Entanglement, Einstein-Podolsky-Rosen steering and cryptographical applications

Ioannis Kogias

School of Mathematical Sciences

University Of Nottingham

A thesis submitted for the degree of

Doctor of Philosophy (PhD)

Principal Assessor: Dr Sven Gnutzmann, Mathematical Sciences

External Assessor: Professor Myungshik Kim, Imperial College London

Acknowledgements

Who would have told me that a PhD experience abroad can be so fulfilling! I spent the past three years as a PhD student in Gerardo Adesso's Quantum Correlations group in Nottingham, years that have been most influential on my life and personal/professional development. The life as a PhD student involved such a wild a range of emotions. Extremely positive, on one hand, as for example when I attended numerous conferences/summer schools around the world (Brazil, Taiwan, Spain, Denmark, Germany, UK) during which I met so many lovely people, when my own research ideas got published, when I presented my work in workshops/seminars, with all those group gatherings and picnics. And extremely negative, on the other hand, when the project I had been working on for three months lead to a dead end, when I did not have a clear idea on what to work on for months, when my ideas ended up in the garbage bin, when I spent weeks frustrated and exhausted. I am grateful for all these experiences, positive and negative, as they all contributed to my personal and professional growth.

This thesis would not have been possible without the help and support of quite a few people. First and foremost, many thanks to my parents Ifigeneia and Menios, and to my brother Vasilis, who supported me over the years, made sure I get through the hard times, and always reminded me to go after what I truly desire in life (ego aside).

Many many thanks to my supervisor and two-times Oscar winner Gerardo Adesso, who supported me enormously during my PhD and made this journey extremely pleasant. Gerardo was always there to give me substantial guidance, to provide me with ideas when I was stuck, or to listen to and help me develop my own ideas. Numerous times did he receive e-mails from me, "Gerardo, I got this result!", followed by an "I was wrong" a few minutes later. When I eventually got an idea that was actually correct, he wouldn't believe me until at least few days passed

and the idea had survived my own judgement. As the months and years went by, I came to the point where when having an awesome idea I wouldn't believe it myself until I verify it. Then I knew I had matured. Gerardo supported all my travels, magically finding funding and using his contacts when required; as a *thank you*, while both in Rio de Janeiro, I managed to go for scuba-diving in the Atlantic ocean exactly when Gerardo was giving a talk at the summer school (Paraty 2013) I was supposed to be attending. The official excuse is that the boat's departure was delayed.

I would also like to thank my second supervisor Ivette Fuentes for her support during the first months of my PhD, her group had been most warm and friendly.

Next I would like to thank all those people who I collaborated with over the years. From the Nottingham ex-crew, thanks to Sammy Ragy and Antony Lee for all the work and discussions. Many thanks to Antonio Acin and his gigantic group who hosted me for a few months in ICFO (Barcelona), it has been an unforgettable experience. Thanks to Toni's top guns Daniel Cavalcanti and Paul Skrzypczyk for a very fruitful collaboration. Also, many thanks to Qiongyi He and Yu Xiang from Peking, our collaboration was a total success. Yu I hope you enjoyed your stay in Nottingham and didn't give up on Alice's book. Finally, thanks to Diogo Soares-Pinto for hosting me in Sao Paolo for a couple of days at the beginning of my PhD, and thanks to Otfried Gühne, Roope Uola and Constantino Budroni for hosting me in Siegen last winter.

I had the pleasure in 2014 to be part of the organizing committee of a PhD student conference held in the University of Nottingham, dubbed *Quantum Roundabout* (don't ask me why). Thanks to the super hard-working Luis Correa whose role in the organization had been vital. Luis thank you for being a good friend and for making me aware of Gerardo's group when we first met back in 2012 in Aberystwyth. Thanks to Katarzyna Macieszczak (Kasia) for her invaluable friendship and support; you are a lifelong friend. Many many thanks to the rest of the Roundabouters Marco Cianciaruso, Benjamin Everest, Thomas Bromley and Sara Di Martino.

Finally, many thanks to all those people I never collaborated with but still made my life very pleasant during this PhD. First and foremost, my ex house mates:

my dearest Xiaofei Sun, miss Laurita Vilkaite, Alban Notts and Sandra Trebunia, thanks for making our house so warm and for the countless (sensible, or not) chats, and thanks to Andreas Finke who, although not my house mate, has been a great friend. Many thanks to the rest of the Quantum Correlations group members in Nottingham: Tommaso Tufarelli, Pietro Liuzzo Scorpo, Rosanna Nichols, Bartosz Regula, Buqing Xu, Carmine Napoli; enjoy the rest of the journey! Finally, many thanks to all the Bachata people in Nottingham (LTP and the rest) who provided me with powerful entertainment during the PhD life.

Giannis

Abstract

This PhD Dissertation collects results of my own work on the topic of continuous variable (CV) quantum teleportation, which is one of the most important applications of quantum entanglement, as well as on the understanding, quantification, detection, and applications of a type of quantum correlations known as Einstein-Podolsky-Rosen (EPR) steering, for both bipartite and multipartite systems and with a main focus on CV systems.

For the first results, we examine and compare two fundamentally different teleportation schemes; the well-known continuous variable scheme of Vaidman, Braunstein and Kimble, and a recently proposed hybrid scheme by Andersen and Ralph. We analyse the teleportation of ensembles of arbitrary pure single-mode Gaussian states using these schemes and compare their performance against classical strategies that utilize no entanglement (benchmarks). Our analysis brings into question any advantage due to non-Gaussianity for quantum teleportation of Gaussian states.

For the second part of the results, we study bipartite EPR-steering. We propose a novel powerful method to detect steering in quantum systems of any dimension in a systematic and hierarchical way. Our method includes previous results of the literature as special cases on one hand, and goes beyond them on the other. We proceed to the quantification of steering-type correlations, and introduce a measure of steering for arbitrary bipartite Gaussian states, prove many useful properties, and provide with an operational interpretation of the proposed measure in terms of the key rate in one-sided device independent quantum key distribution. Finally, we show how the Gaussian steering measure gives a lower bound to a more general quantifier of which Gaussian states are proven to be extremal. We proceed to the study of multipartite steering, and derive laws for the distribution of Gaussian

steering among different parties in multipartite Gaussian states. We define an indicator of collective steering-type correlations, which is interpreted operationally in terms of the guaranteed secret key rate in the multi-party cryptographic task of quantum secret sharing.

The final results look at the cryptographical task of quantum secret sharing, whose security has remained unproven almost two decades after its original conception. By utilizing intuition and ideas from steering, we manage to establish for the first time an unconditional security proof for CV entanglement-based quantum secret sharing schemes, and demonstrate their practical feasibility. Our results establish quantum secret sharing as a viable and practically relevant primitive for quantum communication technologies.

Contents

Publications

This thesis is based on work presented in the following publications:

I "Continuous-variable versus hybrid schemes for quantum teleportation of Gaussian states" [1]

II "Quantification of Gaussian quantum steering" [2]

III "Einstein-Podolsky-Rosen steering measure for two-mode continuous variable states" [3]

IV "Hierarchy of Steering Criteria Based on Moments for All Bipartite Quantum Systems" [4]

V "Multipartite Gaussian steering: monogamy constraints and cryptographical applications" [5]

VI "Unconditional Security of Entanglement-Based Quantum Secret Sharing Schemes" [6]

List of Figures

LIST OF FIGURES

1

Introduction

Canadian Prime Minister Mr Justin Trudeau recently took the opportunity during a public speech at the Perimeter Institute, Canada, to answer a reporter's question on what quantum computing is about, surprising everyone with his knowledge on the subject and bringing a lot of media attention to a new upcoming *quantum era* in technologies. Mr Trudeau was there to announce significant continued funding for quantum information and computing [1]. A few years ago, the company D-Wave built a controversial machine claimed to be a quantum computer that can solve particular problems of interest much faster than any classical machine, while NASA and Google have already invested in D-Wave's product. Microsoft and IBM have invested in their own Quantum Computing departments working towards the implementation of a universal quantum computer. More interestingly, at this very moment of writing these words, IBM made their 5-qubit quantum processor freely available to the public, to be accessed by anyone on-line, giving people the opportunity to program IBM's mini-quantum computer via an on-line platform which subsequently implements the written quantum algorithm on one of IBM's quantum processors [2]. In the United Kingdom the government has invested hundreds of millions of pounds to support research in the development of quantum technologies [3], while a billion-euro investment was announced last month by the European Commission to support a gigantic multi-national quantum technologies project [4]. Why all this mobility worldwide?

[1] https://www.theguardian.com/science/life-and-physics/2016/apr/16/justin-trudeau-and-quantum-computers

[2] http://www.forbes.com/sites/alexkonrad/2016/05/04/ibm-put-a-quantum-processor-on-the-cloud/#6b73f98a3f7f

[3] http://uknqt.epsrc.ac.uk/

[4] http://www.nature.com/news/europe-plans-giant-billion-euro-quantum-technologies-project-1.19796?WT.mc_id=FBK_NatureNews

Let us take a brief look at the history that brought us up to this point of major investments in quantum technologies.

Quantum theory has contributed immensely to our understanding of the physical world, and is the cornerstone behind the developments of ground-breaking applications including the LASER, semi-conductors, and others. Quantum theory was originally conceived to be the theory of the smallest, the unseen, describing how particles of the subatomic world can be at many places at once (the *superposition* principle), and how these particles can be "intimately connected" with each other no matter how far apart they are (*entaglement*), or how the properties of a particle (like its spin, position or momentum) do not really exist before we actually measure them. Obviously, it's the weirdest theory the human kind ever thought of, and one that even Einstein, one of the greatest theoretical physicists, denied to accept. Miraculously, quantum theory works wonders in describing our world. So, it's not the theory that is weird; it's the universe itself. However, in the earlier years of quantum theory, it wasn't technologically possible to manipulate individual quantum systems and to therefore directly observe all these 'crazy' quantum effects, like superposition and entanglement. Supplementing Einstein's disbeliefs, some of the founding fathers of quantum theory had trouble believing that we will ever reach a point of experiment with individual quantum particles. In Schrödinger's own words [16], *"We never experiment with just one electron or atom or (small) molecule. In thought experiments, we sometimes assume that we do; this invariably entails ridiculous consequences. In the first place it is fair to state that we are not experimenting with single particles anymore than we can raise ichthyosauria in the zoo."*

Although quantum theory is almost 90 years old, it's been only the past few decades that major advances in technology allowed us to individually address quantum particles, and actually observe and manipulate their quantum properties; to bring them in a superposition of states and to entangle them on demand, which was previously thought impossible. It was soon realized that the preservation of such quantum features, not observed in our classical macroscopic world, demands complete isolation of the particle from its environment, otherwise the process of *decoherence* will destroy any "quantumness". This is exactly why the macroscopic world looks nothing like the quantum.

In the 80s and 90s people started to realize that the ability to individually manipulate quantum particles can lead to unimaginable applications. Quantum cryptography was one of the first applications to be realized; encoding messages in the fragile quantum properties of particles can actually provides us with an unconditional security and secrecy, that it would simply

be impossible to achieve with classical means. A potential eavesdropper cannot even "touch" the particles that carry the secret without destroying their quantum properties, as (s)he acts as an external environment and unavoidably invokes decoherence to the system. Quantum cryptography is *already* commercially available for real-world applications by the Swiss company Id-Quantique [1], while more companies are expected to enter the market soon. The concept of a quantum computer is yet another big idea that holds a lot of promise for the future. A quantum computer utilizes quantum properties, like superposition and entanglement, to make computations and solve many important problems exponentially faster than any classical machine. A famous, by now, example to illustrate the potential power of quantum computers is P. Shor's quantum algorithm which, when implemented with a full-fledged quantum computer, would break the widely-used RSA cryptosystem in a matter of minutes or hours, when the best (classical) supercomputer that could ever be built would require as much time as the age of the universe using the best currently known classical algorithms. Quantum cryptography and quantum computing are some of the brightest examples quantum technologies have to offer, among others, with deep implications for the future generations, and this fact explains why governments and the industry invest more and more into quantum technologies, as reported in the beginning of this introduction.

At a more fundamental level, all these new technologies require careful understanding of the basic science they utilize. Quantum systems can be correlated in ways that classical systems cannot, and it has been widely recognized that these so-called *quantum correlations* (of which, entanglement is only a special case) lurk behind the 'quantum advantages' of quantum technologies. A careful characterization of quantum correlations in composite quantum systems has been proven to be a fruitful path in assessing the usefulness of quantum states in non-classical tasks. In particular, the quantification and detection of various types of quantum correlations present in quantum states are important research avenues in the field. Providing with measures of quantum correlations we are able to deal with questions like, "*How much* of this quantum property is required to perform a given task?". This question is of importance given the presence of noise in all realistic implementations of tasks, which proves detrimental for large amounts of correlations. In a more practical level, detection techniques are also very important if we are to experimentally verify that a given quantum state possesses the desired property we are looking for. These are precisely the kind of questions we deal with in this thesis, and it's exactly the intuition acquired from this endeavour that will allow us in the final

[1] http://www.idquantique.com/

part of the thesis to show how a particular type of quantum correlations, known as steering, can be utilized in order to prove, for the first time, the unconditional security of a cryptographical task known as *quantum secret sharing*.

This PhD Dissertation collects my personal contributions to the understanding, quantification, detection, structure, operational interpretation and applications of entanglement and, particularly, a recently formalized type of quantum correlations known as Einstein-Podolsky-Rosen steering, with a main focus on continuous variable systems. The results presented in this thesis have appeared in Refs. [1, 2, 3, 4, 5, 6].

The thesis is organized as follows:

In Part I we introduce the reader to basic concepts that will be utilized later on in the thesis. In particular, in Chapter 2 we give a short introduction to the very basic concepts of quantum theory and quantum information. In Chapter 3 we introduce continuous variable systems and the useful framework of phase-space to study them. In particular, we focus on the important class of Gaussian states and discuss their structural properties, while we list and provide useful formulas for a plethora of, frequently utilized, Gaussian states. Finally, in Chapter 4 we make a brief introduction to the concept of *quantum correlations*, of which entanglement and steering are only special cases, in order to give some perspective. We talk about the hierarchy quantum correlations form and list some of the non-classical tasks each type of quantum correlations are good for.

In Part II we deal with entanglement and, one of its most important and counter-intuitive applications, *quantum teleportation*. In Chapter 5 we introduce the concept of entanglement, with a main focus on bipartite systems. We discuss about entanglement detection techniques that will be of use and even inspire us to create novel powerful tools for steering detection in Part III. We then talk about ways to quantify entanglement, in particular, introduce two entanglement measures from the literature that will also be put to good use in Part III. In Chapter 6 we introduce the highly non-classical task of *quantum teleportation* and describe the protocol for both qubits and continuous variable states. We then examine and compare two fundamentally different teleportation schemes; the well-known continuous variable scheme of Vaidman, Braunstein and Kimble (VBK), and a recently proposed hybrid scheme by Andersen and Ralph (AR). We analyze the teleportation of ensembles of arbitrary pure single-mode Gaussian states

using these schemes and see how they fare against the optimal measure-and-prepare strategies the benchmarks. In the VBK case, we allow for non-unit gain tuning and additionally consider a class of nonGaussian resources in order to optimize performance. The results suggest that the AR scheme may likely be a more suitable candidate for beating the benchmarks in the teleportation of squeezing, capable of achieving this for moderate resources in comparison to the VBK scheme. Moreover, our quantification of resources, whereby different protocols are compared at fixed values of the entanglement entropy or the mean energy of the resource states, brings into question any advantage due to non-Gaussianity for quantum teleportation of Gaussian states.

In Part III we deal with a type of quantum correlations known as *Einstein-Podolsky-Rosen steering*; or, steering for short. In Chapter 7 we give a brief historical overview on the Einstein-Podolsky-Rosen paradox and how this led Schrödinger to the concept of steering, which was only recently properly formalized as a distinct type of quantum correlations, relevant in various quantum information tasks. In Chapter 8 we first make a short introduction to steering detection methods, point out problems and gaps in the literature, and propose in return a new method that provides with a very efficient, systematic and hierarchical way of detecting bipartite steering in arbitrary quantum systems of any dimension, including continuous variable systems, based on moments of observables of the parties involved. Previously known steering criteria are recovered as special cases of our approach. The proposed method allows us to derive optimal steering witnesses for arbitrary families of quantum states, and provides a systematic framework to analytically derive non-linear steering criteria. We also discuss relevant examples and, in particular, provide an optimal steering witness for a lossy single-photon Bell state; the witness can be implemented just by linear optics and homodyne detection, and detects steering with a higher loss tolerance than any other known method. In Chapter 9 We introduce a computable measure of steering for arbitrary bipartite Gaussian states of continuous variable systems. For two-mode Gaussian states, the measure reduces to a form of coherent information, which is proven never to exceed entanglement, and to reduce to it on pure states. We provide an operational connection between our measure and the key rate in one-sided device-independent quantum key distribution. We further prove that Peres conjecture holds in its stronger form within the fully Gaussian regime: namely, steering bound entangled Gaussian states by Gaussian measurements is impossible. In Chapter 10 we generalize the Gaussian steering measure

proposed in Chapter 9 to arbitrary CV states. We further show that Gaussian states are extremal with respect to the more general measure, minimizing it among all continuous variable states with fixed second moments. As a byproduct of our analysis, we generalize and relate well-known steering criteria. Finally an operational interpretation is provided, as the proposed measure is also shown to quantify a guaranteed key rate in one-sided device independent quantum key distribution. In Chapter 11 we study the structure of multipartite steering. In particular we derive laws for the distribution of quantum steering among different parties in multipartite Gaussian states under Gaussian measurements. We prove that a monogamy relation akin to the generalized Coffman-Kundu-Wootters inequality holds quantitatively for the Gaussian steering measure introduced in Chapter 9. We then define the residual Gaussian steering, stemming from the monogamy inequality, as an indicator of collective steering-type correlations. For pure three-mode Gaussian states, the residual acts a quantifier of genuine multipartite steering, and is interpreted operationally in terms of the guaranteed key rate in the task of secure quantum secret sharing, which we will discuss in detail in the next chapter. Optimal resource states for the latter protocol are identified, and their possible experimental implementation discussed. Our results pin down the role of multipartite steering for quantum communication.

In the final Part IV, and final Chapter 12, we introduce the cryptographical task of quantum secret sharing. Secret sharing is a conventional protocol to distribute a secret message to a group of parties, who cannot access it individually but need to cooperate in order to decode it. While several variants of this protocol have been investigated, including realizations using quantum systems, the security of quantum secret sharing schemes still remains unproven almost two decades after their original conception. Here we establish an unconditional security proof for continuous variable entanglement-based quantum secret sharing schemes, in the limit of asymptotic keys and for an arbitrary number of players, by utilizing ideas from the recently developed one-sided device-independent approach to quantum key distribution. We demonstrate the practical feasibility of our scheme, which can be implemented by Gaussian states and homodyne measurements, with no need for ideal single-photon sources or quantum memories. Our results establish quantum secret sharing as a viable and practically relevant primitive for quantum communication technologies.

Part I

Basics

2

Quantum Information basics

In this first chapter we will briefly review some basic concepts of quantum theory and quantum information that will be utilized later on in the thesis. This introduction will unavoidably be brief and not thorough. We refer the reader, however, to the excellent textbook by Nielsen and Chuang [17], a widely used standard reference on the subject, for further details on basic (and, not so basic) concepts in quantum information.

2.1 Quantum systems: the pure case

Our main focus in this thesis will be to investigate how to utilize quantum systems in order to perform tasks (like, quantum teleportation and unconditionally secure cryptography) that we would be unable to perform without their delicate quantum properties. A legitimate question would then be, *what is a quantum system*? Our first answer to this question will be quite mathematical.

Definition 2.1.1. *A quantum system is any physical system for the mathematical description of which (for example, its motion in space, interaction with other systems, etc) one is obliged to assign to it a normed complex inner product space, known as a Hilbert space $\mathcal{H}^d$ of some dimension d, with the physical state of the considered system being described by a vector (or, an ensemble of vectors) $|\psi\rangle \in \mathcal{H}^d$, known as the quantum state, in that Hilbert space.*

Before diving into the mathematical details of quantum theory, it's worthwhile to get some intuition of how this definition relates to the world around us. It's instructive to first point out that in the definition of a quantum system we don't require from the size of the system to be "small". Usually when people hear about quantum mechanics they usually imagine an

atom, or a photon, or anything that is very very ..very small. This intuition originates from the fact that we don't observe quantum effects in big objects and in our everyday lives, while, another contributing factor, is that the theory of quantum mechanics is known to have been conceived to describe atomic and subatomic particles in the first place. Given the advances in our understanding of quantum theory in recent decades, this intuition turns out to be wrong and misleading. According to that understanding, big objects do not behave quantum mechanically because they are never properly isolated from their environment. Although quantum mechanics was conceived to describe atomic particles, it turned out that, to the best of our knowledge, systems of in principle *any size* can behave quantum mechanically under appropriate conditions. But, the larger the object the harder it is to isolate. Experiments testing the quantum properties of larger and larger objects are being devised [18], while the current record of 'largest object' to have been brought into a quantum state is a large organic molecule comprised of up to 810 atoms [19], or in terms of subatomic particles about 5000 protons, 5000 neutrons and 5000 electrons, ..all in a single "particle". Mesoscopic systems that have being brought into a quantum state include Bose-Einstein condensates (BECs) [20] and mechanical nano-oscillators [21, 22], while proving the non-classical nature of such systems can be surprisingly difficult [23].

Although we cannot be certain that macroscopic objects of our everyday lives can be ever brought into a quantum state, and thus behave quantum mechanically, according to quantum theory there exists no fundamental "size"-restriction to systems that can be described as quantum, while all on-going experiments are in favour of these predictions. The ultimate challenge will be to bring a concious organism into a quantum state and, as far fetched as it may sound, there have been theoretical proposals that support the feasibility of such experiments [24, 25]. The ability to do so will be a starting point to experimentally address fundamental questions, such as the role of life and consciousness in quantum mechanics. But this is a story for another book. What's important for us is that we got some intuition about what quantum *is*, and now we should be ready to dive into the mathematical formulation of quantum theory that will be of use throughout the thesis.

A quantum state $|\psi\rangle$ has unity norm, $\langle\psi|\psi\rangle = 1$, and contains all the information about the properties of the system that can in principle be available to us. Such vector states are known as *pure states*. Pure states describe quantum systems that are either completely isolated, or interact solely with classical (i.e., not quantum) systems. For example, a state $|\psi\rangle$ can describe the state of an atom when the atom is either perfectly isolated or, if it interacts with a classical system,

like the classical electromagnetic field. In both cases, one can assign a hamiltonian operator $\hat{H}(t)$ to the quantum system (time-dependent in general for interacting systems), which governs the system's dynamics at all times through the celebrated Schrödinger equation,

$$\hat{H}(t)|\psi(t)\rangle = i\hbar\partial_t|\psi(t)\rangle. \tag{2.1}$$

This evolution is *unitary* and, consequently, the state will remain pure at all times, as can be seen by explicitly solving (2.1),

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle, \quad \text{with,} \quad \hat{U}(t) = \exp\left(-\frac{i}{\hbar}\int_0^t d\tau\hat{H}(\tau)\right), \tag{2.2}$$

with, $\hat{U}(t)^\dagger\,\hat{U}(t) = \mathbb{I}$. Such isolated quantum systems are called *closed*.

The most elementary of quantum systems is the *qubit*, described by a Hilbert space of the smallest dimension $d = 2$. The state space of a qubit is spanned by two state vectors, say, $|0\rangle$ and $|1\rangle$, which form a basis and are orthogonal to each other. A most general pure state $|\psi\rangle$ of a qubit will then be a linear combination of these basis states,

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.3}$$

with $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. An example of such a quantum system would be the hydrogen atom, where the states $|0\rangle, |1\rangle$ represent its ground and first excited states respectively, or a photon, where the basis states would represent its two polarization states. The number of systems that can be represented by a quantum state of the very same form is countless, and this showcases the impressive generality of quantum theory to describe our world.

The linear form of the quantum state $|\psi\rangle$ (2.3), expressed as the sum of two distinct states $|0\rangle$ and $|1\rangle$, is the celebrated *superposition principle*, which is a consequence of the linearity of Schrödinger's equation (2.1). The interpretation of the superposition principle is highly non-trivial, as when the system is being measured it's always found occupying either the state $|0\rangle$ or $|1\rangle$ (with probabilities $|a|^2, |b|^2$ respectively), never both simultaneously. One the other hand, if one assumes that before the measurement the system occupied either of the basis states and we just cannot know which one, one is then lead to wrong physical predictions. The superposition principle puzzled, and still puzzles, physicists for over a century, and lies at the core of phenomena like *entanglement* and *Bell-nonlocality* that have found various practical applications in the field of Quantum Information and Foundations.

2.1.1 Observables and quantum measurements

The observation of quantum systems is crucial if we are to test the predictions of quantum theory in the laboratory. The quantum state $|\psi\rangle$ captures, as mentioned earlier, "all that can be said" about the quantum system; but how can one make an observation? How will the quantum system be affected by an observation? One way is through the so-called *projective measurements*, that we explain next. Every observable property of a quantum system is described mathematically by an operator, say $\hat{A}$, that is hermitian, $\hat{A}^\dagger = \hat{A}$, and is known as an *observable*. Every observable admits a *spectral decomposition*,

$$\hat{A} = \sum_{n=1}^{d} a_n \hat{P}_n, \tag{2.4}$$

where a_n are the possible experimental outcomes of the property $\hat{A}$ (e.g., direction of spin, position in space, etc), while $\hat{P}_n$ are projection operators ($\hat{P}_n^2 = \hat{P}_n$, with $\sum_n \hat{P}_n = \mathbb{I}$) each associated with an outcome a_n, and $n = 1, \ldots, d$ where d is dimension of the Hilbert space. Now, given a quantum state $|\psi\rangle$, a measurement of the observable $\hat{A}$ on that state will give a *random* outcome a_n with probability $p_n = \langle\psi|\hat{P}_n|\psi\rangle$, while the initial state of the system will change as

$$|\psi\rangle \to |\psi'\rangle = \frac{1}{\sqrt{p_n}} \hat{P}_n |\psi\rangle,$$

being an eigenstate of $\hat{A}$ with eigenvalue a_n. In contrast to classical physics, generally speaking in the quantum regime one cannot make an observation without disturbing the initial state of the system, unless the latter is an eigenstate of the measured observable. Therefore, looking at the general case of arbitrary initial states, in order to measure a property $\hat{A}$ of a quantum state $|\psi\rangle$, the experimenter is required to prepare the system in the same initial state $|\psi\rangle$ multiple times, each time making the same measurement and getting random outcomes a_n with probabilities p_n. In the limit of infinite preparations (or, copies) of the system one can acquire the expectation value of the desired property,

$$\langle\hat{A}\rangle \equiv \sum_{n=1}^{d} p_n a_n = \langle\psi|\hat{A}|\psi\rangle. \tag{2.5}$$

The presented measurement theory, which constitutes one of the postulates of quantum mechanics, can be generalized to more general "non-projective" measurements, known in the literature as POVMs (positive operator-valued measure).

General measurements (POVMs) *Given a quantum state $|\psi\rangle$, a general POVM measurement is described by a set of operators $\hat{M}_n$, each associated with a measurement outcome m_n. A random outcome occurs after the measurement with probability*

$$p_n = \langle\psi|\hat{M}_n^\dagger \hat{M}_n|\psi\rangle, \tag{2.6}$$

while the initial state changes to,

$$|\psi\rangle \to |\psi'\rangle = \frac{1}{\sqrt{p_n}}\hat{M}_n|\psi\rangle, \tag{2.7}$$

with the measurement operators satisfying

$$\sum_n \hat{M}_n^\dagger \hat{M}_n = \mathbb{I}, \tag{2.8}$$

which expresses the completion relation, $\sum_n p_n = 1$.

Hilbert space dimension The physical importance of the Hilbert space dimension d is evident in Eqs. (2.4) and (2.5). When we measure an observable $\hat{A}$ of a quantum state $|\psi\rangle \in \mathcal{H}$, we will always get at most d different outcomes a_n ($n = 1, \ldots, d$), each corresponding to an eigenstate $|a_n\rangle$ of $\hat{A}$, while the set of eigenstates $\{|a_n\rangle\}$ form an orthonormal basis in the Hilbert space. If our system is a qubit ($d = 2$), for example, all its observable quantities can have at most two distinct outcomes. Such an elementary quantum system can be physically implemented by a variety of systems, like the spin states of an electron (spin - up $|\uparrow\rangle$ or down $|\downarrow\rangle$), or the polarization of a photon (right $|\circlearrowright\rangle$ or left $|\circlearrowleft\rangle$ circular polarization). Such quantum systems described by Hilbert spaces of finite dimension d, therefore spanned by a basis $\{|a_n\rangle\}$ with a discrete and finite number of elements, are called *discrete-variable* systems. The same system can be described by a different kind of Hilbert space if we look at different properties. Take the previous example of an electron whose spin states behave as a qubit, but consider its position in space, instead, as the observable quantity. Since position is continuous, measuring it can give us infinitely many and continuous outcomes $x \in (-\infty, +\infty)$, with the eigenstates $\{|x\rangle\}$ of the relevant observable of position, $\hat{x}|x\rangle = x|x\rangle$, forming an orthonormal basis for the Hilbert space comprised by infinitely many and continuous elements. The dimension of such Hilbert spaces is thus infinite ($d = \infty$) and systems that are described by such spaces are called *continuous-variable* systems.

2.1.2 Description of multiple systems

Up to now we discussed about single quantum systems, that are isolated from other quantum systems and are consequently described by pure states. However, most interesting phenomena that we will examine in detail later on in the thesis come about when we have more than one systems. How can we describe multiple quantum systems with the current formalism? First, we assign a Hilbert space $\mathcal{H}$ to each of the, say N, systems (with, $i = 1, \ldots, N$). Next, it is a postulate of quantum mechanics that the Hilbert space of all N systems is the tensor product of all such Hilbert spaces,

$$\mathcal{H} = \bigotimes_{j=1}^{N} \mathcal{H}_j. \tag{2.9}$$

Although Eq. (2.9) is a postulate, it's straightforward to see that it's a very natural one when we consider independent systems as it leads straightforwardly to the law of multiplication of probabilities of independent events. For ease of demonstration, consider the case of two independent quantum systems A and B where $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, being described by states $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$ respectively. According to the tensor product structure, the state of the joint system AB will be $|\psi\rangle_A \otimes |\phi\rangle_B \in \mathcal{H}_{AB}$. Next, assume that we measure separate observables $\hat{A} : \mathcal{H}_A$, $\hat{B} : \mathcal{H}_B$ on these two independent systems, and get random outcomes a_n, b_m with corresponding projectors $\hat{N}_n, \hat{M}_m$, respectively. In the joint space $\mathcal{H}_{AB}$, the corresponding joint observable will also have a tensor product form, $\hat{A} \otimes \hat{B} : \mathcal{H}_A \otimes \mathcal{H}_B$, with corresponding outcome $a_n\, b_m$ and projector $\hat{N}_n \otimes \hat{M}_m$. The probability of observing the joint outcome $a_n\, b_m$ on the product state $|\Psi\rangle \equiv |\psi\rangle_A \otimes |\phi\rangle_B$ will be, according to the rule (2.16),

$$p(a_n, b_m) = \langle \Psi | \hat{N}_n \otimes \hat{M}_m | \Psi \rangle = p(a_n) \cdot p(b_m), \tag{2.10}$$

retrieving the intuitive product rule for independent events.

However when *correlated* quantum systems are considered, the tensor product structure (2.9) leads to very counter-intuitive predictions and phenomena. Consider, again for simplicity, two (possibly, interacting) quantum systems. Assuming the joint bipartite system is isolated it can be desribed by a pure bipartite state $|\psi\rangle_{AB}$ that evolves unitarily under Schrödinger's equation,

$$\hat{H}_{AB} |\psi\rangle_{AB} = i\hbar \partial_t |\psi\rangle_{AB}, \tag{2.11}$$

where $\hat{H}_{AB}$ is the hamiltonian describing both systems and their mutual interaction. Irrespectively of the exact details of its evolution in time, $|\psi\rangle_{AB}$ (being a vector in a Hilbert space

$\mathcal{H}_A \otimes \mathcal{H}_B$) can always be expanded to an orthonormal basis in that space. Namely, considering such a basis $\{|\psi_i\rangle_A\} \in \mathcal{H}_A$ and $\{|\phi_j\rangle_B\} \in \mathcal{H}_B$ for each individual space, we will have,

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |\psi_i\rangle_A \otimes |\phi_j\rangle_B. \tag{2.12}$$

In general, the state (2.12) is not a product state but a superposition of different states for each system, and is called an *entangled state*. Entanglement expresses the fact that systems A and B do not have a well-defined local quantum state independently of each other prior to measurement, just like a single quantum particle with a spatial wavefunction $\psi(x)$ does not have a well-defined position before we measure it. We will discuss in more detail about entanglement in Chapter 5.

In the next section, we will generalize the description of quantum systems, from pure to *mixed* states. However, why would such a generalization be required in the first place? Aren't pure states general enough? As we shall see, they are not. In the beginning of this chapter, we postulated that a quantum system -call it, A- isolated from other quantum systems is described by a pure state that evolves under Schrödinger's equation. However when system A interacts with a system B, and the joint bipartite system itself is isolated, they get entangled and their joint state $|\psi\rangle_{AB}$ will be a pure state of the form (2.12). Now imagine we prepared this bipartite state, but in our laboratory only system A is available to us; there is no access to system B (system B could be a photon that escaped our laboratory). What is the quantum description of A going to be? Looking at Eq. (2.12) we see that system A does not have a well defined pure state independently of B. Since B is inaccessible, what one would observe on A is a random occurrence of each $|\psi_i\rangle_A$ with some probability $\sum_j |c_{ij}|^2$. A more general treatment of quantum states is required to take into account such, and all possible, situations that involve statistical mixtures of pure states.

2.2 Quantum systems: the mixed case

We have defined quantum systems in terms of pure states, but not all quantum systems; only those that are either isolated or interact with effectively classical systems (like, an atom interacting with a classical electromagnetic field). Only in these two cases can a system have a well-defined pure quantum state at each point in time that evolves according to Schrödinger's equation. However, in the real world quantum systems cannot be perfectly isolated; for example, two massive particles may be arbitrarily far apart however their gravitational potential is

always non-zero (although, negligibly small for practical purposes). Also, a preparation procedure of a quantum state in the laboratory always involves other quantum systems interacting with the system of interest, and consequently there will always be some reminiscent interaction between them. Even if we are keen to preparing a pure state, this reminiscent interaction will always lead to some mixedness (perhaps, very small). Therefore, any quantum system unavoidably interacts with other quantum systems (the, so-called, *environment*); i.e., they are *open* quantum systems.

During such interactions, the pure state of the system under consideration evolves non-unitarily, and changes in a non-deterministic way from a well-defined state $|\psi\rangle$ to a statistical mixture of pure states $|\psi_i\rangle$ with probability p_i. In other words, the system behaves like it randomly occupied one of the pure states $|\psi_i\rangle$ with probability p_i, without us being able to know, in general, which one. The reason behind this behaviour of open systems is *entanglement*, as we discussed at the end of the previous section. The details of the observed mixture $\{|\psi_i\rangle, p_i\}$ depends entirely on the particular interaction. Such a quantum "state", which involves statistical mixtures of pure states and/or ignorance of the observer about the exact pure state description of the system in each preparation, is called a *mixed state*.

Density matrix *The most general description of a quantum system (be it, pure or mixed) is given by an operator $\hat{\rho}$ (instead of a vector state) with the following properties,*

$$\text{i) } \hat{\rho} \geq 0, \quad \text{ii) } \mathrm{tr}\hat{\rho} = 1, \tag{2.13}$$

meaning that its eigenvalues are real, non-negative and sum-up to one. The expectation value of any observable $\hat{A}$ is then given by,

$$\langle \hat{A} \rangle = \mathrm{tr}[\hat{A}\,\hat{\rho}]. \tag{2.14}$$

The spectral decomposition of a density matrix $\hat{\rho}$ with respect to its eigenvalues p_i and eigenstates $|\phi_i\rangle$, will be, $\hat{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i|$. A density matrix describes: a) a pure state if the decomposition has only one non-zero eigenvalue, i.e. $\hat{\rho} = |\phi\rangle\langle\phi|$, satisfying $\hat{\rho}^2 = \hat{\rho}$, b) a mixed state if otherwise ($\hat{\rho}^2 \neq \hat{\rho}$). Defining $\mu = \mathrm{tr}\hat{\rho}^2 \geq 0$ as the purity of the state, we then have the following criterion for how mixed a given state is,

$$\begin{aligned} \mu = 1 \quad &: \text{pure state}, \\ \mu < 1 \quad &: \text{mixed state}. \end{aligned} \tag{2.15}$$

In the rest of the thesis we will refer to the density matrix as the "quantum state" of the system, be it pure or mixed.

A state $\hat{\rho}$ provides with the complete description for a quantum system, as seen by Eq. (2.14). The framework of general quantum measurements, described in the case of pure states above, can be generalized to a state $\hat{\rho}$ of any mixedness, as seen below.

General measurements (POVMs) *Given a quantum state $\hat{\rho}$, a general POVM measurement is described by a set of operators $\hat{M}_n$, each associated with a measurement outcome m_n. A random outcome occurs after the measurement with probability*

$$p_n = \mathrm{tr}\left(\hat{M}_n \hat{\rho} \hat{M}_n^\dagger\right), \tag{2.16}$$

while the initial state changes to,

$$\hat{\rho} \to \hat{\rho}' = \frac{\hat{M}_n \hat{\rho} \hat{M}_n^\dagger}{\mathrm{tr}\left(\hat{M}_n \hat{\rho} \hat{M}_n^\dagger\right)}, \tag{2.17}$$

with the measurement operators satisfying

$$\sum_n \hat{M}_n^\dagger \hat{M}_n = \mathbb{I}, \tag{2.18}$$

which expresses the completion relation, $\sum_n p_n = 1$.

We have defined the most general description of quantum states and measurements, and now we want to consider the description of a quantum system when it is part of a larger system. For example, consider the bipartite state $\hat{\rho}_{AE} : \mathcal{H}_A \otimes \mathcal{H}_E$ where A is the system of interest (e.g., an atom) while E is some arbitrary environment (e.g., air molecules). Since A is all that we have access to, meaning that all the observables we can measure act on the Hilbert space of A alone, i.e. $\hat{A} \otimes \mathbb{I} : \mathcal{H}_A \otimes \mathcal{H}_E$. In such a scenario, following Rule (2.14) for observable quantities, the average value of an arbitrary observable on A will be equal to,

$$\langle \hat{A} \rangle = \mathrm{tr}[(\hat{A} \otimes \mathbb{I})\, \hat{\rho}_{AE}] = \mathrm{tr}[\hat{A}\, \hat{\rho}_A]. \tag{2.19}$$

The *reduced quantum state* $\hat{\rho}_A = \mathrm{tr}_E(\hat{\rho}_{AE}) : \mathcal{H}_A$ satisfies all the bona fide requirements, $\hat{\rho}_A \geq 0$ and $\mathrm{tr}\hat{\rho}_A = 1$, and offers a complete description of system A (independently of E) while it's obtained by taking the partial trace of $\hat{\rho}_{AE}$ over the degrees of freedom of the environment E.

2.2.1 Time evolution

The *time evolution* of a general state $\hat{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i| : \mathcal{H}$ depends entirely on whether the system is interacting with other quantum systems or not, during the evolution. If not, and

is isolated, then each state $|\phi_i\rangle$ of the statistical mixture will evolve unitarily as usual via Schrödinger's equation, i.e. $|\phi_i(t)\rangle = \hat{U}(t)|\phi_i\rangle$. Therefore, a generally mixed state of an isolated system will generally evolve in time as,

$$\hat{\rho}(t) = \sum_i p_i \, |\phi_i(t)\rangle\langle\phi_i(t)| = \hat{U}(t)\,\hat{\rho}\,\hat{U}(t)^\dagger. \tag{2.20}$$

In the most general case, however, the quantum system of interest described by $\hat{\rho}_A : \mathcal{H}_A$ is only part of a bigger system, interacting with some environment E that we don't have access to; like, an ion unavoidably interacting with air molecules. We would like then to know what is the most general evolution of such open systems. By considering the environment E large enough, such that systems A and E jointly are isolated from the rest of the universe, we invoke the postulate of quantum theory that such an isolated quantum system should be described by a pure state $|\psi\rangle_{AE}$ that evolves unitarily in time as $\hat{U}(t)|\psi\rangle_{AE}$, for some evolution operator $\hat{U}(t)$. The reduced state of the system of interest will then evolve as,

$$\hat{\rho}_A(t) = \mathrm{tr}_E\left[\hat{U}(t)|\psi\rangle_{AE}\langle\psi|\hat{U}(t)^\dagger\right], \tag{2.21}$$

which is a non-unitary evolution - a characteristic of open quantum systems. The time evolution presented in Eq. (2.21), although completely general, is not very useful as the exact form of the evolution operator $\hat{U}(t)$ and the initial state $|\psi\rangle_{AE}$ is almost always unknown.

The measurement process It's very interesting to note that, under a simple assumption regarding the interaction between A and E, where E can be thought of as an arbitrary macroscopic measuring apparatus, Weinberg very recently showed [26] that an open evolution of the type (2.21) can describe the non-unitary "collapse" of $\hat{\rho}_A(t)$ during a measurement process (described by projection operators $\hat{M}_n$),

$$\hat{\rho}_A(t \to \infty) = \sum_n \hat{M}_n \hat{\rho}_A \hat{M}_n,$$

with $p_n = \mathrm{tr}(\hat{M}_n\hat{\rho}_A\hat{M}_n)$, a form that was previously *postulated* (not derived) in Eq. (2.17). The assumption Weinberg used to derive this result was non-decreasing von Neumann entropy of $\hat{\rho}_A(t)$ for all t. This assumption holds true when A interacts with *big enough* environments E so that there is no back flow of information to the system, and therefore the dynamics become effectively irreversible. In other words, this assumption is a necessary requirement for E to be viewed as a macroscopic measuring apparatus.

2.2.2 Operational interpretation of the density matrix

The *operational interpretation* of a mixed density matrix $\hat{\rho}_A = \sum_i p_i |\phi_i\rangle\langle\phi_i|$, as a statistical mixture of various pure states, is non-trivial: Does the system *really* occupy one of the pure states of the mixture, or is it just a mathematical decomposition without physical significance? To examine this point further let us consider the following *maximally mixed* state of a single qubit,

$$\begin{aligned}\hat{\rho}_A = \frac{\mathbb{I}}{2} &= \frac{|\uparrow_z\rangle_A\langle\uparrow_z| + |\downarrow_z\rangle_A\langle\downarrow_z|}{2} \\ &= \frac{|\uparrow_x\rangle_A\langle\uparrow_x| + |\downarrow_x\rangle_A\langle\downarrow_x|}{2},\end{aligned} \tag{2.22}$$

where we considered two different orthonormal bases, eigenstates of the Pauli operators $\hat{\sigma}_{z(x)}$ respectively.

It's apparent that the same $\hat{\rho}_A = \mathbb{I}/2$ can be prepared in various fundamentally different ways, while providing with the same statistical predictions. For example, we may create such a state by using an unbiased coin to randomly decide whether to prepare the actual state of the system to be $|\uparrow_z\rangle_A$ or $|\downarrow_z\rangle_A$, while erasing the which-state information afterwards. Similarly for the x-direction. Although fundamentally different, the two preparation procedures lead to the same statistical predictions. In both cases, and for a given copy of the state, the system actually occupies one of the pure states of the decomposition (2.22) and we just don't know which one.

There is yet another way to prepare such a maximally mixed state, by considering system A to be entangled with another system, call it E, with their joint state being described by the so-called singlet state,

$$|\phi^+\rangle_{AE} = \frac{|\uparrow_z\rangle_A|\uparrow_z\rangle_E + |\downarrow_z\rangle_A|\downarrow_z\rangle_E}{\sqrt{2}}, \tag{2.23}$$

which also gives a maximally mixed reduced state for system A when E is not available and, therefore, traced-out: $\hat{\rho}_A = \mathrm{tr}_E|\phi^+\rangle_{AE}\langle\phi^+| = \mathbb{I}/2$. Notice that in this scenario and given a single copy λ of the state (2.23), systems A and E cannot be independently assigned a particular (pure or mixed) state before measurement. To see why, assume that for each copy λ we could assign an arbitrary state $\hat{\rho}^\lambda_{A(E)} : \mathcal{H}_{A(E)}$ to systems A and E respectively. Since the assignment of a state for the two systems is independent of each other, then for each copy λ their joint "hidden" state will be a product state; $\hat{\rho}^\lambda_A \otimes \hat{\rho}^\lambda_E$. Because the particular λ is assumed to be unknown, each $\hat{\rho}^\lambda_A \otimes \hat{\rho}^\lambda_E$ should appear with some probability p_λ and the final (mixed) state that would be

actually observed is,

$$\hat{\rho}_{AE} = \sum_{\lambda} p_{\lambda} \hat{\rho}_A^{\lambda} \otimes \hat{\rho}_E^{\lambda}. \tag{2.24}$$

The state $\hat{\rho}_{\text{sep}}^{AE}$ is known as a *separable state* because for its preparation no entanglement is required. Coming back to our original question: Does system A, described and prepared by $\hat{\rho}_A = \mathbb{I}/2$ and $|\phi^+\rangle_{AE}$ respectively, occupy a particular state for each given copy of $\hat{\rho}_A$? The answer will certainly be *negative* if the density matrix form of (2.23), i.e. $\hat{\rho}^{AE} = |\phi^+\rangle_{AE}\langle\phi^+|$, cannot be expressed in the separable form (2.24). And, indeed, this is the case; the maximally entangled state $|\phi^+\rangle_{AE}$ violates the separability condition (2.24). In Part II we will discuss in more detail about experimental criteria that can infer whether a given quantum state can be expressed in a separable form (2.24).

Conclusion Given a quantum system A described by a state $\hat{\rho}_A = \sum_i p_i |\phi_i\rangle_A\langle\phi_i|$, we cannot know in general whether the system actually occupies the states $|\phi_i\rangle_A$ of the decomposition, for a given copy of the state, unless we precisely know how the state $\hat{\rho}_A$ was prepared. If system A is entangled with some arbitrary system E (and, therefore, their state cannot be written in the separable form (2.24)), then, as we showed above, we can be certain that system A cannot have occupied any particular state (be it pure, or mixed) independently of system E, before measurement.

3

Continuous variable systems: An introduction

Continuous variable (CV) quantum systems -i.e., systems whose observables can have continuous spectra (see Chapter 2)- play a prominent role in the field of Quantum Information. They have been recognized as a powerful "analog" alternative to the "digital" qubits for quantum information processing, and are attractive candidates for the implementation of a wide variety of non-classical tasks and applications, such as: quantum computation, quantum communication, quantum cryptography, quantum teleportation and quantum state and channel discrimination. More details about these tasks, with relevant references, can be found in a recent review on Gaussian Quantum information by Weedbrook *et al.* [27], while for all the concepts that will be discussed in this Chapter one can also consult the following Refs. [27, 28, 29, 30] for additional details and original references.

3.1 Canonical formalism

The physical implementations of CV quantum systems can vary. Here, we will consider a particular type of system that is well-suited for quantum communication and cryptographical applications. A major requirement for an operational quantum communication scheme is the fast transaction of quantum information, i.e. of information encoded in quantum systems, among spatially separated parties. A best candidate to store and transmit quantum information in a fast and reliable manner is the quantized electromagnetic field: a) it has the maximum possible propagation speed c (the speed of light), while b) its weak interaction with the sur-

rounding environment protects the encoded quantum information from unwanted corruption. Below we will focus on the mathematical formalism describing the free electromagnetic field, which also applies to other bosonic systems; like, the collective magnetic moments of atomic ensembles.

The quantized electromagnetic (or, photonic) field is a *bosonic* quantum field whose excitations are spin-1 particles known as *photons*. A characteristic of a given photonic field is the number of *modes* it possesses, with different number of photons occupying different modes. A "mode" is a collective description of photons with a specific well-defined observable property of the system, like: energy, position, angular momentum, etc. For example, photons with the same energy $\hbar\omega_k$ occupy the same mode-k, while photons that are well-separated in different spatial regions occupy different spatial modes. The number of modes one can have in virtually infinite, but in practice we always deal with a finite number of modes, say N. Each mode with a particular property, say, k, is described by a Fock space $\mathcal{H}_k$. A Fock space is a generalization of the single-particle Hilbert space to many particles with the total number of particles being allowed to vary. The Hilbert space of an N-mode photonic field will be a tensor product structure over the Fock spaces of all considered modes,

$$\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k. \tag{3.1}$$

An N-mode photonic field can be shown to be described by a very simple Hamiltonian of N independent harmonic oscillators, with each oscillator describing a mode with particular energy $\hbar\omega_k$,

$$\hat{H} = \sum_{k=1}^{N} \hat{H}_k, \text{ with } \hat{H}_k = \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2}\right), \tag{3.2}$$

Here $\hat{a}_k^\dagger$, $\hat{a}_k$ are the creation and annihilation operators of a photon in mode k with energy $\hbar\omega_k$. Since photons are spin-1 bosons, these operators satisfy bosonic commutation relations,

$$[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{k\,k'}, \quad \text{and} \quad [\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0, \tag{3.3}$$

compared to the anti-commutator that would be used in the case of fermions.

The field can be described by yet another set of (dimensionless) operators, the so-called *quadrature* field observables, defined as,

$$\hat{q}_k = \frac{\hat{a}_k + \hat{a}_k^\dagger}{\sqrt{2}}, \quad \hat{p}_k = \frac{\hat{a}_k - \hat{a}_k^\dagger}{i\sqrt{2}}, \tag{3.4}$$

where we adopted natural units $\hbar = 1$. These operators are field observables, therefore hermitian, and satisfy the canonical commutation relation,

$$[\hat{q}_k, \hat{p}_{k'}] = i\,\delta_{k\,k'}\mathbb{I}. \tag{3.5}$$

Moreover, expressing the field Hamiltonian $\hat{H}_k$ in terms of these observables, we find the very familiar form $\hat{H}_k = \frac{1}{2}(\hat{q}_k^2 + \hat{p}_k^2)$ that describes a quantum harmonic oscillator with position and momentum observables denoted as $\hat{q}_k$, $\hat{p}_k$ respectively. Due to this intuitive correspondence, the field observables are sometimes referred to as 'position'- and 'momentum'-like quadratures, but keep in mind that they don't represent the actual position and momentum of the photons. Rather, the field quadratures are related to the electric and magnetic field operators of the photonic field. For more details, see Ref. [29].

We can group the canonical commutation relations (CCR) of an N-mode field in a convenient and compact way by first defining the vector,

$$\hat{\mathbf{R}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^{\mathrm{T}} \tag{3.6}$$

which allows us to write all CCR among any modes of the field as,

$$[\hat{R}_k, \hat{R}_l] = i\,\Omega_{kl}\mathbb{I}, \tag{3.7}$$

where $\mathbf{\Omega}$ is the N-mode *symplectic form*,

$$\mathbf{\Omega} = \bigoplus_{k=1}^{N} \boldsymbol{\omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix}, \quad \text{with} \quad \boldsymbol{\omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{3.8}$$

The symplectic form will play a protagonist role in our later discussion on the celebrated Gaussian states and their formalism.

Now let us consider the quantum state description of the field excitations. We start by finding a set of states that forms an orthonormal basis in the Hilbert space. We know, from the previous chapter, that the eigenvectors of an observable form a basis that can be used to express any other quantum state that belongs in the same Hilbert space. The observable we will consider is the single-mode Hamiltonian operator $\hat{\mathcal{H}}_k = \hat{n}_k + \frac{1}{2}$ of the photonic field, expressed via the *number operator*,

$$\hat{n}_k := \hat{a}_k^\dagger \hat{a}_k.$$

The eigenvectors of $\hat{n}_k$ (and, hence, of $\hat{\mathcal{H}}_k$) are known as Fock (or, number) states $\{|n\rangle\}_{n=0}^{\infty}$, since the eigenvalue n_k counts the number of photons in the mode k, due to $\hat{n}_k|n\rangle = n|n\rangle$. The set of number states form a basis in $\mathcal{H}_k$ as any state $|\psi\rangle \in \mathcal{H}_k$ can be expressed w.r.t. this basis,

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n |n\rangle. \tag{3.9}$$

The state $|n\rangle$ is interpreted as having n photons occupying the same mode of frequency k, while $|0\rangle$ denotes the well-known *vacuum state* occupied by zero photons. The action of the creation/annihilation operators over these states is well-defined and is actually determined by the commutation relations (3.3). We have,

$$\hat{a}_k|0\rangle = 0, \quad \hat{a}_k|n\rangle = \sqrt{n}\,|n-1\rangle, \tag{3.10}$$

and,

$$\hat{a}_k^{\dagger}|n\rangle = \sqrt{n+1}\,|n+1\rangle. \tag{3.11}$$

with $n \geq 0$.

3.1.1 How to *prepare* the vacuum

As described earlier, the vacuum state $|0\rangle$ of the electromagnetic field contains zero photons. Being the ground-state of the electromagnetic field's Hamiltonian, the vacuum state actually represents what we call *empty space*. The first counter-intuitive observation we make here is that empty space is actually described by a quantum state; therefore, *empty space is not nothing*, it's *something*. The interaction with the ever-present $|0\rangle$ in all of empty space is exactly the reason why excited atoms -wherever they're located- always decay. Yet another counter-intuitive phenomenon is that the vacuum state can be itself expanded in a basis of the eigenstates $\{|l\rangle\}$ of an observable $\hat{L}$ that does not commute with the Hamiltonian of the electromagnetic field, $[\hat{H}, \hat{L}] \neq 0$,

$$|0\rangle = \sum_{l} c_l |l\rangle. \tag{3.12}$$

An example of such an observable $\hat{L}$ could be the electric field, with its non-zero expectation value on the vacuum, $\langle 0|\hat{L}^2|0\rangle \neq 0$, being well-known as *vacuum fluctuations*. The expansion (3.12) implies that the vacuum state is actually a superposition of states $|l\rangle$ that they themselves contain a non-zero average number of photons $\langle l|\hat{n}|l\rangle \neq 0$, since,

$$|l\rangle = w_0|0\rangle + \sum_{n=1}^{\infty} w_n |n\rangle, \tag{3.13}$$

with $w_n \neq 0$ in general.

To understand how counter-intuitive this phenomenon is consider the following *preparation procedure* of the vacuum state $|0\rangle$: Instead of letting Nature give us the vacuum for free, let us actually prepare it. We go to our laboratory and prepare separate copies of each of the states $\{|l\rangle\}$. Since $\langle l|\hat{n}|l\rangle \neq 0$, every time we'd measure a state $|l\rangle$ in the Fock basis $\{|n\rangle\}$ the probability of detecting photons would be non-zero. In other words, our photodetectors would sometimes click. However, instead of measuring them, we bring all states $|l\rangle$ together to interfere with each other in a way such that the superposed state $\sum_l c_l |l\rangle$ is formed [31], having the particular coefficients c_l appearing in Eq. (3.12). The final quantum state formed is actually the vacuum state, due to (3.12), and every time we measure this newly formed state in the Fock basis ..we will *never* detect any photon, even though before the interference we would. *The photons completely disappeared*; we prepared the vacuum state ...empty space!

The explanation behind this is the wave phenomenon known by the name *destructive interference*, a phenomenon continuously observed and demonstrated in quantum interference experiments with diverse quantum systems; from photons, to throwing large molecules onto a double slit and witnessing an interference pattern at the output. The dark fringes of the pattern are places where the molecules are never detected, and that's because the quantum waves at those places interfere destructively. In complete analogy, all states $|n\rangle$ with non-zero number of photons ($n \geq 1$) interfere destructively during the interference of the $|l\rangle$ states and only the vacuum component $|0\rangle$ eventually survives. What is also impressive to think about is the conceptual difference between what the destructive interference implies in the case of a double-slit experiment and what the preparation of the vacuum: In a double-slit experiment the interference alters the observed trajectory of the molecules. However, in the preparation of the vacuum discussed here, the interference alters not the photons' trajectories, but their *objective existence*. Usually we are used to photons (dis)appearing in the presence of other systems, like atoms, that absorb/emit them, but in this case the phenomenon is genuinely different as we only considered quantum states of (isolated) photons that overlap. Mind-boggling!

3.2 Phase-space representation

A pure state $|\psi\rangle$ of a bosonic quantum field belongs to an infinite dimensional space $\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k$. Even in the simplest examples, we are always left with cumbersome expressions involving infinite sums over some eigenbasis, like in Eq. (3.9). Generalizing to arbitrary,

mixed in general, states $\hat{\rho}$ makes the algebra involved even more cumbersome, limiting the intuition one can get from infinite matrices. There is, yet, another equivalent way to represent quantum states that can be more didactic and intuitive, and which substantially simplifies the calculations in many cases of interest.

Every CV quantum state $\hat{\rho}$ has an equivalent representation in terms of suitable multivariate functions, such as the *characteristic function*

$$\chi_\rho(\boldsymbol{\xi}) = \mathrm{tr}[\hat{\rho}\,\hat{D}(\boldsymbol{\xi})], \tag{3.14}$$

where we define the *Weyl operator*

$$\hat{D}(\boldsymbol{\xi}) = \exp\left(i\hat{\mathbf{R}}^{\mathrm{T}}\,\boldsymbol{\Omega}\,\boldsymbol{\xi}\right), \tag{3.15}$$

with $\boldsymbol{\xi} \in \mathbb{R}^{2N}$. Although this expression still seems hard to deal with, we will see later on in particular examples that this function actually gets a very simple (and, perhaps, intuitive) form. We will also see in Chapter 6 that the task of quantum teleportation of CV states has a very simple description when using the characteristic function formalism.

Via Fourrier transform of the characteristic function, one can get a well-known *quasi-probability* distribution, the *Wigner function*,

$$W_\rho(\mathbf{x}) = \frac{1}{\pi^2}\int_{\mathbb{R}^{2N}} \chi_\rho(\boldsymbol{\xi}) e^{i\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Omega}\mathbf{x}}\, d^{2N}\boldsymbol{\xi}. \tag{3.16}$$

The *normalization* condition for these functions is,

$$1 = \mathrm{tr}\hat{\rho} = \int_{\mathbb{R}^{2N}} W_\rho(\mathbf{x}) d^{2N}\mathbf{x} = \chi_\rho(0), \tag{3.17}$$

while the *purity* of the state is given by,

$$\mu_\rho = \mathrm{tr}\hat{\rho}^2 = (2\pi)^N \int_{\mathbb{R}^{2N}} [W_\rho(\mathbf{x})]^2 d^{2N}\mathbf{x} = \int_{\mathbb{R}^{2N}} |\chi_\rho(\boldsymbol{\xi})|^2 d^{2N}\boldsymbol{\xi}. \tag{3.18}$$

The Wigner function can be given yet another form, sometimes easier to use, in terms of the eigenstates $|\mathbf{x}\rangle$ of the position-like quadrature operators $\{\hat{q}_j\}$,

$$W_\rho(\mathbf{q},\mathbf{p}) = \frac{1}{\pi^N}\int_{\mathbb{R}^N} \langle \mathbf{q}+\mathbf{x}|\hat{\rho}|\mathbf{q}-\mathbf{x}\rangle\, e^{2i\mathbf{x}\cdot\mathbf{p}}\, d^N\mathbf{x}, \tag{3.19}$$

with $\hat{q}_j|\mathbf{x}\rangle = \mathbf{x}|\mathbf{x}\rangle$ for $j = 1,\ldots,N$, and $\mathbf{x},\mathbf{p} \in \mathbb{R}^N$. The Wigner function can be used to calculate the average values of symmetrized observables. For example,

$$\langle \hat{R}_k\hat{R}_l + \hat{R}_l\hat{R}_k\rangle = 2\int_{\mathbb{R}^{2N}} R_k R_l\, W_\rho(\mathbf{q},\mathbf{p})\, d^N\mathbf{q}\, d^N\mathbf{p}, \tag{3.20}$$

where $\hat{\mathbf{R}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^{\mathrm{T}}$. Formula (3.20) will come in handy later on in the thesis, allowing us to compute all second-order moments that fully define a Gaussian state.

Finally, the Wigner function enjoys a nice operational interpretation as its marginal integral over all variables q_i except q_N,

$$\langle q_N|\hat{\rho}|q_N\rangle = \int_{\mathbb{R}^{2N-1}} W_\rho(q_1, p_1, \ldots, q_N, p_N)\, dq_1 \cdots dq_{N-1}\, dp_1 \cdots dp_N, \tag{3.21}$$

gives the correct probability of observing measurement outcome q_N when measuring the quadrature $\hat{q}_N$. Similar considerations hold for the other quadratures. Properties (3.17),(3.20) and (3.21) resemble the Wigner function to a probability distribution. However, the Wigner function can take negative values in contrast to a *bona fide* probability distribution, therefore the name: *quasi*-probability distribution.

3.3 Gaussian states

Gaussian states constitute versatile resources for quantum communication protocols with bosonic CV systems [27, 32, 33, 34, 35], while they naturally occur as ground or thermal equilibrium states of any physical quantum system in the 'small-oscillations' limit [36, 37]. Moreover, some optical transformations such as those associated with beam splitters and phase shifters, as well as noisy evolutions leading to loss or amplification of quantum states, are naturally Gaussian: i.e., they map Gaussian states into Gaussian states. Gaussian states are furthermore particularly easy to prepare and control in a range of experimental set-ups including primarily quantum optics, trapped ions, atomic ensembles, optomechanics, as well as networks interfacing these diverse technologies [35]. From the mathematical perspective, Gaussian states are technically accessible, since they are completely described by a finite number of degrees of freedom only (first and second moments of the canonical mode operators) as we will see below, despite their infinite-dimensional support.

3.3.1 Structural properties

The set of Gaussian states is, by definition, the set of states with Gaussian characteristic function χ and quasi-probability distribution W on the multimode quantum phase space. The general form of such multivariate N-mode Gaussian functions is,

$$f(\mathbf{x}) = C \exp\left(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} + \mathbf{b}^{\mathrm{T}}\mathbf{x}\right), \tag{3.22}$$

where $\mathbf{x} = (x_1, \ldots, x_N)^{\mathrm{T}}$, $\mathbf{b} = (b_1, \ldots, b_N)^{\mathrm{T}}$, and $\mathbf{A}$ is an $N \times N$ positive-definite matrix. The most relevant quantities that characterize these distributions are the statistical moments of the quantum state $\hat{\rho}$, and Gaussian distributions specifically are uniquely defined solely by the first and second moments.

The *first moments* of an N-mode state are defined by the displacement vector,

$$\bar{\mathbf{x}} := \langle \hat{\mathbf{R}} \rangle_\rho = \mathrm{tr}\left(\hat{\mathbf{R}}\,\hat{\rho}\right), \tag{3.23}$$

where $\hat{\mathbf{R}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^{\mathrm{T}}$. The *second moments* of the state form the so-called *covariance matrix* (CM) $\boldsymbol{\sigma} = \left(\sigma_{ij}\right)$ of the state,

$$\sigma_{ij} = \langle \hat{R}_i \hat{R}_j + \hat{R}_j \hat{R}_i \rangle_\rho - 2\langle \hat{R}_i \rangle_\rho \langle \hat{R}_j \rangle_\rho. \tag{3.24}$$

Since Gaussian states are uniquely defined by their $\bar{\mathbf{x}}$ and $\boldsymbol{\sigma}$, i.e. $\hat{\rho}_G = \hat{\rho}(\bar{\mathbf{x}}, \boldsymbol{\sigma})$, we can express their corresponding Gaussian characteristic and Wigner functions solely in terms of these quantities,

$$\chi_\rho(\boldsymbol{\xi}) = e^{-\frac{1}{4}\boldsymbol{\xi}^{\mathrm{T}}\boldsymbol{\Omega}\boldsymbol{\sigma}\boldsymbol{\Omega}^{\mathrm{T}}\boldsymbol{\xi} - i(\boldsymbol{\Omega}\bar{\mathbf{x}})^{\mathrm{T}}\boldsymbol{\xi}}, \tag{3.25}$$

$$W_\rho(\mathbf{x}) = \frac{1}{\pi^N}\frac{1}{\det(\boldsymbol{\sigma})}\, e^{-(\mathbf{x}-\bar{\mathbf{x}})^{\mathrm{T}}\boldsymbol{\sigma}^{-1}(\mathbf{x}-\bar{\mathbf{x}})}, \tag{3.26}$$

with $\boldsymbol{\xi}, \mathbf{x} \in \mathbb{R}^{2N}$.

The covariance matrix $\boldsymbol{\sigma}$ is a $2N \times 2N$, real and symmetric matrix, while for every physical state $\hat{\rho}$ (Gaussian, or not) the corresponding $\boldsymbol{\sigma}$ must satisfy the *bona fide* condition [38, 39]

$$\boldsymbol{\sigma} + i\,\boldsymbol{\Omega} \geq 0. \tag{3.27}$$

For a single mode, this condition (3.27) is equivalent to an uncertainty relation by Dodonov, Kurmyshev and Man'ko [40] imposed on the canonical operators, and is a stronger version of Heisenberg's uncertainty relation. One can easily see this, by considering a single mode CM,

$$\boldsymbol{\sigma} = \begin{pmatrix} \sigma_{qq} & \sigma_{qp} \\ \sigma_{qp} & \sigma_{pp} \end{pmatrix},$$

the *bona fide* condition (3.27) on the 2×2 matrix is equivalent to the positivity of its determinant $\det(\boldsymbol{\sigma} + i\,\boldsymbol{\Omega}) \geq 0$, which in turn gives the generalized uncertainty relation [40],

$$\sigma_{qq}\sigma_{pp} - \sigma_{qp}^2 \geq 1. \tag{3.28}$$

Realizing that the CM's diagonal elements are nothing but twice the variances of the canonical operators,

$$\sigma_{qq} = 2V(\hat{q}), \text{ with } V(\hat{q}) \equiv \langle \hat{q}^2 \rangle_\rho - \langle \hat{q} \rangle_\rho^2, \tag{3.29}$$

(similarly for momentum) we immediately see that when $\sigma_{qp} = 0$ we recover precisely Heisenberg's uncertainty principle, $V(\hat{q})V(\hat{p}) \geq \frac{1}{4}$.

Gaussian states can also be pure or mixed, and the *purity* μ_ρ of a state is determined very conveniently solely by its CM,

$$\mu_\rho = \mathrm{tr}\rho^2 = \frac{1}{\sqrt{\det \boldsymbol{\sigma}}}, \tag{3.30}$$

implying,

$$\det \boldsymbol{\sigma} = \begin{cases} +1 & \Rightarrow \text{ pure} \\ > 1 & \Rightarrow \text{ mixed.} \end{cases} \tag{3.31}$$

3.3.2 Examples of Gaussian states and Gaussian unitaries

Now that we have laid out the general formalism let us present some important classes of Gaussian states together with the corresponding Gaussian unitary operations that can prepare them.

3.3.2.1 Coherent states and displacements

Let us go back in our discussion at the beginning of this chapter, Eq. (3.10), where we introduced the annihilation operator $\hat{a}$ and defined through it the vacuum state of the field, $\hat{a}|0\rangle = 0$. The operator $\hat{a}$ is important in its own right as the eigenstates of this operator are the infamous *coherent states*,

$$\hat{a}|\alpha\rangle = a|\alpha\rangle, \tag{3.32}$$

with $\alpha \in \mathbb{C}$ being the coherent amplitude. A single mode coherent state $|\alpha\rangle$ describes, ideally, a laser beam of some particular frequency and, hence, is so widely used in laboratory experiments of such diversity that it's impossible to overestimate its importance. Although quite "classical" in nature, coherent states also constitute the basic ingredient of the unconditionally secure CV quantum key distribution [41].

A coherent state $|\alpha\rangle$ can be generated by acting with the Weyl operator (3.15) on the vacuum, an operation known as *displacement*,

$$\hat{D}(\alpha)|0\rangle = |\alpha\rangle. \tag{3.33}$$

In terms of the Fock basis the coherent state can be expressed as

$$|\alpha\rangle = e^{\frac{1}{2}|\alpha|^2} \sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{3.34}$$

which may seem rather complex, but not any more if one studies its Wigner function which takes a rather simple Gaussian form,

$$W_\alpha(q,p) = \frac{1}{\pi} \exp\left[-(q-q_\alpha)^2 - (p-p_\alpha)^2\right], \tag{3.35}$$

with q_α, p_α representing the real and imaginary part of the complex coherent amplitude α; i.e., $\alpha = q_\alpha + ip_\alpha$. The first and second moments, which fully define a coherent state, also have a simple form,

$$\bar{\mathbf{x}} = \sqrt{2} \begin{pmatrix} q_a \\ p_a \end{pmatrix}, \quad \boldsymbol{\sigma} = \mathbf{I}. \tag{3.36}$$

Given a coherent state $|\alpha\rangle$ one can retrieve the vacuum state by letting the amplitude go to zero $\alpha \to 0$ with a corresponding Wigner function $W_0(q,p)$, from Eq. (3.35). Based on the moments (3.36), it's interesting to note that the amplitude α determines only the first moments of the state with the CM being completely independent. A special characteristic of coherent states is that they are minimum uncertainty states saturating Heisenberg's uncertainty principle $V(\hat{q})V(\hat{p}) = \frac{1}{4}$. This is the minimum variance which is reachable symmetrically by position and momentum, and it is also known as *vacuum noise* or *quantum shot-noise*.

The single-mode Weyl operator (3.15),

$$\hat{D}(\alpha) = \exp\left(\alpha\, \hat{a}^\dagger - \alpha^* \hat{a}\right), \tag{3.37}$$

is a Gaussian unitary operator, satisfying $\hat{D}^\dagger(\alpha)\hat{D}(\alpha) = \mathbb{I}$ and $\hat{D}^\dagger(\alpha) = \hat{D}(-\alpha)$, that preserves the Gaussianity of the states it acts on. For example, the vacuum state $|0\rangle$ is a Gaussian state and by acting on it with $\hat{D}(\alpha)$ we preserve its Gaussianity by obtaining another Gaussian state, the coherent state $|\alpha\rangle$. The Weyl operator is also known as the *displacement operator*: Acting on a random state $\hat{\rho}$ with the Gaussian unitary $\hat{D}(\alpha)$, and employing the Heisenberg picture (where the unitaries act on the observables instead of the quantum states), we find the following transformations,

$$\hat{a} \to \hat{a} + \alpha, \quad \hat{\mathbf{R}} \to \hat{\mathbf{R}} + \mathbf{d}_\alpha, \tag{3.38}$$

where $\hat{\mathbf{R}} = (\hat{q}, \hat{p})^{\mathrm{T}}$ and $\bar{\mathbf{x}}_\alpha = \sqrt{2}(q_\alpha, p_\alpha)^{\mathrm{T}}$. Therefore, in the phase-space picture, the effect of the Weyl operator is to *displace* the state around but without changing its form and

characteristics. A coherent state is then nothing but a vacuum state displaced in phase space, having the same characteristics with $|0\rangle$ except of an increased mean photon number (energy), $\langle|\alpha|\hat{n}|\alpha\rangle = |\alpha|^2$.

3.3.2.2 Thermal states

An important class of Gaussian states are the so-called *thermal states*. Bosonic thermal states are defined as the ones maximizing the von Neumann entropy,

$$S = -\mathrm{tr}\left(\hat{\rho}\log\hat{\rho}\right), \tag{3.39}$$

for a fixed energy (or, mean number of photons), $\bar{n} \equiv \langle\hat{n}\rangle_\rho \geq 0$. Their representation in the Fock basis reads,

$$\hat{\rho}^{\mathrm{th}}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n|. \tag{3.40}$$

Such states have a Gaussian Wigner function, zero first moments and a very simple covariance matrix that completely defines these states,

$$\boldsymbol{\sigma} = (2\bar{n}+1)\mathbf{I}. \tag{3.41}$$

3.3.2.3 Single-mode squeezing and squeezed states

Squeezed states are an important class of photonic states that are widely used in quantum information tasks to achieve performances that are classically unattainable. Squeezed states have the characteristic that they contain only an even number of photons, and are physically created by pumping a non-linear crystal with a bright laser.

Mathematically, the so-called *squeezed vacuum states* are obtained by acting with the single-mode squeezing operator,

$$\hat{S}(\zeta) = \exp\left[\frac{1}{2}\left(\zeta\hat{a}^{\dagger\,2} - \zeta^*\hat{a}^2\right)\right], \text{ where } \zeta = re^{i\theta}, \tag{3.42}$$

on the vacuum state,

$$|\zeta\rangle \equiv \hat{S}(\zeta)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{n!} \frac{e^{i\,n\,\theta}}{2^n} \tanh^n r\, |2n\rangle. \tag{3.43}$$

The parameter r is known as the *squeezing degree* of the state. High squeezing degree is one of the most desirable resources in CV quantum information as it improves the performance of

non-classical tasks (e.g. in quantum cryptographical applications or quantum computing) that utilize such states. The squeezing phase θ determines which quadrature will be (anti-)squeezed while the squeezing degree r determines by how much. The Wigner function of this state for a phase $\theta = 0$ (a choice that basically allows for p to be squeezed) has, again, a Gaussian form,

$$W_r(q,p) = \frac{1}{\pi}\exp\left(-\Delta^2 q^2 - \frac{p^2}{\Delta^2}\right), \tag{3.44}$$

with $\Delta = \exp(-r)$. For $\Delta = 1$ (or, $r = 0$) one obtains the Wigner function of the symmetric vacuum state with both position and momenta having the same uncertainty. For $\Delta < 1$ (or, $r > 0$), however, one of the quadrature variances (momentum p) is squeezed below the quantum shot-noise, while the other (position q) is anti-squeezed above it. In the limit of infinite squeezing $r \to \infty$, $|r\rangle$ tends to an (unphysical) exact eigenstate of the momentum operator $\hat{p}$, having a well-defined momentum.

In experimental papers squeezing is often measured in deciBels, defined in a way such that a squeezing degree r corresponds to,

$$\#\ \mathrm{dB} = 10\log_{10}\left[e^{2r}\right]. \tag{3.45}$$

Finally, single-mode squeezed states are completely characterized by zero first moments and covariance matrix equal to,

$$\boldsymbol{\sigma} = \begin{pmatrix} \cosh(2r) + \cos(\theta)\sinh(2r) & \sin(\theta)\sinh(2r) \\ \sin(\theta)\sinh(2r) & \cosh(2r) - \cos(\theta)\sinh(2r) \end{pmatrix}, \tag{3.46}$$

where we indeed verify, given our previous discussion for $\theta = 0$, that the variance of momentum is squeezed below the quantum shot-noise limit; $V(\hat{p}) = \frac{1}{2}e^{-2r} < \frac{1}{2}$, for $r > 0$.

3.3.2.4 Coherent squeezed states

The most general single-mode pure Gaussian state can be obtained by acting simultaneously with the displacement and squeezing operators on the vacuum state,

$$|\psi_{\alpha,\zeta}\rangle = \hat{D}(\alpha)\hat{S}(\zeta)|0\rangle, \tag{3.47}$$

and is, hence, completely described by two complex numbers $\alpha = q_\alpha + i\,p_\alpha$ and $\zeta = re^{i\theta}$. The first and second moments of this state are,

$$\mathbf{d} = \sqrt{2}\begin{pmatrix} q_a \\ p_a \end{pmatrix}, \tag{3.48}$$

$$\boldsymbol{\sigma} = \begin{pmatrix} \cosh(2r) + \cos(\theta)\sinh(2r) & \sin(\theta)\sinh(2r) \\ \sin(\theta)\sinh(2r) & \cosh(2r) - \cos(\theta)\sinh(2r) \end{pmatrix}. \tag{3.49}$$

3.3.2.5 Two-mode squeezing and squeezed states

A very important class of states are the two-mode squeezed states, with each mode (say, A and B) being spatially separated from the other while both having approximately well-defined energy (or, frequency). Such a state can be created either by appropriately pumping a non-linear crystal which generates pairs of photons in two different modes, or, by separately creating two single-mode squeezed states and passing them jointly through a beam-splitter. In both cases, the result is the bipartite state

$$|r\rangle_{AB} = \hat{S}_{AB}(r)|0,0\rangle_{AB}, \tag{3.50}$$

where $|0,0\rangle_{AB} \equiv |0\rangle_A \otimes |0\rangle_B$ denotes the vacuums for the different modes A and B. We also introduced the two-mode squeezing operator

$$\hat{S}_{AB}(r) = \exp\left[r\left(\hat{a}^\dagger\hat{b}^\dagger - \hat{a}\hat{b}\right)\right], \tag{3.51}$$

which is unitary, r is squeezing degree, and $\hat{a}^{(\dagger)}, \hat{b}^{(\dagger)}$ are the creation/annihilation operators for the modes A, B respectively. The Fock basis representation of the state is,

$$|r\rangle_{AB} = \sqrt{1-\tanh^2 r}\sum_{n=0}^{\infty}\tanh^n r\,|n\rangle_A|n\rangle_B. \tag{3.52}$$

This is a Gaussian state with vanishing first moments and a covariance matrix

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \tag{3.53}$$

The usefulness of the two-mode squeezed state lies in the strong correlations among the modes. In the limit of infinite squeezing the state approaches asymptotically the Einstein-Podolsky-Rosen state

$$|\psi\rangle_{\text{EPR}} \sim \delta(\hat{q}_A - \hat{q}_B)\,\delta(\hat{p}_A + \hat{p}_B), \tag{3.54}$$

with the positions and momenta of the modes being perfectly correlated and anti-correlated respectively. The EPR state (3.54) was utilized by Einstein, Podolsky and Rosen to (wrongly) argue that quantum mechanics is incomplete. We will discuss in more detail about this issue, which is known as the EPR paradox, in Chapter 7.

3.3.3 Symplectic formalism

When dealing with Gaussian states, an important class of operations are the so-called Gaussian unitaries. These are unitary operations that preserve both the purity and the Gaussianity of the state. We have already encountered examples of Gaussian unitaries, like the Weyl (or, displacement) operator $\hat{D}(\alpha)$ (3.15) and the squeezing operator $\hat{S}(\zeta)$ (3.42), and there are plenty of more interesting examples of such unitaries that are routinely utilized both in theory and experiment, like beam splitters and phase shifters. Let us denote an arbitrary Gaussian unitary as $\hat{U}_G$. The way $\hat{U}_G$ acts on the state space is to map a Gaussian state $\hat{\rho}_{\bar{\mathbf{x}},\boldsymbol{\sigma}}$ onto another Gaussian state $\hat{\rho}_{\bar{\mathbf{x}}',\boldsymbol{\sigma}'}$ of the same purity,

$$\hat{\rho}_{\bar{\mathbf{x}},\boldsymbol{\sigma}} \longrightarrow \hat{\rho}_{\bar{\mathbf{x}}',\boldsymbol{\sigma}'} = \hat{U}_G \hat{\rho}_{\bar{\mathbf{x}},\boldsymbol{\sigma}} \hat{U}_G^\dagger. \tag{3.55}$$

Given the mathematical convenience of dealing with Gaussian states using their first and second moments, instead of their quantum states, we would like to find how a unitary $\hat{U}_G$ transforms the moments themselves. Unitary transformations on a Hilbert space are mapped to real symplectic transformations on the first and second moments as,

$$\hat{\rho}_{\bar{\mathbf{x}}',\boldsymbol{\sigma}'} = \hat{U}_G \hat{\rho}_{\bar{\mathbf{x}},\boldsymbol{\sigma}} \hat{U}_G^\dagger \longrightarrow \begin{cases} \bar{\mathbf{x}}' = \mathbf{S}\,\bar{\mathbf{x}} + \mathbf{d} \\ \boldsymbol{\sigma}' = \mathbf{S}\,\boldsymbol{\sigma}\,\mathbf{S}^{\mathrm{T}}, \end{cases} \tag{3.56}$$

where $\mathbf{d} \in \mathbb{R}^{2N}$, and $\mathbf{S}$ is a square $2N \times 2N$ real matrix. The pair $(\mathbf{d}, \mathbf{S})$ represents the Gaussian unitary operation in the space of first and second moments, while $\mathbf{S}$ is known as a *symplectic matrix*. This simple transformation rule holds, however, only for *Gaussian* unitary transformations which are defined as those unitary operators whose exponents are, at most, quadratic in the mode operators. In any other case, the unitary would be *non-Gaussian*. The set of all symplectic matrices belong to the so-called symplectic group $\mathrm{Sp}(2N,\mathbb{R})$, defined as

$$\mathrm{Sp}(2N,\mathbb{R}) = \left\{ \mathbf{S} \,:\, \mathbf{S}\boldsymbol{\Omega}\mathbf{S}^{\mathrm{T}} = \boldsymbol{\Omega} \right\}, \tag{3.57}$$

where $\boldsymbol{\Omega}$ is the symplectic form defined in Eq. (3.8).

3.3.3.1 Examples

Let us study some important examples of Gaussian unitaries with their corresponding symplectic matrices.

Phase shift. A single-mode rotation in phase space by an angle $\phi/2$ is known as phase shift, and is represented by the unitary operation

$$\hat{U}(\phi) = \exp\left(i\phi\hat{a}^\dagger\hat{a}\right). \tag{3.58}$$

It's corresponding symplectic matrix reads,

$$\mathbf{S}(\phi) = \begin{pmatrix} \cos\left(\frac{\phi}{2}\right) & -\sin\left(\frac{\phi}{2}\right) \\ \sin\left(\frac{\phi}{2}\right) & \cos\left(\frac{\phi}{2}\right) \end{pmatrix}. \tag{3.59}$$

Beam splitter. A most common unitary operation is the ideal (phase-free) beam splitter, which takes as input two modes A and B and coherently combines them such that the output modes are,

$$\hat{U}_{A,B}(\phi) : \begin{cases} \hat{a} \longrightarrow \hat{a}\cos\phi + \hat{b}\sin\phi \\ \hat{b} \longrightarrow \hat{a}\sin\phi - \hat{b}\cos\phi. \end{cases} \tag{3.60}$$

A beam splitter with transmissivity τ corresponds to a rotation of $\phi = \arccos\sqrt{\tau}$. In particular, a balanced $50:50$ beam splitter having $\tau = 1/2$, corresponds to $\phi = \pi/4$. The symplectic matrix that describes the ideal beam splitter is,

$$\mathbf{S}_{A,B}(\tau) = \begin{pmatrix} \sqrt{\tau} & 0 & \sqrt{1-\tau} & 0 \\ 0 & \sqrt{\tau} & 0 & \sqrt{1-\tau} \\ \sqrt{1-\tau} & 0 & -\sqrt{\tau} & 0 \\ 0 & \sqrt{1-\tau} & 0 & -\sqrt{\tau} \end{pmatrix}. \tag{3.61}$$

Single-mode squeezing. The squeezing operator that was introduced in Eq. (3.42),

$$\hat{S}(\zeta) = \exp\left[\frac{1}{2}\left(\zeta\hat{a}^{\dagger\,2} - \zeta^*\hat{a}^2\right)\right], \text{ where } \zeta = re^{i\theta}, \tag{3.62}$$

has the following symplectic representation,

$$\mathbf{S}(r,\theta) = \begin{pmatrix} \cosh(r) + \cos(\theta)\sinh(r) & \sin(\theta)\sinh(r) \\ \sin(\theta)\sinh(r) & \cosh(r) - \cos(\theta)\sinh(r) \end{pmatrix}. \tag{3.63}$$

Two-mode squeezing by beam splitting single-mode squeezed states. As we mentioned previously, a two-mode squeezed state $|r\rangle_{AB}$ can be prepared by passing two independent single-mode squeezed states through a balanced $50:50$ beam splitter (see Fig. 3.1). Now that we

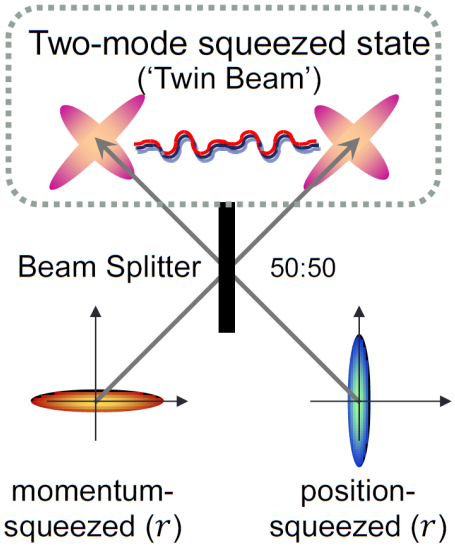

Figure 3.1: The preparation procedure of a two-mode squeezed state is pictorially demonstrated, by sending position- and momentum-squeezed states through a balanced 50:50 beam splitter. For the mathematical description of the process, see text. (From G. Adesso's tutorial lecture in Paraty Summer School, Brazil, 2013)

have introduced all the relevant mathematical machinery that describe such a process, let us see how to get the CM of a two-mode squeezed state (3.53) by such an operation.

We start with two single-mode squeezed states, with mode A being squeezed in the p-quadrature while mode B in the q-quadrature. Their individual CMs will be,

$$\boldsymbol{\sigma}_A(r) = \begin{pmatrix} e^{2r} & 0 \\ 0 & e^{-2r} \end{pmatrix}, \quad \boldsymbol{\sigma}_B(r) = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}, \tag{3.64}$$

with their joint product state being described by the CM,

$$\boldsymbol{\sigma}_{AB}(r) = \boldsymbol{\sigma}_A(r) \oplus \boldsymbol{\sigma}_B(r).$$

Next, the $50:50$ beam splitter, with transmissivity $\tau = 1/2$, acts on the joint state $\boldsymbol{\sigma}_{AB}(r)$ via the symplectic matrix $\mathbf{S}_{A,B}(\tau)$ Eq. (3.61), and through the transformation rule Eq. (3.56), giving the desired output state

$$\begin{aligned} \boldsymbol{\sigma}'_{AB}(r) &= \mathbf{S}_{A,B}(1/2)\, \boldsymbol{\sigma}_{AB}(r)\, \mathbf{S}^{\mathrm{T}}_{A,B}(1/2) \\ &= \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}, \end{aligned} \tag{3.65}$$

which is precisely the CM of the two-mode squeezed state derived in Eq. (3.53).

3.3.4 Standard forms

An N-mode Gaussian state $\hat{\rho}$ has, in general, arbitrary first moments $\bar{\mathbf{x}}$ and covariance matrix $\boldsymbol{\sigma}$, with all the matrix elements of the latter being in general non-zero. In other words, the form of $(\bar{\mathbf{x}}, \boldsymbol{\sigma})$ is in general 'non-standard' and complicated, and the point of this section is to show that a simpler *standard form* exists for arbitrary Gaussian states.

Let us first discuss the context behind such a simplification: given a state with moments $(\bar{\mathbf{x}}, \boldsymbol{\sigma})$, why would one alter it to get a different form (even though, simpler) of the state? In the field of quantum information, when we study N-mode states we implicitly assume that these states will be used for some non-classical protocol that involves distribution of each mode of the state to different users (as, for example, happens in quantum communication and cryptographical applications). In such scenarios, if we can alter the state giving it a simpler form, then as long as the new simpler state performs equally well (not worse) in the considered task then we can only benefit from such a simplification. The state can be altered by the N users (each holding a different mode) by applying *local operations and classical communication* (LOCC), and in particular Gaussian unitary local operations. The class of LOCC operations are known not to increase the amount of entanglement in a quantum state.

Given this context, standard forms have been derived in the literature for general N-mode Gaussian states that can be attained by starting from an arbitrary Gaussian state and then use suitable Gaussian unitary LOCC. For details, see Refs [42, 43, 44]. In the following, we only report the results for general two-mode and pure three-mode states that will be utilized later on in the thesis.

Two modes [45] The expression of the two-mode CM $\boldsymbol{\sigma}_{AB}$ in terms of the three 2×2 matrices $\mathbf{A}, \mathbf{B}, \mathbf{C}$, that will be useful in the following, takes the form

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathrm{T}} & \mathbf{B} \end{pmatrix}. \tag{3.66}$$

For any two-mode CM $\boldsymbol{\sigma}_{AB}$ there is a local symplectic operation $\mathbf{S} = \mathbf{S}_1 \oplus \mathbf{S}_2$ which brings $\boldsymbol{\sigma}$ in the standard form $\bar{\boldsymbol{\sigma}}_{AB}$

$$\bar{\boldsymbol{\sigma}}_{AB} = \begin{pmatrix} a & 0 & c_1 & 0 \\ 0 & a & 0 & c_2 \\ c_1 & 0 & b & 0 \\ 0 & c_2 & 0 & b \end{pmatrix}. \tag{3.67}$$

The covariances a, b, c_1 and c_2 are determined by the four local symplectic invariants (i.e., invariants under local unitary operations) $\sigma_{AB} = (ab - c_1^2)(ab - c_2^2)$, $\det \mathbf{A} = a^2$, $\det \mathbf{B} = b^2$, and $\det \mathbf{C} = c_1 c_2$. The standard form corresponding to any CM is unique (up to a common sign flip in c_1 and c_2).

Three modes [46] The general form of a three-mode CM $\boldsymbol{\sigma}$ is given in terms of the 2×2 matrices $\boldsymbol{\alpha}_i, \mathbf{e}_{ij}$ (for, $i, j = 1, 2, 3$),

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\alpha}_1 & \mathbf{e}_{12} & \mathbf{e}_{13} \\ \mathbf{e}_{12}^{\mathrm{T}} & \boldsymbol{\alpha}_2 & \mathbf{e}_{23} \\ \mathbf{e}_{13}^{\mathrm{T}} & \mathbf{e}_{23}^{\mathrm{T}} & \boldsymbol{\alpha}_3 \end{pmatrix}. \tag{3.68}$$

For any pure three-mode CM $\boldsymbol{\sigma}$ (i.e., states with $\det \boldsymbol{\sigma} = 1$) there is a local symplectic operation $\mathbf{S} = \mathbf{S}_1 \oplus \mathbf{S}_2 \oplus \mathbf{S}_3$ which brings $\boldsymbol{\sigma}$ in the standard form $\boldsymbol{\sigma}_{\mathrm{sf}}$

$$\boldsymbol{\sigma}_{\mathrm{sf}} = \begin{pmatrix} a_1 & 0 & e_{12}^{+} & 0 & e_{13}^{+} & 0 \\ 0 & a_1 & 0 & e_{12}^{-} & 0 & e_{13}^{-} \\ e_{12}^{+} & 0 & a_2 & 0 & e_{23}^{+} & 0 \\ 0 & e_{12}^{-} & 0 & a_2 & 0 & e_{23}^{-} \\ e_{13}^{+} & 0 & e_{23}^{+} & 0 & a_3 & 0 \\ 0 & e_{13}^{-} & 0 & e_{23}^{-} & 0 & a_3 \end{pmatrix}, \tag{3.69}$$

where the symplectic invariants $a_i = \sqrt{\det \boldsymbol{\alpha}_i} = \mu_i^{-1}$ are related to the purities of the reduced CMs $\boldsymbol{\alpha}_i$, and

$$\begin{aligned} e_{ij}^{\pm} \equiv \Big(\Big[(a_i - a_j)^2 - (a_k - 1)^2 \Big] \Big[(a_i - a_j)^2 - (a_k + 1)^2 \Big] \pm \\ \sqrt{\Big[(a_i + a_j)^2 - (a_k - 1)^2 \Big] \Big[(a_i + a_j)^2 - (a_k + 1)^2 \Big]} \Big)^{1/2} / \left(4 \sqrt{a_i a_j} \right). \end{aligned} \tag{3.70}$$

3.3.5 Homodyne measurements

The importance of quadrature measurements in the description of bosonic CV systems cannot be overstated, and especially in the case of Gaussian states where the first and second moments of the quadratures are enough to fully characterize them. Homodyne measurement is a simple technique that allows us to measure the desired quadratures $\hat{q}$ and $\hat{p}$ of a single-mode.

Let us assume that a is the mode the quadratures of which, $\hat{q}$ and $\hat{p}$ we'd like to measure. We implement the scheme considered in Fig. 3.2, where we consider a balanced $50 : 50$ beam splitter with the inputs modes being a, a_{LO} and the output modes b_1, b_2, with a_{LO} being

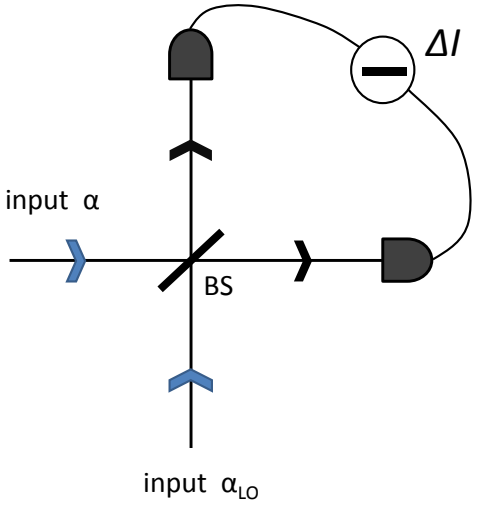

Figure 3.2: Homodyne measurement

an auxiliary field, to be described below, that will help us with the measurement. We then measure the intensity difference ΔI of the two output modes, using photocurrent detectors,

$$\Delta I = \langle \hat{b}_1^\dagger \hat{b}_1 - \hat{b}_2^\dagger \hat{b}_2 \rangle = \langle \hat{a}^\dagger \hat{a}_{\mathrm{LO}} + \hat{a}_{\mathrm{LO}}^\dagger \hat{a} \rangle, \tag{3.71}$$

where we ΔI it w.r.t. the input modes by using the quadrature transformation rule Eq. (3.60) for a balanced beam splitter. We then assume that the field mode a_{LO} is a strong local oscillator, i.e. a bright coherent state $|\alpha_{\mathrm{LO}}\rangle$ with a large photon number. It's therefore reasonable to describe this oscillator with the complex number α_{LO}, and therefore replace the operators $\hat{a}_{\mathrm{LO}}, \hat{a}_{\mathrm{LO}}^\dagger$ with the complex amplitudes $\alpha_{\mathrm{LO}}, \alpha_{\mathrm{LO}}^*$ of the now "classical" field,

$$\Delta I = \langle \hat{a}^\dagger \alpha_{\mathrm{LO}} + \alpha_{\mathrm{LO}}^* \hat{a} \rangle. \tag{3.72}$$

By introducing the phase ζ of the local oscillator, $\alpha_{\mathrm{LO}} = |\alpha_{\mathrm{LO}}| e^{i\zeta}$, fixing it to the values $\zeta = 0$ and $\frac{\pi}{2}$ it allows us to measure the desired quadratures $\hat{p}$ and $\hat{q}$ respectively,

$$\zeta = 0: \quad \Delta I = \sqrt{2}\, |\alpha_{\mathrm{LO}}|\, \langle \hat{p} \rangle \tag{3.73}$$

$$\zeta = \frac{\pi}{2}: \quad \Delta I = \sqrt{2}\, |\alpha_{\mathrm{LO}}|\, \langle \hat{q} \rangle. \tag{3.74}$$

4

The pyramid of quantum correlations

The advent of quantum information theory together with the technological advancements that allowed us to address and manipulate individual quantum systems, has put a solid foundations for the rise of a *second quantum revolution* that is expected to provide us with immense applications never thought possible before. In the previous century, a first quantum revolution gave rise to ground-breaking technologies like the LASER, semi-conductors, solar panels, etc. Such novel applications although made possible by a better understanding of quantum theory, they didn't really make use of genuine quantum effects, such as entanglement and superposition. The anticipated applications of the second quantum revolution, including quantum computing and quantum simulations to quantum communications and metrological applications, draw their power particularly from such genuinely quantum properties. An important and timely question that was asked is,

What are the quantum properties that provide with a quantum advantage?

A particularly fruitful way to deal with this question is to focus, for reasons to become clear shortly, at the achievable correlations among different subsystems. Considering for simplicity a bipartite system A and B, the term *correlation*, in general, is defined by the set of joint probability distributions of simultaneous measurements x, y performed on each of the subsystems A, B respectively, with corresponding outcomes X, Y; i.e., $\{P(X, Y|x, y)\}$. In the case of quantum systems, measurement operators can be assigned (projectors or, more generally, POVMs), giving

$$P(X, Y|x, y) = \mathrm{tr}\left[\left(\hat{N}_X \otimes \hat{M}_Y\right) \hat{\rho}_{AB}\right]. \tag{4.1}$$

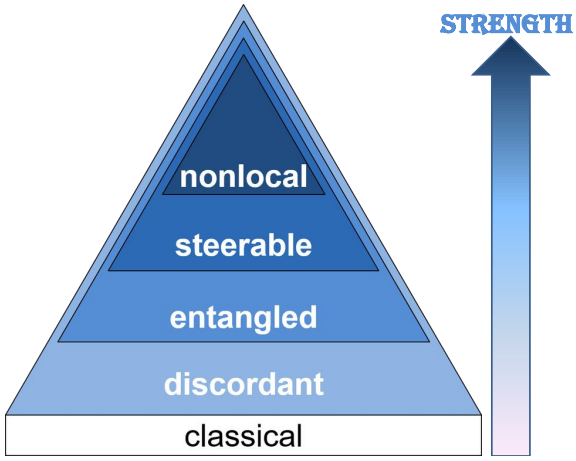

Figure 4.1: Hierarchy of correlations in composite quantum systems

In general, correlations among composite quantum states, of the type (4.1), are known as *quantum correlations*. How is this relevant to the question posed above? If one looks at some of the first and most important proposed applications in quantum information theory, like Shor's quantum algorithm [47] that can break the RSA cryptosystem exponentially faster than any classical algorithm, or Ekert's quantum cryptographic protocol [48] that provides with unconditional secrecy in communications; they all rely on *entanglement*. Entanglement is a particular type of strong quantum correlations with highly non-classical features. Due to this connection between entanglement and novel applications in the early years of quantum information theory, theoretical and experimental attention was mainly focused on developing and preserving entanglement among different subsystems. It was once thought that entanglement is the only kind of non-classical correlations featured in quantum systems; i.e., unentangled states were though to be useless in terms of providing some quantum advantage in a given task.

It was soon realized, however, that entanglement is just part of a larger *zoo* of different types of quantum correlations, which we depict in Fig. 4.1 in the form of a pyramid. Just for illustration purposes, we can imagine the area of the pyramid to indicate the set of all quantum states in all of Hilbert space, with each particular point representing a distinct quantum state (without meaning to imply that the actual geometry of the Hilbert space is a pyramid). Each type of correlation forms a triangle in the pyramid, and a point that falls into the triangle features the particular property. Obviously, the bigger the triangle of a property the more states it includes with that property. The arrow on the right side of the pyramid indicates the strength of the correlations, which increases as we climb the pyramid upwards.

At the bottom of the pyramid, having the least strength of all, distinctly lie the set of states featuring solely *classical correlations* also achievable by effectively classical systems. This part of Hilbert space is actually negligibly small [49], and undoubtedly constitutes the "non-interesting" part of Hilbert space.

The first level in the pyramid, contains all those states that feature *discord* [50]. Discordant states constitute almost the whole Hilbert space [49], and most importantly this most elementary type of quantum correlations features non-classical behaviour, yet they don't necessarily contain any entanglement. This realization came as a surprise in the community, when evidence arose that discord might be the key resource behind the speed-up of a particular quantum algorithm, known as DQC1 [51]. Although up to this day there has been no consensus regarding the clear operational link between discord and a speed-up, discordant has been shown to be useful in various non-classical tasks in quantum information and communication, including: local broadcasting, entanglement distribution, quantum state merging, remote state preparation, quantum cryptography, quantum locking, quantum metrology, and lastly state discrimination and quantum illumination. For details regarding such applications see Ref. [50, 52, 53].

The second level represents the more correlated *entangled* states [54], and as is seen, entangled states necessarily contain discord. This type of correlations is a case of study in the present thesis, together with one of the most important non-classical applications that entanglement allows for; quantum teleportation. For more details, see Part II.

The third level contains even stronger correlations, known as *steering*. As shown in Fig. 4.1, steerable states necessarily feature both entanglement and discord. Steering was recently formalized by Wiseman *et al.* [12] as a novel type of quantum correlations, intimately related to the infamous Einstein-Podolsky-Rosen paradox [55], and has found various interesting applications in tasks with the advantage that no characterization is made for some of the parties (i.e., unknown Hilbert space). Examples of tasks that are implemented in such a one-sided device independent fashion are: entanglement certification, randomness generation, sub-channel discrimination, self-testing, quantum key distribution and quantum secret sharing. See Ref. [56] for a recent review on some of these topics. Steering-type correlations in bipartite and multipartite systems will be exhaustively studied in Part III.

The final level in the pyramid contains the strongest type of quantum correlations allowed by the laws of quantum mechanics, known as *Bell-nonlocality* [57, 58]. Bell-nonlocality is admittedly the most non-classical feature of quantum theory and its mere existence has shaken our perceptions about how the world works in a fundamental level. Nonlocal states also feature

all the weaker types of correlations. Therefore, besides the optimal performance of nonlocal states in all the aforementioned tasks, Bell-nonlocality allows for the implementation of tasks that make no characterization of any of the parties involved, i.e. in a device-independent manner. Examples of such tasks are: entanglement certification, randomness generation and quantum key distribution. For a recent review on nonlocality see Ref. [59], while only very recently three different experimental groups demonstrated the first loophole-free Bell inequality violations in Refs [60, 61, 62].

4.1 If nonlocality is best, why bother 'bout the rest?

Nonlocal correlations are seen to sit at the top of the pyramid representing the strongest type of all quantum correlations, and therefore, by definition, quantum states with nonlocal correlations perform best in all non-classical tasks we individually listed for each of the weaker types of correlations. Why do we then consider all these different types of correlations and don't simply prepare the ultimate resource, nonlocality, straight away?

One reason is *noise*. Any real-world implementation of a task is unavoidably noisy and, consequently, subject to decoherence. The effect of decoherence can be seen as climbing *down* the pyramid, as it gradually destroys the quantum correlations in the state. Therefore, it's usually hard to create a pure maximally entangled state with nonlocal correlations, and it would be great to know if we can implement the same task with a weaker type of correlations.

Another important reason is *insufficient experimental equipment*. In some cases, the quantum states with the "perfect correlations" that are optimal for the given task cannot be efficiently prepared in the laboratory with today's technology. Quantum key distribution (QKD) with qubit systems is a task that falls exactly into this category. It's known, for example, that the optimal states for QKD are ideal single photon states which give very high secret key rates. However, there currently exist no single photon sources that can produce ideal single photon states. Moreover, if sending single-photon states is one thing, then measuring them is another. A perfect measurement of such a state requires perfect single-photon detectors. The current efficiency, however, of such detectors is not very high although progress has being made.

Moreover, in the case of continuous variable systems, in order to observe nonlocal correlations one is obliged to either prepare a non-Gaussian state or to perform so-called non-Gaussian measurements on a Gaussian state. Even if the entanglement of the state tends to infinity, nonlocality cannot be manifested unless there exists an element of non-Gaussianity (either in the

state, or in the measurement, or in both). Although, Gaussian state and Gaussian measurements (like, quadrature measurements) are routinely prepared/performed in quantum optics laboratories around the world, creating non-Gaussianities is experimentally demanding which implies that nonlocality is a scarce resource when it comes to continuous variable systems. However, although Gaussian states and measurements cannot produce nonlocal correlations, they can produce steering-type correlations, and as the entanglement of the state increases, steering increases as well unboundendly. This implies the following remarkable realization: We can perform a task that requires steering, like one-sided device independent QKD, arbitrarily well even if we don't have access to nonlocal correlations. This is a demonstration that different types of quantum correlations can, under particular constraints, be regarded as completely independent resources.

Part II

Entanglement and applications

5

Quantum entanglement

In this chapter we will introduce the concept of entanglement, and describe particular entanglement detection and quantification techniques that will be put to use in Part III, with the main focus being continuous variable (CV) states. We will then introduce the task of *quantum teleportation*, and present novel results on the topic which were published in *Physical Review A* [1]. In particular, we will critically examine how efficiently current teleportation schemes can teleport general pure Gaussian states, and how such schemes perform against prepare & measure strategies that make use of no entanglement.

5.1 Introduction

It's no secret that quantum theory has been puzzling physicists, since its birth in the early years of the 20th century, due to its seemingly total departure from the classical world. Quantum theory predicted phenomena, like: the superposition principle, Bohr's complementarity, Heisenberg's uncertainty principle and the quantization of radiation. But what is it exactly that makes the quantum stranger than the classical? This question was hotly debated by the founding fathers of quantum theory, and the answer is not clear. The superposition principle already existed in classical wave mechanics as waves can be superposed. Also, Bohr's complementarity and Heisenberg's uncertainty principle also have a counterpart in classical waves and in particular in the trade-off between the knowledge of the position of a wave and its wavelength. The quantization of radiation, which Planck was forced to postulate in an 'act of desperation' to explain the intensity profile of the black-body radiation, although non-existent in classical

physics it can at least be mimicked -energy can be coarse-grained classically. What is it then that makes quantum theory so special?

Schrödinger found the answer to be, *entanglement*; it's the one quantum phenomenon that has absolutely no classical counterpart and cannot even be mimicked by classical systems. As we already briefly discussed in Chapter 2, entanglement is a consequence of the superposition principle when applied to multiple systems. The reason it's so counter-intuitive and presents a radical departure from classical physics can be summarized as follows:

α) When two (or, more) quantum systems are entangled, they are no longer independent from one another and behave like a single inseparable quantum system. This phenomenon is expressed by the fact that the most complete description we can have for a composite quantum system, fundamentally contains no (or, less) information about its parts. In other words, we can perfectly know the quantum state of the composite system, but be completely uncertain for the quantum state of the subsystems. This is a strikingly non-classical phenomenon: In classical physics, almost by definition, a complete knowledge of the whole directly implies complete knowledge of the parts. Surprisingly, in the quantum realm *..the whole can be less uncertain than either of its parts*.

β) The utterly non-classical phenomenon described in α) may still be refuted by some as an incompleteness of quantum theory. In fact this is exactly how Einstein, Podolsky and Rosen reacted to the puzzling phenomenon of entanglement in their infamous EPR paper, to be discussed in Part III, arguing in favour of the theory's incompleteness. After all, if quantum theory is an incomplete theory why should we care about the catchphrase "the whole can be less uncertain than either of its parts"? A more complete theory, if existed, could actually provide with the (missing) description of the parts after all. Although this is a valid point, John Bell managed to raise the level of the discussion about the incompleteness of quantum theory from a philosophical level to an experimentally testable one. He realized that entanglement predicts so strong correlations among independent and spatially separated quantum systems that cannot be explained by any theory that describe the subsystems as independent, and without invoking *nonlocality* (i.e., an instantaneous 'action-at-a-distance" between the subsystems). This phenomenon has been termed *Bell-nonlocality* and is the epitome of quantum weirdness (see, Fig. 4.1).

Besides any philosophical debates, it has become clear in the recent years that entanglement is a new quantum resource for tasks which can not be performed by means of classical resources. Entanglement is the resource that enables universal quantum computers which can solve some important classes of problems exponentially faster than any classical machine. Entanglement is also an a necessary resource in quantum communication, quantum key distribution and other cryptographical applications, as well as in quantum metrology [63] where entangled probes are utilized to achieve unprecedented accuracy in parameter estimation. Another most important application of entanglement is quantum teleportation, a task that allows us to "teleport" arbitrary quantum states to distant unknown locations without physically sending the system. See Refs [64, 65] for more details on the applications of entanglement. Given the importance of entanglement not only for the foundations of quantum theory but also for the development of new quantum technologies, it is a pre-requisite that for entanglement to be any useful one should be able to detect it and quantify it. Is a quantum state entangled or not, and if yes *how much* entanglement does it possess? We will briefly examine these questions in the next sections.

5.2 Entanglement detection

Entanglement, or non-separability, is the particular feature of composite quantum states that does not allow for an independent local description of the parts; in other words, it is impossible to assign particular (even though, unknown) quantum states to the subsystems when they are part of an entangled state. If such an assignment is possible, the state is called *separable* which is the opposite of entangled (or, non-separable). For the following, let us focus to arbitrary bipartite states $\hat{\rho}_{AB}$ and, hence, bipartite entanglement. Below we give the definition of separable states, therefore defining entangled states as those that are not separable.

Definition 5.2.1. *A bipartite quantum state $\hat{\rho}_{AB} : \mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if there exists an assignment of states $\hat{\rho}_A^\lambda : \mathcal{H}_A$ and $\hat{\rho}_B^\lambda : \mathcal{H}_B$, and probabilities p_λ, such that the bipartite state can be written in the form,*

$$\hat{\rho}_{AB} = \sum_\lambda p_\lambda \hat{\rho}_A^\lambda \otimes \hat{\rho}_B^\lambda, \quad \text{with,} \quad \sum_\lambda p_\lambda = 1. \tag{5.1}$$

In the special case of pure states this definition collapses to the product state, $|\psi\rangle_{AB} = |\chi\rangle_A \otimes |\phi\rangle_B$.

States of the form (5.1) are called separable because they can be created without the use of any entanglement, and just by local operations and classical communication (LOCC) between Alice (for, A) and Bob (for, B). In particular, Alice and Bob collaboratively choose a particular λ, with probability p_λ, and for that choice they prepare the product state $\hat{\rho}_A^\lambda \otimes \hat{\rho}_B^\lambda$. Forgetting the "which-$\lambda$" information leads to a state of the separable form (5.1).

Given a state $\hat{\rho}_{AB}$, how can we tell if it is entangled? Below we examine various ways to detect entanglement.

5.2.1 Entanglement Witnesses

Imagine an experiment taking place in a laboratory where a pair of particles is produced in an unknown bipartite quantum state by, say, some physical process. How can we tell whether the produced state is entangled? Here, is where the entanglement witnesses join the scene. In simple words, an entanglement witness is an observable which we can measure. By measuring its mean value with respect to the unknown quantum state we can infer about the state's entanglement as follows:

Definition 5.2.2. *We call an observable $\hat{W}$ an entanglement witness if*
- $Tr\left[\hat{W}\hat{\rho}_S\right] \geq 0$ *- for all separable states $\hat{\rho}_S$,*
- $Tr\left[\hat{W}\hat{\rho}_E\right] < 0$ *- for at least one entangled state $\hat{\rho}_E$.*

In order to easier understand this concept, let us work out a specific example.

Example Consider two spin-$\frac{1}{2}$ particles coupled by a Heisenberg interaction $\hat{H} = -J\vec{\sigma}_A\vec{\sigma}_B$ where J is the coupling strength and $\vec{\sigma}$ denotes the Pauli matrices of particles A and B respectively. It's easy to see that for any separable state of the form (5.1), the absolute average energy of the system is bounded from above as,

$$\left|\left\langle \hat{H}\right\rangle_S\right| = J\left|\sum_\lambda p_\lambda \langle\vec{\sigma}_A\rangle_\lambda\langle\vec{\sigma}_B\rangle_\lambda\right| \leq J\sum_\lambda p_\lambda\left|\langle\vec{\sigma}_A\rangle_\lambda\langle\vec{\sigma}_B\rangle_\lambda\right| \leq J, \tag{5.2}$$

where we used, $\left|\langle\vec{\sigma}_A\rangle_\lambda\langle\vec{\sigma}_B\rangle_\lambda\right| \leq 1$. However, consider that the two particles are in the singlet state

$$\left|\psi^-\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\downarrow_z\rangle_B - |\downarrow_z\rangle_A|\uparrow_z\rangle_B\right),$$

which is a maximally entangled state. For this state, the average energy of the system obviously exceeds the previous bound,

$$\left\langle \hat{H}\right\rangle_{\psi^-} = {}_{AB}\left\langle\psi^-\right|\hat{H}\left|\psi^-\right\rangle_{AB} = 3J. \tag{5.3}$$

This fact constitutes the Hamiltonian $\hat{H} = -J\vec{\sigma}_A\vec{\sigma}_B$ an entanglement witness, which can be measured in the lab and reveal entanglement without us knowing the quantum state of the particles.

Some of the important problems that have concerned the literature over the years are the construction of entanglement witnesses and their optimality. Regarding the latter, a witness W_1 is considered to be finer than W_2, if it detects all the entangled states that W_2 does. Consequently, it's natural to try and find procedures that give the *optimal* witness, i.e. the one such that no other witness can outperform. Such an investigation was carried out, for example, by Lewenstein *et. al.* in [66]. In Part III we will utilize the concept of witnesses to detect quantum steering, a form of quantum correlations that is stronger than plain entanglement.

5.2.2 The Peres-Horodecki PPT criterion

One of the most important separability criteria, the Positive Partial Transposition (PPT) criterion, was first developed by A. Peres [67] and has found immense uses both for discrete and continuous variable systems. The key idea behind this criterion is that any bipartite state of the separable form (5.1) remains a valid quantum state if we consider the operation of partial transposition on $\hat{\rho}_{AB}$ (say, w.r.t. system B), i.e. $\hat{\rho}_{AB}^{\mathrm{T_B}}$, defined as the total transposition of any of the subsystems,

$$\hat{\rho}_{AB}^{\mathrm{T_B}} = \sum_{\lambda} p_\lambda \hat{\rho}_A^\lambda \otimes (\hat{\rho}_B^\lambda)^{\mathrm{T}}. \tag{5.4}$$

On a given basis, the total transposition of an operator is defined as,

$${}_B\langle n|(\hat{\rho}_B^\lambda)^{\mathrm{T}}|m\rangle_B = {}_B\langle m|\hat{\rho}_B^\lambda|n\rangle_B. \tag{5.5}$$

It's straightforward to see that a totally transposed density matrix $(\hat{\rho}_B^\lambda)^{\mathrm{T}}$ also represents a physical state, as it remains a positive semi-definite operator with unit trace: $(\hat{\rho}_B^\lambda)^{\mathrm{T}} \geq 0$ and $\mathrm{tr}(\hat{\rho}_B^\lambda)^{\mathrm{T}} = 1$. We conclude that $\hat{\rho}_{AB}^{\mathrm{T_B}}$ should have non-negative eigenvalues for any separable state $\hat{\rho}_{AB}$. However, if a given state $\hat{\rho}_{AB}$ is entangled some of the eigenvalues of the partial transposed $\hat{\rho}_{AB}^{\mathrm{T_B}}$ *could* be negative.

The PPT criterion *All separable states $\hat{\rho}_{AB}$ remain positive under partial transposition, $\hat{\rho}_{AB}^{\mathrm{T_B}} \geq 0$.*

The PPT criterion gives a necessary condition for separability, but not always sufficient. Few months after the publication of Peres' result, the Horodecki family proved [68] that the PPT criterion is actually necessary and sufficient for separability in the case of discrete variable systems of dimensions 2×2 and 2×3. In the case of continuous variable systems, the PPT criterion was proven by Simon [69] to also be necessary and sufficient for two-mode Gaussian states, and was extended by Werner and Wolf to $1 \times N$-mode states [70]. We will examine Simon's formulation in the next section. It suffices to say that these contributions made PPT a very powerful and simple criterion.

Finally, for Hilbert space dimensions other than $2 \times 2(3)$ for DV systems, and than $1 \times N$-mode Gaussian states for CV systems, there exist PPT entangled states, i.e. entangled states whose partial transpose has only positive eigenvalues, whose entanglement is undetectable by the PPT criterion. This type of entanglement is known as *bound entanglement* [71]. In Chapter 9, we will show that bound entangled Gaussian states cannot provide with stronger correlations the steering-type when only Gaussian measurements are considered.

5.2.2.1 Application to Gaussian states

With increasing Hilbert space dimension, any separability criterion can be expected to be more and more difficult to implement in practice. The PPT criterion itself was seen to be most effective for the smallest Hilbert space dimensions 2×2 and 2×3, while failing to detect all the existing entanglement of higher dimensional states. One would thus expect that in the limit of infinite dimension, describing CV systems, the PPT criterion would be useless. Contrary to expectations, Simon proved in Ref. [45] that PPT becomes a necessary and sufficient for separability for two-mode Gaussian states, and even extended later on to $1 \times N$-modes by Werner and Wolf [70]. It seems, therefore, that PPT is more effective in CV than in DV systems.

Central to Simon's idea was the realization that the partial transpose operation acquires, in the continuous case, a beautiful geometric interpretation as mirror reflection in the Wigner phase space,

$$\hat{\rho} \longrightarrow \hat{\rho}^{\mathrm{T}} \Longleftrightarrow W(q,p) \longrightarrow W(q,-p). \tag{5.6}$$

Any physical Gaussian state $\hat{\rho}_{AB}$ with CM $\boldsymbol{\sigma}_{AB}$ satisfies the *bona fide* condition (3.27),

$$\boldsymbol{\sigma}_{AB} + i\,\boldsymbol{\Omega}_A \oplus \boldsymbol{\Omega}_B \geq 0. \tag{5.7}$$

If $\hat{\rho}_{AB}$ is separable, then $\hat{\rho}_{AB}^{\mathrm{T_B}}$ should be a physical state with CM $\tilde{\boldsymbol{\sigma}}_{AB}$ (obtained from $\hat{\rho}_{AB}^{\mathrm{T_B}}$ by, $\hat{p}_B \to -\hat{p}_B$) satisfying the corresponding *bona fide* condition, which can equivalently be expressed in terms of the original CM $\boldsymbol{\sigma}_{AB}$ as

$$\boldsymbol{\sigma}_{AB} + i\,(-\boldsymbol{\Omega}_A) \oplus \boldsymbol{\Omega}_B \geq 0. \tag{5.8}$$

Ineq. (5.8) is Simon's separability criterion which is an application of the Peres-Horodecki PTT criterion in phase space. This condition is satisfied by *all separable states*, whether multi-mode or (non-)Gaussian. In the particular case of $1 \times N$-mode Gaussian states the condition becomes necessary and sufficient for separability, and therefore detects all the entanglement of such states. In the more general case of $M \times N$-modes (with both $N, M > 1$) there exist Gaussian entangled states that do satisfy (5.8), therefore being bound entangled. For the sake of completeness, let us mention another important second-order entanglement criterion due to Dual *et al.* [72], which was derived independently of the Peres-Horodecki criterion but has been shown to be necessary and sufficient only for two-mode Gaussian states.

5.2.3 Shchukin and Vogel's higher order criteria

So far, our discussion on second-order separability criteria for bipartite continuous variables systems has focused on Simon's and Duan *et al.*'s separability criteria, which are of *second-order*, as they contain moments of quadratures only up to second order; i.e., $\langle \hat{q}^n\, \hat{p}^m \rangle$ with $n+m \leq 2$. Second-order criteria are important mainly due to their simple experimental implementation and their sufficiency for the important class of $1 \times N$ Gaussian states.

However, Gaussian states constitute only a tiny (although, important) fraction of the most general states living in the Hilbert space, with some of the more exotic ones also being of great importance for experiments and technological applications. For such cases where the second-order criteria are useless, higher-order criteria were derived that can be more efficient in entanglement detection. Shchukin and Vogel [73] developed a method based on moments of quadratures to systematically derive entanglement criteria of arbitrary order. Their method forms a hierarchy of criteria, meaning that the next criterion in the hierarchy is always better than, or equal to, the previous one. Interestingly, the method's generality is showcased by the fact that it contains other entanglement criteria, independently derived in the literature, as special cases; including Simon's and Duan *et al.*'s criteria [69, 72]. Let us examine in a bit more detail the method of Shchukin and Vogel, as it will be our main inspiration in Chapter 8.2 where we will introduce a similar in spirit hierarchy of criteria for steering detection.

The idea of Shchukin and Vogel is also based on the partial transposition which preserves the positivity of separable states. Consider an arbitrary (generally, not hermitian) operator $\hat{f} : \mathcal{H}_A \otimes \mathcal{H}_B$ and from it construct the observable $\hat{f}^\dagger \hat{f}$, which is hermitian. It's straightforward then to see that the average value of any such observable is non-negative for any physical state $\hat{\rho}_{AB} \geq 0$,

$$\langle \hat{f}^\dagger \hat{f} \rangle_{\rho_{AB}} = \mathrm{tr}[\hat{f}^\dagger \hat{f} \hat{\rho}_{AB}] = \sum_n p_n \| \hat{f} |p_n\rangle_{AB} \|^2 \geq 0, \quad \forall \hat{f}, \tag{5.9}$$

where $\hat{\rho}_{AB}|p_n\rangle_{AB} = p_n|p_n\rangle_{AB}$. Employing the PPT criterion, any separable state $\hat{\rho}_{AB}$ satisfies

$$\mathrm{tr}[\hat{f}^\dagger \hat{f} \hat{\rho}_{AB}^{\mathrm{T}_B}] \geq 0, \quad \forall \hat{f}, \tag{5.10}$$

since $\hat{\rho}_{AB}^{\mathrm{T_B}} \geq 0$. Eq. (5.10) can only be violated by entangled states and thus forms the basis of the hierarchy. Now, the most general form of an arbitrary operator $\hat{f}$ is

$$\hat{f} = \sum_{n,m,k,l=0}^{\infty} c_{nkml}\, \hat{a}^{\dagger n} \hat{a}^m \hat{b}^{\dagger k} \hat{b}^l, \tag{5.11}$$

where $\hat{a}^{(\dagger)}, \hat{b}^{(\dagger)}$ are annihilation(creation) operators for modes A and B respectively, while

$$c_{nmkl} = {}_A\langle n| \otimes {}_B\langle k|\, \hat{f} |m\rangle_A \otimes |l\rangle_B \equiv {}_{AB}\langle nk|\, \hat{f} |ml\rangle_{AB}. \tag{5.12}$$

Substituting (5.11) back to (5.10), we get

$$\mathrm{tr}[\hat{f}^\dagger \hat{f} \hat{\rho}_{AB}^{\mathrm{T}_B}] = \sum_{n,k,\ldots,s=0}^{\infty} c^*_{pqrs}\, c_{nmkl}\, M_{pqrs,nmkl} \geq 0, \quad \forall \hat{f}, \tag{5.13}$$

with,

$$M_{pqrs,nmkl} = \langle \hat{a}^{\dagger q} \hat{a}^p \hat{a}^{\dagger n} \hat{a}^m \hat{b}^{\dagger s} \hat{b}^r \hat{b}^{\dagger k} \hat{b}^l \rangle_{\rho_{AB}^{\mathrm{T_B}}} = \langle \hat{a}^{\dagger q} \hat{a}^p \hat{a}^{\dagger n} \hat{a}^m \hat{b}^{\dagger l} \hat{b}^k \hat{b}^{\dagger r} \hat{b}^s \rangle_{\rho_{AB}}. \tag{5.14}$$

It's useful then to consider the criterion (5.13)) in its matrix form,

$$\mathbf{c} \cdot \mathbf{M} \cdot \mathbf{c}^\dagger \geq 0, \ \forall c \in \mathbb{C}, \tag{5.15}$$

is equivalent to the hermitian matrix $\mathbf{M}$ being positive semi-definite; $\mathbf{M} \geq 0$. A hermitian matrix $\mathbf{M}$ is known to be positive semi-definite *iff* all its principal minors are non-negative [74]. The matrix elements of $\mathbf{M}$ are defined as,

$$M_{ij} = \left\langle \hat{a}^{\dagger q} \hat{a}^p \hat{a}^{\dagger n} \hat{a}^m \hat{b}^{\dagger l} \hat{b}^k \hat{b}^{\dagger r} \hat{b}^s \right\rangle, \tag{5.16}$$

where $i = (n, m, k, l)$, $j = (p, q, r, s)$ is the ith row and jth column respectively, and we use the following numbering rule for the multi-indices,

$$i < j \;\Leftrightarrow\; \begin{cases} |i| < |j| & \text{or} \\ |i| = |j| & \text{and } i <' j, \end{cases} \tag{5.17}$$

where we defined $|i| = n + m + k + l$ and $i <' j$ means that the first non-zero difference $r - k, s - l, p - n, q - m$ is positive.

Example Let us calculate a fourth-order criterion already derived in [73]. Deleting all lines and columns of the infinite matrix $\mathbf{M}$ except $i, j = 1, 5, 12$, we get the following principal minor S which must be non-negative for all separable states,

$$S = \begin{vmatrix} M_{11} & M_{15} & M_{1,12} \\ M_{51} & M_{55} & M_{5,12} \\ M_{12,1} & M_{12,5} & M_{12,12} \end{vmatrix} = \begin{vmatrix} 1 & \langle \hat{b}^\dagger \rangle & \langle \hat{a}\hat{b}^\dagger \rangle \\ \langle \hat{b} \rangle & \langle \hat{b}^\dagger \hat{b} \rangle & \langle \hat{a}\, \hat{b}^\dagger \hat{b} \rangle \\ \langle \hat{a}^\dagger \hat{b} \rangle & \langle \hat{a}^\dagger \hat{b}^\dagger \hat{b} \rangle & \langle \hat{a}^\dagger \hat{a}\, \hat{b}^\dagger \hat{b} \rangle \end{vmatrix} \geq 0. \tag{5.18}$$

Applying the criterion S on the following entangled coherent state,

$$|\psi\rangle_{AB} = N(\alpha, \beta)\ \left(|\alpha, \beta\rangle_{AB} - |-\alpha, -\beta\rangle_{AB}\right), \tag{5.19}$$

where $|\alpha\rangle_A, |\beta\rangle_B$ are coherent states, we find,

$$S = -|\alpha|^2 |\beta|^4 \frac{\coth\left(|\alpha|^2 + |\beta|^2\right)}{\sinh^2\left(|\alpha|^2 + |\beta|^2\right)} < 0, \quad \forall \alpha, \beta \neq 0, \tag{5.20}$$

detecting entanglement in the state for all non-zero amplitudes α, β, when the second order criterion of Simon fail to detect entanglement for any value of the amplitudes. Finally, Simon's second-order criterion is seen to correspond to the following principal minor of $\mathbf{M}$,

$$I_{\text{Simon}} = \begin{vmatrix} 1 & \langle \hat{a} \rangle & \langle \hat{a}^\dagger \rangle & \langle \hat{b}^\dagger \rangle & \langle \hat{b} \rangle \\ \langle \hat{a}^\dagger \rangle & \langle \hat{a}^\dagger \hat{a} \rangle & \langle \hat{a}^{\dagger 2} \rangle & \langle \hat{a}^\dagger\, \hat{b}^\dagger \rangle & \langle \hat{a}^\dagger \hat{b} \rangle \\ \langle \hat{a} \rangle & \langle \hat{a}^2 \rangle & \langle \hat{a}\hat{a}^\dagger \rangle & \langle \hat{a}\, \hat{b}^\dagger \rangle & \langle \hat{a}\, \hat{b} \rangle \\ \langle \hat{b} \rangle & \langle \hat{a}\, \hat{b} \rangle & \langle \hat{a}^\dagger \hat{b} \rangle & \langle \hat{b}^\dagger \hat{b} \rangle & \langle \hat{b}^2 \rangle \\ \langle \hat{b}^\dagger \rangle & \langle \hat{a}\, \hat{b}^\dagger \rangle & \langle \hat{a}^\dagger \hat{b}^\dagger \rangle & \langle \hat{b}^{\dagger 2} \rangle & \langle \hat{b}\hat{b}^\dagger \rangle \end{vmatrix} \geq 0, \tag{5.21}$$

which, for states in standard form (3.67), can be shown to be equivalent to Eq. (5.8),

$$\boldsymbol{\sigma}_{AB} + i\,(-\boldsymbol{\Omega}_A) \oplus \boldsymbol{\Omega}_B \geq 0. \tag{5.22}$$

5.3 Entanglement quantification

We have now come to one of the most important topics in quantum information, namely that of *entanglement measures.* The question that we want to explore is,

Can entanglement be quantified?

It's not even clear that such a question has a meaning after all. A state can surely be either entangled or separable, but in what sense may we say that one state is more entangled than the other? As for an example, consider the following entangled states; the maximally entangled singlet

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|10\rangle_{AB} - |01\rangle_{AB}\right), \tag{5.23}$$

and a non-maximally entangled state,

$$|\Psi\rangle_{AB} = \sqrt{(1-\epsilon)}\,|10\rangle_{AB} + \sqrt{\epsilon}\,|01\rangle_{AB}, \text{ with } \epsilon << 1. \tag{5.24}$$

They are both entangled, for every ϵ, so why should we consider $|\Psi\rangle_{AB}$ to be less entangled than $|\psi^-\rangle_{AB}$? Intuitively it would make sense to make such a distinction, as for $\epsilon \longrightarrow 0$ the correlations of the state $|\Psi\rangle_{AB} \approx |1\rangle_A \otimes |0\rangle_B$ are very close to those of a product (or, separable) state [75]. This is geometric argument shows that the "distance" of an entangled state from the set of separable states seems to provide a meaningful way to quantify entanglement. Also, we could consider tasks in quantum information for which entanglement is a resource, with separable states being useless, and argue that for such tasks the state $|\Psi\rangle_{AB}$ would be perform much worse than the singlet, as it's very close to a separable state.

We gave two simple example of two popular approaches in entanglement quantification: the axiomatic and the operational approach. The *operational approach* was initiated by Bennett *et al.* [76, 77] and it's based on how efficient an entangled state is for a given quantum information task of which entanglement is a necessary resource. Examples of such tasks are: the teleportation of quantum states, device-independent quantum key distribution, quantum secret sharing, quantum super-dense coding etc. In such tasks, Bell states, like the singlet (5.23), perform with maximum efficiency and for that reason they are called *maximally* entangled states. Entangled states like (5.24) or, more generally, entangled mixed states, do not perform as well due to their weaker correlations. For example, such non-maximally entangled states cannot perfectly teleport a quantum state, and cannot maximally violate Bell inequalities giving a reduced communication rate in quantum cryptography.

The realization that Bell states, like the singlet, provide with maximum performance in quantum information tasks, is the key ingredient for the operational quantification of entanglement in general states. As we have discussed, quantum entanglement cannot be created by LOCC; the latter can only conserve the entanglement or destroy it. The idea is then to use LOCC to convert a given bipartite quantum state $\hat{\rho}$ to a common currency, e.g. a singlet state that operates best in quantum information tasks. The amount of entanglement present in $\hat{\rho}_{AB}$ would then be expressed by the number of singlets one can extract from the state. One can have an implicit ordering in the amount of entanglement two different states $\hat{\rho}_1$ and $\hat{\rho}_2$ may have, by comparing the number of singlets one can extract from them. Examples of operational entanglement measures include:

Entanglement of distillation [77] It's defined as the ratio of the maximum number k_{max} of singlets that can be extracted from $n \to \infty$ copies of some bipartite state $\hat{\rho}_{AB}$ via the optimal LOCC procedure, to the number of copies n,

$$E_D\left(\hat{\rho}_{AB}\right) = \lim_{n\to\infty} \frac{k_{\max}}{n} = \sup_{\text{LOCC}} \lim_{n\to\infty} \frac{k}{n}, \tag{5.25}$$

where $\sup_{LOCC}$ denotes the maximization over all possible LOCC protocols that can achieve the desired distillation. The larger the $E_D\left(\hat{\rho}_{AB}\right)$ the more singlets can be distilled from $\hat{\rho}_{AB}^{\otimes n}$, and therefore the more entangled $\hat{\rho}_{AB}$ is considered to be. When $\hat{\rho}_{AB}$ is pure, $E_D\left(\hat{\rho}_{AB}\right)$ is equal to the *entropy of entanglement* defined as the von Neumann entropy $S\left(\hat{\rho}_A\right)$ of the reduced state of either the subsystems,

$$E_D\left(\hat{\rho}_{AB}\right) = S\left(\hat{\rho}_A\right) = S\left(\hat{\rho}_B\right), \tag{5.26}$$

where, $S\left(\hat{\rho}\right) = -\text{tr}[\hat{\rho}\log\hat{\rho}]$. The distillable entanglement vanishes for bound entangled states.

Entanglement cost [77] It's defined as the ratio of the least number k_{min} of singlets required to form n copies of the given state $\hat{\rho}_{AB}$ by using the optimal LOCC procedure, to the number of copies n,

$$E_C\left(\hat{\rho}_{AB}\right) = \lim_{n\to\infty} \frac{k_{\min}}{n} = \inf_{\text{LOCC}} \lim_{n\to\infty} \frac{k}{n}, \tag{5.27}$$

where $\inf_{\text{LOCC}}$ denotes the minimization over all possible LOCC protocols. Similarly, the larger the $E_C\left(\hat{\rho}_{AB}\right)$ the more singlets are required to form $\hat{\rho}_{AB}^{\otimes n}$, hence the more entangled $\hat{\rho}_{AB}$ is considered to be. This entanglement measure is also important in an operational sense, but, as the entanglement of distillation, it's very difficult to calculate due to the required optimization

over all LOCC protocols. In the case of pure states the equality between the two entanglement measures can be shown, $E_D(\hat{\rho}_{AB}) = E_C(\hat{\rho}_{AB}) = S(\hat{\rho}_A)$.
This is by no means an exhaustive list of the operational entanglement measures that can be found in the literature, and the reader is referred to the comprehensive review of Ref. [78] on the entanglement measures.

The *axiomatic approach* in entanglement quantification was initiated by Vedral *et al.* [75], and the idea is that any function of the quantum state that satisfies some basic intuitive postulates could be regarded as an entanglement measure. The most important of the postulates are:
i) *Monotonicity under LOCC*. As entanglement cannot be deterministically created by local operations and communication, consequently no entanglement measure should increase by LOCC. If we denote as Λ the map of an LOCC operation on the state, any entanglement measure $E[\hat{\rho}_{AB}]$ should satisfy

$$E\left[\Lambda\left(\hat{\rho}_{AB}\right)\right] \leq E\left[\hat{\rho}_{AB}\right]. \tag{5.28}$$

ii) *Vanishing on separable states*. By definition, separable states have no entanglement, hence any entanglement measure should equal a minimum constant C for all separable states,

$$\mathrm{E}\left[\hat{\rho}_{sep}\right] = C, \quad \forall \hat{\rho}_{sep}, \tag{5.29}$$

where it's natural to set $C = 0$.
A well-known entanglement measure belonging in this category is the *relative entropy of entanglement* [54], which utilizes a geometric distance in Hilbert space to measure the 'distance' of the state of interest to the set of separable states.

These two are the most basic postulates that all entanglement measures should satisfy. Additional postulates may be introduced, and for a more detailed overview see [54, 78]. Next, we will briefly analyse two entanglement measures, the *negativity* and the *Gaussian Rényi-2 entropy*, that will be of use to use in Chapter 9.

5.3.1 Negativity

The entanglement cost and the entanglement of distillation, that we previously discussed, though very important, are very difficult to be calculated analytically, due to the minimization/maximization condition over all LOCC operations. So, practically E_D and E_F as given by (5.25) and (5.27), respectively, are just formal expressions. The importance of having practical and computable entanglement measures led Vidal and Werner *et al.* to introduce the *negativity*

measure [79][80] (although, historically, this quantity was first used by Życzkowski *et al.* [81], and proven to be an entanglement monotone for the first time by Kim *et al.* [79]), which falls in the category of the axiomatic entanglement measures.

The negativity measure is based on the Peres-Horodecki PPT criterion; if a bipartite state $\hat{\rho}$ is entangled then the partially transposed state $\hat{\rho}^{T_B}$ may have negative eigenvalues, which we denote as $\{\lambda_i\}$. The negativity is then defined as,

$$N(\rho) = \left| \sum_i \lambda_i \right|, \quad \text{with} \quad \lambda_i < 0. \tag{5.30}$$

This expression is intuitive as the more entangled the state is, the further away it should be from a separable state (whose $\lambda_i = 0, \forall i$), and therefore the larger the $|\lambda_i|$ and, hence, the $N(\rho)$, would be. This measure is practical as the eigenvalues λ_i are easily calculable. Negativity can be shown to satisfy various desirable properties:

Properties of Negativity

- $N(\rho)$ *is an entanglement monotone*, i.e. it does not increase under *LOCC*,

$$N(\Lambda[\rho]) \leq N(\rho), \tag{5.31}$$

  where $\Lambda[\cdot]$ denotes an LOCC operation.

- $N(\rho)$ *vanishes for all separable states*; $N\left(\rho_{sep}\right) = 0, \ \forall \rho_{sep}$.

- $N(\rho)$ *provides an explicit lower bound on how close* ρ *can be taken, by means of LOCC, to the maximally entangled state* $\left|\varphi^+\right\rangle$ in terms of the singlet geometric distance.

- $N(\rho)$ *provides an upper bound to teleportation capacity*, i.e. the ability of ρ to faithfully teleport a quantum state.

- $N(\rho)$ *provides an upper bound to the entanglement of distillation* E_D, i.e.

$$E_D(\rho) \leq E_N(\rho), \tag{5.32}$$

  where the quantity

$$E_N(\rho) \equiv \log(1 + 2N(\rho)), \tag{5.33}$$

  is known as *logarithmic negativity*.

We see, that, *negativity* satisfies all the basic postulates that the axiomatic approach of entanglement measures imposes [75]. Moreover, it also has an operational meaning as it bounds the teleportation capacity and distillation rate. It's worth noting however that the negativity can vanish on some entangled states, namely bound entangled states.

5.3.2 Gaussian Renyi-2 entanglement

A particularly useful entanglement measure for CV states is the Gaussian Rényi-2 entanglement entropy [82]. This measure is based on the concept of Rényi-α entropies, as its name signifies, which are defined as

$$\mathcal{S}_\alpha(\hat{\rho}) = (1-\alpha)^{-1} \ln \mathrm{tr}\,(\hat{\rho}^\alpha)\,, \tag{5.34}$$

where $0 < \alpha < \infty$. The Rényi$-\alpha$ entropies are a family of additive entropies, whose interpretation is linked to thermodynamical quantities, and in particular related to derivatives of the free energy w.r.t. temperature [83]. Also, Rényi$-\alpha$ entropies have found applications on diverse topics such as the study of channel capacities [84, 85], work value of information [86, 87] and the entanglement spectra in many-body systems [88]. Any of the Rényi$-\alpha$ entropies (5.34) when applied on bipartite pure states $\hat{\rho}_{AB}$, and in particular on the reduced state $\hat{\rho}_A$ of one of the subsystems (say, A), can be shown to be entanglement monotones, for any α. As a special case, in the limit $\alpha \to 1$ Eq. (5.34) reduces to the von-Neumann entropy, which is indeed an entanglement monotone for bipartite pure states.

The entanglement measure we will consider here is based on the Rényi-2 entropy, for $\alpha = 2$ in Eq. (5.34),

$$\mathcal{S}_2(\hat{\rho}) = -\ln \mathrm{tr}(\hat{\rho}^2), \tag{5.35}$$

evaluated as said on the reduced state of one of the subsystems, proven to be an entanglement monotone for pure states. Considering arbitrary n-mode Gaussian states with CM $\boldsymbol{\sigma}$, by using Eq. (3.30) we can express the Rényi-2 entropy in terms of the state's CM,

$$\mathcal{S}_2(\hat{\rho}) = \frac{1}{2} \ln(\det \boldsymbol{\sigma}), \tag{5.36}$$

ranging from zero, for pure states ($\det \boldsymbol{\sigma} = 1$) and growing unboundedly with increasing mixedness of the state.

The Gaussian Rényi-2 entanglement monotone is then defined over all states, pure or mixed, by extending the Rényi-2 entropy via a Gaussian convex-roof procedure,

$$\mathcal{E}(\hat{\rho}_{AB}) = \inf_{\{p_i,|\psi_i\rangle\}} \sum_i p_i \, \mathcal{S}_2 \left(\mathrm{tr}_B |\psi_i\rangle_{AB}\langle\psi_i|\right), \tag{5.37}$$

where the minimization is over all Gaussian decompositions $\{p_i, |\psi_i\rangle_{AB}\}$ of the state $\hat{\rho}_{AB}$; i.e., $\hat{\rho}_{AB} = \sum_i p_i |\psi_i\rangle_{AB}\langle\psi_i|$. Intuitively, the involved optimization, dubbed Gaussian convex-roof, searches for all those possible ensembles of Gaussian states that can prepare our desired state $\hat{\rho}_{AB}$ with the least possible entanglement.

In Ref. [82] this entanglement measure was proven to satisfy a monogamy inequality for all n-mode Gaussian states $\hat{\rho}_{A_1A_2\ldots A_n}$,

$$\mathcal{E}(\hat{\rho}_{A_1:A_2\ldots A_n}) - \sum_{j=2}^{n} \mathcal{E}(\hat{\rho}_{A_1:A_j}) \geq 0, \tag{5.38}$$

where each A_j comprises of a single mode only, which poses fundamental restrictions on the distribution of entanglement among the modes.

6

Quantum teleportation

Quantum teleportation [7, 8, 10] is a remarkable application of quantum entanglement and a cornerstone of quantum information, simple enough to be taught in introductory-level quantum information courses, yet important enough to maintain a position at the forefront of contemporary research. In practical terms, teleportation is an indispensable tool for the transmission of quantum information. This stands as one of the pillars of a networked system, along with storage and processing. Schemes such as quantum repeaters [89] - pivotal for quantum communication over large distances - quantum gate teleportation [90] and measurement-based computing [91], all derive from the basic scheme of quantum teleportation. In the past two decades there has been significant experimental progress in the field of teleportation, on a variety of different systems [92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111]. An important class of these are continuous variable systems, which range from atomic ensembles to optical modes and beyond [112, 113].

6.1 Teleportation tutorial

In this section we will present the task of quantum teleportation in its archetypical form utilizing qubit systems [10] . Imagine two spatially separated parties, Alice and Bob. Alice is given an *unknown* quantum state $|\psi\rangle$ (e.g., could be the output of her quantum computer) and she wants to send it to Bob. What are their options?

Option (A): Physical transportation Why not do the *obvious*? Alice physically sends the quantum state to Bob through a quantum channel. This option would be viable only if the

physical system described by $|\psi\rangle$ is a photon due to its fast transmission. The drawback of this approach comes under the name of *decoherence*. An actual physical transportation of the quantum state through a lossy quantum channel, will unavoidably corrupt it due to the added noise. As a result, Bob will receive a noisy state. As the losses in fibres increase exponentially with the distance of the parties, we can safely conclude that this is not a viable option.

Option (B): Measure & Prepare Alice measures her single copy of $|\psi\rangle$ to get some information about which state it is, and she communicates the result to Bob. Bob then attempts to prepare Alice's unknown state based on the knowledge of her measurement. Such schemes are known as Measure & Prepare schemes and do not utilize any shared entanglement. The basic problem with this approach is that Alice has just a *single* copy of the state, therefore state tomography is not possible and the exact form of $|\psi\rangle$ cannot be known. Moreover, if $|\psi\rangle$ was a completely random state from the Hilbert space then a single measurement can give *no information* and this method would be useless. However, in most cases the input state is not completely random but belongs in an "alphabet", i.e. a *known* set of states $\{|\psi_i\rangle, p_i\}$ with $|\psi_i\rangle$ being given randomly to Alice with probability p_i. In such more restrictive scenarios, M&P strategies can partially reconstruct the unknown state, while they perform better the smaller the alphabet. In the next section, we will examine the performance of such schemes in more detail. For now it suffices to say that option (B) is in general *inferior* to the option we will discuss next.

Option (C): *Teleport it!* Let us now examine a more exotic and efficient way to send quantum states to distant parties which utilizes the magical property of entanglement. Before proceeding with the actual protocol, let us make some necessary remarks. A vital assumption of any teleportation scheme is that Alice and Bob, before attempting to implement the protocol, already share a known entangled pair of qubits described by the maximally entangled state,

$$\left|\phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right). \tag{6.1}$$

This entangled pair has nothing to do with the unknown state Alice wants to send to Bob; it could have been distributed to Alice and Bob in the past (perhaps, years ago) and was stored in their quantum memories (assuming such quantum memories were available). However, one may argue that the physical distribution of these entangled states to Alice and Bob are subject to decoherence, just like Option (A). What's the difference then? The difference is that there exist

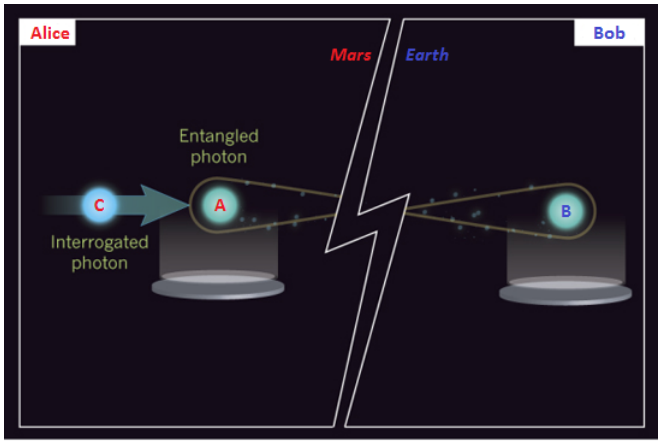

Figure 6.1: The setup for quantum teleportation is depicted. Alice and Bob, separated by an -in principle- arbitrarily large distance, share an entangled pair of qubits A and B (e.g. photons). Alice wants to teleport the unknown quantum state of her qubit C, to Bob's qubit B, by taking advantage of the shared entanglement.

schemes, known as *quantum repeaters* [89], that in principle can allow for known maximally entangled states to travel over long distances maintaining an arbitrarily high fidelity by utilizing error correction in intermediate nodes during their travel. On the other hand, Option (A) is not feasible, since there exist no similar scheme able to faithfully deliver an arbitrary unknown state over long distances. Let us now proceed with the teleportation protocol [10]:

Alice wants to send to Bob the unknown qubit state

$$|\psi\rangle_C = a\,|0\rangle + b\,|1\rangle\,, \tag{6.2}$$

where the amplitudes a, b are unknown. To accomplish that, she will utilize the shared entanglement with Bob as a resource to perform the teleportation protocol. The situation is depicted in Fig. 6.1.

6.1.1 Ideal qubit quantum teleportation

Let us examine the teleportation protocol for qubits in more detail:

Step 1 - Initial condition The initial joint quantum state of the three qubits involved is

$$\begin{aligned} |\psi\rangle_C \otimes \left|\varphi^+\right\rangle_{AB} &= (a|0\rangle_C + b|1\rangle_C) \otimes \frac{1}{\sqrt{2}}\,(|00\rangle_{AB} + |11\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}\,(a|000\rangle_{CAB} + a|011\rangle_{CAB} + b|100\rangle_{CAB} + b|111\rangle_{CAB})\,. \end{aligned} \tag{6.3}$$

Step 2 - Joint measurement Alice makes a joint measurement on her qubits C and A, in the so-called Bell basis comprised of the following states,

$$\left|\psi^{\pm}\right\rangle_{CA} = \frac{1}{\sqrt{2}}\left(|01\rangle_{CA} \pm |10\rangle_{CA}\right) \tag{6.4}$$

$$\left|\varphi^{\pm}\right\rangle_{CA} = \frac{1}{\sqrt{2}}\left(|00\rangle_{CA} \pm |11\rangle_{CA}\right). \tag{6.5}$$

In order to show how Alice's Bell measurement will affect the joint state (6.3), let us re-express the joint quantum state of qubits ABC w.r.t. that basis,

$$\begin{aligned} |\psi\rangle_C \otimes \left|\varphi^{+}\right\rangle_{AB} = &\frac{1}{2}\left|\varphi^{+}\right\rangle_{CA} \otimes |\psi\rangle_{\mathrm{B}} + \frac{1}{2}\left|\psi^{+}\right\rangle_{CA} \otimes (\hat{\sigma}_x|\psi\rangle_{\mathrm{B}}) \\ &+ \frac{1}{2}\left|\psi^{-}\right\rangle_{CA} \otimes \left(-i\hat{\sigma}_y|\psi\rangle_{\mathrm{B}}\right) + \frac{1}{2}\left|\varphi^{-}\right\rangle_{CA} \otimes (\hat{\sigma}_z|\psi\rangle_{\mathrm{B}}). \end{aligned} \tag{6.6}$$

When Alice performs the measurement on the basis $\left\{\left|\varphi^{\pm}\right\rangle_{CA}, \left|\psi^{\pm}\right\rangle_{CA}\right\}$, she will acquire one of four possible outcomes. As can be easily seen from (6.5), if Alice's result is $\left|\varphi^{+}\right\rangle_{CA}$, then Bob's qubit will be in the exact state $|\psi\rangle_{\mathrm{B}} = a|0\rangle_{\mathrm{B}} + b|1\rangle_{\mathrm{B}}$ Alice wanted to teleport! For the rest of the results, $\left|\varphi^{-}\right\rangle_{CA}$, $\left|\psi^{\pm}\right\rangle_{CA}$ Bob's state is *almost* what Alice wanted to teleport.

Step 3 - Classical communication In order for Bob to acquire the exact state, Alice classicalyy communicate to him the result of her measurement: $\varphi^{+}, \varphi^{-}, \psi^{-}$, or ψ^{+}.

Step 4 - Conditional operation Bob performs one of the following operations on his qubit B conditioned on Alice's measurement outcome,

$$\varphi^{+}: \quad \underbrace{\mathbb{I}}\cdot|\psi\rangle_{\mathrm{B}} = |\psi\rangle_{\mathrm{B}} \tag{6.7}$$

$$\psi^{+}: \quad \underbrace{\hat{\sigma}_x}\cdot(\hat{\sigma}_x|\psi\rangle_{\mathrm{B}}) = |\psi\rangle_{\mathrm{B}} \tag{6.8}$$

$$\psi^{-}: \quad \underbrace{\hat{\sigma}_y}\cdot\left(\hat{\sigma}_y|\psi\rangle_{\mathrm{B}}\right) = |\psi\rangle_{\mathrm{B}} \tag{6.9}$$

$$\varphi^{-}: \quad \underbrace{\hat{\sigma}_z}\cdot(\hat{\sigma}_z|\psi\rangle_{\mathrm{B}}) = |\psi\rangle_{\mathrm{B}}. \tag{6.10}$$

After Bob applying the required local operation the exact unknown state $|\psi\rangle$ is acquired. **Teleportation successful!**

6.1.2 Ideal CV quantum teleportation

The first proposal for a CV quantum teleportation was due to Vaidman [7], who considered the ideal case in which Alice and Bob share a CV maximally entangled state, with perfect correlations, to teleport an arbitrary single-mode CV state. Notice that when we deal with CV systems maximal entanglement is physically unattainable, in sharp contrast to DV systems, as it requires infinite energy. However, considering maximal entanglement as a limiting case that can be asymptotically attained by a finitely entangled state, Vaidman's proposal is very useful in providing us intuition on how CV teleportation works. The results of Vaidman were generalized later on to finite entangled states by Braunstein and Kimble [8].

It is most convenient to demonstrate Vaidman's CV teleportation protocol in the Heisenberg picture:

Step 1 - Initial condition Alice and Bob initially share two modes A and B of a maximally entangled EPR state, which can be attained by a two-mode squeezed state Eq. (3.53) in the limit of infinite squeezing, $r \to \infty$. The quadratures of the two modes are correlated such that

$$\hat{q}_A - \hat{q}_B = \hat{p}_A + \hat{p}_B = 0. \tag{6.11}$$

Alice's goal is to teleport to Bob an unknown input state described by an *input* mode with quadratures $\hat{q}_{in}, \hat{p}_{in}$

Step 2 - Joint measurement Alice then performs a joint measurement on the input mode and her entangled mode A. In particular, this joint measurement will actually be a so-called Bell measurement, comprised by subsequent operations:

(2a) Beam splitter mixing Alice mixes the two modes with a balanced 50 : 50 beam splitter, obtaining output modes " + " and " − " with corresponding quadratures,

$$\hat{q}_\pm = (\hat{q}_A \pm \hat{q}_{in})/\sqrt{2}, \quad \hat{p}_\pm = (\hat{p}_A \pm \hat{p}_{in})/\sqrt{2}. \tag{6.12}$$

(2b) Homodyne detection Alice makes a homodyne measurement (see Sec. 3.3.5, for details) the output quadratures $\hat{q}_-$ and $\hat{p}_+$, which is the mathematical equivalent of applying the

projectors $|q\rangle_-\langle q|$ and $|p\rangle_+\langle p|$ respectively. Denoting her outcomes as (q_-, p_+), her measurement causes $\hat{q}_- \to q_-$ and $\hat{p}_+ \to p_+$, therefore from Eq. (6.12) the quadratures of her mode A can be expressed as,

$$\hat{q}_A = \hat{q}_{in} + \sqrt{2}\, q_-\,, \quad \hat{p}_A = -\hat{p}_{in} + \sqrt{2}\, p_+. \tag{6.13}$$

Due to the perfect correlations that Bob shares with Alice, as seen in Eq. (6.11), Bob's quadratures are instantaneously projected as

$$\hat{q}_B = \hat{q}_{in} + \sqrt{2} q_-\,, \quad \hat{p}_B = \hat{p}_{in} - \sqrt{2}\, p_+. \tag{6.14}$$

Step 3 - Classical communication Up to this point, Bob is correlated to Alice's unknown input state, as seen in Eq. (6.14). However, he cannot retrieve Alice's state because of the unknown amplitudes (q_-, p_+) that are also involved in the correlations. Alice, therefore, classically communicates to Bob this pair of numbers (q_-, p_+).

Step 4 - Conditional displacement Bob uses the classical information (q_-, p_+) to perform a conditional displacement on his own mode B, which is the final step of the teleportation process,

$$\begin{aligned} \hat{q}_B &\longrightarrow \hat{q}'_B = \hat{q}_B - \sqrt{2}\, q_- = \hat{q}_{in}\,, \\ \hat{p}_B &\longrightarrow \hat{p}'_B = \hat{p}_B + \sqrt{2}\, p_+ = \hat{p}_{in}. \end{aligned} \tag{6.15}$$

Teleportation successful! As is seen in Eq. (6.15), Bob's final quadratures are equal to the ones of Alice's unknown input mode. This is equivalent as saying, that Bob's final state $\hat{\rho}_B$ is the same as the input unknown state of Alice $\hat{\rho}_{in}$.

6.2 Teleportation of Gaussian states

Now that we got familiar with the archetypical ideal protocols for quantum teleportation both for DV and CV systems, let us move on to the teleportation of CV states with finite entanglement. In particular, in this section we examine and compare two fundamentally different teleportation schemes for CV states; the well-known continuous variable scheme of Vaidman, Braunstein and Kimble (VBK), and a recently proposed hybrid scheme by Andersen and Ralph (AR). We analyze the teleportation of ensembles of arbitrary pure single-mode Gaussian states using these schemes and see how they fare against the optimal measure-and-prepare strategies – the benchmarks.

One product of the focus on quantum teleportation has been the development of teleportation benchmarks [114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124]. Put crudely, these benchmarks determine how good a teleportation-like procedure must be such that it could have been performed only with a shared entangled resource. Due to the relative difficulty of creating and maintaining long distance entanglement, these benchmarks are of practical interest as well as theoretical. For Gaussian states, which compose some of our most practical and popular continuous variable resources (as well as including the set of all 'classical' optical states [120]), general benchmarks for quantum teleportation have only very recently been derived [117].

To clarify further, it is necessary to first decompose a quantum teleportation system into its essential components and procedures as in Fig. 6.2. We initialize the system by providing the state to be teleported (input) and a "resource state". Subsequently, Alice performs a joint measurement on the input and her part of the resource state and communicates the result to Bob, who performs a local operation on his state conditioned upon this measurement. The resource state, or set of resource states, which carries the entanglement shared between the two systems is what we consider to be the quantum part of the protocol. The classical communication conducted after Alice's measurement is by comparison very cheap, and thus we consider classical resources to be free, as is customary in quantum information resource theory.

To measure how 'good' a teleportation is, for input and output states $|\psi\rangle_{\text{in}}$ and $\hat{\rho}_{\text{out}}$ respectively, we use the fidelity

$$\mathcal{F} = {}_{\text{in}}\langle\psi|\hat{\rho}_{\text{out}}|\psi\rangle_{\text{in}}, \tag{6.16}$$

for which $\mathcal{F} = 1$ indicates a perfect teleportation [125, 126]. A benchmark determines how large the average fidelity over a set of input states needs to be before it can be said with certainty that entanglement was necessary for the protocol used; that is, benchmarks set the limit on what a strategy can achieve using only local operations and classical communication. In a sense, we might say that a quantum teleportation procedure is not *truly* quantum unless it surpasses the optimal classical strategy in this regard: given some results from an unknown procedure, we can only definitively say that some entanglement was used if they exceed the benchmark.

Subsequently we employ benchmarks recently derived by Chiribella and Adesso [117] in order to assess different teleportation schemes for general sets of single-mode Gaussian state inputs. High-fidelity teleportation of Gaussian states is one essential ingredient for future realizations of quantum communication networks interfacing light and matter [127, 128, 129], yet no effective scheme has been devised so far (to the best of our knowledge) to teleport effectively ensembles of squeezed states with limited resources.

We analyze the original single-mode Gaussian-state teleportation scheme, derived by Vaidman [7], and Braunstein and Kimble [8] (VBK), in which a two-mode-squeezed vacuum state is used as the resource, and contrast this with a scheme recently introduced by Andersen and Ralph [9] (AR), where the quantum resource consists of N two-qubit Bell states.

We find that the VBK teleportation is actually inferior to the AR teleportation within a particular realistic and important parameter range. This persists even when improvements to the VBK scheme are considered, such as gain tuning [130] and the possible introduction of sources of non-Gaussianity into the scheme. For a small amount of 'resources' (to be quantified precisely in the following), the AR teleportation beats the VBK scheme in all considered variations, although in the presence of larger amounts of resources the advantage of the AR scheme fades away. Notably, the VBK scheme requires in excess of 10 dB of squeezing to exceed the benchmarks for teleportation of squeezed vacuum states without gain-tuning [117]. This value is teetering on the edge of the highest squeezing ever achieved in current optical experiments [131, 132], rendering untuned VBK teleportation incapable of beating the benchmarks even with state-of-the-art technology. Our analysis indicates that AR teleportation may provide a more viable candidate for this purpose. There is, however, an important catch. A crucial difference between the two protocols is that the AR scheme is *probabilistic*, while the original VBK protocol is *deterministic*, or 'unconditional' [94]. We dedicate ample discussion in the subsequent sections to address this point fairly.

6.3 Continuous variable quantum teleportation schemes

6.3.1 Vaidman-Braunstein-Kimble teleportation protocol

As before, we are considering two distant parties, Alice and Bob, who share a two-mode continuous variable entangled state $\hat{\rho}_{AB}$ (resource) of modes A and B respectively, where Alice wants to teleport an unknown quantum state $\hat{\rho}_{\text{in}}$ to Bob. The protocol Alice is going to use is a refined version of Vaidman's protocol (as described in Sec. 6.1.2) by Braunstein and Kimble, depicted in Fig. 6.3, which utilizes finitely entangled shared states $\hat{\rho}_{AB}$ and therefore manages only an approximate teleportation. The VBK protocol utilizes the same four steps described in Sec. 6.1.2, with a small modification in *Step 4*. In particular, for Vaidman's ideal protocol it's optimal for Bob to make a conditional displacement as in Eq. (6.15). However, for finite shared correlations, this displacement is no longer optimal and the refined VBK protocol allows for a

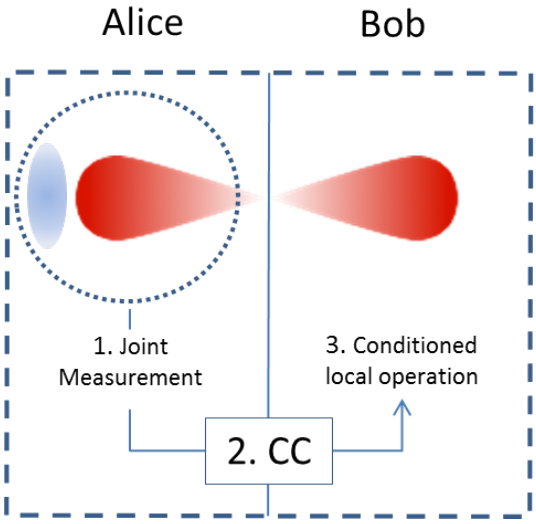

Figure 6.2: A conceptual diagram for a general teleportation scheme. The leftmost (blue) ellipse indicates the input state and the double cone (red) denotes the resource. The results of (1) a joint measurement, performed by Alice, are (2) classically communicated (CC) to Bob, who performs (3) a local operation conditioned on the measurement result of Alice, in order to recreate the input state using his part of the resource.

so-called *gain factor* g [130] in Bob's conditional displacements,

$$\begin{aligned} \hat{q}_B &\longrightarrow \hat{q}'_B = \hat{q}_B - g\sqrt{2}\, q_-, \\ \hat{p}_B &\longrightarrow \hat{p}'_B = \hat{p}_B + g\sqrt{2}\, p_+. \end{aligned} \tag{6.17}$$

that is chosen suitably, depending on the shared state $\hat{\rho}_{AB}$ in order to optimize the teleportation fidelity. As suspected, in the limit of infinite entanglement the optimal gain factor reduces to $g \to 1$, however the optimal value is $g \neq 1$ in general.

Bob's output $\hat{\rho}_{\text{out}}$ after the completion of the teleportation process is directly related to the entangled state $\hat{\rho}_{AB}$ and the input state $\hat{\rho}_{\text{in}}$. This relation has a simple expression in the characteristic function representation [133, 134],

$$\begin{aligned} \chi_{\text{out}}(\alpha) &= \text{Tr}\left[\hat{D}_{\text{out}}(-\alpha)\,\hat{\rho}_{\text{out}}\right] \\ &= \chi_{\text{in}}(g\,\alpha)\;\chi_{AB}(g\,\alpha^*, \alpha), \end{aligned} \tag{6.18}$$

where g is the gain factor of the protocol [130], $\hat{D}_k(\alpha) = \exp[\alpha \hat{a}_k^\dagger - \alpha^* \hat{a}_k]$ is the displacement operator acting on the mode k with annihilation operator $\hat{a}_k$, and

$$\chi_{\text{in}}(\alpha) = \text{Tr}\left[\hat{D}_{\text{in}}(-\alpha)\,\hat{\rho}_{\text{in}}\right], \tag{6.19}$$

$$\chi_{AB}(\alpha_1, \alpha_2) = \text{Tr}\left[\hat{D}_A(-\alpha_1)\,\hat{D}_B(-\alpha_2)\,\hat{\rho}_{AB}\right], \tag{6.20}$$

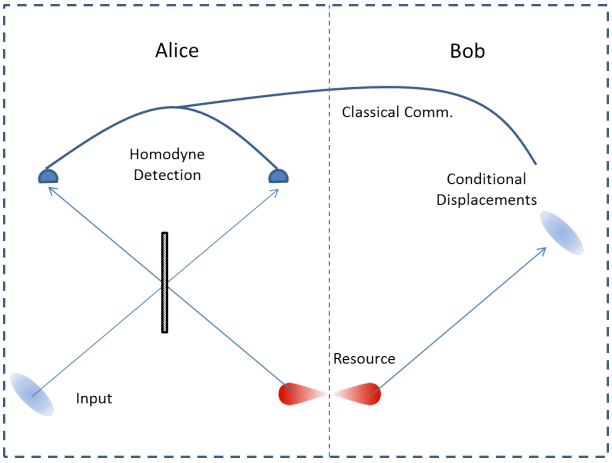

Figure 6.3: A schematic for the VBK teleportation scheme [7, 8]. The shared resource state is a two-mode entangled state.

are the characteristic functions of the input state and the two-mode entangled states respectively. The fidelity $\mathcal{F}$ [114] can be computed by the above formalism with a formula, which for pure input states takes the form

$$\begin{aligned}\mathcal{F}_{VBK} &= {}_{\text{in}}\langle\psi|\hat{\rho}_{\text{out}}|\psi\rangle_{\text{in}} \\ &= \frac{1}{\pi}\int d^2\alpha\, \chi_{\text{in}}(\alpha)\, \chi_{\text{out}}(-\alpha).\end{aligned} \tag{6.21}$$

By using Eq. (6.18) we can express the fidelity solely w.r.t. the characteristic functions of the input and resource states,

$$\mathcal{F}_{VBK} = \frac{1}{\pi}\int d^2\alpha\, \chi_{\text{in}}(\alpha)\, \chi_{\text{in}}(-g\,\alpha)\, \chi_{AB}(-g\,\alpha^*, -\alpha). \tag{6.22}$$

For resource states $\hat{\rho}_{AB}$ with finite entanglement, one has $\mathcal{F} < 1$ strictly. Thus, a major contrast of this protocol with teleportation of finite-dimensional systems is that, even in principle, a perfect fidelity cannot be achieved. Even worse, in practice, large amounts of entanglement cannot be achieved. In an attempt to overcome this difficulty, a new teleportation scheme has been recently proposed, which we will examine next.

6.3.2 Andersen-Ralph teleportation protocol

The idea of the Andersen and Ralph (AR) scheme [9], illustrated in Fig. 6.4, is to remove the need for a single resource state with large entanglement, replacing it by multiple ones with lesser entanglement. This is done by splitting the input state using an N-splitter network to

create N identical modes (preferably with a vanishing probability of having more than one mean photon per mode). In the coherent state basis this global beam-splitter transformation of the input state takes the following form,

$$\int d^2\alpha \, \langle \alpha \mid \psi \rangle_{in} \, |\alpha\rangle \rightarrow \int d^2\alpha \, \langle \alpha \mid \psi \rangle_{in} \, \left| \frac{\alpha}{\sqrt{N}} \right\rangle^{\otimes N}, \tag{6.23}$$

The N split inputs are then truncated into states of the form $c_0|0\rangle + c_1|1\rangle$ and can be separately teleported using N maximally entangled two-qubit Bell states:

$$|\phi\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|10\rangle_{AB} + |01\rangle_{AB} \right), \tag{6.24}$$

where $|0\rangle$ and $|1\rangle$ are the vacuum and one-photon states respectively. At the output, the N teleported modes are recombined in a similar beam-splitter network to produce the final output multiphoton state, which takes the form [9]

$$|\Psi\rangle_{\text{out}} = \frac{1}{\sqrt{P_{\text{suc}}(|\psi_{\text{in}}\rangle)}} \sum_{k=0}^{N} \langle k \mid \psi \rangle_{\text{in}} \left(\begin{array}{c} N \\ k \end{array} \right) \frac{k!}{N^k} \, |k\rangle_{\text{out}}, \tag{6.25}$$

where the input-state dependent normalization constant $P_{\text{suc}}(|\psi_{\text{in}}\rangle)$ is defined as

$$P_{\text{suc}}(|\psi_{\text{in}}\rangle) = \sum_{k=0}^{N} \left| \langle k \mid \psi \rangle_{\text{in}} \right|^2 \left(\begin{array}{c} N \\ k \end{array} \right)^2 \frac{k!^2}{N^{2k}}. \tag{6.26}$$

The quality of the teleportation process will be quantified by the fidelity, which is found to be

$$\mathcal{F}_{AR} = \left| {}_{\text{in}}\langle \psi \mid \Psi \rangle_{\text{out}} \right|^2 = \frac{1}{P_{\text{suc}}(|\psi_{\text{in}}\rangle)} \left| \sum_{k=0}^{N} \left(\begin{array}{c} N \\ k \end{array} \right) \frac{k!}{N^k} \left| \langle k \mid \psi \rangle_{\text{in}} \right|^2 \right|^2. \tag{6.27}$$

In principle, this protocol allows large amounts of shared entanglement to be exploited by dividing it amongst the N single-photon teleporters, removing the need for large two-mode squeezing as in the VBK protocol. However, the protocol is intrinsically *probabilistic*, in that occasionally no output will be registered, for two reasons. The first is the truncation procedure: if large photon-number terms exist with significant probability in the state $|\psi\rangle_{\text{in}}$ then projecting onto the $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ sector of the Fock space may have only a small chance of success. Secondly, to recombine the N teleported modes, we demand all the photons to exit only one port, i.e. we wish to measure $|0\rangle$ in each of the detectors of Fig. 6.4, while in any other case the protocol fails. The overall probability of success of the AR scheme is none other than the aforementioned normalization factor $P_{\text{suc}}(|\psi_{\text{in}}\rangle)$, Eq. (6.26). Finally, notice that probabilistic teleportation is acceptable for tasks such as entanglement distillation and quantum cryptography, the situation is clearly different for quantum communication where the input quantum information must be fully preserved.

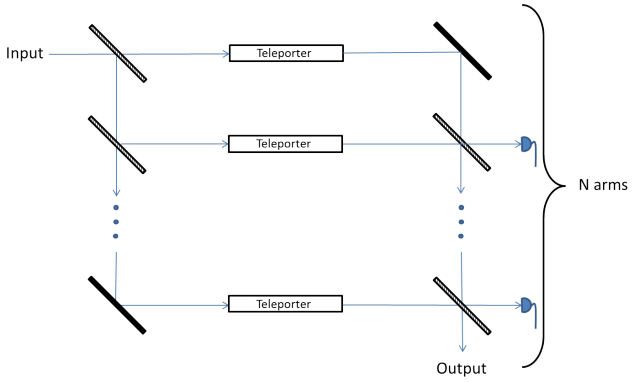

Figure 6.4: A schematic for the AR teleportation scheme [9]. The shared resources are N two-qubit Bell states. Each teleporter is a typical qubit teleporter as originally introduced in [10]. The dark solid rectangles at the (bottom-left and top-right) corners indicate mirrors, and the other striped ones indicate beam splitters.

6.3.3 Teleportation benchmarks

Benchmarks provide a fidelity threshold $\bar{\mathcal{F}}_c$, corresponding to the maximum average fidelity that can be achieved by classical measure and prepare schemes, without the two parties sharing any entangled resources, see e.g. [114]. We consider in general *probabilistic* measure and prepare strategies, according to which we restrict our output to when we have a successful measurement and entirely discard and ignore the outputs for when we do not. Expressing this mathematically, we have [117, 135]

$$\bar{\mathcal{F}}_c = \sum_{x\in X}\sum_{y\in Y_{\text{suc}}} p(x|suc)\frac{\langle\psi_x|\hat{\Pi}_y|\psi_x\rangle}{\sum_{y'\in Y_{\text{suc}}}\langle\psi_x|\hat{\Pi}_{y'}|\psi_x\rangle}\langle\psi_x|\hat{\rho}_y|\psi_x\rangle \tag{6.28}$$

Here, our measurement consists of the positive-operator-valued-measure elements $\{\hat{\Pi}_y\}$ and we discard all output results when $y \notin Y_{\text{suc}}$ where Y_{suc} constitutes the set of what we consider to be favourable outcomes. Additionally, $p(x|\text{suc})$ denotes the probability that, given a successful outcome, the input state was $|\psi_x\rangle$ and finally, the term $\langle\psi_x|\hat{\rho}_y|\psi_x\rangle$ represents the corresponding fidelity where we prepare the state $\hat{\rho}_y$ conditioned on an output y.

To derive benchmarks, it is necessary to define a prior probability distribution (henceforth *prior*), from which the input states to be teleported are drawn. This is also a realistic requirement (rather than always choosing a flat prior) since in a laboratory setting, constraints imposed by the apparatus, such as on the energy of producible states, will automatically impose a somehow nontrivial prior.

Estimating the best classical strategy is a hard problem, and only partial results were known for specific classes of input states (e.g. coherent states [120]). The general benchmark for teleporting arbitrary pure single-mode Gaussian states was only recently derived by Chiribella and Adesso [117]; the authors calculated the classical fidelity threshold for two classes of input single-mode states, namely undisplaced squeezed states, and general (displaced squeezed) pure Gaussian states.

6.3.3.1 Benchmark for arbitrary squeezed vacuum states

We consider an input ensemble containing squeezed states, introduced in Sec. 3.3.2.3,

$$|\xi\rangle = \hat{S}(\xi)|0\rangle, \tag{6.29}$$

where $\hat{S}(\xi) = \exp[-\frac{\xi}{2}\hat{a}^{\dagger 2} + \frac{\xi^*}{2}\hat{a}^2]$ is the single-mode squeezing operator and $\xi = s\,e^{i\varphi}$ is an arbitrary complex squeezing parameter. A state with complex squeezing ξ is drawn from the input ensemble according to the prior

$$p_\beta^S(s,\varphi) = \frac{1}{2\pi}\frac{\beta \sinh s}{(\cosh s)^{\beta+1}}, \tag{6.30}$$

where β^{-1} adjusts the width of the squeezing distribution, while the phase φ is uniformly distributed, yielding the $\frac{1}{2\pi}$ prefactor. For a given β, the classical fidelity threshold is found to be,

$$\bar{\mathcal{F}}_c^S(\beta) = \frac{1+\beta}{2+\beta}. \tag{6.31}$$

We see that even when Alice is completely ignorant about the squeezing of the state drawn, i.e. when $\beta \to 0$, the fidelity achieved without any entanglement is $\frac{1}{2}$ [117]. This is analogous to the benchmark for non-squeezed, coherent input states with totally unknown displacement [120].

6.3.3.2 Benchmark for general displaced squeezed Gaussian states

A general pure, single-mode Gaussian state can be represented as a displaced squeezed state, as introduced in Sec. 3.3.2.4,

$$|\alpha,\xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)|0\rangle, \tag{6.32}$$

where $\hat{D}(\alpha)$ is the displacement operator and $\hat{S}(\xi)$ the squeezing operator defined above. A state, with displacement amplitude α and complex squeezing ξ, is drawn from the input ensemble according to the probability distribution,

$$p^{G}_{\lambda,\beta}(\alpha, s, \varphi) = \frac{\lambda\beta}{2\pi^2} \frac{\sinh s}{(\cosh s)^{\beta+2}} e^{-\lambda|\alpha|^2 + \lambda \mathrm{Re}\left(e^{-i\varphi}\alpha^2\right)\tanh s}, \tag{6.33}$$

where β^{-1}, λ^{-1} adjust the widths of the squeezing and displacement distributions, respectively. Note that this distribution correctly reproduces the probability distribution (6.30) for squeezed-only states, $\int d^2\alpha \; p^{G}_{\lambda,\beta}(\alpha, s, \varphi) = p^{S}_{\beta}(s, \varphi)$. For given β, λ, the classical fidelity threshold for this ensemble is found to be,

$$\bar{\mathcal{F}}^{G}_{c}(\lambda, \beta) = \left(\frac{1+\lambda}{2+\lambda}\right)\left(\frac{1+\beta}{2+\beta}\right). \tag{6.34}$$

When Alice is completely ignorant of both the displacement and the squeezing of the state drawn, i.e. $\lambda \to 0$ and $\beta \to 0$, the best achievable fidelity without use of any entanglement is $\frac{1}{4}$ [117].

6.4 Comparison of the teleportation protocols: Quantifying resources

A vital topic to tackle for the understanding of this chapter, and to facilitate fair comparison of teleportation schemes in general, is how to quantify *resources*. For a quantum teleportation scheme, it is customary to consider the resource to be the entangled state shared. We have then some freedom on what property of the resource state to choose for quantification and comparison. For our purposes, we choose two quantifiers as resources: the mean energy and the entanglement degree of the shared entangled state, and we perform independent comparisons of different schemes for given values of each.

Henceforth, *entanglement* is synonymous with entropy of entanglement, defined for a pure resource state $\hat{\rho}_{AB} = |\phi\rangle_{AB}\langle\phi|$ as the von Neumann entropy,

$$S(\hat{\rho}_A) = -\mathrm{Tr}\left[\hat{\rho}_A \log_2 \hat{\rho}_A\right], \tag{6.35}$$

of the reduced state $\hat{\rho}_A = \mathrm{Tr}(\hat{\rho}_{AB})$. Additionally, *energy* is defined by the total mean photon number in the modes A and B,

$$E_\phi = \left\langle \hat{a}^{\dagger}_{A}\hat{a}_{A} \right\rangle + \left\langle \hat{a}^{\dagger}_{B}\hat{a}_{B} \right\rangle, \tag{6.36}$$

where $\hat{a}_{A,B}$ refers to the bosonic annihilation operator for mode A, B respectively.

These quantities are fairly straightforward to employ for comparing deterministic teleportation protocols; however, it is not immediately obvious how to compare probabilistic teleportations with differing success probabilities. In practice, furthermore, the resources truly utilized in any teleportation experiment are much more complicated than just these two quantities: everything from the energy used to power the equipment, to the manpower required to build it can be considered a resource if we wish to be omnicomprehensive in our definitions. While we certainly shall not explicitly consider these factors, they do implicitly impact in a very significant way to how we compare probabilistic teleportation schemes.

To this effect, we consider two possible interpretations for how we consider resources. The first interpretation counts the average resources required to achieve the teleportation of a state: we refer to this as the *naive picture*, since it only counts the units of energy or entanglement, with no other weighting. For example, a two-arm AR scheme with a 50% probability of success would require 2 runs of 2 ebits and thus use 4 ebits of entanglement per successful teleportation on average. However, this interpretation is not suitable for practical comparisons: it builds a false equivalence between, for example, one usage of a 4-arm AR interferometer and two usages of a 2-arm interferometer. In practice, a 4-arm interferometer would be comparatively much more costly to assemble. Similarly, 4 ebits in the VBK scheme correspond to 13.7 dB of entanglement, and the current experimental limit is about 10 dB [131, 132], whereas 2 ebits correspond to a value of 7.7 dB, which is fairly achievable; in this sense, two uses of a 2 ebit scheme are not comparable to one use of a 4 ebit scheme, in general, due primarily to the technological limitations of creating the extra entanglement.

We therefore adopt a *pragmatic picture*, whereby we attempt to account for the realistic limitations on teleportation schemes. To do this we first assume that producing the input states for teleportation is effectively free. As such, nothing important is lost on a failed teleportation attempt: this assumption is consistent with the formulation of the benchmarks, for which we freely discard states upon unsuccessful measurement outcomes. Indeed, even for deterministic schemes, thousands of (normally unaccounted for) independent runs are in practice repeated in the lab for a given input state, in order to perform state tomography on the output for experimental determination of the teleportation fidelity. In essence, building a teleportation setup is costly (in terms of acquiring a certain entanglement source, for instance), while running it repeatedly is assumed to be cheap in comparison. Furthermore, as we have been assuming all along, the classical communication required for teleportation is so cheap in comparison to

entanglement that it can be neglected in our quantitative comparison. For all of the above, in the pragmatic approach we choose to ultimately ignore the probability of success for a scheme (or equivalently the number of runs required to achieve a certain fidelity), and merely compare the number of ebits or units of energy (e.g. photons, phonons) utilized in individual runs, whether successful or not. While a fully objective comparison of different schemes is perhaps not possible in principle, we believe this approach is fair and sufficient.

With this point of view in mind, it can be shown [135] that a general (possibly probabilistic) *quantum* teleportation protocol yields an average fidelity over a certain input ensemble given by the formula

$$\bar{\mathcal{F}}_q = \sum_{x\in X}\sum_{y\in Y_{\text{suc}}} p(x|\text{suc})\frac{\langle\Psi_{x,r}|\hat{\Pi}_y|\Psi_{x,r}\rangle}{\sum_{y'\in Y_{\text{suc}}}\langle\Psi_{x,r}|\hat{\Pi}_{y'}|\Psi_{x,r}\rangle}\langle\psi_x|\hat{\rho}_y|\psi_x\rangle. \tag{6.37}$$

Note how this only differs from the equation for the classical benchmark (6.28) in that, in the quantum case, we do not consider a measurement directly upon the input state, but rather upon the joint state $|\Psi_{x,r}\rangle = |\psi_x\rangle \otimes |\phi_r\rangle$, where $|\phi_r\rangle \equiv |\phi\rangle_{AB}$ refers to the shared resource state.

To summarize, then, we simply define our resources by the value of entanglement (in ebits) or energy (in units) of $|\phi\rangle_{AB}$ irrespective of any other factor.

6.4.1 Resources for the AR scheme

In the case of the AR scheme, the natural choice for the resource states is given by the maximally entangled two-photon Bell states, e.g. $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|10\rangle_{AB} + |01\rangle_{AB})$, since with these states we can achieve perfect teleportation in the $\{|0\rangle, |1\rangle\}$ subspace [10]. As the von Neumann entropy of a Bell state amounts to 1 ebit, for an N-arm set up with N Bell states the total entanglement resource is given straightforwardly (exploiting additivity of the von Neumann entropy) by

$$S_{AR}\left(|\phi\rangle_{AB}\langle\phi|^{\otimes N}\right) = N \text{ ebits}. \tag{6.38}$$

Similarly, the energy of the resource states $|\phi\rangle_{\text{AR}}\langle\phi|^{\otimes N}$ is the sum of energies for each $|\phi\rangle_{AB}\langle\phi|$,

$$E_{\text{AR}}\left(|\phi\rangle_{AB}\langle\phi|^{\otimes N}\right) = N \text{ units}. \tag{6.39}$$

6.4.2 Resources for the VBK scheme

In the VBK scheme we will consider shared entangled states which belong to a general non-Gaussian class encompassing so-called 'squeezed Bell-like states', first studied by Dell'Anno

et al. [134],

$$|\phi_{SB}\rangle_{AB} = \hat{S}_{AB}(\zeta)\left[\cos\delta|0,0\rangle_{AB} + e^{i\theta}\sin\delta|1,1\rangle_{AB}\right], \tag{6.40}$$

where

$$\hat{S}_{AB}(\zeta) = \exp[-\zeta\hat{a}_A^\dagger\hat{a}_B^\dagger + \zeta^*\hat{a}_A\hat{a}_B] \tag{6.41}$$

is the two-mode squeezing operator with complex squeezing $\zeta = r\,e^{i\varphi}$ and $|n,m\rangle_{AB} = |n\rangle_A\otimes|m\rangle_B$ is a two-mode Fock state.

For $\delta = k\pi$ ($k \in \mathbb{Z}$) we get the well-known two-mode squeezed vacuum (TMSV) state,

$$\hat{S}_{AB}(\zeta)\,|0,0\rangle_{AB}, \tag{6.42}$$

with squeezing r, that is, the paradigmatic Gaussian entangled resource state. For other values of δ, we get non-Gaussian contributions, and we deem it interesting to investigate whether such non-Gaussianity provides an advantage over the use of conventional TMSV states [134, 136], under the terms of comparison defined above.

In the characteristic function representation the state $|\phi_{SB}\rangle_{AB}$ has the form

$$\chi_{SB}(\alpha_1,\alpha_2) = e^{-\frac{|\xi_1|^2+|\xi_2|^2}{2}}\Big[\sin\delta\cos\delta\left(e^{i\theta}\xi_1^*\xi_2^* + e^{-i\theta}\xi_1\xi_2\right) + \sin^2\delta\left(1-|\xi_1|^2\right)\left(1-|\xi_2|^2\right) + \cos^2\delta\Big], \tag{6.43}$$

where $\xi_i = \alpha_i\cosh r + \alpha_j e^{i\varphi}\sinh r$, $(i,\ j=1,\ 2;\ i\neq j)$.

The entanglement $S_{VBK}(r,\phi,\delta,\theta)$ of squeezed Bell-like states can be expressed as a rather long formula [134] which we omit here, limiting ourselves to note that it depends nontrivially on both the complex squeezing ζ and on the non-Gaussian mixing parameter δ and phase θ.

The mean energy of these states has a more concise form,

$$\begin{aligned} E_{\mathrm{VBK}}(r,\varphi,\delta,\theta) &= \left\langle\hat{a}_A^\dagger\hat{a}_A\right\rangle + \left\langle\hat{a}_B^\dagger\hat{a}_B\right\rangle \\ &= 2\sinh^2 r\left(1+\sin^2\delta\right) + 2\sin^2\delta\cosh^2 r - \sin 2\delta\,\sinh 2r\,\cos(\theta-\varphi)\,. \end{aligned} \tag{6.44}$$

6.5 Results

For accurate comparison to the benchmarks [117], we must consider states drawn from the general class of pure Gaussian states $|\alpha,\xi\rangle$ of Eq. (6.32) with probabilities given by the same priors $p^G_{\lambda,\beta}(\alpha,s,\varphi)$ or $p^S_\beta(s,\varphi)$ as used to derive the benchmarks.

We then find the average fidelity for general input states drawn from a prior characterized by widths λ^{-1} and β^{-1} for a scheme with resources (entanglement or energy) of value N to be

$$\bar{\mathcal{F}}_{\rm VBK}\,(\lambda,\,\beta,\,N) = \int d^2\alpha\, d\varphi\, ds\, p^G_{\lambda,\beta}\,(\alpha,s,\varphi)\,\mathcal{F}_{\rm VBK}\,(\alpha,s,\varphi;N)\,, \tag{6.45}$$

for the deterministic VBK scheme, and

$$\bar{\mathcal{F}}_{\rm AR}\,(\lambda,\,\beta,\,N) = \frac{\int d^2\alpha\, d\varphi\, ds\, p^G_{\lambda,\beta}\,(\alpha,s,\varphi)\,P_{\rm suc}\,(\alpha,s,\varphi)\,\mathcal{F}_{\rm AR}\,(\alpha,s,\varphi;N)}{\int d^2\alpha\, d\varphi\, ds\, p^G_{\lambda,\beta}\,(\alpha,s,\varphi)\,P_{\rm suc}\,(\alpha,s,\varphi)},$$

for the probabilistic AR scheme, in accordance with Eq. (6.37).

Both fidelities reduce to the mean fidelity for squeezed-only states upon setting $\alpha = 0$ and substituting the appropriate prior p^S_β in place of $p^G_{\lambda,\beta}$ (or, equivalently, taking the limit $\lambda \to \infty$ in the formulas above).

6.5.1 Comparison I: Fixed entanglement entropy

We will study three different cases, when

$$S_{\rm AR}\left(|\phi\rangle_{AB}\langle\phi|^{\otimes N}\right) = S_{\rm VBK}\,(r,\phi,\delta,\theta) = 2,\ 3,\ \text{and}\ 5\ \ \text{ebits}. \tag{6.46}$$

For the AR scheme, this simply corresponds to considering $N = 2,\ 3$ and 5 branches in the N-splitter, respectively. The teleportation fidelity of a general pure Gaussian input, $|\psi\rangle_{\rm in} = |\alpha,\,\xi\rangle$, using Eq. (6.27), is

$$\mathcal{F}_{\rm AR}\,(\alpha,\ s,\varphi;N) = \frac{1}{P_{\rm suc}}\left|\sum_{k=0}^{N}\left(\begin{array}{c} N \\ k \end{array}\right)\frac{k!}{N^k}|\langle k\mid\alpha,\,\xi\rangle|^2\right|^2, \tag{6.47}$$

which can then be substituted into Eq. (6.46) to find the mean fidelity.

For the VBK scheme, from Eq. (6.22), we see that the fidelity for teleporting a particular displaced squeezed state with characteristic function $\chi_{\alpha,s,\varphi}\,(\gamma)$, via a two-mode squeezed Bell-like shared state, $\chi_{SB}\,(\gamma_A,\gamma_B)$, is given by

$$\mathcal{F}_{\rm VBK}\,(\alpha,\ s,\varphi;\ \ r,\phi,\delta,\theta;\ \ g) = \frac{1}{\pi}\int d^2\gamma\ \chi_{\alpha,s,\varphi}\,(\gamma)\,\chi_{\alpha,s,\varphi}\,(-\gamma)\ \chi_{\rm SB}\,(-g\,\gamma^*,-\gamma)\,. \tag{6.48}$$

This formula can be analytically evaluated for non-unit gain g, but the explicit expression is too long and cumbersome to be reported here.

Given the dependence of $S_{\rm VBK}\,(r,\phi,\delta,\theta)$ on four different parameters, there is a manifold of states associated with any fixed value of entanglement, which can be found by numerically

solving for each case of $N = 2,\ 3,\ 5$ ebits. The optimal resource and best strategy can then obtained by optimizing the average fidelity, Eq. (6.45), over the set of resource states with a given entanglement constraint $S = N$, and additionally optimizing over the gain $0 \leq g \leq 1$. This results in the optimal VBK average fidelity $\bar{\mathcal{F}}^{\text{opt}}_{\text{VBK}}(\lambda, \beta,\ N)$ given N ebits of entanglement available in the form of squeezed Bell-like states.

In what follows, we compare the average fidelities of the two teleportation schemes, $\bar{\mathcal{F}}_{\text{AR}}(\lambda, \beta, N)$ and $\bar{\mathcal{F}}^{opt}_{\text{VBK}}(\lambda, \beta,\ N)$, as we vary the prior distribution parameters λ and β.

6.5.1.1 Results for squeezed states

We begin by comparing the averaged fidelities $\bar{\mathcal{F}}_{\text{AR}}$ and $\bar{\mathcal{F}}_{\text{VBK}}$ as well as the corresponding benchmark $\bar{\mathcal{F}}^{S}_{c}$, for the case of teleporting squeezed states with zero displacement.

The first important result is depicted in Fig. 6.5a, where we set the entanglement resource value at $S = N = 2$ ebits, for various values of β. The AR scheme manages to always beat the benchmark for every β, in sharp contrast to the VBK scheme, even for $\beta \to 0$. In this limit, which corresponds to completely unknown squeezing, the VBK teleportation scheme achieves negligible average fidelity, while both the AR scheme and the benchmark tend to finite values, $\bar{\mathcal{F}}_{\text{AR}} \to 0.58$ and $\bar{\mathcal{F}}^{S}_{c} \to 0.5$ respectively. Even taking into account gain tuning, the optimized VBK scheme can just barely surpass the benchmark at large values β, does not look especially robust against possible experimental deficiencies. A conclusive experimental demonstration of quantum teleportation of an ensemble of squeezed states (with unknown squeezing) achieving fidelities superior to what is classically possible has yet to be achieved, and the present results indicate that the AR scheme may be a more viable candidate for this than the VBK scheme. The fact that only two branches are needed for such a demonstration, makes the scheme experimentally appealing with current technology. Clearly, the probabilistic nature of the AR scheme is a major factor behind its enhanced performance; such a scheme is indeed more likely to reject states which cannot be faithfully transmitted (i.e. high energy input states), and thus it compares favourably to the benchmark even in the limit $\beta \to 0$. The VBK scheme on the other hand teleports the high energy states with vanishing fidelity, reducing the average fidelity to zero for very broad ensembles.

As we increase the entanglement entropy of the shared resource states to $S = 3$ ebits, see Fig. 6.5b, we find that the AR scheme is still superior, but now the VBK scheme clearly violates the benchmark for input ensembles of inverse width $\beta \geq 1.58$. For even greater entanglement of $S = 5$ ebits, Fig. 6.5c, the VBK scheme manages to attain comparable performances to

the AR one at large enough β, while the limit $\beta \to 0$ remains problematic. This level of shared resources is, however, unrealistic: state-of-the-art technologies achieve 10 dB of optical squeezing [131, 132] which is equivalent to only 2.77 ebits of entanglement.

Another interesting result has to do with the performance of the squeezed Bell-like resource states for the VBK scheme. In [134, 136], Dell'Anno *et al.* showed that, at fixed squeezing degree r, non-Gaussian squeezed Bell-like states (i.e., with $\delta \neq 0$) resulted in significant advantage in the teleportation fidelity of single coherent or squeezed states, compared to just using the corresponding Gaussian TMSV with the same r (given by $\delta = 0$). The authors thus concluded that non-Gaussianity in the resource state can significantly improve teleportation performance.

Our results show, however, that such a conclusion is strongly dependent on the terms of comparison. When making the comparison at fixed entanglement entropy, rather than at fixed squeezing degree, we found in all considered cases that, within the general squeezed Bell-like class, the optimal resource state for teleportation of input ensembles of Gaussian states via the gain-optimized VBK scheme actually *does* always reduce to the TMSV. In this respect, therefore, non-Gaussianity is not advantageous for the considered task. One may contend that the advantage observed by Dell'Anno *et al.* was more properly a consequence of the extra entanglement present in the resource (compared to the TMSV at fixed r) and not traceable directly to the non-Gaussian nature of the employed states.

6.5.1.2 Results for general displaced squeezed states

We will now discuss the results for the most general set of pure single-mode Gaussian input states, namely the displaced, squeezed vacuum states. In Fig. 6.6a we report the case of $S = 2$ ebits of shared entanglement. As in the previous case of squeezed-only states, the AR scheme beats the benchmark for all values of the parameters β, λ. On the other hand, it no longer stands so dominant over the VBK scheme; while for small β and large λ the AR scheme is still superior, as we increase β and reduce λ the optimized VBK scheme manages to achieve the best fidelity overall. This relates to the well-known result that the VBK scheme is exceptionally good, by construction, at teleporting displaced states (and in fact, despite being deterministic, always beats the benchmark for teleporting coherent states [120, 137]). As we increase the shared entanglement to $S = 3$ ebits, we see in Fig. 6.6b that the dominance of the AR scheme gets confined to the region of larger λ and smaller β, while for the instance of even larger

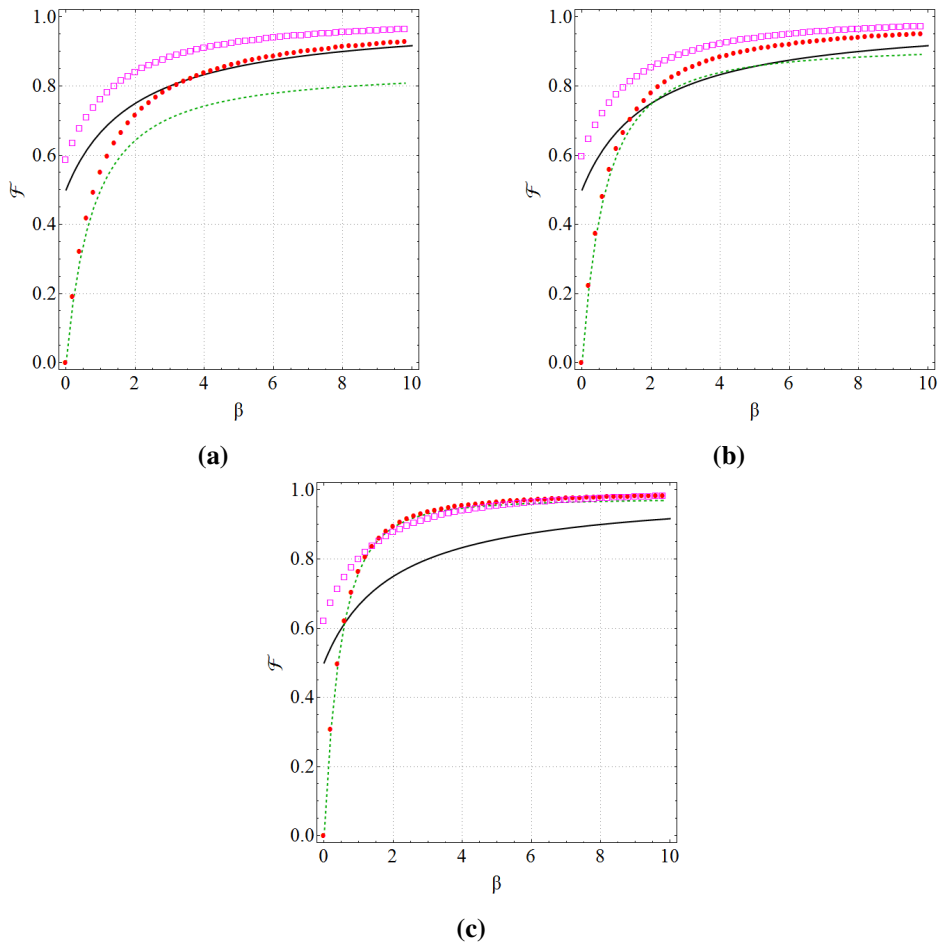

Figure 6.5: Average fidelity of teleportation $\bar{\mathcal{F}}$ for the input set of single-mode squeezed states with prior p^S_β, plotted as a function of the inverse width β, for different amounts of shared entanglement: (a) $S = 2$ ebits, (b) $S = 3$ ebits and (c) $S = 5$ ebits. The comparison is between the AR scheme (magenta open squares), the VBK scheme optimized over all squeezed Bell-like resource states with unit gain (green dashed curve), the gain-tuned VBK scheme optimized over all squeezed Bell-like resource states, amounting to the gain-tuned VBK scheme using TMSV resource states (red filled circles), and the benchmark (black solid line).

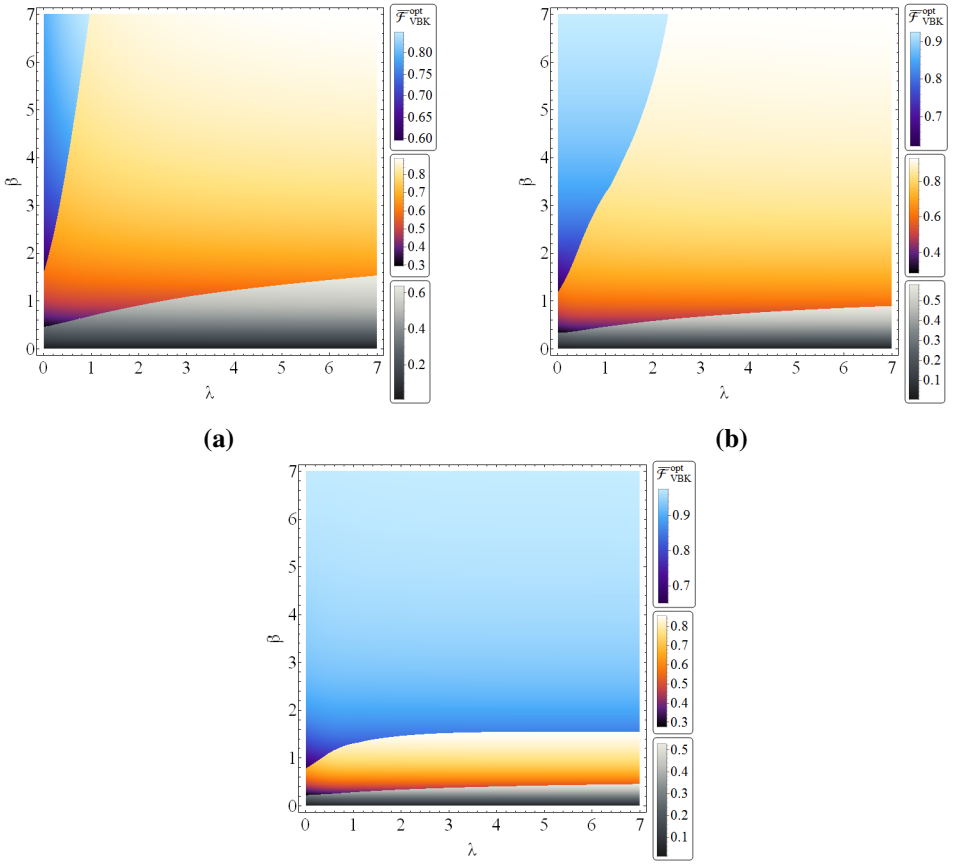

Figure 6.6: Contour plots of the average teleportation fidelity $\bar{\mathcal{F}}^{\text{opt}}_{\text{VBK}}$ for the input set of arbitrary displaced squeezed Gaussian states $|\alpha, \xi\rangle$ distributed according to the prior $p^{G}_{\lambda,\beta}$, for the gain-optimized VBK scheme, as a function of the inverse widths λ, β, at different fixed amounts of shared entanglement: (a) $S = 2$ ebits, (b) $S = 3$ ebits and (c) $S = 5$ ebits. From top-left to bottom-right, the three shaded areas in each figure denote, respectively, the region where the VBK scheme has superior performance compared to both the AR scheme and the benchmark (sea colors), the region where the VBK scheme is inferior to the AR one but still beats the benchmark (solar colors) and the region where the VBK protocol yields a fidelity below the benchmark (grayscale colors). The average fidelity of the AR protocol (not depicted) is found to always beat the benchmark for every value of the parameters λ, β.

entanglement, $S = 5$ ebits of Fig. 6.6a, the VBK protocol wins the comparison in almost the whole parameter region except for small β.

As in the previous subsection, we found again that non-Gaussianity in the shared squeezed Bell-like states yields no advantage in the VBK average teleportation fidelity over the conventional use of TMSV resources. Even in the present more general case of displaced squeezed input states, the fidelity depicted in Fig. 6.6 corresponds in fact to the optimal choice given by the use of a TMSV resource state.

6.5.2 Comparison II: Fixed mean energy

In this section we will compare the two schemes by constraining the energy of their resource states, i.e. by keeping fixed the mean photon number at $E = N = 2,\ 3,\ 5$ units, instead of the entanglement entropy which we considered previously.

As previously observed, the energy used in the AR scheme, $E_{\mathrm{AR}}\left(|\phi\rangle_{AB}\langle\phi|^{\otimes N}\right) = N$ units, is determined by the number of branches in exactly the same way as the entanglement entropy is: each branch corresponds to one ebit of entanglement and one unit of energy. Thus the fidelity of the scheme will still be given by (6.46), and the performance of the scheme is the same as for the fixed entanglement case.

For the VBK scheme, however, the mean energy has a different dependence on the resource state parameters; to identify the optimal resources in the manifold of squeezed Bell-like states with fixed energy, we have thus performed a similar numerical optimization as what done before for the case of fixed entanglement.

6.5.2.1 Results for squeezed states

The teleportation of squeezed states at fixed energy yielded the same results on the optimality of the entangled resources $|\phi_{SB}\rangle_{AB}$ of the VBK scheme: the optimal resource state turns out to be the TMSV over the whole parameter range, yielding no non-Gaussian advantage. This observation enables us to make a neat comparison to the fixed entanglement case. In Fig. 6.7 we show the dependence of the entanglement entropy on the mean energy, for the optimal TMSV resource state; the points corresponding to $S = 2, 3, 5$ ebits are marked explicitly. As we see, the energies $E_{\mathrm{VBK}} = 2, 3, 5$ units that we consider, correspond to entanglement entropies $1.8 \leq S \leq 2.5$ ebits for the TMSV state. Hence, the performances of the VBK protocol will be similar to the ones shown in Figs. 6.5a, 6.5b, which correspond to $S = 2, 3$ ebits respectively;

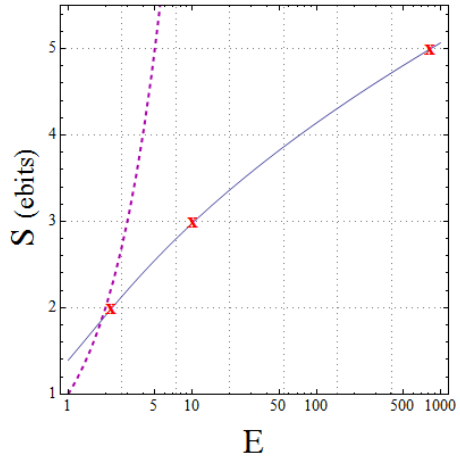

Figure 6.7: The dependence of the entanglement entropy S of the resource states as a function of their mean energy E, plotted for: (a) the multiple Bell resource states for the AR scheme (dashed line) and (b) the optimal TMSV resource states for the VBK scheme. For the latter, the points that correspond to $S = 2, 3, 5$ ebits are marked with crosses to show explicitly the need for large energies (notice the log-linear scale).

the VBK scheme is thus expected to be always inferior compared to the AR scheme within this range of parameters.

We can see from Fig. 6.7 that an entanglement entropy of $S = 5$ ebits corresponds instead to the massive mean photon number of about 833 units for the TMSV used in the optimal VBK scheme. On the other hand, the AR scheme achieves the same entanglement with only 5 photons and this dramatic difference is illustrated in the same figure. In fact, the AR scheme is so superior when considering energy as the resource, that even if we chose to follow the *naive* interpretation described in Sec. 6.4 and counted the photons expended in the failed teleportation attempts, we would still find that a 5-arm scheme utilizes much less than 833 photons as long as $\beta > 1$, which would yield and endured dominance of the AR scheme over the VBK under these terms of comparison.

6.5.2.2 Results for general displaced squeezed states

We confirm once more the TMSV to be the optimal resource state for the VBK scheme, under the fixed energy constraint, when teleporting the general Gaussian set of displaced squeezed states. Adding this to the previous results, we have shown that under the restrictions of fixed energy or fixed entanglement, any non-Gaussianity within the class of squeezed Bell-like states

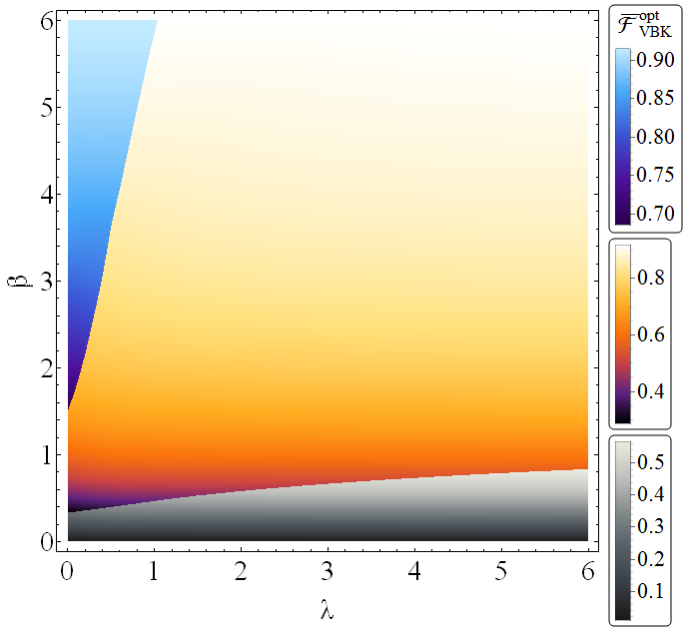

Figure 6.8: Contour plot of the average teleportation fidelity $\bar{\mathcal{F}}^{\text{opt}}_{\text{VBK}}$ for the input set of arbitrary displaced squeezed Gaussian states $|\alpha, \xi\rangle$ distributed according to the prior $p^{G}_{\lambda,\beta}$, for the gain-optimized VBK scheme, as a function of the inverse widths λ, β, at fixed mean energy of the resource states, $E = 5$ units. As in Fig. 6.6, from top-left to bottom-right, the three shaded areas in each figure denote, respectively, the region where the VBK scheme has superior performance compared to both the AR scheme and the benchmark (sea colors), the region where the VBK scheme is inferior to the AR one but still beats the benchmark (solar colors) and the region where the VBK protocol yields a fidelity below the benchmark (grayscale colors). The average fidelity of the AR protocol (not depicted) is found to always beat the benchmark for every value of the parameters λ, β.

will not give any advantage in the optimized VBK continuous variable teleportation of single-mode Gaussian states. We discussed above the relation between entanglement and energy for the optimal TMSV and showed that, for an energy of $E = 5$ units, its entanglement is about 2.5 ebits smaller than the corresponding entanglement of the resource states used in the AR scheme at the same energy. Despite this fact however, as we see in Fig. 6.8, the VBK scheme still manages to beat the AR (and the benchmarks) for small enough values of λ, β. This shows that the AR scheme is still unable to handle broad distributions, i.e. high energy inputs, when its number of branches N is not big enough. For smaller energies $E = 2, 3$ units, the comparative performance of the schemes is similar to Fig. 6.6a since at these energies the corresponding entanglement entropy is around 2 ebits for both schemes.

6.6 Discussion and conclusion

We have compared the Vaidman, Braunstein and Kimble (VBK) continuous variable quantum teleportation protocol [7, 8], to the recently proposed hybrid teleportation protocol of Andersen and Ralph [9], and to the teleportation benchmarks for general Gaussian states recently derived by Chiribella and Adesso [117]. We considered two classes of input single-mode ensembles, comprised of squeezed-only states and arbitrary displaced squeezed states respectively.

For the VBK protocol, non-Gaussian two-mode resources (squeezed Bell-like states [134]) were considered as shared resources and optimizations were performed in order to examine any possible advantage due to non-Gaussianity of the resources for the average teleportation fidelity. In [134, 136], it was found that, under fixed squeezing of the resource state, the presence of non-Gaussianity gave significant advantage for teleportation of displaced squeezed states. These results generalized previous findings when particular non-Gaussian states such as photon-subtracted states, which are a subclass of the squeezed Bell-like states, were analyzed [138, 139, 140, 141].

Motivated by a closer consideration of the resources involved in teleportation protocols, we adopted different terms of comparison. We compared the performance of the various schemes either at fixed entanglement entropy, or at fixed mean energy, of the shared resource states. Under these premises, we found in all considered cases that non-Gaussianity is arguably of no advantage at all: the optimal resources with a fixed entanglement or energy were consistently found to be conventional Gaussian two-mode squeezed vacuum states when the VBK teleportation protocol was considered, taking into account gain optimization [130].

In the case of squeezed input states, we have shown that using only minimal resources, i.e. just 2 ebits of shared entanglement between the two parties, the AR scheme can successfully beat the benchmark in teleporting squeezed states while the VBK scheme, even when gain-optimized, cannot do so in a relevant parameter range. The current technological limitations prevent us from attaining optical squeezing larger than about 10 dB [131, 132], corresponding to a maximum of $S \approx 2.77$ ebits for the VBK scheme. Even with this maximum amount of shared entanglement, the VBK scheme is unable to beat the benchmark without gain-tuning (see Fig. 6.5b) while, when gain-optimized, although it surpasses the benchmark, it still yields an inferior performance to the one of the AR scheme. The case of the fixed energy condition was even less favourable for the VBK scheme, since restricting the number of photons in the two-mode squeezed vacuum to low numbers greatly limits the performance of the scheme. On the other hand, the AR scheme remains as much efficient for low energies since the entanglement is densely distributed over the entangled photons of the resource states, as seen in Fig. 6.7.

In the case of general Gaussian input states, we saw that the AR scheme always beats the benchmark for all values of parameters β, λ of the input ensemble, while the VBK scheme is the most efficient only in teleporting coherent states (i.e. $\lambda \to 0$ and large β). For low resources, e.g. $S = 2, 3$ ebits, the AR scheme was found to perform best in teleporting broad ensembles in squeezing because of its sensitivity to the input states, beating on average the insensitive VBK scheme and the classical benchmark. However, as we reach up to $S = 5$ ebits of shared entanglement, the gain-optimized VBK scheme completely dominates AR over almost all the examined region in the teleportation of general Gaussian states except for the region that corresponds to $\beta \to 0$. We should note however that this amount of entanglement is not achievable with current technology.

While the VBK scheme has traditionally been praised for its deterministic nature, which gained its historic status of an *unconditional* teleportation protocol (as opposed to the initial experimental realisations of discrete-variable teleportation [93] which relied heavily on post-selection), in this case it is this feature which appears to set it at a disadvantage. It may be thus interesting to consider probabilistic alterations to the VBK scheme to see if some advantage can be recaptured. Preliminary calculations on simple conditioning strategies, such as discarding teleportation runs when Alice's quadrature measurements result in outcomes larger than a set threshold, show a minimal improvement over the deterministic VBK scheme. It thus appears that the advantage of the AR scheme does not just stem trivially from its probabilistic nature.

Regardless, we dedicated considerable attention to the issue of establishing fair conditions for comparing probabilistic and deterministic schemes for teleportation of an input ensemble; we expect such a discussion to generate further independent interest in the matter.

Our analysis reveals how hybrid approaches to continuous variable quantum technology can be particularly promising with limited resources. In the case of teleportation, splitting an ensemble of Gaussian states into as few as two or three single-photon channels and performing qubit-like parallel teleportation appears effectively more efficient, even taking into account properly the nonunit probability of success, than realizing an unconditional continuous variable teleporter consuming as much entanglement. Interestingly, a complementary hybrid approach has also very recently been demonstrated by Furusawa and coworkers, who performed deterministic teleportation of a single-photon state by a VBK implementation [142]. Other schemes for the near-deterministic teleportation of hybrid qubits have also been devised [143]. For a review on hybrid quantum optical communication see e.g. [144].

We note that the analysis in the present chapter has focused on ideal teleportation regimes. In a real experiment, both considered schemes will be affected by unavoidable losses and imperfections, perhaps the most important ones being the noisy production of the entangled resources. In any realistic implementation, the resource states would indeed be most typically mixed nonmaximally entangled two-qubit states for the AR case, and two-mode squeezed thermal states for the VBK case. One can then still issue comparisons at fixed entanglement degree (using e.g. the entanglement of formation) or energy, at comparable levels of state purity mirroring the current experimental facilities. These are expected to lead to the same qualitative hierarchy between the two schemes as in the case of pure resource states. Additional sources of imperfections can be considered, like lossy transmission channels in both schemes, the non-unit efficiency of the homodyne detection in the VBK scheme, the dark counts and finite detection efficiency of single-photon detectors during the Bell measurement in the AR case, etc. In this respect, the efficiency of the Bell measurement in the AR scheme is typically much lower than the efficiency of homodyne detections in optical implementations of VBK teleportation. However, this effect is typically absorbed into a lower probability of success for the AR scheme, without impacting significantly on the teleportation fidelity. Therefore, once more, we do not expect significant changes in the comparison between the two schemes and the benchmarks from the point of view of the ensemble fidelity. In short, the analyzed schemes are expected to be quite robust to common sources of imperfection. Nonetheless, we plan to

complement the present investigation of the ideal regime with a forthcoming work, where all such realistic corrections will be taken into account in detail.

To our knowledge, an experiment that verifies unequivocally the use of quantum entanglement during a quantum teleportation protocol, by violating the corresponding fidelity benchmark, has yet to be performed for an ensemble of input squeezed Gaussian states with unknown squeezing (in [110] the input states had unknown displacement but known squeezing). In this chapter we found that the hybrid AR scheme appears to be a good candidate for such a first demonstration. With the necessary technology readily available, it would be of great interest to accomplish such an experiment in the near future. In parallel, we hope this work can stimulate further research into the definition of a possibly refined teleportation protocol tailored to displaced squeezed input states, able to beat both the benchmarks and the AR scheme studied here, while being ideally endowed with an improved probability of success under realistic conditions.

Part III

Einstein-Podolsky-Rosen steering

7

Steering and the EPR paradox

7.1 The Einstein-Podolsky-Rosen paradox

Entanglement is the holy grail of quantum theory, with spectacular implications both for the foundations of the theory, and for real-world applications; including, quantum- computing, communication, cryptography, sensing, etc. In the early years of quantum theory and up to its complete establishment by 1930, however, entanglement still went unnoticed. Einstein, Podolsky and Rosen (EPR) were the first to recognize the counter intuitive features of entanglement, which seemed to involve some sort of "nonlocality" among separated and causally disconnected systems. In 1935, the EPR trio published a paper on the topic [55] where they utilized a continuous variable (CV) entangled state of the form (3.54),

$$|\psi\rangle_{\text{EPR}} \sim \delta(\hat{q}_A - \hat{q}_B)\,\delta(\hat{p}_A + \hat{p}_B), \tag{7.1}$$

to argue -not that entanglement can be useful due to the strong correlations it invokes, but- that entanglement is proof quantum theory must be *incomplete*, and the EPR argument has been known as *the EPR paradox*. Let us examine their argument in more detail.

The utilized EPR state (7.1) is a (in the limit) maximally entangled CV state, which can be experimentally prepared by using a two-mode squeezed state (3.53) and taking the limit of infinite squeezing, $r \longrightarrow \infty$. To have a concrete example in mind, imagine that Alice and Bob have prepared such a state using the photonic field, both holding modes A and B respectively, with $\hat{q}_i, \hat{p}_i$ being their corresponding quadratures which are observables related to the electric and magnetic field operators of their modes. In this limit, and as depicted in (7.1), $|\psi\rangle_{\text{EPR}}$ becomes an exact eigenstate of the observables $\hat{q}_A - \hat{q}_B$ and $\hat{p}_A + \hat{p}_B$ (corresponding to zero

eigenvalue), implying that the individual measurement outcomes of Alice and Bob are exactly (anti-)correlated,

$$q_A = q_B\,, \quad p_A = -p_B. \tag{7.2}$$

And here is the 'paradox': According to EPR, if quantum theory -and, therefore, the quantum state- were to be a complete description of nature it would imply that the local quantum state of one party (say, Bob) is independent of the actions of the other distant, and causally disconnected, party Alice. This notion of independence of causally disconnected systems, is known in more modern terms as *local causality* (due to Bell [57, 58]). But according to Eq. (7.2) something different happens: In particular, if Alice decides to measure the 'position' observable $\hat{q}_A$ of her mode, Bob's mode would instantaneously be projected in one of the position eigenstates $\{|q\rangle_B\}$ of $\hat{q}_B$, as the "collapsed" state $\langle q_A|\psi\rangle_{\rm EPR} : \mathcal{H}_B$ of Bob (after Alice's measurement) would satisfy

$$\hat{q}_B\langle q_A|\psi\rangle_{\rm EPR} = q_A\langle q_A|\psi\rangle_{\rm EPR}, \tag{7.3}$$

due to $(\hat{q}_A - \hat{q}_B)\,|\psi\rangle_{\rm EPR} = 0$. Similarly, if Alice chose to measure $\hat{p}_A$, Bob's mode would instantaneously be projected in one of the momentum eigenstates $\{|p\rangle_B\}$ of $\hat{p}_B$ for Bob. That is, *"as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wavefunctions"* [55]. And here comes the paradox, as, *"the two systems no longer interact, [so] no real change can take place in [Bob's] system in consequence of anything that may be done to [Alice's] system."* [55] Therefore, quantum theory seems to involve an involve an unacceptable "*action at a distance*".

For these reasons, the EPR trio concluded that the quantum state cannot be describing reality, and quantum theory must be *incomplete*. Their hope and intuition was that a complete theory of nature would necessarily satisfy the notion of *local causality*, without featuring any unacceptable "action at a distance". Although the EPR argument is correct in its formulation , the premises on which it was structured on (i.e., local causality) turned out not to be. About 30 years after the EPR paper, Bell realized that the EPR intuition can actually be formulated mathematically and independently of any underlying theory (whether that is quantum theory, or any other more 'complete' *local hidden variable* theory). First, Bell showed that the concept of local causality is equivalent to a *local hidden variable* (LHV) theory. Then Bell proved his famous theorem, that the correlations between distant and causally disconnected systems, as predicted by *any* LHV theory -respecting the concept of *local causality*- are always bounded in strength and should necessarily satisfy the so-called *Bell inequalities* [57, 58]. Quantum

theory turns out to violate Bell's inequalities and this phenomenon is dubbed *Bell-nonlocality* [145]. But let's forget about quantum theory for now, according to EPR it could be incomplete anyway; what about nature itself? Can real physical systems violate Bell's inequalities and, thus, the intuitive concept of local causality? The answer is *yes*. Aspect *et al.* were the first to demonstrate a Bell inequality violation using pairs of polarized entangled photons [146], and very recently three experiments took place demonstrating the first-ever loophole-free Bell inequality violations [60, 61, 62]. Funnily enough, although Bell-nonlocality has been established as a physical phenomenon both experimentally and theoretically, the EPR state (7.1) cannot violate any Bell inequality when quadrature measurements are performed, which was exactly the setting considered in the original EPR argument. The reason is that the probabilities created by Gaussian states and Gaussian measurements always admit a local hidden variable model which by definition satisfies all Bell inequalities. For all bipartite pure states, however, there always exist measurements for both parties that can demonstrate Bell-nonlocality, and in the case of pure Gaussian states (like, the EPR state) non-Gaussian measurements are required for such a demonstration.

7.1.1 Aftermath of EPR: Quantum steering

In the aftermath of the EPR paper, Schrödinger [16] was the first introduce the words "entanglement" and "steering" to describe this spooky "action at a distance" presented in the EPR argument. The word "steering" comes into the picture, as Alice is seen to remotely *steer* Bob's state to an eigenstate of position or momentum (as seen above) depending on the observable she chooses to measure.

Schrödinger was the one to actually introduce the quantum state (or, wavefunction) ψ to describe atoms, and he did believe that it offers a complete description of nature, in contrast to EPR. However, just like the EPR trio, Schrödinger himself could not accept this spooky action at a distance and, to solve this paradox, he suggested (wrongly) that the quantum mechanical description of delocalized entangled systems must be incorrect [16, 147]. In particular, for a pure entangled state like Eq. (7.1), Schrödinger argued that Bob's system can be *"steered or piloted into one or the other type of state at [Alices] mercy in spite of [her] having no access to it"*, and referred to it as a 'paradox' since if such states existed then local causality must be violated.

The conclusion of Schrödinger was, therefore, that Bob's system must have a definite state, even if it is completely unknown, so that "steering" would never be witnessed experimentally.

We call the model Schrödinger had in mind, a *local hidden state* (LHS) model for Bob. We summarize Schrödinger's view on the EPR paradox in the following definition,

Definition 7.1.1. *We say that the EPR paradox exists between two parties Alice and Bob, only if steering from Alice to Bob can be demonstrated and, in turn, steering can be demonstrated only if there is no LHS model for Bob that can explain the observed correlations. Equivalently for the reverse situation, where Bob steers Alice.*

Schrödinger never rigorously defined the concept of a local hidden state model for Bob, and therefore the assumption of the existence of such a model could not be put to experimental test. A precise formulation of a LHS model and steering will be given in Sec. 7.2. Finally, notice that demonstration of Bell-nonlocality already refutes the concept of a LHS model, as we will see later on. Despite the fact that Bell-nonlocality has already settled the issue, we will insist in formulating Schrödinger's concept of steering as it will lead us to recognize a new type of quantum correlations, that are useful not only for an (experimentally) easier demonstration of the EPR paradox, but also for the implementation of novel practical applications.

7.1.2 Reid's criterion

The first attempt to create an experimental criterion to demonstrate the EPR paradox, in a continuous variable setting, was made in the 1980s by Margaret Reid [11]. The importance of Reid's idea is that it allows for the possibility to observe the EPR paradox with realistic finitely entangled CV states that are available in the laboratory; remember that the actual EPR state (3.54), with its perfect correlations, is un-physical since it requires infinite energy.

Reid considered a scenario where Alice and Bob share a pair of two spatially separated particles described by a bipartite state $\hat{\rho}_{AB}$, which is assumed to feature correlated 'positions' and anti-correlated 'momenta' of the two particles. The difference with the EPR scenario is that the correlations are not assumed to be perfect, like

$$Q_A = Q_B\,, \quad P_A = -P_B. \tag{7.4}$$

Reid distinguished three assumptions that EPR made to arrive at their paradox:
Assumption # 1: They assume quantum mechanics predicts correctly at least the results of the experiment.
Assumption # 2: "If without in any way disturbing the system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding

to this quantity." [55]

Assumption # 3: They assume there is "no action at a distance".

Reid then showed that based on these three assumptions we can derive an experimental criterion that should always be satisfied if all three assumptions are true, and violated only if any of these assumptions does not hold (hence, arriving at the EPR paradox). Thus, let's go into more detail on Reid's idea:

If Alice chose to measure the position $\hat{q}_A$ of her own particle A, she would be able to predict Bob's position Q_B with a good enough precision. Assuming Alice would obtain some arbitrary outcome Q_A, let's quantify the precision of the inference of Bob's Q_B by the conditional variance,

$$\Delta^2(Q_B|Q_A) = \langle Q_B^2 \rangle_{Q_A} - \langle Q_B \rangle_{Q_A}^2, \tag{7.5}$$

which is evaluated on the conditional probability distribution $P(Q_B|Q_A)$. If Alice and Bob shared the EPR state, then Alice would make a perfect prediction $\Delta^2(Q_B|Q_A) \to 0$. According now to assumption # 3, since there is no action at a distance Alice's prediction for the position Q_B of particle B is made without disturbing the particle B. Also, due to assumption # 2, the predicted position Q_B must have had a definite pre-determined value inside the range determined by $\Delta^2(Q_B|Q_A)$) independently of Alice's measurement. If, instead, Alice chose to measure the momentum $\hat{p}_A$, then, by similar reasoning, the predicted position P_B must have had a definite pre-determined value inside the range determined by $\Delta^2(P_B|P_A)$) independently of Alice's measurement. To sum up, we have established that given a shared copy of the state $\hat{\rho}_{AB}$, under the assumptions # 2 and # 3 the distribution of the "real" value of Bob's position and momentum -regardless of what observable Alice measures on her particle- *must* follow the distributions $\Delta^2(Q_B|Q_A)$ and $\Delta^2(P_B|P_A)$, respectively. According now to assumption # 1, since the quantum mechanical formalism holds true, the best possible inference of Bob's position and momentum that is allowed by any quantum state, must respect Heisenberg's uncertainty principle (HUP). Therefore, the distributions of the "real" values of Q_B and P_B must satisfy

$$\Delta^2(Q_B|Q_A)\,\Delta^2(P_B|P_A) \geq \frac{1}{4}. \tag{7.6}$$

This criterion is conditioned on some arbitrary outcomes Q_A, P_A of Alice. For convenience, we take the average of each of the variances over all outcomes, defining the *minimum inferred* variance

$$\Delta^2_{\text{min}} Q_B = \int dQ_A \; p(Q_A)\; \Delta^2(Q_B|Q_A), \tag{7.7}$$

and similarly for $\Delta^2_{\text{min}} P_B$. Since the minimum inferred variances are larger or equal to the conditional variances, their product should also satisfy HUP

$$\Delta^2_{\text{min}} Q_B \Delta^2_{\text{min}} P_B \geq \frac{1}{4}. \tag{7.8}$$

Ineq. (7.8) is known as *Reid's criterion*, which is a direct consequence of the three assumptions made by EPR, and should always be satisfied if all three assumptions are valid. A violation of Reid's criterion demonstrates the EPR paradox and forces us to negate at least one of the assumptions. The EPR state (3.54) with its perfect correlations, maximally violates this criterion since it predicts, $\Delta^2_{\text{min}} Q_B \Delta^2_{\text{min}} P_B = 0$. However, as we pointed out in the beginning of this section, this criterion also allows us to demonstrate the EPR paradox even when the correlations between modes A and B are not perfect.

Interestingly, Reid's criterion will be shown in Chapter 8 to be equivalent to the concept of quantum steering to be defined in the next section. Also, in Chapter 9 we will exhaustively study the violation of (7.8) by general Gaussian states. Last but not least, due to the aforementioned connection with steering-type correlations, Reid's criterion has found important applications in one-sided device independent quantum cryptography.

7.2 Steering as a quantum information task

A precise formulation of Schrödinger's concept of steering was put forward very recently by Wiseman, Jones and Doherty [12], who defined steering according to a *task*, also relevant from a quantum information perspective. The task of *steering* involves two parties, Alice and Bob, and the goal in this task is the demonstration by Alice that she can remotely 'steer' Bob's local state by implementing different measurements on her own system. Bob, on the other hand, just like Schrödinger himself, is sceptical about 'steering' due to its seemingly non-local nature, and he believes that there must exist some fixed local hidden state $\hat{\rho}_\lambda : \mathcal{H}_B$ (where, λ is a particular copy of the state) that can explain the observed correlations without requiring any "spooky action at a distance" from Alice. Bob does trust that his own system is described by a known Hilbert space $\mathcal{H}_B$ (e.g., the spin-$\frac{1}{2}$ degrees of freedom of an electron), and that his own measurements are well-described by the axioms of quantum theory, but he doesn't make any assumption about Alice's system or measurements. In other words, Bob requires a clear demonstration of steering on his trusted quantum system, without assuming anything about

Alice. Given this qualitative description of the task, we will proceed by rigorously defining the steering task, together with the formulation of local hidden state models.

We start by defining the scenario in which quantum steering is discussed:

Consider a situation where Alice and Bob share an unknown quantum state $\hat{\rho}_{AB} : \mathcal{H}_A \otimes \mathcal{H}_B$ where, as discussed above, the Hilbert space $\mathcal{H}_A$ of Alice (and, thus, her system and measurements) is completely unknown, whereas $\mathcal{H}_B$ of Bob is known . Alice performs n different measurements on her subsystem, labelled by $x = 1, \ldots, n$, each having outcomes $a \in \lambda(x)$, where $\lambda(x)$ is the set of outcomes corresponding to the measurement x (could be a discrete, or continuous, set). Upon choosing measurement x and getting outcome a, Alice announces to Bob her the pair (a, x), and the state of Bob's subsystem is transformed into the conditional state $\hat{\rho}_{a|x}$ with probability $p(a|x)$.

In the steering scenario, where nothing is assumed about Alice's system and measurements, the only available information for Bob to determine whether Alice can steer his system or not, is the collection of post-measured states and conditional probabilities $\{\hat{\rho}_{a|x}, p(a|x)\}_{a,x}$. This information can be compactly summarized by the so-called *assemblage* $\{\hat{\sigma}_{a|x}\}_{a,x}$, a set that contains all the (unnormalized) quantum states $\hat{\sigma}_{a|x} = p(a|x)\hat{\rho}_{a|x}$, with its norm giving the conditional probability $p(a|x) = \mathrm{tr}\hat{\sigma}_{a|x}$. The question then becomes: Given the assemblage, how can we determine whether Alice can steer Bob's system? Below we provide two equivalent ways to answer this question.

7.2.1 Steering as the impossibility of a local hidden state model

According to Wiseman *et al.*'s definition of quantum steering, and in accordance to Schrödinger's arguments, Bob can be convinced that Alice remotely steered his system only if there exists no local hidden state (LHS) model that can reproduce his observed assemblage $\{\hat{\sigma}_{a|x}\}_{a,x}$. Therefore, let us see below what kind of assemblages a LHS model can reproduce.

According to a LHS model, at a given run of the protocol, source sends a definite (but arbitrary, and unknown) quantum state $\hat{\rho}_\lambda$ to Bob, while the corresponding 'hidden' variable λ that determines Bob's 'hidden' state is assumed to be known by Alice. This is equivalent to saying that, for a given run, Alice knows what state $\hat{\rho}_\lambda$ was given to Bob, while no assumptions are made about Alice's system and announced measurements. Given the information λ, and given her measurement choice x, announces outcome a with probability $p(a|x, \lambda)$. It's further assumed that the variable λ is drawn according to some distribution $q(\lambda)$. Therefore, given a

particular λ and announced pair (a, x), Bob's unnormalized conditional state, at a given run, will be

$$\hat{\sigma}_{a|x,\lambda} = q_\lambda \, p(a|x,\lambda)\, \hat{\rho}_\lambda,$$

where $q_\lambda \, p(a|x,\lambda) = \mathrm{tr}[\hat{\sigma}_{a|x,\lambda}]$ is the probability that Alice announces (a, x) given λ. Since Bob has no access to the variable λ summation over λ must take place, with his final observed assemblage being

$$\hat{\sigma}_{a|x} = \sum_\lambda q_\lambda \, p(a|x,\lambda)\, \hat{\rho}_\lambda, \tag{7.9}$$

with the normalization $p(a|x) = \mathrm{tr}[\hat{\sigma}_{a|x}]$.

An assemblage $\hat{\sigma}_{a|x}$ that admits a decomposition of the form (7.9) can be reproduced by a LHS model, and thus called *unsteerable* as steering cannot be demonstrated. On the contrary, if there exist no distribution q_λ, stochastic map $p(a|x,\lambda)$, and states $\hat{\rho}_\lambda$, such that Bob's observed assemblage $\hat{\sigma}_{a|x}$ be brought in the form (7.9) $\forall\, x, a$, then steering has been demonstrated, as no LHS model can reproduce the correlations, and the assemblage is called *steerable*.

Steerability of bipartite states Quantum steering is defined solely in terms of Bob's assemblage without any reference to the actual bipartite state $\hat{\rho}_{AB}$. A natural question would then be: Given a bipartite state $\hat{\rho}_{AB}$, how can we infer whether it can be used to demonstrate steering from Alice to Bob? Considering a set of measurement operators $\{\hat{M}_{a|x}\}_a$ for Alice, and for the given $\hat{\rho}_{AB}$, Bob's assemblage will simply be

$$\hat{\sigma}_{a|x} = \mathrm{tr}_A \left[\left(\hat{M}_{a|x} \otimes \mathbb{I}_B \right) \cdot \hat{\rho}_{AB} \right], \tag{7.10}$$

where $\sum_a \hat{M}_{a|x} = \mathbb{I}$ and $\hat{M}_{a|x} \geq 0, \ \forall\, x, a$. Then, $\hat{\rho}_{AB}$ is called *steerable* from A to B if it can give rise to a steerable assemblage (7.10) for the considered measurements, or *unsteerable* if it gives rise to an unsteerable assemblage for the given measurements. Notice also that whether steering is demonstrated or not strongly depends on the choice of measurements, and a topic of great interest is to prove whether a given state $\hat{\rho}_{AB}$ is unsteerable for *any* choice (and number) of measurements; a trivial example of such a state is the product state.

7.2.2 Steering as a one-sided device independent entanglement detection

The original definition of steering given by Wiseman *et al.* [12] is described in Sec. 7.2.1, with the LHS models playing a protagonist role. In this section we will give an alternative but equivalent definition, that may be more intuitive to the reader.

Let us forget about steering for a moment, and imagine, again, a scenario where Alice and Bob share a bipartite state $\hat{\rho}_{AB}$. The question we want to deal with now is: Is $\hat{\rho}_{AB}$ entangled? As we have seen in previous parts of the thesis, where we talked about entanglement, $\hat{\rho}_{AB}$ will be entangled if it does not admit the following separable decomposition

$$\hat{\rho}_{AB} = \sum_{\lambda} q_{\lambda} \hat{\rho}_A^{\lambda} \otimes \hat{\rho}_B^{\lambda}. \tag{7.11}$$

However, Eq. (7.11) is equivalent to Bob's assemblage admitting the following form,

$$\begin{aligned} \hat{\sigma}_{a|x} &= \mathrm{tr}_A \left[\left(\hat{M}_{a|x} \otimes \mathbb{I}_B \right) \cdot \hat{\rho}_{AB} \right] \\ &= \sum_{\lambda} q_{\lambda}\, p(a|x, \hat{\rho}_A^{\lambda})\, \hat{\rho}_B^{\lambda} \end{aligned} \tag{7.12}$$

for all possible measurements $\hat{M}_{a|x}$, where $p(a|x, \hat{\rho}_A^{\lambda}) = \mathrm{tr}[\hat{M}_{a|x} \hat{\rho}_A^{\lambda}]$. Notice that in Eq. (7.12) we simply substituted the separable form of Eq. (7.11). Notice that we are still talking about entanglement detection; even though we introduced the assemblage, which we first encountered in the concept of steering, detecting entanglement using Eq. (7.12) is equivalent as detecting entanglement using Eq. (7.11). Steering comes into the picture when we introduce the one-sided device independent (1sDI) framework.

One-sided device independent framework In plain entanglement detection there is always a crucial assumption, that both Hilbert spaces $\mathcal{H}_{A(B)}$ are exactly known; this is what allows us to work conveniently with the bipartite density matrix $\hat{\rho}_{AB}$ and never deal with the, undoubtedly, "uglier" assemblage. This assumption implies, however, that both parties trust their devices, meaning, for example, that Alice (and Bob) can safely assign a mathematical measurement operator $\hat{M}_{a|x}$ acting on her known Hilbert space $\mathcal{H}_A$, to describe the action of her device on her subsystem. If such an assumption is met, then Alice can describe her measurement results using the rules of quantum theory, e.g. $p(a|x, \hat{\rho}_A^{\lambda}) = \mathrm{tr}[\hat{M}_{a|x} \hat{\rho}_A^{\lambda}]$, where this distribution is strongly constrained by the dimension of $\mathcal{H}_A$ and has to obey quantum uncertainty relations.
However, imagine a scenario where Alice's measuring devices cannot be trusted, and no assumptions can be made on how the device acts on the system. Such a scenario is quite common and relevant in quantum cryptography, where the devices of a party may have been hacked by an eavesdropper. Or, imagine a different but equivalent scenario, where Alice herself cannot be trusted (independently of her devices) and may be lying to Bob about her obtained measurements. In both such cases, the Hilbert space of Alice and the measurement operators that

describe her devices (or, her actions) are *completely unknown*. Can we still proceed with the entanglement detection? The answer is yes, but we can no longer use the bipartite density matrix (7.11) for that purpose as before, as no assumption can be made on Alice (and the discussion starts to remind us of steering!). Since Eqs. (7.11) and (7.12) are equivalent, it's most convenient to work with Bob's assemblage. Looking at (7.12), we see that the only place where Alice's (unknown) Hilbert space is involved is via the probability $p(a|x, \hat{\rho}_A^\lambda)$. As we said before, such a probability is in general constrained by the particular Hilbert space the measurement operators act on. However, since $\mathcal{H}_A$ is unknown, we will generalize this distribution to one that is independent of $\mathcal{H}_A$ and, hence, obeys no quantum mechanical constraints. Symbolically, this is expressed by

$$p(a|x, \hat{\rho}_A^\lambda) \longrightarrow p(a|x, \lambda), \tag{7.13}$$

where the classical variable λ just expresses the fact that the new distribution is unconstrained. It's then clear that Alice and Bob will have detected entanglement in their shared state $\hat{\rho}_{AB}$, even though Alice is not trusted, if Bob's assemblage cannot be expressed as,

$$\hat{\sigma}_{a|x} = \sum_\lambda q_\lambda \, p(a|x, \lambda) \, \hat{\rho}_\lambda, \tag{7.14}$$

which is precisely the form of an unsteerable assemblage (7.9). This proves the equivalence between steering and 1s-DI entanglement detection, as steering from *Alice* to *Bob* implies detection of entanglement when no assumptions are made about Alice's measurements, and vice versa.

7.3 Entanglement < *Steering* < Bell-nonlocality

Entanglement, steering, and nonlocality, are all different types of quantum correlations featured among quantum systems. We have already encountered about the pyramid of quantum correlations in Section 4, which reveals a hierarchy among all these types of correlations. In this section we will discuss about how steering fits in-between entanglement and nonlocality.

Entanglement Let us start with entanglement, and lead our way through towards steering and nonlocality. A bipartite quantum state $\hat{\rho}_{AB}$ is entangled if and only if it does not admit a separable decomposition of the form

$$\hat{\rho}_{AB} = \sum_\lambda p_\lambda \hat{\rho}_A^\lambda \otimes \hat{\rho}_B^\lambda. \tag{7.15}$$

It's instructive to translate this condition into an equivalent one that involves joint probability distributions of observed outcomes. Assuming Alice and Bob make measurements labelled by x and y, respectively, with corresponding outcomes a and b, by using the separable form (7.15) in

$$p(a,b|x,y) = \mathrm{tr}\left[\left(\hat{M}_{a|x} \otimes \hat{N}_{b|y}\right)\hat{\rho}_{AB}\right], \tag{7.16}$$

we arrive at the equivalent expression for separability

$$p(a,b|x,y) = \sum_{\lambda} p_\lambda \, p(a|x;\hat{\rho}_A^\lambda)\, p(b|y;\hat{\rho}_B^\lambda), \quad \forall x,y,a,b, \tag{7.17}$$

which will be the main object of our focus.

Before we proceed, let us show how we can prove the equivalence (7.15) $\Leftrightarrow$ (7.17)? The implication $\hat{\rho}_{AB} \Rightarrow \{p(a,b|x,y)\}_{x,y,a,b}$ has already been proved via Eq. (7.16). To prove the reverse, i.e. $\hat{\rho}_{AB} \Leftarrow \{p(a,b|x,y)\}_{x,y,a,b}$, one considers the fact that there exist tomographically complete set of measurements x, y, that allows for the faithful reconstruction of the density matrix $\hat{\rho}_{AB}$ from the observed probability distributions $\{p(a,b|x,y;\hat{\rho}_{AB})\}_{x,y,a,b}$. This proves the desired equivalence.

Steering Considering now "$A \to B$" steering, where Alice demonstrates steering of Bob's state, we have shown that a bipartite state $\hat{\rho}_{AB}$ is unsteerable (i.e., cannot be used to demonstrate "$A \to B$" steering) if Bob's assemblage is of the unsteerable form,

$$\hat{\sigma}_{a|x} = \sum_{\lambda} q_\lambda \, p(a|x,\lambda)\, \hat{\rho}_B^\lambda, \quad \forall a,x. \tag{7.18}$$

Using similar arguments as above, we can show that this condition is equivalent to,

$$p(a,b|x,y) = \sum_{\lambda} p_\lambda \, p(a|x,\lambda)\, p(b|y;\hat{\rho}_B^\lambda), \quad \forall x,y,a,b, \tag{7.19}$$

where, $p(a,b|x,y) = \mathrm{tr}[\hat{N}_{b|y}\,\hat{\sigma}_{a|x}]$. Comparing the two expressions Eqs. (7.17) and (7.19) we spot the only difference is the generalization

$$p(a|x;\hat{\rho}_A^\lambda) \longrightarrow p(a|x,\lambda),$$

from a distribution that depends, and thus is constrained by, Alice's Hilbert space $\mathcal{H}_A$, to an arbitrary distribution $p(a|x,\lambda)$ that is independent of $\mathcal{H}_A$ and thus obeys no quantum mechanical restrictions. In other words, the unsteerability condition (7.19) is independent of Alice's Hilbert

space as it makes no assumptions about this space. This implies that the unsteerability condition (7.19) is harder to violate than the separability condition (7.17). Therefore, a bipartite state $\hat{\rho}_{AB}$ may violate the separability condition but not the unsteerability one, as it would require even stronger correlations. We conclude that steering a form of quantum correlations stronger than plain entanglement, and the demonstration of "$A \rightarrow B$" steering allows for entanglement detection between Alice and Bob when no assumptions are made about Alice's side, i.e. in a one-sided device independent manner.

Bell-nonlocality A bipartite state $\hat{\rho}_{AB}$ is called Bell-nonlocal if its correlations cannot be explained by a separable model of the form (7.17), but with complete independence of both Alice's and Bob's Hilbert spaces,

$$p(a,b|x,y) = \sum_{\lambda} p_{\lambda}\, p(a|x,\lambda)\, p(b|y;\lambda), \quad \forall x,y,a,b, \tag{7.20}$$

where we made the generalization,

$$p(a|x;\hat{\rho}_A^{\lambda}) \longrightarrow p(a|x,\lambda), \quad p(b|y;\hat{\rho}_B^{\lambda}) \longrightarrow p(b|y,\lambda). \tag{7.21}$$

Since both $p(a|x,\lambda)$ and $p(b|y,\lambda)$ are arbitrary probability distributions that obey no quantum mechanical constraints, even stronger quantum correlations are required in order to violate the local decomposition (7.20), compared to the separability (7.17) and the unsteerability (7.19) conditions. Observation of Bell-nonlocal correlations in a bipartite quantum state implies, due to (7.21), entanglement detection between Alice and Bob in a completely device independent manner, i.e. without having made any assumptions about both Alice's and Bob's measuring devices and quantum systems. The mere existence of such strong correlations in physical systems gave rise to a whole new sub-field of cryptography known as, device-independent quantum key distribution. In this task, observation of nonlocal correlations allows Alice and Bob to communicate securely without having to worry about their equipment be possibly hacked by an eavesdropper.

In conclusion, we have proved the desired hierarchical order where steering stands in-between entanglement and nonlocality,

$$\text{entanglement} \leq \textit{steering} \leq \text{nonlocality}. \tag{7.22}$$

In the case of pure states, the equal signs "=" hold in both sides of (7.22).

8

Steering detection

Up to now, we defined the steering-type correlations to be those that do not admit a local hidden state model. We then showed that steering is equivalent to detecting entanglement but in a one-sided device independent manner, where one of the subsystems is not characterized. Detecting steerability of quantum states is essential to assess their suitability for quantum information protocols with partially trusted devices. In this chapter we will introduce various steering detection methods. In Section 8.1 we will first make a brief literature review on the various approaches on steering detection, and show that Reid's criterion on the EPR paradox is actually a steering criterion, confirming the intuition that the concept of steering faithfully describes the EPR paradox.

In Section 8.2 we point out an important gap in the literature regarding steering detection of high dimensional and CV systems, and propose a new method to deal with this problem, which is based on a work published in Physical Review Letters [4]. In particular, we provide a hierarchy of sufficient conditions for the steerability of bipartite quantum states of any dimension, including continuous variable states. Previously known steering criteria are recovered as special cases of our approach. The proposed method allows us to derive optimal steering witnesses for arbitrary families of quantum states, and provides a systematic framework to analytically derive non-linear steering criteria. We also discuss relevant examples and, in particular, provide an optimal steering witness for a lossy single-photon Bell state; the witness can be implemented just by linear optics and homodyne detection, and detects steering with a higher loss tolerance than any other known method.

8.1 Analytical methods: Multiplicative variance criteria

Steering criteria are defined as any criteria that are sufficient to demonstrate steering experimentally. The theory of steering criteria was developed for the first time by E. Cavalcanti *et al.* [148], who identified two main types of EPR-steering criteria: the multiplicative variance criteria that are based on product uncertainty relations involving variances of observables, and the additive convex criteria, based on uncertainty relations which are sums of convex functions. Here we will only review the first type of multiplicative variance criteria, and our purpose is two-fold: First, we want to demonstrate that Reid's criterion (7.8) on the EPR paradox is actually a special case of a steering criterion. Second, we want to show that the derivation of steering criteria using the methods demonstrated in Ref. [148] can be very cumbersome, and that it's not at all straightforward to derive new (and better) steering criteria at will. This will motivate us for Section 8.2 where we propose a new method to overcome these difficulties and derive arbitrary steering criteria in a hierarchical and very systematic way.

For the derivation of multiplicative variance steering criteria below, we follow Ref. [148]. We consider a situation where Alice tries to infer the outcomes of Bobs measurements through measurements on her subsystem. We denote by $B_{\text{est}}(A)$ Alices estimate of the value of Bobs measurement b as a function of the outcomes of her measurement a. As in Sec. II D, the average *inference variance* of B given estimate $B_{\text{est}}(A)$ is defined by

$$\Delta^2_{\text{inf}} B = \langle [B - B_{\text{est}}(A)]^2 \rangle = \sum_{A,B} P(A,B)(B - B_{\text{est}}(A))^2. \tag{8.1}$$

For a given A, the optimal estimator $B_{\text{est}}(A)$ that minimizes Eq. (8.1) is just the mean $\langle B \rangle_A$ of the conditional probability distribution $P(B|A)$, i.e., $B_{\text{est}}(A) = \langle B \rangle_A$. Using this optimal estimator, we denote the *minimum* (or optimal) *inference variance* of B by measurement of a as

$$\begin{aligned} \Delta^2_{\text{min}} B &= \sum_{A,B} P(A,B)(B - \langle B \rangle_A)^2 \\ &= \sum_A P(A) \sum_B P(B|A)(B - \langle B \rangle_A)^2 \\ &= \sum_A P(A) \Delta^2(B|A), \end{aligned} \tag{8.2}$$

where $\Delta^2(B|A)$ is the variance of B as calculated from $P(B|A)$. Notice that $\Delta^2_{\text{min}} B$ as defined in Eq. (8.2) is exactly the quantity (7.7) that we used in the proof of Reid's criterion. As

explained above,

$$\Delta^2_{\text{inf}} B \geq \Delta^2_{\text{min}} B \tag{8.3}$$

for all choices of the estimator $B_{\text{est}}(A)$. This minimum is optimal, but not always experimentally accessible in experiments since it requires one to be able to measure conditional probability distributions which is non-trivial especially if the measurement outcomes are continuous.

We assume that the statistics of experimental outcomes of Alice and Bob can be described by a "$A \to B$" LHS model (7.19), which we write here more conveniently as,

$$P(A, B) = \sum_{\lambda} P(\lambda) P(A|\lambda) P_Q(B|\lambda), \tag{8.4}$$

where for notational simplicity we omit the measurement choices a, b. We also denote with the "Q" subscript in $P_Q(B|\lambda)$ the fact that it's a *quantum* probability distribution constrained by Bob's Hilbert space, while $P(A|\lambda)$ is an arbitrary unconstrained distribution. Assuming this model, the conditional probability of B given A is

$$P(B|A) = \sum_{\lambda} \frac{P(\lambda)P(A|\lambda)}{P(A)} P_Q(B|\lambda) = \sum_{\lambda} P(\lambda|A) P_Q(B|\lambda). \tag{8.5}$$

We will now use a known result that if a probability distribution has a convex decomposition of the type $P(x) = \sum_y P(y)P(x|y)$, then the variance $\Delta^2 x$ over the distribution $P(x)$ cannot be smaller than the average of the variances over the component distributions $P(x|y)$, i.e., $\Delta^2 x \geq \sum_y P(y)\Delta^2(x|y)$. Therefore, by Eq. (8.5), the variance $\Delta^2(B|A)$ satisfies

$$\Delta^2(B|A) \geq \sum_{\lambda} P(\lambda|A) \Delta^2_Q(B|\lambda), \tag{8.6}$$

where $\Delta^2_Q(B|\lambda)$ is the variance of $P_Q(B|\lambda)$. Using this result, we can derive a bound for $\Delta^2_{\text{min}} B$ in Eq. (8.2),

$$\Delta^2_{\text{min}} B \geq \sum_{A,\lambda} P(A, \lambda) \Delta^2_Q(B|\lambda) = \sum_{\lambda} P(\lambda) \Delta^2_Q(B|\lambda). \tag{8.7}$$

Suppose that Bob's set of measurements is comprised by three observables $\{\hat{b}_1, \hat{b}_2, \hat{b}_3\}$, which satisfy the commutation relation $[\hat{b}_1, \hat{b}_2] = i\hat{b}_3$, and with corresponding outcomes B_1, B_2, B_3. The outcomes must then satisfy the Schrödinger-Robertson uncertainty relation,

$$\Delta_Q(B_1|\hat{\rho}) \Delta_Q(B_2|\hat{\rho}) \geq \frac{1}{2} \left| \langle B_3 \rangle_\rho \right|, \tag{8.8}$$

where $\Delta_Q(B_i|\hat{\rho})$ and $\langle B_i \rangle_\rho$ are the standard deviation and the average of B_i in the quantum state $\hat{\rho}_i$, respectively.

We will now use this uncertainty relation together with the Cauchy-Schwarz (CS) inequality to obtain the desired steering criterion. The CS inequality states that, for two vectors u and v, $|u||v| \geq |u \cdot v|$. Now, define $u = \left[\sqrt{P(\lambda_1)}\Delta_Q(B_1|\lambda_1), \sqrt{P(\lambda_2)}\Delta_Q(B_1|\lambda_2), \ldots\right]$ and $v = \left[\sqrt{P(\lambda_1)}\Delta_Q(B_2|\lambda_1), \sqrt{P(\lambda_2)}\Delta_Q(B_2|\lambda_2), \ldots\right]$. Then by Eq. (8.7)

$$\Delta_{\min} B_1 = \sqrt{\Delta^2_{\min} B_1} \geq |u|, \tag{8.9}$$

$$\Delta_{\min} B_2 = \sqrt{\Delta^2_{\min} B_2} \geq |v|. \tag{8.10}$$

Using Eq. (8.9), the CS inequality, and the uncertainty relation (8.8), we obtain

$$\begin{aligned} \Delta_{\min} B_1 \Delta_{\min} B_2 \geq |u||v| \geq |u \cdot v| &= \sum_\lambda P(\lambda)\Delta_Q(B_1|\lambda)\Delta_Q(B_2|\lambda) \\ &\geq \frac{1}{2}\sum_\lambda P(\lambda)\left|\langle B_3\rangle_\lambda\right|, \end{aligned} \tag{8.11}$$

where we denoted with $\langle B\rangle_\lambda$ the expectation value of B calculated from $P_Q(B|\lambda)$. Using again Eq. (8.5) and the fact that $f(x) = |x|$ is a convex function (which means that it satisfies $\sum_x P(x)|x| \geq \left|\sum_x P(x)x\right|$, we obtain a bound for the last term,

$$\begin{aligned} \sum_\lambda P(\lambda)\left|\langle B_3\rangle_\lambda\right| &= \sum_{A_3,\lambda} P(A_3,\lambda)\left|\langle B_3\rangle_\lambda\right| \\ &\geq \sum_{A_3} P(A_3)\left|\sum_\lambda P(\lambda|A_3)\langle B_3\rangle_\lambda\right| \\ &= \sum_{A_3} P(A_3)\langle B_3\rangle_{A_3} \equiv |\langle B_3\rangle|_{\text{inf}}\,. \end{aligned} \tag{8.12}$$

Using now Eq. (8.3), together with Eqs. (8.11) and (8.12), we obtain the following *steering criterion*

$$\Delta_{\text{inf}} B_1 \Delta_{\text{inf}} B_2 \geq \frac{1}{2}|\langle B_3\rangle|_{\text{inf}}\,. \tag{8.13}$$

Ineq. (8.13) represents a whole family of multiplicative variance steering criteria, as the observables $\hat{b}_i$ for Bob are left arbitrary. As we showed, this inequality stems directly from the LHS model (7.19), and an experimental violation implies the failure of such models to explain the measured correlations, demonstrating steering from Alice to Bob. As a side note, notice that the choices of measurement a_1, a_2, a_3 used by Alice to infer the values of the corresponding measurements $\hat{b}_1, \hat{b}_2, \hat{b}_3$ of Bob are arbitrary in this derivation, since we have complete independence from Alice's Hilbert space. For this reason, the specific quantum observables $\hat{a}_i$ played no role in the derivation. In an experimental situation, one would be advised to choose,

of course, those $\hat{a}_i$ which can maximize the violation of Eq. (8.13). Finally, notice the long and cumbersome derivation of steering criteria using such methods. Imagine a situation where this type of criteria cannot detect any steering for a given quantum state, how would we proceed then? Would we attempt another lengthy derivation of some other family of steering criteria, hoping they will be more effective in steering detection? Obviously, such a strategy is not efficient and is certainly not practical. Our own proposal to be introduced in Section 8.2 will offer for the first time such a practical and systematic way for steering detection.

8.1.1 Connection to Reid's criterion

In the above, Bob's observables were left arbitrary. To make the connection with Reid's criterion, let us choose $\hat{b}_1 = \hat{q}_B$, $\hat{b}_2 = \hat{p}_B$ and $\hat{b}_1 = i\,\mathbb{I}$, since $[\hat{q}_B, \hat{p}_B] = i\,\mathbb{I}$. Substituting in Eq. (8.13) we obtain

$$\Delta_{\text{inf}} Q_B \, \Delta_{\text{inf}} P_B \geq \frac{1}{2}, \tag{8.14}$$

which is precisely Reid's criterion (7.8). This provides a formal proof that Reid's criterion on the EPR paradox is a special case of steering, since it's a direct consequence of a LHS model. This also confirms the claim that the concept of steering captures the essence of the EPR paradox.

8.2 A hierarchy of steering criteria based on moments for all bipartite quantum systems

Compared to well-studied entanglement and nonlocality, relatively little progress has been achieved about steering detection. A handful of criteria exist [148, 149, 150, 151, 152, 153, 154, 155], which are however tailored to specific measurement scenarios; i.e., a non-violation would render these criteria useless for the particular situation. An example of such a criterion was examined in Section 8.1. Only very recently some constructive steering criteria were introduced, which give an experimenter the freedom to choose the measurements involved, and allow for an improvement of the detection by performing additional measurements until a violation is observed [156, 157, 158, 159]. These criteria are based on the useful methods of semidefinite programming [160], and the downside in this case is that, so far, they could only be applied to discrete variable (DV) systems with not too high dimension, due to computational limitations. It is then clear that there exists still a gap that needs to be filled about

steering detection, regarding higher dimensional DV systems and general continuous variable (CV) systems.

In this chapter, following our work in Ref. [4], we propose a hierarchy of steering criteria that is directly applicable to bipartite quantum systems of any dimension, including the case of infinite-dimensional systems. Our method avoids the dimension problem by utilizing moments of observables instead of dealing with conditional states, at variance with previous DV proposals. A systematic framework is provided for deriving non-linear steering inequalities in an analytical manner. To the best of our knowledge, our proposed method is the first instance of a hierarchical family of criteria for quantum steering that is valid for any dimension, and shares some similarity in spirit and structure with the hierarchy of moments by Shchukin and Vogel [161] for CV entanglement detection, and with the Navascués-Pironio-Acín hierarchy [162] for the characterization of nonlocal quantum correlations. We show that our approach provides optimal moment-based linear steering witnesses for any chosen states and measurements on both parties, including CV ones. Furthermore, various previously proposed steering criteria are retrieved as special cases of our unifying approach, while new non-linear criteria are derived. Finally, we consider several examples of both DV and CV states, and show that our technique allows to beat the current state-of-the-art in steering detection of a lossy single-photon entangled state with quadrature measurements [155].

8.2.1 Preliminaries

We consider the entanglement certification task in which two distant parties, Alice and Bob, each holding one half of a quantum state ρ_{AB} of a bipartite system (described by a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A, \mathcal{H}_B$ denote the Hilbert spaces of Alice and Bob respectively), want to verify that they share entanglement. Additionally to this, we impose the constraint that Alice's system is unknown (i.e., unknown $\mathcal{H}_A$), and her measurement devices cannot be trusted. This implies that the measurement outcomes Alice announces cannot be assumed to originate from a particular observable on some quantum state of known dimension. The usual entanglement criteria in this case are inapplicable and we need to consider steering criteria to identify any nonseparability between the untrusted Alice and the trusted Bob [12].

In this scenario, Alice performs one out of n unknown measurements (often called 'inputs') on her half of ρ_{AB}, labelled by $x = 1, \ldots, n$, and with probability $p(a|x)$ gets some outcome a. In principle, Alice's measurements are arbitrary, but one can restrict the analysis to projective measurements without losing generality, because the ancilla needed for a non-projective

measurement can always be moved to the definition of the local state on Alice's side. Alice announces the corresponding pair (a, x) to Bob, who then tomographically reconstructs his conditional local (unnormalized) state $\sigma^B_{a|x}$ which is of arbitrary, but known, dimension. Bob's states are defined so that $\mathrm{tr}(\sigma^B_{a|x}) = p(a|x)$. For all possible pairs (a, x), Bob thus obtains the set $\{\sigma^B_{a|x}\}$, called an 'assemblage' [156]. From the assemblage alone, they should judge whether entanglement was present between their shared systems. We refer to this procedure as a *steering test*.

More precisely, based on the observed assemblage, they must determine whether there exists a separable model, i.e., a separable state $\bar{\rho}_{AB} = \sum_\lambda q_\lambda \rho^A_\lambda \otimes \rho^B_\lambda$ on $\mathcal{H}^\star_A \otimes \mathcal{H}_B$, and measurements $\{M_{a|x}\}_x$ for Alice, that reproduce Bob's assemblage if we allowed for arbitrary Hilbert spaces $\mathcal{H}^\star_A$ on Alice. If such a model does not exist, then the shared state must be entangled. A steering test using a separable state $\bar{\rho}_{AB}$, and measurements $\{M_{a|x}\}_x$ associated to each input, necessarily leads to the following form for Bob's conditional (unnormalized) states,

$$\bar{\sigma}^B_{a|x} = \mathrm{tr}_A[(M_{a|x} \otimes \mathbb{I}_B)\bar{\rho}_{AB}] = \sum_\lambda q_\lambda \, p(a|x,\lambda)\rho^B_\lambda, \;\; \forall a, x, \tag{8.15}$$

where $p(a|x,\lambda) = \mathrm{tr}[M_{a|x}\rho^A_\lambda]$ and $p(a|x) = \mathrm{tr}[\bar{\sigma}^B_{a|x}]$. Assemblages of the form (8.15) are called *unsteerable* [12]. One can also prove that, given any unsteerable assemblage, there always exist a separable state and projective measurements for Alice that reproduce it. Furthermore Alice's measurements can be assumed to come from mutually commuting observables [163]. Intuitively, this follows from the fact that a separable model is 'classical' on Alice's side. Therefore, unsteerability is equivalent to the existence of such a separable model.

Our approach is based upon the fact that Bob's conditional states, $\sigma^B_{a|x}$, on which the steering test is based, are in general hard to obtain experimentally when the set of outcomes is large, or even continuous, as Bob would need to do tomography for every pair (a, x). To circumvent this problem we instead consider the more accessible correlations

$$\langle A^\varsigma_x \otimes B^\tau_y \rangle = \sum_{a,b} a^\varsigma \, b^\tau \, P(a, b|x, B_y) = \sum_a a^\varsigma \mathrm{tr}\left[\sigma_{a|x} B^\tau_y\right], \tag{8.16}$$

between the unknown observables $A_x = \sum_a a M_{a|x}$ (with $x = 1, \ldots, n$) measured by Alice, and some known observables B_y on $\mathcal{H}_B$ (with $y = 1, \ldots m$) measured by Bob, with outcomes (eigenvalues) b. In Eq. (8.16), $\varsigma, \tau \geq 0$ are integer powers, and $P(a, b|x, B_y)$ is the observed joint probability distribution. In what follows we will show how to derive tests for steering, based solely upon the observed correlations $\{\langle A^\varsigma_x \otimes B^\tau_y \rangle\}$.

8.2.2 Moment matrices

The main tool we will use is a *moment matrix*, defined as a $k \times k$ matrix $\mathbf{\Gamma}$ with elements

$$\Gamma_{ij} = \langle S_i^\dagger S_j \rangle , \tag{8.17}$$

where $i, j = 1, \ldots, k$, and each operator S_i is some (as-yet unspecified) product of operators for Alice and Bob. As a simple example, if Bob's system is a qubit, one could choose the set $\mathcal{S} = \{\mathbb{I} \otimes \mathbb{I}, A_1 \otimes X, A_2 \otimes Y, A_3 \otimes Z\}$ where Bob's observables X, Y, Z denote the three Pauli operators.

We first remark that such a moment matrix, when constructed from physical observables on quantum states, is always positive semidefinite, i.e. $\mathbf{\Gamma} \geq 0$. This follows immediately, since for any vector $\mathbf{v}$, with elements v_i,

$$\sum_{ij} v_i^* \langle S_i^\dagger S_j \rangle v_j = \left\langle \left(\sum_i v_i^* S_i^\dagger \right) \left(\sum_j S_j v_j \right) \right\rangle \geq 0.$$

The second crucial property is that if the underlying operators satisfy any algebraic properties, then the moment matrix inherits additional structure in the form of linear constraints. For example, if two (hermitian) operators commute, $[S_i, S_j] = 0$, then the corresponding elements of the moment matrix are necessarily equal, $\Gamma_{ij} = \langle S_i^\dagger S_j \rangle = \langle S_j^\dagger S_i \rangle = \Gamma_{ji}$. As a second example, if $S_i^\dagger S_j = i S_k$ and $S_1 = \mathbb{I}$, then $\Gamma_{ij} = \langle S_i^\dagger S_j \rangle = i \langle \mathbb{I}^\dagger S_k \rangle = i \Gamma_{1k}$. In the next section we show that these properties allow us to construct a steering test based upon moment matrices.

8.2.3 Novel detection method based on the moment matrix

Consider a steering test defined by a set of observed correlations (8.16) and take any set of operators $\mathcal{S}$ involving some unknown operators on Alice's untrusted side and known operators on Bob's trusted side. Now consider the unknown moment matrix $\mathbf{\Gamma}$ associate to $\mathcal{S}$ defined as in Eq. (8.17). Some of its matrix elements however are known as they correspond directly to observable data in the steering scenario: these include moments of the form (8.16), and moments of the form $\langle A_x^\varsigma \otimes B \rangle$, with B an arbitrary operator in Bob's trusted operators algebra [164, 165]. All the other elements are not directly available, since they involve products of Alice's unknown operators [166], and are treated as arbitrary (complex, in general) *free* parameters.

Our main goal is to check whether the observed data could be obtained or not by measurements on a separable state. On the level of the moment matrix, assuming that the observables

A_i commute imposes some extra linear constraints between the elements of Γ, as discussed above. Additionally, we can also impose other constraints on Γ given the knowledge of Bob's operators. The idea of our method then relies on searching for values for the free parameters of the constrained Γ that make it positive semidefinite. If no such values are found, then the data are incompatible with a model relying on commuting observables on Alice's side, and consequently no separable state could give rise to it.

More formally, let $\mathcal{R}$ denote a particular simultaneous assignment of values to all independent free parameters, and let $\mathbf{\Gamma}_{\mathcal{R}}$ denote the moment matrix for commuting measurement operators on Alice's side dependent on such an assignment. Then, steering is witnessed from $\mathbf{\Gamma}_{\mathcal{R}}$ if the latter cannot be made positive semidefinite for any possible assignment $\mathcal{R}$ of the free parameters, i.e.,

$$\mathbf{\Gamma}_{\mathcal{R}} \not\geq 0, \ \ \forall\, \mathcal{R} \quad \Rightarrow \quad \{\langle A_x^{\varsigma} \otimes B_y^{\tau} \rangle\} \text{ demonstrates steering.} \tag{8.18}$$

As anticipated, Eq. (8.18) is the central result of this Letter.

The proposed method for investigating steerability through moments of observables shows many advantages. First, it is valid for bipartite quantum systems of any dimension, be it discrete, continuous or even hybrid since everywhere Bob's Hilbert space was assumed arbitrary, while Alice was allowed for an arbitrary (discrete or continuous) set of outcomes. Second, the condition (8.18) serves as an infinite hierarchy of criteria; one may start with a small set of selected operators $\{S_i\}$, that are chosen at will, and can gradually increase this set by adding more moments to improve steering detection. In particular, the operators $\{S_i\}$ can be chosen from the set $\mathcal{S}$ of all strings (products) of operators of Alice's (unknown) observables, A_x and Bob's (known) observables B_y. This infinite set can naturally be partitioned into subsets $\mathcal{S}^{(k)}$ containing all strings of a given length k. For example, with only two operators on each side, $\mathcal{S}^{(0)} = \{\mathbb{I} \otimes \mathbb{I}\}$, $\mathcal{S}^{(1)} = \{A_1 \otimes \mathbb{I}, A_2 \otimes \mathbb{I}, \mathbb{I} \otimes B_1, \mathbb{I} \otimes B_2\}$, $\mathcal{S}^{(2)} = \{A_1A_2 \otimes \mathbb{I}, A_2A_1 \otimes \mathbb{I}, A_1 \otimes B_1, A_1 \otimes B_2, A_2 \otimes B_1, A_2 \otimes B_2, \mathbb{I} \otimes B_1B_2, \mathbb{I} \otimes B_2B_1\}$, etc. Third, checking whether there is any assignment of unknown parameters which makes a matrix positive semidefinite subject to linear constraints is an instance of a semidefinite program (SDP) which can be efficiently solved for many cases of interest. Moreover, the duality theory of SDPs allows us to extract linear inequalities which act as witnesses for steering.

8.2.4 Examples

In the following we consider various families of quantum states, and show that the proposed hierarchy generalizes and includes known steering criteria as special cases.

8.2.4.1 2×2 Werner states

Consider the class of discrete variable two-qubit Werner states [167],

$$\rho_{AB}(w) = w\,|\psi^-\rangle_{AB}\langle\psi^-| + \frac{(1-w)}{4}\,\mathbb{I}_{AB}, \tag{8.19}$$

where $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})$ is the singlet. To check their steerability, we construct the moment matrix (8.17) defined by the previously mentioned set of observables $\mathcal{S} = \{\mathbb{I} \otimes \mathbb{I}, A_1 \otimes X, A_2 \otimes Y, A_3 \otimes Z\}$ for Alice and Bob:

$$\mathbf{\Gamma}_{\mathcal{R}} = \begin{pmatrix} 1 & \langle A_1 \otimes X\rangle & \langle A_2 \otimes Y\rangle & \langle A_3 \otimes Z\rangle \\ \langle A_1 \otimes X\rangle & \langle A_1^2 \otimes X^2\rangle & \langle A_1A_2 \otimes XY\rangle & \langle A_1A_3 \otimes XZ\rangle \\ \langle A_2 \otimes Y\rangle & \langle A_2A_1 \otimes YX\rangle & \langle A_2^2 \otimes Y^2\rangle & \langle A_2A_3 \otimes YZ\rangle \\ \langle A_3 \otimes Z\rangle & \langle A_3A_1 \otimes ZX\rangle & \langle A_3A_2 \otimes ZY\rangle & \langle A_3^2 \otimes Z^2\rangle \end{pmatrix}. \tag{8.20}$$

Consider the statistics of Alice's unknown measurements A_1, A_2, A_3 to originate from spin-measurements X, Y, Z, respectively, on her share of ρ_{AB}. We observe that $\langle A_1^k \otimes B\rangle = \langle X^k \otimes B\rangle_{\rho_{AB}(w)}$, for $k = 1, 2$ and arbitrary B, and similarly for the observable elements that contain A_2^k and A_3^k. Furthermore, the commutativity requirement on Alice's side, together with the algebra of operators on Bob's side (e.g. $\langle A_1A_2 \otimes XY\rangle = -\langle A_2A_1 \otimes YX\rangle$), reduces the number of independent free parameters to three. One can then numerically check the positivity of the moment matrix and find that $\mathbf{\Gamma}_{\mathcal{R}} \not\geq 0$, $\forall \mathcal{R}$, for all $w > w_{\text{min}} = 1/\sqrt{3}$, which is known to be the threshold value for steering when Alice has exactly three inputs [148], as is the case here. The dual of the SDP gives the following *optimal steering witness*, for this family of states and measurements,

$$\langle A_1 \otimes X\rangle + \langle A_2 \otimes Y\rangle + \langle A_3 \otimes Z\rangle \geq -\sqrt{3}, \tag{8.21}$$

which is violated by all Werner states with $w > 1/\sqrt{3}$, while satisfied by all unsteerable states [163]. The steering criterion (8.21) was derived independently elsewhere [148], and we have shown that it is only a special case of our general approach.

Non-linear criteria can also be derived and, remarkably, in an analytical manner. A hermitian matrix is known to be positive semidefinite *iff* all its principal minors are non-negative

[74]. Since $\mathbf{\Gamma}_{\mathcal{R}}$ is by definition hermitian, $\mathbf{\Gamma}_{\mathcal{R}} \geq 0$ implies $\det \mathbf{\Gamma}_{\mathcal{R}} \geq 0$, that can be shown to be satisfied by all unsteerable assemblages *iff* [163]

$$\langle A_1 \otimes X \rangle^2 + \langle A_2 \otimes Y \rangle^2 + \langle A_3 \otimes Z \rangle^2 \leq 1. \tag{8.22}$$

When applied to $\rho_{AB}(w)$, steering detection is achieved for w down to the known threshold value $w_{\min} = 1/\sqrt{3}$. Moreover, based on the positivity of the principal minors of (8.20), other non-linear criteria can be derived with two (instead of three) dichotomic measurements per site [163].

8.2.4.2 Two-mode Gaussian states

Let us consider two-mode Gaussian states ρ^G_{AB}, introduced in Sec. 3.3, with a covariance matrix in the so-called standard form (3.67)

$$\bar{\boldsymbol{\sigma}}_{AB} = \begin{pmatrix} \bar{\mathbf{A}} & \bar{\mathbf{C}} \\ \bar{\mathbf{C}}^{\mathrm{T}} & \bar{\mathbf{B}} \end{pmatrix}, \tag{8.23}$$

where $\bar{\mathbf{A}} = \mathrm{diag}(a, a)$ and $\bar{\mathbf{B}} = \mathrm{diag}(b, b)$ are the marginal covariance matrices of Alice and Bob and $\bar{\mathbf{C}} = \mathrm{diag}(c_1, c_2)$ contains their correlations.

We proceed by investigating the steerability of Gaussian states in standard form (which implies the steerability of any non-Gaussian state with the same second moments thereof) using the following set of quadrature observables, $\mathcal{S} = \{A_1 \otimes \mathbb{I}, A_2 \otimes \mathbb{I}, \mathbb{I} \otimes q_B, \mathbb{I} \otimes p_B\}$, while we consider Alice's unknown measurements A_1, A_2 to originate from measurement of the quadratures q_A, p_A respectively. The corresponding moment matrix $\mathbf{\Gamma}$ (8.17) for Gaussian states in standard form becomes,

$$\mathbf{\Gamma}_{\mathcal{R}} = \frac{1}{16} \begin{pmatrix} a & \mathcal{R} & c_1 & 0 \\ \mathcal{R} & a & 0 & c_2 \\ c_1 & 0 & b & i \\ 0 & c_2 & -i & b \end{pmatrix}, \tag{8.24}$$

with $\mathcal{R} = \langle A_1 A_2 \rangle$ being the only unobservable free (real) parameter with commutativity imposed. We can proceed analytically, by remarking that if ρ^G_{AB} were nonsteerable then there would exist $\mathcal{R}$ such that $\mathbf{\Gamma}_{\mathcal{R}} \geq 0$ which implies $\det \mathbf{\Gamma}_{\mathcal{R}} \geq 0$. The latter, is equivalent to $\det \bar{\boldsymbol{\sigma}}_{AB} - \det \bar{\mathbf{A}} \geq \mathcal{R}^2 (\det \bar{\mathbf{B}} - 1) \geq 0$, where for the second inequality we used the property $\det \bar{\mathbf{B}} \geq 1$ that all physical states must satisfy [28]. Therefore, all unsteerable assemblages necessarily satisfy $\det \bar{\boldsymbol{\sigma}}_{AB} - \det \bar{\mathbf{A}} \geq 0$, while a violation would signal steering since there

exist no $\mathcal{R}$ able to make $\det \mathbf{\Gamma}_{\mathcal{R}}$ non-negative and consequently $\mathbf{\Gamma}_{\mathcal{R}}$ positive semidefinite. The steering condition $\det \bar{\sigma}_{AB} - \det \bar{\mathbf{A}} \geq 0$ derived here can be shown to be satisfied *iff* [12**?**],

$$\bar{\sigma}_{AB} + i(\mathbf{0}_A \oplus \mathbf{\Omega}_B) \geq 0, \tag{8.25}$$

which is precisely Wiseman *et al.*'s necessary and sufficient criterion for the steerability of Gaussian states under Alice's Gaussian measurements [12, 149]. Therefore, yet another criterion turns out to be a special case of our approach and this time in the CV regime. It is worth remarking that the derivation of (8.25) presented here made no assumptions about either Alice's uncharacterized system or the Gaussianity of Bob's subsystem (also, see [3]), in contrast to [12].

8.2.4.3 Lossy N00N states

Consider now the following class of lossy non-Gaussian CV bipartite quantum states,

$$\rho_{AB}^{(N)} = (1-\eta)\ |00\rangle_{AB}\langle 00| + \eta\ |N00N\rangle_{AB}\langle N00N|, \tag{8.26}$$

where $|N00N\rangle_{AB} = \frac{1}{\sqrt{2}}(|N0\rangle_{AB} - |0N\rangle_{AB})$ is the well-known *N00N* state useful in quantum metrology [168], whose imperfect preparation is modelled through a mixing with the vacuum with probability η. For later use, let us define position and momentum observables for each party $A(B)$, given N, as [169]

$$q_{A(B)}^{(N)} = \frac{1}{\sqrt{2}}(a_{A(B)}^{\dagger N} + a_{A(B)}^{N}),\ \ p_{A(B)}^{(N)} = \frac{i}{\sqrt{2}}\left(a_{A(B)}^{\dagger N} - a_{A(B)}^{N}\right),$$

satisfying $[q_{A(B)}^{(N)}, p_{A(B)}^{(N)}] = i$, with $[a_{A(B)}, a_{A(B)}^{\dagger}] = 1$.

For $N = 1$, Eq. (8.26) describes an entangled state produced by splitting a single photon (generated with probability η) at a 50-50 beam splitter. This state is of theoretical [170, 171] and experimental interest [172, 173], and it is very desirable to have an experimentally friendly criterion that allows one to certify some form of nonlocality in its correlations. To our knowledge, the current best steering detection for $\rho_{AB}^{(1)}$ using only quadrature measurements is achieved by a non-linear steering inequality proposed by Jones and Wiseman [155], which can detect steering down to $\eta \geq 0.77$ in the limit of Alice having an infinite number of inputs, while both Alice and Bob bin their outcomes (i.e. for a given outcome x, a value is assigned 0 if $x < 0$, and 1 if $x \geq 0$). For comparison, recently proposed entropic steering criteria [150], employing (unbinned) quadrature measurements for both parties, can be seen to detect steering

for a weaker $\eta \geq 0.94$, while all criteria that involve moments of quadratures up to second order fail to detect any steering at all [11, 12, 148]. We will show that our moment matrix approach outperforms all the previous methods for these states.

To make the comparison fair, we also consider that Alice only performs two quadrature measurements, but allow Bob to measure arbitrary *local* operators, see Appendix for discussion. To test for steering we use

$$\mathcal{S} = \{\mathbb{I}\otimes\mathbb{I}, A_0\otimes q_B, A_0\otimes p_B, A_1\otimes q_B, A_1\otimes p_B, A_0^2\otimes\mathbb{I}, A_1^2\otimes\mathbb{I}, \mathbb{I}\otimes q_B^2, \mathbb{I}\otimes q_B p_B, \mathbb{I}\otimes p_B q_B, \mathbb{I}\otimes p_B^2\},$$

with the observable data calculated assuming Alice's unknown measurements A_1, A_2 are the quadratures q_A, p_A respectively. Here, $q_{A(B)}$,$p_{A(B)}$ correspond to $q^{(N)}_{A(B)}$,$p^{(N)}_{A(B)}$ defined above, with $N = 1$. The set $\mathcal{S}$ defines an 11×11 moment matrix $\mathbf{\Gamma}$ (8.17), with two inputs A_1, A_2 associated to Alice. Following the steps of the detection method, with the observable elements of $\mathbf{\Gamma}$ computed from the state $\rho^{(1)}_{AB}$ [165], we employ SDP to efficiently check (8.18), and manage to detect steering for all η down to the critical value

$$\eta \geq \frac{2}{3} \equiv \eta_c, \tag{8.27}$$

which is lower than what previous methods can achieve. The dual of the SDP gives us the optimal linear steering inequality for $\rho^{(1)}_{AB}$, reported in the Appendix, that is violated for all $\eta \geq \frac{2}{3}$ and satisfied by all unsteerable assemblages. The proposed witness involves for Bob local moments of quadratures up to fourth order and can be efficiently measured by homodyne detection and linear optics [174, 175], therefore demonstrating the experimental feasibility of our proposal.

For any given $N > 1$, we can consider the same set $\mathcal{S}$, with corresponding observables $q^{(N)}_{A(B)}$, $p^{(N)}_{A(B)}$. We have tested our method up to $N = 6$ and observed a steering detection down to $\eta \geq \eta_c^{(N)}$, with $\eta_c^{(N)} \lesssim \frac{2}{3}$ (e.g., $\eta_c^{(6)} \approx 0.61$ for $N = 6$). We conjecture that steering be detectable with our method for all N, although larger values could not be tested due to computational limitations. We should note however that for $N > 1$ the observables $q^{(N)}_{A(B)}$, $p^{(N)}_{A(B)}$ correspond to non-Gaussian measurements that are hard to implement experimentally. On the other hand, for $N > 1$ the feasible quadrature measurements $q_{A(B)}$ and $p_{A(B)}$ could not detect steering in the states of Eq. (8.26) for any η and for the given set $\mathcal{S}$ considered above.

8.2.5 Discussion and conclusion

We proposed an infinite hierarchy of sufficient conditions for bipartite steering applicable to all quantum systems. Other previously known steering criteria were shown to be special cases of our approach, both in the discrete and continuous variable regimes. An optimal witness for an inperfect single-photon entangled state was obtained, which was shown to be more reluctant to losses than previous proposals, and experimentally accessible with linear optics and homodyne detection. In the light of a recently proved equivalence between steering and joint measurability [176, 177, 178], the hierarchy proposed here can also be used to test whether a set of Alice's inputs is not jointly measurable. An interesting future direction would be to extend the present method to multipartite steering detection, in a quantum network scenario with some trusted and some untrusted parties [179, 180, 181].

9

Quantification of Gaussian bipartite steering

Several experiments have been already performed, demonstrating steering and its asymmetry [182, 183, 184, 185, 186, 187, 188, 189, 190], and a number of recent studies have been devoted to improve our understanding of quantum steerability, ranging from the development of better criteria to detect steerable states [148, 150, 151, 191, 192], to the analysis of the distribution of steering among multiple parties [180, 193, 194, 195]. However unlike entanglement, for which a variety of operationally-motivated measures exist [64, 196], there is still a surprisingly scarce literature addressing the fundamental question of *quantifying* how steerable a given quantum state is [157, 158, 197].

In this chapter we present a novel comprehensive quantitative investigation of steerability in the archetypical setting of bipartite continuous variable systems, for which the very notion of EPR steering was originally debated and analyzed [11, 55]. We focus on a fully Gaussian scenario: namely, we consider generally mixed multimode bipartite Gaussian states, that constitute a distinctive corner of the infinite-dimensional Hilbert space [27, 28, 198], and study their steerability under Gaussian measurements [199, 200]. By analyzing the degree of violation of a necessary and sufficient criterion for Gaussian steerability [12, 149], we obtain a *computable* measure of Gaussian steering, and we investigate its properties. In the special case of two-mode Gaussian states, we characterize the maximum allowed steering asymmetry, we connect the measure operationally to the key rate of one-sided device-independent QKD [201], and we show that the Gaussian steering degree is upper bounded by the Gaussian Rényi-2 entanglement [202], with equality on pure states. Finally, we prove in general that (multi-

mode) bound entangled Gaussian states cannot be steered by Gaussian measurements, a result of relevance in view of the recent debate about a conjecture by Peres and its recently proposed strengthening by Pusey [156, 203, 204, 205]. The results of this chapter have been published in Physical Review Letters [2].

9.1 Preliminaries

We focus on a fully Gaussian scenario (see Sec 3.3, for details), where ρ_{AB} is a Gaussian state described by the CM

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathsf{T}} & \mathbf{B} \end{pmatrix}, \tag{9.1}$$

and Alice's measurement set $\mathcal{M}_A$ is also Gaussian (i.e., mapping Gaussian states into Gaussian states). A Gaussian measurement [200], which is generally implemented via symplectic transformations followed by balanced homodyne detection, can be described by a positive operator with a CM $\mathbf{T}^{R_A}$, satisfying $\mathbf{T}^{R_A} + i\,\boldsymbol{\Omega}_A \geq 0$. Every time Alice makes a measurement R_A and gets an outcome r_A, Bob's conditioned state $\rho_B^{r_A|R_A}$ is Gaussian with a CM given by $\mathbf{B}^{R_A} = \mathbf{B} - \mathbf{C}\left(\mathbf{T}^{R_A} + \mathbf{A}\right)^{-1}\mathbf{C}^{\mathsf{T}}$, independent of Alice's outcome.

It can be shown [12] that a general $(n+m)$-mode Gaussian state ρ_{AB} is $A \to B$ steerable by Alice's Gaussian measurements *iff* the condition

$$\boldsymbol{\sigma}_{AB} + i\,(\mathbf{0}_A \oplus \boldsymbol{\Omega}_B) \geq 0, \tag{9.2}$$

is violated. Writing this in matrix form, using (3.66), the nonsteerability inequality (9.2) is equivalent to two simultaneous conditions: (i) $\mathbf{A} > 0$, and (ii) $\mathbf{M}_\sigma^B + i\,\boldsymbol{\Omega}_B \geq 0$, where

$$\mathbf{M}_\sigma^B = \mathbf{B} - \mathbf{C}^{\mathsf{T}}\mathbf{A}^{-1}\mathbf{C} \tag{9.3}$$

is the Schur complement of $\mathbf{A}$ in the CM $\boldsymbol{\sigma}_{AB}$. Condition (i) is always verified since A is a physical CM. Therefore, σ_{AB} is $A \to B$ steerable *iff* the symmetric and positive definite $2m \times 2m$ matrix $\mathbf{M}_\sigma^B$ is not a *bona fide* CM, i.e., if condition (ii) is violated [12, 149]. By Williamson's theorem [206], $\mathbf{M}_\sigma^B$ can be diagonalized by a symplectic transformation $\mathbf{S}_B$ such that $\mathbf{S}_B\mathbf{M}_\sigma^B\mathbf{S}_B^{\mathsf{T}} = \mathrm{diag}\{\bar{\nu}_1^B, \bar{\nu}_1^B, \ldots, \bar{\nu}_m^B, \bar{\nu}_m^B\}$, where $\{\bar{\nu}_j^B\}$ are the symplectic eigenvalues of $\mathbf{M}_\sigma^B$, which can be determined by m local symplectic invariants [207]; alternatively, they can be computed as the orthogonal eigenvalues of the matrix $|i\boldsymbol{\Omega}_B\mathbf{M}_\sigma^B|$. The nonsteerability condition (9.2) is thus equivalent to $\bar{\nu}_j^B \geq 1$ for all $j = 1, \ldots, m$.

9.2 Gaussan steering measure

We then propose to *quantify* how much a a bipartite $(m+n)$-mode Gaussian state with CM $\boldsymbol{\sigma}_{AB}$ is steerable (by Gaussian measurements on Alice's side) via the following quantity

$$\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) := \max\left\{0, -\sum_{j:\bar{\nu}_j^B<1} \ln(\bar{\nu}_j^B)\right\}. \tag{9.4}$$

This quantity, hereby defined as Gaussian $A \to B$ steerability, is invariant under local unitaries (symplectic operations at the CM level), it vanishes *iff* the state described by σ_{AB} is nonsteerable by Gaussian measurements, and it generally quantifies the amount by which the condition (9.2) fails to be fulfilled. Clearly, a corresponding measure of Gaussian $B \to A$ steerability can be obtained by swapping the roles of A and B, resulting in an expression like (9.4), in which the symplectic eigenvalues of the $2n \times 2n$ Schur complement of $\mathbf{B}$, $\mathbf{M}_\sigma^A = \mathbf{A} - \mathbf{C}\,\mathbf{B}^{-1}\mathbf{C}^\mathsf{T}$, appear instead. We highlight the formal similarity with the formula for the logarithmic negativity [64, 196, 208, 209] —an entanglement measure we reviewed in Sec. 5.3.1 which quantifies how much the positivity of the partial transpose condition for separability is violated [69, 70, 210, 211]—for Gaussian states; in the latter case, however, the symplectic eigenvalues of the partially transposed CM are considered [196, 198, 208, 212].

The proposed measure of steering is easily computable for bipartite Gaussian states of an arbitrary number of modes. When the steered party, e.g. Bob in Eq. (9.4), has one mode only ($m = 1$), the Gaussian steerability acquires a particularly simple form. Indeed, in such a case, $\mathbf{M}_\sigma^B$ has a single symplectic eigenvalue, $\bar{\nu}^B = \sqrt{\det \mathbf{M}_\sigma^B}$; recalling that, by definition of Schur complement, $\det \boldsymbol{\sigma}_{AB} = \det \mathbf{A} \det \mathbf{M}_\sigma^B$, we have

$$\begin{aligned}\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) &= \max\left\{0, \tfrac{1}{2}\ln\tfrac{\det \mathbf{A}}{\det \boldsymbol{\sigma}_{AB}}\right\} \\ &= \max\left\{0, \mathcal{S}(\mathbf{A}) - \mathcal{S}(\boldsymbol{\sigma}_{AB})\right\},\end{aligned} \tag{9.5}$$

where we have introduced the Rényi-2 entropy $\mathcal{S}$, which for a Gaussian state with CM $\boldsymbol{\sigma}$ reads $\mathcal{S}(\boldsymbol{\sigma}) = \frac{1}{2}\ln(\det \boldsymbol{\sigma})$ [202]. For more details on the Gaussian Rényi-2 entropy, also see Sec. 5.3.2.

9.2.1 Properties

Interestingly, the quantity $\mathcal{S}(\mathbf{A}) - \mathcal{S}(\boldsymbol{\sigma}_{AB}) \equiv \mathcal{J}^{A\langle B}$ can be seen as a form of quantum *coherent information* [213], but with Rényi-2 entropies replacing the conventional von Neumann entropies. Thanks to this connection, we can now prove some valuable properties of the Gaussian steering measure (9.5) for $(n+1)$-mode Gaussian states, namely:

(a) $\mathcal{G}^{A\to B}$ is convex;

(b) $\mathcal{G}^{A\to B}$ is monotonically decreasing under quantum operations on the (untrusted) steering party Alice, and under local Gaussian operations on the (trusted) steer party Bob;

(c) $\mathcal{G}^{A\to B}$ is additive, i.e., $\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}\oplus\boldsymbol{\tau}_{AB}) = \mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) + \mathcal{G}^{A\to B}(\boldsymbol{\tau}_{AB})$;

(d) $\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) = \mathcal{E}(\boldsymbol{\sigma}^{p}_{AB})$ for $\boldsymbol{\sigma}^{p}_{AB}$ pure, and

(e) $\mathcal{G}^{A\to B}(\sigma_{AB}) \leq \mathcal{E}(\sigma_{AB})$ for σ_{AB} mixed, where $\mathcal{E}$ denotes the Gaussian Rényi-2 measure of entanglement [202]. The proof of (a) follows from the concavity of the Rényi-2 entropy. The proof of the first part of (b) follows from the fact that the Gaussian Rényi-2 coherent information $\mathcal{I}^{A\langle B}$ obeys the data processing inequality (which in turn is a consequence of the strong subadditivity of the Rényi-2 entropy $\mathcal{S}$ for Gaussian states) [202, 213], $\mathcal{I}^{A'\langle B} \leq \mathcal{I}^{A\langle B}$ if A' is obtained from A by the action of a Gaussian quantum channel. The proof of the second part of (b) is lengthier and is reported in the Appendix. Property (c) follows from straightforward linear algebra and the additivity of the logarithm. The proof of (d) is immediate, as for pure states $\mathcal{S}(\boldsymbol{\sigma}^{p}_{AB}) = 0$ and $\mathcal{E}(\boldsymbol{\sigma}^{p}_{AB}) = \mathcal{S}(\mathbf{A})$. Property (e) needs to be proven when $\mathcal{G}^{A\to B} > 0$, in which case $\mathcal{G}^{A\to B} = \mathcal{I}^{A\langle B}$. We recall from Sec. 5.3.2 that the Rényi-2 entanglement of a bipartite Gaussian state ρ_{AB} is defined via a Gaussian convex roof procedure [198, 202],

$$\mathcal{E}(\rho_{AB}) = \inf_{\{p_i,|\psi_i\rangle\}} \sum_i p_i \mathcal{S}(\mathrm{Tr}_B |\psi_i\rangle\langle\psi_i|),$$

where the pure states $\{|\psi_i\rangle\}$ are Gaussian; let us denote by $\{p'_i, |\psi'_i\rangle\}$ the optimal decomposition of ρ_{AB} which minimizes the Rényi-2 entanglement. We have then

$$\begin{aligned}\mathcal{E}(\rho_{AB}) &= \sum_i p'_i \mathcal{S}\left(\mathrm{Tr}_B |\psi'_i\rangle\langle\psi'_i|\right) = \sum_i p'_i \mathcal{I}^{A\langle B}\left(|\psi'_i\rangle\langle\psi'_i|\right)\\ &\geq \mathcal{I}^{A\langle B}\left(\sum_i p'_i |\psi'_i\rangle\langle\psi'_i|\right) = \mathcal{I}^{A\langle B}(\rho_{AB})\\ &= \mathcal{G}^{A\to B}(\rho_{AB}),\end{aligned} \tag{9.6}$$

where we used, in order, properties (d) and (a). Remarkably, properties (d) and (e) demonstrate that our measure of Gaussian steering respects the hierarchy of quantum correlations [12]. In the light of the recently developed resource theory of steering [214] properties (a) and (b) should be satisfied by any proper measure of steering, while properties (c) and (d) should be satisfied by any quantifier that respects the hierarchy of quantum correlations.

In the following, we specialize our attention onto the paradigmatic case of two-mode Gaussian states ($n = m = 1$), for which the degree of steering in both ways can be easily measured according to our definition: $\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) = \max\{0, \mathcal{S}(\mathbf{A}) - \mathcal{S}(\boldsymbol{\sigma}_{AB})\}$ and $\mathcal{G}^{B\to A}(\boldsymbol{\sigma}_{AB}) =$

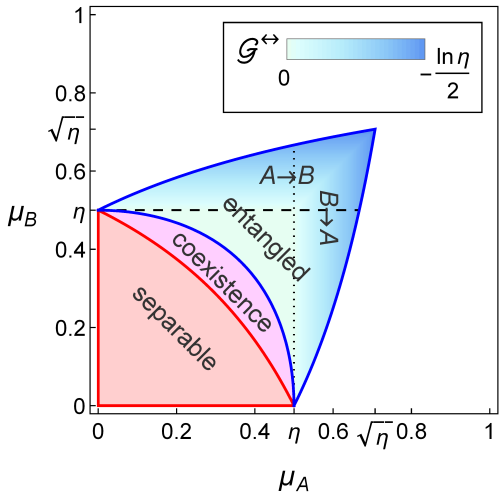

Figure 9.1: Classification of separability and Gaussian steerability of two-mode Gaussian states with marginal purities μ_A and μ_B and global purity $\mu = (\mu_A\mu_B)/\eta$, here plotted for $\eta = \frac{1}{2}$. By Gaussian measurements, states above the dashed line are $A \to B$ steerable and states to the right of the dotted line are $B \to A$ steerable. An overlay of the symmetrized degree of steerability $\mathcal{G}^{\leftrightarrow} \equiv \max\{\mathcal{G}^{A\to B}, \mathcal{G}^{B\to A}\}$ is depicted in the region of entangled states. See text for further details on the various regions and their boundaries.

$\max\{0, \mathcal{S}(\mathbf{B}) - \mathcal{S}(\boldsymbol{\sigma}_{AB})\}$. Qualification and quantification of steering in two-mode Gaussian states thus reduces entirely to an interplay between the global purity $\mu = 1/\sqrt{\det\boldsymbol{\sigma}_{AB}}$ and the two marginal purities $\mu_{A(B)} = 1/\sqrt{\det\mathbf{A(B)}}$. Introducing the ratio $\eta = (\mu_A\mu_B)/\mu$, all physical two-mode Gaussian states live in the region $\eta_0 \leq \eta \leq 1$ where $\eta_0 = \mu_A\mu_B + |\mu_A - \mu_B|$ [212]. States with $\eta_s \leq \eta \leq 1$ where $\eta_s = \mu_A + \mu_B - \mu_A\mu_B$ are necessarily separable, states with $\eta_e \leq \eta < \eta_s$ where $\eta_e = \sqrt{\mu_A^2 + \mu_B^2 - \mu_A^2\mu_B^2}$ can be entangled or separable (coexistence region), while states with $\eta_0 \leq \eta < \eta_e$ are necessarily entangled [212]. Within the latter region, states with $\eta \geq \{\mu_A, \mu_B\}$ are nonsteerable; states with $\eta < \mu_B$ are $A \to B$ steerable; states with $\eta < \mu_A$ are $B \to A$ steerable. This allows us to classify the separability and steerability (by Gaussian measurements) of all two-mode Gaussian states in the (μ_A, μ_B, η) space, completing the programme advanced a decade ago in [212, 215]. A cross-section of this insightful classification for $\eta = \frac{1}{2}$ is visualized in Fig. 9.1.

We have seen in general how steering can never exceed entanglement for Gaussian states (with one steered mode). It is interesting to investigate how *small* $\mathcal{G}^{A\to B}$ can also be for a given Rényi-2 entanglement $\mathcal{E}$, on arbitrary two-mode Gaussian states. To address this question we exploit the local-unitary-invariance of $\mathcal{G}^{A\to B}$, and consider without loss of generality its evalu-

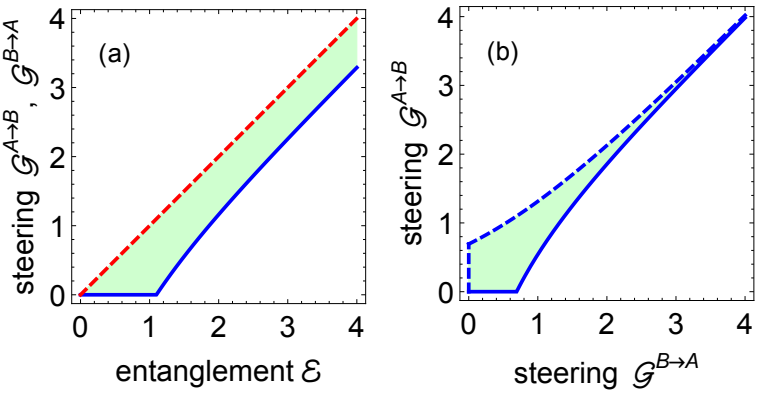

Figure 9.2: Plots of (a) Gaussian steerability versus Gaussian Rényi-2 entanglement and (b) $A \to B$ versus $B \to A$ Gaussian steerability, for two-mode Gaussian states. Physically allowed states fill the shaded (green) regions. Pure states $\boldsymbol{\sigma}^{p}_{AB}$ sit on the upper (dashed) boundary in panel (a); the lower (solid) boundaries in both plots accommodate extremal states $\boldsymbol{\sigma}^{x}_{AB}$, while swapping A and B in them one obtains states $\boldsymbol{\sigma}^{x}_{BA}$ which fill the upper boundary in (b).

ation on CMs (3.66) in standard form (3.67), characterized by $\mathbf{A} = \mathrm{diag}(a, a)$, $\mathbf{B} = \mathrm{diag}(b, b)$, $\mathbf{C} = \mathrm{diag}(c_1, c_2)$. We can then perform a constrained minimization of $\mathcal{G}^{A\to B}$ at fixed $\mathcal{E}$, over the covariances a, b, c_1, c_2, subject to the *bona fide* condition (3.27). We find that the extremal states sit on the boundary $\eta = \eta_0$, and have a CM $\boldsymbol{\sigma}^{x}_{AB}$ specified by

$$b = a - 1 + a/s, \quad c_1 = -c_2 = \sqrt{(a-1)(s+1)(a/s)},$$

with $a \geq s \geq 0$, in the limit $a \to \infty$. For these extremal states, $\mathcal{G}^{A\to B}(\sigma^{x}_{AB}) = \ln(s)$ and $\mathcal{E}(\sigma^{x}_{AB}) = \ln(2s+1)$. Analogous results hold for $\mathcal{G}^{B\to A}$. For all two-mode Gaussian states with a given $\mathcal{E}$, the steering measures thus admit an upper *and* a lower bound [see Fig. 9.2(a)],

$$\max\left\{0,\, \ln\left[\tfrac{1}{2}(e^{\mathcal{E}} - 1)\right]\right\} \leq \{\mathcal{G}^{A\to B},\, \mathcal{G}^{B\to A}\} \leq \mathcal{E}, \tag{9.7}$$

where the leftmost inequality is saturated on the extremal states σ^{x}_{AB}, and the rightmost one on pure (two-mode squeezed) states σ^{p}_{AB}, specified by $b = a$, $c_1 = -c_2 = \sqrt{a^2 - 1}$. This entails, in particular, that all two-mode Gaussian states with $\mathcal{E} > \ln 3 \approx 1.1$ are necessarily steerable in both ways; for highly entangled states, $\mathcal{E} \gg 0$, the Gaussian steering measure (in either way) remains bounded between $\mathcal{E}$ and $\mathcal{E} - \ln 2$.

The asymmetry of steering in the Gaussian setting has been experimentally demonstrated in [184, 216]. Clearly, $\mathcal{G}^{A\to B} \neq \mathcal{G}^{B\to A}$ in general, but how asymmetric can steerability be, at most, on two-mode Gaussian states? By maximizing the difference $|\mathcal{G}^{B\to A} - \mathcal{G}^{A\to B}|$ on standard form

CMs, we find quite intriguingly that the states endowed with maximum steering asymmetry are exactly the ones with CM σ_{AB}^{x} defined above, for which $\mathcal{G}^{A\to B} = \ln(s)$ and $\mathcal{G}^{B\to A} = \ln(s+1)$. For all two-mode Gaussian states, one has then

$$\max\{0,\, \ln[\exp(\mathcal{G}^{A\to B}) - 1]\} \leq \mathcal{G}^{B\to A} \leq \ln[\exp(\mathcal{G}^{A\to B}) + 1]. \tag{9.8}$$

This entails that the steering asymmetry $|\mathcal{G}^{B\to A} - \mathcal{G}^{A\to B}|$ can never exceed $\ln 2$, it is maximal when the state is nonsteerable in one way, and it decreases with increasing steerability in either way [see Fig. 9.2(b)].

9.2.2 Operational interpretation

We now investigate operational interpretations for the proposed steering quantifier(s) for two-mode Gaussian states. We observe from [12, 149] that our measures, evaluated on standard form CMs, are monotonic functions of the product of the (minimum) conditional variances associated to local homodyne detections, which appear in the seminal Reid criterion (7.8) for the EPR paradox [11] described in Chapter 7, namely,

$$4\, V_{Q_A|Q_B} V_{P_A|P_B} = \det \mathbf{M}_{\sigma}^{A} = \det \boldsymbol{\sigma}_{AB} / \det \mathbf{B}, \tag{9.9}$$

and,

$$4\, V_{Q_B|Q_A} V_{P_B|P_A} = \det \mathbf{M}_{\sigma}^{B} = \det \boldsymbol{\sigma}_{AB} / \det \mathbf{A}; \tag{9.10}$$

this renders $\mathcal{G}^{A\to B}$ and $\mathcal{G}^{B\to A}$ directly accessible experimentally. Notice a slight change of notation $\Delta^2_{\text{min}} Q_B \leftrightarrow V_{Q_B|Q_A}$ compared to Reid's criterion Eq. (7.8), in order to make clear the kind of measurement the steering party (here, Alice) performs. Similarly for the other variances.

We can then show that these measures find important applications for the task of one-sided device-independent QKD [217], which has been recently extended to continuous variables [201]. Considering the relevant entanglement-based protocol [218], let a two-mode entangled Gaussian state with CM $\boldsymbol{\sigma}_{AB}$ in standard form be shared between Alice and Bob, who want to establish a secret key. By performing homodyne detections on their modes, and a direct reconciliation scheme (where Alice sends corrections to Bob), they can achieve a secret key rate [201]

$$K \geq \max\left\{0,\, \ln\left(\frac{1}{e\sqrt{V_{Q_A|Q_B} V_{p_A|p_B}}}\right)\right\}. \tag{9.11}$$

This bound can be readily expressed in terms of the $B \to A$ Gaussian steerability of $\boldsymbol{\sigma}_{AB}$, yielding

$$K \geq \max\{0,\ \mathcal{G}^{B\to A}(\boldsymbol{\sigma}_{AB}) + \ln 2 - 1\}. \tag{9.12}$$

In the case of a reverse reconciliation protocol, the corresponding key rate (9.12) would involve $\mathcal{G}^{A\to B}$ rather than $\mathcal{G}^{B\to A}$. Therefore, the degree of Gaussian steerability defined here nicely quantifies the guaranteed key rate achievable within a practical one-sided device independent QKD setting, realizable with current optical technology [184, 201].

9.3 No-go theorem: steering bound entangled states

Finally, we address the more fundamental question of steerability of bound entangled Gaussian states. Peres conjectured that states whose entanglement cannot be distilled, i.e., bound entangled states [64], cannot violate any Bell inequality [203]. Recently, Pusey proposed a stronger conjecture, namely that bound entangled states cannot even display EPR steering [156]. Surprisingly, both conjectures have been now disproven, by identifying steerable [204] and nonlocal [205] bound entangled qudit states. However, the question stayed open for continuous variable systems, and we settle it in the Gaussian case. Let σ_{AB} be the CM of a general bound entangled $(n+m)$-mode Gaussian state. Any such state obeys the *bona fide* condition (3.27)

$$\boldsymbol{\sigma}_{AB} + i\ \boldsymbol{\Omega}_A \oplus \boldsymbol{\Omega}_B \geq 0,$$

as well as Simon's condition (5.8)

$$\boldsymbol{\sigma}_{AB} + i\,(-\boldsymbol{\Omega}_A) \oplus \boldsymbol{\Omega}_B \geq 0,$$

which amounts to positivity under partial transposition [70] (see, Sec. 5.2.2.1 for details). Adding the two matrix inequalities together, one obtains (twice) the nonsteerability condition (9.2). This remarkably simple proof yields a general no-go result: steering bound entangled Gaussian states by Gaussian measurements is impossible; i.e., the Peres-Pusey conjecture holds in a fully Gaussian scenario.

However, we only discussed about the effect of Gaussian measurements on Gaussian states, and the no-go theorem we proved is also constrained into that fully-Gaussian framework. A good question would then be, whether non-Gaussian measurements can steer a state that is unsteerable by Gaussian measurements and thus satisfies Eq. (9.2). Up to very recently it wasn't known whether Gaussian measurements are optimal for steering Gaussian states. They sure are

optimal in the case of entanglement, but are completely useless in the case of nonlocality, and as we discussed in Chapter 4, steering hierarchically falls in-between entanglement and nonlocality. It was finally shown in Refs. [216, 219], by constructing explicit examples of states and measurements, that Gaussian states are not optimal for steering; i.e., there exist Gaussian states that are unsteerable by Gaussian measurements, but are steerable if non-Gaussian measurements are considered.

9.4 Discussion and conclusion

In conclusion, we presented an intuitive and computable quantification of EPR steering [12] for bipartite Gaussian states under Gaussian measurements. We linked our measure to the key rate of one-sided device-independent QKD [201] and proved hierarchical relationships with entanglement. This work delivers substantial advances for the characterization of EPR steering and provides an important addition to the established framework of Gaussian quantum information theory [27, 28, 198]. In principle, our approach might be applied as well to general states: Namely, for a (non-Gaussian) bipartite state ρ_{AB}, one can define an indicator of steerability by Gaussian measurements as in Eq. (9.4), with σ_{AB} denoting the CM of the second moments of ρ_{AB}. This can be connected, in general, to the degree of violation of linear variance criteria for EPR steering [3, 11, 148, 149, 220]. In Chapter 10 we will show how to make such a generalization to non-Gaussian states. Notice however that a bipartite (non-)Gaussian state ρ_{AB} can still be steerable even if its $\mathcal{G}^{A\to B}$ vanishes. In particular, Gaussian states that are unsteerable by Gaussian measurements have recently been shown to be steerable by non-Gaussian measurements. Also, non-Gaussian states may possess EPR correlations only detectable via nonlinear criteria involving higher order moments [4, 148, 150]; for example, a two-qubit pure Bell state is clearly steerable but its CM fails to violate (9.2) (see Sec. 8.2.4.3).

The interplay between EPR steering [12], 'obesity' of steering ellipsoids [221], and other forms of asymmetric nonclassical correlations such as discord [50, 222, 223, 224], is worthy of further investigation. In Chapter 11 we generalize our analysis to multipartite settings [180], in order to derive quantitative monogamy inequalities for steering [194], complementing the existing ones for Gaussian entanglement [198, 202, 225] presented in Sec. 5.3.2.

10

Steering measure for arbitrary two-mode CV states

In this Chapter we present an accessible approach to the quantitative estimation of steerability for *arbitrary* bipartite two-mode continuous variable states and Gaussian (quadrature) measurements. These results will generalize the Gaussian steering measure introduced in Chapter 9, whose validity was restricted strictly to the Gaussian framework, to arbitrary states in the case of two modes. We examine recent experimental criteria for steering [148], the so-called EPR-Reid variance criteria whose applicability extends to all (Gaussian and non-Gaussian) states, and analyze their maximal violation by optimal local quadrature observables for Alice and Bob, in order to capture the largest possible departure from a local hidden state model description of the correlations,

$$P(A,B|a,b) = \sum_{\lambda} P(\lambda)P(A|a,\lambda)P_Q(B|,b\rho_\lambda). \tag{10.1}$$

Hence we define (in Section 10.1) a suitable measure of steering for an arbitrary two-mode state, and we prove that it admits an analytically computable lower bound that captures the degree of steerability of the given state by Gaussian measurements. The lower bound coincides with the Gaussian steering measure introduced in Chapter 9 [2], whose usefulness is here generalized from the Gaussian domain to arbitrary states. We prove Gaussian states to be in fact extremal [226], as they are minimally steerable among all states with the same covariance matrix, according to the measure proposed in this chapter. As a corollary of our analysis, we show (in Section 10.2) that a necessary and sufficient condition for steerability of Gaussian states under Gaussian measurements obtained by Wiseman *et al.* based on covariance matrices

[12, 149], remains valid as a sufficient steering criterion for arbitrary non-Gaussian states, and amounts to Reid's criterion [11, 220] when optimal Gaussian local observables are chosen for the latter. We conclude (in Section 10.3) with a summary of our results and an outlook of currently open questions motivated by the present analysis. This chapter is based on our work Ref. [3] published by the journal JOSA B.

10.1 A steering measure for two-mode states based on quadrature measurements

In general [227], a measure of steering should quantify how much the correlations of a quantum state depart from the expression in Eq. (10.1). Since a manifestation of these correlations can be observed by the violation of suitable EPR-steering criteria, one can get a quantitative estimation of the degree of steerability in a given state by evaluating the maximum violation of a chosen steering criterion as revealed by optimal measurements. One expects that the higher the violation (i.e., the amount of correlations), the more useful the state will be in tasks that use quantum steering as a resource.

In this chapter we consider an arbitrary state $\hat{\rho}_{AB}$ of a two-mode continuous variable system. The relevant steering criteria to our work will be exactly the multiplicative variance EPR-steering criteria [148] we studied in Sec. 8.1, tailored to the scenario where they correspond to Reid's criterion [11]. We consider Reid's scenario here, where Bob measures two canonically conjugate observables on his subsystem, $\hat{q}_B, \hat{p}_B$ with corresponding outcomes Q_B, P_B, and Alice tries to guess Bob's outcomes based on the outcomes of measurements on her own subsystem. As we showed in Sec. 8.1, following [148, 220], considering this scenario a bipartite state $\hat{\rho}_{AB}$ shared by Alice and Bob is steerable by Alice, i.e. "$A \to B$" steerable, if the condition

$$\Delta^2_{\text{min}} Q_B \; \Delta^2_{\text{min}} P_B \geq \frac{1}{4}, \tag{10.2}$$

on the inference variances of Bob, is violated. For the relevant definitions and notation we refer the reader back to the relevant sections 7.1.2 and 8.1.

Notice that the criterion (10.2) is independent of Alice's and Bob's first moments, since displacements of the form $Q_{A(B)} \to Q_{A(B)} + d_{A(B)}$ leave the inference variances (of both position and momentum) invariant as can be easily seen from the definition (8.1). Therefore, first moments will be assumed to be zero in the rest of the chapter without any loss of generality.

We remark that the EPR-steering criterion (10.2) is applicable to arbitrary states and is valid without any assumption on the Hilbert space of Alice's subsystem, as Bob just needs to identify two distinctly labelled measurements performed by Alice [148]. However, in order to keep our analysis accessible, we will further assume that Alice's allowed measurements are restricted to be quadrature ones, i.e., projections on the eigenbasis of (generally rotated) canonically conjugate operators $\hat{q}_A^\theta$ and $\hat{p}_A^\theta$, such that $[\hat{q}_A^\theta, \hat{p}_A^\theta] = i$ in natural units. Although quadrature measurements are not general and not necessarily optimal to detect steerability in all states, they are convenient from a theoretical point of view and can be reliably implemented in laboratory by means of homodyne detections.

One immediately sees that the product of variances in (10.2) is not invariant under local unitary operations (apart from displacements) by Alice and Bob, thus a state might be detected as more or less steerable if some local change of basis is implemented. In order to capture steerability in an invariant way, one can consider the maximum violation of (10.2) that a quantum state $\hat{\rho}_{AB}$ can exhibit, by minimizing the product $\Delta^2_{\text{min}} Q_B \; \Delta^2_{\text{min}} P_B$ over all local unitaries $U_{\text{local}} = U_A \otimes U_B$ for A and B applied to the state.

We then propose to *quantify* the "$A \to B$" steerability of an arbitrary two-mode CV state $\hat{\rho}_{AB}$ detectable by quadrature measurements, via the measure

$$\mathcal{S}^{A\to B}(\hat{\rho}_{AB}) = \max\left\{0, \, -\frac{1}{2}\ln 4\mathcal{F}\right\}, \tag{10.3}$$

where

$$\mathcal{F} = \min_{\{U_{\text{local}}\}} \Delta^2_{\text{min}} Q_B \, \Delta^2_{\text{min}} P_B. \tag{10.4}$$

The measure naturally quantifies the amount of violation of an optimized multiplicative variance EPR-steering criterion of the form (10.2) for an arbitrary state $\hat{\rho}_{AB}$. As one would expect from any proper quantifier of quantum correlations, the measure enjoys local unitary invariance by definition, and it vanishes for all states which are not "$A \to B$" steerable. Also, the reason for the choice of this particular functional form w.r.t. the product of the inference variances is to, as we show later, reduce to the previously proposed Gaussian steering measure $\mathcal{G}$ (10.12) when only second moments are considered.

Calculating $\mathcal{S}^{A\to B}$ in an analytical manner for an arbitrary state is still a difficult task. In general, given a quantum state, the minimization in $\mathcal{F}$ involves both Gaussian and non-Gaussian local unitaries for Alice and Bob, which correspond to violations of (10.2) by Gaussian and non-Gaussian quadrature measurements, respectively. It is possible, though, to obtain a computable lower bound to $\mathcal{S}^{A\to B}$ if one constrains the optimization to Gaussian unitaries only. The

lower bound, presented in the next subsection, will then provide a quantitative indication of the "$A \to B$" steerability of $\hat{\rho}_{AB}$ that can be demonstrated by Gaussian measurements on Alice's subsystem.

10.1.1 Lower bound

To obtain a lower bound for the steering measure $\mathcal{S}^{A\to B}(\hat{\rho}_{AB})$ in terms of second moments, we will show that, for arbitrary states $\hat{\rho}_{AB}$ with corresponding CM σ_{AB}, the product of inference variances $\Delta^2_{\text{inf}} Q_B \, \Delta^2_{\text{inf}} P_B$, acquires its minimum value when σ_{AB} is in the standard form (3.67)

$$\bar{\boldsymbol{\sigma}}_{AB} = \begin{pmatrix} \bar{\mathbf{A}} & \bar{\mathbf{C}} \\ \bar{\mathbf{C}}^{\mathrm{T}} & \bar{\mathbf{B}} \end{pmatrix}, \tag{10.5}$$

where $\bar{\mathbf{A}} = \text{diag}\,(a, a)$, $\bar{\mathbf{B}} = \text{diag}\,(b, b)$, and $\bar{\mathbf{C}} = \text{diag}\,(c_1, c_2)$. Let us begin by considering a steerable $\hat{\rho}_{AB}$ that violates (10.2), so that $\mathcal{S}^{A\to B}(\hat{\rho}_{AB}) > 0$. We use the fact that $\Delta^2_{\text{inf}} Q_B \geq \Delta^2_{\text{min}} Q_B$, when a linear estimator $Q_{\text{est}}(Q_A) = g_q Q_A + d_q$ is used in its definition (8.1); after minimizing the inference variance over the real numbers g_q, d_q and considering vanishing first moments without any loss of generality, we find $\Delta^2_{\text{inf}} Q_B = \langle Q_B^2 \rangle - \langle Q_B Q_A \rangle^2 / \langle Q_A^2 \rangle$ [220]. Similar considerations hold for the inference variance of momentum, where an estimator of the form $P_{\text{est}}(P_A) = g_p P_A + d_p$ will give $\Delta^2_{\text{inf}} P_B = \langle P_B^2 \rangle - \langle P_B P_A \rangle^2 / \langle P_A^2 \rangle$ after optimizing over the real numbers g_p, d_p.

Since a linear estimator is optimal for inferring the variance in the case of Gaussian states [11, 220], but not anymore in the general case, the inequality $\Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B \geq \Delta^2_{\text{min}} Q_B \Delta^2_{\text{min}} P_B$ will be true for all states (with equality on Gaussian states). Hence, $\mathcal{F}$ in (10.3) can be upper bounded as follows,

$$\begin{aligned} \mathcal{F} &= \min_{\{U_G\}\cup\{U_{nG}\}} \Delta^2_{\text{min}} Q_B \Delta^2_{\text{min}} P_B \\ &\leq \min_{\{U_G\}\cup\{U_{nG}\}} \Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B \\ &\leq \min_{\{U_G\}} \Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B, \end{aligned} \tag{10.6}$$

where we have decomposed the set of local unitaries $\{U_{\text{local}}\}$ into Gaussian $\{U_G\}$ and non-Gaussian $\{U_{nG}\}$ ones. The product of inference variances in (10.6) is intended as evaluated from the optimal linear estimator as detailed above [220], namely

$$\Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B = \left(\langle Q_B^2 \rangle - \frac{\langle Q_B Q_A \rangle^2}{\langle Q_A^2 \rangle} \right) \times \left(\langle P_B^2 \rangle - \frac{\langle P_B P_A \rangle^2}{\langle P_A^2 \rangle} \right), \tag{10.7}$$

Since an upper bound on $\mathcal{F}$ will give us the desired lower bound on $\mathcal{S}^{A\to B}$, what remains is to compute this upper bound, i.e., the rightmost quantity in (10.6), which only depends on the CM elements of the state.

Local Gaussian unitaries (that do not give rise to displacements) acting on states $\hat{\rho}_{AB}$, translate on the level of CMs as local symplectic transformations $\mathbf{S}_{\text{local}} = \mathbf{S}_A \oplus \mathbf{S}_B$, acting by congruence: $\boldsymbol{\sigma}_{AB} \mapsto \mathbf{S}_{\text{local}}\boldsymbol{\sigma}_{AB}\mathbf{S}_{\text{local}}^T$ [28, 228]. In order to compute $\min_{\{\mathbf{S}_{\text{local}}\}} \Delta_{\text{inf}}^2 Q_B \Delta_{\text{inf}}^2 P_B$ we can, with no loss of generality, consider a CM $\bar{\boldsymbol{\sigma}}_{AB}$ in standard form, apply an arbitrary local symplectic operation $\mathbf{S}_{\text{local}}$ to it, then evaluate $\Delta_{\text{inf}}^2 Q_B\, \Delta_{\text{inf}}^2 P_B$ on the transformed CM $\mathbf{S}_{\text{local}}\bar{\boldsymbol{\sigma}}_{AB}\mathbf{S}_{\text{local}}^{\text{T}}$, and finally minimize this quantity over all possible matrices $\mathbf{S}_{A(B)}$. To perform the minimization we parametrize the matrix elements of $\mathbf{S}_{A(B)}$ in the following convenient way,

$$\mathbf{S}_{A(B)} = \begin{pmatrix} \frac{1}{(1-u_{A(B)}v_{A(B)})w_{A(B)}} & \frac{v_{A(B)}}{(1-u_{A(B)}v_{A(B)})w_{A(B)}} \\ u_{A(B)}w_{A(B)} & w_{A(B)} \end{pmatrix} \tag{10.8}$$

where the symplectic condition $\mathbf{S}_{A(B)}\boldsymbol{\Omega}_{A(B)}\mathbf{S}_{A(B)}^{\text{T}} = \boldsymbol{\Omega}_{A(B)}$ has been taken into account and the real variables $u_{A(B)}, v_{A(B)}, w_{A(B)}$ are now independent of each other. Performing the (unconstrained) minimization over the variables $u_{A(B)}, v_{A(B)}$ we were able to obtain analytically the global minimum of the product (10.7) with respect to Gaussian observables,

$$4 \min_{\{U_G\}} \left[\Delta_{\text{inf}}^2 Q_B\, \Delta_{\text{inf}}^2 P_B\right] = \det \mathbf{M}_{\sigma}^{B}, \tag{10.9}$$

which also constitutes the upper bound for $\mathcal{F}$ in (10.6). Here the local symplectic invariant $\det \mathbf{M}_{\sigma}^{B} = \left(b - \frac{c_1^2}{a}\right)\left(b - \frac{c_2^2}{a}\right)$ is the determinant of the Schur complement of $\bar{\mathbf{A}}$ in $\bar{\boldsymbol{\sigma}}_{AB}$, first defined in Eq. (9.3) for any two-mode CM,

$$\mathbf{M}_{\sigma}^{B} = \mathbf{B} - \mathbf{C}^{\text{T}}\mathbf{A}^{-1}\mathbf{C}\,. \tag{10.10}$$

The minimum (A.12) can be obtained from every state using the following parameters that determine the local symplectic operations (10.8),

$$(u_A, v_A, u_B, v_B) = \left(\frac{c_1 v_B}{c_2},\ \frac{-ab+c_1^2}{ab-c_2^2}\frac{c_2 v_B}{c_1},\ \frac{-ab+c_1^2}{ab-c_2^2}v_B,\ v_B \right),$$

$\forall\ v_B, w_{A(B)}$. It is evident from (A.12) that the minimum product of inference variances (10.7) is achieved, in particular, when evaluated for a standard form CM $\bar{\boldsymbol{\sigma}}_{AB}$.

Substituting $4\mathcal{F} \leq \det \mathbf{M}_{\sigma}^{B}$ in (10.3), a lower bound for the proposed steering measure of an arbitrary two-mode state $\hat{\rho}_{AB}$ is obtained,

$$\mathcal{S}^{A\to B}(\hat{\rho}_{AB}) \geq \mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB})\,, \tag{10.11}$$

where we recognize the Gaussian steering measure introduced in Chapter 9,

$$\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) = \max\left\{0, -\frac{1}{2}\ln\det\mathbf{M}_{\sigma}^{B}\right\}. \tag{10.12}$$

The lower bound $\mathcal{G}^{A\to B}$ solely depends on local symplectic invariant quantities that uniquely specify the CM of the state. As is known [212], these invariant quantities can be expressed back with respect to the original elements of the CM which one can measure in laboratory, e.g. via homodyne tomography [229]. Henceforth, the lower bound that we obtained is both analytically computable and, also, experimentally accessible in a routinely fashion for any (Gaussian or non-Gaussian) state, since only moments up to second order are involved.

In the following we discuss some useful properties that the steering measure $\mathcal{S}^{A\to B}$ and its lower bound $\mathcal{G}^{A\to B}$ satisfy, and show how these results can be used to link and generalize existing steering criteria.

10.1.2 Properties

In Chapter 9 we introduced a measure of EPR-steering for multi-mode bipartite Gaussian states that dealt with the problem of "*how much a Gaussian state can be steered by Gaussian measurements*". This measure $\mathcal{G}^{A\to B}$ was defined as the amount of violation of the following criterion by Wiseman *et al.* [12, 149],

$$\boldsymbol{\sigma}_{AB} + i\,(\mathbf{0}_A \oplus \boldsymbol{\Omega}_B) \geq 0. \tag{10.13}$$

Violation of (10.13) gives a necessary and sufficient condition for "$A \to B$" steerability of Gaussian states by Gaussian measurements. We recall from the original papers [12, 149], where the details can be found, that for two modes the condition (10.13) is violated *iff* $\det\mathbf{M}_{\sigma}^{B} < 1$, hence equivalently *iff* $\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) > 0$, where the Gaussian steering measure is defined in (10.12). In a two-mode continuous variable system, a non-zero value of Gaussian steering $\mathcal{G}^{A\to B} > 0$ detected on a CM $\boldsymbol{\sigma}_{AB}$, which implies a non-zero value of the more general measure $\mathcal{S}^{A\to B} > 0$ due to (10.11), constitutes therefore not only a necessary and sufficient condition for the steerability by Gaussian measurements of the Gaussian state $\hat{\rho}_{AB}^{G}$ defined by $\boldsymbol{\sigma}_{AB}$, but also a sufficient condition for the steerability of all (non-Gaussian) states $\hat{\rho}_{AB}$ with the same CM $\boldsymbol{\sigma}_{AB}$.

While $\mathcal{S}^{A\to B}$ is hard to study in complete generality, its lower bound $\mathcal{G}^{A\to B}$, however, was shown in Sec. 9.2.1 to satisfy a plethora of valuable properties. The present chapter, thus, validates all the already established properties of $\mathcal{G}^{A\to B}$ as an indicator of steerability by Gaussian measurements, and extends them to arbitrary states.

Interestingly, Ineq. (10.11) suggests that by accessing only the second moments of an arbitrary state, one will not overestimate its steerability according to our measure. We can make this observation rigorous by showing that the steering quantifier $\mathcal{S}^{A\to B}$ satisfies an important *extremality* property as formalized in [226]. Namely, the Gaussian state $\hat{\rho}^{G}_{AB}$ defined by its CM σ_{AB} minimizes $\mathcal{S}^{A\to B}$ among all states $\hat{\rho}_{AB}$ with the same CM σ_{AB}. This follows by recalling that the value of the Reid product (10.7), which appears in (10.6), is independent from the (Gaussian versus non-Gaussian) nature of the state, and that linear inference estimators are globally optimal for Gaussian states as mentioned above [220]. This entails that the middle term in (10.6) can be recast as

$$\begin{aligned} &\min_{\{U_G\}\cup\{U_{nG}\}} (\Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B)_{\hat{\rho}_{AB}} \\ &= \min_{\{U_G\}\cup\{U_{nG}\}} (\Delta^2_{\text{inf}} Q_B \Delta^2_{\text{inf}} P_B)_{\hat{\rho}^{G}_{AB}} \\ &= \min_{\{U_G\}\cup\{U_{nG}\}} (\Delta^2_{\text{min}} Q_B \Delta^2_{\text{min}} P_B)_{\hat{\rho}^{G}_{AB}} \\ &= \mathcal{F}(\hat{\rho}^{G}_{AB}) , \end{aligned} \tag{10.14}$$

where, for the sake of clarity, we have explicitly indicated the states on which the variances are calculated: $\hat{\rho}_{AB}$ denotes an arbitrary two-mode state, and $\hat{\rho}^{G}_{AB}$ corresponds to the reference Gaussian state with the same CM.

Therefore, combining Eqs. (10.3), (10.6), (10.11), and (10.14), we can write the following chain of inequalities for the "$A \to B$" steerability of an arbitrary two-mode state $\hat{\rho}_{AB}$,

$$\mathcal{S}^{A\to B}(\hat{\rho}_{AB}) \geq \mathcal{S}^{A\to B}\left(\hat{\rho}^{G}_{AB}\right) \geq \mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) \ . \tag{10.15}$$

The leftmost inequality in (10.15) embodies the desired extremality property [226] for our steering measure. This is very relevant in a typical experimental situation, where the exact nature of the state $\hat{\rho}_{AB}$ is mostly unknown to the experimentalist. Then, thanks to (10.15) we rest assured that, by assuming a Gaussian nature of the state under scrutiny, the experimentalist will never overestimate the EPR-steering correlations between Alice and Bob as quantified by the measure defined in (10.3).

Finally, coming to operational interpretations for our proposed steering quantifier $\mathcal{S}^{A\to B}$, we show that it is connected to the figure of merit of one-sided device independent quantum key distribution [201], that is, the secret key rate. In the conventional entanglement-based quantum cryptography protocol [218], Alice and Bob share an arbitrary two-mode state $\hat{\rho}_{AB}$, and want to establish a secret key given that Alice does not trust her devices. By performing

local measurements (typically homodyne detections) on their modes, and a direct reconciliation scheme (where Bob sends corrections to Alice) they can achieve the secret key rate [201]

$$K \geq \max\left\{0,\ \ln\left(\frac{1}{e\sqrt{\Delta_{\text{inf}}^2 Q_B \Delta_{\text{inf}}^2 P_B}}\right)\right\}. \tag{10.16}$$

Notice that the secret key rate depends on the expression in (10.7), which is not unitarily invariant. Therefore, it can be optimized over local unitary operations. In the case where $\Delta_{\text{inf}}^2 Q_B \Delta_{\text{inf}}^2 P_B$ takes its minimum value for the given shared $\hat{\rho}_{AB}$, the lower bound on the correspondingly optimal key rate K_{opt} can be readily expressed in terms of the "$A \to B$" steerability measure, yielding

$$K_{\text{opt}} \geq \max\{0,\ \mathcal{S}^{A\to B}(\hat{\rho}_{AB}) + \ln 2 - 1\}. \tag{10.17}$$

Thus, $\mathcal{S}^{A\to B}$ quantifies a guaranteed key rate for any given state. If a reverse reconciliation protocol is used (in which Alice sends corrections to Bob) the quantifier $\mathcal{S}^{B\to A}$ of the inverse steering direction enters (10.17) instead. Thus, one sees that the asymmetric nature of steering correlations can play a decisive role in communication protocols that rely on them as resources. In the cryptographic scenario discussed, if the shared state $\hat{\rho}_{AB}$ is only one-way steerable, say $A \to B$, then a reverse reconciliation protocol that relies on $\mathcal{S}^{B\to A}$ is not possible. A looser lower bound to the key rate (10.17) can also be expressed in terms of $\mathcal{G}^{A\to B}$ by using (10.11), in case one wants to study the advantage that Gaussian steering alone gives for the key distribution, or one just wants to get an estimate.

10.2 Reid, Wiseman, and a stronger steering test

Finally, we discuss the implications of our work on existing EPR-steering criteria [11, 12]. The second order EPR-steering criteria by Reid (10.2) and Wiseman *et al.* (10.13), are perhaps the most well-known ones for continuous variable systems. Although a comparison between them has been issued before in a special case (two-mode Gaussian states in standard form) [149], they appear to exhibit quite distinct features in general [148]. On one hand, Wiseman *et al.*'s criterion (10.13), defined only in the Gaussian domain, is invariant under local symplectics and provides a necessary and sufficient condition for steerability of Gaussian states under Gaussian measurements. On the other hand, Reid's criterion (10.2) is applicable to all states but is not invariant under local symplectics and as a result it cannot always detect steerability even on a Gaussian state. As an illustrative example, we show in Fig. 10.1 the performance of the

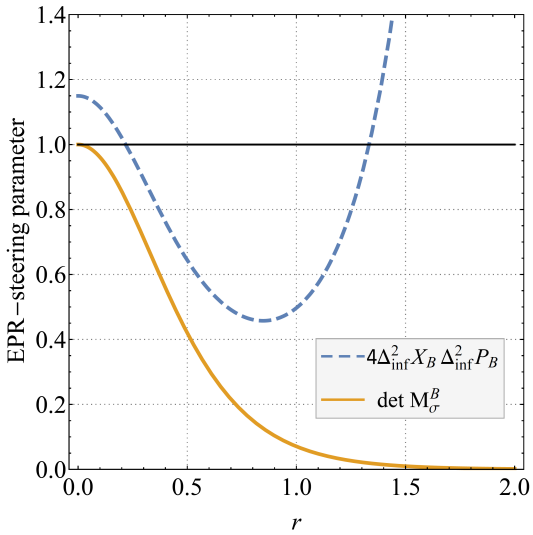

Figure 10.1: We illustrate the performance of Reid's [11] and Wiseman *et al.*'s [12] EPR-steering criteria for the steering detection of a pure two-mode squeezed state with squeezing r (see Sec. 3.3.2.5, for details on these states) , with CM transformed from the standard form by the application of a local symplectic transformation parameterized as in (10.8), with $u_{A(B)} = v_{A(B)}/(1 + v^2_{A(B)})$, $w_{A(B)} = 1 + v^2_{A(B)}$ (in the plot, we choose $v_A = 0.16$ and $v_B = 0.19$). The criteria are represented by their figures of merit, namely the product of conditional variances (dashed blue line) for Reid's criterion (10.2) and the determinant $\det \mathbf{M}_B$ (solid orange line) for Wiseman *et al.*'s criterion (10.13). The two-mode squeezed state is steerable for all $r > 0$, but the aforementioned criteria detect this steerability only when their respective parameters give a value smaller than unity (straight black line). As one can see, we have $\det \mathbf{M}_B < 1$ for all $r > 0$ and independently of any local rotations, while Reid's criterion detects steerability only for a small range of squeezing degrees and is highly affected by local rotations. If the state is sufficiently rotated out of the standard form, the unoptimized Reid's criterion will not be able to detect any steering at all.

two criteria for steering detection in a pure two-mode squeezed state, locally rotated out of its standard form. One can clearly see that Wiseman *et al.*'s criterion is superior to the non-optimized Reid's one, which fails to detect steering in the regimes of very low or very high squeezing [230].

However, it was previously argued [148] that Wiseman *et al.*'s stronger condition could not qualify as a general steering test, and could not be used in an experimental scenario where sources of non-Gaussianity may be present, since the derivation of the criterion and its validity were limited strictly to the Gaussian domain, while general EPR-steering tests should be defined for all states and measurements. The exact connection established by (A.12) between Wiseman *et al.*'s figure of merit, $\det \mathbf{M}^B_\sigma$, and Reid's product of inference variances (10.7),

makes us realize now that the two criteria are just two sides of the same coin; i.e., Wiseman *et al.*'s criterion represents the best performance of Reid's criterion when optimal Gaussian observables are used for the latter. As a byproduct of this connection, we have thus upgraded the validity of Wiseman *et al.*'s criterion to arbitrary two-mode continuous variable states. Namely, our results imply that a violation of (10.13) on any state $\hat{\rho}_{AB}$ with CM $\boldsymbol{\sigma}_{AB}$ is sufficient to certify its "$A \to B$" steerability, as detectable in laboratory by optimal quadrature measurements. This condition can be thus regarded, to the best of our current knowledge, as the strongest experimentally friendly EPR-steering test for arbitrary two-mode states involving moments up to second order.

10.3 Discussion and conclusion

We introduced a quantifier of EPR-steering for arbitrary bipartite two-mode continuous-variable states, that can be estimated both experimentally and theoretically in an analytical manner. Gaussian states were found to be extremal with respect to our measure, minimizing it among all continuous variable states with fixed second moments [226]. By further restricting to Gaussian measurements, we obtained a computable lower bound for any (Gaussian or non-Gaussian) two-mode state, that was shown to satisfy a plethora of good properties [2]. The measure proposed in this chapter is seen to quantify a guaranteed key rate of one-sided device independent quantum key distribution protocols [201]. Finally, this work generalizes and sheds new light on existing steering criteria based on quadrature measurements [11, 12].

Nevertheless many questions still remain, complementing the ones posed previously in [2]. To begin with, it would be worthwhile to extend the results presented here to multi-mode states and see whether a connection similar to Eq. (A.12) still holds. We also leave for further research the possibility that our quantifier (or its lower bound) may enter in other figures of merit for protocols that consume steering as a resource, like the tasks of secure quantum teleportation and teleamplification of Gaussian states [194, 231] or entanglement-assisted Gaussian subchannel discrimination with one-way measurements [157]. Moreover, the proved connection of the measure with entropic quantities in the purely Gaussian scenario could be an instance of a more general property that we believe is worth investigating, possibly making the link with the degree of violation of more powerful (nonlinear) entropic steering tests [150, 151].

11

Multipartite steering, monogamy and cryptographical applications

We derive laws for the distribution of quantum steering among different parties in multipartite Gaussian states under Gaussian measurements. We prove that a monogamy relation akin to the generalized Coffman-Kundu-Wootters inequality holds quantitatively for a recently introduced measure of Gaussian steering. We then define the residual Gaussian steering, stemming from the monogamy inequality, as an indicator of collective steering-type correlations. For pure three-mode Gaussian states, the residual acts a quantifier of genuine multipartite steering, and is interpreted operationally in terms of the guaranteed key rate in the task of secure quantum secret sharing. Optimal resource states for the latter protocol are identified, and their possible experimental implementation discussed. Our results pin down the role of multipartite steering for quantum communication. This chapter is based on our work Ref. [5] which is currently under peer review.

11.1 Preliminaries

With the imminent debacle of Moore's law, and the constant need for faster and more reliable processing of information, quantum technologies are set to radically change the landscape of modern communication and computation. A successful and secure quantum network relies on quantum correlations distributed and shared over many sites [127]. Different kinds of multipartite quantum correlations have been considered as valuable resources for various applications in quantum communication tasks. Multipartite entanglement [232, 233, 234, 235, 236, 237, 238]

and multipartite Bell nonlocality [239, 240, 241, 242] are two well known instances and have received extensive attention in recent developments of quantum information theory, as well as in other branches of modern physics. There has been substantial experimental progress in engineering and detection of both such correlations, by using e.g. photons [243, 244, 245, 246, 247], ions [248], or continuous variable (CV) systems [249, 250, 251, 252]. However, as an intermediate type of quantum correlation between entanglement and Bell nonlocality, multipartite quantum steering [253, 254] still defies a complete understanding. In consideration of the intrinsic relevance of the notion of steering to the foundational core of quantum mechanics, it has become a worthwhile objective to deeply explore the characteristics of multipartite steering distributed over many parties, and to establish what usefulness to multiuser quantum communication protocols can such a resource provide, where bare entanglement is not enough and Bell nonlocality may not be accessible.

The concept of quantum steering was originally introduced by Schrödinger [255] to describe the "spooky action-at-a-distance" effect noted in the Einstein-Podolsky-Rosen (EPR) paradox [55, 220, 256], whereby local measurements performed on one party apparently adjust (steer) the state of another distant party. Recently identified as a distinct type of nonlocality [12, 149], quantum steering is thus a directional form of quantum correlations, characterized by its inherent asymmetry between the parties [2, 4, 257, 258, 259, 260, 261]. Additionally, steering allows verification of entanglement, without assumptions of the full trust of reliability of equipment at all of the nodes of a communication network [148]. Steering is then a natural resource for one-sided device-independent quantum key distribution [201, 262]. For bipartite systems, a comprehensive quantitative investigation of quantum steering has been recently proposed [3, 263, 264, 265] and tested in several systems [189, 216, 266, 267, 268, 269**?**]. Comparatively little is known about steering in multipartite scenarios. For instance, Refs. [180, 270, 271] derived criteria to detect genuine multipartite steering, and Ref. [272] presented some limitations on joint quantum steering in tripartite systems.

Here we extend our studies of bipartite steering presented in Chapters 9 and 10, and we focus on steerability of multipartite Gaussian states of CV systems by Gaussian measurements, a physical scenario which is of primary relevance for experimental implementations [27, 198, 273]. In order to investigate the shareability of Gaussian steering from a quantitative perspective [2], we establish *monogamy* relations imposing constraints on the degree of bipartite EPR steering that can be shared among N-mode CV systems in Gaussian states,

in analogy with the Coffman-Kundu-Wootters (CKW) monogamy inequality for entanglement [236, 237, 274, 275, 276, 277]. We further propose an indicator of collective steering-type correlations, the *residual Gaussian steering* (RGS), stemming from the laws of steering monogamy, that is shown to act as a quantifier of genuine multipartite steering for pure three-mode Gaussian states. Finally, we show how the RGS acquires an operational interpretation in the context of a partially device-independent quantum secret sharing (QSS) protocol [6, 13, 169]. Specifically, taking into account arbitrary eavesdropping and potential cheating strategies of some of the parties [6], the achievable key rate of the protocol is shown to admit tight lower and upper bounds which are simple linear functions of the RGS. This in turn allows us to characterize optimal resources for CV QSS in terms of their multipartite steering degree.

11.2 Monogamy of Gaussian steering

A fundamental property of entanglement, that has profound applications in quantum communication, is known as monogamy [278]. Any two quantum systems that are maximally entangled with each other, cannot be entangled (or, even, classically correlated) with any other third system. Therefore, entanglement cannot be freely shared among different parties. In their seminal paper [274], CKW derived a monogamy inequality that quantitatively describes this phenomenon for any finite entanglement shared among arbitrary three-qubit states ρ

$$\mathcal{C}^2_{A:(BC)}(\rho) \geq \mathcal{C}^2_{A:B}(\rho) + \mathcal{C}^2_{A:C}(\rho), \tag{11.1}$$

where $\mathcal{C}^2_{A:(BC)}(\rho)$ is the squared concurrence, quantifying the amount of bipartite entanglement across the bipartition $A:(BC)$. Osborne and Verstraete later generalized the CKW monogamy inequality to n qubits [276]. For CV systems, however, both the quantification and the study of the distribution of entanglement constitute in general a considerably harder problem. Remarkably, if one focuses on the theoretically and practically relevant class of Gaussian states, various results similar to the qubit case have been derived, using different entanglement measures [198, 236, 237, 275, 277, 279]. Of particular interest to us will be the fact that the Gaussian Rényi-2 entanglement monotone $\mathcal{E}_{A:B}(\rho_{AB})$ introduced in Sec. 5.3.2, which quantifies entanglement of bipartite Gaussian states ρ_{AB}, has been shown to obey a CKW-type monogamy inequality (5.38) for all m-mode Gaussian states $\rho_{A_1\ldots A_m}$ with covariance matrix (CM) $\boldsymbol{\sigma}_{A_1\ldots A_m}$ [277],

$$\mathcal{E}_{A_k:(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\boldsymbol{\sigma}_{A_1\ldots A_m}) - \sum_{j\neq k} \mathcal{E}_{A_k:A_j}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \geq 0, \tag{11.2}$$

where each A_j comprises one mode only.

Quantum steering is a type of correlation that allows for entanglement certification in a multi-mode bipartite state ρ_{AB} even when one of the parties' devices, say Bob's, are completely uncharacterized (untrusted). In this case, we say that Bob can steer Alice's local state [12, 149]. Keeping our focus on Gaussian states and measurements [2], the question, thus, naturally arises: is steering monogamous? Intuitively one would expect that there should exist limitations on the distribution of steering-type correlations, since steering is only a stronger form of the already monogamous entanglement. A partial answer to this question was recently given by Reid [272], who showed that, under restrictions to measurements and detection criteria involving up to second order moments, if a single-mode party A can be steered by a single-mode party B then no other single-mode party C can simultaneously steer A. This was recently generalized to the case of parties B and C comprising an arbitrary number of modes [280].

In the following we provide general quantitative limitations to the distribution of Gaussian steering among many parties, complementing the previous qualitative analysis. For our purposes, we will focus on the Gaussian steering measure introduced in Chapter 9, $\mathcal{G}^{B\to A}(\boldsymbol{\sigma}_{AB})$, which quantifies how much party B can steer party A in a Gaussian state with CM $\boldsymbol{\sigma}_{AB}$ by Gaussian measurements. In particular, we now show that the Gaussian steering measure $\mathcal{G}$ is monogamous, hence satisfies a CKW-type monogamy inequality in direct analogy with entanglement. Consider an arbitrary (pure or mixed) m-mode Gaussian state $\rho_{A_1\ldots A_m}$ with CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$, where each party A_j comprises a single mode ($n_j = 1,\ \forall j = 1,\ldots,m$). Then, the following inequalities hold, $\forall\, k = 1,\ldots,m$:

$$\mathcal{G}^{(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) - \sum_{j\neq k}\mathcal{G}^{A_j\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \;\geq\; 0, \tag{11.3}$$

$$\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\boldsymbol{\sigma}_{A_1\ldots A_m}) - \sum_{j\neq k}\mathcal{G}^{A_k\to A_j}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \;\geq\; 0. \tag{11.4}$$

For pure states with CM $\boldsymbol{\sigma}^{\text{pure}}_{A_1\ldots A_m}$, the proof is straightforward. Namely, recall from [2] that the leftmost terms of (11.3), (11.4) and (11.2) all coincide on pure states. On the other hand, for the marginal states of any two modes i and j one has $\mathcal{E}_{A_i:A_j}\left(\boldsymbol{\sigma}^{\text{pure}}_{A_1\ldots A_m}\right) \geq \mathcal{G}^{A_i\to A_j}\left(\boldsymbol{\sigma}^{\text{pure}}_{A_1\ldots A_m}\right)$ [2]. Inequalities (11.3) and (11.4) then follow readily from the monogamy inequality (11.2) for Gaussian entanglement. The above inequalities are extended to mixed states in Appendix F.

The monogamy inequalities just derived impose additional restrictions to the distribution of Gaussian steering among multiple parties, on top of the ones given in Refs. [272, 280].

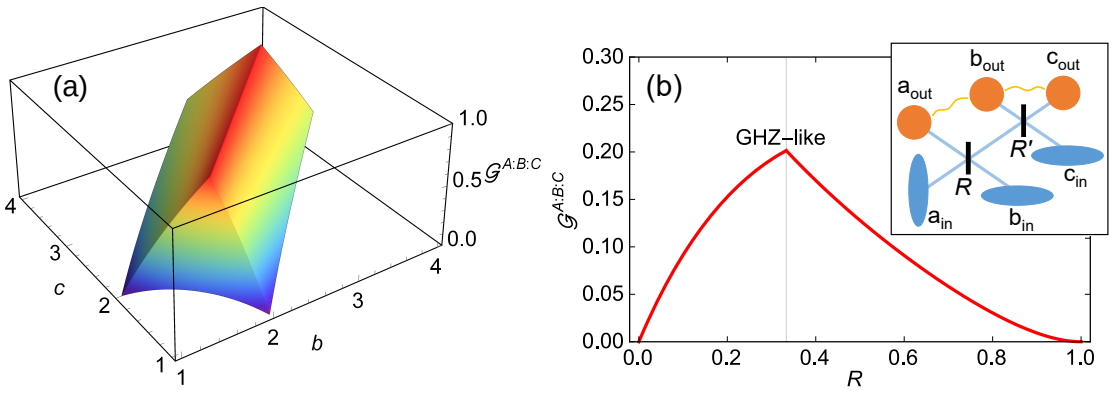

Figure 11.1: Residual tripartite Gaussian steering $\mathcal{G}^{A:B:C}$ for pure three-mode Gaussian states with CM $\boldsymbol{\sigma}_{ABC}^{\text{pure}}$ (a) with fixed $a = 2$ (local variance of subsystem A), and (b) generated by three squeezed vacuum fields at -3 dB injected in two beamsplitters with reflectivities R and R' (see inset), setting $R' = 1/2$ to obtain $b = c$; the permutationally invariant GHZ-like state ($a = b = c$) is obtained at $R = 1/3$.

To analyze these restrictions in more detail, let us focus on a tripartite scenario, in which the monogamy inequalities take the simpler form,

$$\mathcal{G}^{(AB)\to C}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{A\to C}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{B\to C}(\boldsymbol{\sigma}_{ABC}) \geq 0, \tag{11.5}$$

$$\mathcal{G}^{C\to(AB)}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{C\to A}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{C\to B}(\boldsymbol{\sigma}_{ABC}) \geq 0. \tag{11.6}$$

As in the original CKW inequality, these inequalities enjoy a very appealing interpretation: the degree of steering (by Gaussian measurements) exhibited by the state when all three parties are considered (i.e., $\mathcal{G}^{(AB)\to C} > 0$, or, $\mathcal{G}^{C\to(AB)} > 0$) can be larger that the sum of the degrees of steering exhibited by the individual pairs. On a more extreme level, there exist quantum states where parties A and B cannot individually steer party C, i.e., $\mathcal{G}^{A\to C} = \mathcal{G}^{B\to C} = 0$, but collectively they can, i.e., $\mathcal{G}^{(AB)\to C} > 0$. We will see the importance of this type of correlations later when we discuss applications to the task quantum secret sharing.

The residuals of the subtractions in (11.5), (11.6) quantify steering-type correlations that correspond to a collective property of the three parties, not reducible to the properties of the individual pairs. We proceed by investigating this quantitatively in a mode-invariant way. In analogy with what done for entanglement [236, 237, 277], we can calculate the residuals from the monogamy inequalities (11.5) or (11.6) and minimise them over all mode permutations. It turns out that, in the paradigmatic case of pure three-mode Gaussian states with CM $\boldsymbol{\sigma}_{ABC}^{\text{pure}}$

($m = 3$), we obtain the same quantity from either (11.5) or (11.6) (despite the individual inequalities being different, the minimum residual is found invariant under the steering direction and obviously invariant by construction under mode permutations). Explicitly, the RGS for three-mode pure Gaussian states with CM $\boldsymbol{\sigma}_{ABC}^{\text{pure}}$ is defined as

$$\mathcal{G}^{A:B:C}\left(\boldsymbol{\sigma}_{ABC}^{\text{pure}}\right) = \min\left\{\begin{array}{l}\mathcal{G}^{(BC)\to A} - \mathcal{G}^{B\to A} - \mathcal{G}^{C\to A} \\ \mathcal{G}^{(AC)\to B} - \mathcal{G}^{A\to B} - \mathcal{G}^{C\to B} \\ \mathcal{G}^{(AB)\to C} - \mathcal{G}^{A\to C} - \mathcal{G}^{B\to C}\end{array}\right\} \tag{11.7a}$$

$$= \min\left\{\begin{array}{l}\mathcal{G}^{A\to(BC)} - \mathcal{G}^{A\to B} - \mathcal{G}^{A\to C} \\ \mathcal{G}^{B\to(AC)} - \mathcal{G}^{B\to A} - \mathcal{G}^{B\to C} \\ \mathcal{G}^{C\to(AB)} - \mathcal{G}^{C\to A} - \mathcal{G}^{C\to B}\end{array}\right\} \tag{11.7b}$$

$$= \ln\left[\min\left\{\frac{bc}{a}, \frac{ac}{b}, \frac{ab}{c}\right\}\right], \tag{11.7c}$$

where $a = \sqrt{\det\boldsymbol{\sigma}_A}$, $b = \sqrt{\det\boldsymbol{\sigma}_B}$, and $c = \sqrt{\det\boldsymbol{\sigma}_C}$ are local symplectic invariants (with $|b-c|+1 \leq a \leq b+c-1$), fully determining the CM $\sigma_{ABC}^{\text{pure}}$ in standard form [237, 277]. For details on the standard form of pure three mode Gaussian states, see Eq. (3.69) of Sec. 3.3.4. Notice that a slightly different notation is used in Sec. 3.3.4 to facilitate the details of the standard form in more compact formulas, and the following correspondence among notations may be used: $a \leftrightarrow a_1$, $b \leftrightarrow a_2$, $c \leftrightarrow a_3$.

The RGS $\mathcal{G}^{A:B:C}$ is a monotone under Gaussian local operations and classical communication, as can be proven analogously to the case of the residual entanglement of Gaussian states [2, 3, 236, 237, 277]. Furthermore, finding a non-zero value of the RGS certifies genuine tripartite steering, as defined by He and Reid [180], since a sufficient requirement to violate the corresponding biseparable model for pure states is the demonstration of steering in all directions $(BC) \to A$, $(AC) \to B$ and $(AB) \to C$. We can then regard the RGS as a meaningful quantitative indicator of genuine tripartite steering for pure three-mode Gaussian states under Gaussian measurements.

In Fig. 11.1(a) we plot the RGS as a function of b and c for a given a. An elementary analysis reveals that the RGS $\mathcal{G}^{A:B:C}$ is maximized on bisymmetric states with $b = c \geq a$, i.e., when the states are steerable across any global split of the three modes and also $B \leftrightarrow C$ steerable, but no other steering exists between any two parties. In this case, the genuine tripartite steering $\mathcal{G}^{A:B:C}$ reduces to the collective steering $\mathcal{G}^{(BC)\to A} = \mathcal{G}^{A\to(BC)} = \ln a$. This quantitative analysis completes the existing picture of quantum correlations in pure three-mode Gaussian states, together with the cases of tripartite Bell nonlocality in terms of maximum violation of the Svetlichny inequality [242] and genuine tripartite entanglement in terms of Gaussian Rényi-2

entanglement [242]. Bisymmetric states maximize all three forms of nonclassical correlations; compare e.g. our Fig. 11.1(a) with Fig. 1(a)–(b) in [242].

Figure 11.1(b) presents the RGS measure for Gaussian states generated by three squeezed vacuum fields (one in momentum, two in position) with experimentally feasible squeezing parameter $r = 0.345$ (i.e., 3 dB of squeezing) [250, 281, 282] injected at two beamsplitters with reflectivities R and R' as depicted in the inset of Fig. 11.1(b), setting $R' = 1/2$ so that

$$a = \sqrt{1 + 2R(1-R)(\cosh 4r - 1)}, \tag{11.8}$$

$$b = c = \sqrt{[1 + R^2 - (R^2 - 1)\cosh 4r]/2}. \tag{11.9}$$

When $R = 1/3$, one can generate a permutationally invariant Greenberger-Horne-Zeilinger (GHZ)-like state with $a = b = c$ [233]. As one might expect, the latter states maximize the RGS in this case.

For mixed states, the definition of the tripartite steering indicator $\mathcal{G}^{A:B:C}\left(\boldsymbol{\sigma}^{\text{mixed}}_{ABC}\right)$ is not unique anymore, since the two residuals (11.7a) and (11.7b), arising respectively from the two monogamy inequalities (11.3) and (11.4) having opposite steering direction, are not equal in general. One may adopt either quantity depending on the specific setting for which steering is being analyzed, i.e. whether two parties are aiming to steer the remaining one, or the other way around, respectively.

11.3 Operational connections to quantum secret sharing

Secret sharing [283, 284] is a conventional cryptographic protocol in which a dealer (Alice) wants to share a secret with two players, Bob and Charlie, but with one condition: Bob and Charlie should be unable to individually access the secret (which may involve highly confidential information) and their collaboration would be required in order to prevent wrongdoings. Any classical implementation of this task, however, is fundamentally insecure and vulnerable to eavesdropping.

QSS schemes [169, 285] have been proposed to securely accomplish this task, by exploiting multipartite entanglement to secure and split the secret among the players in a single go. Only very recently, however, was an unconditional security proof provided for entanglement-based QSS protocols by us [6]. We will study in detail the proposed protocol and its security proof in Part IV, but for now let's just point to the main results. In our scheme, the goal of the dealer is to establish a secret key with a joint degree of freedom of the players. The players can

only retrieve Alice's key and decode the secret by collaborating and communicating to each other their local measurements to form the joint variable. The security of these schemes stems from the utilized partially device-independent setting, treating the dealer as a trusted party with characterized devices, and the (potentially, dishonest) players as untrusted parties whose measuring devices are described as black boxes. Given this intrinsically asymmetric separation of roles, one would expect that multipartite steering be closely related to the security figure of merit of QSS. Here we prove such a connection quantitatively.

To start with, let us assume that the dealer, Alice, and the players, Bob and Charlie, all perform homodyne measurements of the quadratures $\hat{q}_i, \hat{p}_i$ with outcomes Q_i, P_i, with $i = A, B, C$, on the shared tripartite state. Following [6], a guaranteed (asymptotic) secret key rate for the QSS protocol (extracted from the correlations of Alice's momentum detection P_A and a joint variable $\bar{P}$ for Bob and Charlie) to provide security against external eavesdropping is given by

$$K_E^{A\to\{B,C\}} \geq -\ln\left(e\sqrt{V_{P_A|\bar{P}}V_{Q_A|\bar{Q}}}\right), \tag{11.10}$$

while the key rate providing *unconditional* security against both eavesdropping and dishonest actions of the players is

$$K_{\text{full}}^{A\to\{B,C\}} \geq -\ln\left(e\sqrt{V_{P_A|\bar{P}}\cdot\max\{V_{Q_A|Q_C}, V_{Q_A|Q_B}\}}\right). \tag{11.11}$$

Here, $V_{P_A|\bar{P}} = \int d\bar{P}\, p(\bar{P})\left(\langle P_A^2\rangle_{\bar{P}} - \langle P_A\rangle_{\bar{P}}^2\right)$ is the minimum inference variance of Alice's momentum outcome given the players' joint outcome $\bar{P}$, and similarly for the other variances. A tripartite shared state ρ_{ABC} whose correlations result in nonzero values of the right-hand sides of either (12.5) or (12.10) can be regarded a useful resource for secure QSS against the corresponding threats discussed above.

We focus on pure three-mode Gaussian states with CM $\boldsymbol{\sigma}_{ABC}^{\text{pure}}$ in standard form, fully specified by the local invariants a, b, c as before. Our first observation is that K_E is directly quantified by the collective steering,

$$\mathcal{G}^{(BC)\to A}\left(\boldsymbol{\sigma}_{ABC}^{\text{pure}}\right) = \max\left\{0, \frac{1}{2}\ln\frac{\det\boldsymbol{\sigma}_{BC}}{\det\boldsymbol{\sigma}_{ABC}}\right\}. \tag{11.12}$$

For the considered class of states, one has indeed

$$\frac{\det\boldsymbol{\sigma}_{ABC}}{\det\boldsymbol{\sigma}_{BC}} = 4V_{P_A|\bar{P}}V_{X_A|\bar{X}} = 1/a^2,$$

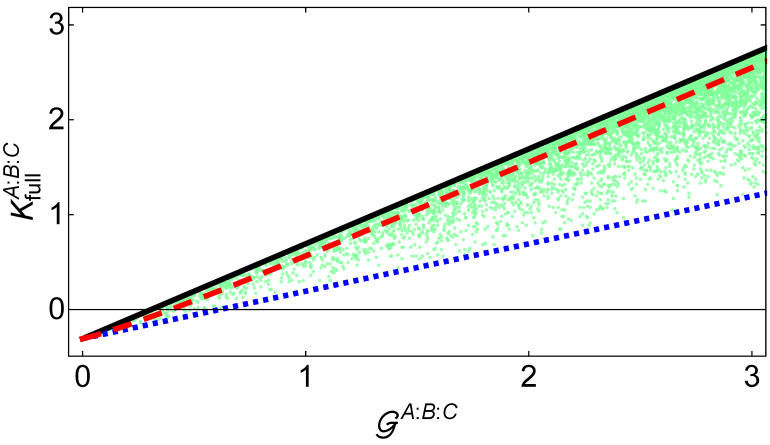

Figure 11.2: Mode-invariant secure QSS key rate versus RGS for 10^5 pure three-mode Gaussian states (dots); see text for details on the lines.

where the joint variables were chosen to have the linear form $\bar{X} = g_X X_B + h_X X_C$ and $\bar{P} = g_P P_B + h_P P_C$, with the real constants $g_{X(P)}, h_{X(P)}$ optimized as to minimize the inferred variances $V_{X_A|\bar{X}}, V_{P_A|\bar{P}}$; see also [2, 201]. Putting everything together, we get:

$$K_E^{A\to\{B,C\}}(\boldsymbol{\sigma}_{ABC}^{\text{pure}}) \geq \max\left\{0,\ \mathcal{G}^{(BC)\to A}\left(\boldsymbol{\sigma}_{ABC}^{\text{pure}}\right) - \ln\frac{e}{2}\right\}. \tag{11.13}$$

We can now define a mode-invariant QSS key rate bound $K_{\text{full}}^{A:B:C}$ that takes into account eavesdropping and potential dishonesty of the players, by minimizing the right-hand side of Eq. (12.10) over the choice of the dealer, i.e., over permutations of A, B, and C. A nonzero value of the figure of merit $K_{\text{full}}^{A:B:C}(\boldsymbol{\sigma}_{ABC})$ on a tripartite Gaussian state with CM $\boldsymbol{\sigma}_{ABC}$ guarantees the usefulness of the state for unconditionally secure QSS, for at least one assignment of the roles. For pure three-mode Gaussian states, the mode-invariant key rate $K_{\text{full}}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}})$ can be evaluated explicitly (although its lengthy expression is omitted here) and analyzed in the physical space of the parameters a, b, c. We find that $K_{\text{full}}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}})$ admits *exact linear upper and lower bounds* as a function of the RGS $\mathcal{G}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}})$, for all states with standard form CM $\boldsymbol{\sigma}_{ABC}^{\text{pure}}$:

$$\frac{\mathcal{G}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}})}{2} - \ln\frac{e}{2} \leq K_{\text{full}}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}}) \leq \mathcal{G}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}}) - \ln\frac{e}{2}. \tag{11.14}$$

The bounds are illustrated in Fig. 11.2 together with a numerical exploration of 10^5 randomly generated pure three-mode Gaussian states. Remarkably, the bounds are tight, and families of states saturating them can be readily provided. Specifically, the lower (dotted blue) boundary is spanned by states with $a \geq 1$, $b = c = (a+1)/2$; conversely, the upper (solid

black) boundary is spanned by states with $a \geq 1$, $b = c \to \infty$. While these cases are clearly extremal, GHZ-like states (dashed red), specified by $a = b = c$ and producible as discussed in Fig. 11.1(b), nearly maximize the QSS key rate at fixed RGS, thus arising as convenient practical resources for the considered task, independently of the distribution of trust. Indeed, a squeezing level of 4.315 dB, referring to the scheme of Fig. 11.1(b), is required to ensure a nonzero key rate using these states. This is well within the current experimental feasibility, since up to 10 dB of squeezing has been demonstrated [281, 282]. In general, by imposing non-negativity of the lower bound in (11.14), we find that $K_{\text{full}}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}}) > 0$ for all pure three-mode Gaussian states with RGS $\mathcal{G}^{A:B:C}(\boldsymbol{\sigma}_{ABC}^{\text{pure}}) > 2\ln(e/2) \approx 0.614$. Our analysis reveals that partially device-independent QSS is empowered by multipartite steering, yielding a direct operational interpretation for the RGS in terms of the guaranteed key rate of the protocol.

11.4 Discussion and conclusions

We showed that a recently proposed measure of quantum steering under Gaussian measurements [2, 3] obeys a CKW-type monogamy inequality for all Gaussian states of an arbitrary number of modes. Notice that the monogamy extends in fact to arbitrary (pure) non-Gaussian states under Gaussian measurements, as it is established solely at the level of covariance matrices. Notice however that resorting to non-Gaussian measurements can lead to extra steerability even for Gaussian states [216, 286], and might allow circumventing some monogamy constraints [272, 280].

In the case of pure three-mode Gaussian states, we argued that the residual steering emerging from the laws of monogamy can act as a quantifier of genuine tripartite steering. The latter measure is endowed with an operational interpretation, as it was shown to provide tight bounds on the mode-invariant key rate of a partially device-independent QSS protocol, whose unconditional security has been very recently investigated [6] and will be presented in detail in Part IV. Our study, combined with [6], provides practical recipes demonstrating that an implementation of QSS secure against eavesdropping and potentially dishonest players is feasible with current technology using tripartite Gaussian states and Gaussian measurements [1].

[1] In the recent experiment of Ref. [254] the principles of partially device-independent QSS were presented, but our present analysis allow us to conclude that the achieved level of steering was not sufficient to obtain a key rate above the unconditional security threshold in that case.

This work realizes important progress for the characterization and the utilization of multipartite quantum correlations to fuel upcoming secure quantum communication technologies, without the need for trust on all the involved parties.

Part IV

Cryptographical applications

12

Quantum secret sharing

In this Chapter we take advantage of our understanding of steering-type quantum correlations obtained in Part III, and apply this understanding and intuition to a cryptographical application in quantum communications, known as, *quantum secret sharing*. Obviously, the need for secrecy and security is essential in communications. Secret sharing is a conventional protocol to distribute a secret message to a group of parties who cannot access it individually but need to cooperate in order to decode it. While several variants of this protocol have been investigated, including realizations using quantum systems, the security of quantum secret sharing schemes still remains unproven almost two decades after their original conception. Here we establish an unconditional security proof for continuous variable entanglement-based quantum secret sharing schemes, in the limit of asymptotic keys and for an arbitrary number of players, by utilizing ideas from the recently developed one-sided device-independent approach to quantum key distribution. We demonstrate the practical feasibility of our scheme, which can be implemented by Gaussian states and homodyne measurements, with no need for ideal single-photon sources or quantum memories. Our results establish quantum secret sharing as a viable and practically relevant primitive for quantum communication technologies. This chapter is based on our work Ref. [6] which is currently under peer review.

12.1 Introduction

Secret sharing [283] is a task where a *dealer* sends a secret S to n (possibly, dishonest) *players* in a way such that the cooperation of a minimum of $k \leq n$ players is required to decode the secret; i.e., $k-1$ players should be unable to decode it even if they collaborated. Protocols that

accomplish this task are known as (k, n)-threshold schemes. The need for such a task appears naturally in a variety of situations, from children's games and online chats, to banking, industry, and military security: the secret message cannot be entrusted to any individual, but coordinated action is required for it to be decrypted in order to prevent wrongdoings.

For the classical implementation of the simplest $(2, 2)$-threshold scheme, Alice, the dealer, encodes her secret into a binary string S and adds to it a random string R of the same length, resulting into the coded cypher $C = S \oplus R$, where "$\oplus$" denotes addition modulo 2. She then sends R and C respectively to the players Bob and Charlie. While the individual parts R and C carry no information about the secret, only by collaboration the players can recover S by adding their strings together: $R \oplus C = S$. General (k, n)-threshold classical schemes are a bit more involved. Such classical secret sharing protocols, however, face the same problem as any other classical key distribution protocol: *eavesdropping*. An eavesdropper, Eve, or even a dishonest player, can in principle intercept the transmission and copy the parts sent from the dealer to the players, thus accessing the secret.

An obvious way to proceed would be for Alice to first employ standard two-party quantum key distribution (QKD) protocols [287], to establish separate secure secret keys with Bob and Charlie, then implement the classical procedure to split the secret S into parts R and C, and use the obtained secret keys to securely transmit these parts to each player. The advantage of this protocol, which we may call parallel-QKD (pQKD), is that it exploits unconditional security offered by the well-studied two-party QKD against eavesdropping and, very importantly, that it can be unconditionally secure against any possible dishonest actions of the players. However, pQKD is demanding in terms of resources since for a general (k, n) scenario it requires the implementation of n distinct QKD protocols plus the implementation of the classical procedure to split the secret [283]. Therefore, as the number of players n increases, pQKD becomes less efficient. The question then is whether we can do better, and the answer lies in what has been known in the literature as *quantum secret sharing* [169] (QSS), which allows for the implementation of a (k, n)-threshold scheme with just a *single* protocol, regardless of the number of players n. Unfortunately, as we shall see below, there exists no provably secure QSS scheme at the moment that enjoys the unconditional security of pQKD against both eavesdropping and dishonesty.

Hillery, Bužek, and Berthiaume [169] (HBB, for short) proposed the first (2,2)- and (3,3)-threshold QSS schemes that use multipartite entanglement to split the classical secret, and

protect it from eavesdropping and dishonest players in a *single* go. Various other entanglement-based (HBB-type) schemes have been proposed [285, 288, 289, 290, 291, 292, 293, 294], some being more economic in terms of the required multipartite entanglement [295, 296], while others allowing for more general (k,n)-threshold schemes [13, 297, 298, 299, 300]. A few experimental demonstrations have also been reported [296, 301, 302, 303, 304]. The security of all current schemes, however, is limited to, either, plain external eavesdropping under the unrealistic assumption of honest players, or, limited type of attacks by eavesdroppers and dishonest participants but for the unrealistic case of the parties sharing a pure maximally entangled state. Furthermore, all such schemes are vulnerable to the participant attack and cheating [285, 305, 306], and no method is currently known to deal with such attacks and conspiracies in general, not even in the ideal case of pure shared states.

Zhang, Li, and Man [307] proposed the first *(n,n)*-threshold scheme that required no entanglement and was claimed to be unconditionally secure, posing a serious alternative to pQKD. Although the scheme unrealistically required perfect single photon sources and quantum memories (rendering it impractical for today's technology), it was later shown to be vulnerable to various participant attacks [308, 309]. In the same category of entanglement-free QSS schemes, Schmid *et al.* proposed a protocol based on a single photon [310]; although originally claimed to be unconditionally secure, this scheme was also shown to be vulnerable to the participant attack [311, 312, 313]. Alterations of these schemes can be devised to deal with particular attacks (e.g., see [308, 309, 311, 312]), however there currently exists no rigorous method to deal with arbitrary participant attacks and conspiracies (a fact also remarked in [313]).

To sum up, almost two decades after the original conception of QSS, none of the existing QSS schemes (with or without entanglement) has been proven to be unconditionally secure against the cheating of dishonest players. Any practical implementation of secure secret sharing is therefore necessarily resorted to the conventional pQKD, while QSS schemes have only served up to now as a theoretical curiosity.

In this Chapter, we consider a continuous variable version of an HBB-type scheme, and provide conditions on the extracted secret key rate for the secret to be unconditionally secure against both external eavesdropping and arbitrary cheating strategies of dishonest participants, in the limit of asymptotic keys, independently of the shared state, and for arbitrary (k,n)-threshold schemes. The central idea in our approach, to rigorously deal with arbitrary cheating strategies, is to treat the measurements announced by the players as an input/output of a black box (i.e., uncharacterized measuring device), in the same way (possibly, hacked) measuring

devices are treated in device-independent QKD [314]. In practice, this translates into making no assumption about the origin of the players' (possibly, faked) announced measurements, in contrast to all previous QSS approaches that considered the players' actions as trusted, and suffered as a consequence from cheating strategies. The dealer, on the other hand, is considered to be a trusted party with trusted devices, which is a natural assumption for this task. It is interesting to note that in device-independent QKD it is the *devices* that are not trusted, while in the task of secret sharing the *players* themselves are not trusted, independently of their devices. Therefore the framework we are proposing, of making no assumptions about the players' measurements, seems very natural for the task of QSS, as very recently discussed in [180, 254]. To prove security against general attacks of an eavesdropper and/or of dishonest players, we make a sharp connection with, and extend all the tools of, the recently developed one-sided DI-QKD (1sDI-QKD) [315], but for continuous variable systems [201], which has been shown to be unconditionally secure in the limit of asymptotic keys.

12.2 The protocol

For ease of illustration, we first focus on the $(2, 2)$-threshold scheme. The dealer Alice prepares a 3-mode continuous variable entangled state, keeps one mode and sends the other modes to the possibly dishonest players, Bob and Charlie, through individual unknown quantum channels. Alice, who is the trusted party with characterized devices, is assumed to perform on her system homodyne measurements of the two canonically conjugate quadratures,

$$\hat{q}_A = \frac{1}{\sqrt{2}}(\hat{a} + \hat{a}^\dagger), \quad \hat{p}_A = \frac{-i}{\sqrt{2}}(\hat{a} - \hat{a}^\dagger),$$

with corresponding outcomes Q_A, P_A, satisfying $[\hat{q}_A, \hat{p}_A] = i\mathbb{I}$ (in natural units with $\hbar = 1$). Bob and Charlie, considered to be untrusted and with uncharacterized devices (black boxes), are allowed for two unspecified measurements each, denoted by the labels $q_{B(C)}, p_{B(C)}$ with corresponding outcomes $Q_{B(C)}, P_{B(C)}$. Nothing is assumed about the true origin of these (possibly, faked) measurements.

In our protocol, Alice's goal is to establish a unique secret key, not with Bob's or Charlie's individual measurements (as in standard two-party QKD), but with a collective (non-local) degree of freedom for Bob and Charlie, say $\bar{Q}$, that strongly correlates with one of Alice's quadratures, say Q_A, and can be accessed only when the players communicate their local measurements, i.e., collaborate. For example, if the three parties shared a maximally entangled

state and their outcomes were perfectly correlated as $Q_A \simeq -Q_B + Q_C$, one would choose $\bar{Q} = -Q_B + Q_C$ as that collective degree of freedom.

In the next step of the protocol, after receiving their copy, all three parties *randomly* choose a local measurement q_i or p_i and measure their copies, getting outcomes Q_i, P_i respectively, with $i = A, B, C$. Alice then sends an additional copy to Bob and Charlie and the procedure is repeated until they have a sufficiently long list of correlated data (*raw key*). The parties then proceed with the standard procedures of standard two-party quantum key distribution as described in Ref. [316]. First is the classical post-processing step of *sifting*, where all parties announce and compare their measurement choices for every single copy of the shared states, and keep only the data originating from correlated measurements (depending on the shared state). The remaining data represent the *sifted key*, while the final *secret key* will be extracted from the Q_A and $\bar{Q}$ measurement outcomes. After the sifting, all parties proceed to the *parameter estimation* stage, where by revealing the outcomes of a random sample of measurements they can upper bound Eve's information, allowing them to estimate the size of the secret key (see below). If the latter is non-zero they can proceed to *direct reconciliation* where Alice publicly sends error-correction instructions to Bob and Charlie (to be applied on $\bar{Q}$) whose purpose is to make the joint outcomes $\bar{Q}$ identical to hers (although still correlated to Eve). Finally, Alice applies *privacy amplification* on her sifted key to completely decorrelate any possible eavesdropper. In particular, she randomly chooses a two-universal hash function h which she applies on her sifted key, resulting in a shorter *secret key* (shorter by an amount estimated in the parameter estimation stage) that is completely decorrelated by any possible eavesdropper. She then publicly announces her choice of the function h to Bob and Charlie. After all these steps, Alice's final string represents the secret key that she uses to encode her secret message, which then sends to the players through a public (authenticated) channel. Bob and Charlie, however, in order to acquire the secret key and decode Alice's secret, have to collaborate and communicate to each other their local outcomes, in order to form the joint outcomes $\bar{Q}$ which are the ones correlated to Alice's key. Only then can they apply Alice's error correction instructions plus the hash function h on their string to transform it exactly into Alice's secret key and decode her message.

12.3 Security proof (1): Eavesdropping

Let us first study security against eavesdropping, following the work of Walk *et al.* [201]. Neglecting detector and reconciliation efficiencies, the direct reconciliation asymptotic secret key rate is known to be lower bounded by the Devetak-Winter formula [201, 317],

$$K \geq I(Q_A : \bar{Q}) - \chi(Q_A : E), \tag{12.1}$$

where $I(Q_A : \bar{Q}) = H(Q_A) - H(Q_A|\bar{Q})$ is the classical mutual information between Alice's variable X_A and the joint variable $\bar{Q}$, with $H(Q) = -\int dQ p(Q) \log p(Q)$ being the Shannon entropy for a variable Q with probability distribution $p(Q)$, and

$$\chi(Q_A : E) = S(E) - \int dQ_A p(Q_A) S(\rho_E^{Q_A}), \tag{12.2}$$

being the Holevo bound [318], which represents the maximum possible knowledge an eavesdropper can get on the key. The term $S(E) = -\mathrm{tr}(\rho_E \log \rho_E)$ is the von Neumann entropy of Eve's reduced state ρ_E, whereas $\rho_E^{Q_A}$ denotes Eve's state conditioned on Alice's measurement of $\hat{q}_A$ with outcome Q_A. A positive value of the right-hand side of (12.1) implies security of the key against collective attacks of the eavesdropper, and by virtue of Ref. [319] also against general coherent attacks (as collective attacks are proved asymptotically optimal).

Defining the conditional von Neumann entropy $S(Q_A|E) = H(Q_A) + \int dQ_A p(Q_A) S(\rho_E^{Q_A}) - S(E)$, and the conditional Shannon entropy $H(Q_A|Q_B) = \int dQ_B p(Q_B) H(Q_A|q_B = Q_B)$, with $H(Q_A|q_B = Q_B) = -\int dQ_A p(Q_A|Q_B) \log p(Q_A|Q_B)$, one can recast the key rate (12.1) as a balance of conditional entropies,

$$K \geq S(Q_A|E) - H(Q_A|\bar{Q}). \tag{12.3}$$

We can now use known entropic uncertainty relations that provide a lower bound to Eve's uncertainty [320, 321, 322, 323],

$$S(Q_A|E) + S(P_A|BC) \geq \log 2\pi, \tag{12.4}$$

for the derivation of which Alice's canonical commutation relations have been assumed, while Eve is assumed to purify the state shared by Alice, Bob and Charlie, i.e., $\rho_{ABC} = \mathrm{tr}_E(|\Psi_{ABCE}\rangle\langle\Psi_{ABCE}|)$. Substituting the uncertainty relation (12.4) back into (12.3) and recalling that $S(P_A|BC) \leq S(P_A|\bar{P}) = H(P_A|\bar{P})$ (since measurements cannot decrease the entropy), where $\bar{P}$ is a joint variable for Bob and Charlie optimally correlated with Alice's momentum P_A, we get $K \geq$

$\log 2\pi - H(Q_A|\bar{Q}) - H(P_A|\bar{P})$, i.e., a bound on the key rate (hence, on Eve's maximal knowledge on the key Q_A) using only conditional Shannon entropies, that can be estimated using the announced measurement outcomes during the parameter estimation stage. To make the bound even more accessible, we would like to express it in terms only of second moments instead of dealing with conditional probability distributions. We use the fact that the Shannon entropy of an arbitrary probability distribution is maximised for a Gaussian distribution of the same variance. In other words, $H(Q_A|\bar{Q}) \leq H_G(Q_A|\bar{Q}) = \log\sqrt{2\pi e V_{Q_A|\bar{Q}}}$, where $V_{Q_A|\bar{Q}} = \int d\bar{Q}p(\bar{Q})\left(\langle Q_A^2\rangle_{\bar{Q}} - \langle Q_A\rangle_{\bar{Q}}^2\right)$ is the minimum inference variance of Alice's position outcome when the joint outcome $\bar{Q}$ is known. Similarly for $H(P_A|P)$. The final key rate is then bounded as follows,

$$K \geq -\log\left(e\sqrt{V_{Q_A|\bar{Q}}V_{P_A|\bar{P}}}\right). \tag{12.5}$$

We see that a nonzero key rate (secure against eavesdropping) can be achieved when $E_{A|BC} \equiv V_{Q_A|\bar{Q}}V_{P_A|\bar{P}} < e^{-2}$.

12.4 Security proof (2): Conditions against dishonesty

Suppose now that Bob is a dishonest player. His goal would be to guess Alice's key (hence, access the secret) using solely his own local measurements, entirely bypassing the required collaboration with Charlie. Notice here that x_B, p_B are his announced measurements which he may have faked, therefore we cannot rely on these to assess Bob's knowledge on the key. A most general cheating strategy for Bob would be: first, to secretly intercept Charlie's mode during its transmission using general coherent attacks to increase his knowledge on Alice's key; second, to lie about his measurements. A positive key rate in (12.5) does not guarantee security against such general participant attacks and cheating.

Here we derive additional conditions on the key rate so that Bob cannot cheat or access the secret by himself. Our key observation is to go back to the Devetak-Winter formula (12.1) and treat Bob as an eavesdropper, together with Eve, meaning that in the Holevo bound $\chi(Q_A : E)$ (that expresses the knowledge of party E on the key Q_A) we will include Bob himself, as,

$$K \geq I(Q_A : \bar{Q}) - \chi(Q_A : EB), \tag{12.6}$$

where EB refers to the unknown joint quantum state of Eve (the eavesdropper, as considered previously) and Bob. A positive key rate in (12.6) would imply security of Alice's key against joint general attacks by Bob and Eve on Charlie's system. Also, Bob and Eve's maximum

knowledge of the key, $\chi(Q_A : EB)$, can be upper bounded (as seen below) using Alice and Charlie's measurements, independently of Bob's (possibly, faked) announced measurements, therefore providing security against Bob's cheating. The uncertainty relation that we will use to bound Bob and Eve's knowledge will be a slightly modified version of (12.4),

$$S(Q_A|EB) + S(P_A|C) \geq \log 2\pi. \tag{12.7}$$

Following similar steps as previously, we end up with the following bound on the key rate,

$$K \geq -\log\left(e\sqrt{V_{Q_A|\bar{Q}}V_{P_A|P_C}}\right). \tag{12.8}$$

Notice that the key rate bound in (12.8) is smaller than the one in (12.5) that did not take dishonesty into account, due to $V_{P_A|\bar{P}} \leq V_{P_A|P_C}$, which is expected since the eavesdroppers' knowledge on the key is increased by including Bob together with Eve.

To intuitively understand why this condition prohibits any cheating from Bob, we recall first that the key is generated solely by the $Q_A, \bar{Q}$ outcomes. By examination of the uncertainty relation Eq. (12.7), taking into account that $\log\sqrt{2\pi e V_{P_A|P_C}} \geq S(P_A|C)$, we see that the better Charlie can estimate Alice's momentum (i.e., small $S(P_A|C)$) the larger Bob and Eve's ignorance should be on the key elements Q_A. The previous condition (12.5), not accounting for participant dishonesty, only demanded small enough $S(P_A|BC)$, which can be true even if $S(P_A|C)$ is arbitrarily large, thus allowing Bob to acquire good knowledge of the key (i.e, small $S(Q_A|EB)$), as seen by Eq. (12.7).

We can also account for Charlie's dishonesty in an exactly analogous manner (just replace $B \leftrightarrow C$ above), leading us to

$$K \geq -\log\left(e\sqrt{V_{Q_A|\bar{Q}}V_{P_A|P_B}}\right). \tag{12.9}$$

Putting everything together, the final bound on the asymptotic key rate to provide unconditional security against general attacks of an eavesdropper, and against arbitrary (individual) cheating methods of both Bob and Charlie, which include the announcement of faked measurements and general attacks of Bob on Charlie's system and of Charlie on Bob's system, is:

$$\begin{aligned} K &\geq I(Q_A : \bar{Q}) - \max\{\chi(Q_A : EB),\ \chi(Q_A : EC)\} \\ &\geq -\log\left(e\sqrt{V_{Q_A|\bar{Q}} \cdot \max\{V_{P_A|P_C}, V_{P_A|P_B}\}}\right), \end{aligned} \tag{12.10}$$

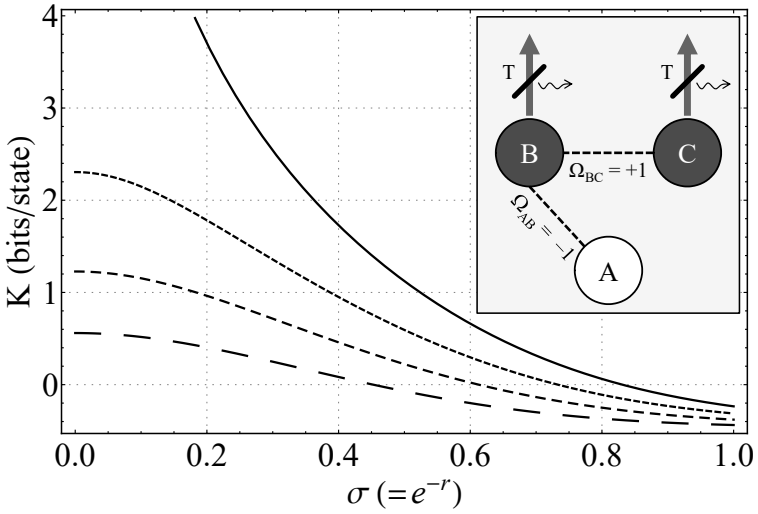

Figure 12.1: The QSS secure key rate K, Eq. (12.10), is plotted against the squeezing r of a 3-mode noisy Gaussian cluster state, obtained from a pure state [13] $\hat{U}_{AB}\hat{U}_{BC}|r\rangle_A|r\rangle_B|r\rangle_C$, with $\hat{U}_{ij} = \exp\left(\Omega_{ij}\hat{q}_i\hat{q}_j\right)$, after Bob's and Charlie's modes undergo individual pure-loss channels, each modelled by a beam-splitter with transmissivity T and zero excess noise (see inset). From top to bottom, the curves correspond to $T = 1,\ 0.95,\ 0.9,\ 0.85$. All parties are assumed to be performing homodyne measurements of $\hat{q}_i$,$\hat{p}_i$, with $i = A, B, C$. The current experimentally accessible squeezing is limited to $r \lesssim 1.15$ (10dB), or $\sigma \gtrsim 0.32$ [14, 15], in which regime a nonzero K is still guaranteed for sufficiently large T, demonstrating the feasibility of our scheme.

which is the minimum of the bounds (12.8),(12.9). A positive key rate (12.10) remarkably provides security against all kinds of attacks that existing QSS protocols suffered from (e.g., fake announced measurements [285], Trojan horse attacks [308], etc.), for the sole reason that the players Bob and Charlie are not assumed to be performing trusted quantum operations but are treated as black boxes, in contrast to all previous schemes.

12.5 Discussion and extensions

In Fig. 12.1 we demonstrate the feasibility of the protocol in a concrete realization, where the key rate (12.10) is plotted against the squeezing degree of a noisy tripartite entangled cluster state. Notice that the same key rate can also be achieved by an equivalent protocol that solely requires bipartite entanglement (that would represent the so-called prepare-and-measure counterpart to the presented protocol, borrowing a QKD terminology), thus further reducing the technological requirements for the state preparation.

Finally, we show how to generalize the secret key rate bound (12.10) to any (k, n)-threshold QSS scheme. To start with, let us denote the n players as $B_1, B_2, \ldots, B_n$. A (k, n)-threshold scheme has two requirements: First, no collaboration of any $k-1$ players should be able to access the secret. We incorporate this requirement into Eq. (12.10) by considering all possible combinations of $k-1$ out of n players, the total number of which equals the binomial coefficient $\binom{n}{k-1}$, as potential collaborative eavesdroppers, and choosing the maximum Holevo information over all collaborations to attain the maximum possible knowledge on the key by any of these groups. Second, any collaboration of k players should be able to decode the message. Let us attribute a joint variable $\bar{Q}_i$ to each k-player collaboration correlated to Alice's Q_A, with $i = 1, \ldots, \binom{n}{k}$. This second requirement translates to Alice sending as much error-correction information as needed, such that even the k-player collaboration least correlated to Alice (i.e., with smallest $I(Q_A : \bar{Q}_i)$) can access Alice's key. Taking the above into account, the key rate of the protocol will be,

$$\begin{aligned} K \geq \min\{&I(Q_A : \bar{Q}_1), \ldots, I(Q_A : \bar{Q}_{\binom{n}{k}})\} \\ &- \max\{\chi(Q_A : ES_1), \ldots, \chi(Q_A : ES_{\binom{n}{k-1}})\}, \end{aligned} \tag{12.11}$$

where S_i denotes a particular sequence of $k-1$ players, e.g., $S_1 = B_1 \cdots B_{k-1}$. A positive value of the right-hand side of Eq. (12.11) guarantees unconditional security of our QSS protocol against eavesdropping and arbitrary collaborative cheating strategies of any group of $k-1$ potentially dishonest players.

12.6 Discussion and conclusions

We presented a practically feasible entanglement-based continuous variable QSS protocol, and derived sufficient conditions for the protocol's secret key rate to provide, for the first time, unconditional security of the dealer's classical secret against general attacks of an eavesdropper and arbitrary cheating strategies, conspiracies and attacks of the (possibly, dishonest) players, for all (k, n)-threshold schemes, and in the limit of asymptotic keys.

In our approach, we identified the most physically relevant framework for QSS to be the one-sided device-independent (1sDI) setting, treating the dealer as a trusted party with characterized devices and the players' devices as black boxes. The natural separation of roles between dealer and players renders QSS a well-suited task for the 1sDI setting, more than two-party QKD itself [324]. Incidentally, while the resource behind 1sDI-QKD is known to

be (bipartite) *steering* [12], a quantum correlation stronger than plain entanglement [64] and weaker than Bell-nonlocality [59], one could suspect a similar connection in the present multiuser scenario. In an accompanying work, we show indeed that *multipartite* steering [180] is the resource behind secure QSS, thus providing an operational interpretation for a multipartite steering measure.

Our work opens many avenues for further exploration. The presented security proof can be extended from asymptotic to finite keys [325], suitable for practical applications, and also to discrete variable systems, used in the original QSS definition [169]. Moreover, although we provided sufficient security conditions for all (k, n)-threshold schemes, the identification of optimal families of states maximizing the key rate for each scheme is left open. Finally, our results pave the way for an unconditionally secure experimental demonstration of QSS, enabling its use in upcoming quantum communication networks.

Part V

Conclusion and perspectives

Conclusion and perspectives

In this thesis we studied various aspects of quantum information, ranging from quantum teleportation, which is an important application of entanglement, to Einstein-Podolsky-Rosen steering-type quantum correlations and the cryptographical task of quantum secret sharing. A summary of the results presented in the thesis can be found in the abstract and, in more detail, in the introduction, while many open questions regarding each research topic can be found in the "*Discussion and conclusion*" section of each chapter. For these reasons we will not repeat these here, but we will instead additionally provide further insight on each topic.

Quantum teleportation is a well-studied topic from a theoretical point of view, while the number of experimental demonstrations have increased immensely over the years. Quantum teleportation has been achieved in laboratories around the world utilizing various systems and technologies, including photonic qubits, nuclear magnetic resonance, optical modes, atomic ensembles, trapped atoms, and solid state systems. Impressive performances have been achieved in terms of teleportation distance, with satellite-based implementations forthcoming. Details on the aforementioned experimental implementations of quantum teleportation, with corresponding references, can be found in a recent review article by Pirandola *et al.* [326]. From a theoretical viewpoint, it would be desirable to design novel quantum information protocols for which quantum teleportation can be a useful resource, as well as to propose more efficient teleportation schemes. It would be fair to say, however, that given the fair amount of theoretical research on the topic, it is the advances in technology that are mostly anticipated in the future (like, achieving better entanglement distribution, and in larger amounts) in order to boost the practical feasibility and performance of quantum teleportation.

Einstein-Podolsky-Rosen steering is a relatively new research topic in quantum information, and many useful results have been produced during the past few years, including novel

detection and quantification techniques some of which were presented in this thesis. Bipartite steering, in particular, has been well-studied and has already been recognized as a useful resource in a variety of quantum information tasks: from quantum key distribution to subchannel discrimination and secure teleportation. Multipartite steering, on the other hand, lacks sufficient understanding and there is no general consensus even in its definition. In particular, clashes in the definition of *genuine* multipartite steering exist in the literature, detection techniques have yet to be developed for continuous variable systems, while quantum information tasks for which multipartite steering acts as a useful resource are not known; excempting the multi-party cryptographical task of quantum secret sharing which was proven by us to be fueled by multipartite steering-type quantum correlations.

Quantum secret sharing is an important cryptographical task that has been studied considerably over the years. The advances reported in this thesis, regarding the obtained unconditional security proof, constitute in our opinion our most original and important contribution as it initiates potential future applications. Potential avenues for further theoretical research are reported in Chapter 12. In practical terms however, similarly to quantum teleportation, the efficient implementation of entanglement-based quantum secret sharing requires considerable technological advances and improvements in the quality of quantum communication networks. An important milestone is especially the experimental implementation of quantum repeater schemes which will allow large amounts of entanglement (hence, large amounts of steering) to be distributed over large distances.

Appendix A

Monotonicity of Gaussian steering under local Gaussian operations of the trusted party

In Chapter 9 we reported on a property of the proposed Gaussian steering quantifier being monotonic under local Gaussian operation of the trusted party, Bob. Below we provide the corresponding proof.

Proof A local Gaussian operation for Bob acts as a completely positive (CP) map on the bipartite quantum state ρ_{AB}, transforming the covariance matrix (CM) $\boldsymbol{\sigma}_{AB}$ as,

$$\boldsymbol{\sigma}_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathrm{T}} & \mathbf{B} \end{pmatrix} \longrightarrow \boldsymbol{\sigma}'_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C}\mathbf{S}^{\mathrm{T}} \\ \mathbf{S}\mathbf{C}^{\mathrm{T}} & \mathbf{S}\mathbf{B}\mathbf{S}^{\mathrm{T}} + \mathbf{G} \end{pmatrix}. \tag{A.1}$$

To prove the desired monotonicity

$$\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) \geq \mathcal{G}^{A\to B}\left(\boldsymbol{\sigma}'_{AB}\right), \tag{A.2}$$

we will instead prove the equivalent statement involving the corresponding Schur complements

$$\det \mathbf{M}_B \leq \det \mathbf{M}'_B. \tag{A.3}$$

A. MONOTONICITY OF GAUSSIAN STEERING UNDER LOCAL GAUSSIAN OPERATIONS OF THE TRUSTED PARTY

We assume that the initial CM is in standard form as usual, with $\mathbf{A} = \mathrm{diag}\,(a, a)$, $\mathbf{B} = \mathrm{diag}\,(b, b)$, $\mathbf{C} = \mathrm{diag}\,(c_1, c_2)$. The $\mathbf{M}'_B$ corresponding to the new CM takes the form,

$$\begin{aligned}\mathbf{M}'_B &= \mathbf{B}' - \mathbf{C}'^{\mathrm{T}}\mathbf{A}^{-1}\mathbf{C}' = \mathbf{S}\mathbf{B}\mathbf{S}^{\mathrm{T}} + \mathbf{G} - \frac{1}{a}\mathbf{C}'^{\mathrm{T}}\mathbf{C}' \\ &= \mathbf{S}\mathbf{B}\mathbf{S}^{\mathrm{T}} + \mathbf{G} - \frac{1}{a}\mathbf{S}\begin{pmatrix} c_1^2 & 0 \\ 0 & c_2^2 \end{pmatrix}\mathbf{S}^{\mathrm{T}} = \mathbf{S}\begin{pmatrix} b - \frac{c_1^2}{a} & 0 \\ 0 & b - \frac{c_2^2}{a} \end{pmatrix}\mathbf{S}^{\mathrm{T}} + \mathbf{G} \\ &= \mathbf{S}\mathbf{M}_B\mathbf{S}^{\mathrm{T}} + \mathbf{G}.\end{aligned} \tag{A.4}$$

Substituting the matrix elements of $\mathbf{S} = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$ and $\mathbf{G} = \begin{pmatrix} g_{11} & g_{12} \\ g_{12} & g_{22} \end{pmatrix}$ we get,

$$\mathbf{M}'_B = \begin{pmatrix} s_{11}^2 V_X + s_{12}^2 V_P + g_{11} & s_{11}s_{21}V_X + s_{22}s_{12}V_P + g_{12} \\ s_{11}s_{21}V_X + s_{22}s_{12}V_P + g_{12} & s_{22}^2 V_P + s_{21}^2 V_X + g_{22} \end{pmatrix} \equiv \begin{pmatrix} \alpha + g_{11} & \gamma + g_{12} \\ \gamma + g_{12} & \beta + g_{22}, \end{pmatrix} \tag{A.5}$$

where i have denoted: $V_X = b - \frac{c_1^2}{a}$, $V_P = b - \frac{c_2^2}{a}$ and $\alpha = s_{11}^2 V_X + s_{12}^2 V_P, \beta = s_{22}^2 V_P + s_{21}^2 V_X$, $\gamma = s_{11}s_{21}V_X + s_{22}s_{12}V_P$. Thus the determinant that we want to minimize acquires the simple form,

$$\det \mathbf{M}'_B = (\alpha + g_{11})(\beta + g_{22}) - (\gamma + g_{12})^2. \tag{A.6}$$

The goal now is to minimize (A.6) over all parameters of Bob's operation, thus showing that there exists no local Gaussian operation for Bob that can make $\det \mathbf{M}'_B$ smaller than $\det \mathbf{M}_B$, proving (A.3). However, the matrix elements of $\mathbf{G}$ and$\mathbf{S}$ that correspond to CP maps must satisfy the conditions [27]

$$g_{11} \geq 0, \quad g_{22} \geq 0, \quad g_{11}g_{22} - (1 - \det \mathbf{S})^2 \geq g_{12}^2. \tag{A.7}$$

We see from (A.6) that $\mathbf{M}'_B$ will be minimum when g_{12} will acquire it's maximum value in (A.7), and also its sign should be the same with that of γ in (A.6). Thus, we will have

$$\det \mathbf{M}'_B = (\alpha + g_{11})(\beta + g_{22}) - \left(\sqrt{g_{11}g_{22} - (1 - \det \mathbf{S})^2 + |\gamma|}\right)^2 \tag{A.8}$$

Minimizing (A.8) over g_{11}, g_{22},

$$\left.\frac{\partial \det \mathbf{M}'_B}{\partial g_{11}}\right|_{g_{11}^\star} = 0, \quad \left.\frac{\partial \det \mathbf{M}'_B}{\partial g_{22}}\right|_{g_{22}^\star} = 0, \tag{A.9}$$

we find that (see Eq. (38)-(40) of Fiurasek) the optimum $\mathbf{G}$ is

$$\mathbf{G}^\star = \frac{|1 - \det \mathbf{S}|}{\sqrt{\alpha\beta - \gamma^2}}\begin{pmatrix} \alpha & \gamma \\ \gamma & \beta \end{pmatrix}, \tag{A.10}$$

while the minimized determinant gets the form,

$$\det \mathbf{M}'_B = \left(|1 - \det \mathbf{S}| + \sqrt{\alpha\beta - \gamma^2} \right)^2 . \tag{A.11}$$

Next step is to minimize this quantity over the elements s_{ij}. By substituting the definitions of α, β, γ and considering the three separate cases (i) $\det \mathbf{S} \geq 1$, (ii) $\det \mathbf{S} = 1$, (iii) $\det \mathbf{S} \leq 1$, we can perform analytically the minimizations without doing any more assumptions, and find that the *global* minimum (in all cases) is

$$\det \mathbf{M}'_B \geq \det \mathbf{M}_B, \tag{A.12}$$

thus concluding the proof.

It's interesting to note that the present calculation is very similar to a calculation by Fiurášek in Ref. [327], where he also optimized over local Gaussian operation but for improving the fidelity of continuous variable teleportation. More specifically, our Eq. (A.6) exactly corresponds to his Eq. (35) in Ref. [327].

A. MONOTONICITY OF GAUSSIAN STEERING UNDER LOCAL GAUSSIAN OPERATIONS OF THE TRUSTED PARTY

Appendix B

Proof of the equivalence between unsteerability and the existence of a separable model

In the proof that follows we assume Bob's Hilbert space to be arbitrary (continuous or discrete variable), while for simplicity we assume discrete outcomes for Alice. The generalization of the proof to continuous outcomes will be immediate as we shall see.

First, we recall that Bob's assemblage $\left\{\sigma^B_{a|x}\right\}$, is unsteerable by Alice's inputs $x = 1, ..., n$ (with corresponding outcomes $a_x = 1, ..., d_x$) *iff* it can be expressed as,

$$\sigma^B_{a|x} = \sum_\lambda q_\lambda p(a|x,\lambda)\rho_\lambda, \quad \forall x, a. \tag{B.1}$$

The first part of the proof amounts to expressing (B.1) in a suitable form in terms of deterministic functions (i.e. the Kronecker delta function) that will prove very helpful. The basic tool we utilize is the following identity,

$$p(a|x,\lambda) = \sum_{a_x} \delta_{a,a_x}\, p(a_x|x,\lambda), \tag{B.2}$$

for a particular input x, while $\delta_{i,j}$ is the Kronecker delta. By inserting in (B.2) the identities, $\sum_{a_i} p(a_i|i,\lambda) = 1$, for every input $i \neq x$, we get,

$$p(a|x,\lambda) = \sum_{a_1 \ldots a_n} \delta_{a,a_x}\, p(a_1|1,\lambda) \cdots p(a_n|n,\lambda), \tag{B.3}$$

where the summation over a_x is implicitly included. Substituting (B.3) back in the assemblage (B.1) we get the desired expression,

$$\sigma^B_{a|x} = \sum_{a_1 \dots a_n} \delta_{a,a_x} \omega_{a_1 \dots a_n}, \tag{B.4}$$

where the unnormalized positive semidefinite operators $\omega_{a_1 \dots a_n} \geq 0$ correspond to,

$$\omega_{a_1 \dots a_n} = \sum_{\lambda} q_\lambda p(a_1|1, \lambda) \cdots p(a_n|n, \lambda) \rho_\lambda. \tag{B.5}$$

In the second part of the proof, we will show that one can always define a separable model $\bar{\rho}_{AB}$ for Alice and Bob, and appropriate measurement operators for Alice, that can reproduce an arbitrary unsteerable assemblage (B.4). Consider each input x of Alice, with outcomes $a_x = 1, ..., d_x$, to correspond to a fictitious observable (hermitian operator) A_x such that,

$$A_x |a_x\rangle_A = a_x |a_x\rangle_A. \tag{B.6}$$

where the same outcomes $a_x = 1, ..., d_x$ correspond to its real eigenvalues with $|a_1\rangle_A, ..., |a_n\rangle_A$ being the corresponding eigenvectors. When Alice announces to Bob a pair (a, x), i.e. measured input x and got outcome a, it will be considered equivalent as if she measured the observable A_x and got the eigenvalue a as an outcome (with corresponding eigenvector $|a\rangle$). Note that such a correspondence $x \leftrightarrow A_x$ can always be made, since the announced outcomes a_x always correspond to eigenvalues of some observable.

Next, *assume* that all the defined observables $\{A_1, ..., A_n\}$ mutually commute,

$$[A_x, A_{x'}] = 0, \quad \forall x \neq x', \tag{B.7}$$

and, therefore, a joint basis exists that diagonalizes all A_x, $\forall x$, simultaneously. We will show that these commuting observables can reproduce the statistics of any unsteerable assemblage by acting on a suitable separable state. Let us denote the vectors of this basis as $\{|a_1 \cdots a_n\rangle\}$, which sum to unity, $\sum_{a_1 \dots a_n} |a_1 \cdots a_n\rangle_A \langle a_1 \cdots a_n| = 1$, and are orthonormal, i.e.,

$$\langle a'_1 ... a'_N | a_1 ... a_N \rangle = \delta_{a_1, a'_1} \cdots \delta_{a_N, a'_N}. \tag{B.8}$$

Due to the simultaneous diagonalization of every observable, it holds, $A_x |a_1 \cdots a_n\rangle_A = a_x |a_1 \cdots a_n\rangle_A$, $\forall a_x, x$.

If ρ_{AB} is the shared state between Alice and Bob, when Alice measures input $x \leftrightarrow A_x$ and announces output a, Bob's (unnormalized) state conditioned on the pair (x, a), will be,

$$\sigma^B_{a|x} = \mathrm{Tr}_A[(M_{a|x} \otimes 1_B) \rho_{AB}], \tag{B.9}$$

where we defined the projectors onto the eigenstates of A_x with eigenvalue a,

$$M_{a|x} = \sum_{a_1 \dots a_N} \delta_{a,a_x} |a_1 \cdots a_N\rangle_A \langle a_1 \cdots a_N|, \tag{B.10}$$

satisfying, $M^2_{a|x} = M_{a|x}$ and $\sum_a M_{a|x} = 1$, $\forall\ x$. Notice the summation over the outcomes of the unannounced inputs, which is due to the inaccessibility of these degrees of freedom to Bob. Using the spectral decomposition of each A_x, we also get an expression for the observables, i.e.,

$$A_x = \sum_{a=1}^{d_x} a\ M_{a|x}. \tag{B.11}$$

Now we will show the desired result that if ρ_{AB} is the following separable state,

$$\bar{\rho}_{AB} = \sum_{a_1,\dots,a_n} |a_1, \dots, a_n\rangle_A \langle a_1, \dots, a_n| \otimes \omega_{a_1 \dots a_n} \tag{B.12}$$

Bob's conditional state (B.9) will correspond to the unsteerable assemblage (B.4) if Alice measures the commuting observables defined in (B.11). We have,

$$\begin{aligned} \bar{\sigma}^B_{a|x} &= \mathrm{Tr}_A[(M_{a|x} \otimes 1_B)\bar{\rho}_{AB}] \\ &= \sum_{a_1 \dots a_N} \sum_{a'_1 \dots a'_N} \delta_{a,a'_x} |\langle a'_1 \dots a'_N | a_1 \dots a_N\rangle|^2 \omega_{a_1 \dots a_N} \\ &= \sum_{a_1 \dots a_N} \delta_{a,a_x} \omega_{a_1 \dots a_N}, \end{aligned} \tag{B.13}$$

matching exactly (B.4), where we used the orthonormality of the states (B.8) and the property $\delta^2_{i,j} = \delta_{i,j}$ of the Kronecker delta.

The generalization of the proof from discrete to continuous outcomes for Alice is straightforward, by replacing all summations with integrals, $\sum_{a_x} \to \int_{-\infty}^{\infty} da_x$ and the Kronecker delta with the Dirac delta function, $\delta_{a,a_x} \to \delta(a - a_x)$, which is a common practice when dealing with continuous Hilbert spaces.

B. PROOF OF THE EQUIVALENCE BETWEEN UNSTEERABILITY AND THE EXISTENCE OF A SEPARABLE MODEL

Appendix C

SDP, Dual and Optimal steering witnesses

First, we will show that the problem (8.18) can be expressed as an SDP [160, 328], and then derive its corresponding dual problem that will lead us to the optimal steering witnesses.

Consider a square $N \times N$ (moment) matrix $\mathbf{\Gamma}$ with arbitrary elements Γ_{ij}. Whether such a matrix is positive semidefinite, i.e. $\mathbf{\Gamma} \geq 0$, is equivalent to whether its smallest eigenvalue, $\lambda_\star$, is non-negative, i.e. $\lambda_\star \geq 0$. The steering detection method outlined in the detection method boils down to finding the maximized $\lambda_\star$ (name it, $\lambda_\star^{\max}$) over all possible (complex, in general) values of the moment matrix's elements $\{\Gamma_{ij}\}$ satisfying at the same time two types of constraints:

(a) All the observable elements of $\mathbf{\Gamma}$ are constrained to be equal to the observable values from the steering test [165].

(b) Linear relations between the unobservable elements, imposed by the commutativity constraint of Alice's operators and the utilization of Bob's operator algebra.

The semidefinite program corresponding to the problem described takes the following standard form [160],

$$\begin{aligned} \lambda_\star^{\max} \;=\; \max_{\lambda,\{\Gamma_{ij}\}} \quad & \lambda \\ \text{subject to} \quad & \mathbf{\Gamma} - \lambda\, 1 \geq 0 \\ & \mathrm{Tr}\left[\mathbf{\Gamma} A_i\right] = b_i, \quad i = 1, ..., k \\ & \mathrm{Tr}\left[\mathbf{\Gamma} C_j\right] = 0, \quad j = 1, ..., l \end{aligned} \tag{C.1}$$

known as the *primal problem*, the output of which will be $\lambda_\star^{\max}$. The first constraint in (C.1)

guarantees that the output of the SDP will be equal to the smallest eigenvalue of the given $\mathbf{\Gamma}$. The second and third constraints correspond to the constraints (a) and (b) respectively, with suitably chosen matrices A_i and C_j depending on the particular $\mathbf{\Gamma}$, while k and l correspond to the total number of observable elements and linear relations respectively. The values b_i are the ones obtained from the steering test, as explained in [165]. Concluding, steering will be witnessed from the SDP (C.1) if $\lambda_\star^{\max} < 0$.

To obtain the dual of the SDP (C.1), the solution of which will give us an upper bound on the quantity of interest $\lambda_\star^{\max}$, we start by writing the Lagrangian of this problem [328],

$$\begin{aligned}\mathcal{L} &= \lambda + \mathrm{tr}[\, Z \cdot (\mathbf{\Gamma} - \lambda\, \mathbb{1})\,] + \\ &\quad + \sum_{i=1}^{k} \mu_i^* \left(b_i - \mathrm{tr}[\mathbf{\Gamma} \cdot A_i]\right) + \sum_{j=1}^{l} \nu_j^* \Big(0 - \mathrm{tr}[\mathbf{\Gamma} \cdot C_j]\Big) \\ &= \sum_{i=1}^{k} \mu_i^* b_i + \lambda\,(1 - \mathrm{tr}Z) + \mathrm{tr}\left[\mathbf{\Gamma} \cdot \left(Z - \sum_{i=1}^{k} \mu_i^* A_i - \sum_{j=1}^{l} \nu_j^* C_j\right)\right]\end{aligned} \tag{C.2}$$

where the $N \times N$ hermitian matrix Z and the complex variables $\{\mu_i\}$ and $\{\nu_j\}$ are the *dual variables* to the first, second and third (sets of) constraints in (C.1) respectively. If we consider the maximized value $\max_{\lambda,\{\mathbf{\Gamma}\}_{ij}} \mathcal{L}$ over the primal variables $\lambda, \{\mathbf{\Gamma}\}_{ij}$, it's straightforward to see from (C.2) that, $\max_{\lambda,\{\mathbf{\Gamma}\}_{ij}} \mathcal{L} \geq \lambda_\star^{\max} + \mathrm{tr}[\, Z \cdot (\mathbf{\Gamma} - \lambda_\star^{\max}\, \mathbb{I})\,]$. Therefore choosing $Z \geq 0$, and since $\mathbf{\Gamma} - \lambda_\star^{\max}\, \mathbb{I} \geq 0$ due to the first constraint in (C.1), we find the following bound,

$$\max_{\lambda,\{\Gamma_{ij}\}} \mathcal{L} \geq \lambda_\star^{\max}, \tag{C.3}$$

Our goal is to use $\max_{\lambda,\{\Gamma_{ij}\}} \mathcal{L}$ to get a good estimate for the figure of merit $\lambda_\star^{\max}$, and in order for the bound (C.3) not to be trivial (i.e. equal to infinity), $\mathcal{L}$ should be bounded from above. We see that this occurs trivially if we set as constraints for the dual variables,

$$\mathrm{tr}\, Z = 1 \tag{C.4}$$

$$Z = \sum_{i=1}^{k} \mu_i^* A_i + \sum_{j=1}^{l} \nu_j^* C_j, \tag{C.5}$$

in addition to $Z \geq 0$. Imposing these constraints on $\mathcal{L}$, the Lagrangian (C.2) optimized over the primal variables takes the simple form,

$$\max_{\lambda,\{\Gamma_{ij}\}} \mathcal{L} = \sum_{i=1}^{k} \mu_i^* b_i \geq \lambda_\star^{\max}. \tag{C.6}$$

Therefore we are lead to an alternative approach to bound the desired quantity $\lambda_\star^{\max}$, by minimizing the left-hand side over the dual variables, for given $\{b_i\}$, leading us to the following *dual problem*,

$$\begin{aligned} \beta_\star \quad = \min_{\{\mu_i\},\{\nu_j\},\{Z_{ij}\}} \quad & \sum_{i=1}^{k} \mu_i^* b_i \\ \text{subject to} \quad & Z \geq 0 \\ & \text{tr} Z = 1, \\ & Z = \sum_{i=1}^{k} \mu_i^* A_i + \sum_{j=1}^{l} \nu_j^* C_j. \end{aligned} \tag{C.7}$$

The output of the dual (C.7), $\beta_\star$, is the tightest upper bound to the figure of merit $\lambda_\star^{\max}$ (C.6) since optimal coefficients $\{\bar{\mu}_i\}$ are found for the given observable values $\{b_i\}$. A negative value, $\beta_\star < 0$, is a sufficient condition for steerability, since it would imply that $\lambda_\star^{\max} < 0$, while a non-negative value $\beta_\star \geq 0$ is obtained for all unsteerable assemblages. Also, note that mere knowledge of the dual matrix Z (output of (C.7)) and the moment matrix $\mathbf{\Gamma}$ is enough to find $\beta_\star$ since, $\text{tr}[\mathbf{\Gamma} Z] = b_\star$, due to the second and third constraints in (C.1). To generalize this witness to any system, and therefore to arbitrary observations, consider arbitrary observable values $\{\bar{b}_i\} \neq \{b_i\}$ but keep the same coefficients $\{\bar{\mu}_i\}$ as before. The following linear inequality, or *steering witness*,

$$\sum_{i=1}^{k} \bar{\mu}_i^* \bar{b}_i \geq 0, \tag{C.8}$$

is satisfied by all unsteerable assemblages while a violation signals steering detection. For the particular $\{b_i\}$ the violation of (C.8) is maximal since the coefficients $\{\bar{\mu}_i\}$ are optimal for these particular values and non-optimal for any other, and therefore we refer to (C.8) as the *optimal steering witness* for the values $\{\bar{b}_i\} = \{b_i\}$, obtained by particular measurements and assemblages.

Finally, it is easy to verify that the primal problem is strictly feasible – i.e. there exists a $\mathbf{\Gamma}$ satisfying all the equality constraints which is strictly positive definite. As such, strong duality holds for the primal and dual SDP problems, such that the optimal value of the primal $\lambda_\star^{\max}$ and the optimal value of the dual $\beta_\star$ are equal.

Appendix D

Analytical derivation of non-linear steering criteria

Consider the moment matrix $\mathbf{\Gamma}_{\mathcal{R}}$ (8.20) obtained by the set of measurements, $\mathcal{S} = \{\mathbb{I}\otimes\mathbb{I}, A_1\otimes X, A_2\otimes Y, A_3\otimes Z\}$, where the statistics of Alice's unknown measurements A_1, A_2, A_3 also originate from "spin"-measurements X, Y, Z. In the following derivation, only the algebra of Alice's and Bob's observables will matter independently of their shared state ρ_{AB}. Applying the steps of the *Detection method*, i.e. commutativity and the operator algebra on Bob's side, the matrix (8.20) can be seen to get the simple form,

$$\mathbf{\Gamma}_{\mathcal{R}} = \begin{pmatrix} 1 & \langle A_1\otimes X\rangle & \langle A_2\otimes Y\rangle & \langle A_3\otimes Z\rangle \\ \langle A_1\otimes X\rangle & 1 & iR_1 & iR_2 \\ \langle A_2\otimes Y\rangle & -iR_1 & 1 & iR_3 \\ \langle A_3\otimes Z\rangle & -iR_2 & -iR_3 & 1 \end{pmatrix}, \tag{D.1}$$

where the three free parameters R_i are real, and equal to, $R_1 = \langle A_1A_2\otimes Z\rangle$, $R_2 = \langle A_2A_3\otimes X\rangle$, and $R_3 = -\langle A_1A_3\otimes Y\rangle$. Notice that the diagonal observable terms are equal to unity independently of the shared state, due to the fact that the Pauli operators, and the observables of Alice, take values ±1, and therefore square to the identity.

As explained in the main text, the necessary condition for unsteerability $\mathbf{\Gamma}_{\mathcal{R}} \geq 0$ implies the following conditions for its principal minors,

$$\det\mathbf{\Gamma}_{\mathcal{R}} = 1 - \langle A_1\otimes X\rangle^2 - \langle A_2\otimes Y\rangle^2 - \langle A_3\otimes Z\rangle^2 + f(R_1,R_2,R_3) \geq 0, \tag{D.2}$$

and,

$$\det P_2 = 1 - \langle A_2 \otimes Y\rangle^2 - \langle A_3 \otimes Z\rangle^2 - R_3^2 \geq 0, \tag{D.3}$$

$$\det P_3 = 1 - \langle A_1 \otimes X\rangle^2 - \langle A_3 \otimes Z\rangle^2 - R_2^2 \geq 0, \tag{D.4}$$

$$\det P_4 = 1 - \langle A_1 \otimes X\rangle^2 - \langle A_2 \otimes Y\rangle^2 - R_1^2 \geq 0, \tag{D.5}$$

with,

$$f(R_1, R_2, R_3) = (R_3 \langle A_1 \otimes X\rangle - R_2 \langle A_2 \otimes Y\rangle + R_1 \langle A_3 \otimes Z\rangle)^2 - R_1^2 - R_2^2 - R_3^2, \tag{D.6}$$

where the matrix P_i is obtained by $\mathbf{\Gamma}_{\mathcal{R}}$ by deleting its i-th row and column. Each of the conditions (D.3)-(D.5) leads to a steering criterion. For example,

$$\det P_2 \geq 0 \;\Rightarrow\; 1 - \langle A_2 \otimes Y\rangle^2 - \langle A_3 \otimes Z\rangle^2 \geq R_3^2 \geq 0, \tag{D.7}$$

and similarly for (D.4),(D.5). A violation of the last inequality in (D.7) signals steering since there exist no assignment for the free parameters R_i that can make (D.7) non-negative. When applied to the family of Werner states these criteria can be seen to detect steering for $w > \frac{1}{\sqrt{2}}$, which is a weaker detection than what the optimal witness (8.21) and the stronger non-linear criterion (8.22) can achieve. This is of course to be expected, since the former criteria only involve two measurement settings per site.

The stronger non-linear criterion (8.22), based on three measurement settings, can be derived from (D.2), where the contribution of the free parameters is grouped in the function $f(R_1, R_2, R_3)$. Our goal is to provide an upper bound for this function, say $f \leq f_{\max}$, and therefore limit its capability of making (D.2) positive for any given measurements. As a simple example of the logic behind, the analogous function in (D.3) would be $-R_3^2$ and is upper bounded by zero, as seen in the steering criterion (D.7). The maximum of $f(R_1, R_2, R_3)$ can be seen to correspond to the following values for R_1, R_2,

$$\partial_{R_1} f = 0\big|_{R_1 = R_1^\star} \;\Rightarrow\; R_1^\star = R_3 \frac{\langle A_1 \otimes X\rangle \langle A_3 \otimes Z\rangle}{\det P_2 + R_3^2} \tag{D.8}$$

$$\partial_{R_2} f = 0\big|_{R_2 = R_2^\star} \;\Rightarrow\; R_2^\star = -R_3 \frac{\langle A_1 \otimes X\rangle \langle A_2 \otimes Y\rangle}{\det P_2 + R_3^2}. \tag{D.9}$$

Therefore,

$$\begin{aligned} f(R_1, R_2, R_3) &\leq f\left(R_1^\star, R_2^\star, R_3\right) \\ &= -R_3^2 \frac{1 - \langle A_1 \otimes X\rangle^2 - \langle A_2 \otimes Y\rangle^2 - \langle A_3 \otimes Z\rangle^2}{\det P_2 + R_3^2}. \end{aligned} \tag{D.10}$$

We employ this bound in (D.2) and find that unsteerability of Bob's assemblage implies,

$$\begin{aligned} &\det \mathbf{\Gamma}_{\mathcal{R}} \geq 0 \quad \Rightarrow \\ &1 - \langle A_1 \otimes X\rangle^2 - \langle A_2 \otimes Y\rangle^2 - \langle A_3 \otimes Z\rangle^2 + f\left(R_1^\star, R_2^\star, R_3\right) \geq 0 \\ &\Leftrightarrow \left(1 - \langle A_1 \otimes X\rangle^2 - \langle A_2 \otimes Y\rangle^2 - \langle A_3 \otimes Z\rangle^2\right) \frac{\det P_2}{\det P_2 + R_3^2} \geq 0 \end{aligned} \tag{D.11}$$

Unsteerable assemblages necessarily satisfy $\det P_2 \geq 0$ (see (D.3)), and therefore the last inequality of (D.11) implies the desired non-linear criterion (8.22),

$$\langle A_1 \otimes X\rangle^2 + \langle A_2 \otimes Y\rangle^2 + \langle A_3 \otimes Z\rangle^2 \leq 1. \tag{D.12}$$

Notice that for the expressions (D.8), (D.9) we have assumed, $|\langle A_2 \otimes Y\rangle| < 1$ and $|\langle A_3 \otimes Z\rangle| < 1$. The cases where equality is attained in either (or both) inequalities should be treated separately, and it's straightforward to see that in every single case the same condition (D.12) is always obtained. Therefore, the validity of (D.12) extends to the whole range of possible experimental outcomes.

Appendix E

Optimal Witness for Lossy Single Photon state

In this appendix we provide the optimal steering witness which certifies the steerability of the noisy single photon state. As described in the main text, we used the 11×11 moment matrix defined by the set of operators $\mathcal{S} = \{\mathbb{I} \otimes \mathbb{I}, A_0 \otimes q_B, A_0 \otimes p_B, A_1 \otimes q_B, A_1 \otimes p_B, A_0^2 \otimes \mathbb{I}, A_1^2 \otimes \mathbb{I}, \mathbb{I} \otimes q_B^2, \mathbb{I} \otimes q_B p_B, \mathbb{I} \otimes p_B q_B, \mathbb{I} \otimes p_B^2\}$. First, note that moments of the form $\langle A_x^k \otimes B \rangle$ appearing in the moment matrix, with B an arbitrary string of length 2 or more, are expected in general to be hard to measure experimentally. In the following we therefore assume these terms to be unobservable (and therefore treat them as free parameters in the moment matrix), and apply only the operator algebra of Bob to place linear relations between them. On the other hand, local moments of the form $\langle \mathbb{I} \otimes B \rangle$ can be measured efficiently by Bob, for example by estimating his local Wigner function or by using a linear optics scheme proposed by Shchukin and Vogel [174], and therefore we keep these moments as observable. The freedom that the method gives us to keep only those measurements that can be efficiently performed as observable, highlights the flexibility of our approach to maintain experimental feasibility. Our ultimate goal is to provide an experimentally-friendly optimal steering witness.

The code was implemented using cvx for MATLAB [329], with the optimal inequality extracted by solving the primal (C.1) and dual (C.7) problems. The optimal inequality (C.8) for

the noisy single photon state with $\eta = 0.67$ is given by

$$\begin{aligned}\beta = 8.1657 - (\langle A_0 \otimes q_B\rangle + \langle A_1 \otimes p_B\rangle) + 0.2508\,(\langle A_0 \otimes q_B^3\rangle + \langle A_1 \otimes p_B^3\rangle) - 0.3110\,(\langle A_0^2\rangle + \langle A_1^2\rangle) \\ + 0.3205\,(\langle A_0^2 \otimes q_B^2\rangle + \langle A_1^2 \otimes p_B^2\rangle) + 0.3020\,(\langle A_0^2 \otimes p_B^2\rangle + \langle A_1^2 \otimes q_B^2\rangle) - 0.0001\,(\langle A_0^3 \otimes q_B\rangle + \langle A_1^3 \otimes p_B\rangle) \\ + 7.7217\,(\langle q_B^4\rangle + \langle p_B^4\rangle) + 15.5451\,\langle q_B^2 p_B^2\rangle - 31.0941\,(\langle q_B^2\rangle + \langle p_B^2\rangle) - 31.0903 i\,\langle q_B p_B\rangle \geq 0,\end{aligned} \tag{E.1}$$

satisified by all unsteerable assemblages, with the state numerically achieving the violation $\beta = -8.88 \times 10^{-4}$, which is (in magnitude) far above the numerical precision. Smaller values of η still show a violation, with numerical evidence suggesting all $\eta > 2/3$ demonstrate steering. The maximum violation of the inequality is $\beta_{\max} = -0.1556$, achieved for $\eta = 1$.

Let us now comment on the experimental feasibility for the estimation of the witness (E.1). Most of the terms in Eq. (E.1) can be efficiently measured by performing homodyne detection. The term that provides some extra difficulty in its measurement is the local fourth-order moment $\langle q_B^2 p_B^2\rangle$ of Bob. As mentioned before, for the estimation of this term Bob could implement tomography on his local state, which doesn't require conditioning on Alice's outcomes. A more efficient approach that avoids tomography would be to use a scheme proposed by Shchukin and Vogel [174], based on linear optics, that was designed to measure such local moments. A similar scheme was recently implemented by Avenhaus *et al.* [175], who managed to accurately measure moments of a single-mode up to eighth order. Therefore, we can safely conclude that the proposed steering witness (E.1) can be efficiently measured in the laboratory.

Finally, let us note that the only terms which appear in the inequality are those which were considered observable in the moment matrix. However, observable terms of the form $\langle A_x^k \otimes B\rangle$, which are experimentally demanding, were considered unobservable, and as one would expect steering detection weakens due to such relaxation. If on the other hand we consider all these experimentally demanding terms to be observable, we find the same critical noise $\eta > 2/3$, with only the magnitude of the violation increasing (and the inequality containing the additional observable terms absent in (E.1)).

Appendix F

Proof of Gaussian steering monogamy inequalities for mixed states

Here we will prove the monogamy inequalities (11.3) and (11.4) for the Gaussian steering $\mathcal{G}$, introduced in Chapter 11, of arbitrary mixed m-mode states with CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$. The two cases, respectively one-mode steered party, and one-mode steering party, will be proven separately, yet both will exploit recent results from [280].

F.1 Gaussian steering monogamy (11.3) for one steered mode

Theorem 1. Given a m-mode CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$, with each A_j comprising one mode, the Gaussian steering measure for one-mode steered party is monogamous:

$$\mathcal{G}^{(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) - \sum_{j\neq k} \mathcal{G}^{A_j\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \geq 0. \tag{F.1}$$

Proof. First of all we notice that it suffices to prove the inequality for tripartite states as in (11.5),

$$\mathcal{G}^{(AB)\to C}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{A\to C}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{B\to C}(\boldsymbol{\sigma}_{ABC}) \geq 0, \tag{F.2}$$

with C being a single mode and A, B being subsystems comprising arbitrary number of modes. One can then apply iteratively this inequality to obtain the corresponding m-partite one (F.1). Explicitly, assuming (F.2) holds, one can start by identifying $A \equiv A_1$, $B \equiv (A_2,\ldots,A_{k-1},A_{k+1},\ldots,A_m)$,

and $C = A_k$, to get:

$$\begin{aligned} & \mathcal{G}^{((A_1)(A_2\ldots,A_{k-1},A_{k+1},\ldots,A_m))\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \\ \geq\ & \mathcal{G}^{(A_1)\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) + \mathcal{G}^{(A_2\ldots,A_{k-1},A_{k+1},\ldots,A_m)\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \\ \vdots\ & \\ \geq\ & \sum_{j\neq k} \mathcal{G}^{A_j\to A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m})\,. \end{aligned}$$

We are thus left to prove the inequality (F.2) for a $(n_A + n_B + n_C)$-mode CM with $n_C = 1$. To do so, recall that from [272, 280] it is impossible for A and B to simultaneously steer the one-mode party C, that is, $\mathcal{G}^{A\to C}(\boldsymbol{\sigma}_{ABC}) > 0$ implies $\mathcal{G}^{B\to C}(\boldsymbol{\sigma}_{ABC}) = 0$ (and vice versa). Therefore, the monogamy relation (F.2) reduces to $\mathcal{G}^{(AB)\to C}(\boldsymbol{\sigma}_{ABC}) - \mathcal{G}^{A\to C}(\boldsymbol{\sigma}_{ABC}) \geq 0$ (or the analogous expression with swapped $A \leftrightarrow B$), which holds true because the Gaussian steering measure (for one-mode steered party C) is monotonically nonincreasing under local Gaussian quantum operations on the steering party (AB) [2], which include discarding subsystem B (or A). This proves Eq. (11.3) in the main text for any m-mode mixed-state CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$. □

F.2 Gaussian steering monogamy (11.4) for one steering mode

Theorem 2. Given a m-mode CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$, with each A_j comprising one mode, the Gaussian steering measure for one-mode steering party is monogamous:

$$\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\boldsymbol{\sigma}_{A_1\ldots A_m}) - \sum_{j\neq k} \mathcal{G}^{A_k\to A_j}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \geq 0. \tag{F.3}$$

Proof. In this case we have to recall the explicit expression of the Gaussian steering measure [2], defined for a bipartite $(n_A + n_B)$-mode state with CM $\boldsymbol{\sigma}_{AB}$ as

$$\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) = \begin{cases} 0, & \bar{\nu}_j^{AB\backslash A} \geq 1\ \forall j = 1,\ldots,n_B\,; \\ -\sum_{j:\bar{\nu}_j^{AB\backslash A}<1} \ln\left(\bar{\nu}_j^{AB\backslash A}\right), & \text{otherwise,} \end{cases} \tag{F.4}$$

where $\{\bar{\nu}_j^{AB\backslash A}\}_{j=1}^{n_B}$ denote the symplectic eigenvalues of the Schur complement $\bar{\boldsymbol{\sigma}}_{AB\backslash A}$ of $\boldsymbol{\sigma}_A$ in $\boldsymbol{\sigma}_{AB}$. By definition of the Schur complement, and observing that $\bar{\boldsymbol{\sigma}}_{AB\backslash A} > 0$ for any valid CM

$\boldsymbol{\sigma}_{AB}$, notice that we can write:

$$\begin{aligned}\sqrt{\frac{\det\boldsymbol{\sigma}_{AB}}{\det\boldsymbol{\sigma}_{A}}} &= \sqrt{\det\bar{\boldsymbol{\sigma}}_{AB\backslash A}} \\ &= \prod_{j=1}^{n_B}\bar{\nu}_j^{AB\backslash A} = \left(\prod_{j:\bar{\nu}_j^{AB\backslash A}<1}\bar{\nu}_j^{AB\backslash A}\right)\left(\prod_{j:\bar{\nu}_j^{AB\backslash A}\geq 1}\bar{\nu}_j^{AB\backslash A}\right) \\ &\geq \left(\prod_{j:\bar{\nu}_j^{AB\backslash A}<1}\bar{\nu}_j^{AB\backslash A}\right).\end{aligned} \tag{F.5}$$

Applying $(-\ln)$ to both sides and recalling Eq. (F.4) we get, for any CM $\boldsymbol{\sigma}_{AB}$ with $\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) > 0$, the bound

$$\mathcal{G}^{A\to B}(\boldsymbol{\sigma}_{AB}) \geq \frac{1}{2}\left[\mathcal{M}(\boldsymbol{\sigma}_A) - \mathcal{M}(\boldsymbol{\sigma}_{AB})\right] = -\frac{1}{2}\mathcal{J}_{B|A}(\boldsymbol{\sigma}_{AB}), \tag{F.6}$$

where $\mathcal{M}(\boldsymbol{\sigma}) = \ln\det\boldsymbol{\sigma}$ is the log-determinant of the CM $\boldsymbol{\sigma}$ [280], and the inequality (F.6) is tight when $n_B = 1$ [2]. We have further identified $\mathcal{J}_{B|A}(\boldsymbol{\sigma}_{AB}) = \mathcal{M}(\boldsymbol{\sigma}_{AB}) - \mathcal{M}(\boldsymbol{\sigma}_A)$ as the conditional log-determinant, a quantity which — in analogy to the standard conditional quantum entropy — is concave on the set of CMs [280] and subadditive with respect to the conditioned subsystems, i.e.,

$$\mathcal{J}_{BC|A}(\boldsymbol{\sigma}_{ABC}) \leq \mathcal{J}_{B|A}(\boldsymbol{\sigma}_{ABC}) + \mathcal{J}_{C|A}(\boldsymbol{\sigma}_{ABC}). \tag{F.7}$$

Notice that the latter property is simply equivalent to the strong subadditivity for the log-determinant of the CM $\boldsymbol{\sigma}_{ABC}$, $\mathcal{M}(\boldsymbol{\sigma}_{AB}) + \mathcal{M}(\boldsymbol{\sigma}_{AC}) - \mathcal{M}(\boldsymbol{\sigma}_A) - \mathcal{M}(\boldsymbol{\sigma}_{ABC}) \geq 0$, established in [277, 280].

To prove (F.3), we first observe that it is sufficient to consider without loss of generality the case in which the multimode term $\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}$ is nonzero (otherwise the inequality is trivial) and all the pairwise terms $\mathcal{G}^{A_k\to A_j}$ in the sum are also nonzero. Obviously, this will imply (F.3) even if some of the latter terms vanish, as there will be less to subtract in such cases.

Applying then Eq. (F.6) to the leftmost term in (F.3), and using repeatedly the negation of

(F.7), i.e. the superadditivity of the negative of the conditional log-determinant, we get

$$\begin{aligned}
& \mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \\
\geq\ & \frac{1}{2}\left[\mathcal{M}(\boldsymbol{\sigma}_{A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m})-\mathcal{M}(\boldsymbol{\sigma}_{A_1\ldots A_m})\right] \\
=\ & -\frac{1}{2}\mathcal{J}_{(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)|A_k}(\boldsymbol{\sigma}_{A_1,\ldots,A_m}) \\
\geq\ & -\frac{1}{2}\sum_{j\neq k}\mathcal{J}_{A_j|A_k}(\boldsymbol{\sigma}_{A_1\ldots A_m}) \\
=\ & \sum_{j\neq k}\mathcal{G}^{A_k\to A_j}(\boldsymbol{\sigma}_{A_1\ldots A_m})\,,
\end{aligned}$$

where in the last step we used again Eq. (F.6) which holds with equality on each of the two-mode terms involving A_k and any A_j, provided $\mathcal{G}^{A_k\to A_j}(\boldsymbol{\sigma}_{A_1\ldots A_m})>0$ as per assumption. This concludes the proof of Eq. (11.4) in the main text for any m-mode mixed-state CM $\boldsymbol{\sigma}_{A_1\ldots A_m}$. □

References

[1] Ioannis Kogias, Sammy Ragy, and Gerardo Adesso. Continuous-variable versus hybrid schemes for quantum teleportation of gaussian states. *Phys. Rev. A*, 89:052324, May 2014. 1, 12, 57

[2] Ioannis Kogias, Antony R. Lee, Sammy Ragy, and Gerardo Adesso. Quantification of gaussian quantum steering. *Physical review letters*, 114:060403, Feb 2015. 1, 12, 132, 141, 150, 152, 154, 156, 159, 160, 200, 201

[3] Ioannis Kogias and Gerardo Adesso. Einstein-podolsky-rosen steering measure for two-mode continuous variable states. *J. Opt. Soc. Am. B*, 32(4):A27, Apr 2015. 1, 12, 128, 139, 142, 152, 156, 160

[4] Ioannis Kogias, Paul Skrzypczyk, Daniel Cavalcanti, Antonio Acín, and Gerardo Adesso. Hierarchy of steering criteria based on moments for all bipartite quantum systems. *Physical review letters*, 115(21):210401, 2015. 1, 12, 117, 122, 139, 152

[5] Yu Xiang, Ioannis Kogias, Gerardo Adesso, and Qiongyi He. Multipartite gaussian steering: monogamy constraints and cryptographical applications. *arXiv preprint arXiv:1603.08173*, 2016. 1, 12, 151

[6] Ioannis Kogias, Yu Xiang, Qiong Yi He, and Gerardo Adesso. Unconditional security of entanglement-based quantum secret sharing schemes. *arXiv:1603.03224*, 2016. 1, 12, 153, 157, 158, 160, 165

[7] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49(2):1473, 1994. 3, 73, 77, 80, 82, 98

[8] Samuel L Braunstein and H Jeff Kimble. Teleportation of continuous quantum variables. *Physical Review Letters*, 80(4):869, 1998. 3, 73, 77, 80, 82, 98

[9] Ulrik L. Andersen and Timothy C. Ralph. High-fidelity teleportation of continuous-variable quantum states using delocalized single photons. *Phys. Rev. Lett.*, 111:050504, Aug 2013. 3, 80, 82, 83, 84, 98

[10] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895, Mar 1993. 3, 73, 75, 84, 88

[11] M. D. Reid. Demonstration of the einstein-podolsky-rosen paradox using nondegenerate parametric amplification. *Phys. Rev. A*, 40:913–923, Jul 1989. 6, 108, 129, 131, 137, 139, 142, 144, 148, 149, 150

[12] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Phys. Rev. Lett.*, 98:140402, Apr 2007. 6, 51, 110, 112, 122, 123, 128, 129, 131, 132, 134, 137, 139, 142, 146, 148, 149, 150, 152, 154, 175

[13] Hoi-Kwan Lau and Christian Weedbrook. Quantum secret sharing with continuous-variable cluster states. *Phys. Rev. A*, 88:042313, Oct 2013. 7, 153, 167, 173

[14] Tobias Eberle, Sebastian Steinlechner, Jöran Bauchrowitz, Vitus Händchen, Henning Vahlbruch, Moritz Mehmet, Helge Müller-Ebhardt, and Roman Schnabel. Quantum enhancement of the zero-area sagnac interferometer topology for gravitational wave detection. *Phys. Rev. Lett.*, 104:251102, Jun 2010. 7, 173

[15] Tobias Eberle, Vitus Händchen, and Roman Schnabel. Stable control of 10 db two-mode squeezed vacuum states of light. *Opt. Express*, 21(9):11546–11553, May 2013. 7, 173

[16] E. Schrödinger. Discussion of probability relations between separated systems. *Proc. Camb. Phil. Soc.*, 31:553, 1935. 10, 107

[17] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010. 17

[18] Markus Arndt and Klaus Hornberger. Testing the limits of quantum mechanical superpositions. *Nature Physics*, 10(4):271–277, 2014. 18

[19] Sandra Eibenberger, Stefan Gerlich, Markus Arndt, Marcel Mayor, and Jens Tüxen. Matter–wave interference of particles selected from a molecular library with masses exceeding 10000 amu. *Physical Chemistry Chemical Physics*, 15(35):14696–14700, 2013. 18

[20] MH Anderson, JR Ensher, MR Matthews, CE Wieman, and EA Cornell. Observation of bose-einstein condensation in a dilute atomic vapor. *Science*, 269:14, 1995. 18

[21] Keith C Schwab and Michael L Roukes. Putting mechanics into quantum mechanics. *Physics Today*, 58(7):36–42, 2005. 18

[22] T Rocheleau, T Ndukum, C Macklin, JB Hertzberg, AA Clerk, and KC Schwab. Preparation and detection of a mechanical resonator near the ground state of motion. *Nature*, 463(7277):72–75, 2010. 18

[23] Andreas Finke, Piyush Jain, and Silke Weinfurtner. On the observation of nonclassical excitations in bose-einstein condensates. *arXiv preprint arXiv:1601.06766*, 2016. 18

[24] Oriol Romero-Isart, Mathieu L Juan, Romain Quidant, and J Ignacio Cirac. Toward quantum superposition of living organisms. *New Journal of Physics*, 12(3):033015, 2010. 18

[25] Tongcang Li and Zhang-Qi Yin. Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator. *Science Bulletin*, pages 1–9, 2016. 18

[26] Steven Weinberg. What happens in a measurement? *Physical Review A*, 93(3):032124, 2016. 26

[27] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012. 29, 35, 131, 139, 152, 182

[28] G. Adesso, S. Ragy, and A. R. Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Syst. Inf. Dyn.*, 21:1440001, 2014. 29, 127, 131, 139, 145

[29] Pieter Kok and Brendon W Lovett. *Introduction to optical quantum information processing*. Cambridge University Press, 2010. 29, 31

[30] Gerardo Adesso and Fabrizio Illuminati. Entanglement in continuous-variable systems: recent advances and current perspectives. *Journal of Physics A: Mathematical and Theoretical*, 40(28):7821, 2007. 29

[31] Michał Oszmaniec, Andrzej Grudka, Michał Horodecki, and Antoni Wójcik. Creating a superposition of unknown quantum states. *Phys. Rev. Lett.*, 116:110403, Mar 2016. 33

[32] Bonny L Schumaker. Quantum mechanical pure states with gaussian wave functions. *Physics Reports*, 135(6):317–408, 1986. 35

[33] Alessandro Ferraro, Stefano Olivares, and Matteo GA Paris. Gaussian states in continuous variable quantum information. *arXiv preprint quant-ph/0503237*, 2005. 35

[34] Samuel L Braunstein and Peter Van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513, 2005. 35

[35] Nicolas J Cerf, Gerd Leuchs, and Eugene S Polzik. *Quantum information with continuous variables of atoms and light*. Imperial College Press, 2007. 35

[36] Norbert Schuch, J Ignacio Cirac, and Michael M Wolf. Quantum states on harmonic lattices. *Communications in mathematical physics*, 267(1):65–92, 2006. 35

[37] Michael M Wolf, Geza Giedke, and J Ignacio Cirac. Extremality of gaussian quantum states. *Physical review letters*, 96(8):080502, 2006. 35

[38] R Simon, N Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: U (n) invariance, squeezing, and normal forms. *Physical Review A*, 49(3):1567, 1994. 36

[39] R Simon, ECG Sudarshan, and N Mukunda. Gaussian-wigner distributions in quantum mechanics and optics. *Physical Review A*, 36(8):3868, 1987. 36

[40] VV Dodonov, EV Kurmyshev, and VI Man'ko. Generalized uncertainty relation and correlated coherent states. *Physics Letters A*, 79(2):150–152, 1980. 36

[41] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003. 37

[42] Alessio Serafini and Gerardo Adesso. Standard forms and entanglement engineering of multimode gaussian states under local operations. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8041, 2007. 45

[43] Gerardo Adesso. Generic entanglement and standard form for n-mode pure gaussian states. *Physical review letters*, 97(13):130502, 2006. 45

[44] Géza Giedke and Barbara Kraus. Gaussian local unitary equivalence of n-mode gaussian states and gaussian transformations by local operations with classical communication. *Physical Review A*, 89(1):012335, 2014. 45

[45] Rajiah Simon. Peres-horodecki separability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2726, 2000. 45, 62

[46] Gerardo Adesso, Alessio Serafini, and Fabrizio Illuminati. Multipartite entanglement in three-mode gaussian states of continuous-variable systems: Quantification, sharing structure, and decoherence. *Physical Review A*, 73(3):032345, 2006. 46

[47] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. 50

[48] Artur K Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661, 1991. 50

[49] A Ferraro, L Aolita, D Cavalcanti, FM Cucchietti, and A Acin. Almost all quantum states have nonclassical correlations. *Physical Review A*, 81(5):052318, 2010. 51

[50] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Rev. Mod. Phys.*, 84:1655–1707, Nov 2012. 51, 139

[51] Animesh Datta, Anil Shaji, and Carlton M Caves. Quantum discord and the power of one qubit. *Physical review letters*, 100(5):050502, 2008. 51

[52] Gerardo Adesso, Thomas Bromley, and Marco Cianciaruso. Measures and applications of quantum correlations. *arXiv preprint quant-ph/1605.00806*, 2016. 51

[53] Daniel Cavalcanti, Leandro Aolita, Sergio Boixo, Kavan Modi, Marco Piani, and Andreas Winter. Operational interpretations of quantum discord. *Physical Review A*, 83(3):032324, 2011. 51

[54] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009. 51, 68

[55] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. 51, 105, 106, 109, 131, 152

[56] D Cavalcanti and P Skrzypczyk. Quantum steering: a short review with focus on semidefinite programming. *arXiv preprint arXiv:1604.00501*, 2016. 51

[57] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1:195, 1964. 51, 106

[58] J. S. Bell. The theory of local beables. *Epistemological Lett.*, 9, 1976. 51, 106

[59] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. 52, 175

[60] B. Hensen *et al.* Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. 52, 107

[61] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015. 52, 107

[62] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of bells theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015. 52, 107

[63] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical review letters*, 96(1):010401, 2006. 59

[64] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009. 59, 131, 133, 138, 175

[65] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, Cambridge, 2000. 59

[66] Maciej Lewenstein, B Kraus, JI Cirac, and P Horodecki. Optimization of entanglement witnesses. *Physical Review A*, 62(5):052310, 2000. 61

[67] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, Aug 1996. 61

[68] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, 1996. 62

[69] R. Simon. *Phys. Rev. Lett.*, 84:2726, 2000. 62, 63, 133, 223

[70] R. F. Werner and M. M. Wolf. *Phys. Rev. Lett.*, 86:3658, 2001. 62, 133, 138

[71] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: is there a bound entanglement in nature? *Physical Review Letters*, 80(24):5239, 1998. 62

[72] Lu-Ming Duan, Géza Giedke, Juan Ignacio Cirac, and Peter Zoller. Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84(12):2722, 2000. 63

[73] E Shchukin and W Vogel. Inseparability criteria for continuous bipartite quantum states. *Physical review letters*, 95(23):230502, 2005. 63, 65

[74] Carl D Meyer. *Matrix analysis and applied linear algebra*. Siam, 2000. 64, 127

[75] Vlatko Vedral, Martin B Plenio, Michael A Rippin, and Peter L Knight. Quantifying entanglement. *Physical Review Letters*, 78(12):2275, 1997. 66, 68, 70

[76] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical review letters*, 76(5):722, 1996. 66

[77] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, 1996. 66, 67

[78] Martin B Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Information and Computation*, 7(1):001–051, 2007. 68

[79] MS Kim, Jinhyoung Lee, D Ahn, and PL Knight. Entanglement induced by a single-mode heat environment. *Physical Review A*, 65(4):040101, 2002. 69

[80] Guifré Vidal and Reinhard F Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, 2002. 69

[81] Karol Życzkowski, Paweł Horodecki, Anna Sanpera, and Maciej Lewenstein. Volume of the set of separable states. *Physical Review A*, 58(2):883, 1998. 69

[82] Gerardo Adesso, Davide Girolami, and Alessio Serafini. Measuring gaussian quantum information and correlations using the rényi entropy of order 2. *Phys. Rev. Lett.*, 109:190502, Nov 2012. 70, 71

[83] John C Baez. Rényi entropy and free energy. *arXiv preprint arXiv:1102.2098*, 2011. 70

[84] Robert Alicki and Mark Fannes. Note on multiple additivity of minimal renyi entropy output of the werner-holevo channels. *Open systems & information dynamics*, 11(04):339–342, 2004. 70

[85] Michael M Wolf and J Eisert. Classical information capacity of a class of quantum channels. *New Journal of Physics*, 7(1):93, 2005. 70

[86] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, 2009. 70

[87] Oscar CO Dahlsten, Renato Renner, Elisabeth Rieper, and Vlatko Vedral. Inadequacy of von neumann entropy for characterizing extractable work. *New Journal of Physics*, 13(5):053015, 2011. 70

[88] Fabio Franchini, AR Its, and VE Korepin. Renyi entropy of the xy spin chain. *Journal of Physics A: Mathematical and Theoretical*, 41(2):025302, 2007. 70

[89] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932, Dec 1998. 73, 75

[90] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999. 73

[91] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001. 73

[92] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 80:1121, Feb 1998. 73

[93] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997. 73, 99

[94] Akira Furusawa, Jens Lykke Sørensen, Samuel L Braunstein, Christopher A Fuchs, H Jeff Kimble, and Eugene S Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998. 73, 80

[95] Mark Riebe, H Häffner, CF Roos, W Hänsel, J Benhelm, GPT Lancaster, TW Körber, C Becher, F Schmidt-Kaler, DFV James, et al. Deterministic quantum teleportation with atoms. *Nature*, 429(6993):734–737, 2004. 73

[96] MD Barrett, J Chiaverini, T Schaetz, J Britton, WM Itano, JD Jost, E Knill, C Langer, D Leibfried, R Ozeri, et al. Deterministic quantum teleportation of atomic qubits. *Nature*, 429(6993):737–739, 2004. 73

[97] Brian Julsgaard, Jacob Sherson, J Ignacio Cirac, Jaromír Fiurášek, and Eugene S Polzik. Experimental demonstration of quantum memory for light. *Nature*, 432(7016):482–486, 2004. 73

[98] Jacob F Sherson, Hanna Krauter, Rasmus K Olsson, Brian Julsgaard, Klemens Hammerer, Ignacio Cirac, and Eugene S Polzik. Quantum teleportation between light and matter. *Nature*, 443(7111):557–560, 2006. 73

[99] N. Takei *et al.* Experimental demonstration of quantum teleportation of a squeezed state. *Phys. Rev. A*, 72:042304, Oct 2005. 73

[100] Hidehiro Yonezawa, Samuel L. Braunstein, and Akira Furusawa. Experimental demonstration of quantum teleportation of broadband squeezing. *Phys. Rev. Lett.*, 99:110503, Sep 2007. 73

[101] K. Honda *et al.* Storage and retrieval of a squeezed vacuum. *Phys. Rev. Lett.*, 100:093601, Mar 2008. 73

[102] Jürgen Appel, Eden Figueroa, Dmitry Korystov, M. Lobino, and A. I. Lvovsky. Quantum memory for squeezed light. *Phys. Rev. Lett.*, 100:093602, Mar 2008. 73

[103] T Chaneliere, DN Matsukevich, SD Jenkins, S-Y Lan, TAB Kennedy, and A Kuzmich. Storage and retrieval of single photons transmitted between remote quantum memories. *Nature*, 438(7069):833–836, 2005. 73

[104] Kyung Soo Choi, Hui Deng, Julien Laurat, and HJ Kimble. Mapping photonic entanglement into and out of a quantum memory. *Nature*, 452(7183):67–71, 2008. 73

[105] Hidehiro Yonezawa, Takao Aoki, and Akira Furusawa. Demonstration of a quantum teleportation network for continuous variables. *Nature*, 431(7007):430–433, 2004. 73

[106] H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, Heng Shen, T. Fernholz, and E. S. Polzik. Deterministic quantum teleportation between distant atomic objects. *Nature Phys.*, 9:400, 2013. 73

[107] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, and C. Monroe. Quantum teleportation between distant matter qubits. *Science*, 323:486, 2009. 73

[108] Morgan P. Hedges, Jevon J. Longdell, Yongmin Li, and Matthew J. Sellars. Efficient quantum memory for light. *Nature*, 465:1052, 2010. 73

[109] Noriyuki Lee, Hugo Benichi, Yuishi Takeno, Shuntaro Takeda, James Webb, Elanor Huntington, and Akira Furusawa. Teleportation of nonclassical wave packets of light. *Science*, 332:330, 2011. 73

[110] K. Jensen *et al.* Quantum memory for entangled continuous-variable states. *Nature Phys.*, 7:13, 2011. 73, 101

[111] X.-S. Ma *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489:269, 2012. 73

[112] N. Cerf, G. Leuchs, and E. S. Polzik, editors. *Quantum Information with Continuous Variables of Atoms and Light*. Imperial College Press, London, 2007. 73

[113] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513, 2005. 73

[114] Samuel L Braunstein, Christopher A Fuchs, and H Jeff Kimble. Criteria for continuous-variable quantum teleportation. *Journal of Modern Optics*, 47(2-3):267–278, 2000. 79, 82, 84

[115] Sandu Popescu. Bell's inequalities versus teleportation: What is nonlocality? *Phys. Rev. Lett.*, 72:797, Feb 1994. 79

[116] Melvyn Ho, Jean-Daniel Bancal, and Valerio Scarani. Device-independent certification of the teleportation of a qubit. *Phys. Rev. A*, 88:052318, Nov 2013. 79

[117] Giulio Chiribella and Gerardo Adesso. Quantum benchmarks for pure single-mode gaussian states. *Phys. Rev. Lett.*, 112:010501, Jan 2014. 79, 80, 84, 85, 86, 89, 98

[118] S. Massar and S. Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74:1259–1263, Feb 1995. 79

[119] Dagmar Bruss and Chiara Macchiavello. Optimal state estimation for d-dimensional quantum systems. 253:249, 1999. 79

[120] K. Hammerer, M. M. Wolf, E. S. Polzik, and J. I. Cirac. Quantum benchmark for storage and transmission of coherent states. *Phys. Rev. Lett.*, 94:150503, Apr 2005. 79, 85, 92

[121] M Owari, M B Plenio, E S Polzik, A Serafini, and M M Wolf. Squeezing the limit: quantum benchmarks for the teleportation and storage of squeezed states. *New J. Phys.*, 10(11):113014, 2008. 79

[122] J. Calsamiglia, M. Aspachs, R. Muñoz Tapia, and E. Bagan. Phase-covariant quantum benchmarks. *Phys. Rev. A*, 79:050301(R), May 2009. 79

[123] Gerardo Adesso and Giulio Chiribella. Quantum benchmark for teleportation and storage of squeezed states. *Phys. Rev. Lett.*, 100:170503, Apr 2008. 79

[124] Madalin Guţă, Peter Bowles, and Gerardo Adesso. Quantum-teleportation benchmarks for independent and identically distributed spin states and displaced thermal states. *Phys. Rev. A*, 82:042310, Oct 2010. 79

[125] Armin Uhlmann. The transition probability in the state space of a^*-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976. 79

[126] Richard Jozsa. Fidelity for mixed quantum states. *Journal of modern optics*, 41(12):2315–2323, 1994. 79

[127] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023, 2008. 79, 151

[128] Klemens Hammerer, Anders S. Sørensen, and Eugene S. Polzik. Quantum interface between light and atomic ensembles. *Rev. Mod. Phys.*, 82:1041, Apr 2010. 79

[129] Akira Furusawa and Nobuyuki Takei. Quantum teleportation for continuous variables and related quantum information processing. *Physics reports*, 443(3):97–119, 2007. 79

[130] Warwick P. Bowen, Nicolas Treps, Ben C. Buchler, R. Schnabel, Timothy C. Ralph, Thomas Symul, and Ping Koy Lam. *IEEE Journal of Selected Topics in Quantum Electronics*, 9:1519, Nov/Dec 2003. 80, 81, 98

[131] T. Eberle *et al.* Quantum enhancement of the zero-area sagnac interferometer topology for gravitational wave detection. *Phys. Rev. Lett.*, 104:251102, Jun 2010. 80, 87, 92, 99

[132] Tobias Eberle, Vitus Händchen, and Roman Schnabel. Stable control of 10 db two-mode squeezed vacuum states of light. *Opt. Express*, 21(9):11546, May 2013. 80, 87, 92, 99

[133] Paulina Marian and Tudor A. Marian. Continuous-variable teleportation in the characteristic-function description. *Phys. Rev. A*, 74:042306, Oct 2006. 81

[134] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati. *Phys. Rev. A*, 76:022301, Aug 2007. 81, 89, 92, 98

[135] Giulio Chiribella and Jinyu Xie. Optimal design and quantum benchmarks for coherent state amplifiers. *Phys. Rev. Lett.*, 110:213602, May 2013. 84, 88

[136] Fabio Dell'Anno, Silvio De Siena, Gerardo Adesso, and Fabrizio Illuminati. *Phys. Rev. A*, 82:062329, Dec 2010. 89, 92, 98

[137] Gerardo Adesso and Fabrizio Illuminati. Equivalence between entanglement and the optimal fidelity of continuous variable teleportation. *Phys. Rev. Lett.*, 95:150503, Oct 2005. 92

[138] T Opatrnỳ, G Kurizki, and D-G Welsch. Improvement on teleportation of continuous variables by photon subtraction via conditional measurement. *Physical Review A*, 61(3):032302, 2000. 98

[139] PT Cochrane, TC Ralph, and GJ Milburn. Teleportation improvement by conditional measurements on the two-mode squeezed vacuum. *Physical Review A*, 65(6):062306, 2002. 98

[140] Stefano Olivares, Matteo GA Paris, and Rodolfo Bonifacio. Teleportation improvement by inconclusive photon subtraction. *Physical Review A*, 67(3):032314, 2003. 98

[141] Akira Kitagawa, Masahiro Takeoka, Masahide Sasaki, and Anthony Chefles. Entanglement evaluation of non-gaussian states generated by photon subtraction from squeezed states. *Physical Review A*, 73(4):042310, 2006. 98

[142] Shuntaro Takeda, Takahiro Mizuta, Maria Fuwa, Peter van Loock, and Akira Furusawa. Deterministic quantum teleportation of photonic quantum bits by a hybrid technique. *Nature*, 500(7462):315–318, 2013. 100

[143] Seung-Woo Lee and Hyunseok Jeong. Near-deterministic quantum teleportation and resource-efficient quantum computation using linear optics and hybrid qubits. *Physical Review A*, 87(2):022326, 2013. 100

[144] Peter van Loock. Optical hybrid approaches to quantum information. *Laser & Photonics Reviews*, 5(2):167–200, 2011. 100

[145] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014. 107

[146] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982. 107

[147] E. Schrödinger. Probability relations between separated systems. *Proc. Camb. Phil. Soc.*, 32:446, 1936. 107

[148] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid. Experimental criteria for steering and the einstein-podolsky-rosen paradox. *Phys. Rev. A*, 80:032112, Sep 2009. 118, 121, 126, 129, 131, 139, 141, 142, 143, 148, 149, 152

[149] S. J. Jones, H. M. Wiseman, and A. C. Doherty. Entanglement, einstein-podolsky-rosen correlations, bell nonlocality, and steering. *Phys. Rev. A*, 76:052116, Nov 2007. 121, 128, 131, 132, 137, 139, 142, 146, 148, 152, 154

[150] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro. Revealing hidden einstein-podolsky-rosen nonlocality. *Phys. Rev. Lett.*, 106:130402, Mar 2011. 121, 128, 131, 139, 150

[151] James Schneeloch, Curtis J. Broadbent, Stephen P. Walborn, Eric G. Cavalcanti, and John C. Howell. Einstein-podolsky-rosen steering inequalities from entropic uncertainty relations. *Phys. Rev. A*, 87:062103, Jun 2013. 121, 131, 150

[152] Tanumoy Pramanik, Marc Kaplan, and A. S. Majumdar. Fine-grained einstein-podolsky-rosen˘steering inequalities. *Phys. Rev. A*, 90:050305, Nov 2014. 121

[153] Priyanka Chowdhury, Tanumoy Pramanik, and Archan S Majumdar. Higher security in one-sided device independent quantum key distribution from more uncertain systems. *arXiv preprint arXiv:1503.04697*, 2015. 121

[154] Eric G Cavalcanti, Christopher J Foster, Maria Fuwa, and Howard M Wiseman. Analogue of the chsh inequality for steering. *J. Opt. Soc. Am. B*, 32(4):A74, 2015. 121

[155] S. J. Jones and H. M. Wiseman. Nonlocality of a single photon: Paths to an einstein-podolsky-rosen-steering experiment. *Phys. Rev. A*, 84:012110, Jul 2011. 121, 122, 128

[156] Matthew F. Pusey. Negativity and steering: A stronger peres conjecture. *Phys. Rev. A*, 88:032313, Sep 2013. 121, 123, 132, 138

[157] Marco Piani and John Watrous. Necessary and sufficient quantum information characterization of einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 114:060404, Feb 2015. 121, 131, 150

[158] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti. Quantifying einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 112:180404, May 2014. 121, 131

[159] Tobias Moroder, Oleg Gittsovich, Marcus Huber, Roope Uola, and Otfried Gühne. Steering maps and their application to dimension-bounded steering. *arXiv preprint arXiv:1412.2623*, 2014. 121

[160] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996. 121, 189

[161] E. Shchukin and W. Vogel. Inseparability criteria for continuous bipartite quantum states. *Phys. Rev. Lett.*, 95:230502, Nov 2005. 122

[162] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. 122

[163] For details, see Appendix (Supplemental Material). 123, 126, 127

[164] There elements may appear non-observable, due to B in general being non-hermitian. However, one can always find observables W and Ω s.t., $B = W - i\Omega$, for any operator B. Henceforth, the desired element can be written as a linear combination of mean values of directly observable quantities. 124

[165] From an experimental point of view, these values (i.e. the data) will be equal to the values observed in the experiment. From a theoretical point of view, when one wants to check the steerability of a quantum state, as we do here, these values will be equal to the values predicted by the state under consideration. 124, 129, 189, 190

[166] Elements of the form $\langle A_1 A_2 \cdots \otimes B_1 \rangle$ for example, are unobservable since they would require a simultaneous measurement of multiple inputs for Alice in order to determine the outcome of the product $A_1 A_2 \cdots$. In a steering test such measurements cannot be performed. 124

[167] Reinhard F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989. 126

[168] Agedi N. Boto, Pieter Kok, Daniel S. Abrams, Samuel L. Braunstein, Colin P. Williams, and Jonathan P. Dowling. Quantum interferometric optical lithography: Exploiting entanglement to beat the diffraction limit. *Phys. Rev. Lett.*, 85:2733–2736, Sep 2000. 128

[169] Mark Hillery. Amplitude-squared squeezing of the electromagnetic field. *Phys. Rev. A*, 36:3796–3802, Oct 1987. 128, 153, 157, 166, 175

[170] S. M. Tan, D. F. Walls, and M. J. Collett. Nonlocality of a single photon. *Phys. Rev. Lett.*, 66:252–255, Jan 1991. 128

[171] Lucien Hardy. Nonlocality of a single photon revisited. *Phys. Rev. Lett.*, 73:2279–2283, Oct 1994. 128

[172] Maria Fuwa, Shuntaro Takeda, Marcin Zwierz, Howard M. Wiseman, and Akira Furusawa. Experimental proof of nonlocal wavefunction collapse for a single particle using homodyne measurements. *Nat. Commun.*, 6, Mar 2015. 128

[173] Egilberto Lombardi, Fabio Sciarrino, Sandu Popescu, and Francesco De Martini. Teleportation of a vacuum˘one-photon qubit. *Phys. Rev. Lett.*, 88:070402, Jan 2002. 128

[174] E. V. Shchukin and W. Vogel. Nonclassical moments and their measurement. *Phys. Rev. A*, 72:043808, Oct 2005. 129, 197, 198

[175] M. Avenhaus, K. Laiho, M. V. Chekhova, and C. Silberhorn. Accessing higher order correlations in quantum optical states by time multiplexing. *Phys. Rev. Lett.*, 104:063602, Feb 2010. 129, 198

[176] Roope Uola, Tobias Moroder, and Otfried Gühne. Joint measurability of generalized measurements implies classicality. *Phys. Rev. Lett.*, 113:160403, Oct 2014. 130

[177] Marco Túlio Quintino, Tamás Vértesi, and Nicolas Brunner. Joint measurability, einstein-podolsky-rosen steering, and bell nonlocality. *Phys. Rev. Lett.*, 113:160402, Oct 2014. 130

[178] Roope Uola, Costantino Budroni, Otfried Gühne, and Juha-Pekka Pellonpää. A one-to-one mapping between steering and joint measurability problems. *arXiv preprint arXiv:1507.08633*, 2015. 130

[179] D Cavalcanti, P Skrzypczyk, GH Aguilar, RV Nery, PH Ribeiro, and SP Walborn. Detecting multipartite entanglement with untrusted measurements in asymmetric quantum networks. *Nat. Commun.*, 6:7941, 2014. 130

[180] Q. Y. He and M. D. Reid. Genuine multipartite einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 111:250403, Dec 2013. 130, 131, 139, 152, 156, 168, 175

[181] Seiji Armstrong, Meng Wang, Run Yan Teh, Qihuang Gong, Qiongyi He, Jiri Janousek, Hans-Albert Bachor, Margaret D. Reid, and Ping Koy Lam. Multipartite einstein-podolsky-rosen steering and genuine tripartite entanglement with optical networks. *Nat Phys*, 11:167, May 2015. 130

[182] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde. Experimental epr-steering using bell-local states. *Nat. Phys.*, 6:845–849, Sep 2010. 131

[183] Tobias Eberle, Vitus Händchen, Jörg Duhme, Torsten Franz, Reinhard F. Werner, and Roman Schnabel. Strong einstein-podolsky-rosen entanglement from a single squeezed light source. *Phys. Rev. A*, 83:052329, May 2011. 131

[184] Vitus Händchen, Tobias Eberle, Sebastian Steinlechner, Aiko Samblowski, Torsten Franz, Reinhard F. Werner, and Roman Schnabel. Observation of one-way einstein-podolsky-rosen steering. *Nat. Photon.*, 6:596–599, Sep 2012. 131, 136, 138

[185] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde. Arbitrarily loss-tolerant einstein-podolsky-rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Phys. Rev. X*, 2:031003, Jul 2012. 131

[186] Bernhard Wittmann, Sven Ramelow, Fabian Steinlechner, Nathan K Langford, Nicolas Brunner, Howard M Wiseman, Rupert Ursin, and Anton Zeilinger. Loophole-free einsteinpodolskyrosen experiment via quantum steering. *New Journal of Physics*, 14(5):053030, 2012. 131

[187] Devin H. Smith, Geoff Gillett, Marcelo P. de Almeida, Cyril Branciard, Alessandro Fedrizzi, Till J. Weinhold, Adriana Lita, Brice Calkins, Thomas Gerrits, Howard M. Wiseman, Sae Woo Nam, and Andrew G. White. Conclusive quantum steering with superconducting transition-edge sensors. *Nat. Commun.*, 3, Jan 2012. 131

[188] Sebastian Steinlechner, Jöran Bauchrowitz, Tobias Eberle, and Roman Schnabel. Strong einstein-podolsky-rosen steering with unconditional entangled states. *Phys. Rev. A*, 87:022104, Feb 2013. 131

[189] Sacha Kocsis, Michael JW Hall, Adam J Bennet, Dylan J Saunders, and Geoff J Pryde. Experimental measurement-device-independent verification of quantum steering. *Nature communications*, 6, 2015. 131, 152

[190] Kai Sun, Jin-Shi Xu, Xiang-Jun Ye, Yu-Chun Wu, Jing-Ling Chen, Chuan-Feng Li, and Guang-Can Guo. Experimental demonstration of the einstein-podolsky-rosen steering game based on the all-versus-nothing proof. *Physical review letters*, 113(14):140402, 2014. 131

[191] E. C. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman. Entanglement verification and steering when alice and bob cannot be trusted. *Phys. Rev. A*, 87:032306, 2013. 131

[192] Tanumoy Pramanik, Marc Kaplan, and Archan S Majumdar. Fine-grained EPR-steering inequalities. *arXiv:1404.7050 [quant-ph]*, 2014. 131

[193] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen. Asymmetric gaussian steering: When alice and bob disagree. *Phys. Rev. A*, 81:022101, Feb 2010. 131

[194] M. D. Reid. Monogamy inequalities for the einstein-podolsky-rosen paradox and quantum steering. *Phys. Rev. A*, 88:062108, Dec 2013. 131, 139, 150

[195] Joseph Bowles, Tamás Vértesi, Marco Túlio Quintino, and Nicolas Brunner. One-way einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 112:200402, May 2014. 131

[196] Martin B. Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Info. Comput.*, 7(1):1, January 2007. 131, 133

[197] A. C. S. Costa, R. M. Angelo, and M. W. Beims. Hierarchy of quantum correlation measures for two-qubit x states. *arXiv:1311.5702 [quant-ph]*, 2013. 131

[198] G. Adesso and F. Illuminati. Entanglement in continuous-variable systems: recent advances and current perspectives. *J. Phys. A: Math. Theor.*, 40:7821, 2007. 131, 133, 134, 139, 152, 153

[199] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Phys. Rev. Lett.*, 89:137903, Sep 2002. 131

[200] Jaromír Fiurášek. Gaussian transformations and distillation of entangled gaussian states. *Phys. Rev. Lett.*, 89:137904, Sep 2002. 131, 132

[201] Nathan Walk, Howard M. Wiseman, and Timothy C. Ralph. Continuous variable one-sided device independent quantum key distribution. *arXiv:1405.6593 [quant-ph]*, 2014. 131, 137, 138, 139, 147, 148, 150, 152, 159, 168, 170

[202] G. Adesso, D. Girolami, and A. Serafini. *Phys. Rev. Lett.*, 109:190502, 2012. 131, 133, 134, 139

[203] Asher Peres. All the bell inequalities. *Found. Phys.*, 29(4):589–614, 1999. 132, 138

[204] Tobias Moroder, Oleg Gittsovich, Marcus Huber, and Otfried Gühne. Steering bound entangled states: A counterexample to the stronger peres conjecture. *arXiv:1405.0262 [quant-ph]*, 2014. 132, 138

[205] Tamas Vértesi and Nicolas Brunner. Disproving the peres conjecture: Bell nonlocality from bipartite bound entanglement. *arXiv:1405.4502 [quant-ph]*, 2014. 132, 138

[206] J. Williamson. *Am. J. Math.*, 58:141, 1936. 132

[207] Alessio Serafini. Multimode uncertainty relations and separability of continuous variable states. *Phys. Rev. Lett.*, 96:110402, Mar 2006. 132

[208] G. Vidal and R. F. Werner. *Phys. Rev. A*, 65:032314, 2002. 133

[209] M. B. Plenio. *Phys. Rev. Lett.*, 95:090503, 2005. 133

[210] A. Peres. *Phys. Rev. Lett.*, 77:1413, 1996. 133

[211] M. Horodecki, P. Horodecki, and R. Horodecki. *Phys. Lett. A*, 223:1, 1996. 133

[212] G. Adesso, A. Serafini, and F. Illuminati. *Phys. Rev. A*, 70:022318, 2004. 133, 135, 146

[213] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, Cambridge, 2013. 133, 134

[214] Rodrigo Gallego and Leandro Aolita. Resource theory of steering. *Physical Review X*, 5(4):041008, 2015. 134

[215] G. Adesso, A. Serafini, and F. Illuminati. *Phys. Rev. Lett.*, 92:087901, 2004. 135

[216] Sabine Wollmann, Nathan Walk, Adam J. Bennet, Howard M. Wiseman, and Geoff J. Pryde. Observation of genuine one-way einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 116:160403, Apr 2016. 136, 139, 152, 160

[217] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, Jan 2012. 137

[218] A. K. Ekert. *Phys. Rev. Lett.*, 67:661, 1991. 137, 147

[219] Se-Wan Ji, Jaehak Lee, Jiyong Park, and Hyunchul Nha. Quantum steering of gaussian states via non-gaussian measurements. *arXiv preprint arXiv:1511.02649*, 2015. 139

[220] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs. *Colloquium* : The einstein-podolsky-rosen paradox: From concepts to applications. *Rev. Mod. Phys.*, 81. 139, 142, 144, 147, 152

[221] Sania Jevtic, Matthew Pusey, David Jennings, and Terry Rudolph. Quantum steering ellipsoids. *Phys. Rev. Lett.*, 113:020402, Jul 2014. 139

[222] G. Adesso and A. Datta. *Phys. Rev. Lett.*, 105:030501, 2010. 139

[223] P. Giorda and M. G. A. Paris. *Phys. Rev. Lett.*, 105:020503, 2010. 139

[224] Q. Y. He, Q. H. Gong, and M. D. Reid. Classifying directional gaussian quantum entanglement, epr steering and discord. *arXiv:1406.6708 [quant-ph]*, 2014. 139

[225] G. Adesso and F. Illuminati. *Phys. Rev. Lett.*, 99:150501, 2007. 139

[226] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of gaussian quantum states. *Phys. Rev. Lett.*, 96:080502, Mar 2006. 141, 147, 150

[227] Charles H. Bennett, Andrzej Grudka, Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Postulates for measures of genuine multipartite correlations. *Phys. Rev. A*, 83:012312, Jan 2011. 142

[228] R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Phys. Rev. A*, 49:1567–1583, Mar 1994. 145

[229] J. Laurat, G. Keller, J. A. Oliveira-Huguenin, C. Fabre, T. Coudreau, A. Serafini, G. Adesso, and F. Illuminati. Entanglement of two-mode gaussian states: characterization and experimental production and manipulation. *J. Opt. B: Quant. Semiclass. Opt.*, 7:S577, 2005. 146

[230] A totally analogous situation is encountered when comparing Duan *et al.*'s [330] and Simon's [69] criteria for separability, where the former shares similar characteristics to Reid's EPR-steering test, while the latter shares similar characteristics to Wiseman *et al.*'s criterion. 149

[231] Qiongyi He, Laura Rosales-Zárate, Gerardo Adesso, and Margaret D Reid. Secure continuous variable teleportation and einstein-podolsky-rosen steering. *Physical Review Letters*, 115(18):180502, 2015. 150

[232] Peter van Loock and Akira Furusawa. Detecting genuine multipartite continuous-variable entanglement. *Phys. Rev. A*, 67:052315, May 2003. 151

[233] P. van Loock and Samuel L. Braunstein. Multipartite entanglement for continuous variables: A quantum teleportation network. *Phys. Rev. Lett.*, 84:3482–3485, Apr 2000. 151, 157

[234] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009. 151

[235] Otfried Guhne and G. Tóth. Entanglement detection. *Phys. Rep.*, 474(16):1 – 75, 2009. 151

[236] Gerardo Adesso and Fabrizio Illuminati. Continuous variable tangle, monogamy inequality, and entanglement sharing in gaussian states of continuous variable systems. *New J. Phys.*, 8(1):15, 2006. 151, 153, 155, 156

[237] G. Adesso, A. Serafini, and F. Illuminati. *Phys. Rev. A*, 73:032345, 2006. 151, 153, 155, 156

[238] Jean-Daniel Bancal, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.*, 106:250404, Jun 2011. 151

[239] George Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35:3066–3069, May 1987. 152

[240] Daniel Collins, Nicolas Gisin, Sandu Popescu, David Roberts, and Valerio Scarani. Bell-type inequalities to detect true n-body nonseparability. *Phys. Rev. Lett.*, 88:170405, Apr 2002. 152

[241] Michael Seevinck and George Svetlichny. Bell-type inequalities for partial separability in n-particle systems and quantum mechanical violations. *Phys. Rev. Lett.*, 89:060401, Jul 2002. 152

[242] Gerardo Adesso and Samanta Piano. Theory of genuine tripartite nonlocality of gaussian states. *Phys. Rev. Lett.*, 112:010401, Jan 2014. 152, 156, 157

[243] Lynden K Shalm, Deny R Hamel, Zhizhong Yan, Christoph Simon, Kevin J Resch, and Thomas Jennewein. Three-photon energy-time entanglement. *Nat. Phys.*, 9(1):19–22, 2013. 152

[244] Yun-Feng Huang, Bi-Heng Liu, Liang Peng, Yu-Hu Li, Li Li, Chuan-Feng Li, and Guang-Can Guo. Experimental generation of an eight-photon greenberger–horne–zeilinger state. *Nat. Commun.*, 2:546, 2011. 152

[245] Xing-Can Yao, Tian-Xiong Wang, Ping Xu, He Lu, Ge-Sheng Pan, Xiao-Hui Bao, Cheng-Zhi Peng, Chao-Yang Lu, Yu-Ao Chen, and Jian-Wei Pan. Observation of eight-photon entanglement. *Nat. Photon.*, 6(4):225–228, 2012. 152

[246] J Lavoie, R Kaltenbaek, and K J Resch. Experimental violation of svetlichny's inequality. *New J. Phys.*, 11(7):073051, 2009. 152

[247] C Erven, E Meyer-Scott, K Fisher, J Lavoie, BL Higgins, Z Yan, CJ Pugh, J-P Bourgoin, R Prevedel, LK Shalm, et al. Experimental three-photon quantum nonlocality under strict locality conditions. *Nat. Photon.*, 8(4):292–296, 2014. 152

[248] Thomas Monz, Philipp Schindler, Julio T. Barreiro, Michael Chwalla, Daniel Nigg, William A. Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, 106:130506, Mar 2011. 152

[249] Seiji Armstrong, Jean-François Morizur, Jiri Janousek, Boris Hage, Nicolas Treps, Ping Koy Lam, and Hans-A Bachor. Programmable multimode quantum networks. *Nat. Commun.*, 3:1026, 2012. 152

[250] Jietai Jing, Jing Zhang, Ying Yan, Fagang Zhao, Changde Xie, and Kunchi Peng. Experimental demonstration of tripartite entanglement and controlled dense coding for continuous variables. *Phys. Rev. Lett.*, 90:167903, Apr 2003. 152, 157

[251] Xiaolong Su, Aihong Tan, Xiaojun Jia, Jing Zhang, Changde Xie, and Kunchi Peng. Experimental preparation of quadripartite cluster and greenberger-horne-zeilinger entangled states for continuous variables. *Phys. Rev. Lett.*, 98:070502, Feb 2007. 152

[252] Shota Yokoyama, Ryuji Ukai, Seiji Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nat. Photon.*, 7(12):982–986, 2013. 152

[253] Che-Ming Li, Kai Chen, Yueh-Nan Chen, Qiang Zhang, Yu-Ao Chen, and Jian-Wei Pan. Genuine high-order einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 115:010402, Jul 2015. 152

[254] Seiji Armstrong, Meng Wang, Run Yan Teh, Qi Huang Gong, Qiong Yi He, Jiri Janousek, Hans-Albert Bachor, Margaret D Reid, and Ping Koy Lam. Multipartite einstein-podolsky-rosen steering and genuine tripartite entanglement with optical networks. *Nat. Phys.*, 11:167–172, 2015. 152, 160, 168

[255] E. Schrödinger. Discussion of probability relations between separated systems. *Math. Proc. Cambridge Philos. Soc.*, 31:555–563, 10 1935. 152

[256] M. D. Reid. Demonstration of the einstein-podolsky-rosen paradox using nondegenerate parametric amplification. *Phys. Rev. A*, 40:913–923, Jul 1989. 152

[257] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro. Revealing hidden einstein-podolsky-rosen nonlocality. *Phys. Rev. Lett.*, 106:130402, Mar 2011. 152

[258] Vitus Händchen, Tobias Eberle, Sebastian Steinlechner, Aiko Samblowski, Torsten Franz, Reinhard F Werner, and Roman Schnabel. Observation of one-way einstein-podolsky-rosen steering. *Nat. Photon.*, 6(9):596–599, 2012. 152

[259] Joseph Bowles, Tamás Vértesi, Marco Túlio Quintino, and Nicolas Brunner. One-way einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 112:200402, May 2014. 152

[260] Marco Túlio Quintino, Tamás Vértesi, Daniel Cavalcanti, Remigiusz Augusiak, Maciej Demianowicz, Antonio Acín, and Nicolas Brunner. Inequivalence of entanglement, steering, and bell nonlocality for general measurements. *Phys. Rev. A*, 92:032107, Sep 2015. 152

[261] Q. Y. He, Q. H. Gong, and M. D. Reid. Classifying directional gaussian entanglement, einstein-podolsky-rosen steering, and discord. *Phys. Rev. Lett.*, 114:060402, Feb 2015. 152

[262] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, Jan 2012. 152

[263] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti. Quantifying einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 112:180404, May 2014. 152

[264] A. C. S. Costa and R. M. Angelo. Quantification of einstein-podolski-rosen steering for two-qubit states. *Phys. Rev. A*, 93:020103, Feb 2016. 152

[265] Q. Y. He, Laura Rosales-Zárate, Gerardo Adesso, and Margaret D. Reid. Secure continuous variable teleportation and einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 115:180502, Oct 2015. 152

[266] Dylan J Saunders, Steve J Jones, Howard M Wiseman, and Geoff J Pryde. Experimental epr-steering using bell-local states. *Nat. Phys.*, 6(11):845–849, 2010. 152

[267] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde. Arbitrarily loss-tolerant einstein-podolsky-rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Phys. Rev. X*, 2:031003, Jul 2012. 152

[268] Kai Sun, Xiang-Jun Ye, Jin-Shi Xu, Xiao-Ye Xu, Jian-Shun Tang, Yu-Chun Wu, Jing-Ling Chen, Chuan-Feng Li, and Guang-Can Guo. Experimental quantification of asymmetric einstein-podolsky-rosen steering. *arXiv:1511.01679 (Phys. Rev. Lett. in press)*, 2015. 152

[269] Kai Sun, Jin-Shi Xu, Xiang-Jun Ye, Yu-Chun Wu, Jing-Ling Chen, Chuan-Feng Li, and Guang-Can Guo. Experimental demonstration of the einstein-podolsky-rosen steering game based on the all-versus-nothing proof. *Phys. Rev. Lett.*, 113:140402, Sep 2014. 152

[270] R. Y. Teh and M. D. Reid. Criteria for genuine n-partite continuous-variable entanglement and einstein-podolsky-rosen steering. *Phys. Rev. A*, 90:062337, Dec 2014. 152

[271] D Cavalcanti, P Skrzypczyk, GH Aguilar, RV Nery, PH Souto Ribeiro, and SP Walborn. Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nat. Commun.*, 6:7941, 2015. 152

[272] M. D. Reid. Monogamy inequalities for the einstein-podolsky-rosen paradox and quantum steering. *Phys. Rev. A*, 88:062108, Dec 2013. 152, 154, 160, 200

[273] N. Cerf, G. Leuchs, and E. S. Polzik, editors. *Quantum Information with Continuous Variables of Atoms and Light*. Imperial College Press, London, 2007. 152

[274] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000. 153

[275] T. Hiroshima, G. Adesso, and F. Illuminati. Monogamy Inequality for Distributed Gaussian Entanglement. *Phys. Rev. Lett.*, 98:050503, 2007. 153

[276] Tobias J. Osborne and Frank Verstraete. General monogamy inequality for bipartite qubit entanglement. *Phys. Rev. Lett.*, 96:220503, Jun 2006. 153

[277] Gerardo Adesso, Davide Girolami, and Alessio Serafini. Measuring gaussian quantum information and correlations using the rényi entropy of order 2. *Phys. Rev. Lett.*, 109:190502, Nov 2012. 153, 155, 156, 201

[278] B. M. Terhal. Is entanglement monogamous? *IBM J. Res. & Dev.*, 48(1):71 –78, 2004. 153

[279] Gerardo Adesso and Fabrizio Illuminati. Strong monogamy of bipartite and genuine multipartite entanglement: The gaussian case. *Phys. Rev. Lett.*, 99:150501, Oct 2007. 153

[280] Gerardo Adesso and R Simon. Strong subadditivity for log-determinant of covariance matrices and its applications. *arXiv:1601.03226*, 2016. 154, 160, 199, 200, 201

[281] Y. Zhou, X. Jia, F. Li, C. Xie, and K. Peng. *Opt. Express*, 23:4952, 2015. 157, 160

[282] T. Eberle, V. Händchen, and R. Schnabel. *Opt. Express*, 21:11546, 2013. 157, 160

[283] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. 157, 165, 166

[284] George Robert Blakley. Safeguarding cryptographic keys. page 313, 1899. 157

[285] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162–168, Jan 1999. 157, 167, 173

[286] Se-Wan Ji, Jaehak Lee, Jiyong Park, and Hyunchul Nha. Quantum steering of Gaussian states via non-Gaussian measurements. *arXiv: 1511.02649*, 2015. 160

[287] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. 166

[288] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A*, 69:052307, May 2004. 167

[289] Zhan-jun Zhang and Zhong-xiao Man. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A*, 72:022303, Aug 2005. 167

[290] Kai Chen and Hoi-Kwong Lo. Multi-partite quantum cryptographic protocols with noisy ghz states. *Quantum Information & Computation*, 7:689–715, Nov 2007. 167

[291] Yadong Wu, Jian Zhou, Xinbao Gong, Ying Guo, Zhi-Ming Zhang, and Guangqiang He. Continuous-variable measurement-device-independent multipartite quantum communication. *arXiv preprint arXiv:1512.03876v2*, 2016. 167

[292] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000. 167

[293] Yao Fu, Hua-Lei Yin, Teng-Yun Chen, and Zeng-Bing Chen. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.*, 114:090501, Mar 2015. 167

[294] Anne Marin and Damian Markham. Equivalence between sharing quantum and classical secrets and error correction. *Phys. Rev. A*, 88:042332, Oct 2013. 167

[295] Fu-Guo Deng, Gui Lu Long, and Hong-Yu Zhou. An efficient quantum secret sharing scheme with einsteinpodolskyrosen pairs. *Physics Letters A*, 340(1-4):43 – 50, 2005. 167

[296] W. Tittel, H. Zbinden, and N. Gisin. Experimental demonstration of quantum secret sharing. *Phys. Rev. A*, 63:042301, Mar 2001. 167

[297] Andrew M Lance, Thomas Symul, Warwick P Bowen, Toms Tyc, Barry C Sanders, and Ping Koy Lam. Continuous variable (2, 3) threshold quantum secret sharing schemes. *New Journal of Physics*, 5(1):4, 2003. 167

[298] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78:042309, Oct 2008. 167

[299] Adrian Keet, Ben Fortescue, Damian Markham, and Barry C. Sanders. Quantum secret sharing with qudit graph states. *Phys. Rev. A*, 82:062315, Dec 2010. 167

[300] Yadong Wu, Runze Cai, Guangqiang He, and Jun Zhang. Quantum secret sharing with continuous variable graph state. *Quantum information processing*, 13(5):1085–1102, 2014. 167

[301] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, and Ping Koy Lam. Tripartite quantum state sharing. *Phys. Rev. Lett.*, 92:177903, Apr 2004. 167

[302] Yu-Ao Chen, An-Ning Zhang, Zhi Zhao, Xiao-Qi Zhou, Chao-Yang Lu, Cheng-Zhi Peng, Tao Yang, and Jian-Wei Pan. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.*, 95:200502, Nov 2005. 167

[303] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter. Experimental demonstration of four-party quantum secret sharing. *Phys. Rev. Lett.*, 98:020503, Jan 2007. 167

[304] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.*, 5(5480), 2014. 167

[305] Su-Juan Qin, Fei Gao, Qiao-Yan Wen, and Fu-Chen Zhu. Cryptanalysis of the hillery-bužek-berthiaume quantum secret-sharing protocol. *Phys. Rev. A*, 76:062324, Dec 2007. 167

[306] Fu-Guo Deng, Xi-Han Li, and Hong-Yu Zhou. Opaque attack on three-party quantum secret sharing based on entanglement. *arXiv preprint arXiv:0705.0279*, 2007. 167

[307] Zhan-jun Zhang, Yong Li, and Zhong-xiao Man. Multiparty quantum secret sharing. *Phys. Rev. A*, 71:044301, Apr 2005. 167

[308] Fu-Guo Deng, Xi-Han Li, Hong-Yu Zhou, and Zhan-jun Zhang. Improving the security of multiparty quantum secret sharing against trojan horse attack. *Phys. Rev. A*, 72:044302, Oct 2005. 167, 173

[309] Su-Juan Qin, Fei Gao, Qiao-Yan Wen, and Fu-Chen Zhu. Improving the security of multiparty quantum secret sharing against an attack with a fake signal. *Physics Letters A*, 357(2):101 – 103, 2006. 167

[310] Christian Schmid, Pavel Trojek, Mohamed Bourennane, Christian Kurtsiefer, Marek Żukowski, and Harald Weinfurter. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.*, 95:230505, Dec 2005. 167

[311] Guang Ping He. Comment on "experimental single qubit quantum secret sharing". *Phys. Rev. Lett.*, 98:028901, Jan 2007. 167

[312] Guang Ping He and ZD Wang. Single qubit quantum secret sharing with improved security. *arXiv preprint quant-ph/0703159*, 2007. 167

[313] Armin Tavakoli, Isabelle Herbauts, Marek Żukowski, and Mohamed Bourennane. Secret sharing with a single *d*-level quantum system. *Phys. Rev. A*, 92:030302, Sep 2015. 167

[314] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007. 168

[315] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, Mar 2011. 168

[316] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008. 169

[317] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005. 170

[318] A. S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. North Holland, Amsterdam, 1982. 170

[319] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102:110504, Mar 2009. 170

[320] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6(9):659–662, 2010. 170

[321] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.*, 55(12):122205, 2014. 170

[322] Rupert L Frank and Elliott H Lieb. Extended quantum conditional entropy and quantum uncertainty inequalities. *Communications in Mathematical Physics*, 323(2):487–495, 2013. 170

[323] Agnes Ferenczi. *Security proof methods for quantum key distribution protocols*. PhD thesis, University of Waterloo, 2013. 170

[324] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, Jan 2012. 174

[325] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109:100502, Sep 2012. 175

[326] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9(10):641–652, 2015. 179

[327] Jaromír Fiurášek. Improving the fidelity of continuous-variable teleportation via local operations. *Physical Review A*, 66(1):012304, 2002. 183

[328] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004. 189, 190

[329] J. F. Sturm, Opt. Methods and Software, **11**-**12**, 625 (1999). M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. http://cvxr.com/cvx, June 2015. 197

[330] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2722–2725, Mar 2000. 223