp\left\{-2\mathcal{J}\cosh 2r\ (2k) + 2\mathcal{J}\sinh 2r\left[2k - 2\frac{(2k)^2}{N}\right]\right\}, \tag{III.83}$$

$$\Pi(\alpha_1', \alpha_2', ..., \alpha_{2k+1}', \alpha_{2k+2}, \alpha_{2k+3}, ..., \alpha_N) = \exp\left\{-2\mathcal{J}\cosh 2r\ (2k+1) + 2\mathcal{J}\sinh 2r\left[2k+1 - 2\frac{(2k+1)^2}{N}\right]\right\}. \tag{III.84}$$

Let us first consider the case of zero squeezing, $r = 0$. The sum from Eq. (III.79) then becomes

$$\mathcal{B}_N(r=0) = 2^{\frac{3-N}{2}}(1+e^{-4\mathcal{J}})^{N/2}\ \sin[N\arctan(e^{-2\mathcal{J}})]. \tag{III.85}$$

As expected, without squeezing, no violations of the Bell-type inequalities are obtained for the unentangled, separable N-mode states: we find $\mathcal{B}_N(r=0) = 2$ if $\mathcal{J} = 0$ for any $N = 3 + 8M$ and $|\mathcal{B}_N(r=0)| < 2$ if $\mathcal{J} > 0$. In the limit $N \to \infty$, we obtain $\mathcal{B}_N(r=0) \to 0$ for any $\mathcal{J} > 0$. Similar expressions as in Eq. (III.85) can be found for $\mathcal{B}_N(r=0)$ in the other cases of odd N, $N = 5+8M$, $N = 7+8M$, and $N = 9+8M$, and in fact, no violations occur. The inequality $|\mathcal{B}_N| \leq 2$ imposed by local realistic theories thus always remains satisfied for zero squeezing.

For $N \leq 5$ parties, we already observed that the maximum violations of $|\mathcal{B}_N| \leq 2$ occur for large squeezing. Let us therefore here again consider the limit of large squeezing ($\cosh 2r \approx \sinh 2r \approx e^{+2r}/2$) and define $\mathcal{A} \equiv \mathcal{J}e^{+2r}$. Now we can write Eq. (III.83) and Eq. (III.84) as

$$\Pi(\alpha_1', \alpha_2', ..., \alpha_{2k}', \alpha_{2k+1}, \alpha_{2k+2}, ..., \alpha_N) = \exp\left[-2\mathcal{A}\ (2k)^2/N\right], \tag{III.86}$$

$$\Pi(\alpha_1', \alpha_2', ..., \alpha_{2k+1}', \alpha_{2k+2}, \alpha_{2k+3}, ..., \alpha_N) = \exp\left[-2\mathcal{A}\ (2k+1)^2/N\right]. \tag{III.87}$$

Figure III.3 shows the maxima of the violations of $|\mathcal{B}_N| \leq 2$ (for our particular choice of settings), calculated with Eq. (III.79)-(III.82) and the asymptotic results

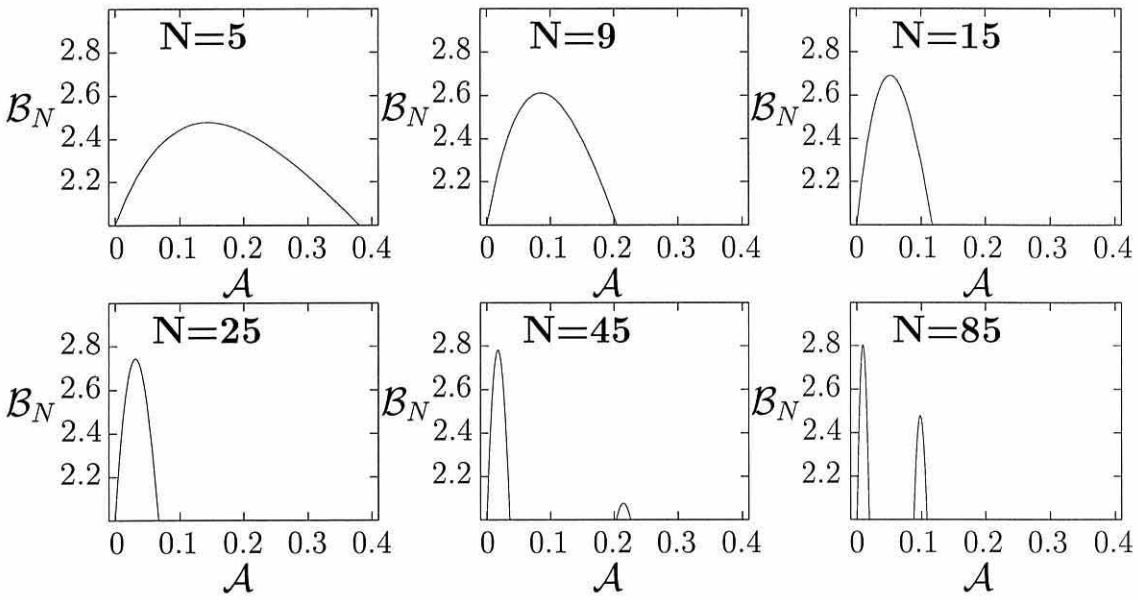

Figure III.3: Maximum violations of the inequality $|\mathcal{B}_N| \leq 2$ imposed by local realistic theories in the limit of large squeezing. $\mathcal{B}_N$ is plotted as a function of $\mathcal{A} \equiv \mathcal{J}e^{+2r}$ for different N.

from Eq. (III.86)-(III.87) for large squeezing. The maximum violation grows from $\mathcal{B}_5^{\max} \approx 2.48$ for $N = 5$ to $\mathcal{B}_{85}^{\max} \approx 2.8$ for $N = 85$ [12]. Within this range, a maximum violation near 2.8 is already attained with $N = 45$ parties and there is only a very small increase from $N = 45$ to $N = 85$. On the other hand, between $N = 5$ and $N = 9$, the maximum violation goes up from 2.48 to about 2.6 which is still significantly less than the increase between $N = 2$ ($\mathcal{B}_2^{\max} \approx 2.19$) and $N = 5$. This is in agreement with our conjecture based on the results for $N \leq 5$: apparently, the maximum violation indeed grows with increasing number of parties, but this growth seems to decelerate for larger numbers of parties. In

[12] Our results suggest that the maximum violation approaches $2.8 \approx 2\sqrt{2}$ for large N. By coincidence, this value of $2\sqrt{2}$ is the maximum violation obtainable with *two* entangled spin-1/2 particles when they share a Bell state.

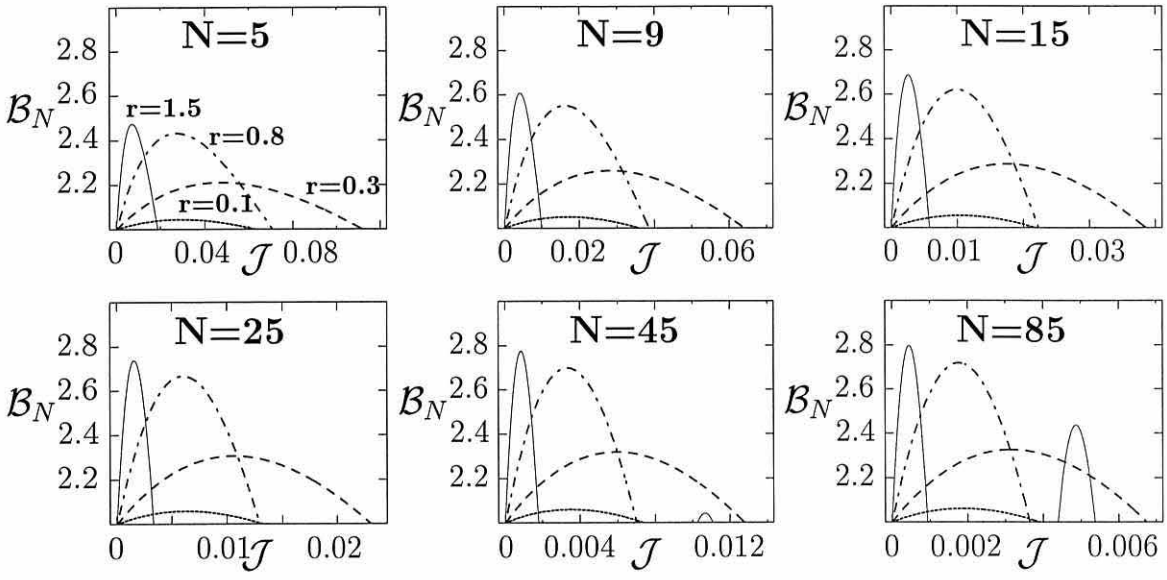

Figure III.4: Violations of the inequality $|\mathcal{B}_N| \leq 2$ imposed by local realistic theories for different N at certain amounts of squeezing of the N-mode states: $r = 0.1$ (≈ 0.9 dB), $r = 0.3$ (≈ 2.6 dB), $r = 0.8$ (≈ 6.9 dB), and $r = 1.5$ (≈ 13 dB). $\mathcal{B}_N$ is plotted as a function of $\mathcal{J}$. Note that the axes of the displacement parameter $\mathcal{J}$ vary in scale. The larger N becomes, the smaller become the displacements required.

fact, from $N = 45$ to $N = 85$, we see a second local maximum emerging rather than a significant further increase of the absolute maximum violation.

In Fig. III.4, calculated with Eq. (III.79)-(III.82) and Eq. (III.83)-(III.84), violations of $|\mathcal{B}_N| \leq 2$ are compared between different numbers of parties at certain amounts of squeezing. As stated earlier, the violations grow with N also for modest finite squeezing, but this increase is smaller than the increase of the maximum violations and becomes unrecognizable for small squeezing. An illustrating example is that a violation comparable to the maximum violation with the two-mode EPR state for large squeezing ($\mathcal{B}_2^{\max} \approx 2.19$) can be attained

with the five-mode state built from five modestly squeezed states (about 2.6 dB each).

An experimental nonlocality test based on the multipartite entangled continuous-variable states using our scheme would be in principle possible. However, such a test lies beyond current capabilities, since it requires detectors capable of resolving the number of absorbed photons [8]. Nevertheless, *the N-mode states which we have unambigously proven to exhibit nonlocality can be relatively easily generated in practice, as opposed to the discrete-variable GHZ states on which all current multi-party nonlocality proofs rely.* Furthermore, other members of the family of entangled N-mode states presented in section 3 could be used as well, in particular, the "cheapest" multi-party entangled state built with just one squeezer. Remember that for sufficiently large squeezing, the latter is equivalent to the "more expensive" N-mode states under local squeezing operations. In fact, for the bipartite state produced with one squeezer, nonlocality with respect to parity measurements has been theoretically demonstrated already [208].

Let us summarize and assess the above results. The degree of nonlocality of the continuous-variable states we considered, if represented by the maximum violation of the corresponding Bell-type inequalities, seems to grow with an increasing number of parties. This growth, however, decelerates for larger numbers of parties. Thus, the 'evolution' of the continuous-variable states' nonlocality with an increasing number of parties and the corresponding 'evolution' of nonlocality for the qubit GHZ states are qualitatively similar but quantitatively different with an exponential increase for the qubits. The reason for this may be that the qubit GHZ states are maximally entangled, whereas the continuous-variable states are nonmaximally entangled for any finite squeezing (for example, the three-mode continuous-variable state behaves more like the qubit W than the qubit GHZ state, as discussed in section 2). In fact, the observation of the nonlocality of the continuous-variable states requires small but nonzero displacements $\mathcal{J} \propto e^{-2r}$,

which is not achievable when the singular maximally entangled states for infinite squeezing are considered.

Finally, the "unbiased" minimum-energy states of the family of entangled N-mode states might yield larger violations. These states are not produced with N equal squeezers (as the states we have analyzed), but with one r_1-squeezer and $N-1$ r_2-squeezers related as in Eq. (III.55). With growing N, the unbiased states increasingly differ from the states that we have used for the nonlocality test [see Eq. (III.56) for large squeezing]. On the other hand, the biased and the unbiased states are equivalent under local squeezing operations and thus cannot differ in their potential nonlocality. In addition, this equivalence shows that also the unbiased states are only nonmaximally entangled for finite squeezing, which suggests that they also do not lead to an exponential increase of the violations as for the qubit GHZ states.

5 Broadband entanglement

In this section, we extend the single-mode description for the bipartite entangled EPR state to a realistic broadband description. The broadband entangled state is generated either directly by nondegenerate parametric amplification (also called "nondegenerate parametric down conversion") or by combining at a beam splitter two independently squeezed fields produced via degenerate down conversion or any other suitable nonlinear interaction.

First, we review the results of Ref. [155] based on the input-output formalism of Collett and Gardiner [66] where a nondegenerate optical parametric amplifier in a cavity (NOPA) is studied. We will see that the upper and lower sidebands of the NOPA output have correlations like those of the two-mode squeezed state in Eq. (III.23) (taking $r = r_1 = r_2$). The optical parametric oscillator is considered polarization nondegenerate but frequency "degenerate" (equal center frequency for the orthogonally polarized output modes). The interaction between the two

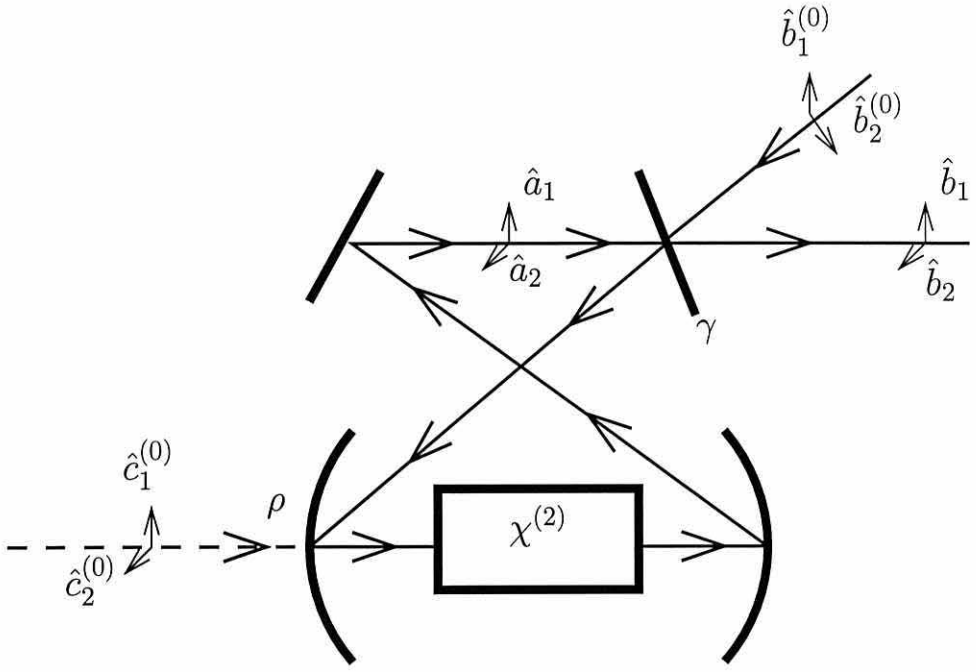

Figure III.5: The NOPA as in Ref. [155]. The two cavity modes $\hat{a}_1$ and $\hat{a}_2$ interact due to the nonlinear $\chi^{(2)}$ medium. The modes $\hat{b}_1^{(0)}$ and $\hat{b}_2^{(0)}$ are the external vacuum input modes, $\hat{b}_1$ and $\hat{b}_2$ are the external output modes, $\hat{c}_1^{(0)}$ and $\hat{c}_2^{(0)}$ are the vacuum modes due to cavity losses, γ is a damping rate and ρ is a loss parameter of the cavity.

modes is due to the nonlinear $\chi^{(2)}$ medium in a cavity (see chapter I) and may be described by the interaction Hamiltonian

$$\hat{H}_{\text{int}} = i\hbar\kappa(\hat{a}_1^\dagger \hat{a}_2^\dagger e^{-2i\omega_0 t} - \hat{a}_1 \hat{a}_2 e^{2i\omega_0 t}) \,. \tag{III.88}$$

The undepleted pump field amplitude at frequency $\omega_{\text{pump}} \equiv 2\omega_0$ is taken to be a c number and without loss of generality we have set the pump phase $\Theta = 0$ [see Eq. (I.157)]. Now input-output relations can be derived relating the cavity modes $\hat{a}_1$ and $\hat{a}_2$ to the external vacuum input modes $\hat{b}_1^{(0)}$ and $\hat{b}_2^{(0)}$, the external output modes $\hat{b}_1$ and $\hat{b}_2$, and two unwanted vacuum modes $\hat{c}_1^{(0)}$ and $\hat{c}_2^{(0)}$ representing cavity losses (Fig. III.5). Recall, the superscript '(0)' refers to vacuum modes.

We define upper-case operators in the rotating frame about the center frequency ω_0,

$$\hat{O}(t) = \hat{o}(t)e^{i\omega_0 t}, \tag{III.89}$$

with $\hat{O} = [\hat{A}_{1,2}; \hat{B}_{1,2}; \hat{B}^{(0)}_{1,2}; \hat{C}^{(0)}_{1,2}]$ and $\hat{o} = [\hat{a}_{1,2}; \hat{b}_{1,2}; \hat{b}^{(0)}_{1,2}; \hat{c}^{(0)}_{1,2}]$. By employing the Fourier transformation

$$\hat{O}(\Omega) = \frac{1}{\sqrt{2\pi}} \int dt\, \hat{O}(t)e^{i\Omega t}, \tag{III.90}$$

the fields may be described as functions of the modulation frequency Ω with the commutation relation $[\hat{O}(\Omega), \hat{O}^\dagger(\Omega')] = \delta(\Omega - \Omega')$. Expressing the outgoing modes in terms of the incoming vacuum modes, one finds [155]

$$\begin{aligned} \hat{B}_j(\Omega) &= \mathcal{G}(\Omega)\hat{B}^{(0)}_j(\Omega) + \mathcal{F}(\Omega)\hat{B}^{(0)\dagger}_k(-\Omega) \\ &\quad + \bar{\mathcal{G}}(\Omega)\hat{C}^{(0)}_j(\Omega) + \bar{\mathcal{F}}(\Omega)\hat{C}^{(0)\dagger}_k(-\Omega), \end{aligned} \tag{III.91}$$

where $k = 3 - j$, $j = 1, 2$ (so k refers to the opposite mode to j), and with coefficients to be specified later.

Let us investigate the lossless case where the output fields become

$$\hat{B}_j(\Omega) = \mathcal{G}(\Omega)\hat{B}^{(0)}_j(\Omega) + \mathcal{F}(\Omega)\hat{B}^{(0)\dagger}_k(-\Omega), \tag{III.92}$$

with

$$\begin{aligned} \mathcal{G}(\Omega) &= \frac{\kappa^2 + \gamma^2/4 + \Omega^2}{(\gamma/2 - i\Omega)^2 - \kappa^2}\ , \\ \mathcal{F}(\Omega) &= \frac{\kappa\gamma}{(\gamma/2 - i\Omega)^2 - \kappa^2}\ . \end{aligned} \tag{III.93}$$

Here, the parameter γ is a damping rate of the cavity (Fig. III.5) and is assumed to be equal for both polarizations. Equation (III.92) represents the input-output relations for a lossless NOPA.

Following Ref. [56], we introduce frequency resolved quadrature amplitudes

given by

$$\begin{aligned}
\hat{X}_j(\Omega) &= \frac{1}{2}[\hat{B}_j(\Omega) + \hat{B}_j^\dagger(-\Omega)], \\
\hat{P}_j(\Omega) &= \frac{1}{2i}[\hat{B}_j(\Omega) - \hat{B}_j^\dagger(-\Omega)], \\
\hat{X}_j^{(0)}(\Omega) &= \frac{1}{2}[\hat{B}_j^{(0)}(\Omega) + \hat{B}_j^{(0)\dagger}(-\Omega)], \\
\hat{P}_j^{(0)}(\Omega) &= \frac{1}{2i}[\hat{B}_j^{(0)}(\Omega) - \hat{B}_j^{(0)\dagger}(-\Omega)],
\end{aligned} \tag{III.94}$$

provided $\Omega \ll \omega_0$. Using them we may write Eq. (III.92) as

$$\begin{aligned}
\hat{X}_j(\Omega) &= \mathcal{G}(\Omega)\hat{X}_j^{(0)}(\Omega) + \mathcal{F}(\Omega)\hat{X}_k^{(0)}(\Omega), \\
\hat{P}_j(\Omega) &= \mathcal{G}(\Omega)\hat{P}_j^{(0)}(\Omega) - \mathcal{F}(\Omega)\hat{P}_k^{(0)}(\Omega).
\end{aligned} \tag{III.95}$$

Here, we have used $\mathcal{G}(\Omega) = \mathcal{G}^*(-\Omega)$ and $\mathcal{F}(\Omega) = \mathcal{F}^*(-\Omega)$.

At this point, we shall show that the output quadratures of a lossless NOPA in Eq. (III.95) correspond to two independently squeezed modes coupled to a two-mode squeezed state at a beam splitter. The operational significance of this fact is that the *broadband* EPR state can be created either by nondegenerate parametric down conversion as described by the interaction Hamiltonian in Eq. (III.88), or by combining at a beam splitter two independently squeezed fields generated via degenerate down conversion [115] [13].

Let us thus define the linear combinations of the two output modes (barred quantities)

$$\begin{aligned}
\hat{\bar{B}}_1 &\equiv \frac{1}{\sqrt{2}}(\hat{B}_1 + \hat{B}_2), \\
\hat{\bar{B}}_2 &\equiv \frac{1}{\sqrt{2}}(\hat{B}_1 - \hat{B}_2),
\end{aligned} \tag{III.96}$$

and of the two vacuum input modes

$$\begin{aligned}
\hat{\bar{B}}_1^{(0)} &\equiv \frac{1}{\sqrt{2}}(\hat{B}_1^{(0)} + \hat{B}_2^{(0)}), \\
\hat{\bar{B}}_2^{(0)} &\equiv \frac{1}{\sqrt{2}}(\hat{B}_1^{(0)} - \hat{B}_2^{(0)}).
\end{aligned} \tag{III.97}$$

[13] As it was done in the quantum teleportation experiment of Ref. [87].

In terms of these combinations, Eq. (III.92) becomes

$$\begin{aligned}\hat{\tilde{B}}_1(\Omega) &= \mathcal{G}(\Omega)\hat{\tilde{B}}_1^{(0)}(\Omega) + \mathcal{F}(\Omega)\hat{\tilde{B}}_1^{(0)\dagger}(-\Omega),\\ \hat{\tilde{B}}_2(\Omega) &= \mathcal{G}(\Omega)\hat{\tilde{B}}_2^{(0)}(\Omega) - \mathcal{F}(\Omega)\hat{\tilde{B}}_2^{(0)\dagger}(-\Omega).\end{aligned} \tag{III.98}$$

In Eq. (III.98), the initially coupled modes of Eq. (III.92) are decoupled, corresponding to two independent degenerate parametric amplifiers.

In the limit $\Omega \to 0$, the two modes of Eq. (III.98) are each in a single-mode squeezed state as in Eq. (I.152). More explicitly, by setting $\mathcal{G}(0) \equiv \cosh r$ and $\mathcal{F}(0) \equiv \sinh r$, the annihilation operators

$$\begin{aligned}\hat{\tilde{B}}_1 &= \cosh r\hat{\tilde{B}}_1^{(0)} + \sinh r\hat{\tilde{B}}_1^{(0)\dagger},\\ \hat{\tilde{B}}_2 &= \cosh r\hat{\tilde{B}}_2^{(0)} - \sinh r\hat{\tilde{B}}_2^{(0)\dagger},\end{aligned} \tag{III.99}$$

have the quadrature operators

$$\begin{aligned}\hat{\tilde{X}}_1 = e^{+r}\hat{\tilde{X}}_1^{(0)}, \quad \hat{\tilde{P}}_1 = e^{-r}\hat{\tilde{P}}_1^{(0)},\\ \hat{\tilde{X}}_2 = e^{-r}\hat{\tilde{X}}_2^{(0)}, \quad \hat{\tilde{P}}_2 = e^{+r}\hat{\tilde{P}}_2^{(0)}.\end{aligned} \tag{III.100}$$

From the alternative perspective of combining two independently squeezed modes at a 50:50 beam splitter to obtain the EPR state, we must simply invert the transformation of Eq. (III.96) and recouple the two modes:

$$\begin{aligned}\hat{B}_1 &= \frac{1}{\sqrt{2}}(\hat{\tilde{B}}_1 + \hat{\tilde{B}}_2)\\ &= \frac{1}{\sqrt{2}}[\cosh r(\hat{\tilde{B}}_1^{(0)} + \hat{\tilde{B}}_2^{(0)}) + \sinh r(\hat{\tilde{B}}_1^{(0)\dagger} - \hat{\tilde{B}}_2^{(0)\dagger})]\\ &= \cosh r\hat{B}_1^{(0)} + \sinh r\hat{B}_2^{(0)\dagger},\\ \hat{B}_2 &= \frac{1}{\sqrt{2}}(\hat{\tilde{B}}_1 - \hat{\tilde{B}}_2)\\ &= \frac{1}{\sqrt{2}}[\cosh r(\hat{\tilde{B}}_1^{(0)} - \hat{\tilde{B}}_2^{(0)}) + \sinh r(\hat{\tilde{B}}_1^{(0)\dagger} + \hat{\tilde{B}}_2^{(0)\dagger})]\\ &= \cosh r\hat{B}_2^{(0)} + \sinh r\hat{B}_1^{(0)\dagger},\end{aligned} \tag{III.101}$$

and

$$\begin{aligned}
\hat{X}_1 &= \frac{1}{\sqrt{2}}(\hat{\tilde{X}}_1 + \hat{\tilde{X}}_2) = \frac{1}{\sqrt{2}}(e^{+r}\hat{\tilde{X}}_1^{(0)} + e^{-r}\hat{\tilde{X}}_2^{(0)}),\\
\hat{P}_1 &= \frac{1}{\sqrt{2}}(\hat{\tilde{P}}_1 + \hat{\tilde{P}}_2) = \frac{1}{\sqrt{2}}(e^{-r}\hat{\tilde{P}}_1^{(0)} + e^{+r}\hat{\tilde{P}}_2^{(0)}),\\
\hat{X}_2 &= \frac{1}{\sqrt{2}}(\hat{\tilde{X}}_1 - \hat{\tilde{X}}_2) = \frac{1}{\sqrt{2}}(e^{+r}\hat{\tilde{X}}_1^{(0)} - e^{-r}\hat{\tilde{X}}_2^{(0)}),\\
\hat{P}_2 &= \frac{1}{\sqrt{2}}(\hat{\tilde{P}}_1 - \hat{\tilde{P}}_2) = \frac{1}{\sqrt{2}}(e^{-r}\hat{\tilde{P}}_1^{(0)} - e^{+r}\hat{\tilde{P}}_2^{(0)}),
\end{aligned} \tag{III.102}$$

as the two-mode squeezed state in Eq. (III.23) (taking $r = r_1 = r_2$). The coupled modes in Eq. (III.101) expressed in terms of $\hat{B}_1^{(0)}$ and $\hat{B}_2^{(0)}$ are the two NOPA output modes of Eq. (III.92), if $\Omega \to 0$ and $\mathcal{G}(0) \equiv \cosh r$, $\mathcal{F}(0) \equiv \sinh r$.

More generally, for $\Omega \neq 0$, the quadratures corresponding to Eq. (III.98),

$$\begin{aligned}
\hat{\tilde{X}}_1(\Omega) &= [\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{X}}_1^{(0)}(\Omega),\\
\hat{\tilde{P}}_1(\Omega) &= [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{P}}_1^{(0)}(\Omega),\\
\hat{\tilde{X}}_2(\Omega) &= [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{X}}_2^{(0)}(\Omega),\\
\hat{\tilde{P}}_2(\Omega) &= [\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{P}}_2^{(0)}(\Omega),
\end{aligned} \tag{III.103}$$

are coupled to yield

$$\begin{aligned}
\hat{X}_1(\Omega) &= \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{X}}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{X}}_2^{(0)}(\Omega),\\
\hat{P}_1(\Omega) &= \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{P}}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{P}}_2^{(0)}(\Omega),\\
\hat{X}_2(\Omega) &= \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{X}}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{X}}_2^{(0)}(\Omega),\\
\hat{P}_2(\Omega) &= \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)]\hat{\tilde{P}}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}}[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)]\hat{\tilde{P}}_2^{(0)}(\Omega).
\end{aligned} \tag{III.104}$$

The quadratures in Eq. (III.104) are precisely the NOPA output quadratures of Eq. (III.95) as anticipated, but now also for the broadband case written in a form analogous to the single-mode description in Eq. (III.23). With the functions $\mathcal{G}(\Omega)$

and $\mathcal{F}(\Omega)$ of Eq. (III.93), we obtain

$$\begin{aligned} \mathcal{G}(\Omega) - \mathcal{F}(\Omega) &= \frac{\gamma/2 - \kappa + i\Omega}{\gamma/2 + \kappa - i\Omega} \ , \\ \mathcal{G}(\Omega) + \mathcal{F}(\Omega) &= \frac{(\gamma/2 + \kappa)^2 + \Omega^2}{(\gamma/2 - i\Omega)^2 - \kappa^2} \ . \end{aligned} \tag{III.105}$$

For the limits $\Omega \to 0$, $\kappa \to \gamma/2$ (the limit of infinite squeezing), we obtain $[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)] \to 0$ and $[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)] \to \infty$. If $\Omega \to 0$, $\kappa \to 0$ (the classical limit of no squeezing), then $[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)] \to 1$ and $[\mathcal{G}(\Omega) + \mathcal{F}(\Omega)] \to 1$. Thus, for $\Omega \to 0$, Eq. (III.104) in the above-mentioned limits corresponds to Eq. (III.102) in the analogous limits $r \to \infty$ (infinite squeezing) and $r \to 0$ (no squeezing). For large squeezing, apparently the individual modes of the "broadband two-mode squeezed state" in Eq. (III.104) are very noisy. In general, the input vacuum modes are amplified in the NOPA, resulting in output modes with large fluctuations. But the correlations between the two modes increase simultaneously, so that $[\hat{X}_1(\Omega) - \hat{X}_2(\Omega)] \to 0$ and $[\hat{P}_1(\Omega) + \hat{P}_2(\Omega)] \to 0$ for $\Omega \to 0$ and $\kappa \to \gamma/2$.

The squeezing spectra of the independently squeezed modes can be derived from Eq. (III.103) and are given by the spectral variances

$$\begin{aligned} \langle \Delta\hat{\tilde{X}}_1^\dagger(\Omega) \Delta\hat{\tilde{X}}_1(\Omega') \rangle &= \langle \Delta\hat{\tilde{P}}_2^\dagger(\Omega) \Delta\hat{\tilde{P}}_2(\Omega') \rangle = \delta(\Omega - \Omega') |S_+(\Omega)|^2 \langle (\Delta\hat{X})^2 \rangle_{\text{vacuum}} , \\ \langle \Delta\hat{\tilde{X}}_2^\dagger(\Omega) \Delta\hat{\tilde{X}}_2(\Omega') \rangle &= \langle \Delta\hat{\tilde{P}}_1^\dagger(\Omega) \Delta\hat{\tilde{P}}_1(\Omega') \rangle = \delta(\Omega - \Omega') |S_-(\Omega)|^2 \langle (\Delta\hat{X})^2 \rangle_{\text{vacuum}} , \end{aligned} \tag{III.106}$$

here with $|S_+(\Omega)|^2 = |\mathcal{G}(\Omega) + \mathcal{F}(\Omega)|^2$ and $|S_-(\Omega)|^2 = |\mathcal{G}(\Omega) - \mathcal{F}(\Omega)|^2$, and $\langle (\Delta\hat{X})^2 \rangle_{\text{vacuum}} \equiv 1/4$. In general, Eq. (III.106) may define arbitrary squeezing spectra of two statistically identical but independent broadband squeezed states. The two corresponding squeezed modes

$$\begin{aligned} \hat{\tilde{X}}_1(\Omega) &= S_+(\Omega) \hat{\tilde{X}}_1^{(0)}(\Omega), \quad \hat{\tilde{P}}_1(\Omega) = S_-(\Omega) \hat{\tilde{P}}_1^{(0)}(\Omega), \\ \hat{\tilde{X}}_2(\Omega) &= S_-(\Omega) \hat{\tilde{X}}_2^{(0)}(\Omega), \quad \hat{\tilde{P}}_2(\Omega) = S_+(\Omega) \hat{\tilde{P}}_2^{(0)}(\Omega), \end{aligned} \tag{III.107}$$

where $S_-(\Omega)$ refers to the quiet quadratures and $S_+(\Omega)$ to the noisy ones, can be

used as a broadband EPR source when they are combined at a beamsplitter:

$$\begin{aligned}
\hat{X}_1(\Omega) &= \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{X}}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{X}}_2^{(0)}(\Omega), \\
\hat{P}_1(\Omega) &= \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{P}}_1^{(0)}(\Omega) + \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{P}}_2^{(0)}(\Omega), \\
\hat{X}_2(\Omega) &= \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{X}}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{X}}_2^{(0)}(\Omega), \\
\hat{P}_2(\Omega) &= \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{P}}_1^{(0)}(\Omega) - \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{P}}_2^{(0)}(\Omega). \qquad \text{(III.108)}
\end{aligned}$$

Before obtaining this "broadband two-mode squeezed vacuum state", the squeezing of the two initial modes may be generated by any suitable nonlinear interaction, e.g., also by four-wave mixing in a cavity (see chapter I).

In the current chapter, we have presented entangled quantum resources that are potentially useful in entanglement-based continuous-variable quantum communication. By means of squeezed-light sources and beam splitters, entanglement can be generated between an arbitrary number of parties. In order to do so, even only one squeezed state may suffice. We have proposed a family of multipartite entangled continuous-variable states that are truly (though nonmaximally) entangled with respect to all their parties. Further, violations of N-party inequalities imposed by local realism have been found to occur using some of these states. Finally, we have also given a realistic broadband description for the bipartite entangled state. In the following chapter, we will make use of these entanglement resources for (broadband) quantum communication with continuous variables.

IV

Quantum Communication with Continuous Variables

The term quantum communication normally means that quantum information encoded in nonorthogonal quantum states, for instance, qubits $\alpha|0\rangle + \beta|1\rangle$, is to be transferred from a sender ("Alice") to a receiver ("Bob"). In classical communication, the signals (bits) are encoded in classical orthogonal states such as the above qubit state with $\alpha = 0$ or 1. The nonorthogonal quantum states when sent through a quantum communication channel are in any realistic situation subject to environmental-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, namely qubits. These methods are quantum teleportation, combined with a purification of the shared entanglement [17], or quantum error correction (originally proposed for reducing decoherence in a quantum computer [184] rather than in a quantum communication channel). They enable, in principle, completely reliable transmission of quantum information. In this chapter, we will now discuss and develop quantum communication protocols for continuous variables that are based on analogous methods, in particular quantum teleportation.

We will see that not only the generation of the resource (continuous-variable entanglement), but also its *manipulation* via local measurements and unitary operations turns out to be very easy. For instance, completely distinguishing

between maximally entangled states through a suitable measurement, as needed for quantum teleportation, is not possible with the qubit Bell states using only linear optics [138, 199]. 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 feed-forward techniques (see chapter I).

Another very important subject of current research that may fall under the term quantum communication is quantum cryptography or quantum key distribution, which aims at conveying classical information with maximum security against potential eavesdropping. This security is provided by the fact that an eavesdropper is revealed when she ("Eve") is trying to extract the classical information from the quantum system sent. She would have to perform a measurement, and thereby inevitably disturb the quantum system. Quantum cryptography was originally proposed for discrete variables, but recently several proposals for continuous-variable quantum cryptography appeared. We will give an overview of these proposals and briefly discuss possible extensions to more than two parties for so-called quantum secret sharing.

1 Reliable transmission of quantum information

In this section, we are interested in the reliable transmission of continuous-variable quantum information, in particular through quantum teleportation. We will consider the transfer of various kinds of quantum information and quantum features, for instance the teleportation of entanglement. The new results in this section are partly based on van Loock and Braunstein [131, 132] and van Loock, Braunstein, and Kimble [136].

a Teleportation of continuous quantum variables

The teleportation of continuous quantum variables such as position and momentum of a particle, as first proposed in Ref. [198], relies on the entanglement of the states in the original Einstein, Podolsky, and Rosen (EPR) paradox [81]. 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 chapter I. 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 in Ref. [37]. Based on this proposal, in fact, quantum teleportation of arbitrary coherent states has been achieved with a fidelity $F = 0.58 \pm 0.02$ [87]. 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 potentially includes any coherent states [35]. We will 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 an "a priori" (or "unconditional") teleportation with high efficiency [37], as reported in Refs. [32, 87]. In this experiment, three criteria necessary for quantum teleportation were achieved for the first time:

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 the teleported states is higher than that which could be achieved if the sending and the receiving stations were linked only by a classical channel.

Let us now first describe the teleportation of continuous quantum variables in the simplest way, considering just single modes of the electromagnetic field. A realistic broadband description, more appropriate for giving an account of the

mentioned teleportation experiment, will be presented later.

In the teleportation scheme of a single mode of the electromagnetic field, the shared entanglement resource is the two-mode state of Eq. (III.23) [in the original proposal [37], the Wigner function of the finitely squeezed EPR state of Eq. (III.28) was used, corresponding to Eq. (III.23) for $r = r_1 = r_2$]. The entangled state is sent in two halves: one to "Alice" (the teleporter or sender) and the other one to "Bob" (the receiver), as illustrated in Fig. IV.1. 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 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 (see chapter II). According to this analogy, we call Alice's quadrature measurements for the teleportation of the state of a single mode (and of a broadband field in the following sections) "Bell detection". Due to this 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.

b Teleportation protocol in Heisenberg representation

Let us recall that in the state of Eq. (III.23), modes 1 and 2 are entangled to a finite degree. In the limit of infinite squeezing, $r = r_1 = r_2 \to \infty$, the

individual modes become infinitely noisy, but also the EPR correlations between them 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. Alice's mode is then combined at a (phase-free) 50:50 beam splitter with the input mode "in":

$$\begin{aligned} \hat{x}_{\rm u} &= \frac{1}{\sqrt{2}}\hat{x}_{\rm in} - \frac{1}{\sqrt{2}}\hat{x}_1, \quad \hat{p}_{\rm u} = \frac{1}{\sqrt{2}}\hat{p}_{\rm in} - \frac{1}{\sqrt{2}}\hat{p}_1, \\ \hat{x}_{\rm v} &= \frac{1}{\sqrt{2}}\hat{x}_{\rm in} + \frac{1}{\sqrt{2}}\hat{x}_1, \quad \hat{p}_{\rm v} = \frac{1}{\sqrt{2}}\hat{p}_{\rm in} + \frac{1}{\sqrt{2}}\hat{p}_1. \end{aligned} \tag{IV.1}$$

Using Eq. (IV.1) we will find it useful to write Bob's mode 2 as

$$\begin{aligned} \hat{x}_2 &= \hat{x}_{\rm in} - (\hat{x}_1 - \hat{x}_2) - \sqrt{2}\hat{x}_{\rm u} \\ &= \hat{x}_{\rm in} - \sqrt{2}e^{-r_2}\hat{x}_2^{(0)} - \sqrt{2}\hat{x}_{\rm u}, \\ \hat{p}_2 &= \hat{p}_{\rm in} + (\hat{p}_1 + \hat{p}_2) - \sqrt{2}\hat{p}_{\rm v} \\ &= \hat{p}_{\rm in} + \sqrt{2}e^{-r_1}\hat{p}_1^{(0)} - \sqrt{2}\hat{p}_{\rm v}. \end{aligned} \tag{IV.2}$$

Alice's Bell detection yields certain classical values $x_{\rm u}$ and $p_{\rm v}$ for $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$. The quantum variables $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$ become classically determined, random variables. We indicate this by turning $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$ into $x_{\rm u}$ and $p_{\rm v}$. The classical probability distribution of $x_{\rm u}$ and $p_{\rm v}$ is associated with the quantum statistics of the previous operators. 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 $x_{\rm u}$ and $p_{\rm v}$, Bob displaces his mode,

$$\begin{aligned} \hat{x}_2 \longrightarrow \hat{x}_{\rm tel} &= \hat{x}_2 + g\sqrt{2}x_{\rm u}, \\ \hat{p}_2 \longrightarrow \hat{p}_{\rm tel} &= \hat{p}_2 + g\sqrt{2}p_{\rm v}, \end{aligned} \tag{IV.3}$$

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 displacement eliminates $x_{\rm u}$ and $p_{\rm v}$ appearing in Eq. (IV.2) after the collapse

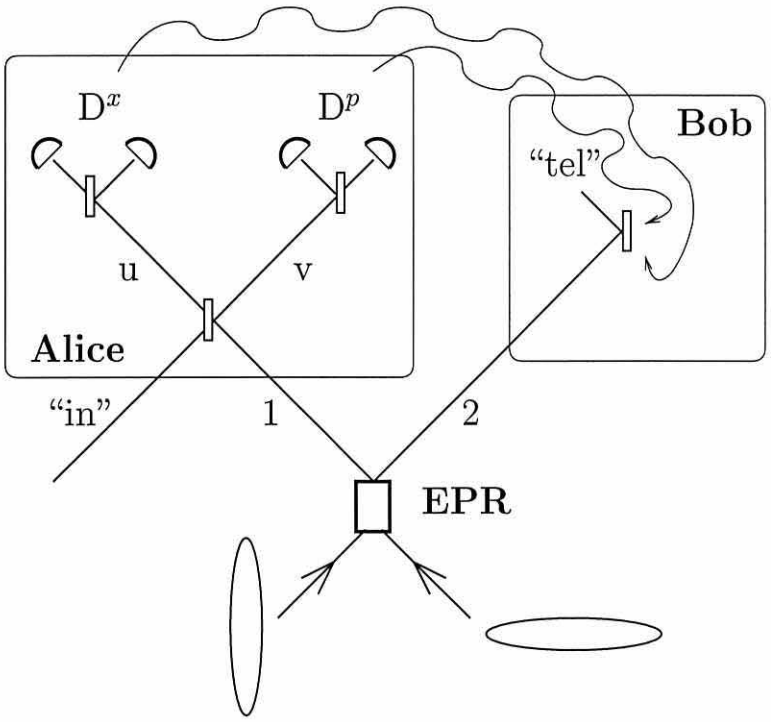

Figure IV.1: Teleportation of a single mode of the electromagnetic field. Alice and Bob share the entangled state of modes 1 and 2. Alice combines the mode "in" to be teleported with her half of the EPR state at a beam splitter. The homodyne detectors D^x and D^p yield classical photocurrents for the quadratures $x_{\rm u}$ and $p_{\rm v}$, respectively. Bob performs phase-space displacements of his half of the EPR state depending on Alice's classical results.

of $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$ due to the Bell detection. The teleported field then becomes

$$\begin{aligned} \hat{x}_{\rm tel} &= \hat{x}_{\rm in} - \sqrt{2}e^{-r_2}\hat{x}_2^{(0)}, \\ \hat{p}_{\rm tel} &= \hat{p}_{\rm in} + \sqrt{2}e^{-r_1}\hat{p}_1^{(0)}. \end{aligned} \tag{IV.4}$$

For an arbitrary gain g, we obtain

$$\begin{aligned} \hat{x}_{\rm tel} &= g\hat{x}_{\rm in} - \frac{g-1}{\sqrt{2}}e^{+r_1}\hat{x}_1^{(0)} - \frac{g+1}{\sqrt{2}}e^{-r_2}\hat{x}_2^{(0)}, \\ \hat{p}_{\rm tel} &= g\hat{p}_{\rm in} + \frac{g-1}{\sqrt{2}}e^{+r_2}\hat{p}_2^{(0)} + \frac{g+1}{\sqrt{2}}e^{-r_1}\hat{p}_1^{(0)}. \end{aligned} \tag{IV.5}$$

Note that these equations take no Bell detector inefficiencies into account.

Consider the case $g = 1$, with $r = r_1 = r_2$. For infinite squeezing $r \to \infty$, Eq. (IV.4) 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 [37]. The two quduties represent the minimal tariff for every "classical teleportation" scheme [35]. 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 (see chapter II). 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 which 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 field to be detected, plus an additional unit of vacuum noise due to the detection [in other words, when measuring a coherent-state Wigner function one obtains as the measured distribution the Q function in Eq. (II.40)].

The second quduty arises when Bob uses the information of Alice's detection to generate the state at amplitude $\sqrt{2}x_{\text{u}} + i\sqrt{2}p_{\text{v}}$ [37]. It can be interpreted as the standard quantum limit imposed on state broadcasting.

c *Teleportation protocol in Schrödinger representation*

In chapter II, we have presented the original discrete-variable teleportation protocol in the Schrödinger representation. First we considered an appropriate decomposition of the entire system, and then we used a "twist" formalism (taking nonmaximally entangled quantum channels into account). We will now deal with

the corresponding decompositions for continuous variables and the twist formalism in this case, assuming $r = r_1 = r_2$ for the entangled state. Let us introduce the continuous-variable analogues, namely the (now unnormalizable) maximally entangled measurement basis states

$$\hat{U}(\gamma) \otimes \mathbb{1} \frac{1}{\sqrt{\pi}} \int dx |x\rangle|x\rangle = \mathbb{1} \otimes \hat{U}(\gamma') \frac{1}{\sqrt{\pi}} \int dx |x\rangle|x\rangle \,, \tag{IV.6}$$

and the distortion operator

$$\hat{\mathcal{D}}(\lambda) = \int dx\, dx'\, f(x, x', \lambda) |x\rangle\langle x'| \,, \tag{IV.7}$$

corresponding to the "standard" (undisplaced) nonmaximally entangled states

$$|\psi(\lambda)\rangle = \int dx\, dx'\, f(x, x', \lambda) |x\rangle|x'\rangle \,. \tag{IV.8}$$

These states $|\psi(\lambda)\rangle \equiv |\psi^{(2)}(\lambda)\rangle$ are effectively two-mode squeezed vacuum states with squeezing described by $\lambda = \tanh^2 r$ [see Eq. (III.26)]. Note that in the limit $\lambda \to 1$, $|\psi(\lambda)\rangle \propto \int dx |x\rangle|x\rangle$ becomes maximally entangled, and the distortion operator becomes proportional to the identity $\hat{\mathcal{D}}(\lambda) \propto \int dx |x\rangle\langle x| = \mathbb{1}$.

The unitary transformations that generate the maximally entangled measurement basis for continuous variables can be written as

$$\hat{U}(\gamma) \equiv \hat{U}(u, v) = \int dx\, e^{2ixv} |x\rangle\langle x - u| \,, \tag{IV.9}$$

with $\hat{U}(\gamma') = \hat{U}^T(\gamma) = \hat{U}(-u, v)$. Using Eq. (IV.6), we see that the "continuous-variable Bell states" are

$$|\Psi(u, v)\rangle = \frac{1}{\sqrt{\pi}} \int dx\, e^{2ixv} |x\rangle|x - u\rangle, \tag{IV.10}$$

and obey the completeness and orthogonality relations

$$\begin{aligned} \int du\, dv\, |\Psi(u, v)\rangle\langle\Psi(u, v)| &= \mathbb{1} \otimes \mathbb{1}, \\ \langle\Psi(u, v)|\Psi(u', v')\rangle &= \delta(u - u')\, \delta(v - v'). \end{aligned} \tag{IV.11}$$

This means that for $\lambda \to 1$, $|\psi(\lambda)\rangle \propto |\Psi(0,0)\rangle$. The unitary transformations in Eq. (IV.9) provide displacements in phase-space by position u and momentum v, and correspond to the displacement operator $\hat{D}(\alpha)$ of Eq. (I.80) with $\alpha = u + iv$ and $\hat{a} = \hat{x} + i\hat{p}$.

The "Bell measurement" by Alice on the maximally entangled basis and the corresponding twist by Bob of the nonmaximally entangled channel state then reads (with the unknown input state $|\phi\rangle_{\rm in} = \int dx\, \phi(x)|x\rangle_{\rm in}$)

$$\begin{aligned} {}_{\rm in,1}\langle\!\langle \overrightarrow{\Psi}(u,v)|\phi\rangle_{\rm in} \otimes |\overleftarrow{\psi}^{(\lambda)}(u,v)\rangle\!\rangle_{1,2} &= \frac{1}{\sqrt{\pi}} \hat{U}(u,v)\hat{\mathcal{D}}(\lambda)\hat{U}^\dagger(u,v)\hat{\tau}_{2,\rm in}|\phi\rangle_{\rm in} \\ &= \frac{1}{\sqrt{\pi}} \hat{U}(u,v)\hat{\mathcal{D}}(\lambda)\hat{U}^\dagger(u,v)|\phi\rangle_2, \end{aligned} \tag{IV.12}$$

with the transfer operator

$$\hat{\tau}_{2,\rm in} = \int dx\, |x\rangle_{2\,\rm in}\langle x| \,, \tag{IV.13}$$

and the twisted nonmaximally entangled state

$$|\overleftarrow{\psi}^{(\lambda)}(u,v)\rangle\!\rangle_{1,2} = \mathbb{1} \otimes \hat{U}(u,v) \int dx\, dx'\, f(x,x',\lambda)|x\rangle_1|x'\rangle_2 \,. \tag{IV.14}$$

The corresponding twist depends on the measured maximally entangled state

$$|\overrightarrow{\Psi}(u,v)\rangle\!\rangle_{\rm in,1} = \hat{U}(u,v) \otimes \mathbb{1}\, \frac{1}{\sqrt{\pi}} \int dx|x\rangle_{\rm in}|x\rangle_1 \,. \tag{IV.15}$$

In this notation, $|\overleftarrow{\psi}^{(\lambda)}(0,0)\rangle\!\rangle = |\overrightarrow{\psi}^{(\lambda)}(0,0)\rangle\!\rangle = |\psi(\lambda)\rangle$ is the undisplaced two-mode squeezed vacuum state. The protocol given here contains two special choices: Alice's measurement is a special POVM, namely a von Neumann projection on a complete orthogonal basis $|\overrightarrow{\Psi}(u,v)\rangle\!\rangle\langle\!\langle\overrightarrow{\Psi}(u,v)|$ [1], and Bob's unitary

[1] Since we are dealing with states having a continuous spectrum, the actual projection operator should be defined as

$$\hat{P}(u,v) \equiv \int_{u-\epsilon}^{u+\epsilon} \int_{v-\epsilon}^{v+\epsilon} du'\, dv'\, |\overrightarrow{\Psi}(u',v')\rangle\!\rangle\langle\!\langle\overrightarrow{\Psi}(u',v')| \,, \tag{IV.16}$$

in order to ensure $\hat{P}^2(u,v) = \hat{P}(u,v)$. For our purposes at this point, however, the simplification $\epsilon \to 0$ suffices.

transformation involves a twist that exactly corresponds to the choice of unit gain $g = 1$ in the displacements of Eq. (IV.3). For imperfect resources or detection, neither the von Neumann projection nor the twist (unit-gain displacements) are necessarily the best choice. What is the best will depend on the special task that is to be fulfilled via quantum teleportation, as we will see later.

Close examination of the (unnormalized) teleported state after the twist, $\hat{U}(u,v)\hat{\mathcal{D}}(\lambda)\hat{U}^{\dagger}(u,v)|\phi\rangle_2$, shows that only for $\lambda \to 1$ (maximally entangled channel) does it correspond to the unknown input state. Furthermore, for a nonmaximally entangled channel, the teleported state still depends on the measurement results u and v after the twist:

$$\hat{U}(u,v)\hat{\mathcal{D}}(\lambda)\hat{U}^{\dagger}(u,v)|\phi\rangle_2 = \int dx\, dx'\, e^{2iv(x-x')} f(x-u, x'-u, \lambda)\phi(x')|x\rangle_2 \,. \tag{IV.17}$$

Taking into account the randomness of the measurement results u and v, the teleported ensemble state is actually a mixture of the above states. The teleported ensemble state is a pure state independent of u and v only for $\lambda \to 1$ (and then it becomes exactly the unknown input state). We made an analogous observation for d-level systems in chapter II. Apparently, *it is a general feature of quantum teleportation using nonmaximally entangled states that the teleported state depends on the Bell measurement results even after the twist operation.* Without using the twist formalism, we may look at the following decomposition which is analogous to the decomposition for discrete variables in Eq. (II.53):

$$\begin{aligned} |\phi\rangle_{\rm in} \otimes |\psi(\lambda)\rangle_{12} &= \frac{1}{\sqrt{\pi}} \int du\, dv\, |\Psi(u,v)\rangle_{{\rm in},1} \hat{U}_2^{\dagger}(u,v) \\ &\quad \times \int dx\, dx'\, e^{2iv(x-x')} f(x-u, x'-u, \lambda)\phi(x')|x\rangle_2 . \end{aligned} \tag{IV.18}$$

After the Bell measurement the state collapses and application of the right $\hat{U}_2(u,v)$ by Bob yields the teleported state in the second line of Eq. (IV.18),

which is identical to the (u,v)-dependent state in Eq. (IV.17). In order to get rid of this (u,v)-dependence of the teleported state (which leads to nonunit fidelity), we could rearrange the decomposition in the following way:

$$|\phi\rangle_{\rm in} \otimes |\psi(\lambda)\rangle_{12} \;=\; \frac{1}{\pi} \int du\, dv\, |\psi^{(\lambda)}(u,v)\rangle_{\rm in,1} \hat{U}_2^{\dagger}(u,v)\, |\phi\rangle_2, \qquad \text{(IV.19)}$$

with the displaced two-mode squeezed states

$$|\psi^{(\lambda)}(u,v)\rangle_{\rm in,1} = \hat{U}(u,v) \otimes \mathbb{1} \int dx\, dx'\, f(x,x',\lambda) |x\rangle_{\rm in} |x'\rangle_1 \; . \qquad \text{(IV.20)}$$

A measurement by Alice that can distinguish between the states $|\psi^{(\lambda)}(u,v)\rangle_{\rm in,1}$ in the decomposition Eq. (IV.19) would enable Bob to retrieve exactly the unknown input state after applying the right $\hat{U}_2(u,v)$. Such a measurement is of course not a simple von Neumann projection as previously, but rather a more general POVM capable of discriminating nonorthogonal states such as $|\psi^{(\lambda)}(u,v)\rangle_{\rm in,1}$. In the case of discrete d-level systems, we mentioned in chapter II that the POVM required can be constructed. Though it sometimes yields inconclusive results, otherwise it leads to perfect teleportation of the unknown input state. In Eq. (IV.19), we have given the continuous-variable analogue to the decomposition for d-level systems of Eq. (II.54) that aims at finding a protocol for this *conclusive teleportation*. The analogous conditions for a corresponding continuous-variable POVM $\hat{E}(u,v,w)$ with conclusive results if $w = w_0$ can be written as

$$\langle \psi^{(\lambda)}(u',v') | \hat{E}(u,v,w_0) | \psi^{(\lambda)}(u',v') \rangle \;\propto\; \delta(u-u')\, \delta(v-v') \; , \qquad \text{(IV.21)}$$

$$\int du\, dv\, dw\, \hat{E}(u,v,w) \;=\; \mathbb{1} \otimes \mathbb{1} \; . \qquad \text{(IV.22)}$$

Equation (IV.21) ensures that the probability for obtaining the result (u,v) if the state is given by (u',v') is nonzero only for the correct result. This implies that

$$\hat{E}(u,v,w_0) \propto |\tilde{\psi}^{(\lambda)}(u,v)\rangle\langle\tilde{\psi}^{(\lambda)}(u,v)| \; , \qquad \text{(IV.23)}$$

with

$$\langle \tilde{\psi}^{(\lambda)}(u,v) | \psi^{(\lambda)}(u',v') \rangle = \delta(u-u')\, \delta(v-v') \; . \qquad \text{(IV.24)}$$

It seems that this last condition can only be fulfilled for $\lambda \to 1$ when $|\tilde{\psi}^{(\lambda)}(u,v)\rangle = |\psi^{(\lambda)}(u,v)\rangle = |\Psi(u,v)\rangle$ and the POVM reduces to the von Neumann projection on the maximally entangled basis (however, we have not proven this statement).

d Teleportation protocol in Wigner representation

The original proposal for the quantum teleportation of continuous variables with a finite degree of entanglement based on two-mode squeezed states ($r = r_1 = r_2$) used the Wigner distribution and its convolution formalism [37]. With the EPR-state Wigner function from Eq. (III.28) $W^{(\lambda)}(x_1,p_1,x_2,p_2) = W^{(\lambda)}(\alpha_1,\alpha_2)$, the whole system after combining mode "in" [which is in an unknown arbitrary quantum state described by $W_{\rm in}(x_{\rm in},p_{\rm in})$] with mode 1 at a phase-free 50:50 beam splitter (having the two outgoing modes $\alpha_{\rm u} = x_{\rm u} + ip_{\rm u}$ and $\alpha_{\rm v} = x_{\rm v} + ip_{\rm v}$) can be written according to the beam splitter transformation rule in Eq. (III.40) as

$$\begin{aligned} W(\alpha_{\rm u},\alpha_{\rm v},\alpha_2) &= \int dx_{\rm in}dp_{\rm in}W_{\rm in}(x_{\rm in},p_{\rm in})\, W^{(\lambda)}\left[\alpha_1 = \frac{1}{\sqrt{2}}(\alpha_{\rm v}-\alpha_{\rm u}),\alpha_2\right] \\ &\quad \times \delta\left[\frac{1}{\sqrt{2}}(x_{\rm u}+x_{\rm v}) - x_{\rm in}\right]\,\delta\left[\frac{1}{\sqrt{2}}(p_{\rm u}+p_{\rm v}) - p_{\rm in}\right]. \end{aligned} \quad \text{(IV.25)}$$

Alice's Bell detection on the maximally entangled basis, i.e., homodyne detections of $x_{\rm u} = (x_{\rm in} - x_1)/\sqrt{2}$ and $p_{\rm v} = (p_{\rm in} + p_1)/\sqrt{2}$, is described by the unnormalized reduced Wigner function after integrating over $x_{\rm v}$ and $p_{\rm u}$:

$$\begin{aligned} \int dx_{\rm v}\, dp_{\rm u}\, W(\alpha_{\rm u},\alpha_{\rm v},\alpha_2) &= \int dx\, dp\, W_{\rm in}(x,p) \\ &\quad \times W^{(\lambda)}\left[x - \sqrt{2}x_{\rm u} + i(\sqrt{2}p_{\rm v} - p),\alpha_2\right]. \end{aligned} \quad \text{(IV.26)}$$

Bob's displacements are now incorporated by the substitution $\alpha_2 = x_2' - \sqrt{2}x_{\rm u} + i(p_2' - \sqrt{2}p_{\rm v})$ in $W^{(\lambda)}$ in Eq. (IV.26). Finally, integration over $x_{\rm u}$ and $p_{\rm v}$ yields the teleported ensemble state (for an ensemble of input states),

$$\begin{aligned} W_{\rm tel}(\alpha_2') &= \frac{1}{\pi\, e^{-2r}} \int d^2\alpha\, W_{\rm in}(\alpha)\, \exp\left(-\frac{|\alpha_2' - \alpha|^2}{e^{-2r}}\right) \\ &\equiv W_{\rm in} \circ G_\sigma\,. \end{aligned} \quad \text{(IV.27)}$$

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.

e Teleportation criteria

The teleportation scheme with Alice and Bob is complete without any further measurement. The quantum state teleported remains unknown to both Alice and Bob (in particular for infinite squeezing there is no information gain at all through Alice's measurement) 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 the 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. IV.2). 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 teleported state back to Victor. Victor's knowledge about the input state and detection of the teleported state enable Victor to verify if quantum teleportation has really occurred. For that 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. In this section, we will discuss such measures in a less rigorous and more intuitive way. The set of input states (or alphabet) shall contain Gaussian states with a coherent amplitude. Any coherent amplitude is allowed, so that for instance a set of coherent states $\{|\alpha\rangle\}$ is unbounded.

The single-mode teleportation scheme of Ref. [37] works for arbitrary input

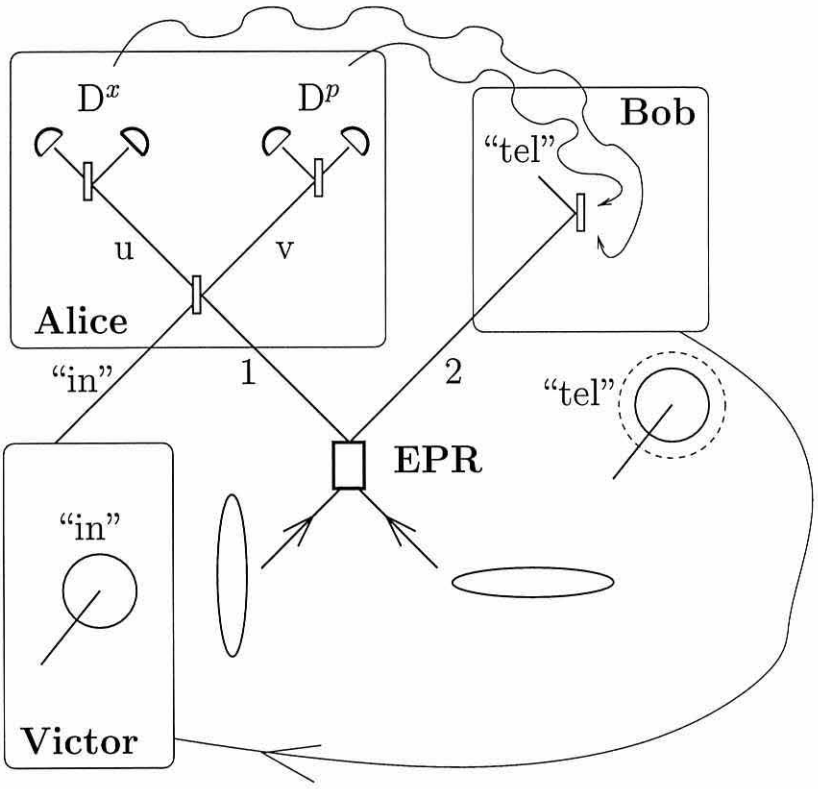

Figure IV.2: Verification of quantum teleportation. The verifier "Victor" is independent of Alice and Bob. Victor prepares the input states which are known to him, but unknown to Alice and Bob. After a supposed quantum teleportation from Alice to Bob, the teleported states are given back to Victor. Due to his knowledge of the input states, Victor can compare the teleported states with the input states.

states, described by any Wigner function W_{in}. 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, the coherent amplitudes of the teleported mode always match those of the input mode when Victor draws states with different amplitudes from the input alphabet in a sequence of trials. 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}. Classical teleportation with $r = 0$ then means the teleported mode has an excess noise of two units of

vacuum $1/2+1/2$ compared 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, we may call it quantum teleportation.

Let us derive this criterion using the least noisy model for classical communication. For the input quadratures of Alice's sending station and the output quadratures at Bob's receiving station, the least noisy (linear) "classical" model can be written as

$$\begin{aligned} \hat{x}_{\text{out},j} &= g_x\,\hat{x}_{\text{in}} + g_x\,s_a^{-1}\hat{x}_a^{(0)} + s_{b,j}^{-1}\hat{x}_{b,j}^{(0)}, \\ \hat{p}_{\text{out},j} &= g_p\,\hat{p}_{\text{in}} - g_p\,s_a\hat{p}_a^{(0)} + s_{b,j}\hat{p}_{b,j}^{(0)}. \end{aligned} \tag{IV.28}$$

This model takes into account that Alice and Bob can only communicate via classical signals, since arbitrarily many copies of the output mode can be made by Bob where the subscript j labels the jth copy. In addition, it ensures that the output quadratures satisfy the commutation relations:

$$\begin{aligned} [\hat{x}_{\text{out},j}, \hat{p}_{\text{out},k}] &= \frac{i}{2}\,\delta_{jk}, \\ [\hat{x}_{\text{out},j}, \hat{x}_{\text{out},k}] &= [\hat{p}_{\text{out},j}, \hat{p}_{\text{out},k}] = 0\ . \end{aligned} \tag{IV.29}$$

Since we are only interested in a single copy of the output we drop the label j. The parameter s_a is given by Alice's measurement strategy and determines the noise penalty due to her homodyne detections. The gains g_x and g_p can be manipulated by Bob in addition to the parameter s_b determining the noise distribution of Bob's original mode. The set of input states may contain pure Gaussian states with a coherent amplitude, described by $\hat{x}_{\text{in}} = \langle\hat{x}_{\text{in}}\rangle + s_v^{-1}\hat{x}^{(0)}$ and $\hat{p}_{\text{in}} = \langle\hat{p}_{\text{in}}\rangle + s_v\hat{p}^{(0)}$. Victor can choose in each trial the coherent amplitude and whether and to what extent the input is squeezed (parameter s_v). Bob is restricted to unit gain, symmetric in both quadratures, $g_x = g_p = 1$, because he always wants to reproduce the input amplitude. After obtaining the output states from Bob, Victor might first verify whether their amplitudes match the corresponding input amplitudes. If not, all the following considerations concerning the excess noise are

redundant, because Alice and Bob can always manipulate this noise by fiddling the gain (less than unit gain reduces the excess noise). If Victor finds overlapping amplitudes in all trials (at least within some small fixed error range), he looks at the excess noise in each trial. For that purpose, let us define the normalized variance

$$V^{\hat{x}}_{\mathrm{out,in}} \equiv \frac{\langle[\Delta(\hat{x}_{\mathrm{out}} - \hat{x}_{\mathrm{in}})]^2\rangle}{\langle(\Delta\hat{x})^2\rangle_{\mathrm{vacuum}}} , \tag{IV.30}$$

and analogously $V^{\hat{p}}_{\mathrm{out,in}}$ with $\hat{x} \to \hat{p}$ throughout. Using Eq. (IV.28) with unit gain, we obtain the noise product

$$V^{\hat{x}}_{\mathrm{out,in}} V^{\hat{p}}_{\mathrm{out,in}} = (s_a^{-2} + s_b^{-2})(s_a^2 + s_b^2). \tag{IV.31}$$

It is minimized for $s_a = s_b$, yielding $V^{\hat{x}}_{\mathrm{out,in}} V^{\hat{p}}_{\mathrm{out,in}} = 4$. The optimum value of 4 is exactly the result we obtain for what we may call classical teleportation, $V^{\hat{x}}_{\mathrm{tel,in}}(r=0) V^{\hat{p}}_{\mathrm{tel,in}}(r=0) = 4$, using Eq. (IV.4) with $r = r_1 = r_2$ and subscript 'out' $\to$ 'tel' in Eq. (IV.30). Thus, we can write our first "fundamental" limit for teleporting states with a coherent amplitude as

$$V^{\hat{x}}_{\mathrm{out,in}} V^{\hat{p}}_{\mathrm{out,in}} \geq V^{\hat{x}}_{\mathrm{tel,in}}(r=0) V^{\hat{p}}_{\mathrm{tel,in}}(r=0) = 4 \ . \tag{IV.32}$$

If on comparing the output states with the input states Victor always finds violations of this inequality, he may already have confidence in Alice's and Bob's honesty (i.e., that they have indeed used entanglement). Equation (IV.32) enables us to assess whether a scheme or protocol is capable of quantum teleportation. Alternatively, instead of looking at the products $V^{\hat{x}}_{\mathrm{out,in}} V^{\hat{p}}_{\mathrm{out,in}}$, we could consider the sums $V^{\hat{x}}_{\mathrm{out,in}} + V^{\hat{p}}_{\mathrm{out,in}} = s_a^{-2} + s_b^{-2} + s_a^2 + s_b^2$ that are minimized for $s_a = s_b = 1$. Then we find the classical boundary $V^{\hat{x}}_{\mathrm{out,in}} + V^{\hat{p}}_{\mathrm{out,in}} \geq 4$.

However, taking into account all the assumptions made for the derivation of Eq. (IV.32), this boundary appears to be less fundamental. First, we have only assumed a linear model. Secondly, we have only considered the variances of two conjugate observables and a specific kind of measurement of these. A rigorous

criterion for quantum teleportation should take into account all possible variables, measurements and strategies that can be used by Alice and Bob. Another "problem" with the boundary of Eq. (IV.32) is that the variances $V_{\mathrm{out,in}}$ are not directly measurable, because the input state is destroyed by the teleportation process. Nonetheless, for Gaussian input states, Victor can combine his knowledge of the input variances V_{in} with the detected variances V_{out} in order to infer $V_{\mathrm{out,in}}$. With a more specific set of Gaussian input states, namely coherent states, the least noisy model for classical communication allows us to determine the directly measurable "fundamental" limit for the normalized variances of the output states

$$V_{\mathrm{out}}^{\hat{x}} V_{\mathrm{out}}^{\hat{p}} \geq 9 \ . \tag{IV.33}$$

We must recall, however, that we did not consider all possible strategies of Alice and Bob. Also for arbitrary s_v (where the input alphabet contains all coherent and squeezed states), Eq. (IV.33) represents a classical boundary, as

$$V_{\mathrm{out}}^{\hat{x}} V_{\mathrm{out}}^{\hat{p}} \ = \ (s_v^{-2} + s_a^{-2} + s_b^{-2})(s_v^2 + s_a^2 + s_b^2) \tag{IV.34}$$

is minimized for $s_v = s_a = s_b$, yielding $V_{\mathrm{out}}^{\hat{x}} V_{\mathrm{out}}^{\hat{p}} = 9$. However, since s_v is unknown to Alice and Bob in every trial, they can attain this classical minimum only by accident. For s_v fixed, e.g., $s_v = 1$ (where the input alphabet contains "only" coherent states), Alice and Bob knowing this s_v can always satisfy $V_{\mathrm{out}}^{\hat{x}} V_{\mathrm{out}}^{\hat{p}} = 9$ in the classical model. Alternatively, the sums $V_{\mathrm{out}}^{\hat{x}} + V_{\mathrm{out}}^{\hat{p}} = s_v^{-2} + s_a^{-2} + s_b^{-2} + s_v^2 + s_a^2 + s_b^2$ are minimized with $s_a = s_b = 1$. In this case, we obtain the s_v-dependent boundary $V_{\mathrm{out}}^{\hat{x}} + V_{\mathrm{out}}^{\hat{p}} \geq s_v^{-2} + s_v^2 + 4$. Without knowing s_v, Alice and Bob can always attain this minimum in the classical model. In every trial, Victor must combine his knowledge of s_v with the detected output variances in order to find violations of this sum inequality.

Using a similar formalism, different criteria were proposed by Ralph and Lam [169]. They define the classical boundaries

$$V_{\mathrm{c}}^{\hat{x}} + V_{\mathrm{c}}^{\hat{p}} \geq 2 \, , \tag{IV.35}$$

and

$$T_{\text{out}}^{\hat{x}} + T_{\text{out}}^{\hat{p}} \leq 1 \,, \tag{IV.36}$$

in terms of the conditional variance

$$V_{\text{c}}^{\hat{x}} \equiv \frac{\langle(\Delta\hat{x}_{\text{out}})^2\rangle}{\langle(\Delta\hat{x})^2\rangle_{\text{vacuum}}}\left(1 - \frac{|\langle\Delta\hat{x}_{\text{out}}\Delta\hat{x}_{\text{in}}\rangle|^2}{\langle(\Delta\hat{x}_{\text{out}})^2\rangle\langle(\Delta\hat{x}_{\text{in}})^2\rangle}\right) , \tag{IV.37}$$

and similarly for $V_{\text{c}}^{\hat{p}}$ with $\hat{x} \to \hat{p}$ throughout, and the transfer coefficient

$$T_{\text{out}}^{\hat{x}} \equiv \frac{\text{SNR}_{\text{out}}^{\hat{x}}}{\text{SNR}_{\text{in}}^{\hat{x}}} , \tag{IV.38}$$

and similarly for $T_{\text{out}}^{\hat{p}}$ with $\hat{x} \to \hat{p}$ throughout. Here, SNR denotes the signal to noise ratio for the square of the mean amplitudes [$\text{SNR}_{\text{out}}^{\hat{x}} = \langle\hat{x}_{\text{out}}\rangle^2/\langle(\Delta\hat{x}_{\text{out}})^2\rangle$].

If Alice and Bob are restricted to using only classical communication, they would not be able to violate *either* of the two inequalities Eq. (IV.35) and Eq. (IV.36). In fact, *these boundaries are two independent limits*, each of them unexceedable in a classical scheme. However, Alice and Bob can simultaneously approach $V_{\text{c}}^{\hat{x}} + V_{\text{c}}^{\hat{p}} = 2$ and $T_{\text{out}}^{\hat{x}} + T_{\text{out}}^{\hat{p}} = 1$ using either an asymmetric classical detection and transmission scheme with coherent-state inputs or a symmetric classical scheme with squeezed-state inputs [169]. For quantum teleportation, Ralph and Lam [169] require their classical limits be simultaneously exceeded, $V_{\text{c}}^{\hat{x}} + V_{\text{c}}^{\hat{p}} < 2$ and $T_{\text{out}}^{\hat{x}} + T_{\text{out}}^{\hat{p}} > 1$. This is only possible for more than 3 dB squeezing in the entanglement source (the two-mode squeezed state) [169]. Apparently, these criteria determine a classical boundary different from that of Eq. (IV.32). For example, in unit-gain teleportation, inequality Eq. (IV.32) is violated for any nonzero squeezing $r > 0$ of the two-mode squeezed state.

Let us briefly explain why we encounter this discrepancy. We have a priori assumed unit gain in "our" scheme to achieve outputs and inputs overlapping in their mean values. This assumption is, of course, motivated by the assessment that good teleportation means good similarity between input and output *states* (here we have already something in mind like the fidelity which will be used

in the next section). First, Victor has to check the match of the amplitudes before looking at the variances. Ralph and Lam permit arbitrary gain, because they are not interested in the similarity of input and output *states*, but instead in certain correlations that manifest separately in the individual quadratures [170]. This point of view originates from the context of quantum non-demolition (QND) measurements [54, 108], which are focused on a single QND variable while the conjugate variable is not of interest. For arbitrary gain, an inequality like Eq. (IV.36), containing the input and output mean values, has to be added to an inequality only for variances like Eq. (IV.35). Ralph and Lam's *best* classical protocol permits output states completely different from the input states, e.g., via asymmetric detection where the lack of information in one quadrature leads on average to output states with amplitudes completely different from the input states. The asymmetric scheme means that Alice is *not* attempting to gain as much information about the *quantum state* as possible, as in an Arthurs-Kelly measurement.

The Arthurs-Kelly measurement, however, is exactly what Alice should do in "our" *best* classical protocol, i.e., classical teleportation. Therefore, "our" best classical protocol always achieves output states already pretty similar to the input states. Apparently, "the best" that can be classically achieved has a different meaning from Ralph and Lam's point of view and from the point of view that we advertise here. Then it is no surprise that the classical boundaries differ as well. Let us now study a more rigorous criterion for quantum teleportation.

f The fidelity criterion for coherent-state teleportation

The rigorous criterion we are looking for to determine the best classical teleportation and to quantify the distinction between classical and quantum teleportation relies on the fidelity F, for an arbitrary input state $|\psi_{\text{in}}\rangle$ defined by [35]

$$F \equiv \langle\psi_{\text{in}}|\hat{\rho}_{\text{out}}|\psi_{\text{in}}\rangle. \tag{IV.39}$$

It is an excellent measure for the similarity between the input and the output state and equals one only if $\hat{\rho}_{\text{out}} = |\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|$. Now Alice and Bob know that Victor draws his states $|\psi_{\text{in}}\rangle$ 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 [35],

$$F_{\text{av}} = \int P(|\psi_{\text{in}}\rangle)\langle\psi_{\text{in}}|\hat{\rho}_{\text{out}}|\psi_{\text{in}}\rangle d|\psi_{\text{in}}\rangle, \tag{IV.40}$$

where $P(|\psi_{\text{in}}\rangle)$ is the probability of drawing a particular state $|\psi_{\text{in}}\rangle$, 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_{av} achievable by Alice and Bob without using entanglement is zero [2]. If the input alphabet is restricted to coherent states of amplitude $\alpha_{\text{in}} = x_{\text{in}} + ip_{\text{in}}$ and $F = \langle\alpha_{\text{in}}|\hat{\rho}_{\text{out}}|\alpha_{\text{in}}\rangle$, 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 [35]

$$F_{\text{av}} \leq \frac{1}{2} \ . \tag{IV.41}$$

Let us outline the derivation of this important boundary as given in Ref. [35], starting with an alphabet of coherent states $|\beta\rangle$ distributed according to a Gaussian distribution

$$p(\beta) = \frac{\lambda}{\pi}\exp(-\lambda|\beta|^2) \ . \tag{IV.42}$$

Taking the limit $\lambda \to 0$ means that the coherent states are uniformly distributed over the entire complex plane and are hence all equally likely to be drawn by Victor. The particular mean value $\langle\beta\rangle = 0$ of the Gaussian distribution $p(\beta)$ can

[2] The corresponding best average fidelity if the set of input states contains all possible quantum states in a d-dimensional Hilbert space is $F_{\text{av}} = 2/(1+d)$ [9]. Thus, one obtains $F_{\text{av}} = 0$ for $d \to \infty$, and also the qubit boundary $F_{\text{av}} = 2/3$ for $d = 2$ (see chapter II).

be chosen without loss of generality. As explained in chapter II, equivalent to the optimal measurement for estimating the unknown amplitude β, namely an Arthurs-Kelly measurement, is the POVM given by the coherent-state projectors

$$\hat{E}_\alpha = \frac{1}{\pi}|\alpha\rangle\langle\alpha| \,, \tag{IV.43}$$

where α labels the measurement result and $\int d^2\alpha\, \hat{E}_\alpha = \mathbb{1}$. Based on Alice's particular result, occurring for a given input amplitude β with probability

$$p(\alpha|\beta)\, d^2\alpha = \langle\beta|\hat{E}_\alpha|\beta\rangle\, d^2\alpha = \frac{1}{\pi}\,|\langle\alpha|\beta\rangle|^2\, d^2\alpha \,, \tag{IV.44}$$

Bob generates a state $|f_\alpha\rangle$. The average fidelity then becomes

$$\begin{aligned} F_{\rm av}(\lambda) &= \int p(\beta) \left(\int \frac{1}{\pi}\,|\langle\alpha|\beta\rangle|^2\,|\langle f_\alpha|\beta\rangle|^2\, d^2\alpha \right) d^2\beta \\ &= \frac{\lambda}{\pi^2} \int d^2\alpha\, d^2\beta\, \exp(-\lambda|\beta|^2)\, \exp(-|\alpha-\beta|^2)\,|\langle f_\alpha|\beta\rangle|^2 \\ &= \frac{\lambda}{\pi^2} \int d^2\alpha\, \exp(-|\alpha|^2) \\ &\quad \times\langle f_\alpha| \left\{ \int d^2\beta\, \exp[-(1+\lambda)|\beta|^2 + 2{\rm Re}\,\alpha^*\beta]\, |\beta\rangle\langle\beta| \right\} |f_\alpha\rangle \,. \end{aligned} \tag{IV.45}$$

The expression in brackets in the last line of Eq. (IV.45) is a positive semi-definite Hermitian operator $\hat{\mathcal{O}}_\alpha$ depending on λ and α. The whole expression in the last line is therefore bounded from above by the largest eigenvalue of $\hat{\mathcal{O}}_\alpha$. Since the positive operator

$$\hat{O} = \int d^2\beta\, \exp[-(1+\lambda)|\beta|^2]\, |\beta\rangle\langle\beta| = \pi \sum_{n=0}^{\infty} (2+\lambda)^{-(n+1)}\, |n\rangle\langle n| \tag{IV.46}$$

has the largest eigenvalue $\pi/(2+\lambda)$ and since

$$\hat{D}\left(\frac{\alpha}{1+\lambda}\right) \hat{O}\, \hat{D}^\dagger\left(\frac{\alpha}{1+\lambda}\right) = \exp\left(\frac{-|\alpha|^2}{1+\lambda}\right) \hat{\mathcal{O}}_\alpha \,, \tag{IV.47}$$

where $\hat{D}(\alpha)$ is the displacement operator, we find for the average fidelity

$$\begin{aligned} F_{\mathrm{av}}(\lambda) &= \frac{\lambda}{\pi^2}\int d^2\alpha \exp\left[-\left(1-\frac{1}{1+\lambda}\right)|\alpha|^2\right] \\ &\quad \times\langle f_\alpha|\left[\hat{D}\left(\frac{\alpha}{1+\lambda}\right)\hat{O}\hat{D}^\dagger\left(\frac{\alpha}{1+\lambda}\right)\right]|f_\alpha\rangle \\ &\leq \frac{\lambda}{\pi(2+\lambda)}\int d^2\alpha \exp\left(-\frac{\lambda}{1+\lambda}|\alpha|^2\right) \\ &= \frac{1+\lambda}{2+\lambda}\,. \end{aligned} \tag{IV.48}$$

Thus, we have derived the maximum average fidelity and the boundary of $(1+\lambda)/(2+\lambda)$ is attained with

$$|f_\alpha\rangle = \hat{D}\left(\frac{\alpha}{1+\lambda}\right)|0\rangle = \left|\frac{\alpha}{1+\lambda}\right\rangle\,. \tag{IV.49}$$

Bob's optimum strategy after receiving Alice's result α is therefore to create a vacuum state displaced by $g\alpha$ with "gain" $g = 1/(1+\lambda)$. Clearly, unit gain turns out to be optimal for $\lambda \to 0$ achieving the maximum average fidelity of $1/2$ in "classical teleportation" [3].

Let us illustrate these results with our single-mode teleportation equations and for simplicity assume an alphabet containing all coherent states with equal probability ($\lambda \to 0$). Up to a factor π, the fidelity $F = \langle\alpha_{\mathrm{in}}|\hat{\rho}_{\mathrm{tel}}|\alpha_{\mathrm{in}}\rangle$ is the Q function of the teleported mode evaluated for α_{in} [and that Q function is a

[3] In this case, the whole derivation of the fidelity boundary here is analogous to the derivation for qubits in chapter II. There, we assumed a fixed but arbitrary input qubit state $|\psi_{\theta_0,\phi_0}\rangle$, corresponding here to an unrestricted alphabet of coherent states. In the qubit case, Bob generates the state $|\psi_{\theta,\phi}\rangle$ depending on the result of the POVM $\hat{E}_{\theta,\phi} = 2\pi|\psi_{\theta,\phi}\rangle\langle\psi_{\theta,\phi}|$. Here, in the case of *arbitrary* coherent states, Bob generates the state $|f_\alpha\rangle = |\alpha\rangle$ depending on the result of the POVM $\hat{E}_\alpha = \frac{1}{\pi}|\alpha\rangle\langle\alpha|$. The state transfer via classical teleportation then results for any input state in output states with the input state's orientation and always the same shrinking factor of the Bloch vector (qubits), or with the input state's mean value and always the same excess noise in phase space (coherent states). Thus, the optimal fidelities are in both cases independent of the particular input state $|\psi_{\theta_0,\phi_0}\rangle$ or $|\beta\rangle$, so that $F = F_{\mathrm{av}} = 2/3$ for qubits and $F = F_{\mathrm{av}} = 1/2$ for coherent states.

bivariate Gaussian with mean value $g(x_{\rm in}+ip_{\rm in})$]:

$$F=\pi Q_{\rm tel}(\alpha_{\rm in})=\frac{1}{2\sqrt{\sigma_x\sigma_p}}\exp\left[-(1-g)^2\left(\frac{x_{\rm in}^2}{2\sigma_x}+\frac{p_{\rm in}^2}{2\sigma_p}\right)\right], \qquad \text{(IV.50)}$$

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. These variances are according to Eq. (IV.5) for a coherent-state input and $\langle(\Delta\hat{x})^2\rangle_{\rm vacuum}=\langle(\Delta\hat{p})^2\rangle_{\rm vacuum}=1/4$ given by (recall that the Q function is a convolution of the Wigner function with a Gaussian of one unit of vacuum, i.e., we have to add that unit to the actual variances of the teleported quadratures)

$$\begin{aligned}\sigma_x &= \frac{1}{4}(1+g^2)+\frac{e^{+2r_1}}{8}(g-1)^2+\frac{e^{-2r_2}}{8}(g+1)^2\,,\\ \sigma_p &= \frac{1}{4}(1+g^2)+\frac{e^{+2r_2}}{8}(g-1)^2+\frac{e^{-2r_1}}{8}(g+1)^2\,. \qquad \text{(IV.51)}\end{aligned}$$

Let us assume $r=r_1=r_2$. For classical teleportation ($r=0$) and $g=1$, we obtain $\sigma_x=\sigma_p=1/2+(1/4)V^{\hat{x}}_{\rm tel,in}(r=0)=1/2+(1/4)V^{\hat{p}}_{\rm tel,in}(r=0)=1/2+1/2=1$ and indeed $F=F_{\rm av}=1/2$. In order to obtain a better fidelity, entanglement is necessary. Then, if $g=1$, we obtain $F=F_{\rm av}>1/2$ for any $r>0$. For $r=0$, the fidelity drops to zero as $g\to\infty$ since the mean amplitude of the teleported state does not match that of the input state and the excess noise increases. For $r=0$ and $g=0$, the fidelity becomes $F=\exp(-|\alpha_{\rm in}|^2)$. Upon averaging over all possible coherent-state inputs, this fidelity also vanishes. Assuming nonunit gain, it is crucial to consider the average fidelity $F_{\rm av}\neq F$. When averaging across the entire complex plane, any nonunit gain yields $F_{\rm av}=0$.

What about the case of different squeezing at the inputs of the beam splitter that creates the entanglement for the quantum teleportation channel, $r_1\neq r_2$? In chapter III, we have found that one squeezed state ($r_1>0$ with $r_2=0$ or $r_2>0$ with $r_1=0$) is a sufficient resource for generating entanglement between an arbitrary number of parties. Applied to the two-party teleportation scenario, we may also expect that the entanglement from only one squeezed state enables

quantum teleportation. In fact, for any $r_1 > 0$ *or* $r_2 > 0$ we obtain $F_{\rm av} = F > 1/2$ with $g = 1$. Of course, reliable teleportation with perfect fidelity $F_{\rm av} = F = 1$ (for $g = 1$) requires $r_1 \to \infty$ *and* $r_2 \to \infty$ and hence *two* single-mode squeezed states combined [4].

What is the maximum fidelity of coherent-state teleportation achievable with one single-mode squeezed state $r_1 > 0$ as entanglement source (without further local squeezers)? For infinite squeezing $r_1 \to \infty$ and $r_2 = 0$, we find $F_{\rm av} = F = 1/\sqrt{2} \approx 0.7 > 1/2$ (with $g = 1$).

In these considerations a non-classical teleportation fidelity $F_{\rm av} > 1/2$ serves as a *sufficient* criterion for the presence of entanglement. This is in perfect accordance with the violation of $\langle(\hat{x}_1 - \hat{x}_2)^2\rangle + \langle(\hat{p}_1 + \hat{p}_2)^2\rangle \geq 1$ [Eq. (III.11) with $\bar{a} = 1$] and also $\langle(\hat{x}_1 - \hat{x}_2)^2\rangle\langle(\hat{p}_1 + \hat{p}_2)^2\rangle \geq 1/4$ [Eq. (III.13)]. All these sufficient criteria including the fidelity criterion for coherent-state teleportation do not necessarily yield equivalent results when entanglement is to be witnessed [5]. For the special case of the entangled two-mode state in Eq. (III.23), they all do witness entanglement for the same squeezing parameters. As an experimental signal for the presence of entanglement all these sufficient criteria can be used. The simpler but less compelling method (compared to performing quantum teleportation) for

[4] Unless Alice and Bob have access to local squeezers and transform the shared entangled state built from one squeezed state into the "canonical" two-mode squeezed state (see chapter III). The resulting 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 two r-squeezers needed to produce the "canonical" two-mode squeezed state (see chapter III).

[5] An example given in chapter III was the bipartite state after tracing out one mode of an entangled tripartite continuous-variable state, for which the results of the product and the sum criteria differ.

the experimental witnessing of entanglement would then be the detection of the variances $\langle(\hat{x}_1 - \hat{x}_2)^2\rangle$ and $\langle(\hat{p}_1 + \hat{p}_2)^2\rangle$ after combining the two relevant modes at a beam splitter [196].

Let us also mention that for an alphabet distributed with arbitrary λ, the λ-dependent optimum gain $g = 1/(1+\lambda)$ and the maximum average fidelity $F_{\rm av} = (1+\lambda)/(2+\lambda)$ achievable without entanglement can also be derived by averaging over the fidelity from Eq. (IV.50) with Eq. (IV.51) and $r = r_1 = r_2 = 0$ [36]. In the same way, but assuming the presence of entanglement in the limit of infinite squeezing $r \to \infty$, one finds that the optimum gain and the optimum average fidelity become λ-independent, $g \to 1$ and $F_{\rm av} \to F$ [36].

Finally, we note that Grangier and Grosshans [99, 100, 102] advertise a fidelity of $F > 2/3$ as *necessary* for quantum teleportation of arbitrary coherent states (without explicit reference to an alphabet), in disagreement with the sufficient condition for quantum teleportation of arbitrary coherent states $F_{\rm av} > 1/2$. The reasoning in Ref. [102] is that only when Bob receives an $F > 2/3$ state 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 with $F > 2/3$ would exist which contradicts the no-cloning boundary for coherent-state duplication (see next chapter). On the other hand, when Bob receives for example a $1/2 < F < 2/3$ state, Alice might have locally made two asymmetric copies, one with $F > 2/3$ and one with $1/2 < F < 2/3$. She might have sent the worse copy to Bob via a perfectly entangled (or sufficiently entangled) EPR channel and kept the better copy. Although this may be relevant for security in quantum cryptography, it disagrees with the common interpretation of quantum teleportation for discrete-variable systems. According to Grangier and Grosshans, the "quantum faxing" region [102] $1/2 < F \leq 2/3$ does not indicate "true" quantum teleportation of coherent states. Similarly, one would have to give the region $2/3 < F \leq 5/6$ (the qubit duplication limit, see next chapter) an

analogous status of only "quantum faxing" when teleportation of arbitrary qubits is considered. We have presented the derivation of both the qubit (chapter II) and the coherent-state boundary, $F_{\mathrm{av}} = 2/3$ and $F_{\mathrm{av}} = 1/2$ respectively, in order to demonstrate the analogy of the derivation itself and hence of the result. A detailed discussion about the different coherent-state teleportation fidelity "boundaries" can be found in Ref. [36].

g Unconditional teleportation of entanglement

In the three optical teleportation experiments so far, in Innsbruck [23], in Rome [20], and in Pasadena [87], the nonorthogonal input states to be teleported were single-photon polarization states (qubits) [23, 20] and coherent states [87]. 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 [212]. In general, it means to entangle 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.* [157]. Practical uses of entanglement swapping have been suggested [22, 21, 42, 80] and it has also been generalized to multiparticle systems [21]. All these investigations have referred exclusively to discrete-variable systems.

For continuous variables, experimental entanglement swapping has not yet been realized in the laboratory, but there have been several theoretical proposals of such an experiment. Polkinghorne and Ralph [164] suggested teleporting polarization-entangled states of single photons using squeezed-state entanglement (in the limit of small squeezing) where the output correlations are verified via Bell inequalities. Tan [196] and van Loock and Braunstein [131] considered the unconditional teleportation (without post-selection of "successful" events by photon detections) of one half of a two-mode squeezed state using different protocols and verification.

In this section, we present the entanglement swapping scheme of Ref. [131]. Particular emphasis is thereby put on two aspects: first, a possible experimental verification of the teleported entanglement is proposed, based on the exploitation of that entanglement for quantum teleportation. This operational verification underlines that the teleported entanglement emerges from the teleporter in an unconditional way, independent of any post-selection and further exploitable every inverse bandwith time [6]. That the teleported entanglement can indeed be used for quantum teleportation shall be confirmed by means of the fidelity criterion for coherent-state teleportation. Secondly, the continuous-variable teleportation scheme succeeds in teleporting entanglement for any nonzero entanglement in the two initial entangled states (of which one provides the teleporter's input and the other one the EPR channel or vice versa). This means that in principle entanglement swapping and its verification can be performed with a resource of only two single-mode squeezed states. Each of these two squeezed states must then be used to generate an entangled state, as described in chapter III. This is in agreement with the previous result that the entanglement built from only one squeezed state suffices to enable quantum teleportation of coherent states.

The two entangled states of the electromagnetic field that we need for continuous-variable entanglement swapping, a two-mode state of modes 1 and 2 and a two-mode state of modes 3 and 4, can be written in the Heisenberg representation as

$$\hat{x}_1 = (e^{+r_1}\hat{x}_1^{(0)} + e^{-r_2}\hat{x}_2^{(0)})/\sqrt{2}, \quad \hat{p}_1 = (e^{-r_1}\hat{p}_1^{(0)} + e^{+r_2}\hat{p}_2^{(0)})/\sqrt{2}, \tag{IV.52}$$

$$\hat{x}_2 = (e^{+r_1}\hat{x}_1^{(0)} - e^{-r_2}\hat{x}_2^{(0)})/\sqrt{2}, \quad \hat{p}_2 = (e^{-r_1}\hat{p}_1^{(0)} - e^{+r_2}\hat{p}_2^{(0)})/\sqrt{2}, \tag{IV.53}$$

$$\hat{x}_3 = (e^{+s_1}\hat{x}_3^{(0)} + e^{-s_2}\hat{x}_4^{(0)})/\sqrt{2}, \quad \hat{p}_3 = (e^{-s_1}\hat{p}_3^{(0)} + e^{+s_2}\hat{p}_4^{(0)})/\sqrt{2}, \tag{IV.54}$$

$$\hat{x}_4 = (e^{+s_1}\hat{x}_3^{(0)} - e^{-s_2}\hat{x}_4^{(0)})/\sqrt{2}, \quad \hat{p}_4 = (e^{-s_1}\hat{p}_3^{(0)} - e^{+s_2}\hat{p}_4^{(0)})/\sqrt{2}. \tag{IV.55}$$

[6] In this section, we will focus on the entanglement swapping protocol in a single-mode description. Later, we will also take finite bandwidths into account.

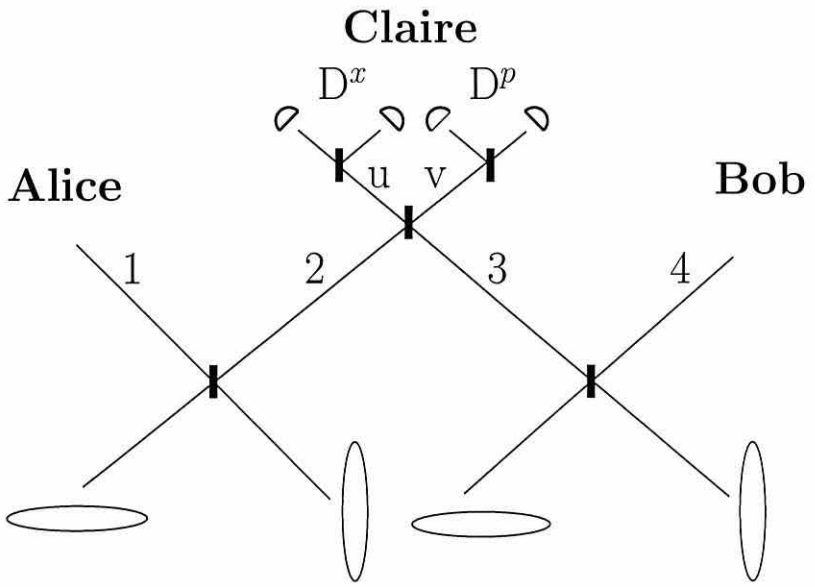

Figure IV.3: Entanglement swapping using four squeezed vacuum states. Before the detections, mode 1 is entangled with mode 2 and mode 3 is entangled with mode 4.

How these two entangled states are generated is sketched in Fig. IV.3. For each entangled state, we combine two squeezed modes at a beam splitter. The four squeezed input states might all have different squeezing, denoted by four different squeezing parameters r_1, r_2, s_1, and s_2.

Let us now introduce "Alice", "Bob", and "Claire" to illustrate the whole protocol with entanglement swapping and subsequent teleportation of a coherent state. Alice and Claire shall share the entangled state of modes 1 and 2 while Claire and Bob share the other entangled state of modes 3 and 4 (Fig. IV.3). *Thus, initially Alice and Bob do not share an entangled state.* Now Alice wants to teleport an unknown coherent state to Bob and asks Claire for her assistance. Claire combines mode 2 and mode 3 at a beam splitter and detects the quadra-

tures $\hat{x}_{\rm u} = (\hat{x}_2 - \hat{x}_3)/\sqrt{2}$, $\hat{p}_{\rm v} = (\hat{p}_2 + \hat{p}_3)/\sqrt{2}$. Let us write Bob's mode 4 as

$$\begin{aligned} \hat{x}_4 &= \hat{x}_2 - (\hat{x}_3 - \hat{x}_4) - \sqrt{2}\hat{x}_{\rm u}, \\ \hat{p}_4 &= \hat{p}_2 + (\hat{p}_3 + \hat{p}_4) - \sqrt{2}\hat{p}_{\rm v}, \end{aligned} \tag{IV.56}$$

and Alice's mode 1 as

$$\begin{aligned} \hat{x}_1 &= \hat{x}_3 + (\hat{x}_1 - \hat{x}_2) + \sqrt{2}\hat{x}_{\rm u}, \\ \hat{p}_1 &= \hat{p}_3 + (\hat{p}_1 + \hat{p}_2) - \sqrt{2}\hat{p}_{\rm v}. \end{aligned} \tag{IV.57}$$

Claire's detection yields classical results $x_{\rm u}$ and $p_{\rm v}$ and the state of Bob's mode 4 in Eq. (IV.56) and Alice's mode 1 in Eq. (IV.57) collapses correspondingly:

$$\begin{aligned} \hat{x}_4 &= \hat{x}_2 - \sqrt{2}e^{-s_2}\hat{x}_4^{(0)} - \sqrt{2}x_{\rm u}, \\ \hat{p}_4 &= \hat{p}_2 + \sqrt{2}e^{-s_1}\hat{p}_3^{(0)} - \sqrt{2}p_{\rm v}, \\ \hat{x}_1 &= \hat{x}_3 + \sqrt{2}e^{-r_2}\hat{x}_2^{(0)} + \sqrt{2}x_{\rm u}, \\ \hat{p}_1 &= \hat{p}_3 + \sqrt{2}e^{-r_1}\hat{p}_1^{(0)} - \sqrt{2}p_{\rm v}. \end{aligned} \tag{IV.58}$$

For $s = s_1 = s_2 \to \infty$, the quadrature operators of mode 4 become those of mode 2 up to a (random) classical phase-space displacement. In every single projection, mode 4 gets entangled with mode 1 as mode 2 has been before. For $r = r_1 = r_2 \to \infty$, the quadrature operators of mode 1 become those of mode 3 up to a (random) classical phase-space displacement. Again, in every single projection, mode 1 gets entangled with mode 4 as mode 3 has been before. Mode 2 is perfectly teleported to mode 4 ($s \to \infty$) or mode 3 is perfectly teleported to mode 1 ($r \to \infty$) apart from local classical displacements. The entanglement of either of the initial two-mode states is completely preserved for infinite squeezing in the other two-mode state.

What about the situation with finite squeezing? When we treat the classical quantities $x_{\rm u}$ and $p_{\rm v}$ as fixed local displacements, the total variance

$$\begin{aligned} \mathcal{V}(2) &= \langle(\Delta\hat{u})^2\rangle + \langle(\Delta\hat{v})^2\rangle \\ &= e^{-2r_2}/2 + e^{-2s_2}/2 + e^{-2r_1}/2 + e^{-2s_1}/2\,, \end{aligned} \tag{IV.59}$$

with $\hat{u} = \hat{x}_1 - \hat{x}_4$ and $\hat{v} = \hat{p}_1 + \hat{p}_4$, only violates the necessary separability condition $\mathcal{V}(2) \geq 1$ [Eq. (III.11)] for more than 3 dB squeezing ($e^{-2r} < 1/2$ with equal squeezing $r = r_1 = r_2 = s_1 = s_2$). The same applies to the product condition of Eq. (III.13). However, we will see now that modes 1 and 4 are entangled for any nonzero squeezing after Claire's detection.

Clearly, Alice and Bob cannot use modes 1 and 4 for subsequent quantum teleportation without information about Claire's measurement results. Either of them, Alice or Bob, has to receive from Claire the information that the detection of modes 2 and 3 has been performed and its results. Let us assume Bob obtains the classical results of Claire's measurements. Now Bob can displace mode 4 as

$$\begin{aligned} \hat{x}_4 \longrightarrow \hat{x}_4' &= \hat{x}_4 + g_{\text{swap}}\sqrt{2}x_{\text{u}}, \\ \hat{p}_4 \longrightarrow \hat{p}_4' &= \hat{p}_4 + g_{\text{swap}}\sqrt{2}p_{\text{v}}. \end{aligned} \tag{IV.60}$$

The parameter g_{swap} represents the gain for these displacements. Bob's mode then becomes

$$\begin{aligned} \hat{x}_4' &= \frac{g_{\text{swap}}}{\sqrt{2}} e^{+r_1}\hat{x}_1^{(0)} - \frac{g_{\text{swap}}}{\sqrt{2}} e^{-r_2}\hat{x}_2^{(0)} \\ &\quad - \frac{g_{\text{swap}} - 1}{\sqrt{2}} e^{+s_1}\hat{x}_3^{(0)} - \frac{g_{\text{swap}} + 1}{\sqrt{2}} e^{-s_2}\hat{x}_4^{(0)}, \\ \hat{p}_4' &= \frac{g_{\text{swap}}}{\sqrt{2}} e^{-r_1}\hat{p}_1^{(0)} - \frac{g_{\text{swap}}}{\sqrt{2}} e^{+r_2}\hat{p}_2^{(0)} \\ &\quad + \frac{g_{\text{swap}} + 1}{\sqrt{2}} e^{-s_1}\hat{p}_3^{(0)} + \frac{g_{\text{swap}} - 1}{\sqrt{2}} e^{+s_2}\hat{p}_4^{(0)}. \end{aligned} \tag{IV.61}$$

These equations and Eq. (IV.52) describe the *ensemble state* of the outgoing modes 1 and 4′. In this description, the randomness of the classical displacements is taken into account [Eq. (IV.60) means effectively an operator displacement]. Therefore, the value of the gain g_{swap} becomes relevant.

As in "usual" teleportation, Alice now couples the unknown input state she wants to teleport to Bob (described by $\hat{x}_{\text{in}}$, $\hat{p}_{\text{in}}$) with her mode 1 at a beam splitter and measures the combinations $\hat{x}_{\text{u}}' = (\hat{x}_{\text{in}} - \hat{x}_1)/\sqrt{2}$, $\hat{p}_{\text{v}}' = (\hat{p}_{\text{in}} + \hat{p}_1)/\sqrt{2}$. Based

on the classical results sent to him from Alice, Bob displaces his "new" mode 4′, $\hat{x}'_4 \longrightarrow \hat{x}_{\rm tel} = \hat{x}'_4 + g\sqrt{2}x'_{\rm u}$, $\hat{p}'_4 \longrightarrow \hat{p}_{\rm tel} = \hat{p}'_4 + g\sqrt{2}p'_{\rm v}$, with gain g. For $g = 1$ and nonunit detector efficiencies, we find for Bob's outgoing mode

$$\begin{aligned}
\hat{x}_{\rm tel} &= \hat{x}_{\rm in} + \frac{g_{\rm swap}-1}{\sqrt{2}} e^{+r_1}\hat{x}_1^{(0)} - \frac{g_{\rm swap}+1}{\sqrt{2}} e^{-r_2}\hat{x}_2^{(0)} \\
&\quad - \frac{g_{\rm swap}-1}{\sqrt{2}} e^{+s_1}\hat{x}_3^{(0)} - \frac{g_{\rm swap}+1}{\sqrt{2}} e^{-s_2}\hat{x}_4^{(0)} \\
&\quad + g_{\rm swap}\sqrt{\eta_c^{-2}-1}\,(\hat{x}_d^{(0)} + \hat{x}_e^{(0)}) + \sqrt{\eta_a^{-2}-1}\,(\hat{x}_f^{(0)} + \hat{x}_g^{(0)}), \\
\hat{p}_{\rm tel} &= \hat{p}_{\rm in} + \frac{g_{\rm swap}+1}{\sqrt{2}} e^{-r_1}\hat{p}_1^{(0)} - \frac{g_{\rm swap}-1}{\sqrt{2}} e^{+r_2}\hat{p}_2^{(0)} \\
&\quad + \frac{g_{\rm swap}+1}{\sqrt{2}} e^{-s_1}\hat{p}_3^{(0)} + \frac{g_{\rm swap}-1}{\sqrt{2}} e^{+s_2}\hat{p}_4^{(0)} \\
&\quad + g_{\rm swap}\sqrt{\eta_c^{-2}-1}\,(\hat{p}_k^{(0)} + \hat{p}_l^{(0)}) + \sqrt{\eta_a^{-2}-1}\,(\hat{p}_m^{(0)} + \hat{p}_n^{(0)}). \qquad \text{(IV.62)}
\end{aligned}$$

The parameters η_c and η_a describe detector efficiencies in Claire's and Alice's detections, respectively. Note that for $g_{\rm swap} = 1$, Bob's teleported mode in Eq. (IV.62) is the same as if Alice teleports her input state to Claire with unit gain using the entangled state of modes 1 and 2, and Claire teleports the resulting output state to Bob with unit gain using the entangled state of modes 3 and 4.

The teleportation fidelity for a coherent-state input $|\alpha_{\rm in}\rangle$ of Eq. (IV.50), with the variances calculated from Eq. (IV.62) and with gain $g = 1$, now becomes

$$\begin{aligned}
F &= [1 + (g_{\rm swap}-1)^2(e^{+2r_1} + e^{+2s_1})/4 + (g_{\rm swap}+1)^2(e^{-2r_2} + e^{-2s_2})/4 \\
&\quad + g_{\rm swap}^2(\eta_c^{-2}-1) + \eta_a^{-2} - 1]^{-1/2} \\
&\quad \times [1 + (g_{\rm swap}-1)^2(e^{+2r_2} + e^{+2s_2})/4 + (g_{\rm swap}+1)^2(e^{-2r_1} + e^{-2s_1})/4 \\
&\quad + g_{\rm swap}^2(\eta_c^{-2}-1) + \eta_a^{-2} - 1]^{-1/2}\,. \qquad \text{(IV.63)}
\end{aligned}$$

We know that for arbitrary coherent-state inputs, an average fidelity $F_{\rm av} > 1/2$ is only achievable using entanglement. Thus, if for some $g_{\rm swap}$ (for some local displacements of mode 4 by Bob based on Claire's results) $F_{\rm av} > 1/2$, entanglement swapping must have taken place. Otherwise Alice and Bob, who initially did not share entanglement, would not be able to beat the classical fidelity limit

using modes 1 and 4. The assumption $g = 1$ is the optimal choice for Bob's local displacements based on Alice's results assuming an unbounded alphabet of coherent states.

Let us first consider four equally squeezed states $r = r_1 = r_2 = s_1 = s_2$. In this case with unit efficiency ($\eta_c = \eta_a = 1$), the fidelity is optimized for $g_{\rm swap} = \tanh 2r$ and becomes $F_{\rm opt} = (1 + 1/\cosh 2r)^{-1}$. For any $r > 0$, we obtain $F_{\rm opt} > 1/2$. For $\eta_c \neq 1$ and $\eta_a \neq 1$, the optimum gain is $g_{\rm swap} = \sinh 2r/(\cosh 2r + \eta_c^{-2} - 1)$. In the more general case $r = r_1 = r_2$ and $s = s_1 = s_2$, we find the optimum gain

$$g_{\rm swap} = \frac{\sinh 2r + \sinh 2s}{\cosh 2r + \cosh 2s + 2\eta_c^{-2} - 2} \,. \tag{IV.64}$$

Using this gain we obtain the optimum fidelity with unit efficiency

$$F_{\rm opt} = \left\{ 1 + \frac{\cosh[2(r-s)] + 1}{\cosh 2r + \cosh 2s} \right\}^{-1} \,. \tag{IV.65}$$

This fidelity is equal to $1/2$ and never exceeds the classical limit if either $r = 0$ or $s = 0$. *Both* initial two-mode states need to be squeezed and hence entangled for entanglement swapping to occur. Then, for any nonzero squeezing $r > 0$ *and* $s > 0$, we obtain $F_{\rm opt} > 1/2$ indicating that entanglement swapping took place.

Let us now consider the case where each of the two initial entangled states is generated with only one single-mode squeezed state. We set $r = r_1 = s_1$ and $r_2 = s_2 = 0$. For unit efficiency, we find the optimum gain $g_{\rm swap} = \tanh r$. The optimum fidelity then becomes

$$\begin{aligned} F_{\rm opt} \;=\; & \{[1 + 2\,e^{+2r}/(e^{+2r} + 1) + (\tanh r)^2(\eta_c^{-2} - 1) + \eta_a^{-2} - 1] \\ & \times [1 + 2\,e^{-2r}/(e^{-2r} + 1) + (\tanh r)^2(\eta_c^{-2} - 1) + \eta_a^{-2} - 1]\}^{-1/2} \,. \end{aligned} \tag{IV.66}$$

Note that this fidelity can be optimized further for nonunit efficiency, as we have only used the optimum gain for unit efficiency. With unit efficiency ($\eta_c = \eta_a = 1$) this fidelity exceeds the classical limit $F_{\rm opt} > 1/2$ for any nonzero squeezing

$r = r_1 = s_1 > 0$. Hence entanglement swapping can be realized even with only two single-mode squeezed states, provided that two initial entangled states are produced. Indeed, the creation of entanglement is possible using only one single-mode squeezed state for any nonzero squeezing, as discussed in chapter III. In order to achieve perfect teleportation of arbitrary coherent states with fidelity $F = 1$, four infinitely squeezed states $r = r_1 = r_2 = s_1 = s_2 \to \infty$ are necessary and Bob has to perform displacements with $g_{\text{swap}} = 1$ using Claire's results [7]. The optimum fidelity achievable using modes 1 and 4 after entanglement swapping is worse than the optimum fidelity using the entanglement of the initial modes 1 and 2 or 3 and 4. This indicates that the degree of entanglement deteriorates after entanglement swapping compared to the initial entangled states (we will quantify this deterioration later). Figure IV.4 shows a comparison between the optimum fidelities of coherent-state teleportation using entangled states produced from entanglement swapping and without swapping.

The maximum fidelity achievable using the entangled state produced with one squeezer is $F = 1/\sqrt{2}$. The maximum fidelity achievable using the output of entanglement swapping with two equally squeezed single-mode states is $F = 1/\sqrt{3}$. For 6 dB squeezing and detectors with efficiency $\eta^2 = 0.99$, the optimum fidelity using the output of entanglement swapping with two equally squeezed single-mode states becomes $F = 0.5201$. Squeezing of 10 dB and the same efficiency yields $F = 0.5425$. Here, the gain $g_{\text{swap}} = \tanh r$ has been chosen which is the optimum gain with two equally squeezed single-mode states for unit efficiency.

Tan proposes continuous-variable entanglement swapping as the teleportation of the signal beam of a parametric amplifier using the entanglement between signal and idler beams of another parametric amplifier [196]. The entanglement of the teleported signal beam with the idler beam in his protocol is confirmed by combining them at a beam splitter and detecting the $\hat{x}$ quadrature at one output

[7] The whole discussion here excludes the possibility of additional local squeezers.

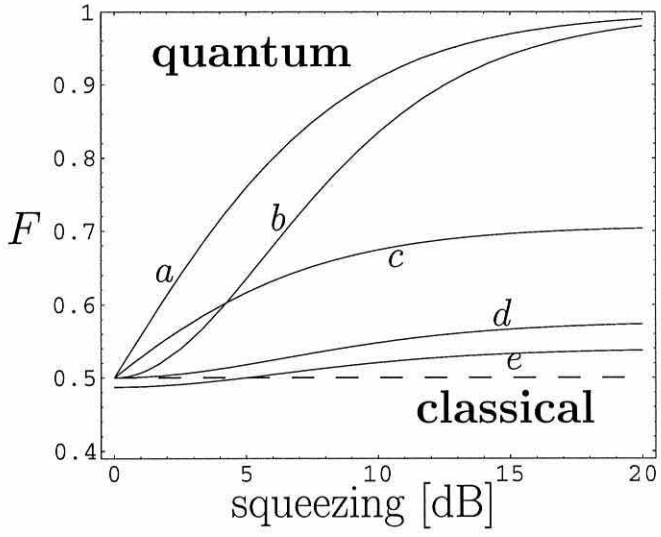

Figure IV.4: Optimum fidelity for the teleportation of an arbitrary coherent state ($g = 1$) using a) entanglement produced with two equally squeezed single-mode states, b) the output of entanglement swapping with four equally squeezed single-mode states, c) entanglement produced with one single-mode squeezed state, d) the output of entanglement swapping with two equally squeezed single-mode states, e) the state as in d) with detector efficiencies $\eta_c^2 = \eta_a^2 = 0.95$.

and the $\hat{p}$ quadrature at the other output: $\hat{x} = (\hat{x}_1 - \hat{x}_4)/\sqrt{2}, \hat{p} = (\hat{p}_1 + \hat{p}_4)/\sqrt{2}$. A violation of the product inequality $\langle \Delta\hat{x}^2 \rangle \langle \Delta\hat{p}^2 \rangle \geq 1/16$ [see Eq. (III.13)] proves the entanglement of modes 1 and 4 [196]. Similarly, one could confirm the entanglement through a violation of the sum inequality $\langle (\hat{x}_1 - \hat{x}_4)^2 \rangle + \langle (\hat{p}_1 + \hat{p}_4)^2 \rangle \geq 1$ [see Eq. (III.11)].

It is obvious that the violation of these inequalities corresponds to a fidelity $F_{\text{av}} > 1/2$ in our subsequent coherent-state teleportation. We have demonstrated that for any nonzero entanglement of modes 1 and 2 *and* of modes 3 and 4, the state of modes 1 and 4 $\hat{\rho}_{14}$ after Claire's detections can always be transformed by some local displacements to a state $\hat{\rho}'_{14}$ that provides $F_{\text{av}} > 1/2$ in coherent-state

teleportation. This state has quadratures violating $\langle(\hat{x}_1 - \hat{x}_4')^2\rangle + \langle(\hat{p}_1 + \hat{p}_4')^2\rangle \geq 1$. We have given the optimum gain $g_{\rm swap}$ for the displacements in any verification scheme, either by further teleportation or by simple detection [8].

In Tan's scheme [196], unit gain $g_{\rm swap} = 1$ was chosen. Therefore the output entanglement is only confirmed if the initial states exceed a certain degree of squeezing (e.g., for equally squeezed states 3 dB). By choosing the right gain, the entanglement can be verified for any squeezing, in principle even if the initial entangled states are built from the minimal resource of two single-mode squeezed states.

Detecting the output and applying Tan's (or Duan *et al.*'s) inequality for verification is relatively easy, but it requires bringing the entangled subsystems together and measuring states that are now local. This provides only an indirect confirmation that the entanglement is preserved through teleportation. The verification scheme proposed here leaves the subsystems separate and directly demonstrates the entanglement by exploiting it in a second round of teleportation.

Let us summarize the key points of the discussion: we have given a protocol for continuous-variable entanglement swapping, i.e., for the unconditional teleportation of entanglement, using squeezed light and linear optics. Entanglement swapping occurs for any nonzero entanglement (any nonzero squeezing) in both of the two initial entanglement sources. *This can be realized even with only two single-mode squeezed states.* The proposed verification scheme would provide a compelling demonstration of unconditional teleportation of entanglement.

[8] Polkinghorne and Ralph [164] have found a similar gain condition which ensures that the correlations of single polarization-entangled photons are verified via Bell inequalities after teleporting them.

h From discrete to continuous-variable entanglement swapping

In this section, we will explain and extend the results of Ref. [131] on the unconditional teleportation of continuous-variable entanglement, presented in the preceding section. For that purpose we consider discrete-variable entanglement swapping with certain nonmaximally entangled states of arbitrary Hilbert space dimension. We will find that the infinite-dimensional limit of entanglement swapping with such states (i.e., infinite-dimensional states in the number representation based on a countable discrete number variable and a continuous phase variable) and alternately entanglement swapping from the outset based on continuous variables (i.e., position and momentum) yield equivalent results. In terms of the ensemble description relevant to the homodyne-detection based quadrature entanglement swapping with two two-mode squeezed states, we will prove the optimality of certain gain conditions for the final displacements. This will also provide an explanation as to why certain gain values yield optimum fidelities in a subsequent quantum teleportation using entanglement from entanglement swapping.

If at least one entangled state from two resources is maximally entangled, entanglement swapping means that one half of the other arbitrarily weak entangled resource is perfectly teleported. Hence the weaker entanglement is exactly preserved in the output. More interesting are the cases in which both resources exhibit only a finite amount of entanglement, either by being mixed states or by being pure nonmaximally entangled states. The latter case has attracted particular attention for qubits, because entanglement swapping turned out to be an "entanglement concentration" procedure, i.e., a process capable of enhancing the degree of entanglement with a certain non-zero probability. The output state can be maximally entangled with some probability, but also less entangled than the initial states with some probability [22]. Using the partial von Neumann entropy as a measure, entanglement increases sometimes and decreases sometimes, but on

average decreases [22]. Using the maximum probability for converting some pure entangled state to a maximally entangled state (by local operations and classical communication) as a measure, then entanglement is, on average, conserved through entanglement swapping (for initial states equally entangled) [22]. If the two resources have different entanglement, this measure yields entanglement at the output corresponding to the smaller initial entanglement [182]. This result has been extended to entanglement swapping chains for d-level systems, where the outgoing (average) entanglement corresponds to that of the initially "weakest link" [103].

For a comparison between discrete and continuous-variable entanglement swapping, we would like to quantify the entanglement emerging from continuous-variable entanglement swapping. In general, quantifying the amount of entanglement in an arbitrary quantum state expanded in a continuous-variable basis (e.g., position basis) is difficult, since the degree of entanglement cannot be simply extracted from the Schmidt basis form of the states as for discrete variables. One possible approach to quantification is to solve particular eigenvalue equations which may require numerical approximations [159]. However, here we will find it very easy to quantify the outgoing entangled state (both in a single-shot picture and optimized in an ensemble picture), since it can be identified as a Schmidt decomposable pure two-mode squeezed state.

Universal entanglement swapping: Let us assume two initial entangled states $|\psi(\lambda)\rangle_{12}$ and $|\psi(\lambda')\rangle_{34}$ of any dimension, entangled between subsystems 1 and 2 and between 3 and 4. The projected state of 1 and 4 after a Bell measurement (a projection on the basis of maximally entangled states) of 2 and 3 can be written in the following compact (normalized) form according to the twist formalism:

$$\frac{\hat{\mathcal{D}}_4(\lambda')\hat{U}_4^\dagger(\gamma)|\psi(\lambda)\rangle_{14}}{\|\hat{\mathcal{D}}_4(\lambda')\hat{U}_4^\dagger(\gamma)|\psi(\lambda)\rangle_{14}\|} = \frac{\hat{\mathcal{D}}_1(\lambda)\hat{U}_1^\dagger(\gamma')|\psi(\lambda')\rangle_{14}}{\|\hat{\mathcal{D}}_1(\lambda)\hat{U}_1^\dagger(\gamma')|\psi(\lambda')\rangle_{14}\|} \,. \tag{IV.67}$$

In this formalism, the initial nonmaximally entangled states are in the discrete case those from Eq. (II.52) with $c_n \equiv c_n(\lambda)$, in the continuous case those from Eq. (IV.8). The maximally entangled measurement basis is in the former case given by Eq. (II.58), and in the latter case by the unnormalizable states in Eq. (IV.6).

We consider the projected state without final unitary transformation of either subsystem, e.g., a final "twist", the output of entanglement swapping. The parameters λ and λ' represent the degree of entanglement of the initial states with $\lambda \to 1$ ($\lambda \in [0,1)$) for maximum entanglement. The distortion operator $\hat{\mathcal{D}}(\lambda)$ that describes the effect of a nonmaximally entangled channel used for quantum teleportation has the discrete form of Eq. (II.63) with $c_n \equiv c_n(\lambda)$, and the continuous form of Eq. (IV.7). It is proportional to the identity for $\lambda \to 1$. If either initial state is maximally entangled, one can see in Eq. (IV.67) that the projected state corresponds exactly to the other nonmaximally entangled initial state up to a local unitary transformation.

The discrete case: As we have studied in chapter II, the unitary transformations that generate the maximally entangled basis in the discrete case are

$$\hat{U}(\gamma) \equiv \hat{U}(\alpha,\beta) = \sum_{k=0}^{d-1} \exp(2\pi i k\beta/d)|k\rangle\langle k \oplus \alpha| \,, \tag{IV.68}$$

where $\alpha = 0, 1, ..., d-1$, and $\beta = 0, 1, ..., d-1$. Let us first investigate qubit entanglement swapping with $d = 2$ [22]. For simplicity, in this case we can set $c_n(\lambda) \equiv c_n$ ($n = 0, 1$) with $c_0^2 + c_1^2 = 1$. With the two entangled states

$$\begin{aligned} |\psi\rangle_{12} &= c_0|00\rangle_{12} + c_1|11\rangle_{12} \,, \\ |\psi\rangle_{34} &= c_0'|00\rangle_{34} + c_1'|11\rangle_{34} \,, \end{aligned} \tag{IV.69}$$

the projected states of 1 and 4 after measuring 2 and 3 with respect to the Bell basis [the four Bell states in Eq. (II.58) with Eq. (IV.68) for $d = 2$], become

according to Eq. (IV.67) using Eqs. (II.63,IV.68) for $d = 2$ and assuming equal initial entanglement ($c_0 = c_0'$)

$$\frac{1}{\sqrt{2P_0}} \left(c_0^2|00\rangle_{14} \pm c_1^2|11\rangle_{14}\right) , \tag{IV.70}$$

or

$$\frac{1}{\sqrt{2P_1}} \left(c_0 c_1|01\rangle_{14} \pm c_1 c_0|10\rangle_{14}\right) = \frac{1}{\sqrt{2}} \left(|01\rangle_{14} \pm |10\rangle_{14}\right) , \tag{IV.71}$$

with the probabilities for obtaining these states, $P_0 = (c_0^4 + c_1^4)/2$ and $P_1 = c_0^2 c_1^2$. With probability $2P_1$ one directly obtains a maximally entangled state ($\alpha = 1$, $\beta = 0, 1$), with probability $2P_0$, the output is even less entangled than the initial states ($\alpha = 0$, $\beta = 0, 1$). This means that the partial von Neumann entropy, $E_{\text{v.N.}} = -\text{Tr}\hat{\rho}_1 \log \hat{\rho}_1 = -\text{Tr}\hat{\rho}_4 \log \hat{\rho}_4$ with $\text{Tr}_4\hat{\rho}_{14} = \hat{\rho}_1$ and $\text{Tr}_1\hat{\rho}_{14} = \hat{\rho}_4$, sometimes decreases, sometimes increases, but on average decreases:

$$\bar{E}_{\text{v.N.}} = 2c_0^2 c_1^2 - c_0^4 \log \frac{c_0^4}{c_0^4 + c_1^4} - c_1^4 \log \frac{c_1^4}{c_0^4 + c_1^4} , \tag{IV.72}$$

where the entropy of the initial states is $E_{\text{v.N.}}^{\text{in}} = -c_0^2 \log c_0^2 - c_1^2 \log c_1^2$. However, there is a measure of entanglement which is conserved on average:

$$\bar{E}_{\max} = E_{\max}^{\text{in}} = 2c_1^2 , \tag{IV.73}$$

assuming $c_1 < c_0$.

This measure is defined as the maximum probability of concentrating maximum entanglement from a pure bipartite state via local operations and classical communication [22]. If the two initial states have different entanglement ($c_0 \neq c_0'$), no measurement result directly yields a maximally entangled state, but a subsequent unitary transformation can lead to perfect entanglement [182]. On average, the maximum probability for concentrating maximum entanglement from the output states of entanglement swapping (averaged upon the four possible output states) then becomes $\bar{E}_{\max} = 2c_1^2$ for $c_1 < c_1'$ and $\bar{E}_{\max} = 2{c_1'}^2$ for

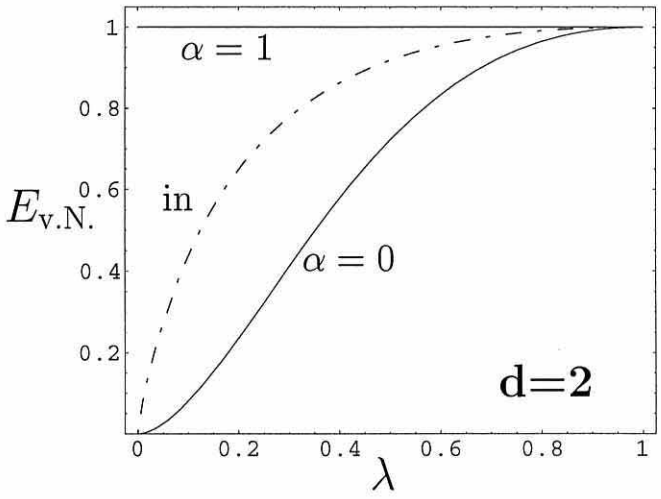

Figure IV.5: The partial entropy after entanglement swapping with two qubit pairs ($d = 2$) conditioned on the Bell measurement results ($\alpha = 0$ and $\beta = 0$ or 1, $\alpha = 1$ and $\beta = 0$ or 1) as a function of λ, describing the amount of entanglement of the equally entangled initial states as shown by the dashed line with no entanglement for $\lambda = 0$ and maximum entanglement for $\lambda \to 1$. The dimension is "ebits" ($\log \equiv \log_2$).

$c_1' < c_1$ (always with $c_1 < c_0$, $c_1' < c_0'$). On average, the entanglement $E_{\max}^{\text{in}}$ of the less entangled initial state is conserved.

In the following, the coefficients in Eq. (II.52) may be chosen as

$$c_n(\lambda) = \sqrt{\frac{\lambda^n - \lambda^{n+1}}{1 - \lambda^d}}\,, \tag{IV.74}$$

where $\sum_{n=0}^{d-1} c_n^2(\lambda) = 1$ is satisfied. This is the most suitable form with regard to our aim of comparing discrete with continuous-variable entanglement swapping. Note that the initial states are not entangled for $\lambda = 0$ and maximally entangled for $\lambda \to 1$ where $c_{n+1}(\lambda)/c_n(\lambda) \to 1$. Using this form for qubits ($d = 2$) seems a bit awkward, but within the range $\lambda \in [0, 1)$ we can equivalently describe all possible initial states as in Eq. (IV.69) (with $c_1 < c_0$, $c_1' < c_0'$), approaching maximally entangled states in the limit $\lambda \to 1$. With the coefficients from Eq. (IV.74)

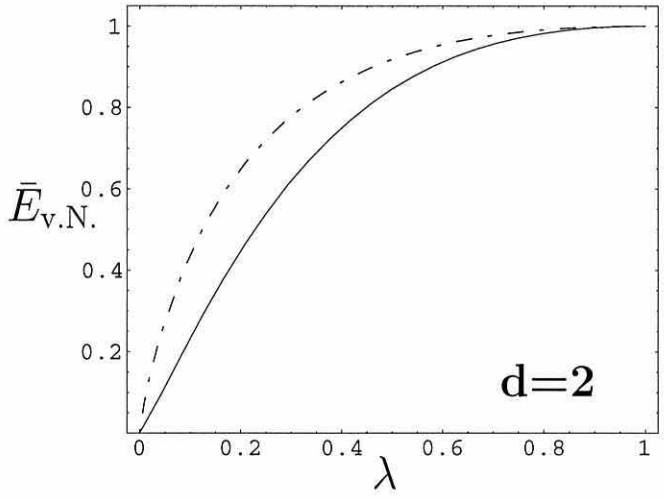

Figure IV.6: The average partial entropy after entanglement swapping with two qubit pairs ($d = 2$) as a function of λ, describing the amount of entanglement of the equally entangled initial states as shown by the dashed line with no entanglement for $\lambda = 0$ and maximum entanglement for $\lambda \to 1$.

($d = 2$), we obtain the average entropy for the output states (for equally entangled inputs),

$$\bar{E}_{\text{v.N.}} = \frac{(1+\lambda^2)\log(1+\lambda^2) - \lambda^2 \log \lambda^2 + 2\lambda}{(1+\lambda)^2}\,, \tag{IV.75}$$

where the entropy of the initial states is $E^{\text{in}}_{\text{v.N.}} = \log(1+\lambda) - (\lambda \log \lambda)/(1+\lambda)$. The entropy conditioned on the measurement results becomes 1 for $\alpha = 1$ and $\beta = 0$ or 1, and

$$E_{\text{v.N.}} = \log(1+\lambda^2) - \frac{\lambda^2 \log \lambda^2}{1+\lambda^2} \tag{IV.76}$$

for $\alpha = 0$ and $\beta = 0$ or 1. In the latter case, λ *is replaced by* λ^2 *compared to the input entropy.* The partial von Neumann entropy after qubit entanglement swapping, conditioned on the measurement results and on average, is shown in Figs. IV.5 and IV.6 respectively.

Let us now consider the general discrete d-level case. The initial entangled states $|\psi(\lambda)\rangle_{12}$ and $|\psi(\lambda')\rangle_{34}$ are described as in Eq. (II.52). The projected states of 1 and 4 after measuring 2 and 3 with respect to the Bell basis [Eq. (II.58) with Eq. (IV.68)] become now according to Eq. (IV.67) using Eqs. (II.63,IV.68)

$$\frac{1}{\sqrt{P_\alpha\, d}} \sum_{k=0}^{d-1} \exp(-2\pi i k\beta/d)\, c_k(\lambda) c_{k\oplus\alpha}(\lambda') |k\rangle_1 |k\oplus\alpha\rangle_4 \;, \tag{IV.77}$$

with the probabilities for obtaining these states,

$$P_\alpha = \frac{1}{d} \sum_{k=0}^{d-1} c_k^2(\lambda) c_{k\oplus\alpha}^2(\lambda') \;. \tag{IV.78}$$

Using this result, we obtain the output partial entropy (conditioned on the measurement results α)

$$E_{\text{v.N.}} = -\frac{1}{P_\alpha d} \sum_{k=0}^{d-1} c_k^2(\lambda) c_{k\oplus\alpha}^2(\lambda') \log \frac{c_k^2(\lambda) c_{k\oplus\alpha}^2(\lambda')}{P_\alpha\, d}, \tag{IV.79}$$

and the average partial entropy

$$\bar{E}_{\text{v.N.}} = -\sum_{\alpha=0}^{d-1} \sum_{k=0}^{d-1} c_k^2(\lambda) c_{k\oplus\alpha}^2(\lambda') \log \frac{c_k^2(\lambda) c_{k\oplus\alpha}^2(\lambda')}{P_\alpha\, d}. \tag{IV.80}$$

Here, the probabilities P_α and the dimension d cancel due to the averaging with d states having the same entropy for given α and varying β. The entropy of the initial states is $E_{\text{v.N.}}^{\text{in}} = -\sum_{k=0}^{d-1} c_k^2(\lambda) \log c_k^2(\lambda)$ and similarly for λ'.

The partial von Neumann entropy is our measure for comparison between discrete and continuous-variable entanglement swapping, and we will see that, both in the discrete limit $d \to \infty$ and in a scheme fully based on continuous variables, $\bar{E}_{\text{v.N.}} = E_{\text{v.N.}}$. The other entanglement measure mentioned above for qubit entanglement swapping, the maximum probability for concentrating maximum entanglement $E_{\max}$, was used by Hardy and Song for analyzing d-level entanglement swapping chains [103]. Their result was that for a broad class of states, $\bar{E}_{\max} = E_{\max}^{\text{in}}$, where $\bar{E}_{\max}$ refers to the two ends of the chain after entanglement swapping and $E_{\max}^{\text{in}}$ to the initially "weakest link" of the chain. For

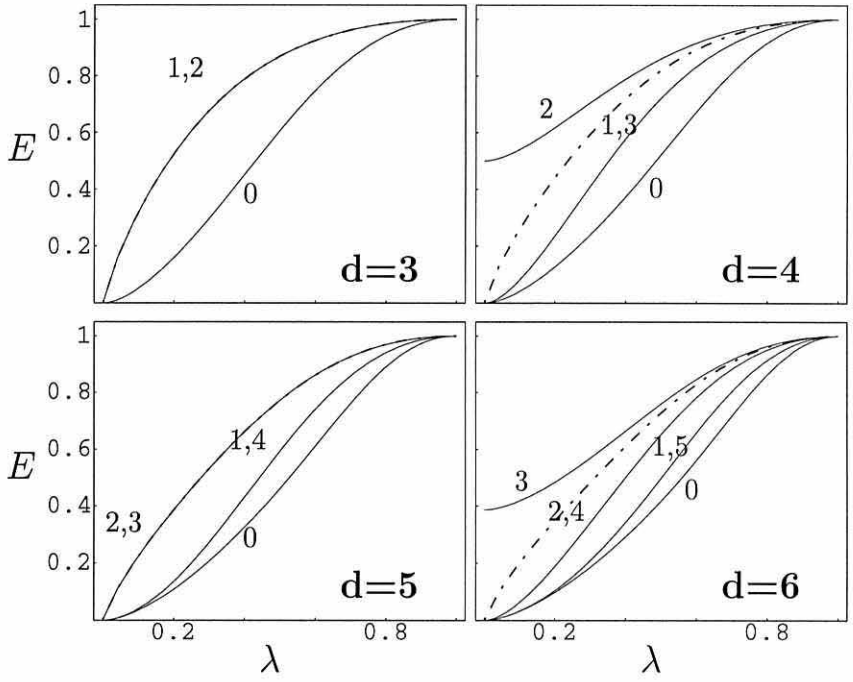

Figure IV.7: The partial entropy $E \equiv E_{\text{v.N.}}$ after entanglement swapping with two qu*d*it pairs ($d = 3, 4, 5, 6$) conditioned on the measurement results $\alpha = 0...d-1$ as a function of λ, describing the amount of entanglement of the equally entangled initial states as shown by the dashed line with no entanglement for $\lambda = 0$ and maximum entanglement for $\lambda \to 1$. The dimension is "e*d*its" ($\log \equiv \log_d$). Note that for $d = 3$ and $d = 5$, the results $\alpha = 1, 2$ and $\alpha = 2, 3$ reproduce the input entanglement, respectively.

qubit entanglement swapping with *two* initial states, this result indeed always holds [Eq. (IV.73)]. With respect to our intended comparison, we are mainly interested in states such as in Eq. (II.52) with $c_n \equiv c_n(\lambda)$ (described by only one parameter λ) rather than in states with more freedom in their Schmidt coefficients [103]. Further, the entanglement measure $E_{\max}$ always vanishes in the case of continuous variables, since it is impossible to concentrate maximum entanglement represented by the unphysical states in Eq. (IV.6). The output partial entropy conditioned on the measurement results α for d-level entanglement swapping is

shown in Fig. IV.7.

The infinite-dimensional limit: The initial entangled states of Eq. (II.52) take on the following form in the infinite-dimensional limit ($d \to \infty$) with the coefficients from Eq. (IV.74):

$$|\psi(\lambda)\rangle = \sqrt{1-\lambda}\sum_{n=0}^{\infty} \lambda^{n/2}|n\rangle|n\rangle \; . \tag{IV.81}$$

By setting $\lambda = \tanh^2 r$, these states become two-mode squeezed vacuum states expanded in the discrete number basis with the squeezing parameter r. This means that the initial entangled states in continuous-variable entanglement swapping and in discrete-variable entanglement swapping for $d \to \infty$ with the coefficients from Eq. (IV.74) are identical. The difference between the two schemes relies on the different measurement bases, the discrete maximally entangled number states and the continuous maximally entangled position states.

Using Eq. (IV.77) for the projected states, again with the coefficients from Eq. (IV.74) and the probabilities P_α from Eq. (IV.78), we find that

$$\lim_{d\to\infty} \frac{c_k(\lambda)c_{k\oplus\alpha}(\lambda')}{\sqrt{P_\alpha\, d}} = [(1-\lambda\lambda')(\lambda\lambda')^k]^{1/2} \; , \tag{IV.82}$$

yielding the output states

$$\sqrt{1-\Lambda}\sum_{n=0}^{\infty} e^{-in\phi_0}\sqrt{\Lambda}^n\, |n\rangle_1|n+n_0\rangle_4 \; , \tag{IV.83}$$

with $\Lambda = \lambda\lambda'$. The projected states are again effectively two-mode squeezed states with a "new" squeezing parameter given by $\tanh^2 R = \Lambda = \lambda\lambda' = \tanh^2 r \tanh^2 r'$. These states still depend on the measurement results α (through a relative number displacement given by $n_0 \equiv \alpha$) and β (through the phase factors $e^{-in\phi_0}$ with $2\pi\beta/d \to \phi_0$ for $d \to \infty$), but their degree of entanglement apparently no longer depends on the results α as it did for finite d. The partial von Neumann entropy becomes

$$\bar{E}_{\text{v.N.}} = E_{\text{v.N.}} = -\log(1-\Lambda) - \frac{\Lambda}{1-\Lambda}\log\Lambda \; , \tag{IV.84}$$

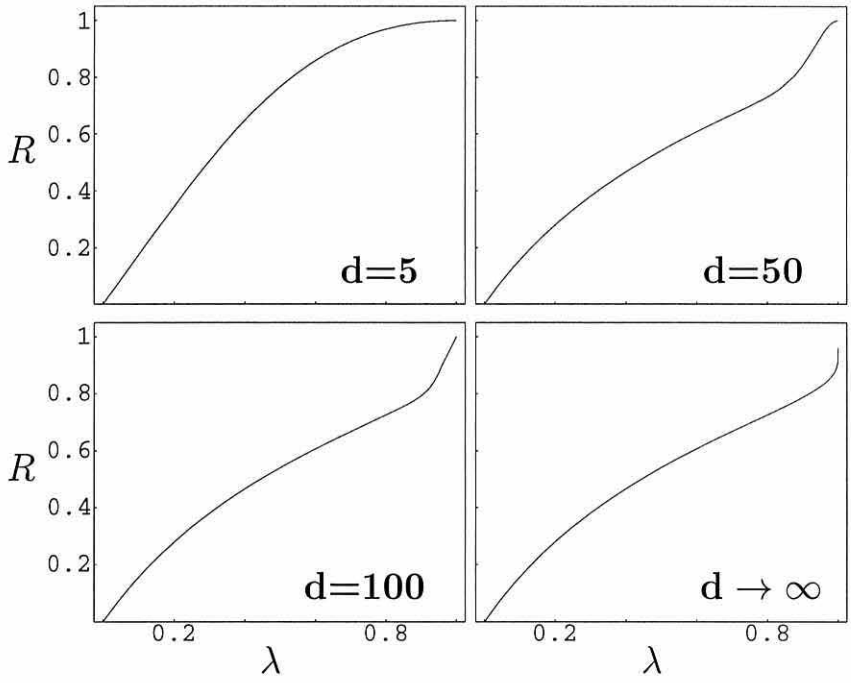

Figure IV.8: The ratio $R = \bar{E}_{\text{v.N.}}/E^{\text{in}}_{\text{v.N.}}$ of the average partial entropy after entanglement swapping and the initial entropy for two qu*d*it pairs ($d = 5, 50, 100, \infty$) as a function of λ, describing the amount of entanglement of the equally entangled initial states. Note that for $d \to \infty$, $\bar{E}_{\text{v.N.}} = E_{\text{v.N.}}$.

where the partial entropy of the input states is $E^{\text{in}}_{\text{v.N.}} = -\log(1-\lambda) - (\lambda \log \lambda)/(1-\lambda)$ and similarly for λ'. We see that the outgoing entanglement can be obtained by simply replacing λ and λ' of the input states by $\Lambda = \lambda\lambda'$ for the output state. For equal input entanglement, the initial λ is replaced by λ^2 as a result of entanglement swapping, just as for qubits when a less entangled output state is obtained rather than a maximally entangled state. *However, in the infinite-dimensional limit, there is no dependence on the measurement results, i.e., any result yields the same output entanglement in contrast to the finite-dimensional case.*

The average entropy is always degraded through entanglement swapping regardless of the dimension of the participating systems. However, the comparison

in Fig. IV.8 demonstrates that the degree of this deterioration grows with increasing dimension. In fact, for $d \to \infty$, the outgoing entanglement deteriorates by the largest amount compared to the cases with finite d.

The continuous case: Let us now consider the entanglement swapping scheme based solely on continuous single-mode quadratures. In particular, the measurements are now homodyne detections determining $u = x_2 - x_3$ and $v = p_2 + p_3$, and hence projecting modes 2 and 3 on the continuous-variable basis in Eq. (IV.6). Using Eqs. (IV.67,IV.8,IV.7) and the unitary transformations (phase-space displacements) in Eq. (IV.9) which span the continuous-variable Bell basis in Eq. (IV.6) [or Eq. (IV.10)], we find the output of entanglement swapping to be the following (unnormalized) state:

$$\begin{aligned} &\propto \int dx\, dx'\, dx'' e^{-2ixv} f(x, x', \lambda)\, f(x-u, x'', \lambda')\, |x'\rangle_1 |x''\rangle_4, \\ &= \int dx\, dx'\, dx'' e^{-2ixv} f(x+u, x', \lambda)\, f(x, x'', \lambda')\, |x'\rangle_1 |x''\rangle_4. \end{aligned} \quad \text{(IV.85)}$$

It is the projected state after the Bell measurement of modes 2 and 3 conditioned upon the results u and v. Additional unitary transformations, i.e., the final step in "usual" quantum teleportation, are here phase-space displacements of either mode 1 [by $U_1(-u, v)$] or mode 4 [by $U_4(u, v)$], transforming the projected state into either

$$\propto \int dx\, dx'\, dx'' e^{2i(x'-x)v} f(x, x'', \lambda')\, f(x+u, x'+u, \lambda)\, |x'\rangle_1 |x''\rangle_4, \quad \text{(IV.86)}$$

or

$$\propto \int dx\, dx'\, dx'' e^{2i(x''-x)v} f(x, x', \lambda)\, f(x-u, x''-u, \lambda')\, |x'\rangle_1 |x''\rangle_4, \quad \text{(IV.87)}$$

respectively. The resulting states correspond to the output after a final twist, i.e., displacements "twisting" the initial entangled states with respect to the measured entangled states. In Eq. (IV.86), the EPR channel of modes 1 and 2 has been

twisted by applying $U_1(-u,v)$, in Eq. (IV.87), the EPR channel of modes 3 and 4 has been twisted by applying $U_4(u,v)$. The outgoing state still depends on u and v except for $\lambda \to 1$ in the former case and $\lambda' \to 1$ in the latter case (corresponding to perfect teleportation of mode 3 to mode 1 and of mode 2 to mode 4 respectively). In an ensemble description, the results u and v are classically determined, but random due to the randomness of the Bell measurements. Thus, the twist, corresponding to unit-gain displacements of either mode 4 or mode 1, does not in general yield the optimum pure-state entanglement for the ensemble output state of modes 1 and 4.

Before we discuss the ensemble picture in order to find the optimal final displacements, let us also look at the reduced state in the Wigner representation. The initial entangled states can be described by the Wigner function $W^{(\lambda)}(x_1,p_1,x_2,p_2)$ of Eq. (III.28) with squeezing $\lambda = \tanh^2 r$, and similarly for modes 3 and 4, $W^{(\lambda')}(x_3,p_3,x_4,p_4)$ with squeezing $\lambda' = \tanh^2 r'$.

Recall that the Bell measurement is experimentally performed by detecting the output modes (labeled by the indices u and v) of a 50:50 beam splitter with, in this case, modes 2 and 3 as the input modes. The following quadratures are measured: $x_{\rm u} = (x_2 - x_3)/\sqrt{2}$ and $p_{\rm v} = (p_2 + p_3)/\sqrt{2}$, determining the parameters of the Bell states $u = \sqrt{2}x_{\rm u}$ and $v = \sqrt{2}p_{\rm v}$. After a little algebra, we can express the whole system behind the beam splitter and before the Bell detection in terms of modes u, v, 1, and 4,

$$\begin{aligned} W(x_{\rm u},p_{\rm u},x_{\rm v},p_{\rm v},x_1,p_1,x_4,p_4) &= \frac{16}{\pi^4} \\ &\times \exp\{-e^{-2r}[(x_1 + x_{\rm u}/\sqrt{2} + x_{\rm v}/\sqrt{2})^2 + (p_1 - p_{\rm u}/\sqrt{2} - p_{\rm v}/\sqrt{2})^2] \\ &\quad -e^{+2r}[(x_1 - x_{\rm u}/\sqrt{2} - x_{\rm v}/\sqrt{2})^2 + (p_1 + p_{\rm u}/\sqrt{2} + p_{\rm v}/\sqrt{2})^2] \\ &\quad -e^{-2r'}[(x_{\rm v}/\sqrt{2} - x_{\rm u}/\sqrt{2} + x_4)^2 + (p_{\rm v}/\sqrt{2} - p_{\rm u}/\sqrt{2} - p_4)^2] \\ &\quad -e^{+2r'}[(x_{\rm v}/\sqrt{2} - x_{\rm u}/\sqrt{2} - x_4)^2 + (p_{\rm v}/\sqrt{2} - p_{\rm u}/\sqrt{2} + p_4)^2]\}. \end{aligned} \tag{IV.88}$$

The (unnormalized) reduced state after the Bell detection is now obtained by integrating over $x_{\rm v}$ and $p_{\rm u}$:

$$\begin{aligned}
&\propto \int dx_{\rm v}\, dp_{\rm u} W(x_{\rm u}, p_{\rm u}, x_{\rm v}, p_{\rm v}, x_1, p_1, x_4, p_4) \\
&\propto \exp\Bigg\{ - e^{-2r}[(x_1 + x_{\rm u}/\sqrt{2})^2 + (p_1 - p_{\rm v}/\sqrt{2})^2] \\
&\quad - e^{-2r'}[(x_4 - x_{\rm u}/\sqrt{2})^2 + (p_4 - p_{\rm v}/\sqrt{2})^2] \\
&\quad - e^{+2r}[(x_1 - x_{\rm u}/\sqrt{2})^2 + (p_1 + p_{\rm v}/\sqrt{2})^2] \\
&\quad - e^{+2r'}[(x_4 + x_{\rm u}/\sqrt{2})^2 + (p_4 + p_{\rm v}/\sqrt{2})^2] \\
&\quad + \frac{[\sqrt{2}(\sinh 2r\, x_1 + \sinh 2r'\, x_4) - (\cosh 2r - \cosh 2r')x_{\rm u}]^2}{\cosh 2r + \cosh 2r'} \\
&\quad + \frac{[\sqrt{2}(\sinh 2r'\, p_4 - \sinh 2r\, p_1) - (\cosh 2r - \cosh 2r')p_{\rm v}]^2}{\cosh 2r + \cosh 2r'} \Bigg\}.
\end{aligned} \tag{IV.89}$$

Let us now apply the following variable substitutions,

$$\begin{aligned}
x_1 &= x_1' + g^{(1)} x_{\rm u}/\sqrt{2}, \quad p_1 = p_1' - g^{(1)} p_{\rm v}/\sqrt{2}, \\
x_4 &= x_4' - g^{(2)} x_{\rm u}/\sqrt{2}, \quad p_4 = p_4' - g^{(2)} p_{\rm v}/\sqrt{2}.
\end{aligned} \tag{IV.90}$$

These substitutions shift the output quadratures of modes 1 and 4 by constant numbers without changing their correlations or entanglement (they can be thought of as *local* displacements of the quadratures by known and fixed amounts). In terms of the new variables x_1', p_1', etc., with the right choice (and only for that choice) of the parameters $g^{(1)}$ and $g^{(2)}$, namely

$$\begin{aligned}
g^{(1)} &= \frac{2\sinh 2r}{\cosh 2r + \cosh 2r'}, \\
g^{(2)} &= \frac{2\sinh 2r'}{\cosh 2r + \cosh 2r'},
\end{aligned} \tag{IV.91}$$

the reduced Wigner function no longer depends on $x_{\rm u}$ and $p_{\rm v}$: the right choice of $g^{(1)}$ and $g^{(2)}$ eliminates all terms in the exponential proportional to $x_1' x_{\rm u}$, $x_4' x_{\rm u}$, etc. All terms in the exponential proportional to $x_{\rm u}^2$ or $p_{\rm v}^2$ only contribute to the

normalization. The reduced Wigner function then reads

$$W(x_1', p_1', x_4', p_4') \propto \exp\left[-2\frac{1+\cosh 2r\cosh 2r'}{\cosh 2r+\cosh 2r'}\left(x_1'^2+x_4'^2+p_1'^2+p_4'^2\right) + 4\frac{\sinh 2r\sinh 2r'}{\cosh 2r+\cosh 2r'}(x_1'x_4'-p_1'p_4')\right]. \quad \text{(IV.92)}$$

From this Wigner function we can extract the correlation matrix which has the form

$$V^{(2)} = \frac{1}{4}\begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & -b \\ b & 0 & a & 0 \\ 0 & -b & 0 & a \end{pmatrix}, \quad \text{(IV.93)}$$

with

$$a = \frac{1+\cosh 2r\cosh 2r'}{\cosh 2r+\cosh 2r'}, \quad b = \frac{\sinh 2r\sinh 2r'}{\cosh 2r+\cosh 2r'}. \quad \text{(IV.94)}$$

By comparison of the above correlation matrix with the correlation matrix of a two-mode squeezed vacuum state [with elements $a = \cosh 2r$ and $b = \sinh 2r$, see Eq. (III.30)], we can conclude: the reduced state in any single shot is a pure two-mode squeezed vacuum state (up to fixed local displacements) with

$$\begin{aligned} a &= \cosh 2R = \frac{1+\cosh 2r\cosh 2r'}{\cosh 2r+\cosh 2r'}, \\ b &= \sinh 2R = \frac{\sinh 2r\sinh 2r'}{\cosh 2r+\cosh 2r'}, \end{aligned} \quad \text{(IV.95)}$$

since indeed $\cosh^2 2R - \sinh^2 2R = 1$. The above result is in fact equivalent to that obtained for discrete variables in the infinite-dimensional limit,

$$\tanh^2 R = \tanh^2 r \tanh^2 r' . \quad \text{(IV.96)}$$

For any nonzero squeezing in *both* initial entangled states, $r > 0$ *and* $r' > 0$, entanglement swapping occurs, i.e., $R > 0$, but the quality of the entanglement always deteriorates, $R < r$ and $R < r'$ (unless $r \to \infty$, then $R = r'$, or $r' \to \infty$,

then $R = r$). This is in agreement with the results of the previous section, where the quality of the entanglement after continuous-variable entanglement swapping was not quantified, but assessed due to its performance as a resource for quantum teleportation. However, there we considered the ensemble output state as the resource whose quality of the entanglement cannot exceed that of the reduced state in a single shot. Let us examine this further.

Instead of the variable substitutions that removed terms proportional to $x_1 x_{\mathrm{u}}$, $x_4 x_{\mathrm{u}}$, etc., in the reduced Wigner function, we could have simply neglected these terms. For known and fixed x_{u}, p_{v}, these terms do not change the correlations or the entanglement of modes 1 and 4. They represent known and fixed local displacements in the outgoing nonmaximally entangled state. By comparison with the known entanglement of two-mode squeezed states, we also would have obtained the result of Eq. (IV.96). The situation is different, when x_{u} and p_{v} are not fixed but random variables, taking into account the randomness of the Bell measurement results. In this case, the reduced state becomes mixed. This mixedness can be manifest in two qualitatively different ways which shall be illustrated by the example of entanglement swapping with qubits, assuming for the moment maximum initial entanglement.

First, the results of the Bell measurement on qubits 2 and 3 performed by Claire may not be known to Alice and Bob who are at the locations of qubits 1 and 4 respectively. If Alice and Bob do not receive any classical information from Claire, they end up sharing a maximally mixed state, a mixture of all four Bell states (each with equal weight) corresponding to the four possible measurement outcomes. The knowledge of whether Claire performed that measurement at all and that she measured in the Bell basis only specifies the decomposition of the maximally mixed state of 1 and 4. Alice and Bob know they share a Bell state, but they do not know which particular one. In order to exploit the quantum resource that they potentially share it is crucial to them to receive the

classical information of Claire's result. This scenario corresponds to a "single shot picture", where the output state for a single measurement shot is mixed due to the lack of classical information about the random result. Another kind of mixedness can emerge at the output in a scenario where Alice and Bob are provided with the classical information from Claire, but they can make use of their potential quantum resource only on average. They effectively share a random sequence of all four Bell states. Although this ensemble state is again maximally mixed, Alice and Bob can purify it by applying a corresponding sequence of unitary transformations (depending on Claire's results) that always result in one particular Bell state, making also the ensemble state a pure Bell state.

Considering continuous variables where the ensemble state at the output is relevant to experimental realizations including verification via homodyne detection (measuring quadrature variances), the significance of the displacements in Eq. (IV.90) becomes clear. Any randomness of the measurement results x_{u} and p_{v} (i.e., correlations of the quadratures of modes 1 and 4 with the random classical variables x_{u} and p_{v}) can be eliminated from the output ensemble state by continuously applying appropriate displacements with the right gains. This removes the "classical noise" of the mixed ensemble state and makes it a pure two-mode squeezed state with squeezing R. The consequence of the fact that we are dealing with nonmaximally entangled input states here is that appropriate displacements have to be applied to both modes 1 and 4 with nonunit gains. In other words, the appropriate unitary transformations that optimize the ensemble output are not simple twists, i.e., one-sided unit-gain displacements by either Alice or Bob.

As a result, we know now the size of the optimal entanglement that can be obtained after entanglement swapping using measurements on the continuous-variable Bell basis. This optimum represents an upper bound for the entanglement of the output ensemble state, since one cannot do better on average than for a single shot.

Let us now investigate the ensemble output state for arbitrary final displacements. The simplest way to directly obtain the ensemble output state of modes 1 and 4 after the Bell detection and arbitrary displacements is a calculation in the Heisenberg picture with the two initial two-mode squeezed states

$$\begin{aligned}
\hat{a}_1 &= (\cosh r\hat{a}_1^{(0)} + \sinh r\hat{a}_1^{(0)\dagger} + \cosh r\hat{a}_2^{(0)} - \sinh r\hat{a}_2^{(0)\dagger})/\sqrt{2},\\
\hat{a}_2 &= (\cosh r\hat{a}_1^{(0)} + \sinh r\hat{a}_1^{(0)\dagger} - \cosh r\hat{a}_2^{(0)} + \sinh r\hat{a}_2^{(0)\dagger})/\sqrt{2},\\
\hat{a}_3 &= (\cosh r'\hat{a}_3^{(0)} + \sinh r'\hat{a}_3^{(0)\dagger} + \cosh r'\hat{a}_4^{(0)} - \sinh r'\hat{a}_4^{(0)\dagger})/\sqrt{2},\\
\hat{a}_4 &= (\cosh r'\hat{a}_3^{(0)} + \sinh r'\hat{a}_3^{(0)\dagger} - \cosh r'\hat{a}_4^{(0)} + \sinh r'\hat{a}_4^{(0)\dagger})/\sqrt{2}.
\end{aligned} \tag{IV.97}$$

Using the relations [recall $\hat{x}_{\mathrm{u}} = (\hat{x}_2 - \hat{x}_3)/\sqrt{2}$, $\hat{p}_{\mathrm{v}} = (\hat{p}_2 + \hat{p}_3)/\sqrt{2}$]

$$\begin{aligned}
\hat{x}_1 &= g^{(1)}\hat{x}_3/2 + \hat{x}_1 - g^{(1)}\hat{x}_2/2 + g^{(1)}\hat{x}_{\mathrm{u}}/\sqrt{2},\\
\hat{p}_1 &= g^{(1)}\hat{p}_3/2 + \hat{p}_1 + g^{(1)}\hat{p}_2/2 - g^{(1)}\hat{p}_{\mathrm{v}}/\sqrt{2},\\
\hat{x}_4 &= g^{(2)}\hat{x}_2/2 + \hat{x}_4 - g^{(2)}\hat{x}_3/2 - g^{(2)}\hat{x}_{\mathrm{u}}/\sqrt{2},\\
\hat{p}_4 &= g^{(2)}\hat{p}_2/2 + \hat{p}_4 + g^{(2)}\hat{p}_3/2 - g^{(2)}\hat{p}_{\mathrm{v}}/\sqrt{2},
\end{aligned} \tag{IV.98}$$

and applying the operator displacements corresponding to Eq. (IV.90), we can calculate the correlation matrix of the outgoing ensemble state of modes $1'$ and $4'$ from the operators $\hat{x}_1'$, $\hat{p}_1'$, etc., and obtain

$$V^{(2)} = \frac{1}{4}\begin{pmatrix} a & 0 & b & 0\\ 0 & a & 0 & -b\\ b & 0 & a' & 0\\ 0 & -b & 0 & a' \end{pmatrix}, \tag{IV.99}$$

with

$$\begin{aligned}
a &= g^{(1)2}(\cosh 2r + \cosh 2r')/4 + \cosh 2r - g^{(1)}\sinh 2r,\\
a' &= g^{(2)2}(\cosh 2r + \cosh 2r')/4 + \cosh 2r' - g^{(2)}\sinh 2r',\\
b &= (g^{(2)}/2)\sinh 2r + (g^{(1)}/2)\sinh 2r' - g^{(1)}g^{(2)}(\cosh 2r + \cosh 2r')/4.
\end{aligned} \tag{IV.100}$$

For the "right" gains from Eq. (IV.91), the correlation matrix of the outgoing ensemble state in Eqs. (IV.99,IV.100) becomes indeed that of Eqs. (IV.93,IV.94) (that of the reduced single-shot state apart from local fixed displacements). Thus, in this case, the ensemble output state is a pure two-mode squeezed state with squeezing R given by Eq. (IV.96). *It contains the optimum amount of entanglement available on average.*

The above correlation matrix corresponds to the ensemble state after Alice's displacements of mode 1 by $\sqrt{2}(-x_{\rm u}+ip_{\rm v})$ with gain $g^{(1)}/2$ *and* Bob's displacements of mode 4 by $\sqrt{2}(x_{\rm u}+ip_{\rm v})$ with gain $g^{(2)}/2$. Let us also write down the correlation matrix of the ensemble state of modes 1 and $4'$ after displacing only mode 4 with gain $g_{\rm swap}$. We obtain it by setting $g^{(1)}=0$ and $g^{(2)}=2g_{\rm swap}$ in Eqs. (IV.99,IV.100), and it becomes $V^{(2)}$ of Eq. (IV.99) with

$$\begin{aligned} a &= \cosh 2r, \\ a' &= g_{\rm swap}^2(\cosh 2r+\cosh 2r')+\cosh 2r'-2g_{\rm swap}\sinh 2r', \\ b &= g_{\rm swap}\sinh 2r. \end{aligned} \qquad \text{(IV.101)}$$

We also would have obtained this matrix by using Eq. (IV.52) and Eq. (IV.61) with $r=r_1=r_2$ and $r'=s_1=s_2$, since there we considered one-sided displacements by Bob with gain $g_{\rm swap}$.

Let us further investigate and summarize whether and in what circumstances the above ensemble states are pure or mixed and separable or inseparable after two-sided and one-sided displacements. In order to determine their purity we can rearrange the correlation matrices into the form $\tilde{V}^{(2)}$ and apply the purity check given in chapter I. As for their inseparability, we can use the criteria from chapter III.

The results we obtain are as follows:

1.) In the case of *one-sided displacements of mode 4 by Bob*, the ensemble state given by Eqs. (IV.99,IV.101) is *always mixed for any gain unless we have* $r'\to\infty$ *and unit gain.* A pure state for $r'\to\infty$ and unit gain is what we expected, because

we know that the final twist (appropriate unit-gain displacements) of a maximally entangled EPR channel ($r' \to \infty$) leads to a teleported state independent of the Bell measurement results.

2.) We have seen in the previous section that the ensemble state after *one-sided displacements of mode 4 by Bob* enables quantum teleportation of arbitrary coherent states with fidelity $F_{\rm av} > 1/2$ for any $r > 0$ and $r' > 0$, provided the gain $g_{\rm swap} = (\sinh 2r + \sinh 2r')/(\cosh 2r + \cosh 2r')$ is used. This proves the state's inseparability in that case. With unit gain $g_{\rm swap} = 1$, squeezing of $e^{-2r} = e^{-2r'} < 1/2$ (if $r = r'$) is required to ensure $F_{\rm av} > 1/2$. Nevertheless, *also for unit gain, we find that the ensemble state given by Eqs. (IV.99,IV.101) is inseparable for any* $r > 0$ *and* $r' > 0$. We obtain this result by applying Simon's simplified necessary separability condition in Eq. (III.7) for the standard form $V_I^{(2)}$ of Eq. (III.4). It is violated for any $r > 0$ and $r' > 0$.

3.) In the case of *two-sided displacements, i.e., displacements of mode 4 by Bob and of mode 1 by Alice*, the ensemble state given by Eqs. (IV.99,IV.100) is *always mixed for any gains unless we have the "right" gains from Eq. (IV.91).* The ensemble state becomes a pure two-mode squeezed state only for those right gains. This state's squeezing R is given by Eq. (IV.96) and the state is obviously inseparable for any $r > 0$ and $r' > 0$.

Apparently, a pure ensemble state at the output requires local operations acting on both modes 1 and 4. Using the right gains for these operations guarantees that the optimum amount of entanglement can be retrieved from modes $1'$ and $4'$. However, the fidelity attainable in coherent-state teleportation when the two-mode squeezed state of modes $1'$ and $4'$ is used (after applying $g^{(1)} = g^{(2)} = \tanh 2r$ for $r = r'$) is the same as the fidelity we obtained in the preceding section using modes 1 and $4'$ after displacing only mode 4 with the optimum gain for $r = r'$, $g_{\rm swap} = \tanh 2r$. In fact, displacements of mode 1 by $\sqrt{2}(-x_{\rm u} + ip_{\rm v})$ with gain $g^{(1)}/2 = \tanh 2r/2$ and displacements of mode

4 by $\sqrt{2}(x_{\rm u} + ip_{\rm v})$ with gain $g^{(2)}/2 = \tanh 2r/2$ lead to the same total variance $\mathcal{V}(2) = \langle(\hat{x}_1' - \hat{x}_4')^2\rangle + \langle(\hat{p}_1' + \hat{p}_4')^2\rangle$ as displacements of only mode 4 with $g_{\rm swap} = \tanh 2r$, $\mathcal{V}(2) = \langle(\hat{x}_1 - \hat{x}_4')^2\rangle + \langle(\hat{p}_1 + \hat{p}_4')^2\rangle$. From a practical point of view, it would be therefore easier to displace only mode 4 with $g_{\rm swap} = \tanh 2r$ without degrading the performance, provided $r = r'$. A well-defined pure two-mode squeezed state, however, emerges at the output only after two-sided displacements with the gains from Eq. (IV.91).

In summary, we have seen that the gains of the local displacements employed after the continuous-variable Bell measurement in an entanglement swapping scheme affect the purity of the outgoing ensemble state. Although purity is not necessarily required to ensure an optimum performance of that state when it is used for quantum teleportation, only purity guarantees the optimum amount of entanglement in the ensemble output state. This optimum amount is identical to the degree of entanglement present in the reduced state for any single shot of the continuous-variable Bell measurement. It is also identical to the degree of entanglement of the projected state after a Bell measurement in the discrete d-level number basis when the limit $d \to \infty$ is taken.

i Exploiting multipartite entanglement: A quantum teleportation network

In this section, we give an example of a quantum communication scheme that exploits entanglement shared by an arbitrary number of parties. Within such a network quantum information can be transferred from any location (sending station) to any other location (receiving station). Classical information about local measurements at all the remaining locations available at the receiving station thereby enhances the fidelity of the teleported quantum state at the receiving station. This section is based on van Loock and Braunstein [132] [9].

[9] The scheme presented in this paper proved in an operational way that one single-mode squeezed state and linear optics suffice to produce entanglement between an arbitrary number of modes. In chapter III, we have verified this result using a different approach.

Let us first consider the following decomposition for an unknown input state $|\phi\rangle_{\rm in}$ and the maximally entangled (infinitely squeezed) version of the N-partite states from chapter III, $\frac{1}{\sqrt{\pi}}\int dx\,|x\rangle_1|x\rangle_2\cdots|x\rangle_N$:

$$|\phi\rangle_{\rm in}\otimes\frac{1}{\sqrt{\pi}}\int dx\,|x\rangle_1|x\rangle_2\cdots|x\rangle_N = \frac{1}{\sqrt{\pi^N}}\int dudv\prod_{j\neq k,l}^{N}dw_j\,|\Psi(u,v)\rangle_{{\rm in},k} \times \hat{U}_j^\dagger(u,0)|p=w_j\rangle_j\hat{U}_l^\dagger\left(u,v+\sum_{i\neq k,l}^{N}w_i\right)|\phi\rangle_l, \tag{IV.102}$$

with $k,l=1,2,...,N$ where $k\neq l$, and with the continuous-variable Bell states $|\Psi(u,v)\rangle$ of Eq. (IV.10) and the unitary transformations of Eq. (IV.9). From this decomposition, we can recognize a possible teleportation protocol using the N-partite entanglement: a Bell basis projection of mode "in" and mode k leaves mode l in the input state up to a corresponding unitary transformation, provided that all $N-2$ remaining modes are projected onto the momentum basis $|p=w_j\rangle_j$. The corresponding unitary transformation involves the usual displacements by the Bell measurement results (u,v) and a momentum displacement by the sum of all momenta obtained for the $N-2$ remaining modes.

How well does this quantum teleportation scheme based on multipartite entanglement work for finitely squeezed entanglement resources? Let us analyze this first for a teleportation protocol involving three participants, say, Alice, Bob, and Claire. The three modes of the tripartite entangled state in Eq. (III.34) are sent to Alice, Bob, and Claire, respectively. Suppose Alice wants to teleport an unknown quantum state and couples her mode 1 with the unknown input mode "in": $\hat{x}_{\rm u}=(\hat{x}_{\rm in}-\hat{x}_1)/\sqrt{2}$, $\hat{p}_{\rm v}=(\hat{p}_{\rm in}+\hat{p}_1)/\sqrt{2}$. Let us write Bob's mode 2 and

Claire's mode 3 as

$$\begin{aligned}
\hat{x}_2 &= \hat{x}_{\rm in} - (\hat{x}_1 - \hat{x}_2) - \sqrt{2}\hat{x}_{\rm u}, \\
\hat{p}_2 &= \hat{p}_{\rm in} + (\hat{p}_1 + \hat{p}_2 + g^{(3)}\hat{p}_3) - \sqrt{2}\hat{p}_{\rm v} - g^{(3)}\hat{p}_3, \\
\hat{x}_3 &= \hat{x}_{\rm in} - (\hat{x}_1 - \hat{x}_3) - \sqrt{2}\hat{x}_{\rm u}, \\
\hat{p}_3 &= \hat{p}_{\rm in} + (\hat{p}_1 + g^{(3)}\hat{p}_2 + \hat{p}_3) - \sqrt{2}\hat{p}_{\rm v} - g^{(3)}\hat{p}_2,
\end{aligned} \tag{IV.103}$$

where $g^{(3)}$ is another gain parameter determined later. Alice measures certain classical values $x_{\rm u}$ and $p_{\rm v}$ for $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$. The operators $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$ in Eq. (IV.103) collapse. This time Alice sends her classical results $x_{\rm u}$ and $p_{\rm v}$ either to Bob or Claire via classical channels. Now either Bob or Claire is able to reconstitute the input state provided that additional classical information is received: Bob needs the result of a momentum-detection by Claire reducing $\hat{p}_3$ to p_3 and Claire needs the result of a momentum-detection by Bob reducing $\hat{p}_2$ to p_2. Assuming that Claire detects her mode 3 and sends the result to Bob, a displacement of Bob's mode 2,

$$\begin{aligned}
\hat{x}_2 \longrightarrow \hat{x}_{\rm tel} &= \hat{x}_2 + g\sqrt{2}x_{\rm u}, \\
\hat{p}_2 \longrightarrow \hat{p}_{\rm tel} &= \hat{p}_2 + g\sqrt{2}p_{\rm v} + g^{(3)}\,p_3,
\end{aligned} \tag{IV.104}$$

accomplishes the teleportation. For $g = 1$, the teleported mode becomes

$$\hat{x}_{\rm tel} = \hat{x}_{\rm in} - (\sqrt{3}e^{-r_2}\hat{x}_2^{(0)} - e^{-r_3}\hat{x}_3^{(0)})/\sqrt{2}, \tag{IV.105}$$

$$\begin{aligned}
\hat{p}_{\rm tel} &= \hat{p}_{\rm in} + (2 + g^{(3)})e^{-r_1}\hat{p}_1^{(0)}/\sqrt{3} \\
&\quad + (1 - g^{(3)})e^{+r_2}\hat{p}_2^{(0)}/\sqrt{6} + (1 - g^{(3)})e^{+r_3}\hat{p}_3^{(0)}/\sqrt{2}\,.
\end{aligned}$$

When $r = r_1 = r_2 = r_3$, the optimum teleportation fidelity is achieved with

$$g^{(3)} = \frac{e^{+4r} - 1}{e^{+4r} + 1/2}, \tag{IV.106}$$

and it becomes for a coherent-state input with Eq. (IV.105) and Eq. (IV.50) for $g = 1$ (where $F = F_{\rm av}$)

$$F_{\rm opt} = \left\{\left[1 + e^{-2r}\right]\left[1 + 3/(2e^{+2r} + e^{-2r})\right]\right\}^{-1/2}. \tag{IV.107}$$

For $r = 0$, we obtain $F_{\rm opt} = 1/2$. Perfect teleportation with fidelity $F_{\rm opt} = 1$ is achieved for infinite squeezing in *all three* single-mode squeezed states $r \to \infty$ (where $g^{(3)} = 1$). For any $r > 0$, we find $F_{\rm opt} > 1/2$. Furthermore, $F > 1/2$ can even be satisfied using the entanglement built from only *one* single-mode squeezed state. In this case (with $r_2 = r_3 = 0$), we obtain the optimum fidelity

$$F_{\rm opt} = \left[2 + 6/(1 + 2e^{+2r_1})\right]^{-1/2} \tag{IV.108}$$

for

$$g^{(3)} = \frac{e^{+2r_1} - 1}{e^{+2r_1} + 1/2}. \tag{IV.109}$$

We still obtain $F_{\rm opt} > 1/2$ for any $r_1 > 0$. If Alice and Bob arrange to teleport Alice's unknown coherent state to Claire (and both send the required classical information to Claire who then performs the corresponding displacements), one can easily see that with optimum gain the fidelity also exceeds the classical limit for any $r_1 > 0$ when $r_2 = r_3 = 0$. In fact, Alice, Bob, and Claire can allow any one of them to be sender and any other to be receiver. For $r_1, r_2, r_3 \to \infty$ and unit gain, quantum teleportation is perfect with $F = 1$. If $r = r_1 = r_2 = r_3$, coherent-state teleportation with $F > 1/2$ between any two of Alice, Bob, and Claire is achieved for any $r > 0$, provided optimum gain is used. Even if the tripartite entanglement is based only on one squeezed state, the teleportation is better than classical with any sender and receiver chosen and any nonzero squeezing. For $r_1 \to \infty$ (with $r_2 = r_3 = 0$), we find the same maximum fidelity $F = 1/\sqrt{2}$ as in the two-party scheme involving only Alice and Bob [10].

Let us investigate the general N-party case. For the entangled state in Eq. (III.37) with $r = r_1 = r_2 = \cdots = r_N$, we find momentum quadrature

[10] The whole discussion here again excludes the possibility of additional local squeezers.

operators for any N correlated as

$$\left\langle \left(\hat{p}_k + \hat{p}_l + g^{(N)} \sum_{j \neq k,l}^{N} \hat{p}_j \right)^2 \right\rangle = \frac{[2 + (N-2)g^{(N)}]^2}{4N} e^{-2r} + \frac{(g^{(N)} - 1)^2 (N-2)}{2N} e^{+2r} , \tag{IV.110}$$

where $k \neq l$. This variance becomes zero and yields perfect correlations for $r \to \infty$ and $g^{(N)} = 1$. The correlations of the position quadrature operators are those from Eq. (III.35), $\langle (\hat{x}_k - \hat{x}_l)^2 \rangle = e^{-2r}/2$. With only one squeezed mode (squeezing r_1) and $N-1$ vacuum modes ($r_2 = r_3 = \cdots = r_N = 0$), the variance in Eq. (IV.110) becomes

$$\left\langle \left(\hat{p}_k + \hat{p}_l + g^{(N)} \sum_{j \neq k,l}^{N} \hat{p}_j \right)^2 \right\rangle = \frac{[2 + (N-2)g^{(N)}]^2}{4N} e^{-2r_1} + \frac{(g^{(N)} - 1)^2 (N-2)}{2N} , \tag{IV.111}$$

For the positions, we have the result from Eq. (III.36), $\langle (\hat{x}_k - \hat{x}_l)^2 \rangle = 1/2$.

Let us now assume that the N modes are sent to N different locations. We arbitrarily choose two locations of them as the sending (mode k) and the receiving station (mode l) for teleportation. The teleportation protocol is almost the same as in the N=3-case. However, now the receiver needs the classical information of the sender's detection of the quadratures $\hat{x}_{\mathrm{u}} = (\hat{x}_{\mathrm{in}} - \hat{x}_k)/\sqrt{2}$, $\hat{p}_{\mathrm{v}} = (\hat{p}_{\mathrm{in}} + \hat{p}_k)/\sqrt{2}$, and in addition the classical results of $N-2$ momentum-detections at the $N-2$ remaining stations. This can be seen by writing mode l as

$$\begin{aligned} \hat{x}_l &= \hat{x}_{\mathrm{in}} - (\hat{x}_k - \hat{x}_l) - \sqrt{2}\hat{x}_{\mathrm{u}}, \\ \hat{p}_l &= \hat{p}_{\mathrm{in}} + \hat{p}_k + \hat{p}_l + g^{(N)} \sum_{j \neq k,l}^{N} \hat{p}_j - \sqrt{2}\hat{p}_{\mathrm{v}} - g^{(N)} \sum_{j \neq k,l}^{N} \hat{p}_j . \end{aligned} \tag{IV.112}$$

Finally, the receiver displaces his mode by the sum of all classical results received,

$$\begin{aligned} \hat{x}_l \longrightarrow \hat{x}_{\mathrm{tel}} &= \hat{x}_l + g\sqrt{2}x_{\mathrm{u}}, \\ \hat{p}_l \longrightarrow \hat{p}_{\mathrm{tel}} &= \hat{p}_l + g\sqrt{2}p_{\mathrm{v}} + g^{(N)} \sum_{j \neq k,l}^{N} p_j . \end{aligned} \tag{IV.113}$$

For $g = 1$, the teleported mode becomes

$$\begin{aligned} \hat{x}_{\rm tel} &= \hat{x}_{\rm in} - (\hat{x}_k - \hat{x}_l), \\ \hat{p}_{\rm tel} &= \hat{p}_{\rm in} + \hat{p}_k + \hat{p}_l + g^{(N)} \sum_{j \neq k,l}^{N} \hat{p}_j. \end{aligned} \tag{IV.114}$$

Now we can optimize the teleportation fidelity using Eq. (IV.110) and find the optimum gain

$$g^{(N)} = \frac{e^{+4r} - 1}{e^{+4r} + (N-2)/2}, \tag{IV.115}$$

assuming $r = r_1 = r_2 = \cdots = r_N$. For a coherent-state input, we obtain the optimum fidelity according to Eq. (IV.50) with $g = 1$ (where $F = F_{\rm av}$)

$$F_{\rm opt} = \left\{1 + e^{-2r}\right\}^{-1/2} \left\{1 + N/[2e^{+2r} + (N-2)e^{-2r}]\right\}^{-1/2}. \tag{IV.116}$$

Again, for $r = 0$, we have $F_{\rm opt} = 1/2$. Perfect teleportation with $F_{\rm opt} = 1$ in any of the $N(N-1)/2$ channels (of course not simultaneously by no-cloning, see chapter II) is achieved with infinite squeezing in *all* single-mode squeezed states $r \to \infty$ (where $g^{(N)} = 1$) for any sending and receiving station chosen from the N locations. For any $r > 0$, we find $F_{\rm opt} > 1/2$, *provided* $N \leq 29$. Interestingly, if $N \geq 27$, $F_{\rm opt}$ reaches a maximum and then drops to a minimum before approaching 1 when the squeezing is increased. For $N \geq 30$, the minimum is below $1/2$, but the maximum (at sufficiently small squeezing) still exceeds $1/2$. Figure IV.9 shows the fidelity of Eq.(IV.116) for squeezing in dB.

What about using only *one* single-mode squeezed state in this N-mode scheme? Even in this case (with $r_2 = r_3 = \cdots = r_N = 0$), quantum teleportation is possible in any of the $N(N-1)/2$ channels for any N. We obtain the optimum fidelity for coherent-state teleportation

$$F_{\rm opt} = \left[2 + 2N/(N - 2 + 2e^{+2r_1})\right]^{-1/2} \tag{IV.117}$$

for

$$g^{(N)} = \frac{e^{+2r_1} - 1}{e^{+2r_1} + (N-2)/2}. \tag{IV.118}$$

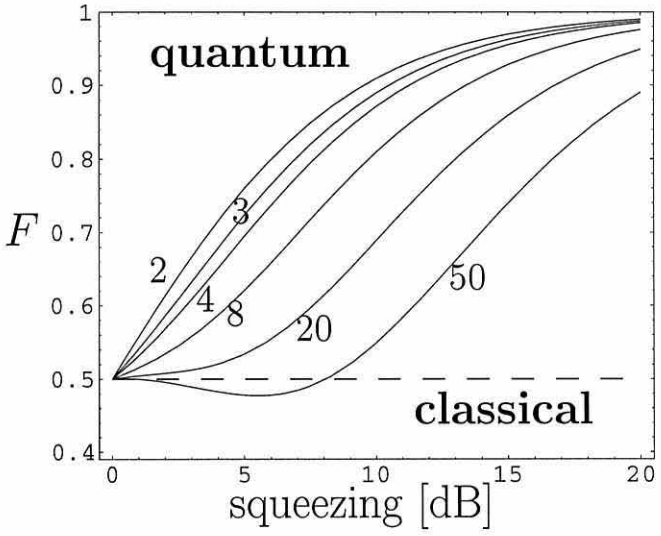

Figure IV.9: N squeezed states: Optimized fidelity for the teleportation of an arbitrary coherent state from any sender to any receiver chosen from N (= 2, 3, 4, 8, 20 and 50) parties. A fidelity $F > 0.5$ ("quantum") requires N-partite entanglement, here produced with N equally squeezed single-mode states. For $N \geq 30$, the fidelity of our protocol becomes classical for some squeezing, but always exceeds 0.5 for sufficiently *small* squeezing and approaches 1 for infinite squeezing.

This fidelity is shown in Fig. IV.10 for squeezing in dB. We obtain $F_{\text{opt}} > 1/2$ for any $r_1 > 0$ and *arbitrary* N. In the limit $r_1 \to \infty$, we find the maximum fidelity $F = 1/\sqrt{2}$ for any N.

By first considering only the momentum detections at the $N - 2$ stations without the teleportation from k to l, we can give our protocol also the quality of a "distillation" of bipartite entanglement from N-partite entanglement [11].

The bipartite entanglement can be verified experimentally by applying suffi-

[11] For infinite squeezing, this is analogous to the retrieval of a Bell state from a qubit GHZ state through local measurements in the *conjugate* basis considered in Eq. (II.22). Here, the conjugate basis of the position basis is the momentum basis.

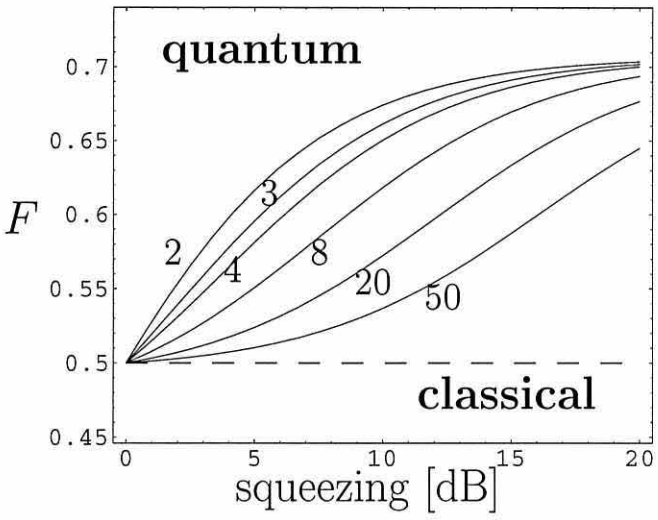

Figure IV.10: One squeezed state: Optimized fidelity for the teleportation of an arbitrary coherent state from any sender to any receiver chosen from N (= 2, 3, 4, 8, 20 and 50) parties. A fidelity $F > 0.5$ ("quantum") requires N-partite entanglement, here produced with *one* single-mode squeezed state.

cient inseparability criteria through detections of the combined modes [196] or through quantum teleportation as shown. The sufficient inseparability criteria applied to the *ensemble* state (with N equal squeezers) after that distillation and after the optimum displacements yield for the necessary sum condition [see Eq. (III.11)]

$$\begin{aligned}\langle(\hat{x}_k-\hat{x}_l)^2\rangle+\langle(\hat{p}_k+\hat{p}_l')^2\rangle &= \langle(\hat{x}_k-\hat{x}_l)^2\rangle+\left\langle\left(\hat{p}_k+\hat{p}_l+g^{(N)}\sum_{j\neq k,l}^{N}\hat{p}_j\right)^2\right\rangle \\ &= \frac{e^{-2r}}{2}+\frac{N}{2[2e^{+2r}+(N-2)e^{-2r}]}\geq 1, \quad \text{(IV.119)}\end{aligned}$$

and for the necessary product condition [see Eq. (III.13)]

$$\langle(\hat{x}_k-\hat{x}_l)^2\rangle\langle(\hat{p}_k+\hat{p}_l')^2\rangle = \frac{Ne^{-2r}}{2e^{+2r}+(N-2)e^{-2r}}\geq 1. \quad \text{(IV.120)}$$

The product condition is violated for any $r > 0$ and any N, proving the insepara-

bility of the "distilled" bipartite state in that case. The sum condition, however, is violated for any $r > 0$ only if $N \leq 17$. For $N \geq 18$, there are squeezing values $r > 0$ that do not yield violations of the sum condition. Nevertheless, we still obtain nonclassical fidelities when using the state for coherent-state teleportation, $F_{\text{opt}} > 1/2$ for any $r > 0$ if $N \leq 29$. Here we encounter another example of quantum states for which the sufficient inseparability criteria yield different results. These quantum states are Gaussian states whose correlation matrix is not in the standard form $V_{II}^{(2)}$ of Eq. (III.5). The sufficient and necessary separability condition for Gaussian states in Eq. (III.9) is therefore not directly applicable and differs from the necessary separability condition for arbitrary states in Eq. (III.11).

What about the purity of the bipartite entangled states distilled from the N-partite entangled states? This question is particularly interesting, because we know that bipartite mixed-state entanglement is already present in any pair of modes of the N-partite entangled states without any measurements (as shown for three parties in chapter III). Does the classical information gain through the detection of the remaining modes enhance the entanglement in any pair of modes? Is the bipartite mixed-state entanglement existing in any pair literally "distilled", i.e., purified through the detections? If yes, can we retrieve that distilled pure-state entanglement of the reduced single-shot state also on average in the ensemble state? In fact, we can, and we show now that the optimum gain in the displacements by the $N - 2$ momenta ensures that the optimum entanglement is recovered in the ensemble state, very much like in the previously discussed entanglement swapping scheme.

Let us consider the tripartite state given by the Wigner function $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (III.43) for $N = 3$. We can describe the momentum detection of mode 3

by integrating over its position,

$$\int dx_3\, W_{\text{out}}(\mathbf{x},\mathbf{p}) \;\propto\; \exp\left\{\frac{2}{3}\frac{(e^{+2r}-e^{-2r})^2}{e^{-2r}+2e^{+2r}}(x_1+x_2)^2 \right. \\ -\frac{2}{3}e^{-2r}[(x_1+x_2)^2+(p_1-p_2)^2+(p_2-p_3)^2+(p_1-p_3)^2] \\ \left. -\frac{2}{3}e^{+2r}[(p_1+p_2+p_3)^2+(x_1-x_2)^2+x_1^2+x_2^2]\right\}. \tag{IV.121}$$

Applying the following variable substitutions for the momenta of modes 1 and 2,

$$p_1 = p_1' - g^{(3)}\, p_3/2, \quad p_2 = p_2' - g^{(3)}\, p_3/2, \tag{IV.122}$$

with $g^{(3)}$ from Eq. (IV.106), converts the reduced Wigner function of Eq. (IV.121) into (apart from normalization terms containing p_3^2, assumed to be constant in a single shot)

$$W(x_1,p_1',x_2,p_2') \;\propto\; \exp\left\{\frac{2}{3}\frac{(e^{+2r}-e^{-2r})^2}{e^{-2r}+2e^{+2r}}(x_1+x_2)^2 \right. \\ -\frac{2}{3}e^{-2r}[(x_1+x_2)^2+(p_1'-p_2')^2+{p_1'}^2+{p_2'}^2] \\ \left. -\frac{2}{3}e^{+2r}[(p_1'+p_2')^2+(x_1-x_2)^2+x_1^2+x_2^2]\right\}. \tag{IV.123}$$

Similar to the entanglement swapping scheme, the "right gain" eliminates from the reduced Wigner function all terms containing correlations of the momenta of modes 1 and 2 with the potentially random, detected momentum p_3 (terms containing p_1p_3 or p_2p_3).

From the Gaussian two-mode Wigner function in Eq. (IV.123), we can now

extract the bipartite correlation matrix

$$V^{(2)} = \frac{1}{4}\begin{pmatrix} \frac{1}{3}e^{+2r} + \frac{2}{3}e^{-2r} & 0 & \frac{1}{3}(e^{+2r} - e^{-2r}) & 0 \\ 0 & \frac{e^{+4r}+2}{e^{-2r}+2e^{+2r}} & 0 & \frac{1-e^{+4r}}{e^{-2r}+2e^{+2r}} \\ \frac{1}{3}(e^{+2r} - e^{-2r}) & 0 & \frac{1}{3}e^{+2r} + \frac{2}{3}e^{-2r} & 0 \\ 0 & \frac{1-e^{+4r}}{e^{-2r}+2e^{+2r}} & 0 & \frac{e^{+4r}+2}{e^{-2r}+2e^{+2r}} \end{pmatrix}. \tag{IV.124}$$

The purity test in chapter I after rearranging this correlation matrix to the form $\tilde{V}^{(2)}$ indeed confirms: the above state is a well-defined pure quantum state. However, it cannot be written in the form of a two-mode squeezed state, and hence its entanglement cannot be simply quantified via the Schmidt decomposition in Fock space. Nevertheless, it contains the maximum amount of entanglement distillable, since it is the reduced state for any single shot apart from local fixed momentum displacements. This entanglement can be retrieved also on average in the distilled ensemble state, when momentum displacements with the "right gain" are performed corresponding to the substitutions in Eq. (IV.122).

Apparently, a pure ensemble state after the distillation requires momentum displacements of both modes 1 and 2. However, the fidelity attainable in coherent-state teleportation when the distilled state of modes 1 and 2 is used [after applying momentum displacements by p_3 of both modes with gain $g^{(3)}/2$ for $g^{(3)}$ from Eq. (IV.106)] is the same as the fidelity we obtained previously after displacing only one mode with gain $g^{(3)}$ [see Eq. (IV.104) etc.]. Just like in the entanglement swapping scheme, purity of the output ensemble state is not necessarily required to ensure the optimum performance in quantum teleportation, but only purity guarantees the optimum entanglement for the distilled state.

For $N = 4$ and $N = 5$, we have also calculated the correlation matrix of the bipartite state distilled from the N-partite state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ in Eq. (III.43) via momentum detections of $N - 2$ modes. It is the reduced state for any single shot (after integrating over x_3, x_4,...,x_N) apart from local fixed momentum

displacements given by the substitutions

$$\begin{aligned} p_1 &= p_1' - g^{(N)}\, p_3/2 - g^{(N)}\, p_4/2 - \cdots - g^{(N)}\, p_N/2, \\ p_2 &= p_2' - g^{(N)}\, p_3/2 - g^{(N)}\, p_4/2 - \cdots - g^{(N)}\, p_N/2, \end{aligned} \tag{IV.125}$$

with $g^{(N)}$ of Eq. (IV.115). Simultaneously, it is the optimum pure ensemble state distillable on average using momentum detections and the displacements according to Eq. (IV.125) with the optimum gain $g^{(N)}$ in Eq. (IV.115). The calculation for $N = 4$ and $N = 5$ yields the following correlation matrix of that state,

$$V^{(2)} = \frac{1}{4} \times \begin{pmatrix} \frac{1}{N}e^{+2r} + \frac{N-1}{N}e^{-2r} & 0 & \frac{1}{N}(e^{+2r} - e^{-2r}) & 0 \\ 0 & \frac{e^{+4r}+N-1}{(N-2)e^{-2r}+2e^{+2r}} & 0 & \frac{1-e^{+4r}}{(N-2)e^{-2r}+2e^{+2r}} \\ \frac{1}{N}(e^{+2r} - e^{-2r}) & 0 & \frac{1}{N}e^{+2r} + \frac{N-1}{N}e^{-2r} & 0 \\ 0 & \frac{1-e^{+4r}}{(N-2)e^{-2r}+2e^{+2r}} & 0 & \frac{e^{+4r}+N-1}{(N-2)e^{-2r}+2e^{+2r}} \end{pmatrix}. \tag{IV.126}$$

This state is a well-defined pure state *for any* N according to the purity test in chapter I. Therefore, we conjecture that it represents the correct reduced state (apart from local fixed momentum displacements) and the correct optimum ensemble state distilled from $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ of Eq. (III.43) *for any* N.

Apparently, the mixed-state entanglement already present in any pair of modes of the N-partite entangled state $W_{\text{out}}(\mathbf{x}, \mathbf{p})$ of Eq. (III.43) can indeed be "purified" by gaining classical information through measurements of the remaining modes. Without this distillation, how good would the performance in quantum teleportation be if the existing mixed-state entanglement was used? We can calculate the corresponding fidelity for the teleportation of arbitrary coherent states using the Heisenberg operator equations for the N-partite state in Eq. (III.37), those of the teleportation protocol in Eq. (IV.2), and those for the

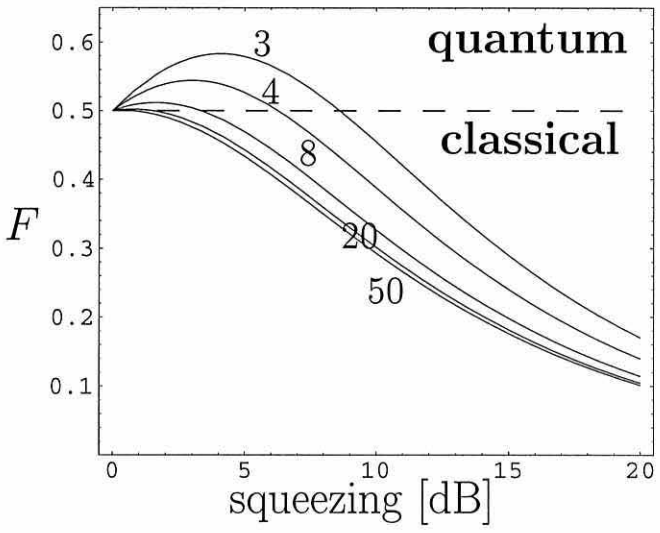

Figure IV.11: Fidelity for the teleportation of an arbitrary coherent state from any sender to any receiver chosen from N (= 2, 3, 4, 8, 20 and 50) parties. The bipartite entanglement used is not distilled from the N-partite entangled state via $N-2$ measurements as that in Fig IV.9, but it is rather the mixed-state entanglement of any pair of modes already present without detections (after tracing out $N-2$ modes). The N-partite entangled state here is the one produced with N equal squeezers. For sufficiently small squeezing, a fidelity $F > 0.5$ ("quantum") can still be achieved.

fidelity in Eq. (IV.50) with gain $g = 1$. The fidelities we obtain are

$$F = \left\{1 + e^{-2r}\right\}^{-1/2} \left\{1 + [2e^{-2r} + (N-2)e^{+2r}]/N\right\}^{-1/2}, \quad \text{(IV.127)}$$

with entanglement built from N equally squeezed states (squeezing r), and

$$F = \left\{2 + [4e^{-2r_1} + 2(N-2)]/N\right\}^{-1/2}, \quad \text{(IV.128)}$$

using entanglement produced with one squeezed state (squeezing r_1).

Figure IV.11 and Fig. IV.12 show these fidelities as a function of the squeezing in dB. For N-partite entanglement produced with N largely squeezed states, the

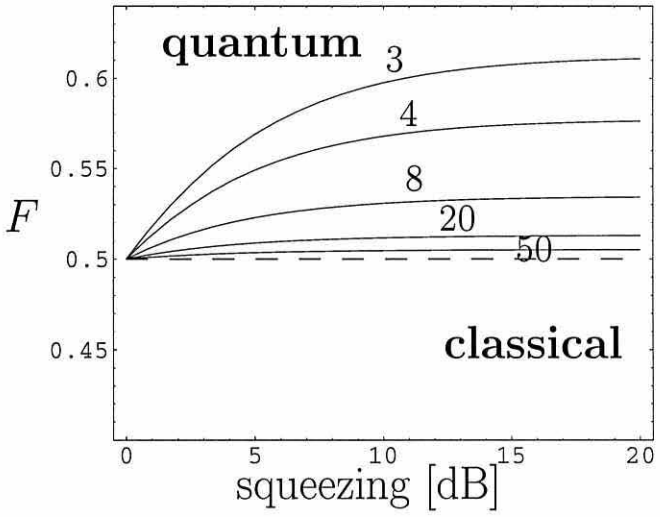

Figure IV.12: Fidelity for the teleportation of an arbitrary coherent state from any sender to any receiver chosen from N (= 2, 3, 4, 8, 20 and 50) parties. The bipartite entanglement used is not distilled from the N-partite entangled state via $N-2$ measurements as that in Fig IV.10, but it is rather the mixed-state entanglement of any pair of modes already present without detections (after tracing out $N-2$ modes). The N-partite entangled state here is the one produced with only one squeezed state. A fidelity $F > 0.5$ ("quantum") is achieved for any nonzero squeezing.

fidelity obtained without distillation drops far below 1/2. The fidelity is significantly enhanced through distillation in this case. For N-partite entanglement generated with N modestly squeezed states and for that produced with only one squeezed state, the enhancement through distillation is less significant.

In summary, we have considered a quantum teleportation network using members of the family of continuous-variable multipartite entangled states presented in chapter III. In order to achieve quantum teleportation with good fidelity from any mode to any other mode, pure-state bipartite entanglement can be distilled from the multipartite states. Like in the entanglement swapping scheme, we

have found that this pure-state entanglement can be retrieved also on average, provided the local displacements based on the $N-2$ momentum measurement results are performed with optimum gain. It seems to be a general feature of the manipulation of the nonmaximally entangled continuous-variable states that such an optimum gain value exists for any local displacements based on local measurement results. Only this gain guarantees the optimal manipulation of the ensemble states. We finally note that the "unbiased" N-mode states of the family of continuous-variable multipartite entangled states (see chapter III) may yield better teleportation fidelities, though they are equivalent under local squeezing operations to the states that we have used. This conjecture applies especially to coherent-state teleportation which is optimized for excess noise symmetric in x and p.

j Broadband teleportation and entanglement swapping

In this section, we extend the protocols for continuous-variable quantum teleportation from single modes to electromagnetic fields having finite bandwidth. We also include a broadband description of the continuous-variable entanglement swapping scheme. This section is based on van Loock, Braunstein, and Kimble [136].

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. (III.108). The incoming electromagnetic field to be teleported, $\hat{E}_{\rm in}(z,t) = \hat{E}_{\rm in}^{(+)}(z,t) + \hat{E}_{\rm in}^{(-)}(z,t)$, traveling in the positive-z direction and having a single unspecified polarization, can be described by its positive-frequency part

$$\hat{E}_{\rm in}^{(+)}(z,t) \;=\; [\hat{E}_{\rm in}^{(-)}(z,t)]^{\dagger} = \int_{\rm W} d\omega \frac{1}{\sqrt{2\pi}} \left(\frac{u\hbar\omega}{2cA_{\rm tr}}\right)^{1/2} \hat{b}_{\rm in}(\omega) e^{-i\omega(t-z/c)}. \tag{IV.129}$$

The integral runs over a relevant bandwidth W centered on ω_0, and the other parameters are the same as in Eq. (I.28). The annihilation and creation opera-

tors $\hat{b}_{\rm in}(\omega)$ and $\hat{b}^\dagger_{\rm in}(\omega)$ satisfy the commutation relations $[\hat{b}_{\rm in}(\omega), \hat{b}_{\rm in}(\omega')] = 0$ and $[\hat{b}_{\rm in}(\omega), \hat{b}^\dagger_{\rm in}(\omega')] = \delta(\omega - \omega')$. The incoming electromagnetic field may now be written in a rotating frame,

$$\begin{aligned} \hat{B}_{\rm in}(t) &= \hat{X}_{\rm in}(t) + i\hat{P}_{\rm in}(t) \\ &= [\hat{x}_{\rm in}(t) + i\hat{p}_{\rm in}(t)]e^{i\omega_0 t} = \hat{b}_{\rm in}(t)e^{i\omega_0 t}, \end{aligned} \tag{IV.130}$$

as in Eq. (III.89) with

$$\hat{B}_{\rm in}(\Omega) = \frac{1}{\sqrt{2\pi}} \int dt \hat{B}_{\rm in}(t) e^{i\Omega t}, \tag{IV.131}$$

and commutation relations $[\hat{B}_{\rm in}(\Omega), \hat{B}_{\rm in}(\Omega')] = 0$, $[\hat{B}_{\rm in}(\Omega), \hat{B}^\dagger_{\rm in}(\Omega')] = \delta(\Omega - \Omega')$.

Of course, the unknown input field is not completely arbitrary. In the case of an EPR state from the nondegenerate parametric amplifier (NOPA), we will see that for successful quantum teleportation, the center of the input field's spectral range W should be around the NOPA's central frequency ω_0 (half the pump frequency of the NOPA). Further, as we shall see, its spectral width should be small with respect to the NOPA bandwidth to benefit from the EPR correlations of the NOPA output. As for the transverse structure and the single polarization of the input field, we assume that both are known to all participants.

In spite of these complications, the teleportation protocol is performed in a fashion almost identical to the zero-bandwidth case. The EPR state of modes 1 and 2 is produced either directly as the NOPA output or by combining two independently squeezed beams, as discussed in chapter III. Mode 1 is sent to Alice and mode 2 is sent to Bob where for the case of the NOPA, these modes correspond to two orthogonal polarizations. Alice arranges to combine mode 1 with the unknown input field at a 50:50 beam splitter, yielding for the relevant quadratures

$$\begin{aligned} \hat{X}_{\rm u}(\Omega) &= \frac{1}{\sqrt{2}}\hat{X}_{\rm in}(\Omega) - \frac{1}{\sqrt{2}}\hat{X}_1(\Omega), \\ \hat{P}_{\rm v}(\Omega) &= \frac{1}{\sqrt{2}}\hat{P}_{\rm in}(\Omega) + \frac{1}{\sqrt{2}}\hat{P}_1(\Omega). \end{aligned} \tag{IV.132}$$

Using Eq. (IV.132) we will find it useful to write the quadrature operators of Bob's mode 2 as

$$\begin{aligned}
\hat{X}_2(\Omega) &= \hat{X}_{\rm in}(\Omega) - [\hat{X}_1(\Omega) - \hat{X}_2(\Omega)] - \sqrt{2}\hat{X}_{\rm u}(\Omega) \\
&= \hat{X}_{\rm in}(\Omega) - \sqrt{2}S_-(\Omega)\hat{\tilde{X}}_2^{(0)}(\Omega) - \sqrt{2}\hat{X}_{\rm u}(\Omega), \\
\hat{P}_2(\Omega) &= \hat{P}_{\rm in}(\Omega) + [\hat{P}_1(\Omega) + \hat{P}_2(\Omega)] - \sqrt{2}\hat{P}_{\rm v}(\Omega) \\
&= \hat{P}_{\rm in}(\Omega) + \sqrt{2}S_-(\Omega)\hat{\tilde{P}}_1^{(0)}(\Omega) - \sqrt{2}\hat{P}_{\rm v}(\Omega). \qquad \text{(IV.133)}
\end{aligned}$$

Here we have used Eq. (III.108). Alice's Bell measurement now means the detection of the beams "u" and "v": the photocurrent operators for the two homodyne detections, $\hat{i}_{\rm u}(t) \propto |E_{\rm LO}^X|\hat{X}_{\rm u}(t)$ and $\hat{i}_{\rm v}(t) \propto |E_{\rm LO}^P|\hat{P}_{\rm v}(t)$, can be written (without loss of generality we assume $\Omega > 0$) as

$$\begin{aligned}
\hat{i}_{\rm u}(t) &\propto |E_{\rm LO}^X| \int_{\rm W} d\Omega\, h_{\rm el}(\Omega) \left[\hat{X}_{\rm u}(\Omega)e^{-i\Omega t} + \hat{X}_{\rm u}^\dagger(\Omega)e^{i\Omega t}\right], \\
\hat{i}_{\rm v}(t) &\propto |E_{\rm LO}^P| \int_{\rm W} d\Omega\, h_{\rm el}(\Omega) \left[\hat{P}_{\rm v}(\Omega)e^{-i\Omega t} + \hat{P}_{\rm v}^\dagger(\Omega)e^{i\Omega t}\right], \qquad \text{(IV.134)}
\end{aligned}$$

with a noiseless, classical local oscillator (LO) and $h_{\rm el}(\Omega)$ representing the detectors' responses within their electronic bandwidths $\Delta\Omega_{\rm el}$: $h_{\rm el}(\Omega) = 1$ for $\Omega \leq \Delta\Omega_{\rm el}$ and zero otherwise. We assume that the relevant bandwidth W ($\sim$ MHz) is fully covered by the electronic bandwidth of the detectors ($\sim$ GHz). Therefore, $h_{\rm el}(\Omega) \approx 1$ in Eq. (IV.134) 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. The whole feedforward process, continuously performed in the time domain (i.e., essentially performed every inverse-bandwidth time), includes Alice's detections, her classical transmission and the corresponding amplitude and phase modulations of Bob's EPR beam. Any *relative* delays between the classical information conveyed by Alice and Bob's EPR beam must be such that $\Delta t \ll 1/\Delta\Omega$ with the inverse bandwidth of the EPR source $1/\Delta\Omega$. Expressed in the frequency

domain, the final modulations can be described by the classical "displacements"

$$\begin{aligned} \hat{X}_2(\Omega) \longrightarrow \hat{X}_{\rm tel}(\Omega) &= \hat{X}_2(\Omega) + g(\Omega)\sqrt{2}X_{\rm u}(\Omega), \\ \hat{P}_2(\Omega) \longrightarrow \hat{P}_{\rm tel}(\Omega) &= \hat{P}_2(\Omega) + g(\Omega)\sqrt{2}P_{\rm v}(\Omega). \end{aligned} \tag{IV.135}$$

The parameter $g(\Omega)$ is the gain, now in general depending on Ω.

For $g(\Omega) \equiv 1$, Bob's displacements in Eq. (IV.135) eliminate $\hat{X}_{\rm u}(\Omega)$ and $\hat{P}_{\rm v}(\Omega)$ in Eq. (IV.133). The same applies to the Hermitian conjugate versions of Eq. (IV.133) and Eq. (IV.135). With unit gain the teleported field is

$$\begin{aligned} \hat{X}_{\rm tel}(\Omega) &= \hat{X}_{\rm in}(\Omega) - \sqrt{2}S_-(\Omega)\hat{\tilde{X}}_2^{(0)}(\Omega), \\ \hat{P}_{\rm tel}(\Omega) &= \hat{P}_{\rm in}(\Omega) + \sqrt{2}S_-(\Omega)\hat{\tilde{P}}_1^{(0)}(\Omega). \end{aligned} \tag{IV.136}$$

While for an arbitrary gain $g(\Omega)$, the teleported field becomes

$$\begin{aligned} \hat{X}_{\rm tel}(\Omega) = g(\Omega)\hat{X}_{\rm in}(\Omega) &- \frac{g(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{X}}_1^{(0)}(\Omega) \\ &- \frac{g(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{X}}_2^{(0)}(\Omega), \\ \hat{P}_{\rm tel}(\Omega) = g(\Omega)\hat{P}_{\rm in}(\Omega) &+ \frac{g(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{P}}_2^{(0)}(\Omega) \\ &+ \frac{g(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{P}}_1^{(0)}(\Omega). \end{aligned} \tag{IV.137}$$

In general, these equations contain non-Hermitian operators with non-real coefficients. Let us assume an EPR state from the NOPA, $S_\pm(\Omega) = \mathcal{G}(\Omega) \pm \mathcal{F}(\Omega)$ [Eq. (III.105)]. In the zero-bandwidth limit, the quadrature operators are Hermitian and the coefficients in Eq. (IV.136) and Eq. (IV.137) are real. For $\Omega \to 0$ and $g(\Omega) = 1$, the teleported quadratures computed from the above equations become $\hat{X}_{\rm tel} = \hat{X}_{\rm in}$ and $\hat{P}_{\rm tel} = \hat{P}_{\rm in}$, if $\kappa \to \gamma/2$ and hence $[\mathcal{G}(\Omega) - \mathcal{F}(\Omega)] \to 0$ (infinite squeezing). Apparently, in unit-gain teleportation, the complete disappearance of the two classical "quduties" for perfect teleportation requires $\Omega = 0$ (for an EPR state generated from a NOPA). Does this mean an increasing bandwidth

always leads to deteriorating quantum teleportation? In order to make quantitative statements we calculate the spectral variances of the teleported quadratures for a coherent-state input to obtain a "fidelity spectrum".

Let us employ teleportation equations for the real and imaginary parts of the non-Hermitian quadrature operators. In order to achieve nonzero average fidelity when teleporting fields with coherent amplitude, we assume $g(\Omega) \equiv 1$. According to Eq. (IV.136), the real and imaginary parts of the teleported quadratures are

$$\begin{aligned}
\mathrm{Re}\hat{X}_{\mathrm{tel}}(\Omega) &= \mathrm{Re}\hat{X}_{\mathrm{in}}(\Omega) - \sqrt{2}\mathrm{Re}[S_-(\Omega)]\mathrm{Re}\hat{\tilde{X}}_2^{(0)}(\Omega) + \sqrt{2}\mathrm{Im}[S_-(\Omega)]\mathrm{Im}\hat{\tilde{X}}_2^{(0)}(\Omega), \\
\mathrm{Re}\hat{P}_{\mathrm{tel}}(\Omega) &= \mathrm{Re}\hat{P}_{\mathrm{in}}(\Omega) + \sqrt{2}\mathrm{Re}[S_-(\Omega)]\mathrm{Re}\hat{\tilde{P}}_1^{(0)}(\Omega) - \sqrt{2}\mathrm{Im}[S_-(\Omega)]\mathrm{Im}\hat{\tilde{P}}_1^{(0)}(\Omega), \\
\mathrm{Im}\hat{X}_{\mathrm{tel}}(\Omega) &= \mathrm{Im}\hat{X}_{\mathrm{in}}(\Omega) - \sqrt{2}\mathrm{Im}[S_-(\Omega)]\mathrm{Re}\hat{\tilde{X}}_2^{(0)}(\Omega) - \sqrt{2}\mathrm{Re}[S_-(\Omega)]\mathrm{Im}\hat{\tilde{X}}_2^{(0)}(\Omega), \\
\mathrm{Im}\hat{P}_{\mathrm{tel}}(\Omega) &= \mathrm{Im}\hat{P}_{\mathrm{in}}(\Omega) + \sqrt{2}\mathrm{Im}[S_-(\Omega)]\mathrm{Re}\hat{\tilde{P}}_1^{(0)}(\Omega) + \sqrt{2}\mathrm{Re}[S_-(\Omega)]\mathrm{Im}\hat{\tilde{P}}_1^{(0)}(\Omega).
\end{aligned} \tag{IV.138}$$

Their only nontrivial commutators are

$$[\mathrm{Re}\hat{X}_j(\Omega), \mathrm{Re}\hat{P}_j(\Omega')] = [\mathrm{Im}\hat{X}_j(\Omega), \mathrm{Im}\hat{P}_j(\Omega')] = \frac{i}{4}\,\delta(\Omega - \Omega'), \tag{IV.139}$$

where we have used Eq. (III.94) and $[\hat{B}_j(\Omega), \hat{B}_j^\dagger(\Omega')] = \delta(\Omega - \Omega')$.

We define spectral variances as in Eq. (IV.30),

$$\frac{\langle \Delta[\mathrm{Re}\hat{X}_{\mathrm{tel}}(\Omega) - \mathrm{Re}\hat{X}_{\mathrm{in}}(\Omega)]\Delta[\mathrm{Re}\hat{X}_{\mathrm{tel}}(\Omega') - \mathrm{Re}\hat{X}_{\mathrm{in}}(\Omega')]\rangle}{\langle (\Delta \mathrm{Re}\hat{X})^2\rangle_{\mathrm{vacuum}}} \equiv \delta(\Omega - \Omega') V_{\mathrm{tel,in}}^{\mathrm{Re}\hat{X}}(\Omega). \tag{IV.140}$$

We similarly define $V_{\mathrm{tel,in}}^{\mathrm{Re}\hat{P}}(\Omega)$, $V_{\mathrm{tel,in}}^{\mathrm{Im}\hat{X}}(\Omega)$ and $V_{\mathrm{tel,in}}^{\mathrm{Im}\hat{P}}(\Omega)$ with $\mathrm{Re}\hat{X} \to \mathrm{Re}\hat{P}$ etc. throughout.

From Eq. (IV.138), we obtain

$$V_{\mathrm{tel,in}}^{\mathrm{Re}\hat{X}}(\Omega) = V_{\mathrm{tel,in}}^{\mathrm{Re}\hat{P}}(\Omega) = V_{\mathrm{tel,in}}^{\mathrm{Im}\hat{X}}(\Omega) = V_{\mathrm{tel,in}}^{\mathrm{Im}\hat{P}}(\Omega) = 2\,|S_-(\Omega)|^2. \tag{IV.141}$$

Here we have used the facts that

$$\begin{aligned} \langle \Delta \mathrm{Re}\hat{\tilde{X}}_j^{(0)}(\Omega) \Delta \mathrm{Re}\hat{\tilde{X}}_j^{(0)}(\Omega') \rangle &= \delta(\Omega - \Omega') \langle (\Delta \mathrm{Re}\hat{X})^2 \rangle_{\mathrm{vacuum}} \\ = \langle \Delta \mathrm{Im}\hat{\tilde{X}}_j^{(0)}(\Omega) \Delta \mathrm{Im}\hat{\tilde{X}}_j^{(0)}(\Omega') \rangle &= \delta(\Omega - \Omega') \langle (\Delta \mathrm{Im}\hat{X})^2 \rangle_{\mathrm{vacuum}}, \end{aligned} \tag{IV.142}$$

and similarly for the other quadrature, and further that

$$\langle \Delta \mathrm{Re}\hat{\tilde{X}}_j^{(0)}(\Omega) \Delta \mathrm{Im}\hat{\tilde{X}}_j^{(0)}(\Omega') \rangle = \langle \Delta \mathrm{Re}\hat{\tilde{P}}_j^{(0)}(\Omega) \Delta \mathrm{Im}\hat{\tilde{P}}_j^{(0)}(\Omega') \rangle = 0 \ . \tag{IV.143}$$

Thus, 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. (III.107). The excess noise in each teleported quadrature after the teleportation process is, relative to the vacuum noise, *twice* the squeezing spectrum $|S_-(\Omega)|^2$ of Eq. (III.106).

We may also obtain these results by directly defining

$$\frac{\langle \Delta[\hat{X}_{\mathrm{tel}}^\dagger(\Omega) - \hat{X}_{\mathrm{in}}^\dagger(\Omega)] \Delta[\hat{X}_{\mathrm{tel}}(\Omega') - \hat{X}_{\mathrm{in}}(\Omega')] \rangle}{\langle (\Delta \hat{X})^2 \rangle_{\mathrm{vacuum}}} \equiv \delta(\Omega - \Omega') V_{\mathrm{tel,in}}^{\hat{X}}(\Omega). \tag{IV.144}$$

We similarly define $V_{\mathrm{tel,in}}^{\hat{P}}(\Omega)$ with $\hat{X} \to \hat{P}$ throughout. Using Eq. (IV.136), these variances become for $g(\Omega) \equiv 1$

$$V_{\mathrm{tel,in}}^{\hat{X}}(\Omega) = V_{\mathrm{tel,in}}^{\hat{P}}(\Omega) = 2\,|S_-(\Omega)|^2. \tag{IV.145}$$

We shall now calculate some limits for $V_{\mathrm{tel,in}}^{\hat{X}}(\Omega)$ of Eq. (IV.145), assuming an EPR state from the NOPA, $S_-(\Omega) = \mathcal{G}(\Omega) - \mathcal{F}(\Omega)$. Since $V_{\mathrm{tel,in}}^{\hat{X}}(\Omega) = V_{\mathrm{tel,in}}^{\hat{P}}(\Omega)$ and $g(\Omega) \equiv 1$, we can name the limits according to the criterion of Eq. (IV.32).

Classical teleportation, $\kappa \to 0$:

$V_{\mathrm{tel,in}}^{\hat{X}}(\Omega) = 2$, which is independent of the modulation frequency Ω.

Zero-bandwidth quantum teleportation, $\Omega \to 0$, $\kappa > 0$:
$V^{\hat{X}}_{\mathrm{tel,in}}(\Omega) = 2\,[1 - 2\kappa\gamma/(\kappa + \gamma/2)^2]$, and in the ideal case of infinite squeezing $\kappa \to \gamma/2$: $V^{\hat{X}}_{\mathrm{tel,in}}(\Omega) = 0$.
Broadband quantum teleportation, $\Omega > 0$, $\kappa > 0$:
$V^{\hat{X}}_{\mathrm{tel,in}}(\Omega) = 2\,\{1 - 2\kappa\gamma/[(\kappa + \gamma/2)^2 + \Omega^2]\}$, and in the ideal case $\kappa \to \gamma/2$: $V^{\hat{X}}_{\mathrm{tel,in}}(\Omega) = 2\,[\Omega^2/(\gamma^2 + \Omega^2)]$. So it turns out that even for a finite bandwidth ideal quantum teleportation can be approached provided $\Omega \ll \gamma$.

We can express $V^{\hat{X}}_{\mathrm{tel,in}}(\Omega)$ in terms of experimental parameters relevant to a NOPA. For this purpose, we use the dimensionless quantities in Ref. [155],

$$\epsilon = \frac{2\kappa}{\gamma + \rho} = \sqrt{\frac{P_{\mathrm{pump}}}{P_{\mathrm{thres}}}}\ , \quad \omega = \frac{2\Omega}{\gamma + \rho} = \frac{\Omega}{2\pi}\,\frac{2F_{\mathrm{cav}}}{\nu_{\mathrm{FSR}}}\ . \tag{IV.146}$$

Here, P_{pump} is the pump power, P_{thres} is the threshold value, F_{cav} is the measured finesse of the cavity, ν_{FSR} is its free spectral range, and the parameter ρ describes cavity losses (see Fig. III.5). Note that we now use the symbol ω as a normalized modulation frequency in contrast to Eq. (IV.129) (and the following commutators) where it was the actual frequency of the field operators in the non-rotating frame.

The spectral variances for the lossless case ($\rho = 0$) can be written as a function of ϵ and ω, namely

$$V^{\hat{X}}_{\mathrm{tel,in}}(\epsilon, \omega) = V^{\hat{P}}_{\mathrm{tel,in}}(\epsilon, \omega) = 2\,\left[1 - \frac{4\epsilon}{(\epsilon + 1)^2 + \omega^2}\right]. \tag{IV.147}$$

Now, the classical limit is $\epsilon \to 0$ ($V^{\hat{X}}_{\mathrm{tel,in}} = 2$, independent of ω) and the ideal case is $\epsilon \to 1$ [$V^{\hat{X}}_{\mathrm{tel,in}}(\epsilon, \omega) = 2\omega^2/(4+\omega^2)$]. Obviously, perfect quantum teleportation is achieved for $\epsilon \to 1$ and $\omega \to 0$. This limit can also be approached for finite $\Omega \neq 0$ provided $\omega \ll 1$ or $\Omega \ll \gamma$. Note that this condition is not specific to broadband teleportation, but is simply the condition for broadband squeezing, i.e., for the generation of highly squeezed quadratures at nonzero modulation frequencies Ω.

Let us now assume coherent-state inputs at all frequencies Ω in the relevant bandwidth W, $\langle \Delta\hat{X}^{\dagger}_{\mathrm{in}}(\Omega)\Delta\hat{X}_{\mathrm{in}}(\Omega')\rangle = \langle \Delta\hat{P}^{\dagger}_{\mathrm{in}}(\Omega)\Delta\hat{P}_{\mathrm{in}}(\Omega')\rangle = \frac{1}{4}\delta(\Omega - \Omega')$ [with

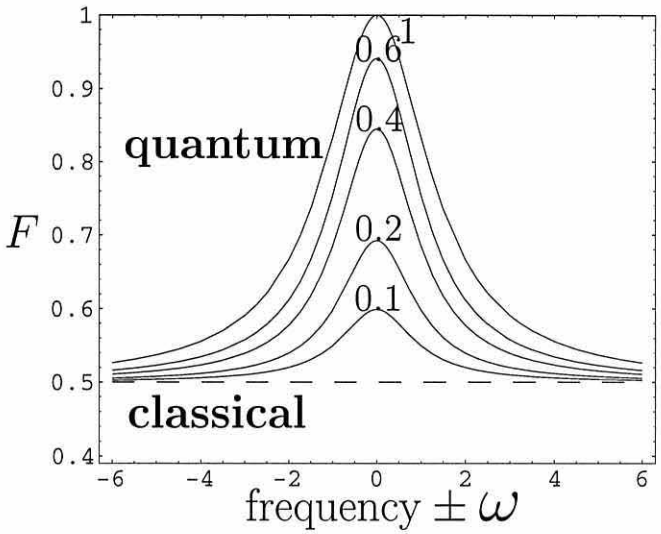

Figure IV.13: Fidelity spectrum of coherent-state teleportation using entanglement from the NOPA. The fidelities here are functions of the normalized modulation frequency $\pm\omega$ for different ϵ (0.1, 0.2, 0.4, 0.6, 1).

$\langle \Delta \mathrm{Re}\hat{X}_{\mathrm{in}}(\Omega) \Delta \mathrm{Re}\hat{X}_{\mathrm{in}}(\Omega') \rangle = \frac{1}{8}\delta(\Omega - \Omega')$ etc.]. In order to obtain a spectrum of the fidelities in Eq. (IV.50) with $g \to g(\Omega) \equiv 1$, we need the spectrum of the Q functions of the teleported field with the spectral variances $\sigma_x(\Omega) = \sigma_p(\Omega) = \frac{1}{2} + \frac{1}{4} V^{\hat{X}}_{\mathrm{tel,in}}(\Omega)$. We obtain the "fidelity spectrum"

$$F(\Omega) = \frac{1}{1 + |S_-(\Omega)|^2} \ . \tag{IV.148}$$

Finally, with the new quantities ϵ and ω, the fidelity spectrum for quantum teleportation of arbitrary broadband coherent states using broadband entanglement from the NOPA is given by

$$F(\epsilon, \omega) = \left[2 - \frac{4\epsilon}{(\epsilon + 1)^2 + \omega^2} \right]^{-1} \ . \tag{IV.149}$$

For different values of ϵ, the spectrum of fidelities is shown in Fig. IV.13. From the single-mode protocol (with ideal detectors), we know that any nonzero squeezing enables quantum teleportation and coherent-state inputs can be teleported with $F = F_{\mathrm{av}} > 1/2$ for any $r > 0$. Correspondingly, the fidelity from

Eq. (IV.149) exceeds 1/2 for any nonzero ϵ at all finite frequencies, as, provided $\epsilon > 0$, there is no squeezing at all only when $\omega \to \infty$. However, we had assumed [see after Eq. (III.94): $\Omega \ll \omega_0$] modulation frequencies Ω much smaller than the NOPA center frequency ω_0. In fact, for $\Omega \to \omega_0$, squeezing becomes impossible at the frequency Ω [56]. Within the region $\Omega \ll \omega_0$, the squeezing bandwith is limited and hence so is the bandwith of quantum teleportation $\Delta\omega \equiv 2\omega_{\max}$ where $F(\omega) \approx 1/2$ (< 0.51) for all $\omega > \omega_{\max}$ and $F(\omega) > 1/2$ (≥ 0.51) for all $\omega \leq \omega_{\max}$. According to Fig. IV.13, we could say that the "effective teleportation bandwidth" is just about $\Delta\omega \approx 5.8$ ($\epsilon = 0.1$), $\Delta\omega \approx 8.6$ ($\epsilon = 0.2$), $\Delta\omega \approx 12.4$ ($\epsilon = 0.4$), $\Delta\omega \approx 15.2$ ($\epsilon = 0.6$) and $\Delta\omega \approx 19.6$ ($\epsilon = 1$). The maximum fidelities at frequency $\omega = 0$ are $F_{\max} \approx 0.6$ ($\epsilon = 0.1$), $F_{\max} \approx 0.69$ ($\epsilon = 0.2$), $F_{\max} \approx 0.84$ ($\epsilon = 0.4$), $F_{\max} \approx 0.94$ ($\epsilon = 0.6$) and, of course, $F_{\max} = 1$ ($\epsilon = 1$).

As discussed for single modes, we particularly want our teleportation device to be capable of teleporting entanglement. In the Heisenberg picture, the broadband extension of that entanglement swapping is straightforward. Before any detections (see Fig. IV.3), Alice (mode 1) and Claire (mode 2) share the broadband two-mode squeezed state of Eq. (III.108), whereas Claire (mode 3) and Bob (mode 4) share the corresponding entangled state of modes 3 and 4 given by

$$\begin{aligned}
\hat{X}_3(\Omega) &= \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{X}}_3^{(0)}(\Omega) + \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{X}}_4^{(0)}(\Omega), \\
\hat{P}_3(\Omega) &= \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{P}}_3^{(0)}(\Omega) + \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{P}}_4^{(0)}(\Omega), \\
\hat{X}_4(\Omega) &= \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{X}}_3^{(0)}(\Omega) - \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{X}}_4^{(0)}(\Omega), \\
\hat{P}_4(\Omega) &= \frac{1}{\sqrt{2}} S_-(\Omega) \hat{\tilde{P}}_3^{(0)}(\Omega) - \frac{1}{\sqrt{2}} S_+(\Omega) \hat{\tilde{P}}_4^{(0)}(\Omega). \qquad \text{(IV.150)}
\end{aligned}$$

Let us interpret the entanglement swapping here as the quantum teleportation of mode 2 to mode 4 using the entanglement of modes 3 and 4. This means we want Bob to perform "displacements" based on the classical results of Claire's Bell detection determining $\hat{X}_{\rm u}(\Omega) = [\hat{X}_2(\Omega) - \hat{X}_3(\Omega)]/\sqrt{2}, \hat{P}_{\rm v}(\Omega) = [\hat{P}_2(\Omega) + \hat{P}_3(\Omega)]/\sqrt{2}$. These final "displacements" (amplitude and phase modu-

lations) of mode 4 are crucial in order to reveal the entanglement from entanglement swapping and, for verification, to finally exploit it in a second round of quantum teleportation using the previously unentangled modes 1 and 4. The entire teleportation process with arbitrary gain $g(\Omega)$ that led to Eq. (IV.137), yields now, for the teleportation of mode 2 to mode 4, the teleported mode 4′ [where in Eq. (IV.137) simply $\hat{X}_{\rm tel}(\Omega) \to \hat{X}_4'(\Omega), \hat{P}_{\rm tel}(\Omega) \to \hat{P}_4'(\Omega), \hat{X}_{\rm in}(\Omega) \to \hat{X}_2(\Omega), \hat{P}_{\rm in}(\Omega) \to \hat{P}_2(\Omega), \hat{\tilde{X}}_1^{(0)}(\Omega) \to \hat{\tilde{X}}_3^{(0)}(\Omega), \hat{\tilde{P}}_1^{(0)}(\Omega) \to \hat{\tilde{P}}_3^{(0)}(\Omega), \hat{\tilde{X}}_2^{(0)}(\Omega) \to \hat{\tilde{X}}_4^{(0)}(\Omega), \hat{\tilde{P}}_2^{(0)}(\Omega) \to \hat{\tilde{P}}_4^{(0)}(\Omega)$ and $g(\Omega) \to g_{\rm swap}(\Omega)$],

$$\begin{aligned}
\hat{X}_4'(\Omega) &= \frac{g_{\rm swap}(\Omega)}{\sqrt{2}}[S_+(\Omega)\hat{\tilde{X}}_1^{(0)}(\Omega) - S_-(\Omega)\hat{\tilde{X}}_2^{(0)}(\Omega)] \\
&\quad - \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{X}}_3^{(0)}(\Omega) - \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{X}}_4^{(0)}(\Omega), \\
\hat{P}_4'(\Omega) &= \frac{g_{\rm swap}(\Omega)}{\sqrt{2}}[S_-(\Omega)\hat{\tilde{P}}_1^{(0)}(\Omega) - S_+(\Omega)\hat{\tilde{P}}_2^{(0)}(\Omega)] \\
&\quad + \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{P}}_3^{(0)}(\Omega) + \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{P}}_4^{(0)}(\Omega).
\end{aligned} \tag{IV.151}$$

Provided entanglement swapping is successful, Alice and Bob can use their modes 1 and 4′ for a further quantum teleportation. Assuming unit gain in this "second teleportation", where the unknown input state described by $\hat{X}_{\rm in}(\Omega)$, $\hat{P}_{\rm in}(\Omega)$ is to be teleported, we obtain the teleported field

$$\begin{aligned}
\hat{X}_{\rm tel}(\Omega) &= \hat{X}_{\rm in}(\Omega) + \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{X}}_1^{(0)}(\Omega) - \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{X}}_2^{(0)}(\Omega) \\
&\quad - \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{X}}_3^{(0)}(\Omega) - \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{X}}_4^{(0)}(\Omega), \\
\hat{P}_{\rm tel}(\Omega) &= \hat{P}_{\rm in}(\Omega) + \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{P}}_1^{(0)}(\Omega) - \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{P}}_2^{(0)}(\Omega) \\
&\quad + \frac{g_{\rm swap}(\Omega)+1}{\sqrt{2}}S_-(\Omega)\hat{\tilde{P}}_3^{(0)}(\Omega) + \frac{g_{\rm swap}(\Omega)-1}{\sqrt{2}}S_+(\Omega)\hat{\tilde{P}}_4^{(0)}(\Omega).
\end{aligned} \tag{IV.152}$$

Calculating the fidelity spectrum for coherent-state inputs we find

$$F(\Omega) = \{1 + [g_{\rm swap}(\Omega) - 1]^2 |S_+(\Omega)|^2/2 + [g_{\rm swap}(\Omega) + 1]^2 |S_-(\Omega)|^2/2\}^{-1} . \quad \text{(IV.153)}$$

The optimum gain, depending on the amount of squeezing, that maximizes this fidelity at different frequencies then turns out to be

$$g_{\rm swap}(\Omega) = \frac{|S_+(\Omega)|^2 - |S_-(\Omega)|^2}{|S_+(\Omega)|^2 + |S_-(\Omega)|^2} . \quad \text{(IV.154)}$$

Let us now assume that the broadband entanglement comes from the NOPA (two NOPA's with equal squeezing spectra), $|S_-(\Omega)|^2 \to |S_-(\epsilon,\omega)|^2 = 1 - 4\epsilon/[(\epsilon+1)^2+\omega^2]$, $|S_+(\Omega)|^2 \to |S_+(\epsilon,\omega)|^2 = 1 + 4\epsilon/[(\epsilon-1)^2+\omega^2]$. The optimized fidelity then becomes

$$F_{\rm opt}(\epsilon,\omega) = \left\{1 + 2\,\frac{[(\epsilon+1)^2+\omega^2][(\epsilon-1)^2+\omega^2]}{[(\epsilon+1)^2+\omega^2]^2 + [(\epsilon-1)^2+\omega^2]^2}\right\}^{-1} . \quad \text{(IV.155)}$$

The spectrum of these optimized fidelities is shown in Fig. IV.14 for different ϵ values. Again, we know from the single-mode protocol with ideal detectors that any nonzero squeezing in both initial entanglement sources is sufficient for entanglement swapping to occur. In this case, modes 1 and $4'$ enable quantum teleportation and coherent-state inputs can be teleported with $F = F_{\rm av} > 1/2$. The fidelity of Eq. (IV.155) is $1/2$ for $\epsilon = 0$ and becomes $F_{\rm opt}(\epsilon,\omega) > 1/2$ for any $\epsilon > 0$, provided that ω does not become infinite (but we had assumed $\Omega \ll \omega_0$). In this sense, the squeezing or entanglement bandwidth is preserved through entanglement swapping. At each frequency where the initial states were squeezed and entangled, the output state of modes 1 and $4'$ is also entangled, but with less squeezing and a worse quality of entanglement.

At frequencies with initially very small entanglement, the entanglement becomes even smaller after entanglement swapping, but never vanishes completely (recall the single-mode result for the squeezing emerging from entanglement swapping, $\tanh^2 R = \tanh^4 r$ with equal initial entanglement, $r = r'$). Thus, the effective bandwidth of squeezing or entanglement decreases through entanglement

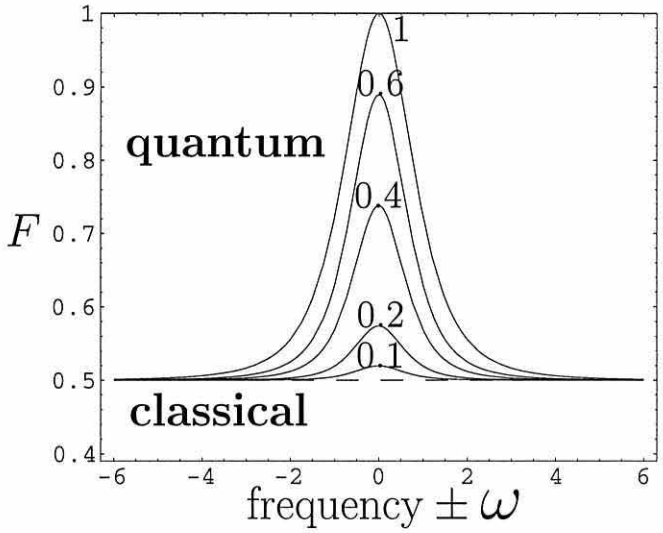

Figure IV.14: Fidelity spectrum of coherent-state teleportation using the output of entanglement swapping with two equally squeezed (entangled) NOPA's. The fidelities here are functions of the normalized modulation frequency $\pm\omega$ for different ϵ (0.1, 0.2, 0.4, 0.6, and 1).

swapping. Then, compared to the teleportation bandwidth using broadband two-mode squeezed states without entanglement swapping, the bandwidth of teleportation using the output of entanglement swapping is effectively smaller. The spectrum of the fidelities in Eq. (IV.155) is narrower and the "effective teleportation bandwidth" is now about $\Delta\omega \approx 1.2$ ($\epsilon = 0.1$), $\Delta\omega \approx 2.6$ ($\epsilon = 0.2$), $\Delta\omega \approx 4.2$ ($\epsilon = 0.4$), $\Delta\omega \approx 5.2$ ($\epsilon = 0.6$) and $\Delta\omega \approx 6.8$ ($\epsilon = 1$). The maximum fidelities at frequency $\omega = 0$ are $F_{\max} \approx 0.52$ ($\epsilon = 0.1$), $F_{\max} \approx 0.57$ ($\epsilon = 0.2$), $F_{\max} \approx 0.74$ ($\epsilon = 0.4$), $F_{\max} \approx 0.89$ ($\epsilon = 0.6$) and, still, $F_{\max} = 1$ ($\epsilon = 1$).

Let us extend the previous calculations and include losses from the NOPA cavity and inefficiencies in Alice's Bell detection. For this purpose, we use Eq. (III.91) for the outgoing NOPA modes. We consider losses and inefficiencies for unit-gain teleportation. By combining the unknown input mode with the NOPA mode 1,

the relevant quadratures from Eq. (IV.132) now become

$$\begin{aligned}\hat{X}_{\rm u}(\Omega) &= \frac{\eta}{\sqrt{2}}\hat{X}_{\rm in}(\Omega) - \frac{\eta}{\sqrt{2}}\hat{X}_1(\Omega) \\ &\quad + \sqrt{\frac{1-\eta^2}{2}}\hat{X}_D^{(0)}(\Omega) + \sqrt{\frac{1-\eta^2}{2}}\hat{X}_E^{(0)}(\Omega), \\ \hat{P}_{\rm v}(\Omega) &= \frac{\eta}{\sqrt{2}}\hat{P}_{\rm in}(\Omega) + \frac{\eta}{\sqrt{2}}\hat{P}_1(\Omega) \\ &\quad + \sqrt{\frac{1-\eta^2}{2}}\hat{P}_F^{(0)}(\Omega) + \sqrt{\frac{1-\eta^2}{2}}\hat{P}_G^{(0)}(\Omega). \end{aligned} \tag{IV.156}$$

The last two terms in each quadrature in Eq. (IV.156) represent additional noise due to homodyne detection inefficiencies (the detector amplitude efficiency η is assumed to be constant over the bandwidth of interest). Using Eq. (IV.156) it is useful to write the quadratures of NOPA mode 2 corresponding to Eq. (III.91) as

$$\begin{aligned}\hat{X}_2(\Omega) &= \hat{X}_{\rm in}(\Omega) - [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)][\hat{X}_1^{(0)}(\Omega) - \hat{X}_2^{(0)}(\Omega)] \\ &\quad - [\bar{\mathcal{G}}(\Omega) - \bar{\mathcal{F}}(\Omega)][\hat{X}_{C,1}^{(0)}(\Omega) - \hat{X}_{C,2}^{(0)}(\Omega)] \\ &\quad + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{X}_D^{(0)}(\Omega) + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{X}_E^{(0)}(\Omega) - \frac{\sqrt{2}}{\eta}\hat{X}_{\rm u}(\Omega), \\ \hat{P}_2(\Omega) &= \hat{P}_{\rm in}(\Omega) + [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)][\hat{P}_1^{(0)}(\Omega) + \hat{P}_2^{(0)}(\Omega)] \\ &\quad + [\bar{\mathcal{G}}(\Omega) - \bar{\mathcal{F}}(\Omega)][\hat{P}_{C,1}^{(0)}(\Omega) + \hat{P}_{C,2}^{(0)}(\Omega)] \\ &\quad + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{P}_F^{(0)}(\Omega) + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{P}_G^{(0)}(\Omega) - \frac{\sqrt{2}}{\eta}\hat{P}_{\rm v}(\Omega), \end{aligned} \tag{IV.157}$$

where now [155]

$$\begin{aligned}\mathcal{G}(\Omega) &= \frac{\kappa^2 + \left(\frac{\gamma-\rho}{2} + i\Omega\right)\left(\frac{\gamma+\rho}{2} - i\Omega\right)}{\left(\frac{\gamma+\rho}{2} - i\Omega\right)^2 - \kappa^2}, \\ \mathcal{F}(\Omega) &= \frac{\kappa\gamma}{\left(\frac{\gamma+\rho}{2} - i\Omega\right)^2 - \kappa^2}, \end{aligned}$$

$$\bar{\mathcal{G}}(\Omega) = \frac{\sqrt{\gamma\rho}\left(\frac{\gamma+\rho}{2} - i\Omega\right)}{\left(\frac{\gamma+\rho}{2} - i\Omega\right)^2 - \kappa^2},$$
$$\bar{\mathcal{F}}(\Omega) = \frac{\kappa\sqrt{\gamma\rho}}{\left(\frac{\gamma+\rho}{2} - i\Omega\right)^2 - \kappa^2}, \qquad \text{(IV.158)}$$

still with $\mathcal{G}(\Omega) = \mathcal{G}^*(-\Omega)$, $\mathcal{F}(\Omega) = \mathcal{F}^*(-\Omega)$ and also $\bar{\mathcal{G}}(\Omega) = \bar{\mathcal{G}}^*(-\Omega)$, $\bar{\mathcal{F}}(\Omega) = \bar{\mathcal{F}}^*(-\Omega)$. The quadratures $\hat{X}^{(0)}_{C,j}(\Omega)$ and $\hat{P}^{(0)}_{C,j}(\Omega)$ are those of the vacuum modes $\hat{C}^{(0)}_j(\Omega)$ in Eq. (III.91) according to Eq. (III.94).

Again, $\hat{X}_{\rm u}(\Omega)$ and $\hat{P}_{\rm v}(\Omega)$ in Eq. (IV.157) can be considered as classically determined quantities $X_{\rm u}(\Omega)$ and $P_{\rm v}(\Omega)$ due to Alice's measurements. The appropriate amplitude and phase modulations of mode 2 performed by Bob are described by

$$\hat{X}_2(\Omega) \longrightarrow \hat{X}_{\rm tel}(\Omega) = \hat{X}_2(\Omega) + g(\Omega)\frac{\sqrt{2}}{\eta}X_{\rm u}(\Omega),$$
$$\hat{P}_2(\Omega) \longrightarrow \hat{P}_{\rm tel}(\Omega) = \hat{P}_2(\Omega) + g(\Omega)\frac{\sqrt{2}}{\eta}P_{\rm v}(\Omega). \qquad \text{(IV.159)}$$

For $g(\Omega) \equiv 1$, the teleported quadratures become

$$\begin{aligned}
\hat{X}_{\rm tel}(\Omega) &= \hat{X}_{\rm in}(\Omega) - [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)][\hat{X}^{(0)}_1(\Omega) - \hat{X}^{(0)}_2(\Omega)] \\
&\quad - [\bar{\mathcal{G}}(\Omega) - \bar{\mathcal{F}}(\Omega)][\hat{X}^{(0)}_{C,1}(\Omega) - \hat{X}^{(0)}_{C,2}(\Omega)] \\
&\quad + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{X}^{(0)}_D(\Omega) + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{X}^{(0)}_E(\Omega), \\
\hat{P}_{\rm tel}(\Omega) &= \hat{P}_{\rm in}(\Omega) + [\mathcal{G}(\Omega) - \mathcal{F}(\Omega)][\hat{P}^{(0)}_1(\Omega) + \hat{P}^{(0)}_2(\Omega)] \\
&\quad + [\bar{\mathcal{G}}(\Omega) - \bar{\mathcal{F}}(\Omega)][\hat{P}^{(0)}_{C,1}(\Omega) + \hat{P}^{(0)}_{C,2}(\Omega)] \\
&\quad + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{P}^{(0)}_F(\Omega) + \sqrt{\frac{1-\eta^2}{\eta^2}}\hat{P}^{(0)}_G(\Omega). \qquad \text{(IV.160)}
\end{aligned}$$

We calculate for this case again the spectral variances using the dimensionless variables of Eq. (IV.146),

$$V^{\hat{X}}_{\rm tel,in}(\epsilon,\omega) = V^{\hat{P}}_{\rm tel,in}(\epsilon,\omega) = 2\left[1 - \frac{4\epsilon\beta}{(\epsilon+1)^2+\omega^2}\right] + 2\,\frac{1-\eta^2}{\eta^2}, \qquad \text{(IV.161)}$$

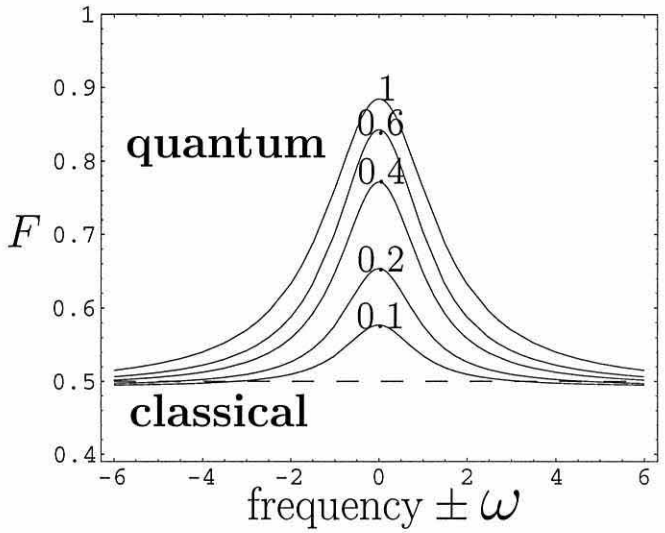

Figure IV.15: Fidelity spectrum of coherent-state teleportation using entanglement from the NOPA. The fidelities here are functions of the normalized modulation frequency $\pm\omega$ for different ϵ (0.1, 0.2, 0.4, 0.6, and 1). Bell detector efficiencies $\eta^2 = 0.97$ and cavity losses with $\beta = 0.9$ have been included here.

where $\beta = \gamma/(\gamma + \rho)$ is a "cavity escape efficiency" [155]. With the spectral Q function variances of the teleported field $\sigma_x(\Omega) = \sigma_p(\Omega) = \frac{1}{2} + \frac{1}{4}V^{\hat{X}}_{\text{tel,in}}(\Omega)$, now for coherent-state inputs, we find the fidelity spectrum (taking unit gain) as

$$F(\epsilon, \omega) = \left[2 - \frac{4\epsilon\beta}{(\epsilon+1)^2 + \omega^2} + \frac{1-\eta^2}{\eta^2}\right]^{-1} . \qquad \text{(IV.162)}$$

Using the values $\epsilon = 0.77$, $\omega = 0.56$ and $\beta = 0.9$, the measured values in the EPR experiment of Ref. [155] for maximum pump power (but still below threshold), and a Bell detector efficiency $\eta^2 = 0.97$ (as in the teleportation experiment of Ref. [87]), we obtain $V^{\hat{X}}_{\text{tel,in}} = V^{\hat{P}}_{\text{tel,in}} = 0.453$ and a fidelity $F = 0.815$. The measured value for the "normalized analysis frequency" $\omega = 0.56$ corresponds to the measured finesse $F_{\text{cav}} = 180$, the free spectral range $\nu_{\text{FSR}} = 790$ MHz and the spectrum analyzer frequency $\Omega/2\pi = 1.1$ MHz [155].

In the teleportation experiment of Ref. [87], the teleported states described

fields at 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 nonclassical fidelity was achieved at these higher frequencies Ω. The amount of squeezing at these frequencies was about 3 dB. The spectrum of the fidelities in Eq. (IV.162) is shown in Fig. IV.15 for different ϵ values.

The scheme presented allows the broadband transmission of nonorthogonal quantum states. Given an alphabet of arbitrary Gaussian states with unknown coherent amplitudes, on average, the optimum teleportation fidelity is attained with unit gain at all relevant frequencies. Optimal teleportation of one half of an entangled state (entanglement swapping) requires a squeezing-dependent, and hence frequency-dependent, nonunit gain. Effectively, also with optimum gain, the bandwidth of entanglement becomes smaller after entanglement swapping compared to the bandwidth of entanglement of the initial states, as the quality of the entanglement deteriorates at each frequency for finite squeezing.

In the particular case of a NOPA as the entanglement source, the best quantum teleportation occurs in the frequency regime close to the center frequency (half the NOPA's pump frequency). In general, a suitable EPR source for broadband teleportation can be obtained by combining two independent broadband squeezed states at a beam splitter (as discussed in chapter III). Provided ideal Bell detection, unit-gain teleportation will then in general produce an excess noise in each teleported quadrature of twice the squeezing spectrum of the quiet quadrature in the corresponding broadband squeezed state (for the NOPA, cavity loss appears in the squeezing spectrum). Thus, good broadband teleportation requires good broadband squeezing. However, the entanglement source's squeezing spectrum for its quiet quadrature need not be a minimum near the center frequency ($\Omega = 0$) as for the optical parametric oscillator. In general, it might have large excess noise there and be quiet at $\Omega \neq 0$ as for four-wave mixing in a cavity [192]. The spectral range to be teleported $\Delta\Omega$ should always be in the

"quiet region" of the squeezing spectrum.

The scheme presented here allows very efficient teleportation of broadband quantum states: the quantum state at the input (a coherent, a squeezed, an entangled or any other state), describing the input field at modulation frequency Ω within a bandwidth $\Delta\Omega$, is teleported on each and every trial (where the duration of a single trial is given by the inverse-bandwidth time $1/\Delta\Omega$). Every inverse-bandwidth time, a quantum state is teleported with nonclassical fidelity or previously unentangled fields become entangled. Also the output of entanglement swapping can therefore be used for efficient quantum teleportation, succeeding every inverse-bandwidth time.

In contrast, discrete-variable optical implementations so far involve weak down conversion and enable only relatively rare transfers of quantum states. In the experiment of Ref. [23], a fourfold coincidence (i.e., "successful" teleportation [38]) occurred at a rate of 1/40 Hz for a UV pump pulse rate of 80 MHz [201] yielding an overall efficiency of 3×10^{-10} (events per pulse). Note that due to filtering and collection difficulties the photodetectors in this experiment operated with an effective efficiency of only about 10% [201].

We conclude this chapter with a few remarks on methods for the reliable transmission of quantum information other than teleportation. As already mentioned in the introduction to this chapter, these methods include quantum error correction [184] and entanglement purification [17]. In quantum error correction 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 recieving 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 in Refs. [184, 49, 118]. Shortly after the proposal for the realization of continuous-variable teleportation, the known qubit quantum error correction codes were translated to continuous variables [26, 130]. These schemes appeared to require active nonlinear operations such as quantum non-demolition coupling for the implementation of the C-NOT gate [26]. However, later it turned out that also continuous-variable quantum error correction codes can be implemented using only linear optics and resources of squeezed light [27]. This was shown for the nine-wavepacket code [27], the analogue of Shor's nine-qubit code [184]. An open question is still how to implement the five-wavepacket code using only linear optics and squeezed light. Similar to the formulation of the quantum circuits presented in this thesis, also continuous-variable quantum error correction can be recast in the Heisenberg representation and then analyzed in a realistic broadband description [135].

Entanglement purification aims at "purifying" a mixed entangled state after its two halves have been distributed through noisy channels [17]. It relies on local operations and classical communication, and it works only in a probabilistic fashion (for instance, for purifying an ensemble of entangled qubit pairs, some are discarded and others are kept depending on local measurement results [17]). After an entangled state has been purified, it can be used for quantum teleportation with high fidelity.

A "continuous-variable" entanglement purification scheme was proposed by Duan *et al.* based on local photon number quantum non-demolition measurements [75]. The entanglement of bipartite Gaussian states can be both concentrated and purified using this scheme [75, 90]. However, though feasible [76], its experimental realization is very difficult. Moreover, in this scheme, the purified entangled states (or the concentrated entangled states having a higher degree of entanglement than the initial states) end up in a finite-dimensional Hilbert space. How to purify or concentrate continuous-variable entangled states to ob-

tain better *continuous-variable* entanglement is still an open question and subject of current research.

Finally, we mention that also quantum dense coding [14] has been proposed for continuous variables [39]. Dense coding means the efficient transmission of classical information by sending quantum information. For example, in a protocol where only one qubit (one half of a Bell state) is actually sent to the receiver, two classical bits can be conveyed using local operations. It was shown that by utilizing the entanglement of a two-mode squeezed state, coherent communication (based on coherent states) can always be beaten [39]. The continuous-variable scheme attains a capacity approaching twice that theoretically achievable in the absence of entanglement [39].

2 Secure transmission of classical information using quantum protection

In this section, we give a brief overview of recent proposals for continuous-variable quantum cryptography. This overview is taken from Braunstein and van Loock [40]. We will conclude this section with a few remarks on quantum secret sharing with continuous variables.

a Quantum cryptography

Early ideas and recent progress: For qubit based quantum cryptography there have been two basic schemes. Those involving the sending of states from non-orthogonal bases, such as the original "BB84 protocol" [13], and those based on sharing entanglement between the sender and receiver, such as Ekert's scheme [83]. A similar distinction can be made for the various proposals for continuous-variable quantum cryptography.

The schemes that do not rely on entanglement are mostly based on alphabets involving (non-orthogonal) coherent states as the signal states. For example, in

Ref. [147], Mu *et al.* utilize four coherent states and four specific local oscillator settings for the homodyne detection, enabling the receiver to conclusively identify a bit value. In Ref. [112], Huttner *et al.* use generalized measurements (POVM's) instead, which may sometimes yield inconclusive results for a bit value encoded in weak (and non-orthogonal) coherent states. The scheme of Huttner *et al.* is actually a combination of the BB84 and "B92" qubit protocols [13, 12], the latter of which requires just two arbitrary non-orthogonal states. The basic idea behind this combination is to make the two states in each pair of basis states, which are orthogonal in BB84, non-orthogonal instead, like in B92. By using non-orthogonal states in each pair, one gets the additional advantage of the B92 protocol, namely, that an eavesdropper 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 less than one photon), is then turned into a virtue. How a receiver optimally distinguishes between two coherent signal states for these coherent-state schemes was shown by Banaszek [6] to be possible using a simple optical arrangement.

The use of squeezed states rather than coherent states was recently investigated by Hillery [104]. His analysis of security is in some sense realistic, though ignoring collective attacks, because it explicitly includes the effects of loss. In addition, two kinds of eavesdropper attack are studied: man-in-the-middle (or intercept-resend) measuring a single quadrature; and quantum-tap using a beam splitter after which again only a single quadrature is measured. Hillery found that losses produced a significant degradation in performance, however, he suggested that this problem could be ameliorated by pre-amplification.

The entanglement-based quantum cryptographic schemes within the framework of continuous-variable quantum optics rely on the correlations of the quadratures of two-mode squeezed states. Cohen [65] considered the idealized case with

an unphysical infinite amount of squeezing to give perfect correlations. More realistically, Pereira *et al.* [161] (which we note 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 uses pre-shared entanglement).

Ralph [167] has recently considered continuous-variable quantum cryptography in two variations: first, a scheme where the information is encoded onto just a single (bright) coherent state, and second, an entanglement-based scheme, where 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 non-collective attacks by an eavesdropper. The first two involved the eavesdropper 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) 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 á la Arthurs-Kelly) was used to maximize information retrieval.

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

an eavesdropping strategy based on quantum teleportation and shows again that there is a favourable trade-off between the extractable classical information and the disturbance of the signals passed on to the receiver [168]. 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 [168] includes an analysis of losses. His work has also studied the most extensive set of non-collective attacks of those schemes discussed in this section.

Reid [173] has considered a similar scheme, exploiting the Bell-type correlations between the modes of a two-mode squeezed state. In fact, this scheme is directly analogous to Ekert's qubit scheme [83]. The protection against an eavesdropper is provided by Alice and Bob 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.

Experimental progress has also been made, as reported recently by Hirano *et al.* [106], where a BB84-like (entanglement-free) quantum cryptography scheme was implemented at telecommunication wavelengths using four non-orthogonal coherent states. No attempt at implementing any eavesdropper strategy is made. Finally, we note two other very recent works by Silberhorn *et al.* [187] and by Bencheikh *et al.* [11].

Absolute theoretical security: From single-wavepacket non-collective attacks considered above there has been great progress recently for continuous-variable quantum cryptography in the detailed proof of absolute theoretical security for one scheme [97, 98]. This scheme is the continuous-variable analogue of the original BB84 scheme. Following the Shor and Preskill [185] proof for absolute security for the original qubit proposal, Gottesman and Preskill have generalized the proof.

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 capture 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, squeezing signal states of just 2.51 dB are sufficient in principle to ensure the protocol's security. Heuristically, it appears that the original rough and ready reasoning of security based on single-shot non-collective attacks really does impart absolute security. This suggests strongly that the protocols discussed previously will be found to be similarly absolutely secure when enhanced or supplemented by classical error correction and privacy amplification.

Remaining issues appear to be:

1.) Re-analysis of this proof in a broadband context. In particular, can the protocol be run in a *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 approach 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.) At the moment all the continuous-variable quantum cryptographic schemes

claim to provide working protocols over distances comparable to the attenuation length of the quantum channel. Some way needs to be found to go beyond this severe limitation (unless a long-range free space approach is used, say bouncing off satellites). Working at communication wavelengths with low-loss fibers is still somewhat limited by detector efficiency in this regime, further, it would appear that orders of magnitude improvement would not be possible in this way. The alternative would be to introduce some sort of repeater system, either classical or quantum. The only provably secure approach would be via quantum repeaters, constructed via quantum error correction or some sort of quantum purification protocol.

4.) Finally, experimental verifiability of the claims of absolute security. This last point will now be considered.

Towards verifying experimental security and optimal eavesdropping strategies: So, we have seen that there are already beginning to be theoretical proofs for absolute security. Unfortunately, such theoretical proofs must be treated somewhat sceptically. 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 resolve 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 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, but 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. Although the cloning of discrete-variable quantum information is now very well understood, that for continuous quantum variables has only undergone recent preliminary analysis (see next chapter). It should be noted that Ralph suggests using teleportation as an eavesdropping strategy [167]. This strategy deserves more consideration, but it unnecessarily limits the eavesdropper to non-collective attacks. By contrast, general cloning strategies *should* encompass the same performance, but without imposing this restriction.

Most recently Cerf *et al.* [60] have applied the work on 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 the next chapter, both for optimal local cloning and optimal "telecloning".

In summary, there is now one theoretically proven secure quantum cryptographic scheme involving quantum continuous variables. 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 to real implementations and whether new loopholes will not be created during this phase. This should be investigated both theoretically and experimentally by considering eavesdropping strategies, initially based on asymmetric cloning, as suitable verification strategies. Cloning of continuous quantum variables is the subject of the next chapter.

b Quantum secret sharing

Quantum secret sharing can be thought of as a multi-party generalization of quantum cryptography where a message is not only protected against potential eavesdroppers. In addition, the relevant information 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 [105]. 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 [105]. In the former case, a key can be established between all participants and using the key requires all participants working together. An eavesdropper would introduce errors and could be detected. In the latter case, for example a qubit can be recovered after its quantum information has been split into two or more parts (obviously, only the former scenario is a multi-party extension of what is known as quantum cryptography).

In the context of continuous variables, the analogue 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 similarly exploited as the two-mode correlations in the above entanglement-based quantum cryptography schemes. In fact, their exploitation is equivalent to the two-party sender-receiver scenario when all participants except for the sender team up and share the information about local momentum measurements to yield a total "receiver momentum". This would enable to secretly share classical information protected against eavesdropping. Such a scheme should be analyzed in more detail taking into account finite squeezing of the entangled states.

We have already seen in a previous section that by using continuous-variable

multipartite entanglement (with large squeezing) nonorthogonal quantum states such as coherent states can be transferred from a sender to an arbitrary receiver with high fidelity, provided this receiver obtains additional classical information about momentum detections of the other participants. Since the generation of multipartite entanglement is relatively easy for continuous variables, quantum secret sharing based on these states is feasible with current technology. Very recently, continuous-variable secret sharing of quantum information was considered by Tyc and Sanders [197]. The multi-mode entangled states used in their scheme are also producible with squeezed light and beam splitters.

In the next chapter, we now turn to an issue relevant to the question of security in continuous-variable quantum cryptography and secret sharing: cloning of continuous quantum variables.

V

Quantum Cloning with Continuous Variables

Quantum information encoded in nonorthogonal quantum states can be perfectly transferred between two distant locations that are linked by a maximally entangled state and a classical communication channel. This quantum teleportation has been the main subject of the thesis and it is a prime example of quantum information processing where otherwise impossible cryptographic, computational, and communication tasks can be performed through the presence of shared entanglement. In principle, perfect teleportation with unit fidelity from a sender to a *single* receiver is possible in accordance with quantum mechanics. Of course, we have seen that nonmaximally entangled quantum channels such as two-mode squeezed states only allow imperfect replicas of the sender's quantum state emerging at the receiver's location. But there is no fundamental law that prevents us from perfectly transferring a quantum state in the limit of maximum shared entanglement. The no-cloning theorem (see chapter II), for instance, is not violated by perfect quantum teleportation from Alice to Bob, since the input state prior to its retrieval by Bob is changed at Alice's location due to her Bell measurement.

What about conveying quantum information via a "multiuser quantum channel" (MQC) simultaneously to several receivers? The no-cloning theorem that generally forbids *perfect* cloning (or copying) of unknown nonorthogonal quantum states then also disallows cloning over a distance. This prevents the MQC from being able to produce *exact* clones of the sender's input state at all receiving stations. The MQC, however, can provide each receiver with at least a part of the input quantum information and distribute *approximate* clones with non-

unit fidelity [47]. This cloning at a distance or "telecloning" may be seen as the "natural generalization of teleportation to the many-recipient case" [149].

In this chapter, we are mainly concerned about whether we can find entangled states that may function as an MQC for conveying continuous-variable quantum information. First, however, we have to review some fundamental results that go "beyond the no-cloning theorem" and refer to the possibility of "local" approximate cloning of quantum states. These results were first derived for discrete variables [47]. Applying them to continuous quantum variables, we will discuss local cloning in a universal fashion for arbitrary continuous-variable states [29] and in a state-dependent fashion for Gaussian states [59, 58]. Then, we will present a local cloning circuit capable of transforming N identical coherent states into M optimal approximate copies ($M > N$). After a brief discussion of qubit telecloning [149], we will finally deal with continuous-variable telecloning. The circuits and protocols for local cloning and telecloning with continuous quantum variables are based on Refs. [30, 134].

1 "Local" cloning

First, we are now interested in 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.

a *Beyond no-cloning*

The no-cloning theorem, originally derived for qubits, in general forbids exact copying of unknown nonorthogonal (or simply arbitrary) quantum states. 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 [47, 91, 44, 43, 203]. Based on these results, a cloning experiment has been proposed for qubits encoded as single-photon states [190], and two other optical qubit cloning experiments have been realized already [141, 127].

The advantage of the qubit cloning machine of Bužek and Hillery [47] over the original one by Wootters and Zurek [207] is that it is not input-state dependent. Any input state is copied equally well with the same fidelity and that fidelity is optimal. The Wootters-Zurek cloning device favours certain basis states $\{|0\rangle, |1\rangle\}$ and copies them perfectly. A symmetric superposition $(|0\rangle + |1\rangle)/\sqrt{2}$, however, is duplicated only with a fidelity of 1/2 (see chapter II). Instead of the Wootters-Zurek transformation from Eq. (II.4), Bužek and Hillery proposed

$$\begin{aligned} |0\rangle|A\rangle &\longrightarrow |0\rangle|0\rangle|A_0\rangle + (|0\rangle|1\rangle + |1\rangle|0\rangle)|B_0\rangle \,, \\ |1\rangle|A\rangle &\longrightarrow |1\rangle|1\rangle|A_1\rangle + (|0\rangle|1\rangle + |1\rangle|0\rangle)|B_1\rangle \,. \end{aligned} \tag{V.1}$$

This transformation can be applied to an arbitrary input qubit state $|s\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$. Upon tracing out the apparatus c and then mode b from the resulting state $\hat{\rho}_{abc}$ (see chapter II), the scalar products $\langle A_i|B_j\rangle$ etc. are determined by the unitarity of the transformation in Eq. (V.1) and the requirement of an input-state independent cloning fidelity. This ultimately leads to the output density operator for the original mode [47]

$$\hat{\rho}_a = \frac{5}{6}|s\rangle_{a\,a}\langle s| + \frac{1}{6}|\tilde{s}\rangle_{a\,a}\langle\tilde{s}| \,, \tag{V.2}$$

diagonal in the basis

$$|s\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a \,, \qquad |\tilde{s}\rangle_a = \beta|0\rangle_a - \alpha|1\rangle_a \,. \tag{V.3}$$

The second mode's density operator $\hat{\rho}_b$ takes the same form. The outgoing state of the original a and the copy b still contain off-diagonal terms with information about the input quantum coherence, as opposed to the output states from the

Wootters-Zurek scheme in Eq. (II.8). The cloning fidelity is now independent of α and becomes

$$F = {}_a\langle s|\hat{\rho}_a|s\rangle_a = {}_b\langle s|\hat{\rho}_b|s\rangle_b = \frac{5}{6}. \tag{V.4}$$

This is the optimum averaged fidelity achievable when duplicating an unknown qubit state.

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 [1], Werner was able to derive the cloning map that yields the optimal N to M cloning fidelities for d-dimensional states [203]

$$F = \frac{N(d-1) + M(N+1)}{M(N+d)} \equiv F_{\text{clon},N,M}^{\text{univ},d}\,. \tag{V.5}$$

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.

b *Universal cloners*

A universal cloner is capable of optimally copying arbitrary quantum states with the same fidelity independent of the particular input state. Bužek and Hillery's universal 1 to 2 qubit cloner based on Eq. (V.1) leads to two identical copies $\hat{\rho}_a$

[1] It is pointed out by Werner [203] 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 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 completely positive trace preserving map. Conversely, any linear completely positive trace preserving map can be constructed via the constructive approach.

and $\hat{\rho}_b$ [Eq. (V.2)]. 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 [29]

$$\begin{aligned} \hat{\rho}_a &= (1-A^2)|s\rangle_{a\,a}\langle s| + \frac{A^2}{d}\,\mathbb{1}_a\,, \\ \hat{\rho}_b &= (1-B^2)|s\rangle_{b\,b}\langle s| + \frac{B^2}{d}\,\mathbb{1}_b\,, \end{aligned} \tag{V.6}$$

for an arbitrary d-dimensional input state $|s\rangle_a = \sum_{n=0}^{d-1} c_n|n\rangle_a$. The parameters A and B are related via $A^2 + B^2 + 2AB/d = 1$ [29]. The two extreme cases are 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 [29].

It was also shown by Braunstein *et al.* [29] 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 C-NOT gates pairwise acting on the input qubit a and two qubits b and c in an entangled state [46]. For arbitrary dimensions, the analogous circuit can be used with C-NOT operations generalized to d dimensions, $|n\rangle|m\rangle \to |n\rangle|n \oplus m\rangle$, and a corresponding d-dimensional entangled state of systems b and c [29]. In a discretized phase space (x_k, p_k) [45, 154, 48], the entangled state has the form $|\chi\rangle_{bc} = A|x_0\rangle_b|p_0\rangle_c + B(\sum_{k=0}^{d-1}|x_k\rangle_b|x_k\rangle_c)/\sqrt{d}$, 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 [29]. The parameters A and B are then related as $A^2 + B^2 + 4AB/\sqrt{4 + 2\sinh^2 2r} = 1$ and the C-NOT operations become conditional shifts in phase space, $|x\rangle|y\rangle \rightarrow |x\rangle|x + y\rangle$ [26]. Expressed in terms of position and momentum operators, the sequence of four generalized C-NOT operations [2] acting on modes a (the original), b, and c, can be written as [29, 59]

$$\hat{U}_{abc} = \exp[-2i(\hat{x}_c - \hat{x}_b)\hat{p}_a] \exp[-2i\hat{x}_a(\hat{p}_b + \hat{p}_c)] \,. \tag{V.7}$$

Here, $\exp(-2i\hat{x}_k\hat{p}_l)$ corresponds to a single C-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 $1/2$ [29]. Similarly, for universal symmetric N to M cloning of arbitrary continuous-variable states, one obtains the optimum cloning fidelity [29]

$$F^{\text{univ},\infty}_{\text{clon},N,M} = \frac{N}{M} \,, \tag{V.8}$$

which is exactly the infinite-dimensional limit $d \rightarrow \infty$ of Werner's result in Eq. (V.5). 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

[2] Note that the C-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, $\hat{U}_{ab} = \sum_{n,m=0}^{d-1} |n\rangle_{a\,a}\langle n| \otimes |n \oplus m\rangle_{b\,b}\langle m|$ and $\hat{U}^\dagger_{ab}$ differ describing conditional shifts in opposite directions. The same applies to the continuous-variable C-NOT operation $|x\rangle|y\rangle \rightarrow |x\rangle|x + y\rangle$ [26]. Therefore, there is a slight modification in the sequence of four C-NOT's from $d = 2$ to $d > 2$: $\hat{U}_{ca}\hat{U}^\dagger_{ba}\hat{U}_{ac}\hat{U}_{ab}$. Making the C-NOT its own inverse $\hat{U} = \hat{U}^\dagger$ could be achieved by defining $|x\rangle|y\rangle \rightarrow |x\rangle|x - y\rangle$ [3].

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 [29]. 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 [29].

Let us summarize at this point: we have discussed fidelity boundaries for universal N to M cloners. These boundaries, the optimum 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 optimum 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 will now turn to this question.

c "State-dependent" Gaussian cloners

In the first papers that considered continuous-variable cloning, the set of input states to be copied was restricted to Gaussian states [59, 58]. The optimal cloning fidelity for turning N identical but arbitrary coherent states into M identical approximate copies,

$$F_{\mathrm{clon},N,M}^{\mathrm{coh\,st},\infty} = MN/(MN + M - N) \,, \tag{V.9}$$

was derived in Ref. [58]. The approach there 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 [43]. 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 $\eta_{\rm clon}(N,M)$, shrinking the Bloch vector of the original input state (see chapter II)

$$\hat{\rho}_a^{\rm in} = \frac{1}{2}(\mathbb{1}_a + \vec{s}_a^{\rm in} \cdot \vec{\sigma}) \,, \tag{V.10}$$

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

$$\hat{\rho}_a^{\rm out} = \frac{1}{2}[\mathbb{1}_a + \eta_{\rm clon}(N,M)\, \vec{s}_a^{\rm in} \cdot \vec{\sigma}] \,. \tag{V.11}$$

The optimum cloners are those with maximum $\eta_{\rm clon}(N,M) \equiv \bar{\eta}_{\rm clon}(N,M)$. 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 $\bar{\eta}_{\rm clon}(N,\infty)$ equals the shrinking factor for the optimal quantum state estimation through measurements $\bar{\eta}_{\rm meas}(N)$ given N identical input states. This leads to the inequality $\eta_{\rm clon}(N,M)\,\eta_{\rm clon}(M,L) \leq \bar{\eta}_{\rm clon}(N,L)$ and also (with $L \to \infty$) $\eta_{\rm clon}(N,M)\,\bar{\eta}_{\rm clon}(M,\infty) \leq \bar{\eta}_{\rm clon}(N,\infty)$, which gives the lowest upper bound

$$\eta_{\rm clon}(N,M) \leq \frac{\bar{\eta}_{\rm clon}(N,\infty)}{\bar{\eta}_{\rm clon}(M,\infty)} = \frac{\bar{\eta}_{\rm meas}(N)}{\bar{\eta}_{\rm meas}(M)} \,. \tag{V.12}$$

Because of the optimum shrinking factor $\bar{\eta}_{\rm meas}(N) = N/(N+2)$ due to a measurement (see chapter II), we obtain

$$\bar{\eta}_{\rm clon}(N,M) = \frac{N}{M}\frac{M+2}{N+2} \,. \tag{V.13}$$

This result yields the correct optimum $N \to M$ cloning fidelity in Eq. (V.5) for dimension $d = 2$, using Eq. (II.75) with $\bar{\eta}_{\rm meas}(N)$ replaced by $\bar{\eta}_{\rm clon}(N,M)$. In fact, the fidelity does not depend on the particular input state Bloch vector $\vec{s}_a^{\rm in}$ and its parameters θ_0 and ϕ_0 [see chapter II, Eq. (II.74)].

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, $\lambda_{\rm clon}(N,L) = \lambda_{\rm clon}(N,M) + \lambda_{\rm clon}(M,L)$. With the optimum (minimal) excess noise variances defined by $\bar{\lambda}_{\rm clon}(N,L)$, we find now the largest lower bound

$$\lambda_{\rm clon}(N,M) \geq \bar{\lambda}_{\rm clon}(N,\infty) - \bar{\lambda}_{\rm clon}(M,\infty) \; . \tag{V.14}$$

The quantity $\bar{\lambda}_{\rm clon}(N,\infty)$ can be inferred from quantum estimation theory [107], because it equals the quadrature variance of an optimal joint measurement of $\hat{x}$ and $\hat{p}$ on N identically prepared systems, $\bar{\lambda}_{\rm clon}(N,\infty) = \bar{\lambda}_{\rm meas}(N) = 1/2N$ [58]. 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 $\bar{\lambda}_{\rm meas}(1) = 1/2 = 1/4 + 1/4$ [5], 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 optimum average fidelity of $1/2$ for arbitrary coherent states, as discussed in the previous chapter). Since infinitely many copies can be made that 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 [43], the optimal measurement (optimal state estimation) turns out to be the optimal $N \to \infty$ cloner, and hence $\bar{\lambda}_{\rm clon}(N,\infty) = \bar{\lambda}_{\rm meas}(N) = 1/2N$. This result combined with the inequality of Eq. (V.14) gives the optimum (minimal) excess noise induced by an $N \to M$ cloning process [58],

$$\bar{\lambda}_{\rm clon}(N,M) = \frac{M-N}{2MN} \; . \tag{V.15}$$

Inserting this excess noise into Eq. (IV.50) with $g = 1$ and a coherent-state input [where $\sigma_x = \sigma_p = 1/2 + \bar{\lambda}_{\rm clon}(N,M)$] leads to the correct fidelity in Eq. (V.9). 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 (see later the specific cloning circuit). 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. 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 (see later). 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.

What we have now seen is that the same analogy that applies to the classical teleportation of qubits (chapter II) and of coherent states (chapter IV) is relevant to optimal $N \to M$ cloning: for arbitrary (pure) qubit states, 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 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-C-NOT transformation in Eq. (V.7) can be used to construct an optimal $1 \to 2$ coherent-state cloner, covariant under displacement and rotation in phase space [59]. The entangled state of modes b and c then has

to be (in our units) [59]

$$|\chi\rangle_{bc} \propto \int dx\, dy\, \exp(-x^2 - y^2)\, |x\rangle|x + y\rangle\ . \tag{V.16}$$

In the following section, we will present a local cloning circuit that enables optimal $N \to M$ cloning of coherent states. In the special $1 \to 2$ case, its design is simpler and the resources needed much cheaper than for the Four-C-NOT cloner.

d An $\boldsymbol{N}$ *to* $\boldsymbol{M}$ *local 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 quantum cryptography, for instance, this problem happens to be strongly related to the assessment of security [86]. We will use the Heisenberg representation in order to explicitly derive an $N \to M$ symmetric cloning transformation that attains Eq. (V.9). Remarkably, it appears that implementing this transformation only requires a phase-insensitive linear amplifier and a series of beam splitters [30].

Let $|\Psi\rangle = |\alpha\rangle^{\otimes N} \otimes |0\rangle^{\otimes M-N} \otimes |0\rangle_z$ denote the initial joint state of the N input modes to be cloned (prepared in the coherent state $|\alpha\rangle$), the additional $M - N$ blank modes, and an ancillary mode z. The blank modes and the ancilla are assumed to be initially in the vacuum state $|0\rangle$. Let $\{\hat{x}_k, \hat{p}_k\}$ denote the pair of quadrature operators associated with each mode k involved in the cloning transformation: $k = 0 \ldots N-1$ refers to the N original input modes, and $k = N \ldots M-1$ refers to the additional blank modes [for simplicity, here we do not explicitly label vacuum modes by a superscript "(0)"]. We are looking for some unitary transformation $\hat{U}$ that when acting on $|\Psi\rangle$ results in a state $|\Psi''\rangle = \hat{U}|\Psi\rangle$ such that the M modes are left in the same (mixed) state which is maximally 'close' to $|\alpha\rangle$. In the Heisenberg picture, this transformation can be described

alternatively by a canonical transformation acting on the operators $\{\hat{x}_k, \hat{p}_k\}$:

$$\hat{x}_k'' = \hat{U}^\dagger \, \hat{x}_k \, \hat{U}, \quad \hat{p}_k'' = \hat{U}^\dagger \, \hat{p}_k \, \hat{U}, \tag{V.17}$$

while leaving the state $|\Psi\rangle$ invariant. We will work in the Heisenberg picture and use the above notation throughout this section, with $\hat{x}_k''$ denoting the clones (i.e., the output modes of the cloning circuit except the ancilla z). We will now impose several requirements on transformation (V.17) that translate the expected properties for an optimal cloning transformation. First, we require that the M output modes have the desired mean values:

$$\begin{aligned} \langle \hat{x}_k'' \rangle &= \langle \hat{x}_0 \rangle = \langle \alpha | \hat{x} | \alpha \rangle, \\ \langle \hat{p}_k'' \rangle &= \langle \hat{p}_0 \rangle = \langle \alpha | \hat{p} | \alpha \rangle, \end{aligned} \tag{V.18}$$

for $k = 0 \ldots M-1$. Our second requirement is covariance with respect to rotation in phase space. Coherent states have the property that the quadrature variances are left invariant by rotations in phase space. So, for any input mode k of the cloning transformation and for any operator $\hat{v}_k = c\,\hat{x}_k + d\,\hat{p}_k$ (where c and d are complex numbers satisfying $|c|^2 + |d|^2 = 1$), the (input) error variance λ_{v_k} is the same:

$$\lambda_{v_k} = \langle (\hat{v}_k)^2 \rangle - \langle \hat{v}_k \rangle^2 = \langle (\Delta \hat{x})^2 \rangle_{\text{vacuum}} = \frac{1}{4}. \tag{V.19}$$

We impose this property to be conserved through the cloning process. Taking optimality into account, Eq. (V.15), rotational covariance at the output yields:

$$\lambda_{v_k''} = \left(1 + \frac{2}{N} - \frac{2}{M}\right) \langle (\Delta \hat{x})^2 \rangle_{\text{vacuum}}, \tag{V.20}$$

where $\hat{v}_k'' = c\,\hat{x}_k'' + d\,\hat{p}_k''$. Our third requirement is, of course, the unitarity of the cloning transformation (V.17). In the Heisenberg picture, this is equivalent to demanding that the commutation relations are preserved throughout the evolution:

$$[\hat{x}_j'', \hat{x}_k''] = [\hat{p}_j'', \hat{p}_k''] = 0, \quad [\hat{x}_j'', \hat{p}_k''] = \frac{i}{2}\delta_{jk}, \tag{V.21}$$

for $j, k = 0 \ldots M-1$ and for the ancilla.

Let us first focus on coherent-state duplication ($N = 1$, $M = 2$). A simple transformation obeying the three conditions mentioned above is given by:

$$\begin{aligned} \hat{x}_0'' &= \hat{x}_0 + \frac{\hat{x}_1}{\sqrt{2}} + \frac{\hat{x}_z}{\sqrt{2}}, & \hat{p}_0'' &= \hat{p}_0 + \frac{\hat{p}_1}{\sqrt{2}} - \frac{\hat{p}_z}{\sqrt{2}}, \\ \hat{x}_1'' &= \hat{x}_0 - \frac{\hat{x}_1}{\sqrt{2}} + \frac{\hat{x}_z}{\sqrt{2}}, & \hat{p}_1'' &= \hat{p}_0 - \frac{\hat{p}_1}{\sqrt{2}} - \frac{\hat{p}_z}{\sqrt{2}}, \\ \hat{x}_z' &= \hat{x}_0 + \sqrt{2}\,\hat{x}_z, & \hat{p}_z' &= -\hat{p}_0 + \sqrt{2}\,\hat{p}_z. \end{aligned} \tag{V.22}$$

This transformation clearly conserves the commutation rules, and yields the expected mean values $(\langle \hat{x}_0 \rangle, \langle \hat{p}_0 \rangle)$ for the two clones (modes $0''$ and $1''$). Also, one can check that the quadrature variances of both clones are equal to $2\langle (\Delta \hat{x})^2 \rangle_{\text{vacuum}}$, in accordance with Eq. (V.20). Interestingly, we note here that the state in which the ancilla z is left after cloning is centered on $(\langle \hat{x}_0 \rangle, -\langle \hat{p}_0 \rangle)$, that is the *phase-conjugated* state $|\alpha^*\rangle$. This means that, in analogy with the universal qubit cloning machine [47], the continuous-variable cloner generates an "anticlone" (or time-reversed state) together with the two clones.

Now, let us show how this duplicator can be implemented in practice. Equation (V.22) can be interpreted as a sequence of two canonical transformations:

$$\begin{aligned} \hat{a}_0' &= \sqrt{2}\hat{a}_0 + \hat{a}_z^\dagger, & \hat{a}_z' &= \hat{a}_0^\dagger + \sqrt{2}\hat{a}_z, \\ \hat{a}_0'' &= \frac{1}{\sqrt{2}}(\hat{a}_0' + \hat{a}_1), & \hat{a}_1'' &= \frac{1}{\sqrt{2}}(\hat{a}_0' - \hat{a}_1), \end{aligned} \tag{V.23}$$

where $\hat{a}_k = \hat{x}_k + i\hat{p}_k$ and $\hat{a}_k^\dagger = \hat{x}_k - i\hat{p}_k$ denote the annihilation and creation operators for mode k.

As shown in Fig. V.1, the interpretation of this transformation 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 [57]. Clearly, rotational covariance is guaranteed here by the use of a *phase-insensitive* amplifier. As discussed in Ref. [53], the ancilla z involved

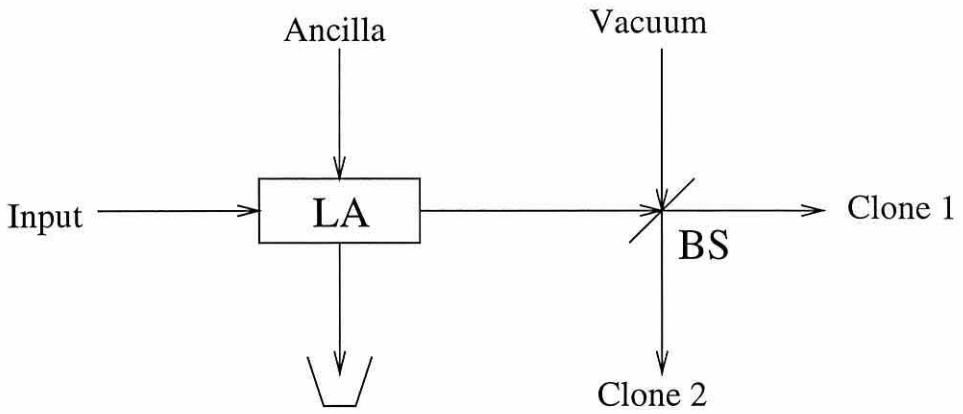

Figure V.1: Implementation of a $1 \rightarrow 2$ continuous-variable cloning machine. LA stands for linear amplifier, and BS represents a phase-free 50:50 beam splitter.

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 [53]:

$$\lambda_{LA} \geq (G-1)/4. \tag{V.24}$$

Hence, the optimal amplifier of gain $G = 2$ yields $\lambda_{LA} = 1/4$, so that our cloning transformation is indeed optimal.

Let us now consider the $N \rightarrow M$ cloning transformation. In order to achieve cloning, energy has to be brought to the $M - N$ blank modes in order to drive them from the vacuum into a state which has the desired mean value. We will again achieve this with the help of a linear amplifier. From Eq. (V.24), we see that the cloning induced noise essentially originates from the amplification process, and grows with the amplifier gain. Therefore, we should preferably amplify as little as possible. The cloning procedure should then be as follows: (i) symmetrically amplifying the N input modes by *concentrating* them into one

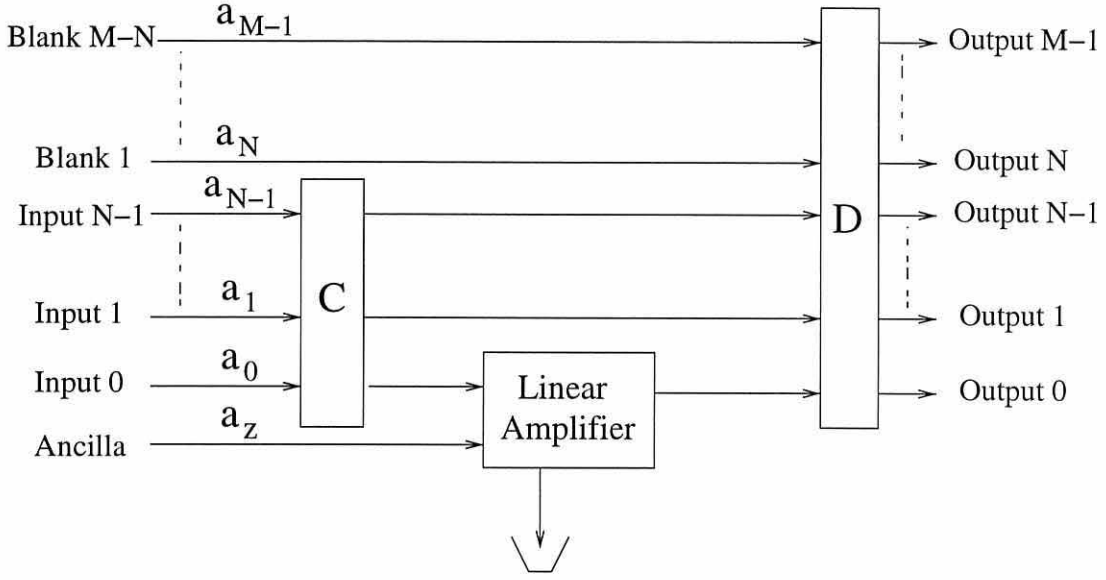

Figure V.2: Implementation of an $N \to M$ continuous-variable cloning machine. C stands for the amplitude concentration operation, while D refers to the amplitude distribution. Both can be achieved by using a DFT, or, alternatively, an inverse "N-splitter" and an "M-splitter" (in which case we shift the indices by one in the text, i.e., $k = 1 \ldots M$).

single mode, which is then amplified; (ii) symmetrically *distributing* the output of this amplifier among the M output modes. As we will see, a convenient way to achieve these concentration and distribution processes is provided by the Discrete Fourier Transform (DFT). Cloning is then achieved by the following three-step procedure (see Fig. V.2). First step: a DFT (acting on N modes),

$$\hat{a}'_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \exp(ikl2\pi/N)\, \hat{a}_l, \tag{V.25}$$

with $k = 0 \ldots N-1$. This operation concentrates the energy of the N input modes into one single mode (renamed $\hat{a}_0$) and leaves the remaining $N-1$ modes $(\hat{a}'_1 \ldots \hat{a}'_{N-1})$ in the vacuum. Second step: the mode $\hat{a}_0$ is amplified with a linear

amplifier of gain $G = M/N$. This results in

$$\begin{aligned} \hat{a}'_0 &= \sqrt{\frac{M}{N}}\,\hat{a}_0 + \sqrt{\frac{M}{N}-1}\,\hat{a}_z^\dagger, \\ \hat{a}'_z &= \sqrt{\frac{M}{N}-1}\,\hat{a}_0^\dagger + \sqrt{\frac{M}{N}}\,\hat{a}_z. \end{aligned} \tag{V.26}$$

Third step: amplitude distribution by performing a DFT (acting on M modes) between the mode $\hat{a}'_0$ and $M-1$ modes in the vacuum state:

$$\hat{a}''_k = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} \exp(ikl2\pi/M)\,\hat{a}'_l, \tag{V.27}$$

with $k = 0 \ldots M-1$, and $\hat{a}'_i = \hat{a}_i$ for $i = N \ldots M-1$. The DFT now distributes the energy contained in the output of the amplifier among the M output clones.

It is readily checked that this procedure meets our three requirements, and is optimal provided that the amplifier is optimal, that is $\lambda_{LA} = [(M/N) - 1]/4$. The quadrature variances of the M output modes coincide with Eq. (V.20). As in the case of duplication, the quality of cloning decreases as λ_{LA} increases, that is, cloning and amplifying coherent states are two equivalent problems here. For $1 \to 2$ cloning, we have seen that the final amplitude distribution among the output clones is achieved with a single beam splitter. In fact, any unitary matrix such as the DFT used here can be realized with a sequence of beam splitters (and phase shifters) [171]. This means that the $N \to M$ cloning transformation can be implemented using only passive optical elements with the addition of a *single* linear amplifier.

We will now explicitly give the 'simplest' beam splitter combination that enables the above transformation. For convenience, let us now use the indices $k = 1 \ldots N$ for the N original input modes $\hat{a}_k$, and $k = N+1 \ldots M$ for the additional blank modes $\hat{a}_k$. With an ideal (phase-free) beam splitter operation acting on two modes $\hat{c}_k$ and $\hat{c}_l$ (see chapter I),

$$\begin{pmatrix} \hat{c}'_k \\ \hat{c}'_l \end{pmatrix} = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} \hat{c}_k \\ \hat{c}_l \end{pmatrix}, \tag{V.28}$$

we define a matrix $B_{kl}(\theta)$ which is an M-dimensional identity matrix with the entries I_{kk}, I_{kl}, I_{lk}, and I_{ll} replaced by the corresponding entries of the above beam splitter matrix. Now we can use a sequence of beam splitters acting on M modes ("M-splitter", as also used in chapter III),

$$\begin{aligned} \mathcal{U}(M) \;\equiv\; & B_{M-1\,M}\left(\sin^{-1}\frac{1}{\sqrt{2}}\right) B_{M-2\,M-1}\left(\sin^{-1}\frac{1}{\sqrt{3}}\right) \\ & \times\cdots\times B_{12}\left(\sin^{-1}\frac{1}{\sqrt{M}}\right) . \end{aligned} \tag{V.29}$$

In order to concentrate the N identical inputs, we send them through an inverse N-splitter,

$$\left(\begin{array}{cccc}\hat{a}'_1 & \hat{a}'_2 & \cdots & \hat{a}'_N\end{array}\right)^T = \mathcal{U}^\dagger(N)\left(\begin{array}{cccc}\hat{a}_1 & \hat{a}_2 & \cdots & \hat{a}_N\end{array}\right)^T . \tag{V.30}$$

Again, we end up with one mode (renamed $\hat{a}_1$) having non-zero mean value and $N-1$ modes $(\hat{a}'_2 \ldots \hat{a}'_N)$ in the vacuum state. After amplifying mode $\hat{a}_1$, $\hat{a}'_1 = \sqrt{M/N}\,\hat{a}_1 + \sqrt{M/N-1}\,\hat{a}_z^\dagger$, etc., a final M-splitter operation yields the output clones:

$$\left(\begin{array}{cccc}\hat{a}''_1 & \hat{a}''_2 & \cdots & \hat{a}''_M\end{array}\right)^T = \mathcal{U}(M)\left(\begin{array}{cccc}\hat{a}'_1 & \hat{a}'_2 & \cdots & \hat{a}'_M\end{array}\right)^T , \tag{V.31}$$

with $\hat{a}'_i = \hat{a}_i$ for $i = N+1 \ldots M$.

Since the amplification produces extra noise, our cloning circuits use as little amplification as possible. However, rather surprisingly, by first amplifying each input copy $k = 1 \ldots N$ individually,

$$\begin{aligned} \hat{a}'_k &= \sqrt{\frac{M}{N}}\,\hat{a}_k + \sqrt{\frac{M}{N}-1}\,\hat{a}^\dagger_{z,k}, \\ \hat{a}'_{z,k} &= \sqrt{\frac{M}{N}-1}\,\hat{a}^\dagger_k + \sqrt{\frac{M}{N}}\,\hat{a}_{z,k}, \end{aligned} \tag{V.32}$$

a circuit can also be constructed that yields optimum fidelities. In the next step, the amplified modes are *each* sent together with $M-1$ vacuum modes $\hat{b}_{k,1}$, $\hat{b}_{k,2}$,...,$\hat{b}_{k,M-1}$ through an M-splitter

$$\left(\begin{array}{cccc}\hat{a}'_{k,1} & \hat{a}'_{k,2} & \cdots & \hat{a}'_{k,M}\end{array}\right)^T = \mathcal{U}(M)\left(\begin{array}{cccc}\hat{a}'_k & \hat{b}_{k,1} & \cdots & \hat{b}_{k,M-1}\end{array}\right)^T . \tag{V.33}$$

The NM output modes after this operation can be written as

$$\hat{a}'_{k,l} = \frac{1}{\sqrt{N}}\,\hat{a}_k + \sqrt{\frac{M-N}{MN}}\,\hat{a}^\dagger_{z,k} + \hat{d}_{k,l}\ , \tag{V.34}$$

where $l = 1 \ldots M$. The noise in each M-splitter output coming from the $M-1$ vacuum inputs is represented by mode $\hat{d}_{k,l}$ having zero mean value and quadrature variances of $(M-1)/4M$. The final step now consists of M inverse N-splitters acting on all modes with the same index l, i.e., the N modes $\hat{a}'_{k,1}$, and the N modes $\hat{a}'_{k,2}$, etc. The output modes at each N-splitter,

$$\left(\begin{array}{cccc} \hat{a}''_l & \hat{e}_{1,l} & \cdots & \hat{e}_{N-1,l} \end{array}\right)^T = \mathcal{U}^\dagger(N) \left(\begin{array}{cccc} \hat{a}'_{1,l} & \hat{a}'_{2,l} & \cdots & \hat{a}'_{N,l} \end{array}\right)^T , \tag{V.35}$$

contain only noise except for one mode,

$$\hat{a}''_l = \sum_{k=1}^{N} \left(\frac{1}{N}\,\hat{a}_k + \sqrt{\frac{M-N}{MN^2}}\,\hat{a}^\dagger_{z,k} + \frac{1}{\sqrt{N}}\,\hat{d}_{k,l} \right) . \tag{V.36}$$

Again, all M clones are optimal, however, additional noise has been introduced at the intermediate steps which results in $M(N-1)$ 'waste' output modes. We note that this particular circuit demonstrates that $N \to M$ cloning of coherent states is effectively a "classical plumbing" procedure *distributing classical amplitudes.*

Finally, we note that for squeezed-state inputs rather than coherent states, the transformations and circuits presented require all auxiliary vacuum modes (the blank modes and the ancillary mode z) be correspondingly squeezed in order to maintain optimum cloning fidelities. This means, in particular, that the amplifier mode z needs to be *controlled* which requires a device different from a simple phase-insensitive amplifier, namely a two-mode parametric amplifier. One can say that the cloning machine capable of optimal cloning of all squeezed states with *fixed* and *known* squeezing then operates in a non-universal fashion with respect to all possible squeezed states at the input [59, 58].

Let us summarize the results of this section: an optimal N-to-M continuous-variable cloning transformation for coherent states has been derived, which attains the optimum cloning fidelities. A possible experimental implementation

of this local cloner has been proposed. This implementation should be achievable with current technology since it only requires a single linear amplifier and $N + M - 2$ beam splitters. In Ref. [4], an alternative one-to-two (local) cloning scheme was proposed using three non-degenerate optical parametric amplifiers. That scheme is based on the Four-C-NOT cloning transformation in Eq. (V.7) and contains entanglement as an ingredient. By contrast, the local cloning scheme presented here does not require any entanglement. Finally, we pointed out the link between the quality of the best cloner and the minimum noise induced by the amplification of a quantum state, emphasizing that spontaneous emission is once again the mechanism that prevents the perfect cloning of quantum states of light [139, 190, 114]. In the next section, we will present a "telecloning" circuit that enables optimal cloning of coherent states without any amplification. However, entanglement will be the essential ingredient of that circuit.

2 Cloning "at a distance": telecloning

We will now turn to the main goal of this chapter and try to answer the question posed in the introduction: can we convey continuous-variable quantum information via a "multiuser quantum channel" (MQC) simultaneously to several receivers? In this context, we are particularly interested in an MQC that is capable of coherent-state cloning "at a distance" ($1 \to M$ telecloning). Such an MQC has to comply with no-cloning, but it shall operate in an optimal fashion and transmit optimal approximate clones. Furthermore, it shall represent a very efficient (ideally the most efficient) means to transfer continuous-variable quantum states, requiring the cheapest resources for its generation. For example, it might rely on entanglement as a potentially nonlocal resource, since now the output states (clones) are to emerge not from a local cloning circuit, but at receiving stations spatially separated from each other and from the sending station. Of course, the telecloning circuit can also be used for local cloning.

For qubits, telecloning has been studied theoretically, first with one input sent to two receivers [44], and more generally with one input [149] and N identical inputs [78] distributed among M receivers. The telecloning scenario with one input copy and M receivers has been extended to d-level systems [150].

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 $F^{\text{univ},2}_{\text{clon},1,M} > F_{\text{class}} = 2/3$, whereas for $1 \to M$ cloning of *coherent states* we have $F^{\text{coh st},\infty}_{\text{clon},1,M} > F_{\text{class}} = 1/2$ (see previous sections on local cloning and chapters II and IV on classical teleportation). Therefore, optimal telecloning 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 $F^{\text{univ},2}_{\text{clon},1,M} \to F_{\text{class}} = 2/3$ and $F^{\text{coh st},\infty}_{\text{clon},1,M} \to F_{\text{class}} = 1/2$ 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 creates M optimum clones and perfectly teleports one clone to each receiver using M maximally entangled two-party states [149, 150]. In fact, a much more economical strategy is that all participants share a particular multipartite entangled state as a quantum channel. Let us first see how that state may look for qubits.

a *For comparison: telecloning with qubits*

As shown in Ref. [149], an MQC state that enables qubit telecloning can be constructed from the local universal cloning transformation given in Ref. [91]. In the $1 \to M$ case, that transformation acts as follows on the input qubit state $|s\rangle_X = \alpha|0\rangle_X + \beta|1\rangle_X$, the $M-1$ blank qubits in the state $|0\cdots0\rangle_B$, and an

ancilla system with at least M levels initially in the state $|0\cdots0\rangle_A$:

$$\hat{U}\left(|s\rangle_X \otimes |0\cdots0\rangle_A \otimes |0\cdots0\rangle_B\right) = \alpha|\phi_0\rangle_{AC} + \beta|\phi_1\rangle_{AC} \,. \tag{V.37}$$

Here, we follow the notation of Ref. [149]; the input qubit "X" and the $M-1$ blank qubits "B" are after the transformation represented by the M qubits "C" holding the copies. The states in the outgoing superposition are defined as

$$\begin{aligned}
|\phi_0\rangle_{AC} &= \hat{U}\,|0\rangle_X \otimes |0\cdots0\rangle_A \otimes |0\cdots0\rangle_B \\
&= \sum_{j=0}^{M-1} a_j |A_j\rangle_A \otimes |\{0, M-j\},\{1,j\}\rangle_C \,, \\
|\phi_1\rangle_{AC} &= \hat{U}\,|1\rangle_X \otimes |0\cdots0\rangle_A \otimes |0\cdots0\rangle_B \\
&= \sum_{j=0}^{M-1} a_j |A_{M-1-j}\rangle_A \otimes |\{0, j\},\{1,M-j\}\rangle_C \,, \\
a_j &= \sqrt{\frac{2(M-j)}{M(M+1)}} \,,
\end{aligned} \tag{V.38}$$

with the M orthogonal normalized ancilla states $|A_j\rangle_A$ and the symmetric normalized M-qubit state $|\{0, M-j\},\{1,j\}\rangle$ where $M-j$ qubits are in state $|0\rangle$ and j qubits are in state $|1\rangle$ [e.g., for $M=3$ and $j=1$, $|\{0,2\},\{1,1\}\rangle = |W\rangle$ of Eq. (II.19)]. Although only M ancilla levels (or $\log_2 M$ ancilla qubits) are needed, a more convenient form for the ancilla system is the $(M-1)$-qubit state

$$|A_j\rangle_A \equiv |\{0, M-1-j\},\{1,j\}\rangle_A \,. \tag{V.39}$$

The states $|\phi_0\rangle_{AC}$ and $|\phi_1\rangle_{AC}$ are then $(2M-1)$-qubit states with the properties

$$\begin{aligned}
\hat{\sigma}_3 \otimes \cdots \otimes \hat{\sigma}_3 |\phi_0\rangle_{AC} &= |\phi_0\rangle_{AC} \,, \\
\hat{\sigma}_3 \otimes \cdots \otimes \hat{\sigma}_3 |\phi_1\rangle_{AC} &= -|\phi_1\rangle_{AC} \,, \\
\hat{\sigma}_1 \otimes \cdots \otimes \hat{\sigma}_1 |\phi_{0(1)}\rangle_{AC} &= |\phi_{1(0)}\rangle_{AC} \,,
\end{aligned} \tag{V.40}$$

where $\hat{\sigma}_i$ are the Pauli operators [Eq. (II.51)]. Each of the M optimum qubit clones are obtained from the output state of Eq. (V.37) by tracing out the ancilla

and $M-1$ C-qubits, yielding mixed states of the form [91]

$$\hat{\rho} = F^{\text{univ},2}_{\text{clon},1,M} \, |s\rangle\langle s| + (1 - F^{\text{univ},2}_{\text{clon},1,M}) \, |\tilde{s}\rangle\langle\tilde{s}| \, , \tag{V.41}$$

with the state $|\tilde{s}\rangle$ orthogonal to $|s\rangle$ [see Eq. (V.3)].

Also the qubit telecloning scheme would be optimal when the receivers share the output state of Eq. (V.37) at the end (with the M C-qubits in the hands of the M receivers). This can be achieved exactly by using the following entangled $2M$-qubit state as an MQC [149]:

$$|\psi_{\text{MQC}}\rangle_{PAC} = (|0\rangle_P \otimes |\phi_0\rangle_{AC} + |1\rangle_P \otimes |\phi_1\rangle_{AC})/\sqrt{2} \, , \tag{V.42}$$

with $|\phi_0\rangle_{AC}$ and $|\phi_1\rangle_{AC}$ from Eqs. (V.38). The "port" qubit P shall be in the sender's (Alice's) hands (and also the ancilla), the C-qubits are at the different locations of the M receivers. Now Alice wants to teleclone the unknown input qubit state $|s\rangle_X = \alpha|0\rangle_X + \beta|1\rangle_X$ to all receivers. That the telecloning protocol works in a similar way as the simple $1 \to 1$ quantum teleportation protocol can be seen via the decomposition [149]

$$\begin{aligned} |s\rangle_X \otimes |\psi_{\text{MQC}}\rangle_{PAC} \;=\; & \frac{1}{2}|\Phi^+\rangle_{XP}(\alpha|\phi_0\rangle_{AC} + \beta|\phi_1\rangle_{AC}) \\ & + \frac{1}{2}|\Phi^-\rangle_{XP}(\alpha|\phi_0\rangle_{AC} - \beta|\phi_1\rangle_{AC}) \\ & + \frac{1}{2}|\Psi^+\rangle_{XP}(\beta|\phi_0\rangle_{AC} + \alpha|\phi_1\rangle_{AC}) \\ & + \frac{1}{2}|\Psi^-\rangle_{XP}(\beta|\phi_0\rangle_{AC} - \alpha|\phi_1\rangle_{AC}) \, , \end{aligned} \tag{V.43}$$

where the XP-states are the four Bell states [Eq. (II.11)]. After Alice's Bell measurement on qubits X and P, the receivers share either directly the output state of Eq. (V.37) or a state unitarily related to it according to Eq. (V.40). Thus, final unitary transformations of the $2M-1$ AC-qubits, performed locally on each qubit and depending on Alice's classical result accomplish the optimal telecloning.

How much entanglement was actually needed in this qubit telecloning scenario? We know that it is hard to quantify multipartite entanglement, but the

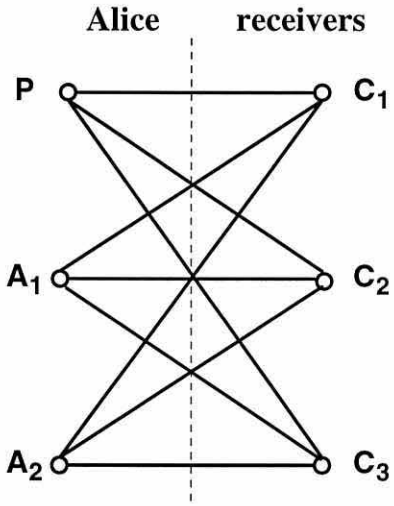

Figure V.3: The symmetry of the qubit telecloning state from Ref. [149] for $M = 3$ with a port qubit P, two ancilla qubits A_1 and A_2, and the three clones C_1, C_2, and C_3 (figure as in Ref. [149]). The lines indicate bipartite entanglement when the other qubits are traced out.

MQC in Eq. (V.42) turns out to have a convenient bipartite structure. In the form [149]

$$|\psi_{\mathrm{MQC}}\rangle_{PAC} = \frac{1}{\sqrt{M+1}} \sum_{j=0}^{M} |\{0, M-j\}, \{1, j\}\rangle_{PA} \otimes |\{0, M-j\}, \{1, j\}\rangle_{C} \,, \tag{V.44}$$

the state's symmetry is revealed. It is symmetric among all PA-qubits and all C-qubits, but also invariant under the exchange of qubits between the two "sides" PA (Alice's side) and C (the receivers' side, see Fig. V.3). Due to this symmetry, any of the $2M$ qubits can function as the telecloning port for sending quantum information to the opposite side.

Now, there are different ways to quantify the bipartite entanglement inherent in the qubit MQC: first, the state can be rewritten as the maximally entangled

state of two $(M+1)$-level particles [149]

$$|\psi_{\mathrm{MQC}}\rangle_{PAC} = \frac{1}{\sqrt{M+1}} \sum_{j=0}^{M} |\, j \,\rangle_{PA} \otimes |\, j \,\rangle_{C} \,, \tag{V.45}$$

with the $M+1$ symmetric states $|\{0, M-j\}, \{1, j\}\rangle$ corresponding to the $(M+1)$-level basis states $|\, j \,\rangle$, $|\, j \,\rangle \equiv |\{0, M-j\}, \{1, j\}\rangle$. In this form, the amount of entanglement between the two sides, PA and C, is given by the partial von Neumann entropy $E_{\mathrm{v.N.}} = \log_2(M+1)$ (in ebits).

Another way to assess and quantify the bipartite entanglement contained in $|\psi_{\mathrm{MQC}}\rangle_{PAC}$ can be immediately found by looking at the form [see Eq. (V.42)]

$$\begin{aligned} |\psi_{\mathrm{MQC}}\rangle_{PAC} &= \frac{1}{\sqrt{M+1}} \\ &\quad \times \sum_{j=0}^{M} (|0\rangle_P \, {}_P\langle 0| \{0, M-j\}, \{1, j\}\rangle_{PA} \otimes |\{0, M-j\}, \{1, j\}\rangle_C \\ &\qquad + |1\rangle_P \, {}_P\langle 1| \{0, M-j\}, \{1, j\}\rangle_{PA} \otimes |\{0, M-j\}, \{1, j\}\rangle_C) \\ &= \frac{1}{\sqrt{2}} (|0\rangle_P \otimes |\phi_0\rangle_{AC} + |1\rangle_P \otimes |\phi_1\rangle_{AC}) \,, \end{aligned} \tag{V.46}$$

with the two basis states consisting of $2M-1$ qubits

$$|\phi_k\rangle_{AC} = \sqrt{\frac{2}{M+1}} \sum_{j=0}^{M} {}_P\langle k| \{0, M-j\}, \{1, j\}\rangle_{PA} \otimes |\{0, M-j\}, \{1, j\}\rangle_C \,, \tag{V.47}$$

where $k = 0, 1$ [see Eq. (V.38) with the symmetric and normalized $(M-1)$-qubit states $|A_j\rangle_A = |\{0, M-1-j\}, \{1, j\}\rangle_A = \sqrt{M/(M-j)}\, {}_P\langle 0| \{0, M-j\}, \{1, j\}\rangle_{PA}$ etc.]. In order to demonstrate the identity of the forms Eq. (V.42) and Eq. (V.44), we have used $|0\rangle_P \, {}_P\langle 0| + |1\rangle_P \, {}_P\langle 1| = \mathbb{1}$ in Eq. (V.46).

In the form of Eq. (V.42), the bipartite entanglement between the port qubit and all the remaining qubits (in particular, all the C-qubits, because there is no entanglement left between the port qubit and the ancilla qubits after tracing out all the C-qubits) turns out to be $E_{\mathrm{v.N.}} = \log_2 2 = 1$ ebit, just as for a maximally entangled Bell state. A similar approach yields for the corresponding MQC that

enables optimal telecloning of arbitrary d-level quantum states (instead of $d = 2$ for qubits) maximum bipartite entanglement with $E_{\text{v.N.}} = \log_2 d$ ebits between the sender and all receivers [150].

b Multiuser quantum channels for continuous variables

In this section, we propose entangled $(M+1)$-mode quantum states as a multiuser quantum channel for continuous-variable communication. Arbitrary quantum states can be sent via this channel *simultaneously* to M remote and separated locations with equal minimum excess noise in each output mode. For a set of coherent-state inputs, the channel realizes optimal symmetric $1 \to M$ cloning at a distance ("telecloning"). It also provides the optimal cloning of coherent states without the need of amplifying the state of interest.

We know from the previous section on discrete-variable telecloning that a certain class of optimum MQC's exhibits maximum bipartite entanglement between the sender and all receivers (with $\log_2 d$ ebits for d-level particles). This suggests that the optimum continuous-variable MQC we are looking for also contains maximum bipartite entanglement. The entanglement of the qubit state $(d = 2)$, $\log_2 2 = 1$ ebit, however, is larger than we expect from the most frugal scheme. It should become vanishingly small as $M \to \infty$, since $F_{\text{clon},1,M}^{\text{univ},2} \to F_{\text{class}} = 2/3$ in that limit. The analogous observation applies to coherent-state cloning: $F_{\text{clon},1,M}^{\text{coh st},\infty} \to F_{\text{class}} = 1/2$ as $M \to \infty$. However, as opposed to the local continuous-variable cloners which do not need any entanglement as a basic ingredient, the continuous-variable telecloner must have entanglement, since $F_{\text{clon},1,M}^{\text{coh st},\infty} > F_{\text{class}} = 1/2$ for all finite M. In a continuous-variable scenario based on the quadratures of single electromagnetic modes, multipartite entangled states can be generated using squeezers and beam splitters, as we know from chapter III. Any maximum bipartite entanglement involved would require infinite squeezing. Do we really need to rely on infinite-squeezing resources or can we find a more economical (and physical!) MQC built from finite squeezing?

Let us now consider the following pure-state $(M+1)$-mode Wigner function:

$$W_{\mathrm{MQC}}(\mathbf{x},\mathbf{p}) = \left(\frac{2}{\pi}\right)^{M+1} \exp\left\{ \begin{aligned} &- 2e^{-2(s+r_1)} \left(\sin\theta_0\, x_1 + \frac{\cos\theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} x_i \right)^2 \\ &- 2e^{+2(s+r_1)} \left(\sin\theta_0\, p_1 + \frac{\cos\theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} p_i \right)^2 \\ &- 2e^{-2(s-r_2)} \left(\cos\theta_0\, x_1 - \frac{\sin\theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} x_i \right)^2 \\ &- 2e^{+2(s-r_2)} \left(\cos\theta_0\, p_1 - \frac{\sin\theta_0}{\sqrt{M}} \sum_{i=2}^{M+1} p_i \right)^2 \\ &- \frac{1}{M} \sum_{i,j=2}^{M+1} \left[e^{-2s}(x_i - x_j)^2 + e^{+2s}(p_i - p_j)^2 \right] \end{aligned} \right\}, \tag{V.48}$$

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

$$\frac{1}{\sqrt{M+1}} \leq \sin\theta_0 \leq \sqrt{\frac{M}{M+1}}\,, \tag{V.49}$$

$$e^{-2r_1} = \frac{\sqrt{M}\sin\theta_0 - \cos\theta_0}{\sqrt{M}\sin\theta_0 + \cos\theta_0}\,, \quad e^{-2r_2} = \frac{\sqrt{M}\cos\theta_0 - \sin\theta_0}{\sqrt{M}\cos\theta_0 + \sin\theta_0}\,. \tag{V.50}$$

This Wigner function describes an appropriate candidate for an MQC, because the state enables optimal $1 \to M$ telecloning of coherent states (or squeezed states with known and fixed squeezing s).

We will explain the meaning of the different parameters in W_{MQC} later and first look at the potential telecloning protocol in which W_{MQC} is used. Let us assume $s = 0$ and $\sin\theta_0 = 1/\sqrt{2}$. Mode 1 may be used as a "port" at the sending station and is combined at a phase-free 50:50 beam splitter with mode "in" which is in an *arbitrary* quantum state described by W_{in}. The whole system after the beam splitter (we call the two modes emerging from the beam splitter

$\alpha_{\rm u} = x_{\rm u} + ip_{\rm u}$ and $\alpha_{\rm v} = x_{\rm v} + ip_{\rm v}$) can be written as

$$W(\alpha_{\rm u}, \alpha_{\rm v}, \alpha_2, ..., \alpha_{M+1}) = \int dx_{\rm in} dp_{\rm in} W_{\rm in}(x_{\rm in}, p_{\rm in}) \times W_{\rm MQC}\left[\alpha_1 = \frac{1}{\sqrt{2}}(\alpha_{\rm v} - \alpha_{\rm u}), \alpha_2, ..., \alpha_{M+1}\right] \times \delta\left[\frac{1}{\sqrt{2}}(x_{\rm u} + x_{\rm v}) - x_{\rm in}\right] \delta\left[\frac{1}{\sqrt{2}}(p_{\rm u} + p_{\rm v}) - p_{\rm in}\right] . \quad \text{(V.51)}$$

The "Bell detection", i.e., homodyne detections of $x_{\rm u} = (x_{\rm in} - x_1)/\sqrt{2}$ and $p_{\rm v} = (p_{\rm in} + p_1)/\sqrt{2}$ can be described by the unnormalized reduced Wigner function after integrating over $x_{\rm v}$ and $p_{\rm u}$:

$$\propto \int dx\, dp\, W_{\rm in}(x, p)\, W_{\rm MQC}\left[x - \sqrt{2}x_{\rm u} + i(\sqrt{2}p_{\rm v} - p), \alpha_2, ..., \alpha_{M+1}\right] . \quad \text{(V.52)}$$

After detection, the M distant and separated locations of modes 2 through $M+1$ *each* need to be provided with the classical information of the measurement results. Finally, "displacing" all these modes as $x_{2...M+1} \longrightarrow x_{2...M+1} + \sqrt{2}x_{\rm u}$ and $p_{2...M+1} \longrightarrow p_{2...M+1} + \sqrt{2}p_{\rm v}$, we obtain the ensemble description of the M-mode output Wigner function after integrating out $x_{\rm u}$ and $p_{\rm v}$ for an ensemble of input states

$$\begin{aligned} W_{\rm out}(\alpha_2, ..., \alpha_{M+1}) &= \frac{2^M}{\pi^M (M-1)} \\ &\times \exp\left\{ + \frac{1}{M}\left[\left(\sum_{i=2}^{M+1} x_i\right)^2 - \sum_{i,j=2}^{M+1}(x_i - x_j)^2 + \left(\sum_{i=2}^{M+1} p_i\right)^2 - \sum_{i,j=2}^{M+1}(p_i - p_j)^2\right]\right\} \\ &\times \int dx\, dp\, W_{\rm in}(x, p)\, \exp[-(x^2 + p^2)] \\ &\quad \times \exp\left\{ - \frac{1}{2}\frac{\sqrt{M}+1}{\sqrt{M}-1}\left[\left(x - \frac{1}{\sqrt{M}}\sum_{i=2}^{M+1} x_i\right)^2 + \left(p - \frac{1}{\sqrt{M}}\sum_{i=2}^{M+1} p_i\right)^2\right]\right. \\ &\quad \left. - \frac{1}{2}\frac{\sqrt{M}-1}{\sqrt{M}+1}\left[\left(x + \frac{1}{\sqrt{M}}\sum_{i=2}^{M+1} x_i\right)^2 + \left(p + \frac{1}{\sqrt{M}}\sum_{i=2}^{M+1} p_i\right)^2\right]\right\}. \end{aligned} \quad \text{(V.53)}$$

This Wigner function is totally symmetric with respect to all M modes. We can therefore choose an arbitrary mode and trace out (integrate out) the remaining $M-1$ modes which leaves us with the one-mode Wigner function of each individual clone

$$\mathrm{Tr}_{3\ldots M+1} W_{\mathrm{out}}(\alpha_2, ..., \alpha_{M+1}) = W_{\mathrm{clon}}(\alpha_2) \equiv W_{\mathrm{clon}}(\alpha). \tag{V.54}$$

The cloned state $W_{\mathrm{clon}}(\alpha) = W_{\mathrm{clon}}(x,p)$ is a convolution of W_{in} with a bivariate Gaussian with the excess noise variances λ_x and λ_p,

$$\begin{aligned} W_{\mathrm{clon}}(x,p) &= \frac{1}{2\pi\sqrt{\lambda_x\lambda_p}} \int dx'dp' W_{\mathrm{in}}(x',p') \\ &\qquad \times \exp\left[-\frac{(x-x')^2}{2\lambda_x} - \frac{(p-p')^2}{2\lambda_p}\right], \end{aligned} \tag{V.55}$$

where our choice $s=0$ leads in Eq. (V.54) to excess noise symmetric in phase space [3], $\lambda_x = \lambda_p = (M-1)/2M$. Recall that in our units, a quadrature's vacuum variance is $1/4$, i.e., $[\hat{x},\hat{p}] = i/2$ and $[\hat{a},\hat{a}^\dagger] = 1$ with $\hat{a} = \hat{x} + i\hat{p}$. The excess noise in each quadrature of each output mode of the telecloning protocol corresponds exactly to the minimal excess noise for optimal approximate symmetric $1 \to M$ cloning from Eq. (V.15), $\bar{\lambda}_{\mathrm{clon}}(1,M) = (M-1)/2M$.

Let us express the fidelity of the (tele-)cloning process in the Wigner representation,

$$F \equiv \langle\psi_{\mathrm{in}}|\hat{\rho}_{\mathrm{clon}}|\psi_{\mathrm{in}}\rangle = \pi \int d^2\alpha W_{\mathrm{in}}(\alpha) W_{\mathrm{clon}}(\alpha)\ . \tag{V.56}$$

Now, for the Wigner function a pure coherent-state or squeezed-state input (with mean values x_0 and p_0 and squeezing parameter s) is:

$$W_{\mathrm{in}}(x,p) = \frac{2}{\pi}\exp[-2e^{-2s}(x-x_0)^2 - 2e^{+2s}(p-p_0)^2]. \tag{V.57}$$

[3] It is not easy to prove the validity of Eq. (V.54) for arbitrary M, but one can verify it for small M. For arbitrary M, one can rely on a proof in the Heisenberg picture, which we will present below.

Since the mean values are conserved by cloning (the covariance condition is satisfied through "unit-gain displacements"), the fidelity does not depend on x_0 and p_0, and without loss of generality we can set $x_0 = p_0 = 0$. Our MQC in Eq. (V.48) with $s = 0$ exactly realizes optimal symmetric $1 \to M$ telecloning of coherent states [$s = 0$ also in Eq. (V.57)], $F = F^{\text{coh st},\infty}_{\text{clon},1,M} = M/(2M-1)$.

Furthermore, the above protocol demonstrates that our MQC is capable of transferring *arbitrary* quantum states W_{in} simultaneously to M remote and separated receivers with equal minimum excess noise in each output mode. Less excess noise emerging from each output for arbitrary W_{in} would imply that we could also beat the optimal-cloning limit for coherent-state inputs. Note that minimum excess noise symmetrically added in phase space does not necessarily ensure optimum telecloning *fidelities* at the outputs. It does for coherent-state inputs, but squeezed-state inputs [$s \neq 0$ in Eq. (V.57)] require asymmetric excess noise, $\lambda_x = e^{+2s}(M-1)/2M$, $\lambda_p = e^{-2s}(M-1)/2M$, according to $F = 2/[\sqrt{(4\lambda_x e^{-4s} + 2e^{-2s})(4\lambda_p e^{4s} + 2e^{2s})}]$ from Eq. (V.56). The correct squeezing parameter s also in W_{MQC}, however, ensures optimum fidelities, just as for the local "non-universal" Gaussian cloner which has a similar s-dependence. The structure of W_{MQC} becomes clearer, when we look at the generation of this state.

The recipe for building such an MQC is now as follows (see Fig. V.4): first produce a bipartite entangled state by combining two squeezed vacua, one squeezed in p with r_1 and the other one squeezed in x with r_2, at a phase-free beam splitter with reflectivity/transmittance parameter $\theta = \theta_0$. Then keep one half as a "port" mode (our mode 1) and send the other half together with $M-1$ ancilla modes through an M-splitter. The ancilla modes $i = 3...M+1$, $\hat{a}'_i = \cosh s\, \hat{a}_i^{(0)} + \sinh s\, \hat{a}_i^{(0)\dagger}$ with $\hat{a}_3^{(0)}$, $\hat{a}_4^{(0)}$, ..., $\hat{a}_{M+1}^{(0)}$ being vacuum modes, are either vacua $s = 0$ or squeezed vacua $s \neq 0$. In the latter case, in order to obtain W_{MQC}, the squeezing of the two inputs of the first beam splitter also needs to be modified by the same amount (given by s). The annihilation operators of the

initial modes $\hat{a}'_j$ before the beam splitters, $j = 1...M+1$, are then given by

$$\begin{aligned}
\hat{a}'_1 &= \cosh(r_1+s)\hat{a}_1^{(0)} + \sinh(r_1+s)\hat{a}_1^{(0)\dagger}, \\
\hat{a}'_2 &= \cosh(r_2-s)\hat{a}_2^{(0)} - \sinh(r_2-s)\hat{a}_2^{(0)\dagger}, \\
\hat{a}'_3 &= \cosh s\hat{a}_3^{(0)} + \sinh s\hat{a}_3^{(0)\dagger}, \\
\hat{a}'_4 &= \cosh s\hat{a}_4^{(0)} + \sinh s\hat{a}_4^{(0)\dagger}, \\
&\vdots \qquad\qquad \vdots \qquad \vdots \\
\hat{a}'_{M+1} &= \cosh s\hat{a}_{M+1}^{(0)} + \sinh s\hat{a}_{M+1}^{(0)\dagger}.
\end{aligned} \tag{V.58}$$

Note that the modes $\hat{a}_1^{(0)}$ and $\hat{a}_2^{(0)}$ are also vacuum modes.

By using the ideal phase-free beam splitter operation from Eq. (V.28), with $B_{kl}(\theta)$ representing an $(M+1)$-dimensional identity matrix with the entries I_{kk}, I_{kl}, I_{lk}, and I_{ll} replaced by the corresponding entries of the beam splitter matrix in Eq. (V.28), the MQC-generating circuit can be written as

$$\left(\begin{array}{cccc} \hat{b}_1 & \hat{b}_2 & \cdots & \hat{b}_{M+1} \end{array} \right)^T = \mathcal{U}_{\mathrm{MQC}}(M+1) \left(\begin{array}{cccc} \hat{a}'_1 & \hat{a}'_2 & \cdots & \hat{a}'_{M+1} \end{array} \right)^T, \tag{V.59}$$

with

$$\begin{aligned}
\mathcal{U}_{\mathrm{MQC}}(M+1) \equiv\ & B_{M\,M+1}\left(\sin^{-1}\frac{1}{\sqrt{2}}\right) B_{M-1\,M}\left(\sin^{-1}\frac{1}{\sqrt{3}}\right) \\
& \times \cdots \times B_{34}\left(\sin^{-1}\frac{1}{\sqrt{M-1}}\right) B_{23}\left(\sin^{-1}\frac{1}{\sqrt{M}}\right) B_{12}\left(\theta_0\right) .
\end{aligned} \tag{V.60}$$

The first beam splitter, acting on modes $\hat{a}'_1$ and $\hat{a}'_2$, has reflectivity/transmittance parameter $\theta = \theta_0$. The remaining beam splitters represent an M-splitter (see Fig. V.4). In Eq. (V.59), the output modes $\hat{b}_j$ correspond to the $M+1$ modes of the MQC state described by W_{MQC} in Eq. (V.48).

In order to prove the optimality of W_{MQC}, let us look at the individual quadra-

tures of that state:

$$(\hat{x}_1\ \hat{p}_1\ \hat{x}_2\ \hat{p}_2\ \hat{x}_3\ \hat{p}_3\ \cdots\ \hat{x}_{M+1}\ \hat{p}_{M+1})^T$$

$$= \begin{pmatrix}
\sin\theta_0 & 0 & \cos\theta_0 & 0 & 0 & 0 & 0 & \cdots \\
0 & \sin\theta_0 & 0 & \cos\theta_0 & 0 & 0 & 0 & \cdots \\
\frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \sqrt{\frac{M-1}{M}} & 0 & 0 & \cdots \\
0 & \frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \sqrt{\frac{M-1}{M}} & 0 & \cdots \\
\frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \frac{-1}{\sqrt{M(M-1)}} & 0 & \sqrt{\frac{M-2}{M-1}} & \cdots \\
0 & \frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \frac{-1}{\sqrt{M(M-1)}} & 0 & \cdots \\
\frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \frac{-1}{\sqrt{M(M-1)}} & 0 & \frac{-1}{\sqrt{(M-1)(M-2)}} & \cdots \\
0 & \frac{\cos\theta_0}{\sqrt{M}} & 0 & \frac{-\sin\theta_0}{\sqrt{M}} & 0 & \frac{-1}{\sqrt{M(M-1)}} & 0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{pmatrix}$$

$$\times\ (\hat{x}'_1\ \hat{p}'_1\ \hat{x}'_2\ \hat{p}'_2\ \hat{x}'_3\ \hat{p}'_3\ \cdots\ \hat{x}'_{M+1}\ \hat{p}'_{M+1})^T\ . \tag{V.61}$$

Here, we have used the notation $\hat{b}_j = \hat{x}_j + i\hat{p}_j$ and $\hat{a}'_j = \hat{x}'_j + i\hat{p}'_j$. The initial quadratures before the beam splitters are

$$\begin{aligned}
\hat{x}'_1 &= e^{+r_1+s}\hat{x}_1^{(0)}, \qquad & \hat{p}'_1 &= e^{-r_1-s}\hat{p}_1^{(0)}, \\
\hat{x}'_2 &= e^{-r_2+s}\hat{x}_2^{(0)}, \qquad & \hat{p}'_2 &= e^{+r_2-s}\hat{p}_2^{(0)},
\end{aligned} \tag{V.62}$$

and

$$\hat{x}'_i = e^{+s}\hat{x}_i^{(0)}, \qquad \hat{p}'_i = e^{-s}\hat{p}_i^{(0)}, \tag{V.63}$$

with $i = 3...M+1$. After the Bell detection via quadrature measurements of $\hat{x}_{\rm u} = (\hat{x}_{\rm in} - \hat{x}_1)/\sqrt{2}$ and $\hat{p}_{\rm v} = (\hat{p}_{\rm in} + \hat{p}_1)/\sqrt{2}$ and after the corresponding (unit-gain)

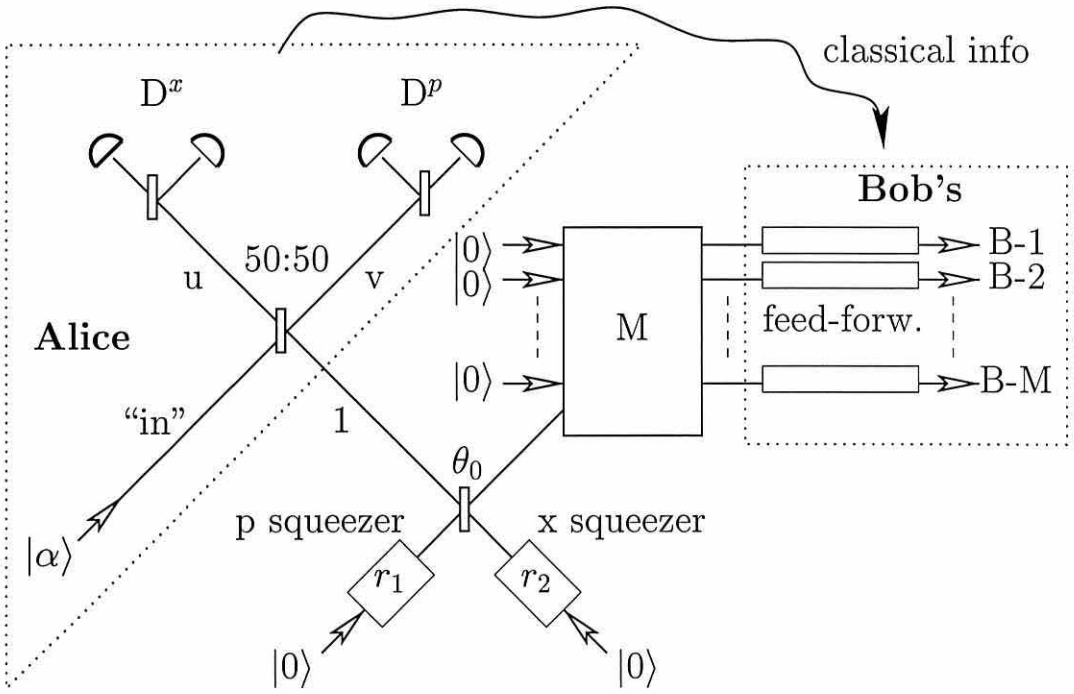

Figure V.4: Optimal telecloning of an arbitrary coherent state from Alice to M spatially separated Bob's. Alice and the Bob's share a particularly simple multipartite entangled state as an MQC (see text).

displacements of the remaining M modes at the receiving stations [4], $\hat{x}_{2\ldots M+1} \longrightarrow \hat{x}^{\text{telecl}}_{2\ldots M+1} = \hat{x}_{2\ldots M+1} + \sqrt{2}\hat{x}_{\text{u}}$ and $\hat{p}_{2\ldots M+1} \longrightarrow \hat{p}^{\text{telecl}}_{2\ldots M+1} = \hat{p}_{2\ldots M+1} + \sqrt{2}\hat{p}_{\text{v}}$, the quadratures of the telecloned modes become

$$\hat{x}_2^{\text{telecl}} = \hat{x}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} - \sin\theta_0\right)\hat{x}'_1 - \left(\frac{\sin\theta_0}{\sqrt{M}} + \cos\theta_0\right)\hat{x}'_2 + \sqrt{\frac{M-1}{M}}\hat{x}'_3,$$

$$\hat{p}_2^{\text{telecl}} = \hat{p}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} + \sin\theta_0\right)\hat{p}'_1 - \left(\frac{\sin\theta_0}{\sqrt{M}} - \cos\theta_0\right)\hat{p}'_2 + \sqrt{\frac{M-1}{M}}\hat{p}'_3,$$

[4] For simplicity, here we do not explicitly include a reduction of $\hat{x}_{\text{u}}$ and $\hat{p}_{\text{v}}$ due to the measurements. Instead, we directly use operator displacements with the "measured operators" $\hat{x}_{\text{u}}$ and $\hat{p}_{\text{v}}$. For a more accurate treatment of the "collapse" due to the Bell measurement in the Heisenberg picture, we refer to the $1 \to 1$ quantum teleportation protocol in chapter IV.

$$
\begin{aligned}
\hat{x}_3^{\text{telecl}} &= \hat{x}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} - \sin\theta_0\right)\hat{x}_1' - \left(\frac{\sin\theta_0}{\sqrt{M}} + \cos\theta_0\right)\hat{x}_2' - \frac{1}{\sqrt{M(M-1)}}\hat{x}_3' \\
&\qquad + \sqrt{\frac{M-2}{M-1}}\hat{x}_4', \\
\hat{p}_3^{\text{telecl}} &= \hat{p}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} + \sin\theta_0\right)\hat{p}_1' - \left(\frac{\sin\theta_0}{\sqrt{M}} - \cos\theta_0\right)\hat{p}_2' - \frac{1}{\sqrt{M(M-1)}}\hat{p}_3' \\
&\qquad + \sqrt{\frac{M-2}{M-1}}\hat{p}_4', \\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
\hat{x}_{M+1}^{\text{telecl}} &= \hat{x}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} - \sin\theta_0\right)\hat{x}_1' - \left(\frac{\sin\theta_0}{\sqrt{M}} + \cos\theta_0\right)\hat{x}_2' - \cdots, \\
\hat{p}_{M+1}^{\text{telecl}} &= \hat{p}_{\text{in}} + \left(\frac{\cos\theta_0}{\sqrt{M}} + \sin\theta_0\right)\hat{p}_1' - \left(\frac{\sin\theta_0}{\sqrt{M}} - \cos\theta_0\right)\hat{p}_2' - \cdots.
\end{aligned}
\tag{V.64}
$$

In these Heisenberg equations, it becomes very clear that the use of unit-gain displacements ensures covariance: any coherent-state input "in" ($s = 0$) would emerge at each receiving station with the same quality, i.e., with the same fidelity. In other words, the clones always contain the correct mean amplitude of the input state (independent of its particular value) plus an excess noise also independent of the particular coherent-state input. This excess noise in the two quadratures according to Eq. (V.64) becomes with Eq. (V.62), Eq. (V.63), and Eq. (V.50)

$$
\begin{aligned}
\lambda_x &= \left(\frac{\cos\theta_0}{\sqrt{M}} - \sin\theta_0\right)^2 \langle(\Delta\hat{x}_1')^2\rangle + \left(\frac{\sin\theta_0}{\sqrt{M}} + \cos\theta_0\right)^2 \langle(\Delta\hat{x}_2')^2\rangle \\
&\quad + \frac{M-1}{M}\langle(\Delta\hat{x}_3')^2\rangle \\
&= \Bigg[\frac{(\cos\theta_0 - \sqrt{M}\sin\theta_0)^2(\sqrt{M}\sin\theta_0 + \cos\theta_0)}{M(\sqrt{M}\sin\theta_0 - \cos\theta_0)} \\
&\quad + \frac{(\sin\theta_0 + \sqrt{M}\cos\theta_0)^2(\sqrt{M}\cos\theta_0 - \sin\theta_0)}{M(\sqrt{M}\cos\theta_0 + \sin\theta_0)} + \frac{M-1}{M}\Bigg] e^{+2s}\langle(\Delta\hat{x})^2\rangle_{\text{vacuum}},
\end{aligned}
$$

$$\begin{aligned}
\lambda_p &= \left(\frac{\cos\theta_0}{\sqrt{M}} + \sin\theta_0\right)^2 \langle(\Delta\hat{p}_1')^2\rangle + \left(\frac{\sin\theta_0}{\sqrt{M}} - \cos\theta_0\right)^2 \langle(\Delta\hat{p}_2')^2\rangle \\
&\quad + \frac{M-1}{M} \langle(\Delta\hat{p}_3')^2\rangle \\
&= \Big[\frac{(\cos\theta_0 + \sqrt{M}\sin\theta_0)^2(\sqrt{M}\sin\theta_0 - \cos\theta_0)}{M(\sqrt{M}\sin\theta_0 + \cos\theta_0)} \\
&\quad + \frac{(\sin\theta_0 - \sqrt{M}\cos\theta_0)^2(\sqrt{M}\cos\theta_0 + \sin\theta_0)}{M(\sqrt{M}\cos\theta_0 - \sin\theta_0)} + \frac{M-1}{M}\Big] e^{-2s}\langle(\Delta\hat{p})^2\rangle_{\text{vacuum}}.
\end{aligned} \tag{V.65}$$

Taking into account Eq. (V.49), we finally obtain

$$\begin{aligned}
\lambda_x &= \frac{1}{4M} e^{+2s}[(\sqrt{M}\sin\theta_0 - \cos\theta_0)(\sqrt{M}\sin\theta_0 + \cos\theta_0) \\
&\qquad + (\sqrt{M}\cos\theta_0 + \sin\theta_0)(\sqrt{M}\cos\theta_0 - \sin\theta_0) + M - 1] \\
&= e^{+2s}\frac{M-1}{2M} = e^{+2s}\bar{\lambda}_{\text{clon}}(1, M), \\
\lambda_p &= \frac{1}{4M} e^{-2s}[(\sqrt{M}\sin\theta_0 + \cos\theta_0)(\sqrt{M}\sin\theta_0 - \cos\theta_0) \\
&\qquad + (\sqrt{M}\cos\theta_0 - \sin\theta_0)(\sqrt{M}\cos\theta_0 + \sin\theta_0) + M - 1] \\
&= e^{-2s}\frac{M-1}{2M} = e^{-2s}\bar{\lambda}_{\text{clon}}(1, M).
\end{aligned} \tag{V.66}$$

This result confirms the optimal telecloning of arbitrary coherent states for $s = 0$. Note that the optimality is independent of the particular choice of the reflectivity/transmittance parameter θ_0 of the first beam splitter, as long as Eq. (V.49) and Eq. (V.50) are fulfilled. For equal squeezers $r_1 = r_2$, optimality requires a 50:50 beam splitter, and vice versa. Either θ_0 or r_1, r_2 can be arbitrarily chosen within the range allowed by Eq. (V.49) and Eq. (V.50).

Also for an alphabet of squeezed states with known and fixed squeezing $s \neq 0$, the optimum telecloning fidelities are maintained due to the s-squeezers for the generation of the MQC. The s-squeezers play exactly the same role as for local cloning, namely to switch between different squeezing of the input states. These instructions imply that, although W_{MQC} is an entangled multi-mode or multi-party state, it is actually *bipartite* entanglement between mode 1 and the M

other modes that makes telecloning possible. The squeezing responsible for the entanglement corresponds to $|10\log_{10}[(\sqrt{M}-1)/(\sqrt{M}+1)]|$ dB (if $r_1 = r_2$), which 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 $F^{\text{coh st},\infty}_{\text{clon},1,M} = M/(2M-1)$ to $F_{\text{class}} = 1/2$.

In order to derive the Wigner function W_{MQC} in Eq. (V.48), one can look at the Heisenberg operator equation Eq. (V.61). It describes the output quadratures of the beam splitters in terms of the input quadratures and has the structure $\mathbf{q}_{\text{out}} = \mathbf{A}\mathbf{q}_{\text{in}}$, where $\mathbf{q}_{\text{in}} = (x'_1, p'_1, x'_2, p'_2, ..., x'_{M+1}, p'_{M+1})^T$ is the vector of the input quadratures and $\mathbf{q}_{\text{out}} = (x_1, p_1, x_2, p_2, ..., x_{M+1}, p_{M+1})^T$ is the vector of the output quadratures. The Wigner function is here transformed by the beam splitter operations as [similarly to Eq. (III.40)]

$$\begin{aligned} W_{\text{MQC}}(x_1, p_1, x_2, p_2, ..., x_{M+1}, p_{M+1}) &\equiv W_{\text{out}}(x_1, p_1, x_2, p_2, ..., x_{M+1}, p_{M+1}) \\ &= W_{\text{in}}[x'_1(x_1, x_2, ..., x_{M+1}), p'_1(p_1, p_2, ..., p_{M+1}), \\ &\qquad x'_2(x_1, x_2, ..., x_{M+1}), p'_2(p_1, p_2, ..., p_{M+1}), ..., \\ &\qquad x'_{M+1}(x_1, x_2, ..., x_{M+1}), p'_{M+1}(p_1, p_2, ..., p_{M+1})]. \end{aligned} \tag{V.67}$$

Inverting the matrix $\mathbf{A}$ from Eq. (V.61) yields the input quadratures in terms of the output quadratures. With that inverse matrix and with the appropriate input Wigner function [see the Heisenberg operators in Eq. (V.62) and Eq. (V.63)]

$$\begin{aligned} W_{\text{in}}(\mathbf{x}', \mathbf{p}') &= \left(\frac{2}{\pi}\right)^{M+1} \exp(-2e^{-2(s+r_1)}{x'_1}^2 - 2e^{+2(s+r_1)}{p'_1}^2) \\ &\quad \times \exp(-2e^{-2(s-r_2)}{x'_2}^2 - 2e^{+2(s-r_2)}{p'_2}^2) \exp(-2e^{-2s}{x'_3}^2 - 2e^{+2s}{p'_3}^2) \\ &\quad \times \cdots \times \exp(-2e^{-2s}{x'_{M+1}}^2 - 2e^{+2s}{p'_{M+1}}^2), \end{aligned} \tag{V.68}$$

one obtains the Wigner function W_{MQC}.

The bipartite character is common between W_{MQC} and the qubit telecloning state proposed by Murao *et al.* [149] (introduced in the previous section). However, as opposed to W_{MQC} (except for $M = 1$), the qubit state contains *maximum* bipartite entanglement. On the other hand, the qubit states are in some sense more symmetric and even more "multiuser-friendly", as they are actually $2M$-partite states containing bipartite entanglement between M parties "on the left side" and M parties "on the right side". As discussed in the previous section, due to this symmetry, *each* particle on *each* side can function as a "port" enabling the transfer of quantum information to all particles on the other side. We can also construct such an MQC for continuous variables with exactly the same properties as the qubit state, but the price we have to pay is that we need infinite squeezing, i.e., maximum bipartite entanglement for any M. The corresponding $2M$-mode state is generated by first producing an infinitely squeezed bipartite EPR state and then sending *both* halves each together with $M-1$ ancilla modes through an M-splitter. Also this MQC enables optimal $1 \to M$ telecloning of coherent states, but instead of a fixed "port", any mode "on the left side" built from the left EPR-half or "on the right side" built from the right EPR-half can now function as a "port" for sending quantum information to the other side [5].

Let us emphasize the analogy between this particular continuous-variable MQC and Murao *et al.'s* qubit telecloning state [149] by displaying them both for $M = 2$ in the Schrödinger representation. The continuous-variable state, expanded in the position basis, is (for $s = 0$)

$$|\psi_{\mathrm{MQC}'}\rangle \propto \int dx\, dy\, dz\, \exp(-y^2 - z^2)\, |x+y\rangle|x-y\rangle|x+z\rangle|x-z\rangle\ , \quad \text{(V.69)}$$

[5] One can easily verify the optimality and the "multi-user character" of that symmetric infinite-squeezing MQC through a calculation in the Heisenberg picture similar to the one we performed for the finite-squeezing MQC with fixed port. Note that the infinite-squeezing MQC contains only *one* infinitely squeezed EPR state. Thus, such a scheme is still more economical than optimal local cloning and subsequent perfect quantum teleportation of all clones to all receivers which requires M infinitely squeezed EPR states.

and the qubit state is [see Eq. (V.44) with $M = 2$]

$$\begin{aligned} |\psi_{\mathrm{MQC}}\rangle_{PAC} &= \frac{1}{\sqrt{3}}\Big[|00\rangle_{PA}|00\rangle_C + \frac{1}{2}(|01\rangle_{PA} + |10\rangle_{PA}) \\ &\qquad \otimes(|01\rangle_C + |10\rangle_C) + |11\rangle_{PA}|11\rangle_C\Big] \qquad \text{(V.70)} \\ &= \frac{1}{\sqrt{3}}(|00\rangle_{PA}|00\rangle_C + |11\rangle_{PA}|11\rangle_C) \\ &\quad + \frac{1}{2\sqrt{3}}(|01\rangle_{PA}|01\rangle_C + |01\rangle_{PA}|10\rangle_C + |10\rangle_{PA}|01\rangle_C + |10\rangle_{PA}|10\rangle_C). \end{aligned}$$

Despite its nice symmetry properties, the continuous-variable state in Eq. (V.69) is an unphysical state as opposed to the state W_{MQC} which does without infinite squeezing. Our results suggest that for qubits, a less symmetric but more economical version of an MQC might also exist, since $F^{\mathrm{univ},2}_{\mathrm{clon},1,M} = (2M+1)/(3M)$ approaches $F_{\mathrm{class}} = 2/3$ as M increases.

An important question now is whether W_{MQC} is indeed the *most* economical version of an MQC. Does our protocol rely on *minimal* squeezing resources? At least the linear optics part, one beam splitter followed by an M-splitter, is certainly the simplest possible choice. Nevertheless, let us consider a much broader class of $M+1$-mode states, namely all multipartite entangled states that can be generated via quadratic interaction Hamiltonians (i.e., an arbitrary combination of multi-port interferometers, squeezers, down-converters, etc.). An arbitrary multi-port interferometer, described by the transformation $\hat{b}_l = \sum_k U_{lk}\hat{a}_k$ with an *arbitrary* unitary matrix U, can be constructed via a network of beam splitters and phase shifters (see chapter I). An arbitrary combination of these linear optical elements with nonlinear optical elements such as single-mode squeezers [$\hat{H}_{\mathrm{int}} \propto i(\hat{a}^{\dagger 2} - \hat{a}^2)$] or two-mode squeezers [$\hat{H}_{\mathrm{int}} \propto i(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1\hat{a}_2)$], i.e., any interaction Hamiltonian quadratic in $\hat{a}$ and $\hat{a}^\dagger$, leads to a linear unitary "Bogoliubov transformation" [28],

$$\hat{b}_l = \sum_k (A_{lk}\hat{a}_k + B_{lk}\hat{a}_k^\dagger) + \zeta_l \,. \qquad \text{(V.71)}$$

Due to the bosonic commutation relations for $\hat{b}_l$, the matrices A and B must

satisfy the conditions $AB^T = (AB^T)^T$ and $AA^\dagger = BB^\dagger + \mathbb{1}$. For the purpose of generating multi-party entanglement, we can assume without loss of generality the transformation

$$\hat{b}_l = \sum_k (A_{lk}\hat{a}_k^{(0)} + B_{lk}\hat{a}_k^{(0)\dagger}) \,, \tag{V.72}$$

where $l, k = 1...M+1$, and with vacuum modes $\hat{a}_k^{(0)}$. Any transformation of the form in Eq. (V.71) can be described via Bloch-Messiah reduction by a sequence of a multi-port interferometer, a set of single-mode squeezers, and another multi-port interferometer. Mathematically, this means $A = UA_DV^\dagger$ and $B = UB_DV^T$, with a pair of unitary matrices U and V and non-negative diagonal matrices A_D and B_D, $A_D^2 = B_D^2 + \mathbb{1}$ [28]. Therefore, here (see Fig. V.5), the transformation in Eq. (V.72) may be decomposed by Bloch-Messiah reduction into a set of $M+1$ squeezers $\hat{a}'_k = \cosh\xi_k\, \hat{a}_k^{(0)} + \sinh\xi_k\, \hat{a}_k^{(0)\dagger}$ with vacuum inputs $\hat{a}_k^{(0)}$ (and ξ_k real), and a subsequent linear multi-port [unitary transformation $U(M+1)$], $\vec{b} = U(M+1)\vec{a'}$ with $\vec{b} = (\hat{b}_1, \hat{b}_2, ..., \hat{b}_{M+1})^T$ etc. [the first multi-port $V^\dagger(M+1)$ before the squeezers leaves the initial vacuum modes unchanged].

Without loss of generality, mode $\hat{b}_1$ can be chosen as a "port", and rather than assuming a phase-free symmetric beam splitter before the "Bell detection", we consider now any unitary matrix $U(2)$ acting on the input mode $\hat{a}_{\rm in}$ and $\hat{b}_1$ as $(\hat{b}_{\rm u}, \hat{b}_{\rm v})^T = U^\dagger(2)(\hat{a}_{\rm in}, \hat{b}_1)^T$. An arbitrary unitary matrix acting on $M+1$ modes can be decomposed into beam splitters and phase shifters as (see chapter I)

$$\begin{aligned} U(M+1) \;=\; & (B_{M\,M+1}B_{M-1\,M+1}\cdots B_{1\,M+1} \\ & \times B_{M-1\,M}B_{M-2\,M}\cdots B_{12}D)^{-1} \,. \end{aligned} \tag{V.73}$$

The $M(M+1)/2$ beam splitter operations each depend on two parameters, $B_{kl} \equiv B_{kl}(\theta_{kl}, \phi_{kl})$. This B_{kl} here is an $M+1$-dimensional identity matrix with the entries I_{kk}, I_{kl}, I_{lk}, and I_{ll} replaced by

$$e^{i\phi_{kl}}\sin\theta_{kl} \,, \qquad e^{i\phi_{kl}}\cos\theta_{kl} \,, \qquad \cos\theta_{kl} \,, \qquad \text{and} \qquad -\sin\theta_{kl} \,, \tag{V.74}$$

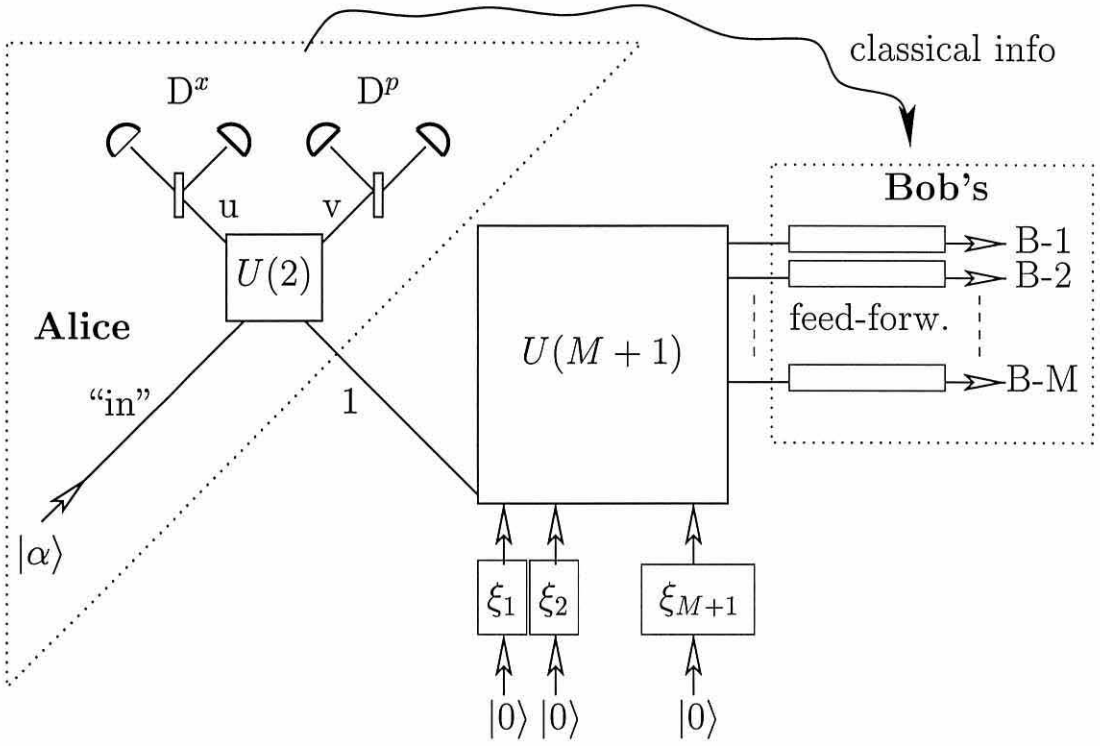

Figure V.5: Telecloning of an arbitrary coherent state from Alice to M spatially separated Bob's. Alice and the Bob's share an arbitrary multipartite entangled state (generated via a quadratic interaction Hamiltonian) as an MQC. Note that the squeezing parameters ξ_k are real (describing either x or p squeezing) and the gains for the feed-forward complex (in order to ensure covariance).

respectively. All extra phase shifts have been put in matrix D having diagonal elements $e^{i\delta_1}, e^{i\delta_2}, ..., e^{i\delta_{M+1}}$ and off-diagonal terms zero. For example, any unitary matrix $U(2) = (B_{12}D)^{-1}$ can be represented by Eq. (I.170), a matrix depending on four parameters such as ϕ_{12}, θ_{12}, δ_1, and δ_2. The entire telecloning process based on this generalization depends on $4 + (M+1)^2 + M + 1 = M^2 + 3M + 6$ parameters [4 for the generalized "Bell detection", $(M+1)^2$ for the beam splitter operations including phase shifters, and $M+1$ real squeezing parameters ξ_k].

Let us write the modes to be detected as [corresponding to an arbitrary uni-

tary transformation $U^{\dagger}(2)$ acting on modes "in" and 1, depending on ϕ_d, θ_d, δ_d, and δ'_d]

$$\begin{aligned} \hat{b}_{\rm u} &= e^{i(\phi_d+\delta_d)} \sin\theta_d \, \hat{a}_{\rm in} + e^{i(\phi_d+\delta'_d)} \cos\theta_d \, \hat{b}_1 \, , \\ \hat{b}_{\rm v} &= e^{i\delta_d} \cos\theta_d \, \hat{a}_{\rm in} - e^{i\delta'_d} \sin\theta_d \, \hat{b}_1 \, . \end{aligned} \tag{V.75}$$

The measured observables shall be the x-quadrature of mode u and the p-quadrature of mode v (which imposes no restriction due to the generality of the transformation prior to the measurements),

$$\begin{aligned} {\rm Re}\hat{b}_{\rm u} \equiv \hat{x}_{\rm u} &= \sin\theta_d[\cos\delta_d(\cos\phi_d\hat{x}_{\rm in} - \sin\phi_d\hat{p}_{\rm in}) - \sin\delta_d(\cos\phi_d\hat{p}_{\rm in} + \sin\phi_d\hat{x}_{\rm in})] \\ &\quad + \cos\theta_d[\cos\delta'_d(\cos\phi_d\hat{x}_1 - \sin\phi_d\hat{p}_1) - \sin\delta'_d(\cos\phi_d\hat{p}_1 + \sin\phi_d\hat{x}_1)] \, , \\ {\rm Im}\hat{b}_{\rm v} \equiv \hat{p}_{\rm v} &= \cos\theta_d(\sin\delta_d\hat{x}_{\rm in} + \cos\delta_d\hat{p}_{\rm in}) - \sin\theta_d(\sin\delta'_d\hat{x}_1 + \cos\delta'_d\hat{p}_1) \, , \end{aligned} \tag{V.76}$$

with $\hat{a}_{\rm in} = \hat{x}_{\rm in} + i\hat{p}_{\rm in}$ and $\hat{b}_1 = \hat{x}_1 + i\hat{p}_1$. The displacements based on the measurement results must obey the covariance condition. For the "gains" g_x and g_p, this requires $g_x\hat{x}_{\rm u} + g_p i\hat{p}_{\rm v} = \hat{x}_{\rm in} + i\hat{p}_{\rm in} + \cdots$, which leads to the constraints

$$\begin{aligned} g_x \sin\theta_d(\cos\delta_d\cos\phi_d - \sin\delta_d\sin\phi_d) + ig_p\cos\theta_d\sin\delta_d &= 1 \, , \\ -g_x \sin\theta_d(\cos\delta_d\sin\phi_d + \sin\delta_d\cos\phi_d) + ig_p\cos\theta_d\cos\delta_d &= i \, . \end{aligned} \tag{V.77}$$

The gains must therefore satisfy

$$g_x = \frac{1 - \dfrac{\sin\delta_d[i + C(\delta_d,\phi_d)]}{\cos\delta_d + \sin\delta_d\, C(\delta_d,\phi_d)}}{\sin\theta_d(\cos\delta_d\cos\phi_d - \sin\delta_d\sin\phi_d)} \, , \tag{V.78}$$

$$g_p = \frac{1 - i\, C(\delta_d,\phi_d)}{\cos\theta_d[\cos\delta_d + \sin\delta_d\, C(\delta_d,\phi_d)]} \, , \tag{V.79}$$

with

$$C(\delta_d,\phi_d) = \frac{\cos\delta_d\sin\phi_d + \sin\delta_d\cos\phi_d}{\cos\delta_d\cos\phi_d - \sin\delta_d\sin\phi_d} \, . \tag{V.80}$$

So far, we have only determined mode $\hat{b}_1$ as the port mode for telecloning, but we have not specified the number of clones M. Let us now assume the simplest

case with two clones and two receivers $M = 2$, i.e., we generate a three-mode MQC, $\vec{b} = U(3)\vec{a'}$ with $\vec{b} = (\hat{b}_1, \hat{b}_2, \hat{b}_3)^T$ and three (possibly squeezed) vacuum modes $\vec{a'} = (\hat{a}'_1, \hat{a}'_2, \hat{a}'_3)^T$ (squeezing ξ_1, ξ_2, ξ_3). After the displacements of modes $\hat{b}_2$ and $\hat{b}_3$ by $g_x\hat{x}_{\rm u} + g_p i\hat{p}_{\rm v}$ at the two receiving stations according to the sender's measurement results (for $\hat{x}_{\rm u}$ and $\hat{p}_{\rm v}$), we obtain with the gains from Eq. (V.78)

$$\begin{aligned}
\hat{b}''_2 &= U_{21}(3)\,\hat{a}'_1 + U_{22}(3)\,\hat{a}'_2 + U_{23}(3)\,\hat{a}'_3 + g_x\hat{x}_{\rm u} + ig_p\hat{p}_{\rm v} \\
&= U_{21}(3)\,\hat{a}'_1 + U_{22}(3)\,\hat{a}'_2 + U_{23}(3)\,\hat{a}'_3 + \hat{x}_{\rm in} + i\hat{p}_{\rm in} \\
&\quad + g_x\cos\theta_d[\cos\delta'_d(\cos\phi_d\hat{x}_1 - \sin\phi_d\hat{p}_1) - \sin\delta'_d(\sin\phi_d\hat{x}_1 + \cos\phi_d\hat{p}_1)] \\
&\quad - ig_p\sin\theta_d(\sin\delta'_d\hat{x}_1 + \cos\delta'_d\hat{p}_1) \\
&= \hat{x}_{\rm in} + i\hat{p}_{\rm in} + U_{21}(3)(\cosh\xi_1\,\hat{a}_1^{(0)} + \sinh\xi_1\,\hat{a}_1^{(0)\dagger}) \\
&\quad + U_{22}(3)(\cosh\xi_2\,\hat{a}_2^{(0)} + \sinh\xi_2\,\hat{a}_2^{(0)\dagger}) + U_{23}(3)(\cosh\xi_3\,\hat{a}_3^{(0)} + \sinh\xi_3\,\hat{a}_3^{(0)\dagger}) \\
&\quad + [g_x\cos\theta_d(\cos\delta'_d\cos\phi_d - \sin\delta'_d\sin\phi_d) - ig_p\sin\theta_d\sin\delta'_d] \\
&\quad \times{\rm Re}[U_{11}(3)(\cosh\xi_1\,\hat{a}_1^{(0)} + \sinh\xi_1\,\hat{a}_1^{(0)\dagger}) + U_{12}(3)(\cosh\xi_2\,\hat{a}_2^{(0)} + \sinh\xi_2\,\hat{a}_2^{(0)\dagger}) \\
&\qquad + U_{13}(3)(\cosh\xi_3\,\hat{a}_3^{(0)} + \sinh\xi_3\,\hat{a}_3^{(0)\dagger})] \\
&\quad - [g_x\cos\theta_d(\cos\delta'_d\sin\phi_d + \sin\delta'_d\cos\phi_d) + ig_p\sin\theta_d\cos\delta'_d] \\
&\quad \times{\rm Im}[U_{11}(3)(\cosh\xi_1\,\hat{a}_1^{(0)} + \sinh\xi_1\,\hat{a}_1^{(0)\dagger}) + U_{12}(3)(\cosh\xi_2\,\hat{a}_2^{(0)} + \sinh\xi_2\,\hat{a}_2^{(0)\dagger}) \\
&\qquad + U_{13}(3)(\cosh\xi_3\,\hat{a}_3^{(0)} + \sinh\xi_3\,\hat{a}_3^{(0)\dagger})]\,. \qquad \text{(V.81)}
\end{aligned}$$

Here, $U_{kl}(3)$ are the corresponding matrix *elements* of $U(3)$ [in contrast to the notation of the beam splitter operations B_{kl} which defined different matrices for different pairs (k, l)]. Mode $\hat{b}''_3$, after displacing mode $\hat{b}_3$, looks the same as mode $\hat{b}''_2$ except for the first two lines,

$$\begin{aligned}
\hat{b}''_3 &= \hat{x}_{\rm in} + i\hat{p}_{\rm in} + U_{31}(3)(\cosh\xi_1\,\hat{a}_1^{(0)} + \sinh\xi_1\,\hat{a}_1^{(0)\dagger}) \\
&\quad + U_{32}(3)(\cosh\xi_2\,\hat{a}_2^{(0)} + \sinh\xi_2\,\hat{a}_2^{(0)\dagger}) + U_{33}(3)(\cosh\xi_3\,\hat{a}_3^{(0)} + \sinh\xi_3\,\hat{a}_3^{(0)\dagger}) \\
&\quad + [g_x\cos\theta_d(\cos\delta'_d\cos\phi_d - \sin\delta'_d\sin\phi_d) - ig_p\sin\theta_d\sin\delta'_d] \\
&\quad \times{\rm Re}[U_{11}(3)(\cosh\xi_1\,\hat{a}_1^{(0)} + \sinh\xi_1\,\hat{a}_1^{(0)\dagger}) + \cdots \\
&\qquad + \cdots \qquad \text{(V.82)}
\end{aligned}$$

Thus, the quadratures of mode $\hat{b}_2''$, $\mathrm{Re}\hat{b}_2'' = \hat{x}_2''$ and $\mathrm{Im}\hat{b}_2'' = \hat{p}_2''$ take on the following form:

$$
\begin{aligned}
\hat{x}_2'' \;=\; & \hat{x}_{\mathrm{in}} + \{\mathrm{Re}U_{21}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Re}U_{11}(3) \\
& \qquad -(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Im}U_{11}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Re}U_{11}(3) + \cos\delta_d'\mathrm{Im}U_{11}(3)]\}\, e^{+\xi_1}\hat{x}_1^{(0)} \\
& - \{\mathrm{Im}U_{21}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Im}U_{11}(3) \\
& \qquad +(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Re}U_{11}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Im}U_{11}(3) - \cos\delta_d'\mathrm{Re}U_{11}(3)]\}\, e^{-\xi_1}\hat{p}_1^{(0)} \\
& + \{\mathrm{Re}U_{22}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Re}U_{12}(3) \\
& \qquad -(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Im}U_{12}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Re}U_{12}(3) + \cos\delta_d'\mathrm{Im}U_{12}(3)]\}\, e^{+\xi_2}\hat{x}_2^{(0)} \\
& - \{\mathrm{Im}U_{22}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Im}U_{12}(3) \\
& \qquad +(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Re}U_{12}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Im}U_{12}(3) - \cos\delta_d'\mathrm{Re}U_{12}(3)]\}\, e^{-\xi_2}\hat{p}_2^{(0)} \\
& + \{\mathrm{Re}U_{23}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Re}U_{13}(3) \\
& \qquad -(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Im}U_{13}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Re}U_{13}(3) + \cos\delta_d'\mathrm{Im}U_{13}(3)]\}\, e^{+\xi_3}\hat{x}_3^{(0)} \\
& - \{\mathrm{Im}U_{23}(3) + \mathrm{Re}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Im}U_{13}(3) \\
& \qquad +(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Re}U_{13}(3)] \\
& \qquad + \mathrm{Im}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Im}U_{13}(3) - \cos\delta_d'\mathrm{Re}U_{13}(3)]\}\, e^{-\xi_3}\hat{p}_3^{(0)}, \\
\hat{p}_2'' \;=\; & \hat{p}_{\mathrm{in}} + \{\mathrm{Im}U_{21}(3) + \mathrm{Im}g_x\,\cos\theta_d[(\cos\delta_d'\cos\phi_d - \sin\delta_d'\sin\phi_d)\mathrm{Re}U_{11}(3) \\
& \qquad -(\cos\delta_d'\sin\phi_d + \sin\delta_d'\cos\phi_d)\mathrm{Im}U_{11}(3)] \\
& \qquad - \mathrm{Re}g_p\,\sin\theta_d[\sin\delta_d'\mathrm{Re}U_{11}(3) + \cos\delta_d'\mathrm{Im}U_{11}(3)]\}\, e^{+\xi_1}\hat{x}_1^{(0)}
\end{aligned}
$$

$$
\begin{aligned}
&+\{\mathrm{Re}U_{21}(3)-\mathrm{Im}g_x\cos\theta_d[(\cos\delta'_d\cos\phi_d-\sin\delta'_d\sin\phi_d)\mathrm{Im}U_{11}(3)\\
&\qquad+(\cos\delta'_d\sin\phi_d+\sin\delta'_d\cos\phi_d)\mathrm{Re}U_{11}(3)]\\
&\qquad+\mathrm{Re}g_p\sin\theta_d[\sin\delta'_d\mathrm{Im}U_{11}(3)-\cos\delta'_d\mathrm{Re}U_{11}(3)]\}\,e^{-\xi_1}\hat{p}_1^{(0)}\\
&+\{\mathrm{Im}U_{22}(3)+\mathrm{Im}g_x\cos\theta_d[(\cos\delta'_d\cos\phi_d-\sin\delta'_d\sin\phi_d)\mathrm{Re}U_{12}(3)\\
&\qquad-(\cos\delta'_d\sin\phi_d+\sin\delta'_d\cos\phi_d)\mathrm{Im}U_{12}(3)]\\
&\qquad-\mathrm{Re}g_p\sin\theta_d[\sin\delta'_d\mathrm{Re}U_{12}(3)+\cos\delta'_d\mathrm{Im}U_{12}(3)]\}\,e^{+\xi_2}\hat{x}_2^{(0)}\\
&+\{\mathrm{Re}U_{22}(3)-\mathrm{Im}g_x\cos\theta_d[(\cos\delta'_d\cos\phi_d-\sin\delta'_d\sin\phi_d)\mathrm{Im}U_{12}(3)\\
&\qquad+(\cos\delta'_d\sin\phi_d+\sin\delta'_d\cos\phi_d)\mathrm{Re}U_{12}(3)]\\
&\qquad+\mathrm{Re}g_p\sin\theta_d[\sin\delta'_d\mathrm{Im}U_{12}(3)-\cos\delta'_d\mathrm{Re}U_{12}(3)]\}\,e^{-\xi_2}\hat{p}_2^{(0)}\\
&+\{\mathrm{Im}U_{23}(3)+\mathrm{Im}g_x\cos\theta_d[(\cos\delta'_d\cos\phi_d-\sin\delta'_d\sin\phi_d)\mathrm{Re}U_{13}(3)\\
&\qquad-(\cos\delta'_d\sin\phi_d+\sin\delta'_d\cos\phi_d)\mathrm{Im}U_{13}(3)]\\
&\qquad-\mathrm{Re}g_p\sin\theta_d[\sin\delta'_d\mathrm{Re}U_{13}(3)+\cos\delta'_d\mathrm{Im}U_{13}(3)]\}\,e^{+\xi_3}\hat{x}_3^{(0)}\\
&+\{\mathrm{Re}U_{23}(3)-\mathrm{Im}g_x\cos\theta_d[(\cos\delta'_d\cos\phi_d-\sin\delta'_d\sin\phi_d)\mathrm{Im}U_{13}(3)\\
&\qquad+(\cos\delta'_d\sin\phi_d+\sin\delta'_d\cos\phi_d)\mathrm{Re}U_{13}(3)]\\
&\qquad+\mathrm{Re}g_p\sin\theta_d[\sin\delta'_d\mathrm{Im}U_{13}(3)-\cos\delta'_d\mathrm{Re}U_{13}(3)]\}\,e^{-\xi_3}\hat{p}_3^{(0)}.
\end{aligned}
\tag{V.83}
$$

Analogously, the quadratures of mode $\hat{b}''_3$, $\mathrm{Re}\hat{b}''_3=\hat{x}''_3$ and $\mathrm{Im}\hat{b}''_3=\hat{p}''_3$, look the same as $\hat{x}''_2$ and $\hat{p}''_2$ with only $\mathrm{Re}U_{2k}(3)$ and $\mathrm{Im}U_{2k}(3)$ replaced by $\mathrm{Re}U_{3k}(3)$ and $\mathrm{Im}U_{3k}(3)$, respectively.

With an optimization algorithm based on a genetic code [166], we have numerically investigated whether our MQC given by W_{MQC} in Eq. (V.48) uses the least total squeezing compared to the general scheme with arbitrary MQC's produced via a quadratic interaction Hamiltonian. With the output quadratures in Eq. (V.83), the resulting fidelities of the general scheme (for $M=2$, depending on 16 parameters) are determined simply by the Q function variances σ_x and σ_p

of the output modes, $F = 1/(2\sqrt{\sigma_x \sigma_p})$ (see chapter IV), since covariance is automatically fulfilled (i.e., the mean quadrature values of modes $2''$ and $3''$ coincide with those of the input mode for any coherent-state input). Optimization, i.e., maximization of the fidelity of say mode $2''$ alone yields unit fidelity corresponding to perfect $1 \rightarrow 1$ teleportation [6]. The simultaneous maximization of the fidelities of modes $2''$ and $3''$ must obey no-cloning and should yield the optimal symmetric $1 \rightarrow 2$ cloning fidelities $F_{\mathrm{clon},1,2}^{\mathrm{coh\,st},\infty} = 2/3$. This optimum value is attained for equal minimal Q function variances $\sigma_{x_2''} = \sigma_{p_2''} = \sigma_{x_3''} = \sigma_{p_3''} = 3/4$ (assuming coherent-state inputs). Within the genetic algorithm, we used the score function $\sigma_{x_2''}\sigma_{p_2''}\sigma_{x_3''}\sigma_{p_3''} \equiv$ "score" to be minimized in order to simultaneously optimize the fidelities of modes $2''$ and $3''$ [optimal "score"$= (3/4)^4 = 0.316406$].

In Table V.1, examples for various runs of the genetic program are shown. The computation for the general $1 \rightarrow 3$ telecloning scheme ($M = 3$) is based on the calculation of a general four-party state due to an arbitrary quadratic interaction Hamiltonian of four modes. Similar to the calculation for $M = 2$, one obtains the three output modes $\hat{b}_2''$, $\hat{b}_3''$, and $\hat{b}_4''$, again with the requirement of covariance. The corresponding fidelities depend on 24 parameters in this case. As the score function, we chose $\sigma_{x_2''}\sigma_{p_2''}\sigma_{x_3''}\sigma_{p_3''}\sigma_{x_4''}\sigma_{p_4''} \equiv$ "score". Minimization of that function ensures simultaneous optimization of all three output fidelities with equal minimal Q function variances $\sigma_{x_2''} = \sigma_{p_2''} = \sigma_{x_3''} = \sigma_{p_3''} = \sigma_{x_4''} = \sigma_{p_4''} = 5/6 = 0.833333$ [$F_{\mathrm{clon},1,3}^{\mathrm{coh\,st},\infty} = 3/5$, optimal "score"$= (5/6)^6 = 0.334896$]. The Fortran program code for the genetic algorithm can be found in the appendix.

The numerical analysis of the generalized telecloning scheme has confirmed

[6] This can be done with the genetic algorithm by minimizing the product $\sigma_{x_2''}\sigma_{p_2''}$, regardless of the value of the product $\sigma_{x_3''}\sigma_{p_3''}$ and hence the fidelity of mode $3''$. In fact, the numerical analysis of such a $1 \rightarrow 1$ teleportation scheme using general *tripartite* entanglement has shown that it still requires at least two modes with large squeezing to approach unit fidelity (without additional local squeezers). In other words, an additional ancilla mode does not help to reduce the amount of squeezing necessary for near unit-fidelity quantum teleportation.

Table V.1: $1 \to M$ telecloning optimized via a genetic code

$M = 2$:					
run	1	2	3	4	5
gen.max	30000	3000	3000	3000	3000
pop.NP	$n \times 20$	$n \times 20$	$n \times 20$	$n \times 20$	$n \times 20$
squeezer 1 [dB]	≈ 0	≈ 0	≈ 0	≈ 0	≈ 0
squeezer 2 [dB]	-9.55	-4.97	-5.13	-9.18	8.07
squeezer 3 [dB]	-8.20	-12.52	-10.88	-9.20	-7.70
$\sigma_{x_2''}$	0.748700	0.750311	0.748972	0.756053	0.748295
$\sigma_{p_2''}$	0.749352	0.749667	0.744099	0.756153	0.758417
$\sigma_{x_3''}$	0.750679	0.750908	0.756397	0.744353	0.742111
$\sigma_{p_3''}$	0.751314	0.750185	0.751413	0.744156	0.752557
score	0.316424	0.316858	0.316757	0.316669	0.316949
$M = 3$:					
run	1	2	3	4	5
gen.max	1000	3000	5000	3000	5000
pop.NP	$n \times 20$	$n \times 20$	$n \times 20$	$n \times 20$	$n \times 20$
squeezer 1 [dB]	0.14	≈ 0	≈ 0	≈ 0	≈ 0
squeezer 2 [dB]	-0.18	-7.58	-0.28	0.45	≈ 0
squeezer 3 [dB]	-7.66	0.27	-3.96	-7.61	-6.86
squeezer 4 [dB]	-2.88	-6.73	-7.88	4.48	-5.38
$\sigma_{x_2''}$	0.845925	0.861773	0.818441	0.853587	0.830673
$\sigma_{p_2''}$	0.829866	0.838706	0.845222	0.827877	0.816434
$\sigma_{x_3''}$	0.835709	0.823998	0.821070	0.832108	0.847605
$\sigma_{p_3''}$	0.819886	0.816272	0.856873	0.830645	0.831913
$\sigma_{x_4''}$	0.854091	0.837779	0.822104	0.843258	0.847707
$\sigma_{p_4''}$	0.847572	0.833984	0.841180	0.818841	0.830731
score	0.348200	0.339665	0.336566	0.337263	0.336766

both for $M = 2$ and $M = 3$ that our MQC given by W_{MQC} in Eq. (V.48) uses the least total squeezing. In every calculation, the optimization (with excess noise symmetric in phase space being optimal) forces $M - 1$ auxiliary modes to approach vacuum. Only a pair of modes has to be squeezed (see Table V.1); each mode by at least $10\log_{10}[(\sqrt{M}-1)/(\sqrt{M}+1)]$ dB (about -7.7 dB for $M = 2$, -5.7 dB for $M = 3$, if equally squeezed, otherwise less squeezing in one mode is at the expense of more squeezing in the other mode, exactly as for our proposed state W_{MQC}). Note that in this general protocol, the squeezing angles of the initial modes are modified by the additional phase degrees of freedom in $U(M + 1)$.

In addition, we also investigated $1 \to 2$ telecloning with general *four-party entanglement* using the genetic algorithm. Such a protocol contains an additional ancilla mode that might be helpful to reduce the amount of squeezing necessary for optimal telecloning. In fact, the $M = 2$ qubit telecloning state from the previous section exhibited entanglement between four parties, including one ancilla particle. On the other hand, the continuous-variable version of that state [Eq. (V.69)], which is also four-party entangled and possesses the same symmetry properties as the qubit state, relied on maximum bipartite entanglement and hence infinite squeezing. The numerical analysis of $1 \to 2$ telecloning with general four-party entanglement has indicated that there is no advantage whatsoever of that scheme compared to the scheme based on tripartite entanglement. With the extra ancilla mode, one ends up with two vacua and two at least 7.7 dB squeezed modes (or one mode squeezed more than 7.7 dB, the other one less). The Q function variances of modes $2''$ and $3''$ take on the optimal values for $1 \to 2$ coherent-state telecloning, $\sigma_{x_2''} = \sigma_{p_2''} = \sigma_{x_3''} = \sigma_{p_3''} = 3/4$, whereas the variances of the ancilla mode $4''$ become arbitrarily large.

In summary of this section, we proposed a particularly simple multiuser quantum channel (MQC) for continuous-variable communication. This MQC enables optimal symmetric $1 \to M$ telecloning of coherent states. More gener-

ally, arbitrary quantum states can be transferred via this MQC from a sender to M receivers with equal minimum excess noise in each output state. Further, the protocol based on the MQC forms a cloning circuit with no need to amplify the input. The generation of the MQC requires no more than two $10\log_{10}[(\sqrt{M}-1)/(\sqrt{M}+1)]$ dB squeezed states and M beam splitters. In the view of our results in chapter III and the recent results of Bowen *et al.* [25], one squeezer might also be sufficient to produce the multi-party entanglement necessary for optimal telecloning. But then additional local squeezers have to be applied to the outgoing modes. This observation, and the numerical analysis of a more general telecloning protocol presented in this section, suggest that the proposed MQC exploits minimal squeezing resources corresponding to the minimum requirements for optimal coherent-state telecloning.

Let us finally summarize the main results of this chapter. Universal local $N \to M$ continuous-variable cloners are simple classical probability distributors achieving the optimum fidelities of N/M. The optimal local $N \to M$ coherent-state cloners turn out to be classical amplitude distributors. They can be realized with a phase-insensitive linear amplifier and beam splitters. Optimal $1 \to M$ telecloning of coherent states can be achieved via a multipartite entangled state that effectively contains simple *nonmaximum bipartite* entanglement. This entanglement is produced, as convenient in the continuous-variable context, with quadrature-squeezed light and linear optics. Since the continuous-variable telecloning scheme presented here does without maximum bipartite entanglement, and the existing qubit scheme relies on maximum two-party entanglement, it remains an open question: what is the most frugal scheme for telecloning qubits?

Appendices

A

Codes for simulating the telecloning circuit

In order to simultaneously optimize the fidelities of the output modes of the generalized telecloning circuit, we used a genetic algorithm [166] for minimizing the score function $\sigma_{x_2''}\sigma_{p_2''}\sigma_{x_3''}\sigma_{p_3''} \equiv$ "score" ($M = 2$, i.e., $1 \to 2$ telecloning) and $\sigma_{x_2''}\sigma_{p_2''}\sigma_{x_3''}\sigma_{p_3''}\sigma_{x_4''}\sigma_{p_4''} \equiv$ "score" ($M = 3$, i.e., $1 \to 3$ telecloning). Here, σ_x and σ_p denote the Q function quadrature variances of the corresponding output modes. They can be calculated according to Eq. (V.83) under the assumption of a coherent-state input.

The entire generalized telecloning process depends on $4+(M+1)^2+M+1 = M^2+3M+6$ parameters [4 for the generalized "Bell detection", $(M+1)^2$ for the beam splitter operations including phase shifters, and $M+1$ for the squeezers]. Therefore, we had to find solutions for the 16 parameters ($M = 2$) and for the 24 parameters ($M = 3$) that globally minimize the corresponding score function. Before inserting the score function in the Fortran program code of the genetic algorithm, we calculated the function with Mathematica.

1 Mathematica code for calculating the score function

First, we calculated the general expression for any unitary matrix constructed by a sequence of beam splitters and phase shifters as in Eq. (V.73) according to Reck *et al.* [171], using the following Mathematica code.

```
(* we derive the general expression for any unitary *)
(* n by n matrix u:                                 *)
n=3;
t=Table[1,{i,n}];
s=DiagonalMatrix[t];
(* p>q *)
(* note that we directly generate the transposed complex conjugate  *)
(* beam splitter matrices of T_pq which are called T[p,q]           *)
Do[
a=Exp[-I*phi[p,q]]*Sin[omega[p,q]];
b=Exp[-I*phi[p,q]]*Cos[omega[p,q]];
c=Cos[omega[p,q]];
d=-Sin[omega[p,q]];
s[[q,q]]=a;
s[[q,p]]=c;
s[[p,q]]=b;
s[[p,p]]=d;
T[p,q]=s;
s=DiagonalMatrix[t],
{p, n},{q, p-1}];
(*  example:  MatrixForm[T[4,3]]    *)
t=Table[Exp[-I*alpha[i]],{i,n}];
s=DiagonalMatrix[t];(* this is the complex conjugate of Reck's D-matrix *)
U[2,1]=s;
Do[
Do[
s=U[p,q] . T[p,q];
U[p,q+1]=s,
```

```
{q, p-1}];
U[p+1,1]=s,
{p, n}];
u=U[n+1,1];
(* examples and tests: *)
A=s . T[2,1] . T[3,1] . T[3,2];
A=s . T[2,1] . T[3,1] . T[3,2] . T[4,1] . T[4,2] . T[4,3];
A=s . T[2,1] . T[3,1] . T[3,2] . T[4,1] . T[4,2] . T[4,3] .
T[5,1] . T[5,2] . T[5,3] . T[5,4];
A == u      True
```

The unitary matrix $U(3)$ is then inserted in the score function for $M = 2$.

```
(* we derive the score function for M=2 (16 parameters) *)
(* 13 parameters are: *)
omega[3,2]=o1;
(*BS reflectivity/transmittance parameter, theta_{23} in text*)
omega[3,1]=o2;
(*BS reflectivity/transmittance parameter, theta_{13} in text*)
omega[2,1]=o3;
(*BS reflectivity/transmittance parameter, theta_{12} in text*)
phi[3,2]=p1;   (* phases phi, phi_{23} in text *)
phi[3,1]=p2;   (*    ...    , phi_{13} in text *)
phi[2,1]=p3;   (*    ...    , phi_{12} in text *)
alpha[1]=a1;   (* extra phases, delta_1 in text *)
alpha[2]=a2;   (*    ...      , delta_2 in text *)
alpha[3]=a3;   (*    ...      , delta_3 in text *)
omegaD=o4;
(* BS parameter of ``Bell detection'', theta_d in text *)
```

```
phiD=p4;        (* phase phi for Bell detection, phi_d in text *)
alphaD=a4;      (* extra phases for Bell detection, delta_d in text *)
alphaD'=a5:     (* extra phases for Bell detection, delta_d' in text *)
(* real and imaginary parts of the unitary transformation:  *)
rtmp=Re[u];
itmp=Im[u];
r=ComplexExpand[rtmp];
i=ComplexExpand[itmp];
(* real and imaginary parts of the gain parameters: alph and bet, *)
(* g_x and g_p in text                                            *)
c= ( Cos[a4]*Sin[p4]+Sin[a4]*Cos[p4] )/
( Cos[a4]*Cos[p4]-Sin[a4]*Sin[p4] );
alph= ( 1-I*(Sin[a4]*(1-I*c))/(Cos[a4]+Sin[a4]*c) )/
( Sin[o4]*(Cos[a4]*Cos[p4]-Sin[a4]*Sin[p4]) );
bet=  ( 1-I*c )/( Cos[o4]*(Cos[a4]+Sin[a4]*c) );
rtmp=Re[alph];
itmp=Im[alph];
reala=ComplexExpand[rtmp];
ima=ComplexExpand[itmp];
rtmp=Re[bet];
itmp=Im[bet];
realb=ComplexExpand[rtmp];
imb=ComplexExpand[itmp];

(* remaining three parameters for three squeezers: *)
(* e1=Exp[-xi_1], e2=Exp[-xi_2], e3=Exp[-xi_3] *)
```

```
(* the Q function variances: *)
f1=(  (1/4)*(1/Sqrt[e1^2])^2*(
r[[2,1]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *r[[1,1]]
         - reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *i[[1,1]]
         + imb*Sin[a5]*Sin[o4]*r[[1,1]]
         + imb*Cos[a5]*Sin[o4]*i[[1,1]] )^2 );
f2=(  (1/4)*(Sqrt[e1^2])^2*(
i[[2,1]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *i[[1,1]]
         + reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *r[[1,1]]
         + imb*Sin[a5]*Sin[o4]*i[[1,1]]
         - imb*Cos[a5]*Sin[o4]*r[[1,1]] )^2  );
f3=(  (1/4)*(1/Sqrt[e2^2])^2*(
r[[2,2]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *r[[1,2]]
         - reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *i[[1,2]]
         + imb*Sin[a5]*Sin[o4]*r[[1,2]]
         + imb*Cos[a5]*Sin[o4]*i[[1,2]] )^2  );
f4=(  (1/4)*(Sqrt[e2^2])^2*(
i[[2,2]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *i[[1,2]]
         + reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *r[[1,2]]
         + imb*Sin[a5]*Sin[o4]*i[[1,2]]
```

```
          - imb*Cos[a5]*Sin[o4]*r[[1,2]] )^2  );
f5=(  (1/4)*(1/Sqrt[e3^2])^2*(
r[[2,3]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *r[[1,3]]
          - reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *i[[1,3]]
          + imb*Sin[a5]*Sin[o4]*r[[1,3]]
          + imb*Cos[a5]*Sin[o4]*i[[1,3]] )^2  );
f6=(  (1/4)*(Sqrt[e3^2])^2*(
i[[2,3]] + reala*(Cos[a5]*Cos[p4]*Cos[o4]-Sin[a5]*Sin[p4]*Cos[o4])
                *i[[1,3]]
          + reala*(Cos[a5]*Sin[p4]*Cos[o4]+Sin[a5]*Cos[p4]*Cos[o4])
                *r[[1,3]]
          + imb*Sin[a5]*Sin[o4]*i[[1,3]]
          - imb*Cos[a5]*Sin[o4]*r[[1,3]] )^2  );
sigx2=(1/2)+f1+f2+f3+f4+f5+f6;
FortranForm[sigx2]
(* Analogously for sigp2, sigx3, and sigp3 *)
```

In the same way, we calculated the unitary matrix $U(4)$ and the score function for $M = 3$ with Mathematica.

2 FORTRAN CODE OF THE GENETIC ALGORITHM

It follows the Fortran code for $M = 2$. The score function is a very long expression and therefore not entirely displayed here. The size of the population of solutions for each generation is 16×20 in the example given (320 solution vectors), where 16 is the number of parameters to fit (the number of components of each solution vector). From the first randomly created generation, the population evolves to a maximum number of 3000 generations here. A new generation is created at each evolution step by "natural selection", similar to biological evolution. Only the "fittest" solutions survive. The "unfit" solutions are discarded and replaced by descendants of the solutions that survived. These descendants are created via mutation and mixing ("crossover") of their parents [144].

```
program genetic
c       uses a GENETIC search algorithm
        implicit real*8 (a-h, o-z)
        integer time
        real RAN
        external time, RAN

c       number of parameters to fit
        parameter (n = 16)
c       maximum number of generations
        parameter ( gen_max = 3000 )
c       population size
        parameter ( NP = n*20 )
c       scaling mutation parameter
        parameter ( Fscale = 0.5 )
```

```
c       recombination parameter
        parameter ( CR = 0.1 )
        real*8 x1(n, NP), x2(n, NP), trial(n), cost(NP), psmallest(n)
        common /var/ f1, f2, f3, f4
c
c       set the random seed
        iseed = time()
c       iseed = 950015448
c
c       initialization
c       initialize the squeezing factors
        do 800 i = 1, NP
         do 700 j = 1, n-13
           trial(j) = 3.0d0*RAN(iseed) + 0.3d0
            x1(j,i) = trial(j)
700      continue
c       initialize the beam splitter parameters: reflectivity
           do 750 j = 4, n-9
            trial(j) = 1.0d0*RAN(iseed)
                  x1(j,i) = trial(j)
750      continue
c       initialize the beam splitter parameters: phases
           do 770 j = 8, n
            trial(j) = 3.0d0*RAN(iseed)
                  x1(j,i) = trial(j)
770      continue
          cost(i) = f( n, trial )
c         write(*,*) i, trial, cost(i)
```

```
800      continue
c        initialize 'smallest'
         jsmallest = 1
         smallest = cost(1)*10

c        halt after 'gen_max' generations
         do 2000 jgen = 1, gen_max
c        loop through the population
           do 1800 i = 1, NP
c        mutate and recombine.
c        randomly generate three *different* vectors
c        from each other and 'i'
1001         ia = 1.0 + NP*RAN(iseed)
             if ( ia.eq.i ) goto 1001
1002         ib = 1.0 + NP*RAN(iseed)
             if ( (ib.eq.i) .or. (ib.eq.ia) ) goto 1002
1003         ic = 1.0 + NP*RAN(iseed)
          if ( (ic.eq.i) .or. (ic.eq.ia) .or. (ic.eq.ib) ) goto 1003
c        randomly pick the first parameter
             j = 1.0 + RAN(iseed)*n
c        load n parameters into trial; perform n - 1 binomial trials
             do 1300 k = 1, n
               if ( (RAN(iseed).le.CR) .or. (k.eq.n) ) then
c        source for 'trial(j)' is a random vector
c        plus weighted differential ..
                 trial(j) = x1(j,ic)+Fscale*( x1(j,ia) - x1(j,ib) )
               else
c        ... or the trial parameter comes from 'x1(j,i)' itself.
```

```
                trial(j) = x1(j,i)
              end if
c       get the next 'j' modulo n
              j = j + 1
              if ( j.gt.n ) j = 1
c       last parameter 'k=n' comes from noisy random vector.
1300        continue
c       evaluate/select.
c       score this trial
            score = f ( n, trial )
            if ( score.le.cost(i) ) then
              do 1400 j = 1, n
c       move trial to secondary vector (for next generation) ..
                x2(j,i) = trial(j)
1400          continue
              cost(i) = score
            else
              do 1450 j = 1, n
c       ... or place the old population member there
                x2(j,i) = x1(j,i)
1450          continue
            end if
1800      continue

c       end of population, swap arrays; move x2 onto x1 for next round
          do 1500 i = 1, NP
            do 1490 j = 1, n
              x1(j,i) = x2(j,i)
```

```
1490        continue
1500      continue

c       keep a record of progress so far
          do 1900 j = 1, NP
            if ( cost(j).lt. smallest ) then
              smallest = cost(j)
              jsmallest = j
               do 1600 kkk = 1, n
                 psmallest(kkk) = x1(kkk,jsmallest)
1600        continue
             end if
c            write(*,*) jgen, j, cost(j)
1900      continue
c       display the progress each generation
          write(*,*) " gen", jgen, "     score=", float(smallest)

2000    continue

         value = f ( n, psmallest )

        dB1 = -20.0d0*dlog10(dabs(psmallest(1)))
        dB2 = -20.0d0*dlog10(dabs(psmallest(2)))
        dB3 = -20.0d0*dlog10(dabs(psmallest(3)))

        write(*,*)
        write(*,*) " parameters:"
        write(*,*) float(psmallest(1)), float(dB1)
```

```
      write(*,*) float(psmallest(2)), float(dB2)
      write(*,*) float(psmallest(3)), float(dB3)
      write(*,*) float(psmallest(4))
      write(*,*) float(psmallest(5))
      write(*,*) float(psmallest(6))
      write(*,*) float(psmallest(7))
      write(*,*) float(psmallest(8))
      write(*,*) float(psmallest(9))
      write(*,*) float(psmallest(10))
      write(*,*) float(psmallest(11))
      write(*,*) float(psmallest(12))
      write(*,*) float(psmallest(13))
      write(*,*) float(psmallest(14))
      write(*,*) float(psmallest(15))
      write(*,*) float(psmallest(16))
      write(*,*)
      write(*,*) float(f1), float(f2), float(f3), float(f4)

      stop
      end

      real*8 function f( n, trial )
      implicit real*8 (a-h, o-z)
      integer n
      real*8 trial(n)
      common /var/ f1, f2, f3, f4
c
      e1 = trial(1)
```

```
      e2 = trial(2)
      e3 = trial(3)
      o1 = trial(4)
      o2 = trial(5)
      o3 = trial(6)
      o4 = trial(7)
      p1 = trial(8)
      p2 = trial(9)
      p3 = trial(10)
      p4 = trial(11)
      a1 = trial(12)
      a2 = trial(13)
      a3 = trial(14)
      a4 = trial(15)
      a5 = trial(16)

c     f=f1*f2*f3*f4=sigx2*sigp2*sigx3*sigp3
            f1 = 0.5 +
     -     (Cos(o3)*Cos(a2 + p2 + p3)*Sin(o2) +
     -      Sin(o2)*Sin(o3)*Sin(a1 + p2 + p3)* ...
           ...     ...    ...    ...
            f4 = 0.5 +
     -        (-(Cos(o2)*Sin(a3 + p2)) -
     -      (2*Cos(o4)*Cos(a1 + p2 + p3)*
     -       Sin(a5)*Sin(o2)*Sin(o3)*Sin(o4))/
     -       ((1 + Cos(2*o4))*(Cos(a4) + ...
c
      f = f1 * f2 * f3 * f4
```

```
c   write(*,*) f1, f2, f3, f4
c   write(*,*) f
return
end
```

BIBLIOGRAPHY

[1] G. P. Agrawal, *Nonlinear Fiber Optics*, Second Edition Academic Press (1995).

[2] Y. Aharonov *et al.*, Ann. Phys. (NY) **39**, 498 (1966).

[3] G. Alber *et al.*, Los Alamos arXive quant-ph/0008022 (2000).

[4] G. M. D'Ariano, F. De Martini, and M. F. Sacchi, Phys. Rev. Lett. **86**, 914 (2001).

[5] E. Arthurs and J. L. Kelly, Jr., Bell. Syst. Tech. J. **44**, 725 (1965).

[6] K. Banaszek, Phys. Lett. A **253**, 12 (1999).

[7] K. Banaszek and K. Wodkiewicz, Phys. Rev. A **58**, 4345 (1998).

[8] K. Banaszek and K. Wodkiewicz, Phys. Rev. Lett. **82**, 2009 (1999).

[9] H. Barnum, PhD thesis (1998), University of New Mexico, Albuquerque, NM, USA.

[10] J. S. Bell, Physics (N.Y.) **1**, 195 (1964).

[11] K. Bencheikh *et al.*, *"Quantum key distribution with continuous variables"*, preprint.

[12] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[13] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conference on Computers, Systems and Signal Processing (IEEE Press, Los Alamitos, Calif. 1984), p. 175.

[14] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[15] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[16] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996).

[17] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).

[18] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).

[19] H. J. Bernstein, J. Math. Phys. **15**, 1677 (1974).

[20] D. Boschi et al., Phys. Rev. Lett. **80**, 1121 (1998).

[21] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).

[22] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **60**, 194 (1999).

[23] D. Bouwmeester et al., Nature **390**, 575 (1997).

[24] D. Bouwmeester *et al.*, Phys. Rev. Lett. **82**, 1345 (1999).

[25] W. P. Bowen, P. K. Lam, and T. C. Ralph, Los Alamos arXive quant-ph/0104108 (2001).

[26] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).

[27] S. L. Braunstein, Nature **394**, 47 (1998).

[28] S. L. Braunstein, Los Alamos arXive quant-ph/9904002 (1999).

[29] S. L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).

[30] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, Phys. Rev. Lett. **86**, 4938 (2001).

[31] S. L. Braunstein and D. D. Crouch, Phys. Rev. A **43**, 330 (1991).

[32] S. L. Braunstein et al., *International Quantum Electronics Conference*, Vol. 7, 1998 OSA Technical Digest Series (Optical Society of America, Washington DC, 1998), p. 133.

[33] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999).

[34] S. L. Braunstein *et al.*, Phys. Rev. Lett. **84**, 3486 (2000).

[35] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, J. Mod. Opt. **47**, 267 (2000).

[36] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, Phys. Rev. A **64**, 022321 (2001).

[37] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[38] S. L. Braunstein and H. J. Kimble, Nature **394**, 840 (1998); D. Bouwmeester et al., Nature **394**, 841 (1998).

[39] S. L. Braunstein and H. J. Kimble, Phys. Rev. A **61**, 042302 (2000).

[40] S. L. Braunstein and P. van Loock, *"Report on the status of security for continuous-variable quantum cryptography"*, QUICOV progress report (2001).

[41] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[42] H.-J. Briegel *et al.*, Phys. Rev. Lett. **81**, 5932 (1998).

[43] D. Bruß, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[44] D. Bruß *et al.*, Phys. Rev. A **57**, 2368 (1998).

[45] V. Bužek *et al.*, Phys. Rev. A **45**, 8079 (1992).

[46] V. Bužek *et al.*, Phys. Rev. A **56**, 3446 (1997).

[47] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[48] V. Bužek, C. H. Keitel, and P. L. Knight, Phys. Rev. A **51**, 2575 (1995).

[49] A. R. Calderbank et al., Phys. Rev. Lett. **78**, 405 (1997).

[50] S. J. Carter, Phys. Rev. A **51**, 3274 (1995).

[51] S. J. Carter *et al.*, Phys. Rev. Lett. **58**, 1841 (1987).

[52] C. M. Caves, Phys. Rev. Lett. **45**, 75 (1980).

[53] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[54] C. M. Caves et al., Rev. Mod. Phys. **52**, 341 (1980).

[55] C. M. Caves and G. J. Milburn, Opt. Commun., to be published; Los Alamos arXive quant-ph/9910001 (2000).

[56] C. M. Caves and B. L. Schumaker, Phys. Rev. A **31**, 3068 (1985).

[57] N. J. Cerf and S. Iblisdir, *Universal copying of coherent states: a Gaussian cloning machine*, in Proc. of the 5th Int. Conf. on Quantum Communication, Measurement and Computing, eds. P. Tombesi and O. Hirota, (Kluwer, 2000); T. C. Ralph, private communication to S. L. Braunstein.

[58] N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000).

[59] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).

[60] N. J. Cerf, M. Lévy, and G. van Assche, Los Alamos arXive quant-ph/0008058.

[61] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[62] R. Clifton and H. Halvorson, Phys. Rev. A **61**, 012108 (2000).

[63] R. Clifton, H. Halvorson, and A. Kent, Phys. Rev. A **61**, 042101 (2000).

[64] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Quantum Mechanics, Volume 1*, Hermann and John Wiley (1977).

[65] O. Cohen, Helv. Phys. Acta **70**, 710 (1997).

[66] M. J. Collett and C. W. Gardiner, Phys. Rev. A **30**, 1386 (1984); **31**, 3761 (1985).

[67] S. Danakas and P. K. Aravind, Phys. Rev. A **45**, 1973 (1992).

[68] P. Deuar, W. J. Munro, and K. Nemoto, Los Alamos arXive quant-ph/0002002 (2000).

[69] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).

[70] D. Dieks, Physics Letters **92A**, 271 (1982).

[71] D. P. DiVincenzo *et al.*, Phys. Rev. A **61**, 062312 (2000).

[72] P. D. Drummond *et al.*, Nature **365**, 307 (1993).

[73] P. D. Drummond and C. W. Gardiner, J. Phys. A **13**, 2353 (1980).

[74] L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 2722 (2000).

[75] L.-M. Duan *et al.*, Phys. Rev. Lett. **84**, 4002 (2000).

[76] L.-M. Duan *et al.*, Phys. Rev. A **62**, 032304 (2000).

[77] W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000).

[78] W. Dür and J. I. Cirac, J. Mod. Opt. **47**, 247 (2000).

[79] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).

[80] W. Dür *et al.*, Phys. Rev. A **59**, 169 (1999).

[81] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[82] J. Eisert and H. J. Briegel, Phys. Rev. A **64**, 022306 (2001).

[83] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[84] R. P. Feynman, A. G. J. Hey (Editor), and R. W. Allen (Editor), *Feynman Lectures on Computation*, Penguin Books (1999).

[85] J. M. Fini, P. L. Hagelstein, and H. A. Haus, Phys. Rev. A **57**, 4842 (1998).

[86] C. A. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997).

[87] A. Furusawa *et al.*, Science **282**, 706 (1998).

[88] C. C. Gerry and P. L. Knight, Am. J. Phys. **65**, 964 (1997).

[89] G. Giedke *et al.*, Los Alamos arXive quant-ph/0103137 (2001).

[90] G. Giedke *et al.*, Los Alamos arXive quant-ph/0104072 (2001).

[91] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[92] N. Gisin and A. Peres, Phys. Lett. A **162**, 15 (1992).

[93] R. J. Glauber, Phys. Rev. Lett. **10**, 84 (1963).

[94] R. J. Glauber, Phys. Rev. **130**, 2529 (1963).

[95] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).

[96] J. P. Gordon and H. A. Haus, Optics Letters **11**, 665 (1986).

[97] D. Gottesman, A. Kitaev, and J. Preskill, Los Alamos arXive quant-ph/0008040 (2000).

[98] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2000).

[99] P. Grangier and F. Grosshans, Los Alamos arXive quant-ph/0009079 (2000).

[100] P. Grangier and F. Grosshans, Los Alamos arXive quant-ph/0010107 (2000).

[101] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[102] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001).

[103] L. Hardy and D. D. Song, Phys. Rev. A **62**, 052315 (2000).

[104] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[105] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[106] T. Hirano, T. Konishi, and R. Namiki, Los Alamos arXive quant-ph/0008037 (2000).

[107] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, p.278 (1982).

[108] M. J. Holland et al., Phys. Rev. A **42**, 2995 (1990).

[109] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[110] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **210**, 377 (1996).

[111] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[112] B. Huttner *et al.*, Phys. Rev. A **51**, 1863 (1995).

[113] F. X. Kärtner and L. Boivin, Phys. Rev. A **53**, 454 (1996).

[114] J. Kempe, C. Simon, and G. Weihs, Phys. Rev. A **62**, 032302 (2000).

[115] H. J. Kimble, in *Fundamental Systems in Quantum Optics, Les Houches, Session LIII, 1990*, eds. J. Dalibard, J. M. Raimond, J. Zinn-Justin (Elsevier Science Publishers, Amsterdam, 1992), pp. 549-674.

[116] M. Kitagawa and Y. Yamamoto, Phys. Rev. A **34**, 3974 (1986).

[117] D. N. Klyshko, Phys. Lett. A **172**, 399 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).

[118] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[119] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).

[120] P. Kok, PhD thesis, University of Wales, Bangor (2000).

[121] P. Kok and S. L. Braunstein, Phys. Rev. A, **61**, 042304 (2000).

[122] K. Kraus, *States, Effects, and Operations*, Springer-Verlag Berlin (1983).

[123] R. Laflamme *et al.*, Phil. Trans. Roy. Soc. Lond. **A356**, 1941 (1998).

[124] Y. Lai and H. A. Haus, Phys. Rev. A **40**, 844 (1989).

[125] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press (1997).

[126] M. D. Levenson *et al.*, Phys. Rev. A **32**, 1550 (1985).

[127] Wan-Li Li *et al.*, Los Alamos arXive quant-ph/0006032 (2000).

[128] N. Linden and S. Popescu, Phys. Rev. Lett. **87**, 047901 (2001).

[129] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).

[130] S. Lloyd and J.-J. E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).

[131] P. van Loock and S. L. Braunstein, Phys. Rev. A **61**, 010302(R) (2000).

[132] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).

[133] P. van Loock and S. L. Braunstein, Phys. Rev. A **63**, 022106 (2001).

[134] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **87**, 247901 (2001).

[135] P. van Loock and S. L. Braunstein, unpublished.

[136] P. van Loock, S. L. Braunstein, and H. J. Kimble, Phys. Rev. A **62**, 022309 (2000).

[137] R. Loudon, *The Quantum Theory of Light*, Oxford University Press, Second Edition (1983).

[138] N. Lütkenhaus, J. Calsamiglia, and K.A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[139] L. Mandel, Nature (London) **304**, 188 (1983).

[140] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press (1995).

[141] F. De Martini and V. Mussi, Fort. der Physik **48**, 413 (2000); F. De Martini, V. Mussi, and F. Bovino, Opt. Commun. **179**, 581 (2000).

[142] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[143] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[144] Z. Michalewicz, *Genetic algorithms + data structures = evolution programs*, Artificial Intelligence Series, Springer Verlag (1992).

[145] D. L. Mills, *Nonlinear Optics*, Springer Verlag Berlin Heidelberg New York (1991).

[146] T. Mor and P. Horodecki, Los Alamos arXive quant-ph/9906039 (1999).

[147] Y. Mu, J. Seberry, and Y. Zheng, Opt. Commun. **123**, 344 (1996).

[148] W. J. Munro, private communication.

[149] M. Murao *et al.*, Phys. Rev. A **59**, 156 (1999).

[150] M. Murao, M. B. Plenio, and V. Vedral, Phys. Rev. A **60**, 032311 (2000).

[151] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[152] M. A. Nielsen and J. Kempe, Los Alamos arXive quant-ph/0011117 (2000).

[153] W. Nolting, *Grundkurs: Theoretische Physik, Quantenmechanik: Grundlagen*, Verlag Zimmermann-Neufang Ulmen (1992).

[154] T. Opatrny *et al.*, Phys. Rev. A **52**, 2419 (1995).

[155] Z. Y. Ou, S. F. Pereira, and H. J. Kimble, Appl. Phys. B **55**, 265 (1992).

[156] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992); B. Yurke and D. Stoler, Phys. Rev. Lett. **79**, 4941 (1997); A. Gilchrist, P. Deuar, and M. D. Reid, Phys. Rev. Lett. **80**, 3169 (1998); W. J. Munro, Phys. Rev. A **59**, 4197 (1999).

[157] J.-W. Pan *et al.*, Phys. Rev. Lett. **80**, 3891 (1998).

[158] M. G. A. Paris, Phys. Rev. A **59**, 1615 (1999).

[159] S. Parker, S. Bose, and M. B. Plenio, Phys. Rev. A **61**, 032305 (2000).

[160] H. Paul, *Photonen: Eine Einführung in die Quantenoptik*, Teubner (1995).

[161] S. F. Pereira, Z. Y. Ou, and H. J. Kimble, Phys. Rev. A **62**, 042311 (2000).

[162] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers (1995).

[163] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[164] R. E. S. Polkinghorne and T. C. Ralph, Phys. Rev. Lett. **83**, 2095 (1999).

[165] J. Preskill, *Physics 229: Advanced mathematical methods of physics: quantum computation and information*, California Institute of Technology (1998); http://www.theory.caltech.edu/people/preskill/ph229.

[166] K. Price and R. Storn, Dr. Dobb's Journal, p.18, April (1997).

[167] T. C. Ralph, Phys. Rev. A **61**, 010303 (2000).

[168] T. C. Ralph, Phys. Rev. A **62**, 062306 (2000).

[169] T. C. Ralph and P. K. Lam, Phys. Rev. Lett. **81**, 5668 (1998).

[170] T. C. Ralph, R. E. S. Polkinghorne, and P. K. Lam, quant-ph/9903003.

[171] M. Reck *et al.*, Phys. Rev. Lett. **73**, 58 (1994).

[172] Ref. [125] and references [119], [185], and [263] therein.

[173] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).

[174] M. Rosenbluh and R. M. Shelby, Phys. Rev. Lett. **66**, 153 (1991).

[175] A. Royer, Phys. Rev. A **15**, 449 (1977); H. Moya-Cessa and P. L. Knight, Phys. Rev. A **48**, 2479 (1993).

[176] P. Rungta *et al.*, Los Alamos arXive quant-ph/0001075 (2000).

[177] E. Schmidt, Math. Annalen **63**, 433 (1906).

[178] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[179] M. O. Scully and M. S. Zubairy, *Quantum Optics*, Cambridge University Press (1997).

[180] R. M. Shelby *et al.*, Phys. Rev. Lett. **57**, 691 (1986).

[181] R. M. Shelby, M. D. Levenson, and P. W. Bayer, Phys. Rev. Lett. **54**, 939 (1985).

[182] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo, Phys. Rev. A **62**, 054301 (2000).

[183] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proc. 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, California, 1994), pp. 124-134.

[184] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[185] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[186] Ch. Silberhorn *et al.*, Phys. Rev. Lett. **86**, 4267 (2001).

[187] Ch. Silberhorn, N. Korolkova, and G. Leuchs, QMB6, Conference Digest, IQEC 2000, Nice, France.

[188] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).

[189] R. Simon, private communication.

[190] C. Simon, G. Weihs, and A. Zeilinger, J. Mod. Opt. **47**, 233 (2000); Phys. Rev. Lett. **84**, 2993 (2000).

[191] A. Sizmann and G. Leuchs, Progress in Optics XXXIX, 373 (1999).

[192] R. E. Slusher et al., Phys. Rev. Lett. **55**, 2409 (1985).

[193] W. Son *et al.*, Los Alamos arXive quant-ph/0012092 (2000).

[194] E. C. G. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).

[195] L. Suskind and J. Glogower, Physics **1**, 49 (1964); S. M. Barnett and D. T. Pegg, J. Phys. A: Math. Gen. **19**, 2849 (1986); D. T. Pegg and S. M. Barnett, Europhys. Lett. **6**, 483 (1988); D. T. Pegg and S. M. Barnett, Phys. Rev. A **39**, 1665 (1989).

[196] S. M. Tan, Phys. Rev. A **60**, 2752 (1999).

[197] T. Tyc and B. C. Sanders, Los Alamos arXive quant-ph/0107074 (2001).

[198] L. Vaidman, Phys. Rev. A **49**, 1473 (1994).

[199] L. Vaidman and N. Yoram, Los Alamos arXive quant-ph/9808040 (1998).

[200] D. F. Walls and G. J. Milburn, *Quantum Optics*, Springer Verlag Berlin Heidelberg New York (1994); special issues on squeezed states, JOSA B 4, 10 (1987); Appl. Phys. B **55**, 3 (1992).

[201] H. Weinfurter, private communication.

[202] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[203] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).

[204] R. F. Werner and M. M. Wolf, Los Alamos arXive quant-ph/0009118.

[205] H. Weyl, *The Theory of Groups and Quantum Mechanics*, Dover, New York (1950).

[206] E. P. Wigner, Phys. Rev. **40**, 749 (1932).

[207] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[208] J. W. Wu, Phys. Rev. A **61**, 022111 (2000).

[209] S. Wu, X. Chen, and Y. Zhang, Phys. Lett. A **275**, 244 (2000).

[210] Y. Yamamoto *et al.*, *Quantum Mechanical Limit in Optical Precision Measurement and Communication*, Progress in Optics XXVIII, 99 (1990).

[211] H. P. Yuen, Phys. Rev. A **13**, 2226 (1976).

[212] M. Zukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993).