Universitat Autònoma de Barcelona

Departament de Física
Grup de Física Teòrica

Quantum Information with Continuous Variable systems

by

Carles Rodó Sarró

Submitted in partial fulfillment
to the requirements for the degree of

Doctor of Philosophy

at the

UNIVERSITAT AUTÒNOMA DE BARCELONA
08193 Bellaterra, Barcelona, Spain.
April, 2010

Under the supervision of
Prof. Anna Sanpera Trigueros

"Ethical axioms are found and tested not
very differently from the axioms of science.
Truth is what stands the test of experience".
Albert Einstein.

Acknowledgments

Han passat ja quasibé cinc anys. Durant aquest temps he tingut l'oportunitat de desenvolupar una important tasca docent al grup de Física Teòrica. Agraeixo en especial al Ramón Muñoz i a l'Eduard Massó amb els qui he compartit la major part de la docència i amb els qui s'ha fet molt agradable treballar.

En segon lloc agraeixo a l'Albert Bramon l'entusiasme amb el que duia les seves classes de Física Quàntica a la llicenciatura, aquella matèria tan estrambòtica... però amb la que un s'encurioseix de seguida. Gràcies a l'Albert he tingut l'oportunitat de fer la recerca del doctorat amb l'Anna Sanpera. Què dir de l'Anna? Doncs una brillant investigadora entregada i molt involucrada no només en la recerca en aquest camp tan d'actualitat de la Informació Quàntica sinó en la seva difusió a estudiants més joves. Gràcies Anna, per la paciència i per trobar sempre temps i esforç en el meu treball.

Fer el doctorat amb l'Anna m'ha obert la possibilitat d'assistir i "actuar" a congressos d'arreu i així poder treballar amb investigadors de relevància. En particular amb el Gerardo Adesso de qui guardo un grat record, generós i molt emprenedor amb ell gran part de la tesis he desenvolupat.

També vull recordar molt especialment als companys i ex-companys de despatx, amb ells he passat la major part del temps Javi, Àlex, Marc, Simone i Joan Antoni; gràcies per les variopintes converses dins i fora la feina.

Finalment agraeixo a la família que m'ha recolzat en aquesta etapa, a la Mirka que ha canviat el meu rumb i al meu pare sobretot. Crec que es deu al teu afan de coneixement i als teves inquietuds que vaig començar a estudiar Física i així, és a tu a qui et dedico la Tesis.

Carles

List of Publications

The articles published during the completion of the PhD which are enclosed in this thesis are:

1. Efficiency in Quantum Key Distribution Protocols with Entangled Gaussian States.
   C. Rodó, O. Romero-Isart, K. Eckert, and A. Sanpera.
   Pre-print version: arXiv:quant-ph/0611277
   Journal-ref: OPEN SYSTEMS & INFORMATION DYNAMICS **14**, 69 (2007)

2. Operational Quantification of Continuous-Variable Correlations.
   C. Rodó, G. Adesso, and A. Sanpera.
   Pre-print version: arXiv:0707:2811
   Journal-ref: PHYSICAL REVIEW LETTERS **100**, 110505, (2008)

3. Multipartite continuous-variable solution for the Byzantine agreement problem.
   R. Neigovzen, C. Rodó, G. Adesso, and A. Sanpera.
   Pre-print version: arXiv:0712.2404
   Journal-ref: PHYSICAL REVIEW A **77**, 062307, (2008)

4. Manipulating mesoscopic multipartite entanglement with atom-light interfaces.
   J. Stasińska, C. Rodó, S. Paganelli, G. Birkl, and A. Sanpera.
   Pre-print version: arXiv:0907.4261
   Journal-ref: PHYSICAL REVIEW A **80**, 062304, (2009)

There is also one article in preparation which is within the framework of this PhD thesis:

1. A covariance matrix formalism for atom-light interfaces.
   J. Stasińska, S. Paganelli, C. Rodó and A. Sanpera.
   Journal-ref: Submitted to NEW JOURNAL OF PHYSICS

Finally, one other article has been published during the PhD which is not related to the topic of this thesis:

1. Transport and entanglement generation in the Bose-Hubbard model.
   O. Romero-Isart, K. Eckert, C. Rodó, and A. Sanpera.
   Pre-print version: quant-ph/0703177
   Journal-ref: JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL **40**, 8019 (2007)

Contents

Chapter 1

Introduction

The theory of Quantum Information emerges as an effort to generalize classical information theory into the quantum realm, by using the laws of quantum physics to encode, process and extract information. It was Rolf Landauer, known among other things for his remarkable contributions to the theory of electrical conductivity, who at the end of 1960 coined the idea that information rather than an abstract mathematical concept, is at the very end a physical process governed by physical laws. At the same time, Richard Feynman in "Simulating Physics with Computers" realized that in order to simulate intrinsically quantum physical processes, a classical computer will necessarily fail by its mere deterministic continuous nature while he showed how a quantum one would succeed efficiently in simulating and computing. At the end of the 80s, David Deutsch in his seminal paper "Quantum theory, the Church-Turing principle and the universal quantum computer" set the ground for the theory of quantum information. He considered a universal classical Turing machine, which is the prototype of any classical computer, and propose the first universal quantum Turing machine paving the way towards quantum circuit modeling.

An algorithm is nothing else than a set of rules to solve efficiently a given problem in a finite number of steps. Problems are usually classified in different complexity classes. An important class of problems are the so-called, non-deterministic polynomial (NP) problems, whose efficient solution using classical computers grows exponentially with the input size of the problem. The cornerstone example of a NP problem is factorization. A big leap in the theory of Quantum Information was done by Peter Shor when he proposed in 1994 a quantum algorithm to factorize a prime number in an efficient way. Precisely the lack of an efficient classical solution to this problem sustains present cryptographic methods. The importance of his discovery, had led to a revolution on the emergent field of quantum information, involving for the first time non-academic interests as Quantum Cryptography with already successful implementations. Simultaneously, in 1995 Ignacio Cirac and Peter Zoller proposed the first realizable model of a quantum computer, using an array of trapped ions, an available technology since the beginning of the 1990.

Since the end of the 1990, until now, very different models, involving solid states devices, quantum dots, quantum optics, ... have emerged as possible candidates to process information in a reliable and powerful way. At the same time, novel problems and solutions have arise by exploiting the properties of quantum laws in many different scenarios. Without the impressive experimental advance in manipulation of quantum systems, either using ultra-cold atoms, photons or ions, Quantum Information would have not reach the enormous current interest.

This thesis deals with the study of quantum communication protocols with Continuous Variable (CV) systems. Continuous Variable systems are those described by canonical conjugated coordinates x and p endowed with infinite dimensional Hilbert spaces, thus involving a complex mathematical structure. A special class of CV states, are the so-called Gaussian states. With them, it has been possible to implement certain quantum tasks as quantum teleportation, quantum cryptography and quantum computation with fantastic experimental success. The importance of Gaussian states is two-fold; firstly, its structural mathematical description makes them much more amenable than any other CV system. Secondly, its production, manipulation and detection with current optical technology can be done with a very high degree of accuracy and control. Nevertheless, it is known that in spite of their exceptional role within the space of all Continuous Variable states, in fact, Gaussian states are not always the best candidates to perform quantum information tasks. Thus non-Gaussian states emerge as potentially good candidates for communication and computation purposes. This dissertation is organized as follows.

In chapter 2, we review the formalism of Continuous Variable systems focussing on Gaussian states. We show that Gaussian states admit an easy mathematical description based on phase-space Wigner functions as well as with covariance matrices. We introduce also the basic ingredients to describe multipartite systems with entanglement together with the most relevant well known results and finally we detail the description of light as a CV system.

In chapter 3, we present a protocol that permits to extract quantum keys from an entangled Continuous Variable system. Differently from discrete systems, Gaussian entangled states cannot be distilled with Gaussian operations only *i.e.* entangled Gaussian states are always bound entangled. However it was already shown, that it is still possible to extract perfectly correlated classical bits to establish secret random keys using an "entanglement based" approach. Differently from previous attempts where the realistic implementation was not considered, we properly modify the protocol using bipartite Gaussian entanglement to perform quantum key distribution in an efficient and realistic way. We describe and demonstrate security in front of different possible attacks on the communication, detailing the resources demanded while quantifying and relating the efficiency of the protocol with the entanglement shared between the parties involved. Our results are reported in [1].

In chapter 4, we move to multipartite Gaussian states. There, we consider a simple 3-partite protocol known as Byzantine Agreement (detectable broadcast). The Byzantine Agreement is an old classical communication problem in which parties (with possible traitors among them) can only communicate pairwise, while trying to reach a common decision. Classically, there is a bound in the number of possible traitors that can be involved in the game if only classical secure channels are used. In the simplest case where three parties are involved, one of them being a traitor, no classical solution exists. Nevertheless, a quantum solution exist, *i.e.* letting a traitor being involved and using as a fundamental resource multipartite entanglement it is permitted to reach a common agreement. We demonstrate that detectable broadcast is also solvable within Continuous Variable using multipartite entangled Gaussian states and Gaussian operations (homodyne detection). Furthermore, we show under which premises concerning entanglement content of the state, noise, inefficient homodyne detectors, our protocol is efficient and applicable with present technology. Our results are reported in [2].

In chapter 5, we move to the problem of quantification of correlations (quantum and/or classical) between two Continuous Variable modes. We propose to define correlations between the two modes as the maximal number of correlated bits extracted via local quadrature measurements on each mode. On Gaussian states, where entanglement is accessible via their covariance matrix our quantification majorizes entanglement, reducing to an entanglement monotone for pure states. For mixed Gaussian states we provide an operational receipt to quantify explicitly the classical correlations presents in the states. We then address non-Gaussian states with our operational quantification that is based on and up to second moments only in contrast to the exact detection of entanglement that generally involves measurements of high-order moments. For non-Gaussian states, such as photonic Bell states, photon subtracted states and mixtures of Gaussian states, the bit quadrature correlations are shown to be also a monotonic function of the negativity. This quantification yields a feasible, operational way to measure non-Gaussian entanglement in current experiments by means of direct homodyne detection, without needing a complete state tomography. Our analysis demonstrates the rather surprising feature that entanglement in the considered non-Guassian examples can thus be detected and experimentally quantified with the same complexity as if dealing with Gaussian states. Our results are reported in [3].

In chapter 6, we focus to atomic ensembles described as CV systems. Entanglement between distant mesoscopic atomic ensembles can be induced by measuring an ancillary light system. We show how to generate, manipulate and detect mesoscopic entanglement between an arbitrary number of atomic samples through a quantum non-demolition matter-light interface. Measurement induced entanglement between two macroscopical atomic samples was reported experimentally in 2001. There, the interaction between a single laser pulse propagating through two spatially separated atomic samples combined with a final projective measurement on the light led to the creation of pure EPR entanglement between the two samples. Due to the quantum non-demolition character of the measurement, verification of the EPR state was done by passing a second pulse and measuring variances on light. Our proposal extends this idea in a non-trivial way for multipartite entanglement (GHZ and cluster-like) without needing local magnetic fields. We propose a novel experimental realization of measurement induced entanglement. Moreover, we show quite surprisingly that given the irreversible character of a measurement, the interaction of the atomic sample with a second pulse light can modify and even reverse the entangling action of the first one leaving the samples in a separable state. Our results are reported in [4] and [5].

Finally, in chapter 7, we conclude summarizing our results, listing some open questions and giving future directions of research.

Chapter 2

Continuous Variable formalism

Continuous Variable (CV) systems are those systems described by two canonical conjugated degrees of freedom *i.e.* there exist two observables that fulfill Canonical Commutation Relations (CCR). This chapter comprises a detailed description of Continuous Variable systems. It provides also the mathematical framework needed to analyze the problems treated within this thesis. After introducing a phase-space formalism and the corresponding quasi-probability distributions I shall restrict first to Gaussian states which describe, among others, coherent, squeezed and thermal states. As a cornerstone example, I will shortly develop the canonical quantization of light, ending by showing how to deal with Gaussian states of light. Presently, these states are the preferred resources in experiments of QI using Continuous Variable systems. For further background information the interested reader is referred to [6, 7, 8, 9, 10, 11, 12].

2.1 Continuous Variable systems

The Canonical Commutation Relations for two canonical observables $\hat{q}$ and $\hat{p}$ read [1]

$$[\hat{q}, \hat{p}] = \mathrm{i}\mathbb{I}. \tag{2.1}$$

So a direct consequence to the fact that two hermitian operators $\hat{q}$ and $\hat{p}$ fulfill the CCR is that

(i) the underlying Hilbert space cannot be finite dimensional. This can be seen by applying the trace into Eq. (2.1). Using finite dimensional operator algebra one would obtain, on one hand, $\mathrm{i}\,\mathrm{dim}\mathcal{H}$, while on the other $\mathrm{tr}(\hat{q}\hat{p}) - \mathrm{tr}(\hat{p}\hat{q}) = 0$.

(ii) $\hat{q}$ and $\hat{p}$ cannot be bounded, since the relation $[\hat{q}^m, \hat{p}] = m\hat{q}^{m-1}\mathrm{i}$ (obtained from $[f(\hat{A}), B] = \frac{df(\hat{A})}{d\hat{A}}[\hat{A}, \hat{B}]$) implies that [2] $||\hat{q}||^m \cdot ||\hat{p}|| \geq \frac{1}{2}||[\hat{q}^m, \hat{p}]|| = \frac{1}{2}m||\hat{q}||^{m-1}$, which means that $||\hat{q}|| \cdot ||\hat{p}|| \geq \frac{1}{2}m$ has to be true for all m.

[1] Quadrature operators are chosen adimensional in such a way that $\hbar$ is not going to appear in any formula.

[2] Using $||\hat{A}|| \cdot ||\hat{B}|| \geq ||\hat{A}\hat{B}|| = \frac{1}{2}||[\hat{A}, \hat{B}] + \{\hat{A}, \hat{B}\}|| \geq \frac{1}{2}||[\hat{A}, \hat{B}]||$.

This is a direct consequence of the fact that $\hat{q}$ and $\hat{p}$ possess a continuous spectra and act in an infinite dimensional Hilbert space.

Examples of CV systems we can think of are the position-momentum of a massive particle, the quadratures of an electromagnetic field, the collective spin of a polarized ensemble of atoms [13] or the radial modes of trapped ions [14]. In all of the examples above, there exist two observables fulfilling (2.1). As we will show, these observables obey the standard bosonic commutation relations and so we call these systems bosonic modes. We can deal with several modes, and in this case, by ordering the operators in canonical pairs through $\hat{R}^T = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_N, \hat{p}_N)$ we can compactly state CCR as

$$[\hat{R}_i, \hat{R}_j] = \mathrm{i}\mathbb{I}(\mathcal{J}_N)_{ij} \tag{2.2}$$

where $i, j = 1, 2, \ldots, 2N$ and $\mathcal{J}_N = \oplus_{\mu=1}^{N} \mathcal{J}$ accounts for all modes. $\mathcal{J}$ is the so-called symplectic matrix which corresponds to an antisymmetric and non-degenerate form fulfilling (i) $\forall \eta, \zeta \in \mathbb{R}^{2N} : \langle \eta | \mathcal{J} | \zeta \rangle = -\langle \zeta | \mathcal{J} | \eta \rangle$ and (ii) $\forall \eta : \langle \eta | \mathcal{J} | \zeta \rangle = 0 \Rightarrow \zeta = 0$. In the appropriate choice of basis (canonical coordinates) the symplectic matrix is brought to the standard form

$$\mathcal{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.3}$$

2.2 Canonical Commutation Relations

Canonical Commutation Relations[3] can also be expressed using annihilation and creation operators $\hat{a}_\mu$ and $\hat{a}_\mu^\dagger$ which obey standard bosonic commutation relations

$$[\hat{a}_\mu, \hat{a}_\nu^\dagger] = \delta_{\mu\nu}, \quad [\hat{a}_\mu, \hat{a}_\nu] = [\hat{a}_\mu^\dagger, \hat{a}_\nu^\dagger] = 0 \tag{2.4}$$

$\mu, \nu = 1, 2, \ldots, N$. The CCR expressed in Eq. (2.2) and (2.4) are related by a unitary matrix $U = 1/\sqrt{2} \begin{pmatrix} \mathbb{I}_N & \mathrm{i}\mathbb{I}_N \\ \mathbb{I}_N & -\mathrm{i}\mathbb{I}_N \end{pmatrix}$ such that if we define $\hat{O}^T = (\hat{a}_1, \hat{a}_2, \ldots, \hat{a}_N, \hat{a}_1^\dagger, \hat{a}_2^\dagger, \ldots, \hat{a}_N^\dagger)$ then $\hat{O}_i = U_{ij} \hat{R}_j$.

Notice that the representation of the CCR up to unitaries is not unique. For instance, for a single mode in the Schrödinger representation each degree of freedom is embedded in $\mathcal{H} = \mathcal{L}^2(\mathbb{R}^2)$, while the operators $\hat{q}$ and $\hat{p}$ act multiplicative and derivative respectively

$$\left.\begin{array}{rcl} \hat{q} & = & q \\ \hat{p} & = & -\mathrm{i}\frac{\partial}{\partial q} \end{array}\right\} \tag{2.5}$$

but also $\hat{q} = +\mathrm{i}\frac{\partial}{\partial p}, \quad \hat{p} = p$ is equally possible. In both representations the operators are unbounded. A way to remove ambiguities (up to unitaries) and to treat with

[3] The CCR are related with the classical Poisson brackets via the 1st quantization transcription: $\{\mathcal{A}, \mathcal{B}\}_{pp} \equiv \sum_\mu (\frac{\partial \mathcal{A}}{\partial Q_\mu} \frac{\partial \mathcal{B}}{\partial P_\mu} - \frac{\partial \mathcal{B}}{\partial Q_\mu} \frac{\partial \mathcal{A}}{\partial P_\mu}) \longrightarrow -\mathrm{i}[\hat{A}, \hat{B}] \equiv -\mathrm{i}(\hat{A}\hat{B} - \hat{B}\hat{A})$ and $\mathcal{A} \longrightarrow \hat{A}$.

bounded operators is by using Weyl operators. The Weyl operator is defined as

$$\hat{W}_\zeta \equiv e^{\mathrm{i}\zeta^T\cdot\mathcal{J}\cdot\hat{R}} \tag{2.6}$$

where $\zeta^T = (\zeta_1, \zeta_2, \dots, \zeta_{2N}) \in \mathbb{R}^{2N}$.

The Weyl operator acts in the states as a translation in the phase-space (displacements $e^{\mathrm{i}\eta\hat{p}}|q\rangle = |q-\eta\rangle$ and kicks $e^{\mathrm{i}\zeta\hat{q}}|q\rangle = e^{\mathrm{i}\zeta q}|q\rangle$) as it can be checked by looking to its action onto an arbitrary position-momentum operator

$$\hat{W}_\zeta^\dagger \hat{R}_i \hat{W}_\zeta = \hat{R}_i - \zeta_i \mathbb{I}. \tag{2.7}$$

It satisfies the Weyl relation

$$\hat{W}_\zeta \hat{W}_\eta = e^{-\frac{\mathrm{i}}{2}\zeta^T\cdot\mathcal{J}\cdot\eta}\hat{W}_{\zeta+\eta}, \tag{2.8}$$

analogously, it fulfills

$$\hat{W}_\zeta \hat{W}_\eta = \hat{W}_\eta \hat{W}_\zeta e^{-\mathrm{i}\zeta^T\cdot\mathcal{J}\cdot\eta}, \tag{2.9}$$

showing the non-commutative character of the canonical observables. There exists only one equivalent representation of the Weyl relation according to the following theorem.

Theorem 2.2.1 (Stone-von Neumann theorem) *Let $\hat{W}_1$ and $\hat{W}_2$ be two Weyl systems over a finite dimensional phase-space ($N < \infty$). If the two Weyl systems are strongly continuous* [4] *and irreducible* [5] *then they are equivalent (up to an unitary).*

2.3 Phase-space

Phase-space formulations of Quantum Mechanics, offers a framework in which quantum phenomena can be described using as much classical language as allowed. There are various formulations of non-relativistic Quantum Mechanics see *e.g.* [15]. These formulations differ in mathematical description, yet each one makes identical predictions for all experimental results.

Phase-space formulations can often provide useful physical insights. Furthermore, it requires dealing only with constant number equations and not with operators, which can be of significant practical advantage. This mathematical advantage arises here from the fact that the infinite-dimensional complex Hilbert space structure which is, in principle, a difficult object to work with, can be mapped into the linear algebra structure of the finite-dimensional real phase-space. We will extend this map and show how to characterize states and operations in sections 2.4.1 and 2.3.2 respectively.

2.3.1 Phase-space geometry

A system of N canonical degrees of freedom is described classically by a $2N$-dimensional real vector space [6] $V \simeq \mathbb{R}^{2N}$. Together with the symplectic form it defines a sym-

[4] $\forall|\psi\rangle \in \mathcal{H} : \lim_{\zeta\to 0} || \, |\psi\rangle - \hat{W}_\zeta|\psi\rangle|| = 0$.

[5] $\forall\zeta \in \mathbb{R}^{2N} : [\hat{W}_\zeta, \hat{A}] = 0 \Rightarrow \hat{A} \propto \mathbb{I}$.

[6] They are isomorphic (there exist a bijective morphism between the two groups).

plectic real vector space (the phase-space) $\Omega \simeq \mathbb{R}^{2N}$. The phase-space is naturally equipped with a complex structure and can be identified with a complex Hilbert space $\mathcal{H}_\Omega \simeq \mathbb{C}^N$. If $\langle \,|\, \rangle$ stands for the scalar product in $\mathcal{H}_\Omega$ and $\langle \,|\, \rangle_\mathcal{J}$ for the symplectic scalar product in Ω their connection reads

$$\langle \eta | \zeta \rangle = \langle \mathcal{J} \eta | \zeta \rangle_\mathcal{J} + \mathrm{i} \langle \eta | \zeta \rangle_\mathcal{J}. \tag{2.10}$$

Notice that $\eta = (q, p) \in \Omega$ while $\eta = q + \mathrm{i}p \in \mathcal{H}_\Omega$ such that any orthonormal basis in $\mathcal{H}_\Omega$ leads to a canonical basis in Ω. Moreover, any Gaussian unitary operator (which preserves the scalar product) acting on $\mathcal{H}_\Omega$, leads to a symplectic operation S in the phase-space in such a way that the symplectic scalar product is also preserved. The inverse is also true provided that the symplectic operation commutes with the symplectic matrix $\mathcal{J}$.

2.3.2 Symplectic operations

Gaussian operations [16] are completely positive maps, thus preserving the Gaussian character on states, that can be implemented by means of Gaussian unitary operators (symplectic operations) plus Bell measurements (homodyne measurements). Homodyne/heterodyne detection is a fundamental Gaussian operation, that is, the physical measurement of one/two of the canonical conjugated coordinates. Nevertheless we will concentrate for the moment with symplectic operations, hence canonical transformations S that preserve the CCR and therefore leave the basic kinematic rules unchanged. That is, if we transform our canonical operators $\hat{R}_S = S \cdot \hat{R}$, still equation (2.2) is fulfilled. In a totally equivalent way, we can define symplectic transformation as the ones which preserve the symplectic scalar product and therefore [7]

$$S^T \cdot \mathcal{J} \cdot S = \mathcal{J}. \tag{2.11}$$

The set of real $2N \times 2N$ matrices S satisfying the above condition form the symplectic group $Sp(2N, \mathbb{R})$. To construct the affine symplectic group we just need to add also the phase-space translations s that transform $\hat{R}_S = S \cdot \hat{R} + s$ and whose group generators are $\hat{G}_i^{(0)} = \mathcal{J}_{ij} \hat{R}_j$. Apart from that, the group generators of the representation of $Sp(2N, \mathbb{R})$ which physically corresponds to the Hamiltonians which perform the symplectic transformations on the states, are of the form $\hat{G}_{ij} = \frac{1}{2}\{\hat{R}_i, \hat{R}_j\}$. This corresponds to hermitian Hamiltonians of quadratic order in the canonical operators. When rewriting them in terms of creation / annihilation operators we can divide it into two groups. Passive generators (compact):

$$\hat{G}_{\mu\nu}^{(1)} = \mathrm{i}\frac{(\hat{a}_\mu^\dagger \hat{a}_\nu - \hat{a}_\nu^\dagger \hat{a}_\mu)}{2}, \quad \hat{G}_{\mu\nu}^{(2)} = \frac{(\hat{a}_\mu^\dagger \hat{a}_\nu + \hat{a}_\nu^\dagger \hat{a}_\mu)}{2},$$

and active generators (non-compact):

[7] From now on we neglect the subscript N in symplectic matrix.

$\hat{G}^{(3)}_{\mu\nu} = \mathrm{i}\frac{(\hat{a}^\dagger_\mu \hat{a}^\dagger_\nu - \hat{a}_\nu \hat{a}_\mu)}{2}$, $\hat{G}^{(4)}_{\mu\nu} = \frac{(\hat{a}^\dagger_\mu \hat{a}^\dagger_\nu + \hat{a}_\nu \hat{a}_\mu)}{2}$.
The passive ones, are generators which commute with all number operators $\hat{n}_\mu \equiv \hat{a}^\dagger_\mu \hat{a}_\mu$, and so, they preserve the total number, in this sense they are passive. If the system under study is the electromagnetic field, what is being preserved under passive transformations is the total number of photons. In such a case, passive transformations can be implemented optically by only using beam splitters, phase shifts and mirrors. Conversely, only by using them, we can implement any Hamiltonian constructed by a linear combination of the compact generators. Finally, with all the five classes of generators, we can generate all the Gaussian unitaries, $\hat{U}_\lambda = e^{\mathrm{i}\lambda\cdot\hat{G}}$.

For one mode ($N = 1$) the simplest passive generator is the phase shift operator and its corresponding symplectic operation in phase-space

$$\hat{U}_\theta = e^{\mathrm{i}\theta\hat{a}^\dagger\hat{a}} \Leftrightarrow S_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{2.12}$$

On the other hand, we have the active generators that change the energy of the state. The most important one is the single mode squeezing operator, whose unitary expression (for a squeezing parameter $r > 0$) and symplectic operation in phase-space reads

$$\hat{U}_r = e^{\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})} \Leftrightarrow S_r = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}. \tag{2.13}$$

For experimental reasons, instead of the parameter r one uses a decibel expression $10\log e^{2r}$ in dBs [8]. The squeezing operator squeezes the uncertainties on q and p in a complementary way *i.e.* it squeezes position while stretches the momentum with the same factor in such a way that the state remains as close to the uncertainty limit as it was before. When the squeezing parameter r is positive we call it a q-squeezer (amplitude squeezer). Analogously p-squeezer or (phase squeezer) occurs for negatives squeezing parameters.

Finally, phase-space translations for one mode are described by the unitary and symplectic operation in phase-space

$$\hat{U}_\alpha = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \Leftrightarrow s_\alpha = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} \tag{2.14}$$

where $\alpha = \frac{q_0 + \mathrm{i}p_0}{\sqrt{2}}$.

For two modes ($N = 2$) the most important non-trivial unitaries are beam splitters (reflectivity $R = \sin^2\theta/2$ and transmitivity $T = \cos^2\theta/2$) and two mode squeezers that amounts respectively to

$$\hat{U}_{BS} = e^{\frac{\theta}{2}(\hat{a}_1\hat{a}_2^\dagger - \hat{a}_1^\dagger\hat{a}_2)} \Leftrightarrow S_{BS} = \begin{pmatrix} \cos\theta/2 & 0 & \sin\theta/2 & 0 \\ 0 & \cos\theta/2 & 0 & \sin\theta/2 \\ -\sin\theta/2 & 0 & \cos\theta/2 & 0 \\ 0 & -\sin\theta/2 & 0 & \cos\theta/2 \end{pmatrix} \tag{2.15}$$

[8] All logarithms are in basis 10, unless differently specified.

and

$$\hat{U}_{TMS} = e^{r(\hat{a}_1\hat{a}_2 - \hat{a}_1^\dagger \hat{a}_2^\dagger)} \Leftrightarrow S_{TMS} = \begin{pmatrix} \cosh r & 0 & \sinh r & 0 \\ 0 & \cosh r & 0 & -\sinh r \\ \sinh r & 0 & \cosh r & 0 \\ 0 & -\sinh r & 0 & \cosh r \end{pmatrix}. \tag{2.16}$$

2.4 Probability distribution functions

One of the most important tools of the phase-space formulation of Quantum Mechanics are the phase-space probability distribution functions. The best known and widely used is the Wigner distribution function, but there is not a unique way of defining a quantum phase-space distribution function. In fact, several distribution functions with different properties, rules of association and operator ordering can also be well defined [17]. For instance sometimes normal ordered ($\mathcal{P}$-function), antinormal ordered ($\mathcal{Q}$-function), generalized antinormal ordered (Husimi-function), standard ordered, antistandard ordered,... distributions can be more convenient depending on the problem being considered. In this thesis we are only going to work with the totally symmetrical ordered one (Weyl ordered); the Wigner distribution function.

Due to the fact that joint probability distributions at a fixed position $\hat{q}$ and momentum $\hat{p}$ are not allowed by Quantum Mechanics (Heisenberg uncertainty theorem), the quantum phase-space distribution functions should be considered simply as a useful mathematical tool. Joint probabilities can be negative, so that one deals rather with quasi-probability distribution. As long as it yields a correct description of physically observable quantities, their use is accepted.

2.4.1 Quantum states and probability distributions

We would like to see here now how to describe quantum systems of CV using probability distributions functions. Let's recall that a density operator $\hat{\rho}$, defines a quantum state iff it satisfies the following properties

$$\mathrm{tr}\hat{\rho} = 1, \quad \hat{\rho} \geq 0 \quad [\Rightarrow \quad \hat{\rho}^\dagger = \hat{\rho}]. \tag{2.17}$$

Such operator belongs to the bounded linear operators Hilbert space $\mathcal{B}(\mathcal{H})$. If the state is pure $\hat{\rho} = |\psi\rangle\langle\psi|$ where $|\psi\rangle$ belongs to a Hilbert space $\mathbb{C}^d$ for qu$d$its, (discrete variables system) or $\mathcal{L}^2(\Omega)$ for N modes, (Continuous Variable system). Notice the inconvenience of density operator formalism for CV since the states belong to an infinite dimensional Hilbert space.

For systems of Continuous Variable, the Wigner distribution function gives a complete description of the state. Given a state $\hat{\rho}$ corresponding to a single mode, the Wigner distribution function is defined as [9]

$$\mathcal{W}_\rho(q,p) = \frac{1}{\pi}\int dx \langle q+x|\hat{\rho}|q-x\rangle e^{-2\mathrm{i}px}. \tag{2.18}$$

This transformation is called Weyl-Fourier transformation and it gives the bridge between density operators and distribution functions. Sometimes, for computational reasons it is better to compute first the characteristic distribution function which is obtained through

$$\chi_\rho(\zeta,\eta) = \mathrm{tr}\{\hat{\rho}\hat{W}_{(\zeta,\eta)}\}. \tag{2.19}$$

The above two distribution functions are fully equivalent in the sense of describing completely our quantum state and are related by a Symplectic-Fourier transform

$$\mathcal{W}_\rho(q,p) = \frac{1}{(2\pi)^2}\int d\zeta \int d\eta\, \chi_\rho(\zeta,\eta) e^{-\mathrm{i}\zeta p + \mathrm{i}\eta q} = \frac{1}{2\pi}\mathcal{SFT}\{\chi_\rho(\zeta,\eta)\}, \tag{2.20}$$

$$\chi_\rho(\zeta,\eta) = \int dq \int dp\, \mathcal{W}_\rho(q,p) e^{\mathrm{i}\zeta p - \mathrm{i}\eta q} = 2\pi\mathcal{SFT}^{-1}\{\mathcal{W}_\rho(q,p)\}. \tag{2.21}$$

The Weyl-Fourier transformation is invertible and it provides a way to recover our density operator from both distribution functions

$$\begin{aligned}\hat{\rho} &= \frac{1}{2\pi}\int dq \int dp \int d\zeta \int d\eta\, \mathcal{W}_\rho(q,p) e^{-\mathrm{i}\zeta p + \mathrm{i}\eta q}\hat{W}_{(-\zeta,-\eta)} = \\ &= \frac{1}{2\pi}\int d\zeta \int d\eta\, \chi_\rho(\zeta,\eta)\hat{W}_{(-\zeta,-\eta)}.\end{aligned} \tag{2.22}$$

At this level, $\mathcal{W}$ (and χ) defines a quantum state iff they satisfy the following properties:

(i) the state is normalized

$$\int dq \int dp\, \mathcal{W}(q,p) = 1, \quad \chi(0,0) = 1 \tag{2.23}$$

and,

(ii) the state is non-negative defined

$$\int dq \int dp\, \mathcal{W}(q,p)\mathcal{W}_p(q,p) \geq 0 \quad [\Rightarrow \quad \mathcal{W}^*(q,p) = \mathcal{W}(q,p)] \tag{2.24}$$

$$\sum_{i,j=1}^{2N} a_i^* a_j \chi(\zeta_j - \zeta_i) e^{\frac{\mathrm{i}}{2}(\zeta_i^T\cdot\mathcal{J}\cdot\zeta_j)} \geq 0 \quad [\Rightarrow \quad \chi^*(\zeta,\eta) = \chi(-\zeta,-\eta)] \tag{2.25}$$

for all pure states $\mathcal{W}_p$ and for all $a_{i,j} \in \mathbb{R}$. This can be shown using the following theorem:

[9] For pure states the definition gets simplified to $\mathcal{W}_\rho(q,p) = \frac{1}{\pi}\int dx\, e^{-2\mathrm{i}px}\psi^*(q-x)\psi(q+x) = = \int dx\, \tilde{\mathcal{W}}_\rho(q,x)e^{-2\mathrm{i}px}$. One can see a direct link between the wave function and the Symplectic-Fourier transform of the Wigner distribution via $\psi(q) = \sqrt{\frac{\pi}{\tilde{\mathcal{W}}(q_0,0)}}\tilde{\mathcal{W}}(\frac{1}{2}(q+q_0), \frac{1}{2}(q-q_0))$.

Theorem 2.4.1 (Quantum Bochner-Khinchin theorem) *For $\chi(\eta)$ to be a characteristic function of a quantum state the following conditions are necessary and sufficient*
1.) $\chi(0) = 1$ and $\chi(\eta)$ is continuous at $\eta = 0$,
2.) $\chi(\eta)$ is $\mathcal{J}-$positive (symplectic-positive defined).

2.4.2 Properties of the Wigner distribution

Properties

i) *Quasidistribution:* It is a real valued quasi-distribution because it admits negatives values.

ii) *T-symmetry:* It has time symmetry

$$t \to -t \Longleftrightarrow \mathcal{W}(q,p,t) \to \mathcal{W}(q,-p,t). \tag{2.26}$$

iii) *X-symmetry:* It has space symmetry

$$q \to -q \Longleftrightarrow \mathcal{W}(q,p,t) \to \mathcal{W}(-q,-p,t). \tag{2.27}$$

iv) *Galilei invariant:* It is Galilei invariant

$$q \to q-a \Longleftrightarrow \mathcal{W}(q,p,t) \to \mathcal{W}(q+a,p,t). \tag{2.28}$$

v) *T-evolution:* The equation of motion for each point in the phase-space is classical in the absence of forces [10]

$$\frac{d\hat{\rho}}{dt} = -\frac{1}{\mathrm{i}}[\hat{\rho},\hat{H}] \Longleftrightarrow \frac{\partial \mathcal{W}(q,p,t)}{\partial t} = -\frac{p}{m}\frac{\partial \mathcal{W}(q,p,t)}{\partial q}. \tag{2.30}$$

vi) *Bounded:* It is bounded

$$|\mathcal{W}(q,p)| \leq \frac{1}{\pi}. \tag{2.31}$$

For pure states [11] the demonstration reads

$$\begin{aligned}|\mathcal{W}(q,p)|^2 = \frac{1}{\pi^2}\left|\int dx\, e^{-2\mathrm{i}px}\psi^*(q-x)\psi(q+x)\right|^2 \leq \\ \leq \frac{1}{\pi^2}\int dx\left|e^{\mathrm{i}px}\psi(q-x)\right|^2 \int dx\left|e^{-\mathrm{i}px}\psi(q+x)\right|^2 = \frac{1}{\pi^2}.\end{aligned} \tag{2.32}$$

[10] Remember that when we are speaking about states of light m has to be interpret as permittivity of vacuum ϵ_0. Notice there is a minus sign difference with Heisenberg's equation of motion.

$$\frac{d\hat{A}}{dt} = \frac{1}{\mathrm{i}}[\hat{A},\hat{H}]. \tag{2.29}$$

[11] For mixed states, use Schwarz's inequality $|\langle\psi_1|\psi_2\rangle|^2 \leq \langle\psi_1|\psi_1\rangle\langle\psi_2|\psi_2\rangle$ at the density operator level *i.e.* $0 \leq \mathrm{tr}(\rho_1\rho_2)^n \leq \mathrm{tr}(\rho_1)^n\mathrm{tr}(\rho_2)^n$ for $n=1$.

vii) *Normalized:* It is well normalized

$$\int dq \int dp\, \mathcal{W}(q,p) = 1. \tag{2.33}$$

viii) *Quantum marginal distributions:* It possesses good marginal distributions [12]

$$\bar{\mathcal{W}}(q) = \int dp\, \mathcal{W}(q,p) = \langle q|\hat{\rho}|q\rangle \geq 0, \tag{2.34}$$

$$\bar{\mathcal{W}}(p) = \int dq\, \mathcal{W}(q,p) = \langle p|\hat{\rho}|p\rangle \geq 0. \tag{2.35}$$

ix) *Orthonormal:* The orthonormality is preserved

$$\left|\int dq\, \psi^*(q)\phi(q)\right|^2 = 2\pi \int dq \int dp\, \mathcal{W}_\psi(q,p)\mathcal{W}_\phi(q,p). \tag{2.36}$$

If the distributions are equal $\psi = \phi$ we conclude $\int dq \int dp\, \mathcal{W}^2(q,p) = \frac{1}{2\pi}$ for all pure states, which is a lower bound in general see appendix 2.B and Eq. (2.81), also it excludes classical distributions such $\mathcal{W}(q,p) = \delta(q-q_0)\delta(p-p_0)$. If they are orthogonal, $\psi \perp \phi$, we conclude $\int dq \int dp\, \mathcal{W}_\psi(q,p)\mathcal{W}_\phi(q,p) = 0$ which tells us that the Wigner distribution function, in general, cannot be everywhere positive.

x) *Complete orthonormal set:* The set of functions $\mathcal{W}_{nm}(q,p)$ form a complete orthonormal set (if $\psi_n(q)$ are already a set)

$$2\int dq \int dp\, \mathcal{W}^*_{nm}(q,p)\mathcal{W}_{n'm'}(q,p) = \frac{1}{2\pi}\,\delta_{nn'}\delta_{mm'}, \tag{2.37}$$

$$\sum_{n,m} \mathcal{W}^*_{nm}(q,p)\mathcal{W}_{nm}(q',p') = \frac{1}{2\pi}\delta(q-q')\delta(p-p'), \tag{2.38}$$

where

$$\mathcal{W}_{nm}(q,p) = \frac{1}{\pi}\int dx\, e^{-2\mathrm{i}px}\psi^*_n(q-x)\psi_m(q+x). \tag{2.39}$$

2.4.3 The generating function of a Classical probability distribution

Denoting by y (x) a random variable which can be discrete $y \in \{y_i\}$ (or continuous $x \in [a,b]$) and its corresponding (density) probability $p(y_i)$ ($p(x)$), we can establish the normalization constrain as

$$\left.\begin{array}{rcl} \sum_i p(y_i) & = & 1 \\ \int_a^b p(x)dx & = & 1 \end{array}\right\}. \tag{2.40}$$

Of relevant importance given a probability distribution are the following quantities:

[12] For pure states they correspond to the square modulus of the wave function in position $|\psi(q)|^2$ and in momentum $|\tilde{\psi}(p)|^2$ representation.

i) *Mean value of* $u(x)$: $E[u(x)] = \int u(x)p(x)dx$.

ii) *Moment of order* m *respect point* c *of* x: $\alpha_c^m = E[(x-c)^m]$.

iii) *Mean value of* x: $\mu = \alpha_0^1 = E[x]$.

iv) *Standard deviation of* x: $\sigma = \sqrt{\mathrm{var}(x)} = \sqrt{\alpha_\mu^2} = \sqrt{E[(x-\mu)^2]}$.

v) *Covariance of* x_i *and* x_j: [13] $C_{ij} = \mathrm{cov}(x_i, x_j) = E[(x_i - \mu_i)(x_j - \mu_j)]$,

where $i, j = 1, 2, \ldots, 2N$.

Theorem 2.4.2 (Taylor's theorem) *Any well behaved distribution function can be reconstructed by its (in general) infinite moments.*

This theorem, of considerable importance, tell us that any distribution $p(x)$ can be retrieved by its moments α_c^m only. We define the vector d and the matrix C called mean vector and covariance matrix by

$$\left.\begin{array}{rcl} C & = & [[\mathrm{cov}(x_i, x_j)]] \\ d & = & [[\mu_i]] \end{array}\right\} . \tag{2.41}$$

What is more important is that d and C encode all the information of 1st and 2nd moments.

If we define the generating function of a distribution function by a Laplace transformation (provided it exists)

$$M(\eta) = \mathcal{LT}\{p(x)\} = E[e^{x\eta}], \tag{2.42}$$

all moments can be obtained by subsequently differentiating the generating function

$$\alpha_0^m = \left.\frac{\partial^{(m)} M(\eta)}{\partial \eta^m}\right|_{\eta=0} . \tag{2.43}$$

2.4.4 The generating function of a quasi-probability distribution

In the same way as in Classical Probability where all the moments of a distribution characterize the distribution, the Wigner quasi-distribution function is fully characterized by its moments. To adapt the classical formalism to the quantum Wigner quasi-distribution function we have to introduce the following transcription $\eta \longrightarrow \mathrm{i}\eta, M \longrightarrow \chi, \mathcal{LT} \longrightarrow \mathcal{FT}$ [14]. We then define the generating function of the Wigner distribution (characteristic function) by a Fourier transformation, which always exists, since the Wigner distribution is an integrable function. In general it is complex and reads

[13] Here subindex i, j labels all the possible variables of the distribution, when they are equal, C_{ii} corresponds to the variance $\mathrm{var}(x_i)$ of the variable x_i.

[14] $\mathcal{LT}\{f(x)\} = \int_0^\infty f(x)\mathrm{e}^{-yx}dx$ while $\mathcal{FT}\{f(x)\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(x)\mathrm{e}^{-\mathrm{i}yx}dx = \tilde{f}(y)$.

$$\chi(\eta) = \mathcal{FT}\{\mathcal{W}(x)\} = E[e^{\mathrm{i}x\eta}], \tag{2.44}$$

then all moments can be obtained by subsequently differentiating the generating function

$$\beta_0^m = \frac{1}{\mathrm{i}^m} \frac{\partial^{(m)}\chi(\eta)}{\partial\eta^m}\Bigg|_{\eta=0} . \tag{2.45}$$

Analogously, we define, given a quantum Wigner distribution function the displacement vector (DV) d (a $2N$ real vector) and the covariance matrix (CM) γ (a $2N \times 2N$ real symmetric matrix). The DV contains the information of the first moments. By the space symmetry only relative DVs are of physical meaning. The CM is much more richer, it contains information (up to second moments) about the purity, entanglement,... The CM γ, corresponding to a physical state must be symplectic-positive defined, *i.e.*

$$\gamma + \mathrm{i}\mathcal{J} \geq 0. \tag{2.46}$$

Such a constrain also implies that, because the symplectic matrix is antisymmetric, that $\gamma \geq 0$. Positivity implies hermiticity which translates here to $\gamma^T = \gamma$. Its useful also to introduce here the symplectic spectrum [15] of the CM because the positivity condition reads, in terms of the symplectic eigenvalues, as $\mu_i \geq 1$, $i = 1, 2, \ldots, N$.

2.5 Gaussian states

Gaussian states are those states with a Gaussian Wigner distribution function. Among all the CV systems, Gaussian states, are of the greatest importance. A Gaussian distribution appears as the limit of many others and occurs in a great variety of different conditions. This fact is reflected in the Central Limit Theorem which is one of the cornerstone of the Classical Probability and Statistics Theory.

Theorem 2.5.1 (Central limit theorem) *Suppose we have n independent random variables $x_1, x_2, \ldots, x_n$ which are all distributed with a mean value μ and a standard deviation σ (each of them can have different arbitrary distribution functions $p_i(x_i)$). In the limit $n \to \infty$ the arithmetic mean $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$ is Gaussian (or normal) distributed with mean value μ and standard deviation $\frac{\sigma}{\sqrt{n}}$* i.e. $\bar{p}(\bar{x}) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(\bar{x}-\mu)^2}{2\sigma^2}}$.

The importance of Gaussian probability distributions is also encoded in the following theorem

[15] Every positive matrix M can be diagonalized under symplectics with a symplectic spectrum symspec(M) of the form $\{\mu_i\}$ and degenerated with multiplicity 2. The values $\{\mu_i\}$ are obtained throw spec$(-\mathrm{i}\mathcal{J}M) = \{\pm\mu_i\}$, $i = 1, 2, \ldots, \frac{\dim(M)}{2}$.

Theorem 2.5.2 (Marcinkiewicz's theorem) *If we define the cumulant generating function as $K(\eta) = \ln M(\eta)$, then, either the cumulant is a polynomial of order 2 or it has infinite terms.*

Lemma 2.5.1 (Gaussianity lemma) *$p(x)$ is a Gaussian(non-Gaussian) distribution iff the cumulant is a polynomial of order 2(∞).*

In general, to describe a probability distribution, all moments are necessary but as long as we are concern with Gaussian distributions, 1st and 2nd moments are sufficient. In fact, all other higher moments can be rewritten in terms of them. This is a consequence of the theorem 2.5.2.

2.5.1 Displacement Vector and Covariance Matrix

The Displacement Vector (DV) and the Covariance Matrix (CM) are enough to describe Gaussian states. Analogously to the classical case, it is straightforward to obtain the moments of order β_0^m of a distribution by differentiating the generating function. Computing 1st and 2nd moments, through (2.19) we get [16]

$$\beta^1_{0,i} = -\mathrm{i}\frac{\partial}{\partial\eta_i}\chi(\eta)\bigg|_{\eta=0} = \mathrm{tr}(\hat{\rho}\hat{R}'_i), \tag{2.47}$$

$$\beta^2_{0,ij} = (-\mathrm{i})^2\frac{\partial^2}{\partial\eta_i\partial\eta_j}\chi(\eta)\bigg|_{\eta=0} = \frac{1}{2}\mathrm{tr}(\hat{\rho}\{\hat{R}'_i,\hat{R}'_j\}) = \mathrm{tr}(\hat{\rho}\hat{R}'_i\hat{R}'_j) - \frac{\mathrm{i}}{2}\mathcal{J}_{ij}, \tag{2.48}$$

where $\hat{R}'_i = \mathcal{J}\cdot\hat{R}_i$.

Finally, we define the DV and the CM as [17]

$$\begin{aligned} d_i &= \mathrm{tr}(\hat{\rho}\hat{R}_i) && (2.49)\\ \gamma_{ij} &= \mathrm{tr}(\hat{\rho}\{\hat{R}_i - d_i\hat{\mathbb{I}}, \hat{R}_j - d_j\hat{\mathbb{I}}\}) = \\ &= 2\mathrm{tr}[\hat{\rho}(\hat{R}_i - d_i\hat{\mathbb{I}})(\hat{R}_j - d_j\hat{\mathbb{I}})] - \mathrm{i}\mathcal{J}_{ij} = && (2.50)\\ &= 2\mathrm{Re}\{\mathrm{tr}[\hat{\rho}(\hat{R}_i - d_i\hat{\mathbb{I}})(\hat{R}_j - d_j\hat{\mathbb{I}})]\}. \end{aligned}$$

[16] Notice: $(\frac{\partial}{\partial\eta_i}e^{\mathrm{i}\eta^T\cdot\hat{R}})\Big|_{\eta_i=0} = \mathrm{i}\hat{R}_i$ and $(\frac{\partial^2}{\partial\eta_i\partial\eta_j}e^{\mathrm{i}\eta^T\cdot\hat{R}})\Big|_{\eta_{i,j}=0} = \frac{1}{2}[\hat{R}_i,\hat{R}_j] - \hat{R}_i\hat{R}_j = -\frac{1}{2}\{\hat{R}_i,\hat{R}_j\}$ where we have used Cambell-Hausdorff formula $e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-\frac{1}{2}[\hat{A},\hat{B}]}$ (when $[\hat{A},\hat{B}] \propto \mathbb{I}$).

[17] For pure states $d_i = \langle\hat{R}_i\rangle_\rho$ and $\gamma_{ij} = \langle\{\hat{R}_i - d_i\hat{\mathbb{I}}, \hat{R}_j - d_j\hat{\mathbb{I}}\}\rangle_\rho = \langle\{\hat{R}_i,\hat{R}_j\}\rangle_\rho - 2\langle\hat{R}_i\rangle_\rho\langle\hat{R}_j\rangle_\rho$, where, by the anticommutator definition, we see a factor 2 of difference with the classical analog and so $\gamma_{ij} \sim 2C_{ij}$. The diagonal terms can be rewritten in terms of the uncertainties as $\gamma_{ii} = 2(\Delta R_i)^2_\rho$ where as usual $(\Delta A)_\psi = \sqrt{\langle\hat{A}^2\rangle_\psi - (\langle\hat{A}\rangle_\psi)^2}$.

2.5.2 Phase-space representation of states

It is important to remark here that symplectic operations at the level of the DV and CM act in such a way that any Gaussian unitary $\hat{U}_S$ maps to the following transformation $\gamma_S = S \cdot \gamma \cdot S^T$ and $d_S = S \cdot d + s$ where S stands for an element of the symplectic group, while s stands for a phase-space translation.

With these definitions it can be shown that the Wigner distribution of any Gaussian state can be written in terms of the DV and CM through [18]

$$\mathcal{W}(\zeta) = \frac{1}{\pi^N \sqrt{\det \gamma}} e^{-(\zeta-d)^T \cdot \frac{1}{\gamma} \cdot (\zeta - d)}, \tag{2.51}$$

while its symplectic-Fourier transform reads

$$\chi(\eta) = e^{\mathrm{i}\eta^T \cdot \mathcal{J} \cdot d - \eta^T \cdot \mathcal{J}^T \frac{\gamma}{4} \mathcal{J} \cdot \eta} = e^{\mathrm{i}\eta^T \cdot d' - \eta^T \cdot \frac{\gamma'}{4} \cdot \eta}, \tag{2.52}$$

where $d'_i = \mathcal{J}_{ij} d_j$ and $\gamma'_{ij} = \mathcal{J}^T_{ik} \gamma_{kl} \mathcal{J}_{lj}$.

It is very useful when dealing with Gaussian states to represent them pictorically in the phase-space. As a example we plot here the Wigner distribution function of a rotated squeezed coherent Gaussian state in the phase-space as seen in Fig. 2.1(a). In Fig. 2.1(b), we plot also its pictorical representation, obtained by an horizontal cut of the Wigner function at a factor $\mathrm{e}^{-1/2}$ of the maximum. This closed curve fulfills the following expression $\frac{\mathcal{W}(\zeta)}{\mathcal{W}(d)} = \mathrm{e}^{-1/2}$ (for Gaussian states is nothing else than an ellipse). The area $A = \frac{\pi}{2} \frac{1}{\mathcal{P}} = \pi \Delta\tilde{q} \Delta\tilde{p}$ is closely related with the purity of the state see (2.80) and naturally constrained by the uncertainty principle in an appropriate frame $(\tilde{q}, \tilde{p})$, the one which uncertainties coincide with the major/minor semiaxes of the ellipse. This can be casted in the following theorem.

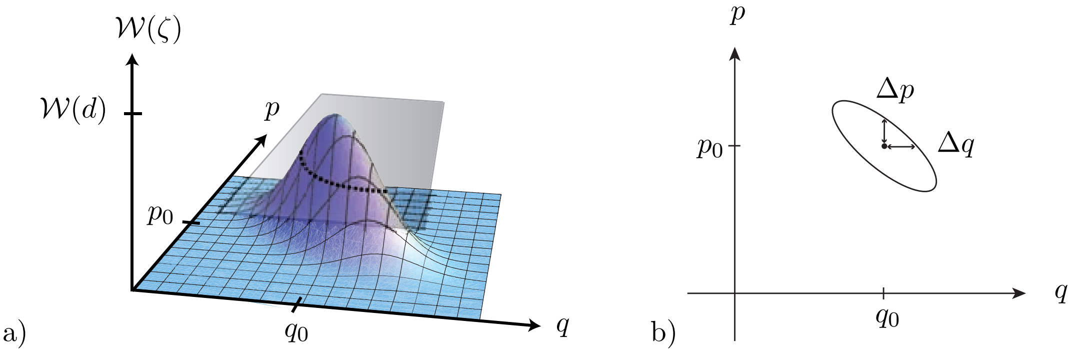

Figure 2.1: A rotated squeezed coherent Gaussian state with rotating angle $\phi = 50°$, squeezing parameter $r = 0.4$ and displacement $\alpha = \frac{q_0 + \mathrm{i}p_0}{\sqrt{2}}$. a) Wigner distribution function of the state where $d^T = (q_0, p_0)$. b) Gaussian state pictorical representation in the phase-space containing the DV and CM information where $2(\Delta q)^2 = \cosh 2r - \sinh 2r \cos 2\phi$ and $2(\Delta p)^2 = \cosh 2r + \sinh 2r \cos 2\phi$.

[18] We see here that $\max[\mathcal{W}(\zeta)] = \mathcal{W}(d) = \frac{1}{\pi^N \sqrt{\det \gamma}} \leq \frac{1}{\pi^N}$ where the equality holds for pure states only (2.31).

Theorem 2.5.3 (Minimum uncertainty states theorem) *Equality in Heisenberg's uncertainty theorem is attained iff the state is a pure Gaussian state* i.e. *a rotated squeezed coherent state,* $|\psi\rangle = \hat{U}_\theta \hat{U}_r \hat{U}_\alpha |0\rangle$.

All pure Gaussian states of one mode, characterized by its γ (and if necessary by d), can be obtained from the vacuum state by an appropriate squeezing+rotation plus displacement in the phase-space. These states, by virtue of theorem 2.5.3, are the minimum uncertainty states. Instead, mixed Gaussian states of one mode can be all obtained from a thermal state through a squeezing+rotation plus displacement.

As the cornerstone examples of Gaussian states, we have the vacuum, coherent, squeezed and thermal states. One can compute their first and second moments and construct the corresponding DV and CM shown below.

- *Vacuum*: $|0\rangle$ s.t. $\hat{a}|0\rangle = 0$

$$\gamma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad d_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2.53}$$

- *(Pure) Coherent*: [19] $|\alpha\rangle = \hat{\mathcal{D}}(\alpha)|0\rangle = \hat{U}_\alpha|0\rangle$

$$\gamma_\alpha = S_\alpha \gamma_0 S_\alpha^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad d_\alpha = S_\alpha d_0 + s_\alpha = \begin{pmatrix} q_0 \\ p_0 \end{pmatrix}, \tag{2.54}$$

where $\alpha = \alpha_R + \mathrm{i}\alpha_I = \frac{q_0 + \mathrm{i}p_0}{\sqrt{2}}$.

- *(Pure) Squeezed*: $|r\rangle = \hat{\mathcal{S}}(r)|0\rangle = \hat{U}_r|0\rangle$

$$\gamma_r = S_r \gamma_0 S_r^T = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}, \quad d_r = S_r d_0 + s_r = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2.55}$$

- *(Mixed) Thermal*: $\hat{\rho}_\beta = \frac{1}{\pi M}\int d^2\alpha |\alpha\rangle\langle\alpha| \mathrm{e}^{-|\alpha|^2/M}$

$$\gamma_\beta = \begin{pmatrix} 2M+1 & 0 \\ 0 & 2M+1 \end{pmatrix}, \quad d_\beta = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \tag{2.56}$$

where $M = \frac{1}{e^{\beta\hbar\omega}-1} \geq 0$ being β the inverse temperature (we fix units such that $k_B = 1$).

In Fig. 2.2 we plot pictorically the above examples.

[19] A Coherent state can alternatively be defined as the eigenstate of the annihilation operator, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. Coherent states form an *overcomplete* non-orthogonal ($|\langle\alpha|\alpha'\rangle|^2 = \mathrm{e}^{-|\alpha-\alpha'|^2}$ because $\langle\alpha|\alpha'\rangle = \exp\left[-(|\alpha|^2 + |\alpha'|^2)/2 + \alpha^*\alpha'\right]$) set basis ($\frac{1}{\pi}\int d^2\alpha|\alpha\rangle\langle\alpha| = \mathbb{I}$) of vectors of the Hilbert space.

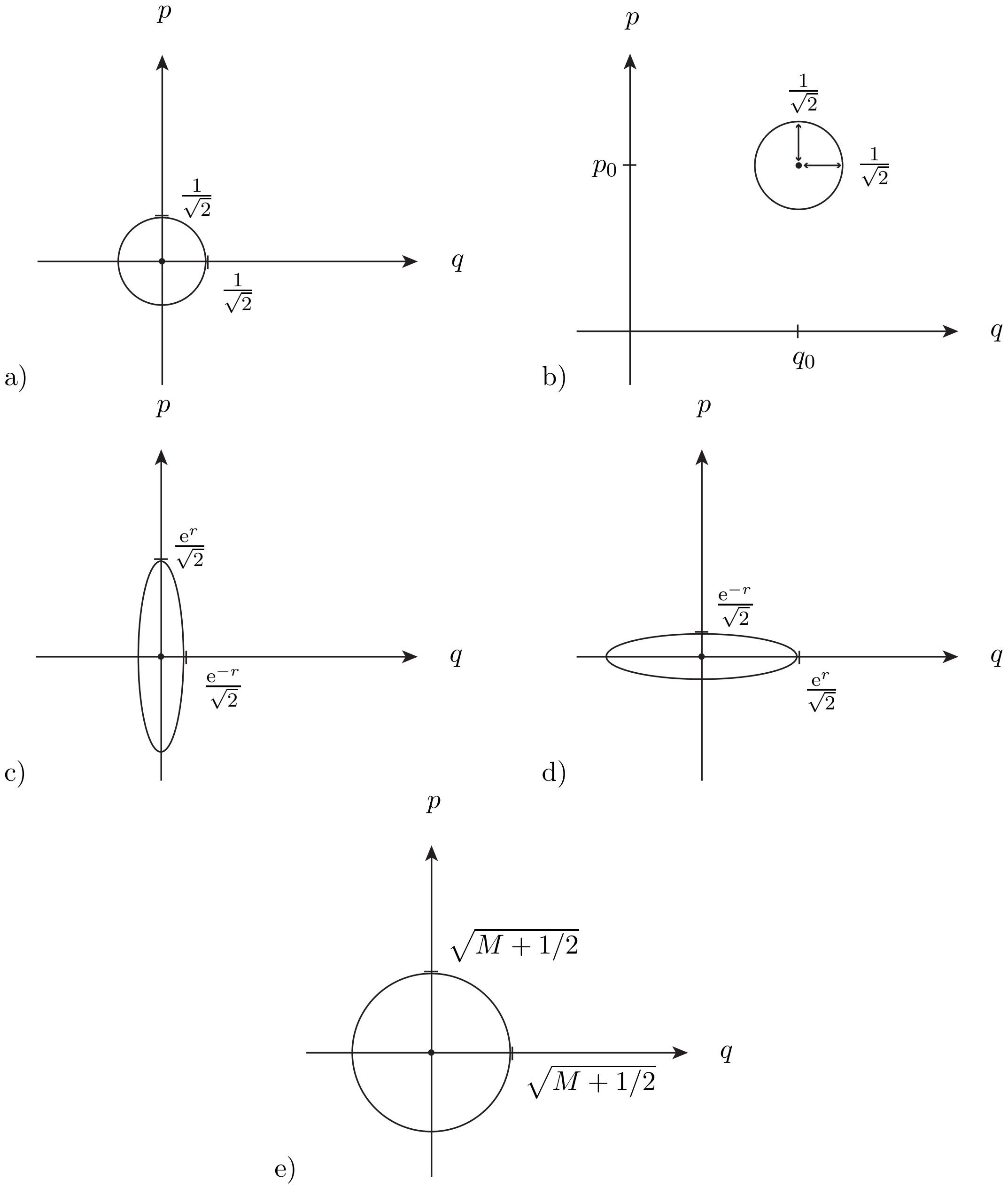

Figure 2.2: a) Vacuum state. b) Coherent state being $\alpha = \frac{q_0+ip_0}{\sqrt{2}}$. c) Squeezed state in position. d) Squeezed state in momentum. e) Thermal state of inverse temperature $\beta = \frac{1}{\hbar\omega}\ln(\frac{M+1}{M})$. All states except the thermal state are pure and are also minimal uncertainty states ($A = \frac{\pi}{2}$).

2.5.3 Hilbert space, phase-space and DV-CM connection

We have already shown how to describe quantum states and operations at different levels *i.e.* Hilbert space, phase-space and DV-CM. Two main connections are needed still to perform calculations in the phase-space: the ordering of the operators and the metric between them.

The Weyl association rule tells us about the ordering operators. Provided we are using the Wigner distribution, which is symmetrical ordered, when working with observables we have to take into account that as we are in the phase-space (we have avoided its operator character) we have to symmetrize them. The way we have to symmetrize operators is

$$e^{\mathrm{i}\zeta\hat{q}+\mathrm{i}\eta\hat{p}} \longrightarrow : e^{\mathrm{i}\zeta\hat{q}+\mathrm{i}\eta\hat{p}} := e^{\mathrm{i}\zeta\hat{q}+\mathrm{i}\eta\hat{p}} \longleftrightarrow e^{\mathrm{i}\zeta q+\mathrm{i}\eta p}, \tag{2.57}$$

where : : stands for the symmetrical order. In general for a polynomial on q and p

$$\hat{q}^n\hat{p}^m \longrightarrow : \hat{q}^n\hat{p}^m := \frac{1}{2^n}\sum_{r=0}^{n}\binom{n}{r}\hat{q}^r\hat{p}^m\hat{q}^{n-r} = \frac{1}{2^m}\sum_{r=0}^{m}\binom{m}{r}\hat{p}^r\hat{q}^n\hat{p}^{m-r} \longleftrightarrow q^np^m. \tag{2.58}$$

Lets us present an example, consider the observable $\mathcal{QP}$, its quantum associated operator is of course $\hat{q}\hat{p}$. We know that $\hat{q}$ and $\hat{p}$ do not commute but in the phase-space qp and pq are functionally treated in the same way. Imagine we need to find its average value, we have then to remove the ambiguity by symmetrizing. The recipe is $\hat{q}\hat{p} \longrightarrow : \hat{q}\hat{p} := \frac{\hat{q}\hat{p}+\hat{p}\hat{q}}{2} \longleftrightarrow qp$. And so the average to be performed is

$$< \mathcal{QP} >=< \hat{q}\hat{p} >_\rho =< \frac{\hat{q}\hat{p}+\hat{p}\hat{q}}{2} + \mathrm{i}/2 >_\rho =< qp + \mathrm{i}/2 >_{\mathcal{W}} . \tag{2.59}$$

Operationally the averages on phase-space (with respect to the Wigner) correspond to the averages of symmetrical ordered operators on the Hilbert space.

More important and relevant averages, concern the moments, which can be obtained via the Wigner distribution as

$$d_i = \mathrm{tr}(\hat{\rho}\hat{R}_i) = \int d^{2N}\zeta \;\; [\zeta_i]\,\mathcal{W}(\zeta) \tag{2.60}$$

and

$$\gamma_{ij} = \mathrm{tr}(\hat{\rho}\{\hat{R}_i - d_i\hat{\mathbb{I}}, \hat{R}_j - d_j\hat{\mathbb{I}}\}) = \int d^{2N}\zeta \;\; [2(\zeta_i - d_i)(\zeta_j - d_j)]\,\mathcal{W}(\zeta) \tag{2.61}$$

where one see explicitly the symmetrization.

Theorem 2.5.4 (Quantum Parseval theorem) *Let $\hat{W}_\zeta$ be a strongly continuous and irreducible Weyl system acting on the Hilbert space $\mathcal{H}_\Omega$ with phase-space Ω. Then $\hat{A} \mapsto A^\chi(\eta) = \mathrm{tr}\{\hat{A}\hat{W}_\eta\}$, with $\eta \in \Omega$, is an isometric map from the Hilbert space $\mathcal{H}_\Omega$ (Hilbert-Schmidt operators) onto the Hilbert space $\mathcal{L}^2(\Omega)$ (square-integrable measurable functions on Ω) such that*

$$\mathrm{tr}(\hat{A}^\dagger\hat{B}) = \frac{1}{(2\pi)^N}\int d^{2N}\eta \;\mathrm{tr}\{\hat{A}\hat{W}_\eta\}^*\mathrm{tr}\{\hat{B}\hat{W}_\eta\}. \tag{2.62}$$

From this theorem of capital importance, follows how to compute the scalar product between operators

$$\begin{aligned}\mathrm{tr}\{\hat{A}^{\dagger}\hat{B}\} &= \frac{1}{(2\pi)^N}\int d^{2N}\eta\; A^{\chi *}(\eta)B^{\chi}(\eta) = \\ &= \frac{1}{(2\pi)^N}\int d^{2N}\zeta\; A^{\mathcal{W}}(\zeta)B^{\mathcal{W}}(\zeta),\end{aligned} \tag{2.63}$$

where the trace of an operator is defined via [20]

$$\mathrm{tr}\{\hat{A}\} = A^{\chi}(0,0) = \frac{1}{(2\pi)^N}\int d^{2N}\zeta\; A^{\mathcal{W}}(\zeta), \tag{2.64}$$

and the expectation value of an observable

$$\begin{aligned}\langle \hat{A}\rangle_{\rho} = \mathrm{tr}\{\hat{\rho}\hat{A}\} &= \frac{1}{(2\pi)^N}\int d^{2N}\eta\; \chi^{*}(\eta)A^{\chi}(\eta) = \\ &= \int d^{2N}\zeta\; \mathcal{W}(\zeta)A^{\mathcal{W}}(\zeta).\end{aligned} \tag{2.65}$$

To justify the above expression we just need to define properly the Fourier-Weyl transform for an arbitrary operator as

$$\begin{aligned}\hat{A} = \mathcal{FWT}\{A^{\chi}(\eta)\} &= \frac{1}{(2\pi)^N}\int d^{2N}\eta\; A^{\chi}(\eta)\hat{W}_{-\eta} = \\ &= \frac{1}{(2\pi)^{2N}}\int d^{2N}\eta \int d^{2N}\zeta\; A^{\mathcal{W}}(\zeta)e^{\mathrm{i}\zeta^T\cdot\mathcal{J}\cdot\eta}\hat{W}_{-\eta},\end{aligned} \tag{2.66}$$

and its inverse

$$A^{\chi}(\eta) = \mathcal{FWT}^{-1}\{\hat{A}\} = \mathrm{tr}\{\hat{A}\hat{W}_{\eta}\}, \tag{2.67}$$

$$A^{\mathcal{W}}(\bar{\zeta},\bar{\eta}) = 2^N\int d^N\lambda\,\langle\bar{\zeta}+\lambda|\hat{A}|\bar{\zeta}-\lambda\rangle e^{-2\mathrm{i}\bar{\eta}\lambda} \tag{2.68}$$

where $\bar{\zeta}^T = (\zeta_1, \zeta_2, \ldots, \zeta_N)$ idem for $\bar{\eta}$.

The two equivalent representations characteristic (χ) and Wigner ($\mathcal{W}$) are $\mathcal{SFT}$ related [21]

$$A^{\mathcal{W}}(\zeta) = \mathcal{SFT}\{A^{\chi}(\eta)\} = \frac{1}{(2\pi)^N}\int d^{2N}\eta\; A^{\chi}(\eta)e^{-\mathrm{i}\zeta^T\cdot\mathcal{J}\cdot\eta}, \tag{2.69}$$

$$A^{\chi}(\eta) = \mathcal{SFT}^{-1}\{A^{\mathcal{W}}(\zeta)\} = \frac{1}{(2\pi)^N}\int d^{2N}\zeta\; A^{\mathcal{W}}(\zeta)e^{\mathrm{i}\zeta^T\cdot\mathcal{J}\cdot\eta}. \tag{2.70}$$

With the above transformations everything is now prepared to be translated in the phase-space.

[20] Use that $\mathbb{I}^{\mathcal{W}} = 1$ and $\mathbb{I}^{\chi} = (2\pi)^N\delta^{(2N)}(\eta)$ computed from Eq. (2.68) and Eq. (2.67).

[21] Notice that $A^{\mathcal{W}} = (2\pi)^N\mathcal{W}$ if $\hat{A} = \hat{\rho}$ see Eq. (2.18) (for normalization convenience) while $A^{\chi} = \chi$ if $\hat{A} = \hat{\rho}$ see Eq. (2.19).

2.5.4 Fidelity and purity of Continuous Variable systems

An important concept in statistical physics is to know how close/similar two distributions are. The natural solution is to construct a distance between distribution by choosing a proper metric in the distribution space. A metric M is well defined if it satisfies the following properties:

i) *Symmetric:* $M(X,Y) = M(Y,X)$.

ii) *Triangle inequality:* $M(X,Z) \leq M(X,Y) + M(Y,Z)$.

iii) *Identity:* $M(X,Y) = 0$ iff $X = Y$.

iv) $\Leftarrow$ i)+ii)+iii) *Non-Negativity:* $M(X,Y) \geq 0$. The demonstration reads $2M(X,Y) = M(X,Y) + M(Y,X) \geq M(X,X) = 0$.

Classically given two probability distributions $\{q_x\}$ and $\{p_x\}$ one can define the trace distance D and the fidelity F between them as follows

$$D(\{q_x\},\{p_x\}) = \frac{1}{2}\sum_x |q_x - p_x|, \tag{2.71}$$

$$F(\{q_x\},\{p_x\}) = \sum_x \sqrt{q_x p_x}, \tag{2.72}$$

while the trace distance is a proper metric this is not the case for the fidelity since it fails to agree with iii).

The quantum analogues quantities are the quantum trace distance [22] and the quantum fidelity

$$\mathcal{D}(\hat{\rho},\hat{\sigma}) = \frac{1}{2}\mathrm{tr}|\hat{\rho} - \hat{\sigma}|, \tag{2.73}$$

$$\mathcal{F}(\hat{\rho},\hat{\sigma}) = \left[\mathrm{tr}\sqrt{\hat{\rho}^{1/2}\hat{\sigma}\hat{\rho}^{1/2}}\right]^2. \tag{2.74}$$

They can be related to the classical ones by considering the probability distributions obtained by a measurement

$$\mathcal{D}(\hat{\rho},\hat{\sigma}) = \max_{\{\hat{E}_n\}} D(\{q_n\},\{p_n\}), \tag{2.75}$$

$$\sqrt{\mathcal{F}(\hat{\rho},\hat{\sigma})} = \min_{\{\hat{E}_n\}} F(\{q_n\},\{p_n\}), \tag{2.76}$$

where $\{q_n\} = \mathrm{tr}(\hat{\rho}\hat{E}_n)$, $\{p_n\} = \mathrm{tr}(\hat{\sigma}\hat{E}_n)$ are the probability distributions of an arbitrary positive-operator-valued measurement (POVM) *i.e.* fulfilling $\sum_n \hat{E}_n = \mathbb{I}$.

[22] Trace distance is constructed throw the trace norm $||\,||_1$ defined for an arbitrary matrix M as $||M||_1 = \mathrm{tr}|M| = \mathrm{tr}\sqrt{M^T M} = \sum \mathrm{singularvalues}(M) = \sum \mathrm{eigenvalues}(\sqrt{M^T M}) = \sum \mathrm{spec}(\sqrt{M^T M})$.

Not only $\mathcal{D}(\hat{\rho},\hat{\sigma})$ is a proper metric, but also are the so-called Bures distance and Bures angle defined as $\mathcal{B}(\hat{\rho},\hat{\sigma}) = \sqrt{2-2\sqrt{\mathcal{F}(\hat{\rho},\hat{\sigma})}}$ and $\mathcal{A}(\hat{\rho},\hat{\sigma}) = \arccos(\sqrt{\mathcal{F}(\hat{\rho},\hat{\sigma})})$ respectively. From now on, we consider exclusively the properties of the quantum fidelity (also-called Bures-Uhlmann fidelity).

It's not obvious but it is symmetric and normalized between 1 (equal states) and 0 (orthogonal states). Its definition is simplified when one of the two states is pure (say $\hat{\rho}_1$), in this case it converges to the Hilbert-Schmidt fidelity

$$\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2) = \mathrm{tr}(\hat{\rho}_1\hat{\rho}_2) = \langle\psi_1|\hat{\rho}_2|\psi_1\rangle. \tag{2.77}$$

In case both states are pure, then, the fidelity becomes simply the overlap (transition probability) between the two states

$$\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2) = |\langle\psi_1|\psi_2\rangle|^2. \tag{2.78}$$

It is useful here to use theorem 2.5.4 to evaluate the Hilbert-Schmidt fidelity between two Gaussian state (when at least one is pure) [23]

$$\begin{aligned}\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2) = \mathrm{tr}(\hat{\rho}_1\hat{\rho}_2) = \left(\frac{1}{2\pi}\right)^N \int d^{2N}\eta\, \chi_1^*(\eta)\chi_2(\eta) = (2\pi)^N \int d^{2N}\zeta\, \mathcal{W}_1(\zeta)\mathcal{W}_2(\zeta) = \\ = \frac{1}{\sqrt{\det(\frac{\gamma_1+\gamma_2}{2})}} e^{-d^T(\frac{1}{\gamma_1+\gamma_2})d}\end{aligned} \tag{2.79}$$

where $\gamma_{1(2)}$ and $d_{1(2)}$ belongs to $\hat{\rho}_{1(2)}$, while $d = d_2 - d_1$.

Another important concept in Quantum Information is the purity $\mathcal{P}$ of a quantum state. In general, a pure state is a state which can be written in a suitable basis as a ket ($\hat{\rho} = |\psi\rangle\langle\psi|$) in the Hilbert space, and so $\hat{\rho}^2 = \hat{\rho}\,[\Rightarrow \mathrm{tr}\hat{\rho}^2 = 1]$. A mixed state, on the contrary, cannot be written as a ket but only as a density operator and then $\hat{\rho}^2 \neq \hat{\rho}$. In Continuous Variable a generic mixed state can always be written (for example using the $\mathcal{Q}$-function representation [24]) as $\hat{\rho} = \int d^2\alpha \mathcal{Q}(\alpha)|\alpha\rangle\langle\alpha|$.

The purity, which measures how close is the state from a pure one, is defined as follows

$$\mathcal{P}(\hat{\rho}) = \mathrm{tr}(\hat{\rho}^2). \tag{2.80}$$

While for qu$d$its it is normalized between 1 (pure states) and $\frac{1}{d}$ (maximally mixed states), for Continuous Variable systems ("$d \to \infty$") maximally mixed states have purity 0. Using theorem 2.5.4 we can evaluate the purity of a Gaussian state [25]

$$\mathcal{P}(\hat{\rho}) = (2\pi)^N \int d^{2N}\zeta\, [\mathcal{W}(\zeta)]^2 = \frac{1}{\sqrt{\det\gamma}}. \tag{2.81}$$

[23] The second and third equality is true for all CV states.

[24] $\mathcal{Q}$-function is defined as $\mathcal{Q}(\alpha) = \frac{1}{\pi}\langle\alpha|\hat{\rho}|\alpha\rangle$ and normalized as $\int d^2\alpha\mathcal{Q}(\alpha) = 1$.

[25] The first equality is true for all CV states.

2.5.5 Bipartite Gaussian states, Schmidt decomposition, purification

At the level of density operators, multipartite systems are described on a tensorial Hilbert space structure. This means that we have to "tensor product" $\otimes$, the Hilbert space of each party *i.e.* $\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k$. Notice however that multipartite Gaussian CV systems have a covariance matrix corresponding to a "direct sum" $\oplus$, of each party's associated phase-space *i.e.* $\Omega = \bigoplus_{k=1}^{N} \Omega_k$. This is reminiscent of the Quantum Parseval theorem, which transforms tensor product between density matrices to products of Wigner functions (and Characteristic functions) and at the same time direct sums of covariance matrices and displacements vectors. Therefore, an advantage on Gaussian states is that we fully describe a state by a finite dimensional $N \times N$ matrix plus a $N \times 1$ vector instead of its corresponding infinite dimensional density matrix. Additionally, dimensionality of the phase-space increases slower, as dimensions are added instead of multiplied. [26]

An important property of Gaussian states is that their reductions are again Gaussians. Imagine we have a bipartite Gaussian state $\hat{\rho}$ with covariance matrix γ composed by $N_A + N_B = N$ modes [27], then tracing the N_B modes corresponds to the reduced state $\hat{\rho}_A = \mathrm{tr}_B \hat{\rho}$ with covariance matrix γ_A obtained by the upper left $N_A \times N_A$ block matrix of γ (vice versa with B). Therefore any bipartite Gaussian state can be written in a block structure as $\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}$, where $A = A^T (= \gamma_A)$ and $B = B^T (= \gamma_B)$ are the reductions while C amounts for the correlations between the modes.

For discrete variables, the Schmidt decomposition asserts that every pure bipartite state $|\psi\rangle$ (supposing $N_A \geq N_B$) can be transformed by local unitary operations to the normal form $|\psi\rangle = \sum_{i=1}^{N_B} \sqrt{\lambda_i} |e_i\rangle \otimes |f_i\rangle$ where $\{e_i\}(\{f_i\})$ are orthonormal basis of $A(B)$ and $\{\lambda_i\}$ is the spectrum of the reduced state for B, $\hat{\rho}_B = \mathrm{tr}_A |\psi\rangle\langle\psi|$ satisfying $\lambda_i \geq 0$ and $\sum_{i=1}^{N_B} \lambda_i^2 = 1$.

Theorem 2.5.5 (Schmidt decomposition) *Every pure bipartite Gaussian states of $N = N_A + N_B$ modes $N_A \geq N_B$, by local symplectic transformations can be brought to the normal form*

$$\gamma = \gamma_0 \oplus \bigoplus_{i=1}^{N_B} \gamma_i, \tag{2.82}$$

where $\gamma_0 = \mathbb{I}_{2(N_A - N_B)}$, $\gamma_i = \begin{pmatrix} \lambda_i & 0 & c_i & 0 \\ 0 & \lambda_i & 0 & -c_i \\ c_i & 0 & \lambda_i & 0 \\ 0 & -c_i & 0 & \lambda_i \end{pmatrix}$, being $c_i = \sqrt{\lambda_i^2 - 1}$ and $\{\lambda_i\}$ the symplectic spectrum of the reduced covariance matrix for B.

[26] Remember that $\dim(\hat{\rho}_1 \otimes \hat{\rho}_2) = \dim(\hat{\rho}_1)\dim(\hat{\rho}_2)$ while $\dim(\gamma_1 \oplus \gamma_2) = \dim(\gamma_1) + \dim(\gamma_2)$.

[27] From now on we suppose $N_A \geq N_B$.

We see a very peculiar behavior here, each mode of B is entangled with at most one mode of A. The remaining $N_A - N_B$ modes of A are uncorrelated.

Lemma 2.5.2 (Standard form I) *Every* 1×1 *mode (mixed) Gaussian state can be transformed, by local symplectic transformations to the standard form*

$$\gamma = \begin{pmatrix} \lambda_a & 0 & c_x & 0 \\ 0 & \lambda_a & 0 & c_p \\ c_x & 0 & \lambda_b & 0 \\ 0 & c_p & 0 & \lambda_b \end{pmatrix}. \tag{2.83}$$

A Gaussian state in the standard form is called symmetric if $\lambda_a = \lambda_b$, and fully symmetric if it is symmetric and in addition $c_x = -c_p$.

There is a simple way to construct the standard form if one uses the following four local symplectic invariants, [28] the purities $\mathcal{P}_A = 1/\sqrt{\det A} = 1/\lambda_a$, $\mathcal{P}_B = 1/\sqrt{\det B} = 1/\lambda_b$, $\mathcal{P} = 1/\sqrt{\det \gamma} = \left[(\lambda_a\lambda_b - c_x^2)(\lambda_a\lambda_b - c_p^2)\right]^{-1/2}$, and the serelian $\Delta = \det A + \det B + 2\det C = \lambda_a^2 + \lambda_b^2 + 2c_x c_p$ because they can be inverted as follows

$$\begin{aligned} \lambda_a &= 1/\mathcal{P}_A, \\ \lambda_b &= 1/\mathcal{P}_B, \\ c_x &= \frac{\sqrt{\mathcal{P}_A\mathcal{P}_B}}{4}(a_- + a_+), \\ c_p &= \frac{\sqrt{\mathcal{P}_A\mathcal{P}_B}}{4}(a_- - a_+), \\ a_\pm &= \sqrt{\left[\Delta - (\mathcal{P}_A \pm \mathcal{P}_B)^2/(\mathcal{P}_A\mathcal{P}_B)^2\right]^2 - 4/\mathcal{P}^2}. \end{aligned} \tag{2.84}$$

The local and global purities, $\mathcal{P}_A$, $\mathcal{P}_B$ and $\mathcal{P}$ of the state are constrained to be less or equal to one, *i.e.* $\lambda_a, \lambda_b \geq 1$ and $(\lambda_a\lambda_b - c_x^2)(\lambda_a\lambda_b - c_p^2) \geq 1$. The symplectic positivity (2.46) implies, in terms of the invariants, that $1 + \frac{1}{\mathcal{P}^2} \geq \Delta$ or equivalently $1 + (\lambda_a\lambda_b - c_x^2)(\lambda_a\lambda_b - c_p^2) \geq \lambda_a^2 + \lambda_b^2 + 2c_x c_p$.

We stress here that all pure bipartite Gaussian states are symmetric ($\lambda_a = \lambda_b = \lambda$) and fulfills $c_x = -c_p = \sqrt{\lambda^2 - 1}$ being $\lambda \geq 1$. Introducing the change of parameters, $\cosh 2r = \lambda$ we can write any pure bipartite 1×1 Gaussian state as a two mode squeezed state $\gamma_{TMS} = S_{TMS}\mathbb{I}S_{TMS}^T = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}$ with positive r.

Lemma 2.5.3 (Purification) *Every (mixed) Gaussian state of* N_A *modes represented by* γ_A *admits a purification,* i.e. *there exist a pure Gaussian state of* $2N_A$

[28] These four invariants can be written in terms of the symplectic spectrum of the covariance matrix of the state and its reductions as $\mathcal{P} = 1/\sqrt{\prod_i \mu_i^2}$, $\Delta = \sum_i \mu_i^2$, $\mathcal{P}_A = 1/\sqrt{\prod_i \mu_{A,i}^2}$, $\mathcal{P}_B = 1/\sqrt{\prod_i \mu_{B,i}^2}$.

modes whose reduction is γ_A *and reads*

$$\gamma = \begin{pmatrix} \gamma_A & C \\ C^T & \theta_A \gamma_A \theta_A^T \end{pmatrix}, \tag{2.85}$$

with $C = \mathcal{J}\sqrt{-(\mathcal{J}\gamma_A)^2 - \mathbb{I}}\,\theta_A$ *where* $\theta_A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{\oplus N_A}$.

2.5.6 States and operations

By virtue of the Choi-Jamiołkowski isomorphism between completely positive (CP) maps acting on $\mathcal{B}(\mathcal{H})$ (physical actions) and positive operators belonging to $\mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H})$ (unnormalized states), Gaussian operations were fully characterized in [16]. In there the authors showed that each Gaussian operation $\mathcal{G}$ can be associated to a corresponding Gaussian state G *i.e.* there exist an isomorphism between Gaussian CP maps and Gaussian states. Since all Gaussian states can be generated from vacuum state by Gaussian unitary operations and discarding subsystems, then symplectic transformations plus homodyne measurements complete all Gaussian operations.

Lemma 2.5.4 (State-operation's isomorphism lemma) *If a* $N_A \times N_B$*-mode Gaussian state* G *is defined by its first and second moments through*

$$G: \quad \Gamma = \left(\begin{array}{cc} \Gamma_A & \Gamma_{AB} \\ \Gamma_{AB}^T & \Gamma_B \end{array} \right), \quad \Delta = \left(\begin{array}{c} \Delta_A \\ \Delta_B \end{array} \right), \tag{2.86}$$

then the application of $\mathcal{G}$ *on a* N_B*-mode Gaussian state* (γ, d) *produces a* N_A*-mode Gaussian state* (γ', d') *such that*

$$\mathcal{G}: \quad \gamma \mapsto \gamma' \quad = \quad \tilde{\Gamma}_A - \tilde{\Gamma}_{AB} \frac{1}{\tilde{\Gamma}_B + \gamma} \tilde{\Gamma}_{AB}^T, \tag{2.87}$$

$$d \mapsto d' \quad = \quad \Delta_A + \tilde{\Gamma}_{AB} \frac{1}{\tilde{\Gamma}_B + \gamma} (\Delta_B + d), \tag{2.88}$$

where $\tilde{\Gamma} = (\mathbb{I}_N \oplus \theta_N)\Gamma(\mathbb{I}_N \oplus \theta_N)$ *with* $N = N_A + N_B$.

Homodyne detection is a typical example of a Gaussian operation, which realizes a projective (or von Newmann) measurement of one quadrature operator, say $\hat{x}$, thus with associated POVM $|x\rangle\langle x|$. Take a Gaussian state γ of N modes, it can always be divided into $N_A \times N_B$ modes as

$$\gamma = \left(\begin{array}{cc} \gamma_A & C \\ C^T & \gamma_B \end{array} \right), \tag{2.89}$$

and with zero displacement vector. Then, a homodyne measurement of $\hat{x}$ on the last N_B modes, by the lemma 2.5.4, can be described by a Gaussian operator $\hat{\rho}_x$ with corresponding DV and CM given by

$$\Delta_x^T = (0, 0, \ldots, x, x, \ldots)$$

and

$$\Gamma_x = \lim_{r \to \infty} \left(\begin{array}{ccc} \cosh r\, \mathbb{I}_{N_A} & \sinh r\, \theta_{N_A} & 0 \\ \sinh r\, \theta_{N_A} & \cosh r\, \mathbb{I}_{N_A} & 0 \\ 0 & 0 & \left(\begin{array}{cc} 1/r & 0 \\ 0 & r \end{array} \right) \mathbb{I}_{N_B} \end{array} \right).$$

Summarizing, if we measure the x component of the last N_B modes corresponding to B, obtaining the result $(x_1, x_2, \ldots, x_{N_B})$, system A will turn into a Gaussian state with covariance matrix

$$\gamma'_A = \gamma_A - C^T (X \gamma_B X)^{\mathcal{MP}} C, \tag{2.90}$$

and displacement vector

$$d'_A = C^T (X \gamma_B X)^{\mathcal{MP}} d'_B, \tag{2.91}$$

where $d'_B = (x_1, 0, x_2, 0, \ldots, x_{N_B}, 0)$, $\mathcal{MP}$ denotes Moore Penrose or pseudo-inverse (inverse on the support whenever the matrix is not of full rank) and X is the projector with diagonal entries diag$(1, 0, 1, 0, \ldots)$.

Heterodyne measurement, whose POVM corresponds to $\frac{1}{\pi}|\alpha\rangle\langle\alpha|$, and in general [29] all POVM of the form $|\gamma, d\rangle\langle\gamma, d|$, can be achieved with homodyne measurement by the use of ancillary systems and beam splitters.

2.6 Entanglement in Continuous Variable: criteria and measures

Concerning bipartite entanglement, for discrete variable systems an important separability criterium based on the partial transpose (time reversal) exists. If $\hat{\rho}$ is a generic state, then $\hat{\rho}^{T_A}$ represents the state after one perform time reversal on subsystem A.

Lemma 2.6.1 (NPPT Peres criterium) *Given a bipartite state $\hat{\rho}$, if it has non-positive partial transpose ($\hat{\rho}^{T_A} \ngeq 0 \Rightarrow \hat{\rho}^{T_B} \ngeq 0$), then $\hat{\rho}$ is entangled* [18].

Lemma 2.6.2 (NPPT Horodecki criterium) *In $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ given a bipartite state $\hat{\rho}$, it is entangled iff it has non-positive partial transpose ($\hat{\rho}^{T_A} \ngeq 0 \Rightarrow \hat{\rho}^{T_B} \ngeq 0$)* [19].

For Continuous Variable states, Peres criterium also holds while Horodecki criterium is true provided our state is composed of $1 \times N$ modes. In particular for Gaussian

[29] All pure Gaussian states can be obtained from $|\alpha\rangle$ by Gaussian unitaries.

states, time reversal is very easy to implement at the covariance matrix level. If $\hat{T}$ is the reversal operator then $S_T = \theta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is the corresponding symplectic operations in phase-space. So we can rewrite the lemma 2.6.2 for Gaussian states.

Lemma 2.6.3 (NPPT Simon criterium) *For $1\times N$ modes given a bipartite Gaussian state γ, it is entangled iff it has non-positive partial transpose ($\theta_A\gamma\theta_A^T + \mathrm{i}\mathcal{J} \ngeq 0 \Rightarrow \theta_B\gamma\theta_B^T + \mathrm{i}\mathcal{J} \ngeq 0$)* [20, 21].

Under partial transposition the serelian changes as $\Delta \to \tilde{\Delta} = \Delta - 4\det C = \lambda_a^2 + \lambda_b^2 - 2c_x c_p$ and so positivity of the partial transpose can be written, in terms of invariants, as $1 + \frac{1}{P^2} \geq \tilde{\Delta}$ while in terms of the symplectic eigenvalues of the partial transpose, as $\tilde{\mu}_i \geq 1$, $i = 1, 2, \ldots, N$.

Lemma 2.6.4 (CV Inseparability Duan criterium)[30] *We define the EPR-like operators, $\hat{u} = |a|\hat{x}_1 + \frac{1}{a}\hat{x}_2$ and $\hat{v} = |a|\hat{p}_1 - \frac{1}{a}\hat{p}_2$ where $a \in \mathbb{R}$. If a bipartite state $\hat{\rho}$ (Gaussian or non-Gaussian) is separable, then $(\Delta\hat{u})_\rho^2 + (\Delta\hat{v})_\rho^2 \geq a^2 + \frac{1}{a^2}$, for all $a \in \mathbb{R}$* [22].

Lemma 2.6.5 (GS Inseparability Duan criterium) *Any bipartite Gaussian state $\hat{\rho}$ can be written in standard form II (by two local squeezings on standard form I) as $\gamma = \begin{pmatrix} n_1 & 0 & c_1 & 0 \\ 0 & n_2 & 0 & c_2 \\ c_1 & 0 & m_1 & 0 \\ 0 & c_2 & 0 & m_2 \end{pmatrix}$ where $\frac{n_1-1}{m_1-1} = \frac{n_2-1}{m_2-1}$, $|c_1| - |c_2| = \sqrt{(n_1-1)(m_1-1)} - \sqrt{(n_2-1)(m_2-1)}$, then the state is separable iff $(\Delta\hat{u})_\rho^2 + (\Delta\hat{v})_\rho^2 \geq a_0^2 + \frac{1}{a_0^2}$, for all $a_0 \in \mathbb{R}$, where $a_0^2 = \sqrt{\frac{m_1-1}{n_1-1}} = \sqrt{\frac{m_2-1}{n_2-1}}$ and EPR-like operators $\hat{u} = a_0\hat{x}_1 - \frac{c_1}{|c_1|}\frac{1}{a_0}\hat{x}_2$ and $\hat{v} = a_0\hat{p}_1 - \frac{c_2}{|c_2|}\frac{1}{a_0}\hat{p}_2$* [22].

Concerning entanglement measures it is usual to deal, as an entanglement measure for pure state, with the entropy of entanglement and for mixed ones with the logarithmic negativity.

- Entropy of entanglement:

$$E_S(\hat{\rho}) = S(\hat{\rho}_A) = -\mathrm{tr}(\hat{\rho}_A \log_2 \hat{\rho}_A), \tag{2.92}$$

  where S is the von Neumann Entropy $S(\hat{\rho}) = -\mathrm{tr}(\hat{\rho}\log_2\hat{\rho})$, and $\hat{\rho}_A$ is the reduction of A. For any CV state it reduces (in terms of the Schmidt coefficients) to

$$E_S(\hat{\rho}) = -\sum_{i=1}^{\infty} \lambda_i^2 \log_2 \lambda_i^2, \tag{2.93}$$

[30] For all CV states a less restrictive upper bound is imposed by the uncertainty principle, *i.e.* $(\Delta\hat{u})_\rho^2 + (\Delta\hat{v})_\rho^2 \geq \left|a^2 - \frac{1}{a^2}\right|$ due to the sum uncertainty relation $(\Delta\hat{A})^2 + (\Delta\hat{B})^2 \geq 2\Delta\hat{A}\Delta\hat{B} \geq |\langle[\hat{A},\hat{B}]\rangle|$.

while for Gaussian states (in terms of the symplectic eigenvalues),

$$E_S(\gamma) = -\sum_{i=1}^{N_A}[(\frac{\mu_i+1}{2})\log_2(\frac{\mu_i+1}{2}) - (\frac{\mu_i-1}{2})\log_2(\frac{\mu_i-1}{2})], \tag{2.94}$$

where $\{\pm\mu_i\} = \mathrm{spec}(-\mathrm{i}\mathcal{J}\gamma_A)$.

The entropy of entanglement is the "unique" measure of entanglement for pure states. It depends only on the Schmidt coefficients and not on the choice of basis, therefore it's invariant under local unitary operations. Furthermore it's unique because all other entanglement measures are in direct correspondence with the entropy of entanglement.

- Logarithmic negativity [23]:

$$E_N(\hat{\rho}) = LN(\hat{\rho}) = \log_2 ||\hat{\rho}^{T_A}||_1, \tag{2.95}$$

where $||\ ||_1$ is the trace norm [31]. For any CV state it can be written (in terms of the negative eigenvalues of the partial transpose) as

$$E_N(\hat{\rho}) = \log_2[1 + 2\sum_{i=1}^{\infty}|\min(\tilde{\lambda}_i, 0)|], \tag{2.96}$$

while for Gaussian states (in terms of the symplectic eigenvalues of the partial transpose),

$$E_N(\gamma) = -\sum_{i=1}^{N}\log_2[\min(\tilde{\mu}_i, 1)], \tag{2.97}$$

where $\{\pm\tilde{\mu}_i\} = \mathrm{spec}(-\mathrm{i}\mathcal{J}\gamma^{T_A})$.

The negativity $N(\hat{\rho}) = \frac{2^{LN(\hat{\rho})-1}}{2}$ is also a computable measure of entanglement for mixed states. It quantifies the violation of the NPPT criterium *i.e.* how much the partial transposition of a density matrix fails to be positive. It's invariant under local unitary operations and an entanglement monotone. For Gaussian states reads

$$N(\gamma) = \frac{1}{2}[\prod_{i=1}^{N}\frac{1}{\min(\tilde{\mu}_i, 1)} - 1]. \tag{2.98}$$

[31] The trace norm for hermitian operators is simple because $||\hat{M}||_1 = \mathrm{tr}\sqrt{\hat{M}^2} = \sum|\mathrm{spec}(\hat{M})| = 1 + 2\sum|\mathrm{negativevalues}(\hat{M})|$.

2.A Appendix: Quantum description of light

2.A.1 Light modes as independent harmonic oscillators

Since Maxwell, we know that classically, light can be relativistically described [32] by the so-called Maxwell field equations. As we will show, each mode of the electromagnetic field is an independent harmonic oscillator with the same classical dynamics. This is shown by constructing the classical Hamiltonian from the Maxwell equations as follows.

We start with Maxwell equations for the electric and magnetic field in presence of sources (ρ) and currents ($\vec{J}$)

$$\begin{aligned} \vec{\nabla}\cdot\vec{E} &= \tfrac{\rho}{\varepsilon_0}, \\ \vec{\nabla}\cdot\vec{B} &= 0, \\ \vec{\nabla}\times\vec{E} &= -\tfrac{\partial\vec{B}}{\partial t}, \\ \vec{\nabla}\times\vec{B} &= \mu_0\varepsilon_0\tfrac{\partial\vec{E}}{\partial t}+\mu_0\vec{J}, \end{aligned} \tag{2.99}$$

where ε_0 is the permittivity and μ_0 the permeability of the vacuum. It's here useful to introduce the scalar, ϕ, and vectorial potential, $\vec{A}$, fields throw $\vec{E}=-\vec{\nabla}\phi-\frac{\partial\vec{A}}{\partial t}$ and $\vec{B}=\vec{\nabla}\times\vec{A}$. They are more fundamental although not so very "physical" (it is not gauge invariant, for example). Nevertheless it helps to simplify the calculations, because in this way we end up with only one scalar and one vectorial second order partial differential equations, being the other two remaining equations trivial identities

$$\begin{aligned} &\vec{\nabla}^2\phi+\tfrac{\partial}{\partial t}(\vec{\nabla}\cdot\vec{A})=-\tfrac{\rho}{\varepsilon_0}, \\ &\vec{\nabla}^2\vec{A}-\vec{\nabla}\cdot(\vec{\nabla}\cdot\vec{A})=\mu_0\varepsilon_0\tfrac{\partial}{\partial t}(\vec{\nabla}\phi+\tfrac{\partial\vec{A}}{\partial t})-\mu_0\vec{J}, \end{aligned} \tag{2.100}$$

From now on we work in free space [33] $\vec{J}=\rho=0[\Rightarrow\phi=0]$. We still have the freedom to fix the gauge. The appropriate gauge is the radiation (Coulomb) gauge $\vec{\nabla}\cdot\vec{A}=0$. As a result we end up with the wave equation [34]

$$\left(\vec{\nabla}^2-\frac{1}{c^2}\frac{\partial^2}{\partial t^2}\right)\vec{A}=\vec{0}. \tag{2.101}$$

An ansatz for the solution of the vector potential can be written as a superposition with polarizations $\alpha=x,y$ and frequencies $\vec{k}$ motivated by the linearity plus a separation on time-space variables

$$\vec{A}(\vec{r},t)=\sum_{k,\alpha}\vec{A}_{k,\alpha}(\vec{r},t)=\sum_{k,\alpha}q_{k,\alpha}(t)\vec{u}_{k,\alpha}(\vec{r}). \tag{2.102}$$

[32] Compactly in covariant form they read $\partial_\mu F^{\mu\nu}=-J^\nu$ and $\partial_\mu\tilde{F}^{\mu\nu}=0$ where $J^\mu=(c\rho,\vec{J})$ is the 4-vector current and $F_{\mu\nu}=\partial_\mu A_\nu-\partial_\nu A_\mu$ the 4-tensor Faraday with $A^\mu=(\phi,c\vec{A})$.

[33] Recall that $\mu_0\varepsilon_0=1/c^2$.

[34] In covariant form it reads $\Box A^\nu=0$.

With such an ansatz, the wave equation decouples in a Helmholtz equation $\vec{\nabla}^2\vec{u}_{k,\alpha}(\vec{r}) = -k^2\vec{u}_{k,\alpha}(\vec{r})$ and a harmonic oscillatory equation $\ddot{q}_{k,\alpha}(t) = -c^2k^2q_{k,\alpha}(t)$. For the spatial solution, it is conventional to define a "box" of volume L^3 in such a way that the normalized solution ($\int_{L^3} d^3\vec{r}\,\vec{u}^*_{k,\alpha}(\vec{r})\vec{u}_{k',\alpha'}(\vec{r}) = \delta_{k,k'}\delta_{\alpha,\alpha'}$) correspond to traveling plane waves

$$\vec{u}_{k,\alpha}(\vec{r}) = \frac{\vec{e}_\alpha}{\sqrt{L^3}}e^{\mathrm{i}\vec{k}\cdot\vec{r}}, \tag{2.103}$$

where $\vec{e}_\alpha$ is the polarization vector. This is so because we have imposed periodic boundary conditions on the walls of the quantization box in order to mimic the behavior of the electromagnetic field in free space (in order to find expressions in the continuum one has to perform the limit $L \to \infty$ appropriately). For the temporal solution, we recall that the corresponding classical Hamiltonian is $H_{k,\alpha} = \frac{1}{2}m\omega_k^2q_{k,\alpha}^2 + \frac{1}{2m}p_{k,\alpha}^2$. The solution is nothing else than a oscillatory movement in the $q_{k,\alpha}(t)$ coordinate. We introduce the conjugate momentum [35], $p_{k,\alpha}(t) = m\dot{q}_{k,\alpha}(t)$. The angular frequency is $\omega_k = c\,k$ while the "mass", which is a free parameter in the Lagrangian formalism, has to be identified with the permittivity ε_0 of the vacuum. Thus one has to solve the coupled system

$$\begin{aligned}\dot{p}_{k,\alpha} &= -\varepsilon_0\omega_k^2q_{k,\alpha},\\ \dot{q}_{k,\alpha} &= \frac{1}{\varepsilon_0}p_{k,\alpha},\end{aligned} \tag{2.104}$$

which decouples with the change of variables [36] $a = \sqrt{\frac{\varepsilon_0\omega}{2\hbar}}(q + \frac{\mathrm{i}p}{\varepsilon_0\omega})$, $a^* = \sqrt{\frac{\varepsilon_0\omega}{2\hbar}}(q - \frac{\mathrm{i}p}{\varepsilon_0\omega})$ to

$$\begin{aligned}\dot{a}_{k,\alpha} &= -\mathrm{i}\omega_k a_{k,\alpha},\\ \dot{a}^*_{k,\alpha} &= \mathrm{i}\omega_k a^*_{k,\alpha},\end{aligned} \tag{2.105}$$

with trivial oscillatory solutions $a_{k,\alpha}(t) = a_{k,\alpha}e^{-\mathrm{i}\omega_k t}$ and $a^*_{k,\alpha}(t) = a^*_{k,\alpha}e^{\mathrm{i}\omega_k t}$. Finally

$$q_{k,\alpha}(t) = \sqrt{\frac{\hbar}{2\varepsilon_0\omega_k}}(a_{k,\alpha}e^{-\mathrm{i}\omega_k t} + a^*_{k,\alpha}e^{\mathrm{i}\omega_k t}). \tag{2.106}$$

Grouping the space and time solution and summing over (k,α) one obtain the electromagnetic waves solution $\vec{A}_{k,\alpha}(\vec{r},t) = f(\vec{k}\cdot\vec{r} \pm \omega_k t)$.

2.A.2 Quantization of the electromagnetic field

If we quantize the solution for the potential vector we can now write it in terms of creation and annihilation operators with bosonic commutation rules $[\hat{a}_{k,\alpha}, \hat{a}^\dagger_{k,\alpha}] = \delta_{k,k'}\delta_{\alpha,\alpha'}$ as

[35] As usual p is the canonical momentum conjugated to x, *i.e.*, $p = \frac{\partial L}{\partial \dot{x}} = m\dot{x}$.

[36] The inverse transformation results in $q = \sqrt{\frac{\hbar}{2\varepsilon_0\omega}}(a^* + a)$ and $p = \mathrm{i}\sqrt{\frac{\varepsilon_0\hbar\omega}{2}}(a^* - a)$.

$$\hat{\vec{A}}(\vec{r},t) = \sum_{k,\alpha}\sqrt{\frac{\hbar}{2\omega_k\varepsilon_0 L^3}}\left(\vec{e}_\alpha \hat{a}_{k,\alpha} e^{\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)} + \vec{e}^{\,*}_\alpha \hat{a}^\dagger_{k,\alpha} e^{-\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)}\right). \qquad (2.107)$$

Quantized electric and magnetic fields can be straightforward recovered via definition of $\vec{A}$. In the Heisenberg picture, the following expressions are obtained

$$\hat{\vec{E}}(\vec{r},t) = -\frac{\partial}{\partial t}\hat{\vec{A}}(\vec{r},t) = \mathrm{i}\sum_{k,\alpha}\sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 L^3}}\left(\vec{e}_\alpha \hat{a}_{k,\alpha} e^{\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)} - \vec{e}^{\,*}_\alpha \hat{a}^\dagger_{k,\alpha} e^{-\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)}\right), \qquad (2.108)$$

where the unitary electric field polarization vector $\vec{e}_\alpha \perp \vec{k}$ because $\vec{\nabla}\cdot\hat{\vec{E}} = 0$ being $\vec{e}^{\,*}_\alpha \cdot \vec{e}_{\alpha'} = \delta_{\alpha,\alpha'}$ and

$$\hat{\vec{B}}(\vec{r},t) = \vec{\nabla}\times\hat{\vec{A}}(\vec{r},t) = \mathrm{i}\sum_{k,\alpha}\sqrt{\frac{\mu_0\hbar\omega_k}{2L^3}}\left(\vec{f}_\alpha \hat{a}_{k,\alpha} e^{\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)} - \vec{f}^{\,*}_\alpha \hat{a}^\dagger_{k,\alpha} e^{-\mathrm{i}(\vec{k}\cdot\vec{r}-\omega_k t)}\right), \qquad (2.109)$$

where the unitary magnetic field polarization vector $\vec{f}_\alpha = \vec{e}_\alpha \times \frac{\vec{k}}{|\vec{k}|} \perp \vec{e}_\alpha, \vec{k}$ fulfills $\vec{f}^{\,*}_\alpha \cdot \vec{f}_{\alpha'} = \delta_{\alpha,\alpha'}$.

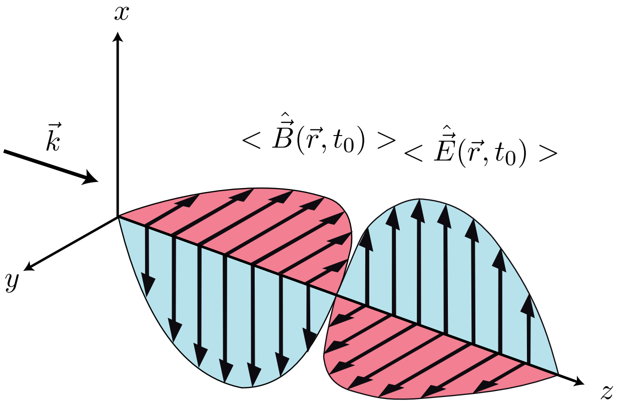
x
$\vec{k}$
$< \hat{\vec{B}}(\vec{r},t_0) >$
$< \hat{\vec{E}}(\vec{r},t_0) >$
y
z

Figure 2.3: Electric, magnetic and wave vectors of an electromagnetic traveling plane wave at a fixed time t_0.

One can compute the Hamiltonian for a single mode

$$\hat{H}_{k,\alpha} = \frac{1}{2}\int_{L^3} d^3\vec{r}\left(\varepsilon_0|\hat{\vec{E}}_{k,\alpha}|^2 + \frac{1}{\mu_0}|\hat{\vec{B}}_{k,\alpha}|^2\right) = \frac{\hbar\omega_k}{2}\left(\hat{a}^\dagger_{k,\alpha}\hat{a}_{k,\alpha} + \hat{a}_{k,\alpha}\hat{a}^\dagger_{k,\alpha}\right), \qquad (2.110)$$

then the total Hamiltonian reads

$$\hat{H}_{EM} = \frac{1}{2}\int_{L^3} d^3\vec{r}\left(\varepsilon_0|\hat{\vec{E}}|^2 + \frac{1}{\mu_0}|\hat{\vec{B}}|^2\right) = \sum_{k,\alpha}\hbar\omega_k\left(\hat{a}^\dagger_{k,\alpha}\hat{a}_{k,\alpha} + \frac{1}{2}\right). \qquad (2.111)$$

It is in this moment when one can, by comparing the above Hamiltonian with the one of the quantized harmonic oscillator

$$\hat{H}_{HO} = \sum_{k,\alpha} \hbar\omega_k \left(\hat{a}^\dagger_{k,\alpha}\hat{a}_{k,\alpha} + \frac{1}{2} \right), \tag{2.112}$$

associate each mode of the electromagnetic field to an independent harmonic oscillator with the same frequency.

2.A.3 Quadratures of the electromagnetic field

To end with the comparison between the light and the harmonic oscillator we present here -in analogy to the position-momentum coordinates of the massive particle in the harmonic oscillator- the amplitude-phase quadratures of light modes. Q-quadrature (amplitude quadrature):

$$\hat{Q}_{k,\alpha} = \frac{\hat{a}^\dagger_{k,\alpha} + \hat{a}_{k,\alpha}}{\sqrt{2}}, \tag{2.113}$$

P-quadrature (phase quadrature):

$$\hat{P}_{k,\alpha} = \mathrm{i}\frac{(\hat{a}^\dagger_{k,\alpha} - \hat{a}_{k,\alpha})}{\sqrt{2}}, \tag{2.114}$$

with bossonic commutation rules

$$[\hat{Q}_{k,\alpha}, \hat{P}_{k',\alpha'}] = \mathrm{i}\delta_{k,k'}\delta_{\alpha,\alpha'}, \tag{2.115}$$

and Heisenberg uncertainty principle

$$\Delta Q \Delta P \geq \frac{1}{2}| < [\hat{Q}, \hat{P}] > | = \frac{1}{2}. \tag{2.116}$$

In terms of the quadratures the Hamiltonian reads

$$\hat{H}_{EM} = \hat{H}_{HO} = \sum_{k,\alpha} \frac{\hbar\omega_k}{2} \left(\hat{Q}^2_{k,\alpha} + \hat{P}^2_{k,\alpha} \right), \tag{2.117}$$

while the electric field [37]

$$|\hat{\vec{E}}(\vec{r},t)| = \sum_{k,\alpha} \sqrt{\frac{\hbar\omega_k}{\varepsilon_0 L^3}} \left(\hat{Q}_{k,\alpha} \sin(\omega_k t - \vec{k}\cdot\vec{r}) - \hat{P}_{k,\alpha} \cos(\omega_k t - \vec{k}\cdot\vec{r}) \right). \tag{2.118}$$

The uncertainty principle is encoded between the non-commuting observables potential field $\hat{\vec{A}}$ and electric $\hat{\vec{E}}$ (or magnetic field $\hat{\vec{B}}$). Quadrature operators are nothing

[37] The classical values for the fields correspond to the expectation values for the quantum fields.

else than observables proportionals to $\hat{\vec{A}}$ and $\hat{\vec{E}}$ at the same time, and so they contain the same information about the light. But in an harmonic oscillator the position and momentum are always one quarter cycle out of phase, therefore the amplitude of the electric field "now" and a quarter cycle later effectively describe both the electric and potential field.

2.A.4 Quantum states of the electromagnetic field

We have seen that the Hamiltonian can be written as an harmonic oscillator for each mode, thus the eigenstates of the Hamiltonian are Fock states, which turn out to be a very suitable basis to express generic quantum states of light. In section 2.5.1 we have described many examples of Gaussian states at the phase-space level. Here the aim is to describe them by looking at the expectation value of the time dependent electric field as well as its fluctuations. To this aim, we compute and plot (see Fig. 2.4), explicitly the expectation value of the electric field. In general

$$< |\hat{\vec{E}}(\vec{r},t)| > \sim < \hat{Q} > \sin(\omega t - \vec{k}\cdot\vec{r}) - < \hat{P} > \cos(\omega t - \vec{k}\cdot\vec{r}), \tag{2.119}$$

and its corresponding uncertainty (fluctuations)

$$\begin{aligned}(\Delta E(\vec{r},t))^2 \sim (\Delta Q)^2 \sin^2(\omega t - \vec{k}\cdot\vec{r}) + (\Delta P)^2 \cos^2(\omega t - \vec{k}\cdot\vec{r}) - \\ - V(\hat{Q},\hat{P}) \sin(\omega t - \vec{k}\cdot\vec{r}) \cos(\omega t - \vec{k}\cdot\vec{r}),\end{aligned} \tag{2.120}$$

where $V(\hat{Q},\hat{P}) =< \{\hat{Q},\hat{P}\} > -2 < \hat{Q} >< \hat{P} >$. We list here the most relevant states of the electromagnetic field. Among them, Gaussian states produced in the lab with coherent laser light and linear optical devices. We write them in the Fock basis as it is a very convenient basis for all calculations needed (see Tabs. 2.121 and 2.122 for detailed calculations).

- *Vacuum state*, $|0\rangle$, is the only Gaussian state of all Fock states. It can be defined as the ground state of the harmonic oscillator.

  $< |\hat{\vec{E}}(\vec{r},t)| >= 0,$

  $\Delta E(\vec{r},t) \sim \sqrt{\frac{1}{2}}.$

- *Fock states* [38], $|n\rangle$, are eigenstates of the number operator, and thus, so of the energy because $\hat{H}|n\rangle = E_n|n\rangle$. They are non-Gaussian and can be written as the n-th excitation (photon) from the vacuum, $|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle$ via the ladder operators that act on them raising and lowering the number of photons presents in the state $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$, $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$.

  $< |\hat{\vec{E}}(\vec{r},t)| >= 0,$

  $\Delta E(\vec{r},t) \sim \sqrt{n + \frac{1}{2}}.$

[38] Complete orthonormal set basis $\langle n|m\rangle = \delta_{n,m}$.

- *Fock superpositions*, $|\psi\rangle = \sum_i \psi_i |n_i\rangle$ are non-Gaussians. The simplest one, is $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with balanced amplitudes.

  $< |\hat{\vec{E}}(\vec{r},t)| > \sim \sqrt{\frac{1}{2}} \sin(\omega t - \vec{k}\cdot\vec{r}),$

  $\Delta E(\vec{r},t) \sim \sqrt{\frac{1}{2}\sin^2(\omega t - \vec{k}\cdot\vec{r}) + \cos^2(\omega t - \vec{k}\cdot\vec{r})}.$

- *Coherent states*, $|\alpha\rangle$, are defined as the eigenstates of the annihilation operator $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ or as $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$. Coherent state have not a well defined the number of photons ($\hat{n} = \hat{a}^\dagger \hat{a}$) because $\langle \hat{n} \rangle_\alpha = |\alpha|^2$ and $(\Delta n)_\alpha = |\alpha|$, nevertheless, as α increases the relative indetermination $\frac{(\Delta n)_\alpha}{\langle \hat{n} \rangle_\alpha} = |\alpha|^{-1}$ tends to zero. Coherent state have equal variance and mean, therefore, its photon distribution is Poissonian. It is immediate to see that if one computes the probability to find n photons in a coherent state *i.e.* $P_n = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}}{n!} \mathrm{e}^{-|\alpha|^2}$ which is clearly a Poissonian distribution with mean and variance $|\alpha|^2$.

  $< |\hat{\vec{E}}(\vec{r},t)| > \sim \sqrt{2}\mathrm{Re}(\alpha) \sin(\omega t - \vec{k}\cdot\vec{r}) - \sqrt{2}\mathrm{Im}(\alpha) \cos(\omega t - \vec{k}\cdot\vec{r}),$

  $\Delta E(\vec{r},t) \sim \sqrt{\frac{1}{2}}.$

- *Squeezed states*, $|r\rangle$, are minimal uncertainty states with arbitrary small uncertainty in one quadrature while increased uncertainty in the orthogonal one. Squeezed states of the light fields are used to enhance precision measurements. They read in Fock basis as $|r\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} (-\frac{1}{2}\tanh r)^n \frac{\sqrt{(2n)!}}{n!} |2n\rangle$.

  $< |\hat{\vec{E}}(\vec{r},t)| >= 0,$

  $\Delta E(\vec{r},t) \sim \sqrt{\frac{1}{2}\mathrm{e}^{-2r}\sin^2(\omega t - \vec{k}\cdot\vec{r}) + \frac{1}{2}\mathrm{e}^{2r}\cos^2(\omega t - \vec{k}\cdot\vec{r})}.$

- *Thermal states*, $\hat{\rho}_\beta$, are a superposition of all Fock states occupied with a probability $P_n = (1 - \mathrm{e}^{-\beta\hbar\omega})\mathrm{e}^{-\beta\hbar\omega n}$. It's the quantum distribution function which describes the thermal state statistics of the blackbody radiation. At the Fock level they read as $\hat{\rho}_\beta = (1 - \mathrm{e}^{-\beta\hbar\omega}) \sum_{n=0}^{\infty} \mathrm{e}^{-\beta\hbar\omega n} |n\rangle\langle n|$.

  $< |\hat{\vec{E}}(\vec{r},t)| >= 0,$

  $\Delta E(\vec{r},t) \sim \sqrt{M + \frac{1}{2}}.$

We can summarize the above results in the following tables:

	$<\hat{Q}>$	$<\hat{P}>$	ΔQ	ΔP	$<\hat{H}>$	$\Delta Q \Delta P \geq \frac{1}{2}$
$\|0\rangle$	0	0	$\sqrt{1/2}$	$\sqrt{1/2}$	$\frac{\hbar\omega}{2}$	1/2
$\|n\rangle$	0	0	$\sqrt{n+1/2}$	$\sqrt{n+1/2}$	$\frac{\hbar\omega}{2}(1+2n)$	n + 1/2
$\|\psi\rangle$	$\sqrt{1/2}$	0	$\sqrt{1/2}$	1	$\hbar\omega$	$\sqrt{1/2}$
$\|\alpha\rangle$	$\sqrt{2}\,\mathrm{Re}(\alpha)$	$\sqrt{2}\,\mathrm{Im}(\alpha)$	$\sqrt{1/2}$	$\sqrt{1/2}$	$\frac{\hbar\omega}{2}(1+2\|\alpha\|^2)$	1/2
$\|r\rangle$	0	0	$\sqrt{\frac{\mathrm{e}^{-2r}}{2}}$	$\sqrt{\frac{\mathrm{e}^{2r}}{2}}$	$\frac{\hbar\omega}{2}\cosh 2r$	1/2
$\hat{\rho}_\beta$	0	0	$\sqrt{M+1/2}$	$\sqrt{M+1/2}$	$\frac{\hbar\omega}{2}(1+2M)$	$M+1/2$

(2.121)

	$<\hat{Q}^2>$	$<\hat{P}^2>$	$<\hat{Q}\hat{P}>$	$<\hat{P}\hat{Q}>$	$V(\hat{Q},\hat{P})$
$\|0\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{\mathrm{i}}{2}$	$-\frac{\mathrm{i}}{2}$	0
$\|n\rangle$	$n+\frac{1}{2}$	$n+\frac{1}{2}$	$\frac{\mathrm{i}}{2}$	$-\frac{\mathrm{i}}{2}$	0
$\|\psi\rangle$	1	1	$\frac{\mathrm{i}}{2}$	$-\frac{\mathrm{i}}{2}$	0
$\|\alpha\rangle$	$\frac{1}{2}(1+2\|\alpha\|^2+\alpha^2+\alpha^{*2})$	$\frac{1}{2}(1+2\|\alpha\|^2-\alpha^2-\alpha^{*2})$	$\frac{\mathrm{i}}{2}(1-\alpha^2+\alpha^{*2})$	$\frac{\mathrm{i}}{2}(-1-\alpha^2+\alpha^{*2})$	0
$\|r\rangle$	$\frac{\mathrm{e}^{-2r}}{2}$	$\frac{\mathrm{e}^{2r}}{2}$	$\frac{\mathrm{i}}{2}$	$-\frac{\mathrm{i}}{2}$	0
$\hat{\rho}_\beta$	$M+\frac{1}{2}$	$M+\frac{1}{2}$	$\frac{\mathrm{i}}{2}$	$-\frac{\mathrm{i}}{2}$	0

(2.122)

Recalling section 2.5.1, on one hand the expectation values of the two quadratures are encoded in the displacement vector which gives the center of the diagrams in the phase-space. On the other, the two uncertainties are encoded in the diagonal terms of the covariance matrix and express the width of the phase-space points. The off diagonal terms (symmetrics) contain the information of the Q-P correlations. We observe then, that the components of the displacement vector are closely related with the amplitude of the electric field while the covariance matrix contains the fluctuations of the electric field. Notice the correspondence $V(\hat{Q},\hat{P}) = \gamma_{12}$. This important term amounts for the correlations in fluctuations and is zero for all minimum uncertainty states.

Analyzing the plots we see two important behaviors. First, as a general feature a superposition of eigenstates of the energy (Fock states) produces a t-dependence in any observable, as one sees in the electric field which oscillates in time. Second, coherent states are the states of an harmonic oscillator system which mimic in the best possible way the classical motion of a particle in a quadratic potential, in this sense, they are the most classical states of light that one can produce. As seen in the plot the expectation value of the electric field oscillates classically while the uncertainty is minimum and coherent with the field.

2.B Appendix: Wigner integrals

As it has been shown the Wigner distribution function is Gaussian whenever the state is Gaussian, with straightforward calculations on can deduce two extremely useful Gaussian integrals

$$\int e^{-\zeta^T\cdot A\cdot\zeta} d^{2N}\zeta = \frac{\pi^N}{\sqrt{\det A}}, \tag{2.123}$$

$$\int e^{-\zeta^T\cdot A\cdot\zeta - b^T\cdot\zeta} d^{2N}\zeta = \frac{\pi^N}{\sqrt{\det A}} e^{b^T\cdot\frac{1}{4A}\cdot b}. \tag{2.124}$$

In the case we are dealing with non-Gaussian states the Wigner distribution function is not any more Gaussian and one is forced to perform non-Gaussian integrals. We give here some very useful formulas that convert the problem of integrating non-Gaussian functions into a derivative problem

$$\begin{aligned}&\int \zeta_i^{m_i}\zeta_j^{m_j}\zeta_k^{m_k}\cdots e^{-\zeta^T\cdot A\cdot\zeta} d^{2N}\zeta = \\ &= (-1)^{m_i+m_j+m_k+\cdots}\frac{\pi^N}{\sqrt{\det A}}\frac{\partial^{m_i}}{\partial b_i^{m_i}}\frac{\partial^{m_j}}{\partial b_j^{m_j}}\frac{\partial^{m_k}}{\partial b_k^{m_k}}\cdots e^{b^T\cdot\frac{1}{4A}\cdot b}\Bigg|_{b_i=0,b_j=0,b_k=0,\ldots},\end{aligned} \tag{2.125}$$

$$\begin{aligned}&\int \zeta_i^{m_i}\zeta_j^{m_j}\zeta_k^{m_k}\cdots e^{-\zeta^T\cdot A\cdot\zeta - c^T\cdot\zeta} d^{2N}\zeta = \\ &= (-1)^{m_i+m_j+m_k+\cdots}\frac{\pi^N}{\sqrt{\det A}}\frac{\partial^{m_i}}{\partial b_i^{m_i}}\frac{\partial^{m_j}}{\partial b_j^{m_j}}\frac{\partial^{m_k}}{\partial b_k^{m_k}}\cdots e^{(b+c)^T\cdot\frac{1}{4A}\cdot(b+c)}\Bigg|_{b_i=0,b_j=0,b_k=0,\ldots}.\end{aligned} \tag{2.126}$$

Extra useful integrals are

$$\int \mathcal{W}(\zeta) d^{2N}\zeta = 1, \tag{2.127}$$

$$\int (\mathcal{W}(\zeta))^2 d^{2N}\zeta = \frac{1}{(2\pi)^N\sqrt{\det\gamma}}, \tag{2.128}$$

$$\int \chi(\eta) d^{2N}\eta = \frac{(4\pi)^N}{\sqrt{\det\gamma}} e^{-d^T\frac{1}{\gamma}d}, \tag{2.129}$$

$$\int (\chi(\eta))^2 d^{2N}\eta = \frac{(2\pi)^N}{\sqrt{\det\gamma}} e^{-d^T\frac{4}{\gamma}d}, \tag{2.130}$$

$$\int |\chi(\eta)|^2 d^{2N}\eta = \frac{(2\pi)^N}{\sqrt{\det\gamma}}. \tag{2.131}$$

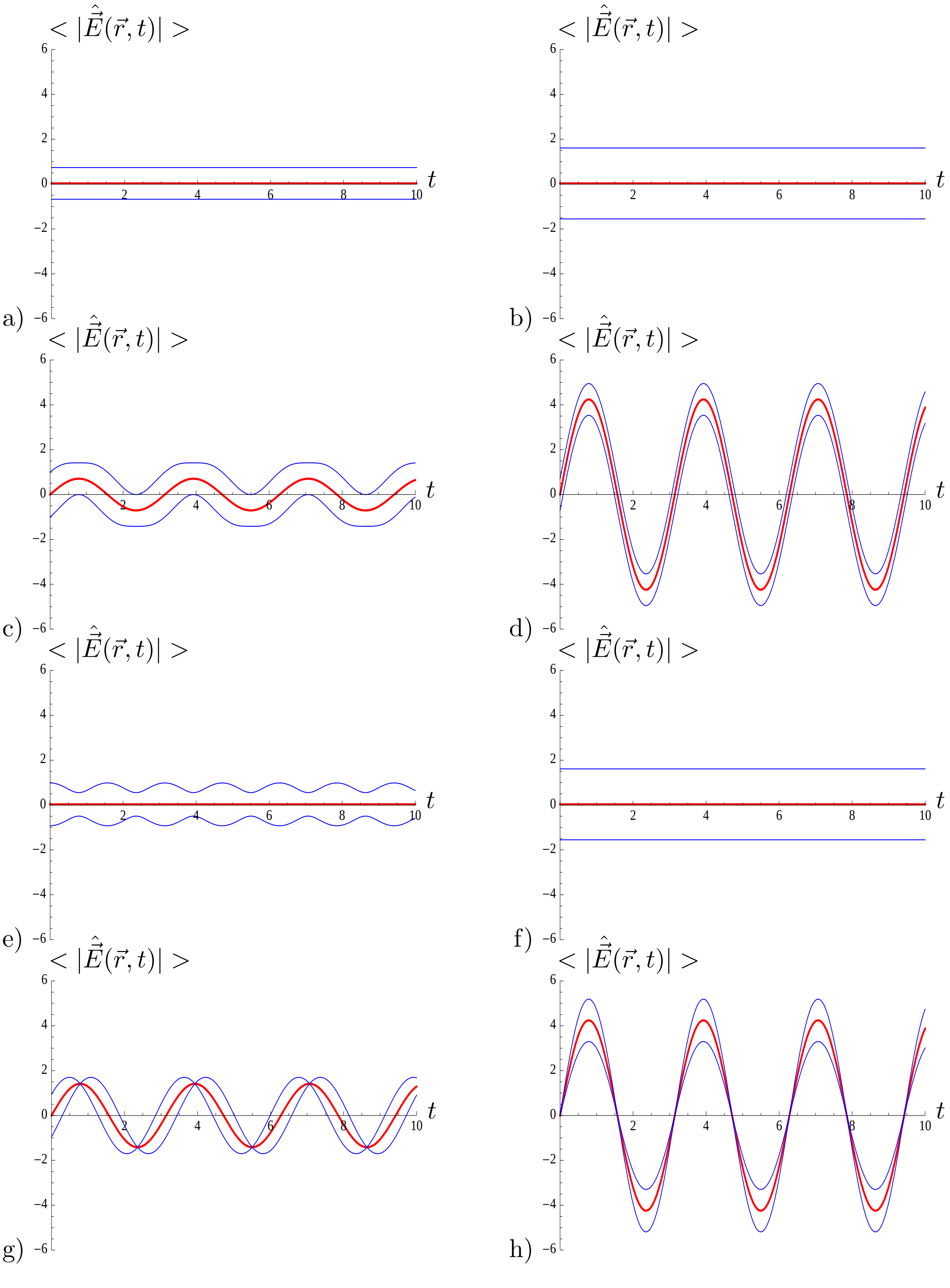

Figure 2.4: In red the average electric field, in blue the associated uncertainty. a) Vacuum, b) Fock, c) Superposition, d) Coherent, e) Squeezed, f) Thermal, g) Coherent squeezed in position (amplitude), h) Coherent squeezed in momentum (phase).

Chapter 3

Quantum Cryptography protocols with Continuous Variable

Cryptography refers to strategies which permit the secure communication between two distant parties (traditionally denoted by Alice and Bob) that wish to communicate secretly. So its purpose is to design new communication algorithms being sure that secrecy is preserved. In Classical Cryptography there is only one cryptographic protocol, known as the ideal Vernam cypher method, which is absolutely secure. The Vernam cypher consists of a *random* secret key (private key), shared between the sender (Alice) and the receiver (Bob), used to encode and decode messages with absolute security. However, this method suffers from two drawbacks. First, if Alice wants to communicate N bits to Bob, they will need to share in advance a key with at least N bits. Second, this key can only be used once to make the method unbreakable. This implies that, the key must originally be exchanged by hand before the communication to keep secrecy and it is essential that the key is totally random and secret. This problem is known as key distribution.

To solve the problem of a private key distribution, classical strategies exist to distribute keys between them albeit being this distribution only partially secure. For example, by designing algorithms which permit distribution of private keys in a "practical secure" way. In such algorithms, security relies on the difficulty to invert some mathematical operations. Since the time needed to break the security of these algorithms to obtain the key is long, then practical security is achievable.

The second problem, the necessity of a new key for each message, is also solved using Public Key Cryptosystems. They work as follows: assume that Alice and Bob possess, in advance, a common secret key. This secret key must be exchanged by hand once, and it has to be random and secure. Using this secret key, Alice and Bob can distribute among them, several private keys. Then, they could use as many distributed private key as necessary to encrypt/decrypt messages through *e.g.* the Vernam cypher method. In other words, any time Alice wants to communicate with

Bob, she only needs to use her secret key to distribute as many private keys as needed to encrypt later on messages. This distribution works as follows, Alice makes one key publicly available, referred as the public key that encodes a private key. From this public key any receiver could in principle extract the private key. But only Bob (the receiver in possession of the secret key) can extract it in an efficient way. Any receiver without the secret key needs to decrypt a problem with NP complexity. This way of distributing private keys can be done even when the secret key's length is much smaller than the private keys needed for the Vernam cypher encryption and even if the secret key is used many times, solving both issues.

In this chapter we have studied the possibility of using Continuous Variable to perform quantum cryptography protocols by means of bipartite entanglement. Like in any practical implementation of a protocol, efficiency is an important issue since resources are not unlimited, thus a special attention will be devoted to the efficient implementation of the protocol. Before explaining how secure cryptography with Continuous Variable can be realized, let us introduce the basic concepts in both classical and quantum scenario.

3.1 Classical Cryptography

3.1.1 Vernam cypher

The best and most well known classical private key (or one-time-pad) cryptosystem is the so-called Vernam cypher. To achieve absolute security, the Vernam cypher requires the prior distribution of a random classical private key, denoted as k. The basic steps of the protocol are the followings:

Encoding: if Alice wants to encode a message m with the key k, she performs the following operation between the message and the key, and sends the encoded message e to Bob

$$\mathrm{Enc}_k(m) = m \oplus k = e. \tag{3.1}$$

Decoding: only Bob, who has also the key, can decode the message (invert the operation) because the key Alice has used is random. Thus, he only needs to use the key again to the encoded message e in order to retrieve the original message m

$$\mathrm{Dec}_k(e) = \mathrm{Dec}_k[\mathrm{Enc}_k(m)] = e \oplus k = d = m. \tag{3.2}$$

Let us illustrate Vernam cypher with an specific example. Alice wants to communicate to Bob, in a secure way, a message m (in a binary string) of *e.g.* 9 bits. They share the key k of the same size as the message (9 bits). Alice encodes her message by applying a XOR (exclusive OR) [1] operation between the message m and the key k.

In the next table we summarize the XOR operation

[1] Also known as AND or $\oplus$ mod (2).

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \tag{3.3}$$

As a result Alice has the encoded message e, that will send to Bob in a public way.

message	$m = 010011101$
key	$k = 110100011$
encoded message	$e = 1000111110$

Then Bob wants to readout the message, and thus, performs the inverse operation (which is again a XOR) between the encoded message e and the key k.

As a result Bob has the decoded message d that coincides with the message Alice wanted to communicate to him.

encoded message	$e = 1000111110$
key	$k = 110100011$
decoded message	$d = 010011101$

3.1.2 Public key distribution: The RSA algorithm

Thus far, Classical Cryptography has not a solution for the distribution of the private key needed to perform Vernam cypher encryption. Such distribution can, however be done in a public and practical secure way with the RSA algorithm. The RSA cryptography algorithm proposed in 1977 by *R*ivest, *S*hamir, and *A*dleman from the MIT is the most commonly used algorithm of a public key. It is widely used in bank's security, electronic commerce and internet, relying on the fact that to decrypt this algorithm one needs to solve the factorization problem which is an NP problem. Even now, there is no efficient classical algorithm known to solve the factorization problem. This means that even though computational resources increase constantly, one simply needs to exploit the NP character of the algorithm to make the solution harder to find. Let us illustrate how it works with the following example.

i) The sender, Alice, chooses two "big" different prime numbers, say $p = 61$ and $q = 53$, she computes its product $n = p\,q = 3233$ and also the following quantity $\phi = (p-1)(q-1) = 3120$.

ii) She chooses a positive integer l smaller and coprime with ϕ, in the example above $l = 17$.

iii) As a secret key, Alice gives to Bob the number k such that $k\,l = 1 \bmod (\phi)$, take for example $k = 2753$. Alice makes public l and n, this is what is called a public key.

iv) With the public key (l and n) anyone can encrypt a message m and send it to Bob, but only Bob, who is in possession of the secret key k, is able to decrypt the message. This method can thus be used to perform Classical Key Distribution. Any time Alice wants to communicate with Bob, she sends a private key encrypted with l and n and only Bob will be able to retrieve it. Once Bob has the private key, Alice can send messages to Bob via the Vernam cypher using this key.

v) Encryption proceeds as follows. Alice wants to distribute a key encoded in a message $m = 123$. She uses the public key and computes the encryption $\mathrm{Enc}_{l,n}(m) = m^l \bmod (n) = e = 855$.

vi) Bob now wants to decrypt the message e to extract a private key, so he calculates $\mathrm{Dec}_{k,n}(e) = \mathrm{Dec}_{k,n}[\mathrm{Enc}_{l,n}(m)] = e^k \bmod (n) = d = m = 123$. Bob is the only one in possession of the secret key k and so the only one that can decrypt the message e to find the private key Alice is going to use with the Vernam cypher to communicate securely with him.

The private key Alice and Bob share can be used more than once to distribute secure keys. In such way, to use the Vernam cypher, one no longer needs to share a long private key because we can distribute many of them in a secure way. Security relies in the fact that, from the encrypted message e, and the public keys l and n it is very difficult to find the private key k (and so m) or the original two prime numbers q and p, even in the case we are reusing the key k. This is because factorization is a NP problem, whose efficient classical solution is not known yet. Security in the RSA algorithm relies on the fact that independently of the computer used, if it is classical, the problem is NP and thus hard to solve.

3.2 The quantum solution to the distribution of the key

The "Quantum Computer" arises here first as a menace for Classical Key Distribution methods and then as the solution for the security in Cryptography. Based on the quantum nature of the microscopic world, such "computers", still in a theoretical stage, are known to be able to solve some hard mathematical problems rapidly. In 1994 Peter Shor proposed a quantum protocol to solve the factorization problem in an efficient way, known as the Shor's algorithm. If such a computer can be realized, current cryptographic protocols will not be anymore secure. Can Quantum Mechanics then offer a solution for a secure Cryptography method? The answer is yes. Since the end of the 80s protocols relying on Quantum Mechanics exists permitting to perform Quantum Cryptography in an unconditional secure way.

At present, Quantum Cryptography is the most important real implementation of Quantum Information. It offers an absolute secure distribution of random keys which combined with the Vernam cypher guarantees completely secure Cryptography. Thus, the Quantum Cryptography problem is in fact the problem of distributing, between two distant parties, a secure random key relying on the laws of Quantum

Mechanics, *i.e.* the Quantum Key Distribution (QKD) problem. If the key is securely distributed, the algorithms used to encode and decode any message can be made public without compromising security. The key consists typically in a random sequence of bits which both, Alice and Bob, share as a string of classically correlated data. The superiority of Quantum Cryptography comes from the fact that the laws of Quantum Mechanics permit to the legitimate users (Alice and Bob) to infer if an eavesdropper has monitored the distribution of the key and has gained information about it. If this is the case, Alice and Bob will both agree in withdrawing the key and will start the distribution of a new one. In contrast, Classical Key Distribution, no matter how difficult the distribution from a technological point of view is, can always be intercepted by an eavesdropper without Alice and Bob realizing it.

In Quantum Cryptography two seemingly independent main schemes exist for QKD. The first one, denoted as "Prepare and Measure" scheme, originally proposed by C.H. Bennett and G. Brassard in 1988 and known as BB84 [24], does not use entangled states shared between Alice and Bob. The key is established by sending non-orthogonal quantum states between the parties and communicating classically the result of some measurements. Security is guaranteed by the quantum nature of the measurements which avoids each party measuring simultaneously non-commuting observables. The second scheme ("Entanglement based"), uses as a resource shared entanglement, like the one originally proposed by A. Ekert in 1991 known as Ekert91 [25]. Here entanglement is explicitly distributed and the security is guaranteed by the nature of quantum correlations and proved by Bell inequalities. However, the two schemes have been shown to be completely equivalent [26], and specifically entanglement stands as a precondition for any secure key distribution [27]. Let us briefly detail these two schemes.

3.2.1 "Prepare and Measure" scheme

Like in any cryptographic protocol, there is always an eavesdropper. The protocol does not avoid an eavesdropper from intercepting the key, but it permits Alice and Bob know if the key has been intercepted, and so that it can be discarded. We sketch here the steps of the BB84 protocol.

i) Alice prepares a secret sequence of random bits and encodes them in the state of a 2-level system *e.g.* a spin-1/2 system by choosing randomly between two bases (Z and X). Alice encodes 0/1 in $|\pm\rangle$ ($|\pm\rangle_x$) according to basis Z (basis X). Then, she sends Bob the states she has prepared. For example:

Alice random bits	0	1	1	0	0	1	1	0	0
Alice random bases	Z	X	X	X	Z	X	Z	X	X
Alice prepared states	$\|+\rangle$	$\|-\rangle_x$	$\|-\rangle_x$	$\|+\rangle_x$	$\|+\rangle$	$\|-\rangle_x$	$\|-\rangle$	$\|+\rangle_x$	$\|+\rangle_x$

ii) Bob receives the states without knowing on which basis have been prepared and measures in another random choice of bases. The outcome of the measurements is going to be retained as the bits received while the state collapses in a certain eigenstate.

Alice prepared states	$\vert+\rangle$	$\vert-\rangle_x$	$\vert-\rangle_x$	$\vert+\rangle_x$	$\vert+\rangle$	$\vert-\rangle_x$	$\vert-\rangle$	$\vert+\rangle_x$	$\vert+\rangle_x$
Bob random bases	X	Z	X	X	X	X	X	X	X
Bob received states	$\vert+\rangle_x$	$\vert+\rangle$	$\vert-\rangle_x$	$\vert+\rangle_x$	$\vert+\rangle_x$	$\vert-\rangle_x$	$\vert-\rangle_x$	$\vert+\rangle_x$	$\vert+\rangle_x$
Bob received bits	0	0	1	0	0	1	1	0	0

iii) Bob communicates to Alice his choice of bases in a public way.

iv) Alice identifies the set of bits for which they have both performed the measurement in the same basis, *i.e.* outcomes 3, 4, 6, 8 and 9 in the above example. Alice and Bob discard the set of data in which they did not agree (the rest).

v) Bob sends part of his data (received bits) to Alice by a public channel. Alice checks the correlation between the data and establishes an error rate. The error rate can come from an eavesdropper or noise effects.

vi) If the error rate is too high they can assume that an eavesdropper has act and they can restart the protocol from the beginning. One can show that, in the case of free noise effect, and under individual attacks (the eavesdropper intercepts, measures, and resents the states) the error rate is bounded to be (for a sufficiently high amount of data) 25%. If Alice deduces that there is not an eavesdropper present, she communicates it to Bob. Alice and Bob use the set of remaining data as a private key. Later on, they can improve security by performing information reconciliation and privacy amplification on the private key before using it to encrypt messages with the Vernam cypher.

Note that the security of the protocol relies in the quantum nature of the measurements. The two bases, Z and X, are associated with eigenbasis of non-commuting observables, $\hat{\sigma}_z$ and $\hat{\sigma}_x$. The eavesdropper cannot measure simultaneously both observables on the same state. Additionally the nocloning theorem prevents her from being able to distinguish with certainty between non-orthogonal quantum state performing cloning, and avoids hence the possibility of resending them to Bob without leaving trace of her intrusion.

3.2.2 "Entanglement based" scheme

A second type of protocols demand as a fundamental resource, shared entanglement between Alice and Bob, like Ekert91. In the same way as in BB84, these protocols permit a secure distribution of a secret key. This can be done as far as the protocol ensures if there has been an interception of the key. We sketch below the steps of this well-known protocol.

i) The first step consists on distributing (along the z-direction) singlet states of a spin-1/2 system between Alice and Bob. Thus Alice and Bob share many copies of a Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$.

ii) Alice and Bob are going to measure in the $x-y$ plane in one of the three directions given by unit vectors $\vec{A}_i = (\cos\phi_i^A, \sin\phi_i^A)$ and $\vec{B}_j = (\cos\phi_j^B, \sin\phi_j^B)$ respectively, where the azimuthal angles are fixed to $\phi_i^A = (0, \pi/4, \pi/2)_i$ and to $\phi_j^B = (\pi/4, \pi/2, 3\pi/4)_j$. Each time they will choose the basis randomly and independently for each pair of incoming particles.

iii) After the measurement has taken place, Alice and Bob can announce in public the directions they have chosen for each measurements and divide them into two separated groups. A first group for which they coincide and a second group for which they do not. The second group of outcomes is made public and it is used to establish the presence or absence of an eavesdropper.

iv) One defines correlation coefficients to test security

$$\mathcal{E}(\vec{A}_i, \vec{B}_j) = \mathcal{P}_{++}(\vec{A}_i, \vec{B}_j) + \mathcal{P}_{--}(\vec{A}_i, \vec{B}_j) - \mathcal{P}_{+-}(\vec{A}_i, \vec{B}_j) - \mathcal{P}_{-+}(\vec{A}_i, \vec{B}_j) \quad (3.4)$$

which is the correlation coefficient of the measurements performed by Alice along $\vec{A}_i$ and by Bob along $\vec{B}_j$. Here $\mathcal{P}_{\pm\pm}(\vec{A}_i, \vec{B}_j)$ denotes the probability the results ±1 has been obtained along $\vec{A}_i$ and ±1 along $\vec{B}_j$. Straightforward calculations give rise to

$\mathcal{P}_{++}(\vec{A}_i, \vec{B}_j) = \frac{1}{2}\sin^2(\phi_i^A - \phi_j^B)$,

$\mathcal{P}_{--}(\vec{A}_i, \vec{B}_j) = \frac{1}{2}\sin^2(\phi_i^A - \phi_j^B)$,

$\mathcal{P}_{+-}(\vec{A}_i, \vec{B}_j) = \frac{1}{2}\cos^2(\phi_i^A - \phi_j^B)$,

$\mathcal{P}_{-+}(\vec{A}_i, \vec{B}_j) = \frac{1}{2}\cos^2(\phi_i^A - \phi_j^B)$.

Thus, according to the Quantum rules $\mathcal{E}(\vec{A}_i, \vec{B}_j) = -\vec{A}_i\vec{B}_j = -\cos\left[2(\phi_i^A - \phi_j^B)\right]$. As expected, if they choose the same orientation, Quantum Mechanics predicts a total anticorrelation in the outcomes $\mathcal{E}(\vec{A}_i, \vec{B}_j) = -1$ as it should be for the rotational invariant singlet state $|\Psi^-\rangle$.

Finally, let us define here a quantity composed of those correlation coefficients for which Alice and Bob have measured in different directions,

$$\mathcal{S} = |\mathcal{E}(\vec{A}_1, \vec{B}_1) + \mathcal{E}(\vec{A}_3, \vec{B}_3) - \mathcal{E}(\vec{A}_1, \vec{B}_3) + \mathcal{E}(\vec{A}_3, \vec{B}_1)|. \quad (3.5)$$

Again, Quantum Mechanics requires, $\mathcal{S} = 2\sqrt{2} > 2$.

v) The CHSH (Clauser, Horne, Shimony, and Holt) inequality, is a generalization of Bell inequalities and asserts that $\mathcal{S} \leq 2$ for any theory compatible with local realism. But Quantum Mechanics, and in particular with Bell states CHSH inequalities are violated. If this is the case, *i.e.* the value of $\mathcal{S}$ that they find is exactly $2\sqrt{2}$, they know that their states have not been disturbed and so the first group of outcomes, that are random, are totally anticorrelated and can be converted into a secret string of bits (provided Bob flips all the bits). This ends the distribution of the private key. One can now, as in the BB84 protocol, perform information reconciliation and privacy amplification on the private key before using it to encrypt messages with Vernam cypher to achieve an absolute secure communication.

Note that security relies in the quantum correlations *i.e.* entanglement and it is guaranteed by the violation of Bell inequalities. In contrast to BB84, Alice do not need in advance a string of random bits because the randomness comes from the measurement process.

3.3 Quantum Key Distribution with Continuous Variable Gaussian states

Quantum Cryptography can be implemented using systems of Continuous Variable *i.e.* using quantum states on infinite dimensional Hilbert spaces. Among all Continuous Variable states, Gaussian states and Gaussian operations, have been the preferred to experimentally implement Quantum Cryptography using "Prepare and Measure" schemes *e.g.* with either squeezed or coherent states [28, 29, 30]. Those schemes do not demand entanglement between the parties. Here we address the problem of the Quantum Key Distribution with entangled Continuous Variable using an "Entanglement based" protocol.

Notice that if Alice and Bob share a collection of distillable entangled states, they can always obtain a smaller number of maximally entangled states from which they can establish a secure key [31] using *e.g.* Ekert91 protocol. The number of singlets (maximally entangled states) that can be extracted from a quantum state using only Local Operations and Classical Communication (LOCC) is referred to as the Entanglement of Distillation E_D. In order to establish a key, another important concept is the number of secret bits K_D, that can be extracted from a quantum state using LOCC. As a secret bit can always be extracted from maximally entangled states, $K_D \geq E_D$.

There are quantum states which cannot be distilled in spite of being entangled, *i.e.*, they have $E_D = 0$. These systems are usually referred to as bound entangled states since its entanglement is bound to the state. Nevertheless, for some of those states it has been shown that $K_D \neq 0$ and thus, they can be used to establish a secret key [32].

A particular case of states that cannot be distilled by "normal" procedures are Continuous Variable Gaussian states, *e.g.*, coherent, squeezed and thermal states of light. By "normal" procedures we mean operations that preserve the Gaussian character of the state (Gaussian operations), they correspond *e.g.* to beam splitters, phase shifts, mirrors, squeezers, etc. Thus, in the Gaussian scenario all entangled

Gaussian states posses bound entanglement. Navascués *et al* [33] have shown that it is also possible using only Gaussian operations to extract a secret key *à la* Ekert91 from entangled Gaussian states, in spite the fact that these states are not distillable. In other words, it has been proven that in the Gaussian scenario all entangled Gaussian states fulfill $GK_D > 0$ (where the letter G stands for Gaussian) while $GE_D = 0$.

The above result implies that in principle any entangled Gaussian state can be used for implementing Quantum Cryptography. However, any real implementation should address the optimization of the resources needed *i.e.* the efficiency of the protocol. The proposed protocol presented in [33] suffers precisely from an efficiency problem because the success probability of the protocol is vanishingly small. Here we will study the consequences of relaxing the protocol to a more realistic scenario preserving the security.

3.3.1 Distributing bits from Gaussian states by digitalizing output measurements

Extracting bits from discrete variables systems can be easily implemented by measuring for example spin observables and associating the up/down orientation, in a fixed axis, as the bit 0/1. In this sense we are digitalizing the output measurements on states. If one uses many copies of a bipartite entangled state it is possible to distribute among two separated parties a pair of bit strings. Such strings of bits possess in general a degree of correlations due to the entanglement present in the state. In the CV scenario and in particular with Gaussian states, the outcome measurements (of canonical variables) fill the continuum, and one needs to digitalize the results in some way. Before proceeding further we detail how to extract correlated string of bits from entangled Gaussian states.

We consider a bipartite CV system of two bosonic modes, A and B (see Fig. 3.1). Quadratures on each mode can be efficiently measured by standard homodyne detection. The probability that measuring the position quadrature $\hat{x}_A$ in mode A results in an outcome x_A with uncertainty σ is given by

$$\mathcal{P}_A(x_A) = \mathrm{tr}[\hat{\rho}_A \hat{\sigma}(x_A)], \tag{3.6}$$

where $\hat{\sigma}(x_A)$ is a single-mode Gaussian (squeezed) state with first moments $\{x_A, 0\}$ and covariance matrix $\mathrm{diag}\{\sigma^2, 1/\sigma^2\}$. In a similar way we define $\mathcal{P}_B(x_B)$ for mode B. The probability distribution associated to a joint measurement of the quadratures $\hat{x}_A$ and $\hat{x}_B$, is given by $\mathcal{P}_{AB}(x_A, x_B) = \mathrm{tr}[\hat{\rho}_{AB}(\hat{\sigma}(x_A) \otimes \hat{\sigma}(x_B))]$.

We digitalize the obtained outputs by assigning the bits $+(-)$ or $0(1)$ to the positive(negative) values of the measured quadratures. This digitalization transforms each joint quadrature measurement into a pair of classical bits. Let us adopt a compact notation by denoting $\mathcal{P}_A^{\pm} \equiv \mathcal{P}_A(\pm|x_A|)$, and $\mathcal{P}_{AB}^{\pm\mp} \equiv \mathcal{P}_{AB}(\pm|x_A|, \mp|x_B|)$. The probability that at a given string index the bits of the corresponding two modes coincide is given by $\mathcal{P}_{AB}^{=} \equiv (\mathcal{P}_{AB}^{++} + \mathcal{P}_{AB}^{--}) / \sum_{\{\alpha=\pm,\beta=\pm\}} \mathcal{P}_{AB}^{\alpha\beta}$. Correspondingly, the probability that they differ is $\mathcal{P}^{\neq}_{AB} \equiv (\mathcal{P}^{+-}_{AB} + \mathcal{P}^{-+}_{AB})/\sum_{\{\alpha=\pm,\beta=\pm\}} \mathcal{P}^{\alpha\beta}_{AB}$. Trivially, $\mathcal{P}^{=}_{AB} + \mathcal{P}^{\neq}_{AB} = 1$. If $\mathcal{P}^{=}_{AB} > \mathcal{P}^{\neq}_{AB}$ the measurement outcomes display correlations, otherwise they display anticorrelations. Notice that, if the two modes are completely uncorrelated, $\mathcal{P}^{=}_{AB} = \mathcal{P}^{\neq}_{AB} = 1/2$.

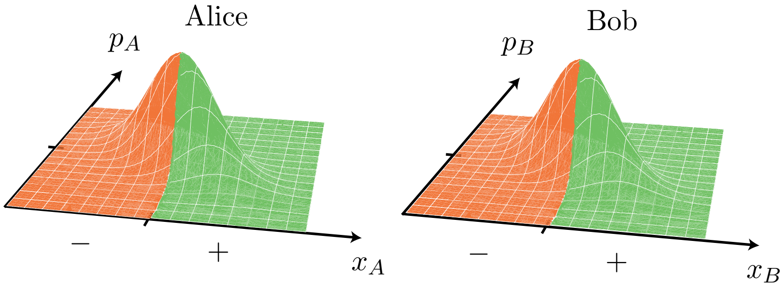

Figure 3.1: Alice and Bob 1×1 mode Gaussian state. The volume below the green zone denotes the probability for positive outcomes measurements of the x quadrature and the orange zone for the negatives outcomes. We have considered the global state with zero displacement vector.

3.3.2 Efficient Quantum Key Distribution using entanglement

It has been noticed that the degree of bit correlations are strongly related with the entanglement present in the states used to distribute the pair of strings of classical bits. We ask ourselves which is the possibility that Alice and Bob distribute total correlated strings of bits (a key) in a secure and efficient way by means of bipartite entangled Gaussian states.

The most general scenario we consider is that the state that Alice and Bob share is mixed, letting thus the possibility that an eavesdropper (Eve) has access to some degrees of freedom entangled with Alice and Bob before their distribution. In this general scenario, as the state of Alice and Bob is mixed it always admit a purification (see lemma 2.5.3). Thus, any mixed Gaussian state of 2 modes can be expressed as the reduction of a pure Gaussian state of 4 modes in such a way that the bipartite mixed Gaussian state (Alice and Bob) can be obtained after tracing out the 2 other modes (Eve). For what follows it is also important the fact that any NPPT Gaussian state of $N \times M$ can be mapped by Gaussian Local Operations and Classical Communication (GLOCC) to an NPPT symmetric state of 1×1 modes *i.e.* preserving the amount of entanglement. Finally, for $1 \times N$ Gaussian states NPPT and entanglement are equivalent concepts. By virtue of the above properties of Gaussian states, it is sufficient to consider the case in which Alice and Bob share many copies of a quantum system of 1×1 modes symmetric mixed NPPT Gaussian state $\hat{\rho}_{AB}$.

While the states that Alice and Bob share correspond to the reduction of a pure 4-mode state, Eve has access to an entangled reduction of two modes. We consider two types of attacks (i) *individual* (or incoherent) attacks, where Eve performs individual measurements, possibly non-Gaussian, over her set of states and (ii) *finite coherent* (or collective) attacks, where Eve waits until the distribution has been performed and, decides which collective measurement gives her more information on the final key.

We define the error probability as the probability that at a given string index the bits of the corresponding two modes differ *i.e.* $\epsilon_{AB} = \mathcal{P}^{\neq}_{AB}$. Having fixed a string of M classical correlated bits, Alice and Bob can apply Classical Advantage Distillation [34] to establish a secret key. To this aim, Alice generates a random bit b and encodes her string of M classical bits ($\vec{b}_A$) into a vector $\vec{b}$ of length M such that $b_{Ai} + b_i = b \bmod (2)$. The vector $\vec{b}$ is made public. Bob checks that for his bits all results $b_{Bi} + b_i = b' \bmod (2)$ are consistent, and in this case accepts the bit b as the first bit of the secret key. The new error probability is given by [35]

$$\epsilon_{AB,M} = \frac{(\epsilon_{AB})^M}{(1-\epsilon_{AB})^M + (\epsilon_{AB})^M} < \left(\frac{\epsilon_{AB}}{1-\epsilon_{AB}}\right)^M, \tag{3.7}$$

which tends to zero for sufficiently large M.

Security with respect to individual attacks from the eavesdropper Eve, can be established if [35]

$$\left(\frac{\epsilon_{AB}}{1-\epsilon_{AB}}\right)^M < |\langle e_{++}|e_{--}\rangle|^M, \tag{3.8}$$

where $|e_{\pm\pm}\rangle$ denotes the state of Eve once Alice and Bob have projected their states onto $|\pm|x_{0A}|, \pm|x_{0B}|\rangle$.

Notice that it is favorable for Alice and Bob to have a high degree of success (ϵ_{AB} small) while Eve can gain information if the overlap between her states after Alice and Bob have measured coincident results ($|\langle e_{++}|e_{--}\rangle|$) is sufficiently small. The above inequalities come from the fact that in the case of individual attacks the error on Eve's estimation of the final bit b is bound from below by a term proportional to $|\langle e_{++}|e_{--}\rangle|^M$ [35]. Therefore, Alice and Bob can establish a key if

$$\frac{\epsilon_{AB}}{1-\epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|. \tag{3.9}$$

In [33] it was shown that any 1×1 NPPT Gaussian state fulfills the above inequality and thus any NPPT Gaussian state can be used to establish a secure key in front of individual eavesdropper attacks. If we assume that Eve performs more powerful attacks, namely finite coherent attacks, then security is only guaranteed if the much more restrictive condition

$$\frac{\epsilon_{AB}}{1-\epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|^2, \tag{3.10}$$

is fulfilled. This new inequality is violated by some NPPT states. Notice that this implies that the analyzed protocol is not good for these states in this more general scenario. Nevertheless, using the recent techniques of [36], one can find states for which the presented protocol allows to extract common bits also secure against this attack.

The analyzed protocol [33], results in an inefficient success since it relies on an exact matching between Alice and Bob outputs as a requirement for security. Notice that since security relies on the fact that Alice and Bob have better correlations than the information the eavesdropper can learn about their state, perfect correlation is not a requirement to establish a secure key. We look for a constructive method to improve efficiency without compromising security. By denoting Alice's outputs by x_{0A}, we calculate which are the outputs x_{0B} Bob can accept so that the correlation established between Alice and Bob can still be used to extract a secret bit. Specifically, we relax the differences between their output quadrature measurements but imposing correlations in the sign of their quadratures *i.e.* we keep correlations in the sign of their output quadratures irrespectively of their numerical value. We thus demand that Alice and Bob associates the bits (+/-) or 0/1 to the positive(negative) value of their respective outcome measurement on each run. Alice will announce publicly the modulus of her outcome measurement each time. We study the efficiency and the security of the protocol if Bob accepts only outcomes measurements that lie in the nearest of Alice's outcomes such that security is guaranteed. Furthermore we analyze the performance of the protocol in terms of the entanglement sharing.

We use the standard form of a bipartite 1×1 mode mixed Gaussian state, (see lemma 2.5.2) for the states shared between Alice and Bob

$$\gamma_{AB} = \begin{pmatrix} \lambda_a & 0 & c_x & 0 \\ 0 & \lambda_a & 0 & -c_p \\ c_x & 0 & \lambda_b & 0 \\ 0 & -c_p & 0 & \lambda_b \end{pmatrix}, \tag{3.11}$$

where, without loss of generality, we flip the sign of c_p and adopt the convention $c_x \geq |c_p| \geq 0$ (we fix also the displacement vector to 0). For simplicity we can deal with mixed symmetric (as said above being totally general) and so $\lambda_a = \lambda_b = \lambda \geq 1$. The positivity condition, see lemma 2.5.2, reads $(\lambda - c_x)(\lambda + c_p) \geq 1$, while the entanglement NPPT condition, see lemma 2.6.3, is given by $(\lambda - c_x)(\lambda - c_p) < 1$. We impose that the global state including Eve is pure (she has access to all degrees of freedom outside Alice an Bob) while the mixed symmetric state, shared by Alice and Bob is just its reduction (see lemma 2.5.3), thus

$$\gamma_{ABE} = \begin{pmatrix} \gamma_{AB} & C \\ C^T & \theta_{AB}\gamma_{AB}\theta_{AB}^T \end{pmatrix}, \tag{3.12}$$

$$C = \mathcal{J}_{AB}\sqrt{-(\mathcal{J}_{AB}\gamma_{AB})^2 - \mathbb{I}_4}\,\theta_{AB} = \begin{pmatrix} 0 & -X & 0 & -Y \\ -X & 0 & -Y & 0 \\ 0 & Y & 0 & -X \\ -Y & 0 & -X & 0 \end{pmatrix}, \tag{3.13}$$

$$\theta_{AB} = \theta_A \oplus \theta_B, \qquad \mathcal{J}_{AB} = \mathcal{J}_A \oplus \mathcal{J}_B, \tag{3.14}$$

where

$$X = \frac{\sqrt{a+b}+\sqrt{a-b}}{2},$$

$$Y = \frac{\sqrt{a+b}-\sqrt{a-b}}{2},$$

and $a = \lambda^2 - c_x c_p - 1$, $b = \lambda(c_x - c_p)$.

Performing a measurement with uncertainty σ, the probability that Alice finds $\pm|x_{0A}|$ while Bob finds $\pm|x_{0B}|$, is given by the overlap between the state of Alice and Bob, $\hat{\rho}_{AB}$, and a pure product state $\hat{\rho}_{A,i}\otimes\hat{\rho}_{B,j}$ (with $i,j=0,1$) of Gaussians centered at $\pm|x_{0A}|$ and $\pm|x_{0B}|$ respectively with σ width (notice $\hat{\rho}_{A,0} \equiv |+|x_{0A}|\rangle\langle +|x_{0A}||$) which gives

$$\begin{aligned}\mathcal{P}^{++}_{AB,\sigma} = \mathcal{P}^{--}_{AB,\sigma} &= \mathrm{tr}[\hat{\rho}_{AB}(\hat{\rho}_{A,0}\otimes\hat{\rho}_{B,0})] = \\ &= (2\pi)^4 \int d^4\zeta_{AB}\, \mathcal{W}_{\rho_{AB}}(\zeta_{AB})\mathcal{W}_{\rho_{A,0}\otimes\rho_{B,0}}(\zeta_{AB}) = \\ &= K(\sigma)\exp\left(\frac{2|x_{0A}||x_{0B}|c_x - (\lambda+\sigma^2)(x_{0A}^2+x_{0B}^2)}{(\lambda+\sigma^2)^2 - c_x^2}\right),\end{aligned} \tag{3.15}$$

for the probability that their symbols do coincide and,

$$\mathcal{P}^{-+}_{AB,\sigma} = \mathcal{P}^{+-}_{AB,\sigma} = K(\sigma)\exp\left(\frac{-2|x_{0A}||x_{0B}|c_x - (\lambda+\sigma^2)(x_{0A}^2+x_{0B}^2)}{(\lambda+\sigma^2)^2 - c_x^2}\right), \tag{3.16}$$

for the probability that they do not coincide, where

$$K(\sigma) = \frac{4\sigma^2}{\sqrt{(\lambda+\sigma^2)^2 - c_x^2}\sqrt{(\lambda\sigma^2+1)^2 - c_p^2\sigma^4}}. \tag{3.17}$$

Their error probability for $\sigma \to 0$ reads

$$\epsilon_{AB} = \lim_{\sigma\to 0}\mathcal{P}^{\neq}_{AB,\sigma} = \frac{1}{1+\exp\left(\frac{4c_x|x_{0A}||x_{0B}|}{\lambda^2-c_x^2}\right)}. \tag{3.18}$$

Let us calculate the bipartite state of Eve $|e_{\pm\pm}\rangle$ after they have mesured (Alice has projected onto $|\pm|x_{0A}|\rangle$ and Bob onto $|\pm|x_{0B}|\rangle$)

$$\gamma_{++} = \gamma_{--} = \begin{pmatrix}\gamma_x & 0 \\ 0 & \gamma_x^{-1}\end{pmatrix}, \qquad \gamma_x = \begin{pmatrix}\lambda & c_x \\ c_x & \lambda\end{pmatrix}, \tag{3.19}$$

$$d_{\pm\pm} = \mp\begin{pmatrix}0 \\ 0 \\ A\delta x_0 - B\Delta x_0 \\ A\delta x_0 + B\Delta x_0\end{pmatrix}, \tag{3.20}$$

where $A = \frac{\sqrt{a+b}}{\lambda+c_x}$, $B = \frac{\sqrt{a-b}}{\lambda-c_x}$, $\Delta x_0 = |x_{0B}| - |x_{0A}|$ and $\delta x_0 = |x_{0B}| + |x_{0A}|$. The overlap between the two states of Eve, which gives a direct quantification of the distinguishability, is given by

$$|\langle e_{++}|e_{--}\rangle|^2 = \frac{1}{\sqrt{\det(\frac{\gamma_{++}+\gamma_{--}}{2})}} e^{-(d_{--}-d_{++})^T(\frac{1}{\gamma_{++}+\gamma_{--}})(d_{--}-d_{++})} =$$

$$= \exp\left(\frac{-4}{\lambda^2 - c_x^2}\left[\left(\frac{x_{0A}^2 + x_{0B}^2}{2}\right)(\lambda^2 - c_x^2 - 1)\lambda + |x_{0A}||x_{0B}|\left(c_x - c_p(\lambda^2 - c_x^2)\right)\right]\right) \tag{3.21}$$

Substituting Eqs. (3.18) and (3.21) into (3.9) one can check, after some algebra, that the last inequality reduces to

$$\left(\frac{x_{0A}^2 + x_{0B}^2}{2}\right)(\lambda^2 - c_x^2 - 1)\lambda + |x_{0A}||x_{0B}|\left(-c_x - c_p(\lambda^2 - c_x^2)\right) < 0. \tag{3.22}$$

Notice that condition (3.22) imposes both, restrictions on the parameters defining the state (λ, c_x, c_p), and on the outcomes of the measurements (x_{0A}, x_{0B}). The constraints on the state parameters are equivalent to demand that the state is NPPT and satisfies

$$(\lambda - c_x)(\lambda + c_x) \geq 1. \tag{3.23}$$

Nevertheless, as $c_x \geq c_p$, any positive state fulfills this condition. Hence for any NPPT symmetric state, there exists, for a given x_{0A}, a range of values of x_{0B} such that secret bits can be extracted (Eq. (3.9) is fulfilled) efficiently. This range is given by

$$\Delta x_0 = |x_{0B}| - |x_{0A}| \in \mathfrak{D}_\alpha = \left[\frac{2}{-\sqrt{\alpha}-1}, \frac{2}{\sqrt{\alpha}-1}\right]|x_{0A}|, \tag{3.24}$$

where

$$\alpha = \left(\frac{c_x - \lambda}{c_x + \lambda}\right)\left[\frac{1 - (\lambda + c_x)(\lambda + c_p)}{1 - (\lambda - c_x)(\lambda - c_p)}\right]. \tag{3.25}$$

After Alice communicates $|x_{0A}|$ to Bob (the signs obtained are kept in secret), he will accept only measurement outputs within the above interval Δx_0. The interval is well defined if $\alpha \geq 1$, which equals to fulfill Eq. (3.23). Notice also that the interval is not symmetric around $|x_{0A}|$ because the probabilities calculated in Eqs. (3.15) and (3.16) do depend on this value in a non-symmetric way. The length D_α of the interval of valid measurements outputs for Bob is given by

$$D_\alpha = \frac{4\sqrt{\alpha}}{\alpha - 1}|x_{0A}|. \tag{3.26}$$

It can be observed that maximal $D_\alpha \to \infty$ ($\alpha = 1$) corresponds to the case when Alice and Bob share a pure state (Eve is disentangled from the system) and thus condition (3.9) is always fulfilled. On the other hand, any mixed NPPT symmetric state ($\alpha > 1$) admits a finite D_α. This ensures a finite efficiency on establishing a secure secret key in front of individual attacks.

If we assume that Eve performs more powerful attacks, namely finite coherent attacks, then security is only guaranteed if

$$\frac{\epsilon_{AB}}{1-\epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|^2. \tag{3.27}$$

This condition is more restrictive than (3.9). With a similar calculation as before we obtain that now security is not guaranteed for all mixed entangled symmetric NPPT states, but only for those that also satisfy

$$\lambda - (\lambda + c_x)(\lambda - c_x)(\lambda - c_p) > 0. \tag{3.28}$$

For such states, and given a measurement result x_{0A} of Alice, Bob will only accept outputs within the range

$$\Delta x_0 = |x_{0B}| - |x_{0A}| \in \mathfrak{D}_\beta = \left[\frac{2}{-\sqrt{\beta}-1}, \frac{2}{\sqrt{\beta}-1}\right] |x_{0A}|, \tag{3.29}$$

where

$$\beta = \frac{2\lambda(\lambda^2 - c_x^2 - 1)}{\lambda - (\lambda + c_x)(\lambda - c_x)(\lambda - c_p)} \geq 1. \tag{3.30}$$

As before, $\beta \geq 1$ is fulfilled by conditions (3.23) and (3.28).

Let us now focus on the efficiency issue. We define the efficiency $E(\gamma_{AB})$ of the protocol for a given state γ_{AB}, as the average probability (over the range of secure outcomes, $\mathfrak{D}$) of obtaining a classically correlated bit. Explicitly,

$$E(\gamma_{AB}) = \int_{\Delta x_0 \in \mathfrak{D}} dx_{0A} dx_{0B} (1 - \epsilon_{AB}) \mathrm{tr}(\hat{\rho}_{AB} |x_{0A}, x_{0B}\rangle\langle x_{0A}, x_{0B}|). \tag{3.31}$$

The marginal distribution in phase-space is easily computed by integrating the corresponding Wigner function in momentum space

$$\begin{aligned} \mathrm{tr}(\hat{\rho}_{AB}|x_{0A}, x_{0B}\rangle\langle x_{0A}, x_{0B}|) &= \int\int dp_A dp_B \mathcal{W}_{\rho_{AB}}(\zeta_{AB}) = \\ &= \frac{\exp\left(\frac{2c_x x_{0A} x_{0B} - \lambda(x_{0A}^2 + x_{0B}^2)}{\lambda^2 - c_x^2}\right)}{\pi\sqrt{\lambda^2 - c_x^2}}, \end{aligned} \tag{3.32}$$

but the final expression of Eq. (3.31) has to be calculated numerically. Note that if Alice and Bob share as a resource M identical states (NPPT state for individual attacks, and NPPT fulfilling condition (3.28) for finite coherent attacks), the number of classically correlated bits that can be extracted from them is $\sim M \times E(\gamma_{AB})$. The efficiency Eq. (3.31) increases with increasing D. In particular, for the protocol given in [33], $D = 0$, and therefore $E(\gamma_{AB}) = 0$ for any state.

We investigate now the dependence of $E(\gamma_{AB})$ with the entanglement of the NPPT mixed symmetric state used for the protocol as well as with the purity of the state. In order to fix one parameter of the states we fix the energy of the states at a fixed value (λ cte). As a measure of the entanglement between Alice and Bob, see (2.97), we compute the logarithmic negativity

$$\mathrm{LN}(\gamma_{AB}) = -\log_2[\min(\tilde{\mu}_-, 1)] - \log_2[\min(\tilde{\mu}_+, 1)] = \log_2\left(\frac{1}{\sqrt{(\lambda - c_x)(\lambda - c_p)}}\right) > 0. \tag{3.33}$$

because $\tilde{\mu}_+ > 1$ and $1 > \tilde{\mu}_- = \sqrt{(\lambda - c_x)(\lambda - c_p)}$.

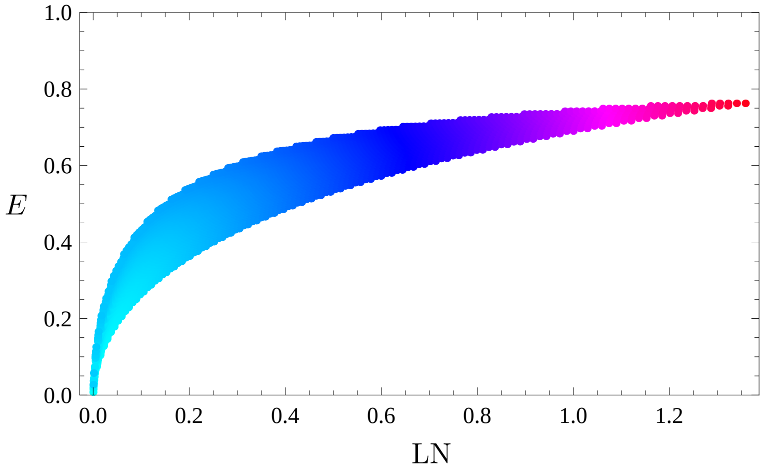

Figure 3.2: Protocol efficiency (quantified by E) versus the entanglement measured by logarithmic negativity LN. The shading from cyan to red corresponds to purity from zero to one.

In Fig. 3.2, we display the efficiency of the protocol (assuming individual attacks) versus entanglement shared between Alice and Bob for different states γ_{AB}. There is not a one-to-one correspondence between efficiency and entanglement, since states with the same entanglement can have different purity, which can lead to different efficiency. This is so because there are two favorable scenarios to fulfill Eq. (3.9). The first one is to demand large correlations so that the relative error ϵ_{AB} of Alice and Bob is small. The second scenario happens when Alice and Bob share a state with high purity, *i.e.*, Eve is very disentangled. In this case, independently of the error ϵ_{AB}, Eq. (3.9) can be fulfilled more easily. Despite the fact that efficiency generally increases with increasing entanglement and increasing purity, this enhancement, as depicted in the figure, is a complex function of the parameters involved. Nevertheless, one can see that there exist an entanglement threshold (around LN $\simeq 0.2$) below which the protocol efficiency diminishes drastically no matter how mixed are the states shared between Alice and Bob.

It is also illustrative to examine the dependence of α (which determines the interval length D_α) on the entanglement of the states shared by Alice and Bob.

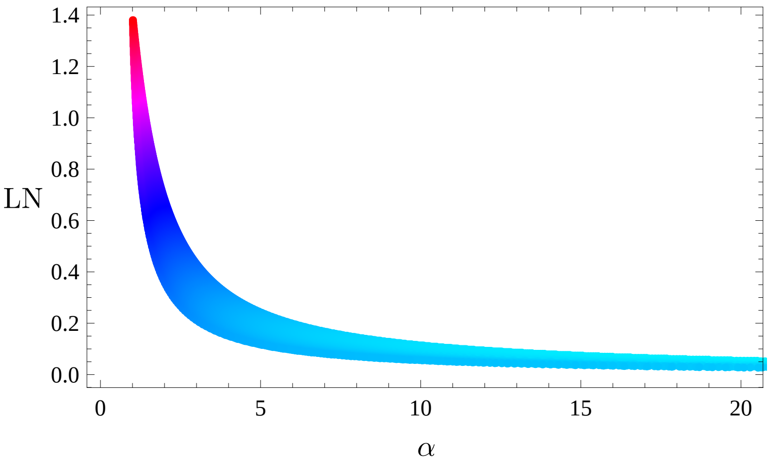

Figure 3.3: Entanglement of the states shared between Alice and Bob measured in terms of the logarithmic negativity LN as a function of the parameter α under individual attacks. The shading from cyan to red corresponds to purity from zero to one.

In Fig. 3.3 we plot the logarithmic negativity of a given state versus the parameter α. States with the same entanglement but different purity are associated to quite different values of α, specially for states with low entanglement (high purity). Nevertheless states with high entanglement permit a large interval length (small α) and, thus, high efficiency.

In both, Fig. 3.2 and Fig. 3.3, we have observed that states with different entanglement give the same efficiency. However it is important to point out that to extract the key's bits, Classical Advantage Distillation [34] stills needs to be performed. The efficiency of Maurer's protocol, strongly increases with decreasing ϵ_{AB}, and, therefore, the states with higher entanglement will provide a higher key rate.

3.4 Conclusions

Efficiency is a key issue for any experimental implementation of Quantum Cryptography since available resources are not unlimited. In this chapter, we have shown that the sharing of entangled Gaussian variables and the use of only Gaussian operations permits efficient Quantum Key Distribution against individual and finite coherent attacks.

We have used the fact that all mixed NPPT symmetric states can be used to extract secret bits to design an algorithm, that efficiently succeeds for a secure extraction of a key. Whereas under individual attacks all mixed NPPT symmetric states admit a finite efficiency, for finite coherent attacks an additional condition constrains the parameters of the states. We have introduced a figure of merit (the efficiency E) to quantify the number of classical correlated bits that can be used to distill a key from a sample of M entangled states. We have observed that this quantity grows with the entanglement shared between Alice and Bob. This relation it is not one-to-one due to the fact that states with less entanglement but with more purity (eavesdropper more disentangled) can be equally efficient. Nevertheless we have point out that, these states would be inefficient, when performing the Classical Advantage Distillation of the key.

Chapter 4

Byzantine agreement problem with Continuous Variable

4.1 Introduction

One of the aims of Quantum Information is to provide new protocols and algorithms (set of rules for solving a problem in a finite number of steps) which exploit quantum resources to find a solution to problems which either lack a solution using classical resources or the solution is extremely hard to implement. In this chapter we analyze a multipartite protocol, the Byzantine agreement problem, by means of multipartite Gaussian entanglement.

The term “Byzantine Agreement” was originally coined by Lamport and Fischer [37] in the context of computer science to analyze the problem of fault tolerance when a faulty processor is sending inconsistent information to other processors. In a cryptographic context, it refers to distributed protocols in which some of the participants might have malicious intentions and could try to sabotage the distributed protocol inducing the honest parties to take contradictory actions between them. This problem is often reformulated in terms of a Byzantine army where there is a general commander who sends the order of attacking or retreating to each one of his lieutenants. Those can also communicate pairwise to reach a common decision concerning attacking or retreating, knowing that there might be traitors among them including the general commander. A traitor could create fake messages to achieve that different parts of the army attack while other retreat, which would put the army at a great disadvantage. The question hence is whether there exists a protocol among all the officials involved that, after its termination, satisfies the following conditions: The commanding general sends an order to his $N-1$ lieutenants such that: (i) All loyal lieutenants obey the same order, (ii) If the commanding general is loyal, then every loyal lieutenant obeys the order he sends. It is assumed that the parties cannot share any previous setup.

Lamport *et al* [38] proved that if the participants only shared pairwise secure classical channels, then Byzantine Agreement or broadcast is only possible iff $t < n/3$

where n is the number of players and t the number of traitors among them. In [39] Fitzi and co-workers introduced a weaker nevertheless important version of Byzantine Agreement known as *detectable broadcast*. Detectable broadcast is said to be achieved if the protocol satisfies the following conditions: (i) If no player is corrupted, then the protocol achieves broadcast and (ii) If one or more players are corrupted, then either the protocol achieves Byzantine Agreement or all honest players abort the protocol. Thus, in a detectable broadcast protocol, cheaters can force the protocol to abort, *i.e.* no action is taken. In such cases all honest players agree on aborting the protocol so that contradictory actions between the honest players are avoided. In the same paper [39], Fitzi, Gisin and Maurer devised a solution to the detectable broadcast problem using multipartite entanglement as a quantum resource. Later on Fitzi *et al* [40] and Iblisdir and Gisin [41] showed that a Quantum Key Distribution (QKD) protocol, which guarantees a private sequences of classical data shared between pairs of parties, suffices to solve detectable broadcast. This situation is reminiscent of quantum cryptography, in which two seemingly independent main schemes exist for QKD, the prepare-and-measure BB84 scheme [24] which does not use entangled states shared between Alice and Bob, and the Ekert91 scheme [25] where indeed entanglement is explicitly distributed and the security is guaranteed by the violations of Bell inequalities. However, the two schemes have been shown to be completely equivalent [26], and specifically entanglement stands as a precondition for any secure key distribution [27].

Detectable broadcast might be regarded in a similar view as Quantum Key Distribution and, arguably, the same reasoning applies to the different protocols advanced for its solution, making explicit or implicit use of multipartite entanglement. In this paper, we adopt an approach *à la* Ekert91, guided by the physical motivation of studying the performance and the usefulness of multipartite entangled states as operational resources to achieve detectable broadcast. While protocols for this task exist for qutrits [39] and qubits [42, 43], in this paper we investigate the possibility of solving detectable broadcast with Continuous Variable (CV) systems, namely with Gaussian states and performing Gaussian operations only. The motivations for this approach are manifold. On the practical side, the recent progresses in CV QKD [44] has shown that the use of efficient homodyne detectors, compared to photon counters employed in BB84 schemes, enables the distribution of secret keys at faster rates over increasingly long distances [45, 46]. On the theoretical side, multipartite entanglement is a central concept whose understanding and characterization (especially in high-dimensional and CV systems), despite recent efforts, is far from being complete. It is important, therefore, to approach this task *operationally*, *i.e.* by connecting entanglement to the success or to the performance of diverse quantum information and communication tasks [47], while exploiting the differences between discrete-variable and continuous-variable scenarios. For Gaussian states of light fields, which are presently the theoretical and experimental pillars of Quantum Information with CVs [48], an important result in this respect is due to van Loock and Braunstein [49]. They introduced a scheme to produce fully symmetric (permutation-invariant) n-mode Gaussian states exhibiting genuine multipartite entanglement. Furthermore, they devised a communication protocol, the "quantum teleportation network", for the distribution of quantum states exploiting such resources, which has been experimentally demonstrated for $n = 3$ [50]. The optimal fidelity characterizing the performance of such a protocol yields an operational quantification of genuine multipartite entanglement in symmetric Gaussian states. This quantification is equivalent to the information-theoretic "residual contangle" measure, a Gaussian entanglement monotone, emerging from the monogamy of quantum correlations [51, 52]. Other applications of multipartite Gaussian entanglement have been advanced and demonstrated, and the reader may find more details in [6, 48], as well as in the two more recent complementary reviews [9] (theoretical) and [53] (experimental).

We have proposed a novel protocol to solve detectable broadcast with symmetric multimode entangled Gaussian states and homodyne detection. This provides an alternative interpretation of multipartite Gaussian entanglement as a resource enabling this kind of secure communication. We concentrate on the case of three parties, and remarkably find that not all three-mode symmetric entangled Gaussian states are useful to achieve a solution: to solve detectable broadcast there is a minimum threshold in the multipartite entanglement. This is at variance with the two-party QKD counterpart: in there, all two-mode entangled Gaussian states are useful to obtain a secure key using Gaussian operations [33]. We eventually discuss how our protocol can be implemented in realistic conditions, namely considering detectors with finite efficiency and yielding not perfectly matched measurement outcomes, and Gaussian resources which are not ideally pure, but possibly (as it is in reality) affected by a certain amount of thermal noise. We show that under these premises the protocol is still efficiently applicable to provide a robust solution to detectable broadcast over a broad range of the involved parameters (noise, entanglement, measurement outcomes and uncertainties), paving the way towards a possible experimental demonstration in a quantum optical setting.

4.2 Detectable broadcast protocol

The protocols to solve detectable broadcast, in the discrete scenario, using entanglement as a resource are based on three differentiated steps:

i) Distribution of the quantum states.

ii) Test of the distributed states.

iii) Protocol by itself.

Step iii) is fundamentally classical, since it uses the outputs of the different measurements of the quantum states to simulate a particular random generator ("primitive"). Let us consider the simplest case, in which only three parties are involve and at most one traitor is allowed, for which no classical solution exists. The parties are traditionally denoted by S (the sender, *i.e.* commander general) and the receivers R_0 and R_1

(*i.e.* lieutenants), and at most, only one is a traitor. In this case, the primitive generates for every invocation a random permutation of the elements $\{0, 1, 2\}$ with *uniform distribution*, *i.e.* $(t_S, t_{R_0}, t_{R_1}) \in \{(0, 1, 2), (0, 2, 1), (1, 0, 2), (1, 2, 0), (2, 0, 1), (2, 1, 0)\}$. In this primitive, no single player n can learn more about the permutation than the value t_n $(n = \{S, R_0, R_1\})$ which she/he obtain *i.e.*, each player ignores how the other two values are assigned to the other two players. Furthermore, nobody else (besides the parties) have access to the sequences.

Entanglement is used in the protocol to distribute classical private random variables with a specific correlation between the players, in such a way that any malicious manipulation of the data can be detected by all honest parties allowing them to abort the protocol. In the discrete variable case such a primitive can be implemented with qutrits using *e.g.* Aharonov states $|\mathcal{A}\rangle = \frac{1}{\sqrt{6}}(|0, 1, 2\rangle + |1, 2, 0\rangle + |2, 0, 1\rangle - |0, 2, 1\rangle - |1, 0, 2\rangle - |2, 1, 0\rangle)$. This choice allows the distribution and test part to be secure [39]. Whenever the three qutrits are all measured in the same basis, all the three results are different. Hence -after discarding all the states used for the testing of the distributed states (step ii))- the players are left with a sequence of outputs that reproduces the desired primitive. We schematically represent this primitive by the table below

j	1	2	3	4	5	6	7	8	9	...
S	2	0	0	1	2	1	0	2	1	...
R_0	1	1	2	0	1	0	1	0	2	...
R_1	0	2	1	2	0	2	2	1	0	...

After accomplishing the distribution and test part of the protocol (steps i) and ii)) detailed in section 4.4, the sender S will broadcast a bit $b \in \{0, 1\}$ ($0 \overset{\wedge}{=}$"attack", $1 \overset{\wedge}{=}$"retreat") to the two receivers using the mentioned distributed and tested primitive and classical secure channels.

Following [39] the broadcast (step iii)) proceeds as follows:

iii-1) We denote by b_i the bits received by R_i, $i = 0, 1$ (notice that if the sender is malicious, the broadcasts bits b_i could be different). Each receiver R_i demands to S to send him the indices j for which S got the result b_i (on the primitive). Each player R_i receives a set of indices J_i.

iii-2) Each R_i test consistency of his own data, *i.e.* checks weather his output on the set of indices he receives (J_i) are all of them different from b_i. If so the data is consistent and he settles his flag to $c_i = b_i$, otherwise his flag is settled to $c_i = \perp$.

iii-3) R_0 and R_1 send their flags to each other. If both flags agree, the protocol terminates with all honest participants agreeing on b.

iii-4) If $c_i = \perp$, then player R_i knows that S is dishonest, the other player is honest and accepts his flag.

iii-5) If both R_0 and R_1 claim to have consistent data but $c_0 \neq c_1$, player R_1 demands from R_0 to send him all the indices $k \in J_0$ for which R_0 has the results $1 - c_0$. R_1 checks now that (i) all indices k from R_0 are not in J_1 and (ii) the output R_1 obtains from indices k correspond to the value 2. If this is the case, R_1 concludes that R_0

is honest and changes his flag to c_0. If not, R_1 knows that R_0 is dishonest and he keeps his flag to c_1. Detectable broadcast is in this way achieved.

4.3 Continuous variable primitive

We first review briefly the basic tools needed to describe multipartite Gaussian states and measurements. Building on the ideas presented in the previous section, we construct a protocol adapted to the Continuous Variable case.

To achieve the primitive presented in the CV set up we consider quantum systems of 3 canonical degrees of freedom, *i.e.* 3 modes (one for each player), associated to a Hilbert space $\mathcal{H} = \mathcal{L}^2(\mathbb{R}^6)$. Following the discussion of the protocol (step iii)) for the implementation of the primitive in the discrete case, we choose to use as a resource a pure, fully inseparable tripartite Gaussian state, completely symmetric under the interchange of the modes [49].

In contrast to the bipartite case where one kind of entanglement exist, the tripartite case is much richer [54] and offers several classes of entanglement. In [55] a classification for Gaussian states, in terms of the non-positivity of the partial transpose across several bipartite partitions (NPPT criterium), was studied. Namely for tripartite Gaussian states described by a covariance matrix γ, 5 classes of states can be distinguished.

i) Class 1 (Fully inseparable states or genuine entangled) iff

$$\begin{aligned} \theta_A \gamma \theta_A^T + \mathrm{i}\mathcal{J} &\ngeq 0, \\ \theta_B \gamma \theta_B^T + \mathrm{i}\mathcal{J} &\ngeq 0, \\ \theta_C \gamma \theta_C^T + \mathrm{i}\mathcal{J} &\ngeq 0. \end{aligned}$$

ii) Class 2 (One-mode biseparable) iff

$$\begin{aligned} \theta_i \gamma \theta_i^T + \mathrm{i}\mathcal{J} &\geq 0, \\ \theta_j \gamma \theta_j^T + \mathrm{i}\mathcal{J} &\ngeq 0, \\ \theta_k \gamma \theta_k^T + \mathrm{i}\mathcal{J} &\ngeq 0, \end{aligned}$$

any permutation of modes (i, j, k) must be considered.

iii) Class 3 (Two-mode biseparable) iff

$$\begin{aligned} \theta_i \gamma \theta_i^T + \mathrm{i}\mathcal{J} &\geq 0, \\ \theta_j \gamma \theta_j^T + \mathrm{i}\mathcal{J} &\geq 0, \\ \theta_k \gamma \theta_k^T + \mathrm{i}\mathcal{J} &\ngeq 0, \end{aligned}$$

any permutation of modes (i, j, k) must be considered.

iv) Class 4 (Three-mode biseparable or bound entanglement)

or Class 5 (Fully separable) iff

$$\theta_A \gamma \theta_A^T + \mathrm{i}\mathcal{J} \geq 0,$$
$$\theta_B \gamma \theta_B^T + \mathrm{i}\mathcal{J} \geq 0,$$
$$\theta_C \gamma \theta_C^T + \mathrm{i}\mathcal{J} \geq 0,$$

with $\mathcal{J} = \oplus_{i=1}^{3} \mathcal{J}$. The condition for full inseparability (truly multipartite entanglement) across the $1 \times 1 \times 1$ mode partition can be rewritten and reads as $\gamma + \mathrm{i}\mathcal{J}_A \ngeq 0$, $\gamma + \mathrm{i}\mathcal{J}_B \ngeq 0$, $\gamma + \mathrm{i}\mathcal{J}_C \ngeq 0$ with $\mathcal{J}_A = \mathcal{J}^T \oplus \mathcal{J} \oplus \mathcal{J}$, analogously for B and C.

A tripartite Gaussian state with such properties (pure, fully inseparable, completely symmetric under the interchange of the modes) with covariance matrix $\gamma(a)$ accepts the following parametrization [55]

$$\gamma(a) = \begin{pmatrix} a & 0 & c & 0 & c & 0 \\ 0 & b & 0 & -c & 0 & -c \\ c & 0 & a & 0 & c & 0 \\ 0 & -c & 0 & b & 0 & -c \\ c & 0 & c & 0 & a & 0 \\ 0 & -c & 0 & -c & 0 & b \end{pmatrix}, \tag{4.1}$$

with $a \geq 1$ and

$$b = \frac{1}{4}(5a - \sqrt{9a^2 - 8}), \tag{4.2}$$
$$c = \frac{1}{4}(a - \sqrt{9a^2 - 8}). \tag{4.3}$$

It follows that $\gamma(a)$ is fully inseparable as soon as $a > 1$. Quantitatively, the genuine tripartite entanglement of the states of (4.1), as measured by the residual contangle [52], is a monotonically increasing function of a and diverges for $a \to \infty$.

So far $\gamma(a)$ appears as the "equivalent" CV version of the discrete Aharonov state $|\mathcal{A}\rangle$, *i.e.* pure, fully inseparable and completely symmetric under exchange of the 3 players. One is tempted to infer, therefore, that the discussed primitive of the discrete case can be straightforwardly generalized to the continuous one. A standard way of transforming the correlations of the shared entangled quantum states $\hat{\rho}_a$ into a sequence of classically correlated data between the 3 players is to perform a homodyne measurement of the quadratures of each mode. Denoting by $\hat{x}_S$, $\hat{x}_{R_0}$, $\hat{x}_{R_1}$ the position (or momentum) operator of each mode, and by x_S, x_{R_0}, x_{R_1} the output of the respective measurements, the players after quadrature measurement on their modes end up with classical correlated data according to the entanglement sharing. In order to proceed with the classical part of the protocol (step iii)) one need to digitalize the outcome measurements into trit correlated data. A standard way to proceed is the following, the 3 players communicate classically with each other and agree, for instance, only on those outcome values for which either $|x_S| = |x_{R_0}| = |x_{R_1}| = \{0, x_0\}$ with $x_0 > 0$. In this way each player can associate the logical trit ($t = 0, 1, 2$) to a positive, negative or null result respectively, willing to map the quadrature correlations into trit correlations. To verify the success of such procedure we define the probability distribution that measuring the quadratures $\hat{x}_S$, $\hat{x}_{R_0}$, $\hat{x}_{R_1}$ an outcome $t_S = j$, $t_{R_0} = k$, $t_{R_1} = l$ is produced with uncertainty σ, being $(j, k, l) \in \{0, 1, 2\}$. Such probability is given by

$$\begin{aligned} \mathcal{P}(j,k,l) &= \mathrm{tr}\hat{\rho}_\sigma^{\{j,k,l\}}\hat{\rho}_a = \\ &= (2\pi)^n \int \mathcal{W}_\sigma^{\{j,k,l\}}(\xi)\mathcal{W}_a(\xi)d^{2n}\xi. \end{aligned} \tag{4.4}$$

Here $\hat{\rho}_\sigma^{\{j,k,l\}} = \hat{\rho}_S^{t_S=j} \otimes \hat{\rho}_{R_0}^{t_{R_0}=k} \otimes \hat{\rho}_{R_1}^{t_{R_1}=l}$ describes the separable state of the 3 modes obtained after each party has measured its corresponding quadrature and obtained an output j, k, l. Thus, the state $\hat{\rho}_\sigma$ of the system after the measure can be described by a fully separable covariance matrix

$$\gamma_\sigma = \begin{pmatrix} \sigma^2 & 0 \\ 0 & 1/\sigma^2 \end{pmatrix} \oplus \begin{pmatrix} \sigma^2 & 0 \\ 0 & 1/\sigma^2 \end{pmatrix} \oplus \begin{pmatrix} \sigma^2 & 0 \\ 0 & 1/\sigma^2 \end{pmatrix},$$

(where each party has a pure one mode Gaussian state) and by a displacement vector $d_\sigma^T = (f_{j,k,l}^{(1)}|x_0|, 0) \oplus (f_{j,k,l}^{(2)}|x_0|, 0) \oplus (f_{j,k,l}^{(3)}|x_0|, 0)$ being $\vec{f}_{j,k,l} = (\pm 1/0, \pm 1/0, \pm 1/0)$ where $\{+1/-1/0\}$ corresponds to the trit values $\{0/1/2\}$. On the other hand $\mathcal{W}_a$ is the Wigner function of the initial tripartite entangled state $\hat{\rho}_a$ described by the covariance matrix $\gamma(a)$ and displacement vector d (to be fixed).

Since Gaussian states are symmetric with respect to their displacement vector, and quadrature output measurements fill the continuum, it is easy to see that a mapping into classical trits such that all possible outputs $\{0, 1, 2\}$ occur with the same and non-vanishing probability is not possible. Therefore, the primitive discussed in the discrete case has to be modified when adapted to the CV scenario. The way we find to overcome this asymmetry of the output's probabilities relies on joining the correlations from pairs of quantum states. First we map the quantum correlations involved in each single quantum state just to classical bits by a "sign binning" (as in CV QKD [33]). That is, first we keep only the results for which the 3 players obtain a coincident output $|x_S| = |x_{R_0}| = |x_{R_1}| = x_0 > 0$, and associate the logical bit $b_n = 0(1)$, where $n = \{S, R_0, R_1\}$, to positive (negative) value of the coincident quadrature $+x_0(-x_0)$. In every measurement the sender makes public his outcome result x_0, whatever the output is (in each run the sender will obtain a different outcome result), but not its sign. In this step, all states are used in the protocol (we will relax the "idealization" of coincident outputs in section 4.6). Second we construct an appropriate primitive consisting of a random permutation of the elements $(i, j, k) \in \{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$. Compulsory for the implementation of the primitive is that every element of the primitive appears with equal probability and any other combination of the outputs not regarded by the primitive is exceedingly small compared to the allowed permutations. In other words, denoting by $p \equiv \mathcal{P}(0,1,1) = \mathcal{P}(1,0,1) = \mathcal{P}(1,1,0)$, and, denoting by $\delta_i \equiv \mathcal{P}(else)$, we require that the corresponding conditional probabilities,

$$\tilde{\mathcal{P}}(b_S, b_{R_0}, b_{R_1}) = \frac{\mathcal{P}(b_S, b_{R_0}, b_{R_1})}{\sum_{i,j,k=\{0,1\}} \mathcal{P}(i,j,k)},$$

fulfill $\tilde{p} \to \frac{1}{3}$ and $\tilde{\delta}_i \to 0$.

If the above conditions are met, it is possible then by invoking two consecutive times the previous generator (*i.e.* using a pair of quantum states of the class (4.1)), to map pairs of bit values to trit values (0,1,2) plus an additional undesired element "u". For instance, the players, after keeping only those bits obtained by coincident quadrature outputs $\pm x_0$, use two consecutive bits m and $m+1$ for the following association

$$\begin{aligned}(1,0) &\to \mathbf{0}\\ (0,1) &\to \mathbf{1}\\ (1,1) &\to \mathbf{2}\\ (0,0) &\to \boldsymbol{u}.\end{aligned}$$

Thus, by concatenating two invocations and using the above association, one generates the permutations corresponding to the primitive $\{(0,1,2),(0,2,1),(1,0,2),(1,2,0),(2,0,1),(2,1,0)\}$ plus a permutation of the undesired element "u" *i.e.* $(u,2,2)$, $(2,u,2)$ and $(2,2,u)$ which will be discarded during the protocol. With all these tools at hand, optimal results for the desired probabilities are achieved for a displacement vector of the form $d^T = -\frac{x_0}{3}(1,0,1,0,1,0)$, and yield

$$\begin{aligned}\delta_1 &= \mathcal{P}(1,1,1) = C(a,\sigma)\exp\left(-\frac{4}{3}\frac{x_0^2}{K_1}\right),\\ \delta_2 &= \mathcal{P}(0,0,0) = C(a,\sigma)\exp\left(-\frac{16}{3}\frac{x_0^2}{K_1}\right),\\ \delta_3 &= \mathcal{P}(0,0,1) = \mathcal{P}(0,1,0) = \mathcal{P}(1,0,0) =\\ &= C(a,\sigma)\exp\left[\frac{-4x_0^2\left(\sigma^2 + \frac{1}{4}\left[5a - \sqrt{9a^2-8}\right]\right)}{K_1K_2}\right],\end{aligned} \tag{4.5}$$

and

$$\begin{aligned}p &= \mathcal{P}(0,1,1) = \mathcal{P}(1,0,1) = \mathcal{P}(1,1,0) =\\ &= C(a,\sigma)\exp\left(-\frac{8}{3}\frac{x_0^2}{K_2}\right),\end{aligned} \tag{4.6}$$

with coefficients $K_1 = \sigma^2 + \frac{1}{2}\left[3a - \sqrt{9a^2-8}\right]$, $K_2 = \sigma^2 + \frac{1}{4}\left[3a + \sqrt{9a^2-8}\right]$, and pre-factor

$$\begin{aligned} C(a,\sigma) = & \left[\det\left(\frac{\gamma_M + \gamma(a)}{2}\right)\right]^{-\frac{1}{2}} = \\ = & \frac{8}{\left(a-c+\sigma^2\right)\left(b+c+\frac{1}{\sigma^2}\right)\sqrt{\left(a+2c+\sigma^2\right)\left(b-2c+\frac{1}{\sigma^2}\right)}}. \end{aligned}$$

The probability distribution depends on the parameters a, x_0 and σ. In the case $a \gg 1$, it can be seen that the conditional probabilities satisfy the following

$$\tilde{p} = \frac{1}{3} - \frac{4}{9}k + O(k^2), \quad \tilde{\delta}_i \to 0, \tag{4.7}$$

with $k = \exp\left[-\frac{4}{3}(\frac{x_0}{\sigma})^2\right]$. In the limit of a perfect, zero-uncertainty homodyne detection ($\sigma \to 0$), $\tilde{p}$ converges exactly to $1/3$. In general, there exists a large region in the parameters space for which $\tilde{p} \to \frac{1}{3}$ and $\tilde{\delta}_i \to 0$, as depicted in Fig. 4.1.

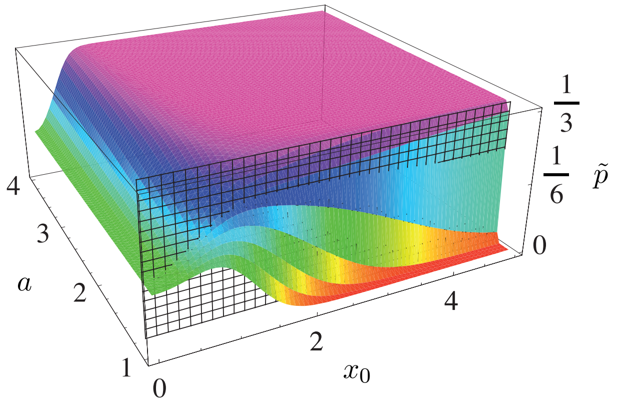

Figure 4.1: Plot of the conditional probability $\tilde{p}$ as a function of the measurement outcome x_0 and the shared entanglement a, for pure symmetric tripartite Gaussian resource states. Detectable broadcast is ideally solvable in the huge, unbounded region of $x_0 \gg 0$, $a \gg 1$, where $\tilde{p} \to 1/3$. The entanglement threshold $a = a_{\text{thresh}} = 5\sqrt{2}/6$ is depicted as well (wireframe surface). All the quantities plotted are adimensional.

However, there is a *lower* bound on the entanglement content of the symmetric Gaussian states of (4.1) in order to fulfill the above conditions. Only for $a \geq a_{\text{thresh}} = \frac{5\sqrt{2}}{6} \approx 1.18$, one has that $\tilde{p} > \tilde{\delta}_i$, which is a necessary condition to implement the primitive. This indicates that not all pure 3-mode symmetric fully entangled Gaussian states can be successfully employed to solve detectable broadcast via our protocol. This entanglement threshold is an *a priori* bound which does not depend on the specific form of the employed resource states. For any parametrization of the covariance matrix of $\hat{\rho}_a$, which is obtainable from $\gamma(a)$ by local unitary squeezing transformations (hence at fixed amount of tripartite entanglement), the same condition discriminating useful resource states is analytically recovered. We remark that this bound becomes tight in the limit $x_0 \to \infty$, meaning that $a \geq a_{\text{thresh}}$ becomes necessary *and* sufficient for the successful implementation of the primitive.

4.4 Distribution and test

We move now to the distribution and test part of the protocol which represents the first step in the execution of the appropriate primitive and has only two possible outputs: global success or global failure. In the case of failure, a player assumes that something went wrong during the execution of the protocol and aborts any further action. In the case of global success, each of the parties ends up with a set $\{K\}$ of classical data, and the protocol proceeds classically, according to the steps explained in section 4.2.

From now on we assume that the players share pairwise secure classical channels and secure (noiseless) quantum channels. The secure distribution and test part uses correlations to validate the fairness of the other parties. Therefore, quantum states are sent through noiseless quantum channels and measures are performed massively. In doing so, it is possible to detect manipulation of the data on a statistical basis and abort the protocol if necessary. In this section we mostly focus on the issue of security in the distribution and security test of the data. This should permit the detection of any malicious manipulation of the data. The explicit effects of sabotage actions will be reported in section 4.5. We postpone the important issue of how well the protocol will succeed in the case that the outputs of the measurements are not perfectly correlated considering the efficiency issue while asserting security, as well as the realistic practical implementation considering noise in the preparation of the states to section 4.6.

The distribution and test part proceeds as follows:

i-1) Without loosing generality, let us assume that R_1 prepares a large number, M, of tripartite systems in state $\hat{\rho}_a$ (*i.e.* with covariance matrix $\gamma(a)$ and displacement d) and sends one subsystem to S and another to R_0.

i-2) R_1 wants to check if the distribution of states is faithfully achieved. To this aim she/he chooses randomly a set of indices for player S, $\{K_S\}$, and a disjoint set of indices for player R_0, $\{K_{R_0}\}$, and sends these two sets over secure classical channels to the corresponding players. Player S sends his/her K_S subsystems to player R_0. For each $m \in \{K_S\}$, R_0 measures the two subsystems in his/her possession and R_1 measures his subsystem. After communication of their results over secure classical channels, they agree on those indices $\{\tilde{K}_S\} \subseteq \{K_S\}$ for which $|x_{R_0}| = |x_{R_1}| = x_0$. R_1 and R_0 check now whether the correlations predicted by the primitive occur: $\tilde{p} = \tilde{\mathcal{P}}(011) = \tilde{\mathcal{P}}(101) = \tilde{\mathcal{P}}(110) = \frac{1}{3}$, $\tilde{\delta}_i = 0$. If the test was successful, *i.e.* if the measurement results were consistent with the assumption that the states have been distributed correctly, the players $i \in \{R_0, R_1\}$ set the flag $f_i = 1$, otherwise $f_i = 0$. In an analogous way, the test is performed for S.

i-3) Players S, R_0 and R_1 send their flags to each other. Every player who receives a flag "0", sets his flag also to "0". Every player with flag "0" aborts the protocol. Otherwise the execution of the protocol proceeds. This step terminates the distribution and test of the quantum systems.

In the second phase of the protocol a selection of the distributed systems is chosen to establish the bit sequences which will be used to implement the quantum primitive. In this phase, again honest parties may abort the protocol if malicious manipulations occur.

ii-1) The players S, R_0 and R_1 agree upon a set of systems which have not been discarded during the distribution and test part.

ii-2) Player S chooses (randomly) two disjoint sets of subsystems labeled by indices $L_S^i \subset \tilde{M}$. He/she sends the set L_S^i to player i and demands player i to send via a noiseless quantum channel his/her subsystems $m \in L_S^i$ to him/her. In each case, the (random) choice L_S^i is secret to party j, *i.e.* player R_1 has no information whatsoever about the set $L_S^{R_0}$. An analogous procedure is adopted by R_0 and R_1.

ii-3) After measuring their whole sequence of subsystems, player $i \in \{S, R_0, R_1\}$ announces publicly, the set of indices $\{\hat{M}_i^m\} \in \hat{M}_i$ for which the output of the quadrature measurement was $|x_0|$. The order in which the players announce their measurement results can be specified initially and based *e.g.* on a rotation principle. (Notice that the announcement of $|x_i| = x_0$ during the actual measurement phase would make possible an effective traitor strategy, since he could manipulate combinations on a systematic basis).

ii-4) Without loss of generality, let us explicitly describe this step of protocol for player S. From the following sets $L_S^{R_0} \cap \hat{M}_{R_1}^m =: U_S^{R_1}$ and $L_S^{R_1} \cap \hat{M}_{R_0}^m =: U_S^{R_0}$ let $\tilde{U}_S^{R_i} \subseteq U_S^{R_i}$ for $i \in \{0,1\}$ be the index set for which the player S measured $\pm x_0$ twice. Analogously to the first phase of the protocol, player S can test if the outputs of his measures agree with the correlations of a proper primitive ($\tilde{\mathcal{P}}(00) = \tilde{\mathcal{P}}(10) = \tilde{\mathcal{P}}(01) = 1/3$ and $\tilde{\mathcal{P}}(11) = 0$) If the test is successful, the player sets his flag $f_S = 1$, otherwise $f_S = 0$. The same procedure is analogously performed by R_0 and R_1. From this step on, the players deal exclusively with the outputs of their measures, *i.e.* classical data and secure classical channels.

ii-5) S checks correlation on his outputs in the following set $\hat{M} := \hat{M}_S^m \cap \hat{M}_{R_0}^m \cap \hat{M}_{R_1}^m \subseteq \hat{M}_S^m$. If the test is successful, S sets his flag $f_S = 1$, otherwise $f_S = 0$. R_0 and R_1 do the equivalent step.

ii-6): From a randomly chosen set $V^S \subset \hat{M}$ player S demands from R_0 and R_1 their measurement results. S tests this control sample for the assumed primitive. If the test is successful, S sets his flag $f_S = 1$, otherwise $f_S = 0$. R_0 (R_1) perform this step with a set $V^{R_0} \subset \hat{M} \backslash V^S$ ($V^{R_1} \subset \hat{M} \backslash (V^S \cup V^{R_0})$) respectively.

ii-7) Every player with a flag 0 aborts the execution of the protocol. Otherwise the players agree upon a set $W := \hat{M} \backslash (V^S \cup V^{R_0} \cup V^{R_1})$ as the result of the invocation of the primitive, which consists in an even number of elements. This step concludes the distribution part of the protocol.

4.5 Primitive: Errors and manipulations

We analyze here the effects of malicious manipulations of the data by dishonest parties and its detection by the honest ones. We examine here two possible sources of error, which can occur during the implementation of the primitive with Gaussian states. While the first source is inherent to the system, the second is caused by an active adversary intervention of a participating party. The inherent error is caused by the occurrence of non-consistent combinations on the invocation of the primitive, that is, the occurrence of outputs $(1,1,1)$, $(0,0,0)$, $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$ has to be considered. This error will propagate along the protocol, so that the probability of finding a combination which is not appropriate is bounded from above from $\eta = 1-(3\tilde{p})^2$.

The second source of errors we want to discuss here corresponds to the local actions that one of the players could do in order to manipulate the measurement results of other players. For instance, let us assume that the player R_0 has malicious intentions and wants to shift the local component of the displacement vector of the distributed state using local transformations. Please note that a shift of the quadrature output x_0, provides the same error in the probability distribution of the outputs as a shift in the corresponding displacement vector. In other words, both types of manipulations produce the same change in the probabilities as calculated in Eq. (4.4). Parameterizing the shift in the displacement vector by the parameter λ, $d^T \mapsto (d')^T = -\frac{x_0}{3}(1,0,1,0,\lambda,0)$, it is interesting to see how that affects the conditional probabilities $\tilde{p}$ and $\tilde{\delta}_i$. If probabilities were changed, player R_0 could try to determine (via subsequent communication with the other players (step ii-3))), with certain probability, the occurrence of the outputs of the other players, thereby gaining additional information. Notice also that S and R_1 cannot realize the local manipulation of R_0 without classical communication between them. This can be trivially seen by realizing that the partial trace $\mathrm{tr}_{R_0}(\hat{\rho}_a(\gamma, d')) = \int \mathcal{W}'_\xi dx_{R_0} dp_{R_0} = \mathcal{W}'_\xi(\gamma_{S,R_1}, d_{S,R_1}) = \mathrm{tr}_{R_0}(\hat{\rho}_a(\gamma, d))$ with

$$\gamma_{S,R_1} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & b & 0 & -c \\ c & 0 & a & 0 \\ 0 & -c & 0 & b \end{pmatrix} \quad \text{and} \quad d_{S,R_1} = \begin{pmatrix} x_1 \\ 0 \\ x_1 \\ 0 \end{pmatrix}. \tag{4.8}$$

Thus the most plausible strategy for a traitor could consist on the following: (i) discrediting honest players by manipulating the displacement vector in such a way that non-consistent combinations appear, (ii) hide successful measurements to the honest players which result in combinations that might be disadvantageous. It is tedious but straightforward to show that by making use of the test steps ii-4)-ii-6) honest parties can detect the effects of such manipulations.

4.6 Efficient realistic implementation

In this section we focus on the efficiency of the proposed protocol and we extend our results to a realistic practical scenario, relaxing the conditions for the obtention of correlated outputs between the players and assuming noise in the preparation of the input states.

The protocol, as discussed in the previous sections, constitutes a nice proof-of-principle of the fact that detectable broadcast is solvable in the CV scenario using multipartite Gaussian entanglement. However, it suffers from its reliance on two main idealizations which render the practical implementation of the primitive unrealistic, or, better said, endowed with zero efficiency. Specifically, we have requested that (i) a *pure* tripartite symmetric Gaussian state is distributed as the entangled resource; and (ii) when the three parties measure (via homodyne detection) the position of their respective modes, their measurement is taken to be ideal, that is not affected by any uncertainty, and moreover all parties have to obtain, up to a sign, *the same* outcome x_0. In reality, assumption (i) is unjustified as inevitable imperfections and losses result instead in the production of mixed thermalized states; on the other hand, the probability associated to measurements under assumption (ii), and hence the probability of achieving broadcast, is vanishingly small [1]. It is interesting, in view of potential practical implementations of our scheme, to study here how its success is affected, and possibly guaranteed, by relaxing the above two assumptions.

To deal with (i), let us recall that the tripartite entangled Gaussian states of (4.1) can be produced in principle by letting three independently squeezed beams (one in momentum, and two in position) interfere at a double beam-splitter, or "tritter" [56], as proposed by van Loock and Braunstein [49]. In practice, the parametric non-linear process employed to squeeze the vacuum is affected by losses which result in the actual generation of squeezed *thermal* states in each single mode. Before the tritter, one then has three independent Gaussian modes with covariance matrices $\gamma_1^{\rm in}(s,n) = {\rm diag}\{ns,\, n/s\}$, $\gamma_2^{\rm in}(s,n) = \gamma_3^{\rm in}(s,n) = {\rm diag}\{n/s,\, ns\}$, respectively, where $s = \exp(2r)$ (with r the squeezing degree in each single mode) and $n \geq 1$ is the noise parameter affecting each mode. The noise n is related to the initial marginal purity $\mathcal{P}_k^{\rm in}$ of each single mode by $n = 1/\mathcal{P}_k^{\rm in}$, and corresponds to a mean number of thermal photons given by $\bar{n}^{\rm th} = (n-1)/2$. For $n = 1$, each mode is in the ideally pure squeezed vacuum state. After the tritter operation, described by the symplectic matrix [49, 56, 57]

$$S_{ttt} = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & \sqrt{\frac{2}{3}} & 0 & 0 \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & -\frac{1}{\sqrt{6}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix},$$

the output covariance matrix of the three modes is given precisely by

$$\gamma^{\text{out}} = S_{ttt} \cdot [\gamma_1^{\text{in}}(s,n) \oplus \gamma_2^{\text{in}}(s,n) \oplus \gamma_3^{\text{in}}(s,n)] \cdot S_{ttt}^T = n\gamma(a), \tag{4.9}$$

where $\gamma(a)$ is defined in (4.1) and we have made the identification $a = (s^2+2)/(3s)$. Eq. (4.9) describes generally mixed, fully symmetric three-mode Gaussian states, with global purity given by $\mathcal{P} = n^{-3}$, thus reducing to the pure instance of (4.1) for $n = \mathcal{P} = 1$. Recall that any additional losses due *e.g.* to an imperfect tritter and/or to the distribution and transmission of the three beams can be embedded into the initial single-mode noise factor n, so that (4.9) provides a realistic description of the states produced in experiments [50, 58]. We therefore consider this more general family of Gaussian states as resources to implement the CV version of the primitive. It may be interesting to recall that also for the general family of states of (4.9) the genuine tripartite entanglement is exactly computable [57] in terms of the residual contangle [52], and as expected, it increases with a and decreases with n.

Concerning the idealization (ii) discussed above, for an efficient implementation we should first of all consider the realistic case of non-ideal homodyne detections, which means that the outcomes are affected by uncertainties quantified by the parameter σ, see (4.4). Furthermore, we should let the parties measure within a finite range, which means specifically that in each measurement run the expected values for the measurement outcomes of the receivers can be shifted of some quantity Δ with respect to the corresponding expectation value of the sender's homodyne detection. So, what we should ask for is that the parties (one sender S and two receivers R_0 and R_1) agree on those outcomes of their measurement results for which $|\hat{x}_S| = x_0 > 0$ and $|\hat{x}_{R_0}|, |\hat{x}_{R_1}| = (x_0 + \Delta) > 0$, once the sender has announced his/her output results x_0 to the other two parties.

Here, the actual results of each measurement are assumed to distribute according to a Gaussian function centered at x_0 (for the sender) and $x_0 + \Delta$ (for the receivers), respectively, with a variance σ. Now the associated events occur with a finite probability. We wish to investigate for which range of the positive shift $\Delta \in [\Delta_{\text{min}}, \Delta_{\text{max}}]$, being $\Delta_{\text{max}} - \Delta_{\text{min}}$ the range, the conditional probability $\tilde{p}$ still approaches 1/3. The wider such range, the higher the probability of success, or efficiency, of the protocol; of course the regions in the space of parameters such that the primitive can be efficiently implemented will depend on the specific boundaries Δ_{min} and Δ_{max} and not only on their difference. Notice than in order to ensure that the sign of the quadratures does not change when allowing a finite range of valid output values (and therefore, correlations between classical bits are properly extracted (see section 4.3)), we always demand the shift Δ to be positive.

This condition can be further relaxed allowing for a non-symmetric range of permitted values around the broadcasted value x_0 but constraining only the absolute value of the shift as $|\Delta_{\text{min}}| < x_0$, ensuring that the sign of the correlations remains unchanged. This extra condition, which could be straightforwardly included in our expressions if one aims at maximizing the efficiency of our protocol, does not modify the analysis of the realistic implementation of the protocol we perform in this section. For the sake of clarity, we remark once again the role of the parameter Δ: allowing a non-zero shift Δ in the computation of the probability $\tilde{p}$, means considering the realistic case in which the outcomes of the measurements performed by each receiver can be not coincident with each other, and not coincident even with the corresponding broadcasted value of x_0. In what if follows we show that the protocol can be run successfully provided that the deviations $|x_{R_0}| - |x_S|$ and $|x_{R_1}| - |x_S|$ (in each run) both lie in between a $\Delta_{\rm min}$ and a $\Delta_{\rm max}$, which will be determined in the following.

To this aim, we can perform an analysis similar to the one of section 4.3, but considering in full generality a non-unit noise factor n, a non-zero uncertainty σ, and a non-zero shift Δ. The calculations of the probabilities follow straightforwardly along the lines of the special (unrealistic) case previously discussed, obtaining

$$\begin{aligned}\tilde{p} \;=\; & \Bigg\{ 3 + 3\mathrm{e}^{-\frac{4(\Delta+x_0)\left[\Delta\left(4\sigma^2+7a-3R\right)+\left(4\sigma^2+3a+R\right)x_0\right]}{9n\left(4\sigma^4+9a\sigma^2-R\sigma^2+4\right)}} + \\ & + \mathrm{e}^{\frac{4x_0\left[4(a-R)\Delta+\left(4\sigma^2+9a-5R\right)x_0\right]}{9n\left(4\sigma^4+9a\sigma^2-R\sigma^2+4\right)}} + \mathrm{e}^{-\frac{32(\Delta+x_0)\left[\Delta\left(\sigma^2+a\right)+\left(\sigma^2+R\right)x_0\right]}{9n\left(4\sigma^4+9a\sigma^2-R\sigma^2+4\right)}} \Bigg\}^{-1}, \end{aligned} \tag{4.10}$$

with $R = \sqrt{9a^2 - 8}$. We find that in the parameter space of a (regulating the entanglement), n (regulating the mixedness), x_0 (regulating the measurement outcome), σ (regulating the measurement uncertainty) and Δ (regulating the measurement shift), there exists a surface which acts as the boundary for the regime in which our primitive can be faithfully implemented, yielding a feasible, robust solution to the broadcast problem. This surface is obtained by requiring that $\tilde{p} = 1/3 - \epsilon$, with the deficit ϵ chosen arbitrarily small. The result is plotted in Fig. 4.2 for $\epsilon = 10^{-7}$ in the three-dimensional space of parameters $x_0/\sqrt{n}$, $\Delta/\sqrt{n}$, and a, for different values of σ.

We consider the primitive as efficiently implementable in the whole region such that $1/3 - \epsilon \leq \tilde{p} \leq 1/3$, which spans the volume above the surface of Fig. 4.2. Notice that for $\sigma = 0$, $n = 1$, and $\Delta_{\rm max} \rightarrow \Delta_{\rm min} \rightarrow 0$, such an useful volume shrinks to a two-dimensional slice (with $a \geq 5\sqrt{2}/6$) which represents the parameter range in which the "ideal" implementation described in section 4.3 is successful.

The figure offers several reading keys. Let us investigate independently how the possibility of solving detectable broadcast via our protocol depends on the individual parameters. For simplicity, we will consider n fixed and eventually discuss its role. We will also for the moment keep the idealization of error-free homodyne measurements ($\sigma = 0$), corresponding to Fig. 4.2(a) which makes the subsequent discussion more tractable. However we will relax such an assumption in the end to show that a realistic description of the homodyne measurement does not significantly affect the performance and the applicability of the protocol. This validates the claims of efficiency that we make in the following.

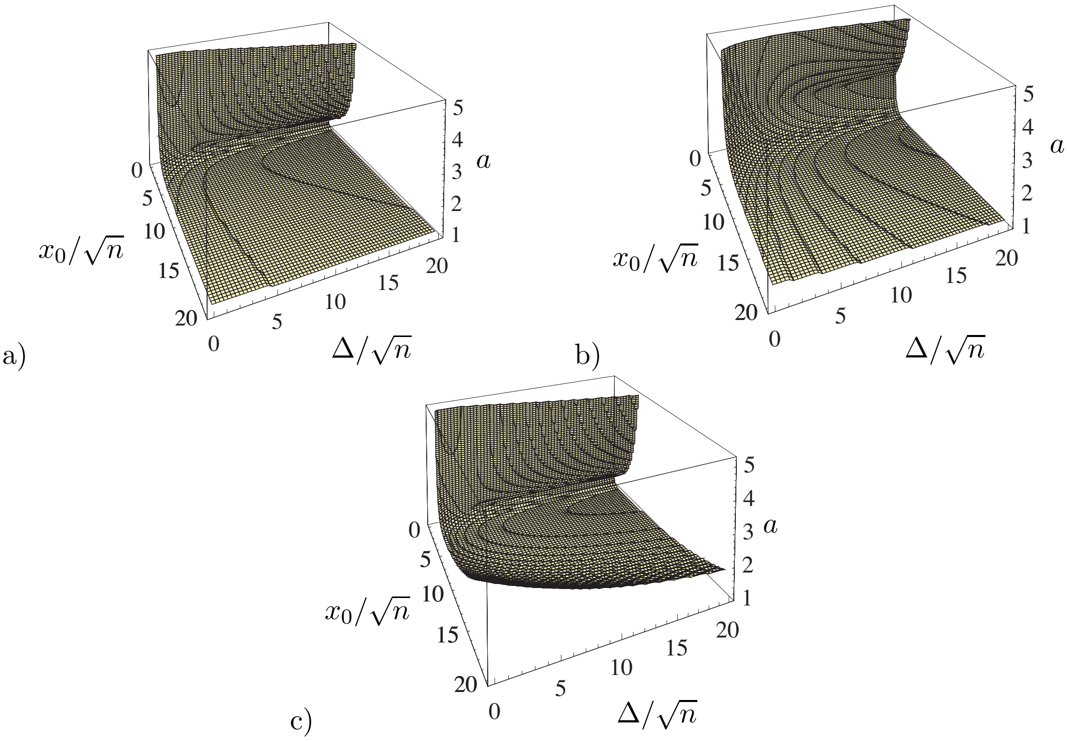

Figure 4.2: Plots, in the space of $x_0/\sqrt{n}$ (quadrature measurement normalized to noise), $\Delta/\sqrt{n}$ (measurement shift normalized to noise), and a (shared entanglement), of the boundary to the useful region for which $\tilde{p} = 1/3 - \epsilon$ ($\epsilon = 10^{-7}$), at different values of the homodyne detection uncertainty (a) $\sigma = 0$ (ideal error-free measurement), (b) $\sigma = 1$ (fixed error, independent of the outcome), and (c) $\sigma = x_0/10$ (proportional error, corresponding to a 90% efficiency in the detectors). Detectable broadcast can be solved efficiently, by means of our protocol, for all values of the parameters which lie above the depicted surface. See text for an extended discussion. All the quantities plotted are adimensional.

4.6.1 Entanglement role

Let us henceforth start with the dependence of the solution on a. Somehow surprisingly, there exist lower *and upper* bounds on the tripartite entanglement such that only for $a_{\min} \leq a \leq a_{\max}$ the protocol achieves a solution. The bounds naturally depend on x_0 and Δ. Specifically, we observe that $a_{\min}$ diverges for $\Delta = 0$ and $x_0 \to 0$, meaning that no feasible solution can be achieved in the low-Δ, low-x_0 regime; the reason being that near $x_0 = 0$ there is not possibility of associating the classical bits "0" and "1" to positive/negative values of the quadratures. The lower bound then goes down reducing to the already devised threshold of $a_{\text{thresh}} = 5\sqrt{2}/6$ for Δ close to zero and $x_0 \gg 0$, and eventually converges to $a = 1$ (*i.e.* all entangled states are useful) for any finite $x_0 \gg 0$ and $\Delta \to \infty$. On the other hand, the upper bound on a, which surprisingly rules out states with too much entanglement, is obviously diverging at $\Delta = 0$ but becomes finite and relevant in the regime of small x_0 and large Δ, eventually reducing to $3/2$ for any finite x_0 and $\Delta \to \infty$.

Summarizing, the two extremal regimes corresponding to $\Delta = 0$ on one hand and $\Delta \to \infty$ on the other hand, both allow a solution of detectable broadcast via our protocol: the main difference is that in the former case one needs states with an entanglement above $a_{\min} = 5\sqrt{2}/6$, while in the latter case one needs states whose entanglement is below $a_{\max} = 3/2$. The regime of finite shift Δ interpolates between these two limits. This means, in terms of useful range, and hence of efficient implementations, that if one is able to produce entangled states precisely with $5\sqrt{2}/6 < a < 3/2$, the protocol is implementable with high efficiency for *any* shift $\Delta \in [0, \infty)$ in the measurement outcomes. *i.e.* with *an infinite range of variability* allowed for the acceptable data resulting from homodyne detections performed by the receivers, for a given outcome x_0 of the sender. This information is important in view of practical implementations, and becomes especially valuable since the engineering of the required entangled resources appears feasible: a squeezing between $4, 5$ and 6 dB is required in each single mode, which is currently achieved in optical experiments [59, 60, 61].

4.6.2 Measurement outcomes role

For a fixed entangled resource, a, Fig. 4.2(a) alternatively, shows that there exist minimum thresholds both for x_0 and Δ in order to achieve a solution to detectable broadcast. While the useful range for x_0 is always unbounded from above, we find that, interestingly, an upper bound $\Delta_{\max}$ exists for $a > 3/2$. Precisely, for a given $a > 3/2$, with increasing x_0 we observe that $\Delta_{\min}$ decreases and $\Delta_{\max}$ increases, *i.e.* the useful range spanned by Δ widens. Conversely, at a given x_0, $\Delta_{\max}$ decreases with increasing entanglement a, reducing the parameter space in which a solution can be found. Consistently with the previous discussion, we conclude again that in realistic conditions ($\Delta > 0$) it is better to have a moderate amount of shared entanglement to solve broadcast with optimal chances.

4.6.3 Thermal noise role

Now, let us note that the noise parameter n simply induces a rescaling of both x_0 and Δ, in such a way that with increasing n the surface bounding the useful range of parameters shrinks, as it could be guessed (the noise degrades the performance of the protocol). Still, with typical noise factors characterizing experimental implementations, *e.g.* $n = 2$, the protocol appears very robust and the solution is still achievable, for a given amount of entanglement (say $a \lesssim 3/2$), provided that x_0 and Δ exceed $\sqrt{2}$ times their respective minimum thresholds obtained for ideally pure resources ($n = 1$).

4.6.4 Homodyne efficiency role

Finally, let us address the important issue of the uncertainty affecting homodyne detections. Any realistic measurement is characterized by a non-zero σ. We have explicitly studied two situations, one in which the absolute error is fixed, corresponding to a constant σ (see Fig. 4.2(b)), and another in which the relative error is fixed to 10%, corresponding to a σ proportional to the measurement outcome x_0 (see Fig. 4.2(c)). The result is that, in both cases, for not exceedingly high values of the error factor, the useful region is obviously reduced but, crucially, the possibility of achieving detectable broadcast via our protocol is still guaranteed in a broad range of values of the parameters. Specifically, as somehow expected, the error model in which σ is proportional to the measurement outcome results in a more consistent modification (shrinkage) of the useful surface, while almost nothing happens in the case of fixed, small σ. In particular, upper bounds on x_0 arise for a practical realization in presence of a proportional error, or in other words due to a limited efficiency in the detection. A significant portion of the parameter space anyway remains valid for a workable implementation of the primitive. Our scheme is thus robust also with respect to the imperfections in the quadrature measurements. We draw the conclusion that the protocol we designed is truly efficient and realistically implementable in non-ideal conditions.

We explicitly depicts $\tilde{p}$, (4.10), for sensible resource values of $a = 3/2$ and $n = 2$, as a function of x_0 and Δ, and according to different values of σ like in Fig. 4.2.

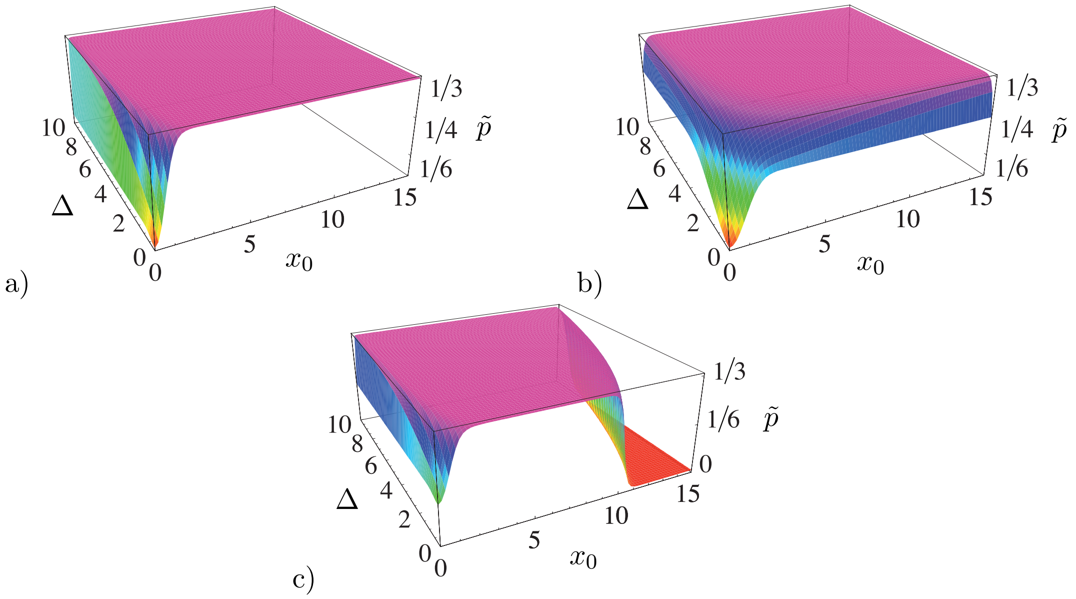

Figure 4.3: Plots of the conditional probability $\tilde{p}$ as a function of the measurement outcome x_0 for the sender and the shift Δ of the measurement outcomes for the receivers, for realistically mixed Gaussian resource states with $n = 2$ and $a = 3/2$. The uncertainty in the homodyne detection is taken to be (a) $\sigma = 0$, (b) $\sigma = 1$, and (c) $\sigma = x_0/10$. Detectable broadcast is *efficiently* solvable in the wide plateau region where $\tilde{p} \to 1/3$. All the quantities plotted are adimensional.

We notice a huge (unbounded from above in the ideal case $\sigma = 0$) region (see Fig. 4.3) in which $\tilde{p} \to 1/3$, yielding an efficient solution to detectable broadcast via our protocol. We have thus identified an optimal "work-point" in terms of the parameters describing the shared Gaussian states, and we have defined the frontiers of application of our scheme in the laboratory practice. In this way, together with the explicit steps of the protocol presented in the previous sections, we obtain a clear-cut recipe for a CV demonstration of detectable broadcast, that we hope it can be experimentally implemented in the near future.

For the sake of completeness, let us mention that from (4.10) we analytically find that $\tilde{p}$ converges *exactly* to 1/3 only in the following limiting cases (for a given finite n and $\sigma = 0$): (i) $a \to \infty$ with $\Delta < 3x_0$; (ii) $x_0 \to \infty$ with $a \geq 5\sqrt{2}/6$; (iii) $\Delta \to \infty$ with $1 < a \leq 3/2$.

4.7 Conclusions

We have proposed in this chapter a protocol to solve detectable broadcast with entangled Continuous Variable using Gaussian states and Gaussian operations only. Our algorithm relies on genuine multipartite entanglement distributed among the three parties, which specifically have to share two copies of a three-mode fully symmetric Gaussian state. Interestingly, we have found that nevertheless not all entangled symmetric Gaussian states can be used to achieve a solution to detectable broadcast: a minimum threshold exists on the required amount of multipartite entanglement. We have moreover analyzed in detail the security of the protocol.

In its ideal formulation, our protocol requires that the parties share pure resource states, and that the outcomes of homodyne detections are perfectly coincident and not affected by any uncertainty; this however entails that our protocol achieves a solution with vanishing probability. To overcome such a practical limitation, we have eventually considered a more realistic situation in which the tripartite Gaussian resources are affected by thermal noise, and, more importantly, the homodyne detections are realistically imperfect, and there is a finite range of allowed values for the measurement outcomes obtained by the parties. We have thoroughly investigated the possibility to solve detectable broadcast via our protocol under these relaxed conditions.

As a result, we have demonstrated that there exists a broad region in the space of the relevant parameters (noise, entanglement, range of the measurement shift, measurement uncertainty) in which the protocol admits an efficient solution. This region encompasses amounts of the required resources which appear attainable with the current optical technology (with a legitimate trade-off between squeezing and losses). We can thus conclude that a feasible, robust implementation of our protocol to solve detectable broadcast with entangled Gaussian states may be in reach. This would represent another important demonstration of the usefulness of genuine multipartite Continuous Variable entanglement for communication tasks, coming to join the recent achievement of a quantum teleportation network [50].

Chapter 5

Classical versus Quantum correlations in Continuous Variable

5.1 Introduction

In the previous chapters via a digitalization procedure we have been able to distill classical correlations from entangled Gaussian states in such a way that we have been able to implement protocols for either cryptographic or detectable broadcast purpose. In this chapter we want to relate the performance on extracting classical correlations from entangled states to the quantum correlations embedded in the states. While Gaussian states (coherent, squeezed, and thermal states) have been originally the preferred resources for both theoretical and practical implementations, a new frontier emerges with non-Gaussian states (Fock states, macroscopic superposition like Schrödinger's cat states, etc.). The latter can be highly non-classical, possess in general "more entanglement" than Gaussian states [62], and allow to overcome some limitations of the Gaussian framework like entanglement distillation [63, 64, 16] and universal quantum computation [65]. Therefore, it is of central relevance to provide proper ways to quantify also non-Gaussian entanglement in an experimental approachable way.

At a fundamental level, the difficulty in the investigation of entanglement (quantum correlations) can be traced back to the subtle task of distinguishing it from classical correlations [66]. Correlations can be regarded as classical if they can be induced onto the subsystems solely by local operations and classical communication, necessarily resulting in a mixed state. On the other hand, if a pure quantum state displays correlations between the subsystems they are of genuinely quantum nature (entanglement). We adopt here a pragmatic approach: if two systems are *in toto* correlated, then this correlation has to be retrieved between the outcomes of some local measurements performed on them. In this chapter, therefore, we investigate quadrature correlations in Continuous Variable (CV) states. We are also motivated by the experimental adequacy: field quadratures can be efficiently measured by homodyne detection, without the need for complete state tomography. Specifically, we study optimal correlations in bit strings obtained by digitalizing the outcomes of joint quadrature measurements on a bipartite two-mode CV system.

5.2 Quadrature measurements and bit correlations.

To study bipartite CV systems we use the well known fact that any NPPT Gaussian state of $N \times M$ modes can be mapped by Gaussian Local Operations and Classical Communication (GLOCC) to an NPPT symmetric state of 1×1 modes *i.e.* preserving the amount of entanglement. Then, for the most general scenario it is sufficient to consider a bipartite CV system of two bosonic modes, A and B. The probability distribution associated to a single/joint measurement of arbitrary rotated quadratures $\hat{x}_A(\theta)$ and $\hat{x}_B(\varphi)$ providing outcomes x_A^θ and x_A^φ, is given by

$$\begin{aligned}
\mathcal{P}_A(x_A^\theta) &= \mathrm{tr}[\hat{\rho}_A \hat{U}_\theta^{A\dagger} \hat{\sigma}(x_A) \hat{U}_\theta^A], && (5.1)\\
\mathcal{P}_{AB}(x_A^\theta, x_B^\varphi) &= \mathrm{tr}[\hat{\rho}_{AB}(\hat{U}_\theta^A \otimes \hat{U}_\varphi^B)(\hat{\sigma}(x_A) \otimes \hat{\sigma}(x_B))(\hat{U}_\theta^{A\dagger} \otimes \hat{U}_\varphi^{B\dagger})] = \\
&= \mathrm{tr}[(\hat{U}_\theta^{A\dagger} \otimes \hat{U}_\varphi^{B\dagger})\hat{\rho}_{AB}(\hat{U}_\theta^A \otimes \hat{U}_\varphi^B)(\hat{\sigma}(x_A) \otimes \hat{\sigma}(x_B))] = \\
&= \mathrm{tr}[\rho_{AB}(\hat{\sigma}(x_A^\theta) \otimes \hat{\sigma}(x_B^\varphi))] = \mathrm{tr}[\hat{\rho}_{AB}^{\theta,\varphi}(\hat{\sigma}(x_A) \otimes \hat{\sigma}(x_B))], && (5.2)
\end{aligned}$$

where $\hat{\sigma}(x_A)$ is a single-mode Gaussian (squeezed) state with first moments $\{x_A, 0\}$ and covariance matrix $\mathrm{diag}\{\sigma^2, 1/\sigma^2\}$. Here $\hat{U}_\theta^A$ is a unitary operator describing a rotation of θ on mode A, corresponding to a symplectic transformation given by $S_{\theta,A} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. Likewise for B. Thus, one can either measure the rotated quadrature (x_A^θ, x_B^φ) on the state (passive view) or antirotate the state ($\hat{\rho}_{AB}^{\theta,\varphi}$) and measure the unrotated quadrature (active view).

To digitalize the obtained output quadrature measurements that spread in a continuum we assign the bits $+$ $(-)$ to the positive (negative) values of the measured quadrature. This digitalization transforms each joint quadrature measurement into a pair of classical bits. A string of such correlated bits can be used *e.g.* to distill a quantum key [33, 1]. Let us adopt a compact notation by denoting (at given angles θ, φ) $\mathcal{P}_A^\pm \equiv \mathcal{P}_A(\pm|x_A^\theta|)$, and $\mathcal{P}_{AB}^{\pm\mp} \equiv \mathcal{P}_{AB}(\pm|x_A^\theta|, \mp|x_B^\varphi|)$. The conditional probability that the bits of the corresponding two modes coincide is given by $\mathcal{P}_{AB}^{=} \equiv (\mathcal{P}_{AB}^{++} + \mathcal{P}_{AB}^{--})/\sum_{\{\alpha=\pm,\beta=\pm\}} \mathcal{P}_{AB}^{\alpha\beta}$. Correspondingly, the probability that they differ is $\mathcal{P}_{AB}^{\neq} \equiv (\mathcal{P}_{AB}^{+-} + \mathcal{P}_{AB}^{-+})/\sum_{\{\alpha=\pm,\beta=\pm\}} \mathcal{P}_{AB}^{\alpha\beta}$. Trivially, $\mathcal{P}_{AB}^{=} + \mathcal{P}_{AB}^{\neq} = 1$. If $\mathcal{P}_{AB}^{=} > \mathcal{P}_{AB}^{\neq}$ the measurement outcomes display correlations, otherwise they display anticorrelations. Notice that, if the two modes are completely uncorrelated, $\mathcal{P}_{AB}^{=} = \mathcal{P}_{AB}^{\neq} = 1/2$. For convenience, we normalize the *degree* of bit correlations as

$$\mathcal{B}(|x_A^\theta|, |x_B^\varphi|) = 2|\mathcal{P}_{AB}^{=} - 1/2| = |\mathcal{P}_{AB}^{=} - \mathcal{P}_{AB}^{\neq}|, \tag{5.3}$$

so that for a completely uncorrelated state $\mathcal{B}(|x_A^\theta|,|x_B^\varphi|)=0$. The interpretation of (5.3) in terms of correlations is meaningful if a *fairness* condition is satisfied: locally, on each single mode, the marginal probabilities associated to the outcomes "+" or "−" must be the same: $\mathcal{P}_A^+ = \mathcal{P}_A^-, \quad \mathcal{P}_B^+ = \mathcal{P}_B^-$ otherwise, (5.3) can systematically display false correlations due to individual unbiasedness.

For a two-mode CV system, whose state is described by a Wigner function $\mathcal{W}$, we define the *"bit quadrature correlations"* Q as the average probability of obtaining a pair of classically correlated bit (in the limit of zero uncertainty) optimized over all possible choices of local quadratures

$$Q(\hat{\rho}) = \sup_{\theta,\varphi} \int\int dx_A^\theta dx_B^\varphi \bar{\mathcal{W}}(x_A^\theta, x_B^\varphi)[\lim_{\sigma\to 0} \mathcal{B}^\sigma(|x_A^\theta|,|x_B^\varphi|)], \tag{5.4}$$

where $\bar{\mathcal{W}}(x_A^\theta, x_B^\varphi) = \int\int dp_A^\theta dp_B^\varphi \mathcal{W}(x_A^\theta, p_A^\theta, x_B^\varphi, p_B^\varphi)$ is the marginal Wigner distribution of the (rotated) positions, and $\{x_A^\theta, p_A^\theta, x_B^\varphi, p_B^\varphi\} = [S_\theta \oplus S_\varphi]\{x_A, p_A, x_B, p_B\}$. We demonstrate numerically (for all clases of Gaussian and non-Gaussian states discussed) that we can write Eq. (5.4) as

$$Q(\hat{\rho}) = \sup_{\theta,\varphi} |E_{A,B}^{\theta,\varphi}(\hat{\rho})| = \sup_{\theta,\varphi} |\int\int dx_A^\theta dx_B^\varphi \bar{\mathcal{W}}(x_A^\theta, x_B^\varphi)\mathrm{sgn}(x_A^\theta x_B^\varphi)|, \tag{5.5}$$

where $E_{A,B}^{\theta,\varphi}(\hat{\rho}) = \int\int dx_A^\theta dx_B^\varphi \bar{\mathcal{W}}(x_A^\theta, x_B^\varphi)\mathrm{sgn}(x_A^\theta x_B^\varphi)$ is the "sign-binned" quadrature correlation function, which has been employed, *e.g.*, in proposed tests of Bell inequalities violation for CV systems.

A homodyne Bell test requires measuring two different rotated quadratures per mode, to achieve violation of the bound [67, 68, 69, 70] $|E_{A,B}^{\theta,\varphi} + E_{A,B}^{\theta',\varphi} + E_{A,B}^{\theta,\varphi'} - E_{A,B}^{\theta',\varphi'}| \leq 2$. Here, we propose to measure a single quadrature per mode, which displays one-shot optimal correlations, unveiling a powerful quantitative connection with Gaussian and non-Gaussian entanglement measured through negativity. While this form is more suitable for an analytic evaluation on specific examples, the definition (5.4) is useful to prove the general properties of Q [1] that we analyze here.

Lemma 5.2.1 Normalization: $0 \leq Q(\hat{\rho}) \leq 1$.

Proof. *It follows from the definition of $Q(\hat{\rho})$, as both $\mathcal{B}$ and the marginal Wigner distribution range between* 0 *and* 1. □

Lemma 5.2.2 Zero on product states: $Q(\hat{\rho}_A \otimes \hat{\rho}_B) = 0$.

Proof. *For a product state the probabilities factorize* i.e. $\mathcal{P}_{AB}^{\alpha\beta} = \mathcal{P}_A^\alpha \mathcal{P}_B^\beta$ *and so* $\mathcal{P}_{AB}^{=} = \mathcal{P}_{AB}^{\neq}$*, where we have used the fairness condition. Namely $\mathcal{B} = 0$, hence the integral in* (5.4) *trivially vanishes.* □

[1] Fair states have necessarily zero first moments, which can be assumed without loss of generality. In general, one could take in (5.4) the difference between $\mathcal{B}$ computed on $\hat{\rho}$ and $\mathcal{B}$ computed on $\hat{\rho}_A \otimes \hat{\rho}_B$. The latter is zero on fair states.

Lemma 5.2.3 Local symplectic invariance: *Let $\hat{U}_{A,B}$ be a unitary operator amounting to a single-mode symplectic operation $S_{A,B}$ on the local phase-space of mode A, B. Then $Q[(\hat{U}_A \otimes \hat{U}_B)\hat{\rho}(\hat{U}_A^\dagger \otimes \hat{U}_B^\dagger)] = Q(\hat{\rho})$.*

Proof. *Any single-mode symplectic operation S can be decomposed in terms of local rotations and local squeezings (Euler decomposition). By definition* (5.4) *is invariant under local rotations, so we need to show that local squeezing transformations, described by symplectic matrices of the form $S_r = \mathrm{diag}\{1/r, r\}$, also leave $Q(\hat{\rho})$ invariant,* i.e. $Q[(\hat{U}_s^A \otimes \hat{U}_t^B)\rho(\hat{U}_s^{A\dagger} \otimes \hat{U}_t^{B\dagger})] = Q(\hat{\rho})$. *Adopting the passive view, the action of local squeezings on the covariance matrix of each Gaussian state $\hat{\sigma}(x_{A,B})$ is irrelevant, as we take eventually the limit $\sigma \to 0$. The first moments are transformed as $d_{A,B} \mapsto S_{s,t}^{-1} d_{A,B}$, so that $\mathcal{B}_{AB}^{\sigma \to 0}(|x_A|, |x_B|) \mapsto \mathcal{B}_{AB}^{\sigma \to 0}(|sx_A|, |tx_B|)$. On the other hand, the Wigner distribution is transformed as $\mathcal{W}(\xi) \mapsto \mathcal{W}[(S_s^{-1} \oplus S_t^{-1})\xi)]$. Summing up, local squeezings transform $\xi = \{x_A, p_A, x_B, p_B\}$ into $\xi_{s,t} = \{sx_A, p_A/s, tx_B, p_B/t\}$. As* (5.4) *involves integration over the four phase-space variables $d^4\xi$, we change the variables noting that $d^4\xi = d^4\xi_{s,t}$, to conclude the proof.* □

It follows from lemmas 5.2.1 and 5.2.2 that if $Q > 0$, then the state necessarily possesses correlations between the two modes. lemma 5.2.3, moreover, suggests that Q embodies not only a qualitative criterion, but might be interpreted as *bona fide* operational quantifier of CV correlations. We will now show that this is the case for various important classes of states.

First, we apply our procedure to Gaussian states (GS), finding that bit quadrature correlations provide a clear-cut quantification of the total correlations between the two modes. They are monotonic with the entanglement on pure states, and can be arbitrarily large on mixed states, the latter possibly containing arbitrarily strong additional classical correlations. We then address non-Gaussian states (NGS), for which the exact detection of entanglement generally involves measurements of high-order moments [71]. The underlying idea is that for NGS obtained by de-gaussifying an initial pure GS and/or by mixing it with a totally uncorrelated state, our measure based entirely on second moment is still expected to be a (quantitative) witness of the quantum part of correlations only, *i.e.* entanglement. We show that this is indeed the case for relevant NGS including photonic Bell states, photon-subtracted states, and mixtures of Gaussian states. Notably, the complete entanglement picture in a recently demonstrated coherent single-photon-subtracted state [72] via a de-gaussification procedure is precisely reproduced here in terms of quadrature correlations only. Our results render non-Gaussian entanglement significantly more accessible in a direct, practical fashion.

5.3 Gaussian states

Even though entanglement of GS is already efficiently accessible via their covariance matrix, we use such states as "test-beds" for understanding the role of Q in discriminating CV correlations. The covariance matrix γ of any two-mode GS $\hat{\rho}$ can be written in standard form as

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \qquad \begin{array}{c} A = \lambda_a \mathbb{I}_2,\ B = \lambda_b \mathbb{I}_2, \\ C = \mathrm{diag}\{c_x, -c_p\}, \end{array}$$

where, without loss of generality, again we flip the sign of c_p and adopt the convention $c_x \geq |c_p| > 0$. We fix also the displacement vector to zero, this fact together with the symmetries of GS is sufficient to fulfill the fairness condition. The covariance matrix γ describes a physical state if, in terms of the four invariants (2 local purities, global purity and serelian), the following relations holds $\mathcal{P}_A, \mathcal{P}_B \geq 1$, $\mathcal{P} \geq 1$ and $1+\frac{1}{\mathcal{P}^2} \geq \Delta$. In standard form these relations transforms, in terms of the parameters as $\lambda_a, \lambda_b \geq 1$, $(\lambda_a\lambda_b - c_x^2)(\lambda_a\lambda_b - c_p^2) \geq 1$ and $1+(\lambda_a\lambda_b - c_x^2)(\lambda_a\lambda_b - c_p^2) \geq \lambda_a^2 + \lambda_b^2 + 2c_x c_p$ (see details in lemma 2.5.2). The negativity see (2.98), quantifying entanglement between the two modes, reads $N(\hat\rho) = \frac{1-\tilde\mu_-}{2\tilde\mu_-}$ because $\tilde\mu_+ > 1 > \tilde\mu_-$ for all two mode entangled GS, where $\tilde\mu_\pm^2 = [\tilde\Delta \pm (\tilde\Delta^2 - 4/\mathcal{P}^2)^{1/2}]/2$. For two-mode GS, (5.4) evaluates to

$$\begin{aligned} Q(\hat\rho_\gamma) &= (2/\pi)\arctan\left(c_x/\sqrt{\lambda_a\lambda_b - c_x^2}\right) = \\ &= (2/\pi)\arctan\left([(\frac{4}{\mathcal{P}_A\mathcal{P}_B[a_- + a_+]})^2 - 1]^{-\frac{1}{2}}\right), \end{aligned} \tag{5.6}$$

where the optimal quadratures are the standard unrotated positions ($\theta = \varphi = 0$) and $a_\pm = \sqrt{[\Delta - (\mathcal{P}_A \pm \mathcal{P}_B)^2/(\mathcal{P}_A\mathcal{P}_B)^2]^2 - 4/\mathcal{P}^2}$. First, we notice that $Q = 0 \Leftrightarrow \hat\rho$ describes a product state: for GS, $Q > 0$ is then *necessary and sufficient* for the presence of correlations. Second, we observe that for pure GS, reducible up to local unitary operations, to the two-mode squeezed states $\hat\rho_r = |\phi_r\rangle\langle\phi_r|$ characterized by $\lambda_a = \lambda_b = \cosh(2r)$ and $c_x = c_p = \sinh(2r)$, Eq. (5.6) yields a monotonic function of the negativity. We compute explicitly Q and expressed in terms of $\tilde\mu_-$ for comparison

$$\begin{aligned} Q(\hat\rho_r) &= (2/\pi)\arctan(\sinh 2r) = \\ &= (2/\pi)\arctan\left(\frac{1-\tilde\mu_-^2}{2\tilde\mu_-}\right), \end{aligned} \tag{5.7}$$

see also Fig. 5.1. Q is thus, as expected, an operational entanglement measure for pure two-mode GS. Third, we find that for mixed states Q *majorizes* entanglement. Given a mixed GS $\hat\rho_N$ with negativity N, it is straightforward to see that $Q(\hat\rho_N)$ via (5.6), is always greater than $Q(|\psi_N\rangle\langle\psi_N|)$, with $|\psi_N\rangle$ being a pure two-mode squeezed state with the same negativity N.

Hence Q quantifies *total* correlations, and the difference $Q(\hat\rho_N) - Q(|\psi_N\rangle\langle\psi_N|)$ (where the first term is due to total correlations and the second to quantum ones) can be naturally regarded as an operational measure of *classical* correlations [2]. We

[2] The emerging measure of classical correlations is special to Gaussian states, where the correlated degrees of freedom are the field quadratures. Different approaches to the quantification of classical vs quantum correlations were proposed [66].

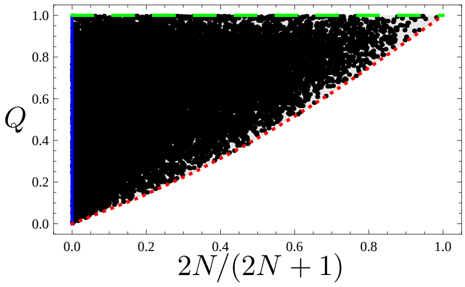

Figure 5.1: Bit quadrature correlations vs normalized negativity N for 18000 random two-mode Gaussian states. The lowermost dotted (red) curve accommodates pure states. The leftmost solid (blue) vertical line denotes separable states parametrized by $c_p = 0$, $c_x = \epsilon(\delta^2 - 1)/\delta$, with $0 \leq \epsilon \leq 1$ and $\delta \to \infty$. The uppermost dashed (green) horizontal line denotes perfectly correlated states with an arbitrary degree of entanglement, parametrized by $c_x = (\delta^2 - 1)/\delta$, $c_p = \epsilon c_x$ (and ϵ, δ as before). Product states (totally uncorrelated) lie at the origin.

have evaluated Q on random two-mode GS as a function of their entanglement, conveniently scaled to $2N/(1 + 2N)$, as shown in Fig. 5.1. Note that for any entanglement content there exist maximally correlated GS with $Q = 1$, and also that separable mixed GS can achieve an arbitrary Q from 0 to 1, their correlations being only classical.

5.4 Non-Gaussian states

Let us now turn our attention towards the even more interesting arena represented by NGS. The description of non-Gaussian states requires an infinite set of statistical moments, so does the entanglement. The best approach to the separability problem of arbitrary bipartite CV states was introduced by Shchukin and Vogel [71]. They provide necessary and sufficient condition for the negativity of the partial transposition *i.e.* entanglement through an infinite series of inequalities based on determinants of successively increasing size matrices containing high order moments of the state. Our aim here is to compute Q on such state. Bit quadrature correlations either in form Eq. (5.4) or Eq. (5.5) can be computed for arbitrary Gaussian and non-Gaussian states at the level of Wigner functions. To this aim one needs to have a way to express arbitrary density operators corresponding to non-Gaussian states into non-Gaussian Wigner functions in a systematical way. Notice that any pure non-Gaussian state can be written as

$$|\psi\rangle = \sum_{n,m=0}^{\infty} \psi_{n,m}|n,m\rangle = \sum_{n,m=0}^{\infty} \psi_{n.m} \frac{(\hat{a}_1^\dagger)^n(\hat{a}_2^\dagger)^m}{\sqrt{n!m!}}|0,0\rangle = f_\psi(\hat{a}_1^\dagger, \hat{a}_2^\dagger)|0,0\rangle, \tag{5.8}$$

that corresponds to a density operator $\hat{\rho}_\psi = f_\psi(\hat{a}_1^\dagger, \hat{a}_2^\dagger)\hat{\rho}_0 f_\psi^*(\hat{a}_1, \hat{a}_2)$, where $\hat{\rho}_0 = |0,0\rangle\langle 0,0|$ is the bipartite vacuum state. Then it is easy, by using the map in Eq. (5.9), to find the Wigner function, $\mathcal{W}_\psi$ corresponding to $\hat{\rho}_\psi$ in terms of the Wigner function of a vacuum state, $\mathcal{W}_0(\zeta) = \frac{1}{\pi^2}\exp(-\zeta^T \cdot \zeta)$.

The action of an operator on a density operator $\hat{\rho}$ is always mirrored by the action of a corresponding differential operator on the corresponding phase-space probability distribution function. We summarize here that result

$$\begin{aligned} \hat{a}\hat{\rho} &\longleftrightarrow (\alpha + \frac{1}{2}\frac{\partial}{\partial\alpha^*})\mathcal{W}_\rho(\alpha,\alpha^*) \\ \hat{\rho}\hat{a} &\longleftrightarrow (\alpha - \frac{1}{2}\frac{\partial}{\partial\alpha^*})\mathcal{W}_\rho(\alpha,\alpha^*) \\ \hat{a}^\dagger\hat{\rho} &\longleftrightarrow (\alpha^* - \frac{1}{2}\frac{\partial}{\partial\alpha})\mathcal{W}_\rho(\alpha,\alpha^*) \\ \hat{\rho}\hat{a}^\dagger &\longleftrightarrow (\alpha^* + \frac{1}{2}\frac{\partial}{\partial\alpha})\mathcal{W}_\rho(\alpha,\alpha^*), \end{aligned} \tag{5.9}$$

similar results holds in the position-momentum base,

$$\begin{aligned} \hat{x}\hat{\rho} &\longleftrightarrow (x + \frac{\mathrm{i}\hbar}{2}\frac{\partial}{\partial p})\mathcal{W}_\rho(x,p) \\ \hat{\rho}\hat{x} &\longleftrightarrow (x - \frac{\mathrm{i}\hbar}{2}\frac{\partial}{\partial p})\mathcal{W}_\rho(x,p) \\ \hat{p}\hat{\rho} &\longleftrightarrow (p - \frac{\mathrm{i}\hbar}{2}\frac{\partial}{\partial x})\mathcal{W}_\rho(x,p) \\ \hat{\rho}\hat{p} &\longleftrightarrow (p + \frac{\mathrm{i}\hbar}{2}\frac{\partial}{\partial x})\mathcal{W}_\rho(x,p). \end{aligned} \tag{5.10}$$

We focus on the most relevant NGS recently discussed in the literature and lastly experimentally realized. Remarkably, we find for all of them a *monotonic* functional dependence between the entanglement (negativity) and the quadrature correlations Q measure of (5.4). This fact indicates that in the preparation of those states, classical correlations are never induced. From a more practical perspective, this observation makes their entanglement amenable to a direct measurement in terms of quadrature correlations.

5.4.1 Photonic Bell states

We consider Bell-like states of the form $|\Phi^\pm\rangle = \sqrt{p}|00\rangle \pm \sqrt{1-p}|11\rangle$ and $|\Psi^\pm\rangle = \sqrt{p}|01\rangle \pm \sqrt{1-p}|10\rangle$ (with $0 \le p \le 1$), which are non-trivial examples of superpositions of Fock states, entangled with respect to the (discrete) photon number. Notice in particular how Ψ^+ for $p = 1/2$ can be obtained by photon addition to the vacuum: $|\Psi^+_{p=1/2}\rangle = \frac{1}{\sqrt{2}}(\hat{a}^\dagger_A + \hat{a}^\dagger_B)|00\rangle$. The negativity of these Bell-like states reads $N_B = \sqrt{p(1-p)}$. For the four of them (and at optimal angles $\theta = \varphi = 0$), (5.4) reads

$$Q_B = (4/\pi)N_B, \tag{5.11}$$

showing a perfect agreement between the quadrature CV correlations and the entanglement.

5.4.2 Photon subtracted states

Most attention is being drawn by those CV states obtained from Gaussian states via subtracting photons [72, 73, 74]: they perform better as resources for protocols like teleportation [75, 76] and allow for loophole-free tests of non-locality [67, 68, 69, 70]. Let us recall their preparation, following [75]. The beam A (B) of a two-mode squeezed state $|\phi_r\rangle$ (created using an squeezed/antisqueezed state and a balanced beam splitter) is let to interfere, via a beam splitter of transmitivity T, with a vacuum mode, see Fig. 5.2. The output is a four-mode Gaussian state of modes $CA'DB'$. Detection of one photon in each of the two beams C and D, conditionally projects the state of modes $A'B'$ into a pure NGS, given in the Fock basis by $|\psi_{ps}^{(T,r)}\rangle = \sum_{n=0}^{\infty} c_n|n,n\rangle$, where $c_n(T,\Lambda) = (n+1)(T\Lambda)^n \left(1-T^2\Lambda^2\right)^{3/2}/\sqrt{1+T^2\Lambda^2}$, and $\Lambda = \tanh r$.

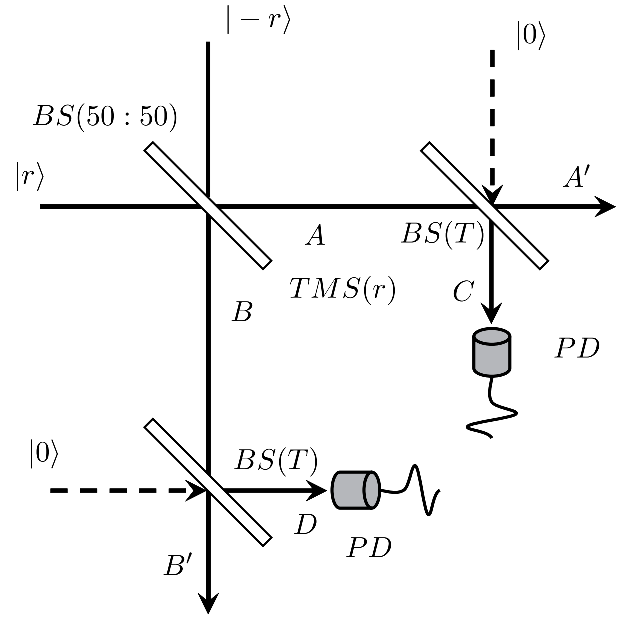

Figure 5.2: Measurement-induced non-Gaussian operation on the two-mode squeezed vacuum state. First, a squeezed and antisqueezed states are let to interfere in a balanced beam splitter, $BS(50:50)$ to produce a two-mode squeezed state $|\phi_r\rangle$. Second, they are both mixed with the vacuum in a beam splitter with transmitivity T denoted as $BS(T)$. Finally, modes C and D are measured with a photodetector, PS.

The limiting case $T \to 1$, occurring with asymptotically vanishing probability, corresponds to an ideal two-photon subtraction, $|\psi_{ps}^{(1,r)}\rangle \propto (\hat{a}_A\hat{a}_B)|\phi_r\rangle$. For any T, the negativity is computable as $N(\psi_{ps}^{(T,r)}) = 2/(1-T\Lambda) - 1/(1+T^2\Lambda^2) - 1$. It increases with r and with T but only in the case $T = 1$ it exceeds $N(\phi_r)$ for any r, diverging for $r \longrightarrow \infty$. For all $T < 1$, the entanglement of $|\psi_{ps}^{(T,r)}\rangle$ eventually saturates, and above a squeezing threshold $r_T \gg 1$, the original GS is more entangled than the resulting non-Gaussian one. Following [67, 68, 69, 70], the explicit expression of the quadrature bit correlations (5.4) can be analytically obtained

$$Q(\psi_{ps}^{(T,r)}) = \sum_{n>m=0}^{\infty} \frac{2^{m+n+3}\pi[\mathcal{F}(m,n) - \mathcal{F}(n,m)]^2 c_m c_n}{(m-n)^2 m! n!},$$

where the c_k's are defined above, $\mathcal{F}(m,n) = \left[\Gamma\left(-\frac{m}{2}\right)\Gamma\left(\frac{1-n}{2}\right)\right]^{-1}$, and Γ is the gamma function. Again optimal quadrature measurements are achieved at $\theta = \varphi = 0$. As depicted in Fig. 5.3, the behavior of the entanglement is fully reproduced by $Q(\psi_{ps}^{(T,r)})$ which again is a monotonic function of N *i.e.* (5.4) is thus measuring truly quantum correlations of this important class of NGS as well.

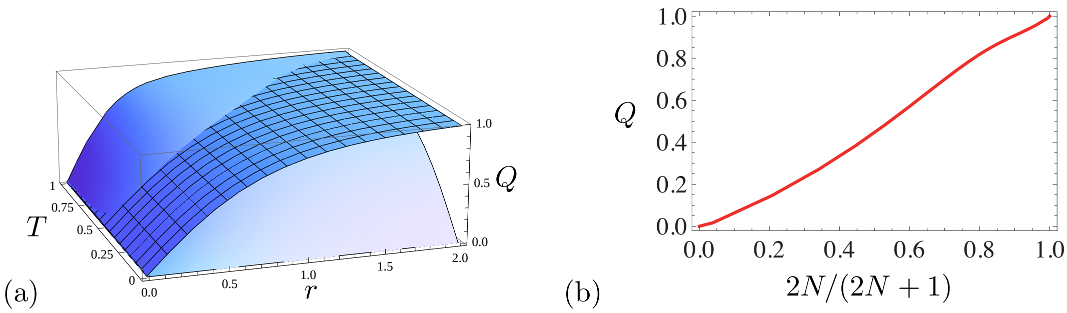

Figure 5.3: (a) Bit quadrature correlations Q vs squeezing r and beam splitter transmitivity T for photon-subtracted states (shaded surface) and for two-mode squeezed states (wireframe surface). (b) Q vs normalized negativity for photon-subtracted states.

5.4.3 Experimental de-gaussified states

Up to now we considered nearly-ideal non-Gaussian situations. We apply now our definition to the coherent photon-subtracted state $\hat{\rho}_{exp}$ recently studied and demonstrated by Ourjoumtsev *et al* [72]. Following their paper for details on the state preparation, we recall that each of the two beams of the two-mode squeezed state $|\phi_r\rangle$ was let to interfere with the vacuum at a beam splitter with reflectivity $R \ll 1$, and by using an avalanche photodiode a single photon was subtracted from the state in a de-localized fashion. The realistic description of the obtained highly mixed state involves many parameters. We fix all to the values obtained from the theoretical calculations and/or experimental data of [72], but for the reflectivity R and the initial squeezing r which are kept free. We then evaluate (5.4) as a function of r for different values of R. Unlike the previous cases, optimal correlations in the state $\hat{\rho}_{exp}$ occur between momentum operators ($\theta = \varphi = \pi/2$).

Also for this realistic mixed case, the correlation measure Q reproduces precisely the behavior of the negativity, as obtained in [72] after full Wigner tomography of the produced state $\hat{\rho}_{exp}$. In particular, the negativity (and Q) increases with the squeezing r, and decreases with R. Below a threshold squeezing which ranges around $\sim$ 3 dB, the NGS exhibits more entanglement (larger Q) than the original two-mode squeezed state. Our results depicted in Fig. 5.4 compare extremely well to the experimental results (Fig. 6 of [72]) where the negativity is plotted there as a function of r for different R's. Thus, the results give an indication of the intimate relation between Q and the negativity of non-Gaussian states beyond idealizations.

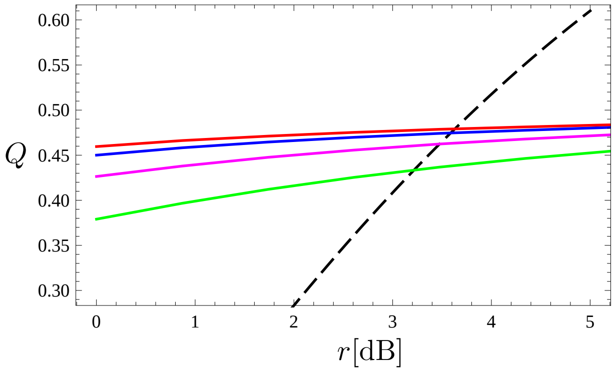

Figure 5.4: Bit quadrature correlations Q vs squeezing r (in decibels) for the de-gaussified states demonstrated in [72] with beam splitter reflectivity R equal to (from top to bottom); 3% (red), 5% (blue), 10% (magenta), 20% (green). The dashed black curve depicts Q for a two-mode squeezed state. See Fig. 6 of [72].

5.4.4 Mixtures of Gaussian states

Recent papers [77, 78] dealt with mixed NGS of the form $\hat{\rho}_m = p|\phi_r\rangle\langle\phi_r| + (1 - p)|00\rangle\langle 00|$, with $0 \leq p \leq 1$. They have a positive Wigner function yet they are NGS (but for the trivial instances $p = 0, 1$). Clearly, the de-gaussification here reduces entanglement and correlations in general, as it involves a mixing with the totally uncorrelated vacuum state. The negativity of such states reads $N_m = N(\hat{\rho}_m) = pN(\phi_r) = p(\mathrm{e}^{2r} - 1)/2$ and is increasing both with r and with p. The same dependency holds for the bit correlations,

$$Q_m = Q(\hat{\rho}_m) = (2p/\pi)\arctan\left(N_m\left[\frac{1}{2N_m + p} + \frac{1}{p}\right]\right), \tag{5.12}$$

which again is a monotonic function of N_m for any p.

A similar result holds for mixtures of photon-subtracted states with the vacuum. We further studied other NGS including photon-added and squeezed Bell-like states [76], and their mixtures with the vacuum, for all we found a direct match between entanglement and Q. Interestingly, this is not true for *all* CV states. By definition, Q quantifies correlations encoded in the second canonical moments only. We have realized that there exist also states *e.g.* the photonic qutrit state $|\psi_h\rangle = |00\rangle/\sqrt{2} + (|02\rangle + |20\rangle)/2]$ which, though being totally uncorrelated up to the second moments ($Q = 0$), are strongly entangled, with correlations embedded only in higher moments. The characterization of such states is an intriguing topic for further study. Finally, we have checked that for all states analyzed, the bit correlations obtained in the conjugate quadrature of the optimal one, *i.e.* $Q(\theta+\pi/2, \varphi+\pi/2)$ are either zero or negligible but a possible "heterodyne" generalization of our approach, involving measurements of two conjugate quadratures per mode, also deserves further attention.

5.5 Conclusions

In this chapter, by analyzing the maximal number of correlated bits (Q) that can be extracted from a CV state via quadrature measurements, we have provided an operational quantification of the entanglement content of several relevant NGS (including the useful photon-subtracted states). Crucially, one can experimentally measure Q by direct homodyne detections (of the quadratures displaying optimal correlations only), in contrast to the much more demanding full tomographical state reconstruction. One can then easily invert the (analytic or numeric) monotonic relation between Q and the negativity to achieve a direct entanglement quantification from the measured data. Our analysis demonstrates the rather surprising feature that entanglement in the considered NGS can thus be detected and experimentally quantified with the same complexity as if dealing with GS. In this respect, it is even more striking that the measure considered in this paper, based on (and accessible in terms of) second moments and homodyne detections only, provides such an exact quantification of entanglement in a broad class of pure and mixed NGS, whose quantum correlations are encoded nontrivially in higher moments too, and currently represent the preferred resources in CV Quantum Information. We focused on optical realizations of CV systems, but our framework equally applies to collective spin components of atomic ensembles [79], and radial modes of trapped ions [14]. Finally, it is also surprising that for all these family of states we have studied, the optimization of just one quadrature scales monotonically with the negativity of the state. Although this could expected for pure Gaussian states, our study demonstrated that the non-Gaussian states obtained either as de-gaussifications of pure Gaussian states or mixings with uncorrelated states preserve this property.

Chapter 6

Measurement induced entanglement in Continuous Variable

6.1 Introduction

In the previous chapters we have presented several implementations of Continuous Variable (CV) systems which demand in advance, as a resource, shared entanglement between the parties involved. In particular, for the Byzantine agreement protocol we demanded a pure, fully inseparable tripartite Gaussian state and completely symmetric under the interchange of the modes with a specific degree of entanglement for an efficient realistic implementation of the protocol. In this chapter our aim is to provide a realistic optical scheme for the creation and manipulation of multipartite Gaussian entanglement of arbitrary modes between atomic gas samples. We concentrate on a matter-light interaction between Gaussian polarized light and polarized atomic samples. For convenience we analyze quantum non-demolition (QND) matter-light interfaces.

Matter-light quantum interfaces refer to those interactions that lead to a faithful transfer of correlations between atoms and photons. The interface, if appropriately tailored, generates an entangled state of matter and light which can be further manipulated (for a review see [13, 80] and references therein). To this aim, a strong coupling between atoms and photons is a must. A pioneering method to enhance the coupling is cavity QED, where atoms and photons are made to interact strongly due to the confinement imposed by the boundaries [81]. An alternative approach to reach the strong coupling regime in *free space* is to use optically thick atomic samples.

Atomic samples with internal degrees of freedom (collective spin) can be made to interact with light via the Faraday effect, which refers to the polarization rotation that is experienced by a linearly polarized light propagating inside a magnetic medium. At the quantum level, the Faraday effect leads to an exchange of fluctuations between matter and light. As demonstrated by Kuzmich and co-workers [82], if an atomic sample interacts with a squeezed light whose polarization is measured afterwards, the collective atomic state is projected into a spin squeezed state (SSS). Furthermore, to produce a long lived SSS, Kuzmich and co-workers [83] proposed a QND measurement, based on off-resonant light propagating through an atomic polarized sample in its ground state.

A step forward within this scheme is measurement induced entanglement between two macroscopic atomic ensembles. As proposed by Duan *et al* [84] and demonstrated by Polzik and co-workers [79], the interaction between a single laser pulse, propagating through two spatially separated atomic ensembles combined with a final projective measurement on the light, leads to an EPR state of the two atomic ensembles. Due to the QND character of the measurement, the verification of entanglement is done by a homodyne measurement of a second laser pulse that has passed through the samples. From such measurements, atomic spin variances inequalities can be checked, asserting whether the samples are entangled or not. A complementary scheme for measurement induced entanglement is also introduced in [85, 86].

The quantum Faraday effect can also be used as a powerful spectroscopic method [87]. Tailoring the spatial shape of the light beam, provides furthermore, a detection method with spatial resolution which opens the possibility to detect phases of strongly correlated systems generated with ultra-cold gases in optical lattices [88, 89, 90].

Here, we analyze the suitability of the Faraday interface in the multipartite scenario. In contrast to the bipartite case, where only one type of entanglement exists, the multipartite case offers a richer situation [91, 55]. Due to this fact, the verification of entanglement using spin variance inequalities [92] becomes an intricate task. We address such problem and provide a scheme for the generation and verification of multipartite entanglement between atomic ensembles. Despite the irreversible character of the entanglement induced by measurement, we find that a second pulse can reverse the action of the first one deleting all the entanglement between the atomic samples. This result has implications in the use of atomic ensembles as quantum memories [93]. Finally, we introduce the CV formalism for further analysis. That is, if one prepares both atoms and light as Gaussian states, then due to the linearity of the equations of evolution for atoms and light, the evolution is Gaussian and it is possible to write the states as covariance matrices and the evolution as a symplectic transformation. The explicit use of the covariance matrix enables for an entanglement verification through covariance matrix criteria.

6.2 Quantum interface description

The basic concept, underlying the QND atom-light interface we will use (see appendix 6.A), is the dipole interaction between an off-resonant linearly polarized light with a polarized atomic ensemble, followed by a quantum homodyne measurement of light. In section 6.3.1 we review the basic known results that permits, to entangle two separated atomic samples by letting light interact with two atomic samples in a fixed direction. In section 6.3.2 we detail our new proposal in which light and atoms are free to interact at arbitrary angles.

On one hand, we consider an ensemble of N_{at} non-interacting alkali atoms with individual total angular momentum $\vec{F} = \vec{I} + \vec{J}$ prepared in the ground state manifold $|F, m_F\rangle$. Further we assume that all atoms are polarized along the x-direction, which corresponds to preparing them in a certain hyperfine state $|F, m_F\rangle$ (*e.g.* in the case of Cesium the hyperfine ground state $6S_{1/2}$ *i.e.* $L = 0$ and $J = S = 1/2$ is split into two hyperfine states with total angular momentum $F = 3$ and $F = 4$ due to a nuclear spin $I = 7/2$). We restrict ourselves to one hyperfine level, $F = 4$, which is possible experimentally because the hyperfine splitting is large compared to typical resolutions of the lasers. Furthermore, it is possible to put (almost) all atoms in the outermost state with $m_F = 4$, being x the axis of quantization. We describe such sample with its collective angular momentum $\hat{\vec{J}} = (\hat{J}_x, \hat{J}_y, \hat{J}_z)$ being $\hat{J}_k = \sum_{n=1}^{N_{at}} \hat{F}_{k,n}$ the total angular momentum of the ensemble ($k = x, y, z$). Then, the $\hat{J}_x$ component of the collective spin can be regarded as a classical number $\hat{J}_x \approx <\hat{J}_x> = N_{at}\hbar F$, while the orthogonal spin components encode all the quantum character. Due to the above approximation, the orthogonal collective angular momentum components can be treated as canonical conjugate variables, $\left[\hat{J}_y/\sqrt{J_x}, \hat{J}_z/\sqrt{J_x}\right] = \mathrm{i}\hbar$.

On the other hand, the polarization of light propagating along the z-direction can be described by the Stokes vector $\hat{\vec{s}} = (\hat{s}_x, \hat{s}_y, \hat{s}_z)$, whose components correspond to the differences between the number of photons (per time unit) with x and y linear polarizations, $\pm\pi/4$ linear polarizations and the two circular polarizations

$$\begin{aligned} \hat{s}_x &= \frac{\hbar}{2}(\hat{n}_x - \hat{n}_y) = \frac{\hbar}{2}(\hat{a}_x^\dagger \hat{a}_x - \hat{a}_y^\dagger \hat{a}_y), \\ \hat{s}_y &= \frac{\hbar}{2}(\hat{n}_\nearrow - \hat{n}_\searrow) = \frac{\hbar}{2}(\hat{a}_x^\dagger \hat{a}_y + \hat{a}_y^\dagger \hat{a}_x), \\ \hat{s}_z &= \frac{\hbar}{2}(\hat{n}_\circlearrowleft - \hat{n}_\circlearrowright) = \frac{\hbar}{2\mathrm{i}}(\hat{a}_x^\dagger \hat{a}_y - \hat{a}_y^\dagger \hat{a}_x). \qquad (6.1) \end{aligned}$$

The above operators have dimension of energy. They are convenient for a microscopic description of interaction between light and atoms, however, we will concentrate on the macroscopic variables, defined as $\hat{S}_k(z) = \int_0^T \hat{s}_k(z,t)dt$ ($k = x, y, z$), where T is the length of the light pulse. Such defined operators correspond now to differences in total number of photons, and obey standard angular momentum commutation rules. For light linearly polarized along the x-direction $\hat{S}_x \approx <\hat{S}_x> = N_{\mathrm{ph}}\hbar/2$. In such case, the orthogonal Stokes components $\hat{S}_y, \hat{S}_z$ are conjugated variables fulfilling canonical commutation relations, $\left[\hat{S}_y/\sqrt{S_x}, \hat{S}_z/\sqrt{S_x}\right] = \mathrm{i}\hbar$.

For a light beam propagating through the atomic sample in the YZ plane at a certain angle α with respect to direction z (see Fig. 6.1), the atom-light interaction can be approximated to the following QND effective interaction Hamiltonian (see appendix 6.A for a detailed derivation)

$$\hat{H}_{\text{int}}^{\text{eff}}(\alpha) = -\frac{a}{T}\hat{S}_z(\hat{J}_z \cos\alpha + \hat{J}_y \sin\alpha). \tag{6.2}$$

The parameter a is the coupling constant with dimensions of the inverse of an action. The interaction is a linear coupling between the Stokes operator and the collective atomic spin operator, thus, the interaction is a Gaussian interaction between two bosonic modes. Also, the states for atoms and light, by the strong polarization constrain, can be treated as two mode enabling us to tackle the atom-light interaction with a CV formalism.

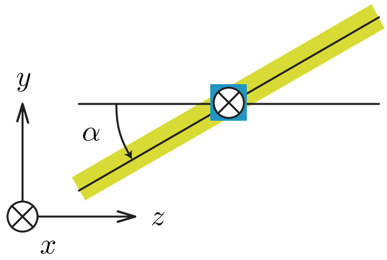

Figure 6.1: A beam passing through an atomic sample at an angle α with respect to z.

The equations of motion [1] for the macroscopic variables for light and atoms are

$$\hat{J}_y^{\text{out}} = \hat{J}_y^{\text{in}} - a\hat{S}_z^{\text{in}} J_x \cos\alpha, \tag{6.3}$$
$$\hat{J}_z^{\text{out}} = \hat{J}_z^{\text{in}} + a\hat{S}_z^{\text{in}} J_x \sin\alpha, \tag{6.4}$$

$$\hat{S}_y^{\text{out}} = \hat{S}_y^{\text{in}} - aS_x(\hat{J}_z^{\text{in}} \cos\alpha + \hat{J}_y^{\text{in}} \sin\alpha), \tag{6.5}$$
$$\hat{S}_z^{\text{out}} = \hat{S}_z^{\text{in}}, \tag{6.6}$$

where the operators $\hat{S}_k^{\text{in/out}}$ as the Stokes operators characterizing the pulse entering ($z = 0$) and leaving ($z = L$) the atomic sample. Analogously, $\hat{J}_k^{\text{in/out}}$ correspond to initial ($t = 0$) and final state ($t = T$) of the atomic spin.

From Eq. (6.5) it is clear that the polarization of the outgoing light carries information about the collective atomic angular momentum. The quantum character of the interface is reflected at the level of fluctuations, *i.e.*,

$$\left(\Delta\hat{S}_y^{\text{out}}\right)^2 = \left(\Delta\hat{S}_y^{\text{in}}\right)^2 + a^2 S_x^2 \left(\Delta[\hat{J}_z^{\text{in}} \cos\alpha + \hat{J}_y^{\text{in}} \sin\alpha]\right)^2. \tag{6.7}$$

At the same time, Eqs. (6.3) and (6.4) show the QND character of the Hamiltonian, *i.e.*, the measured combination $\hat{J}_z^{\text{in}} \cos\alpha + \hat{J}_y^{\text{in}} \sin\alpha$ is not affected by the interaction

[1] In the particular configuration of Fig. 6.1, both the Hamiltonian and the equations of motion can be deduced after an anti x-rotation of angle α to the corresponding expressions of appendix 6.A.

since it commutes with the effective Hamiltonian. This fact allows to measure the fluctuations of the atomic spin components with the minimal disruption permitted by Quantum Mechanics.

In the following sections we will generalize the above formalism to the interaction of a light pulse with an arbitrary number, N_s, of spatially separated atomic samples. Variables characterizing each sample will be denoted by $\hat{J}_k^{(i)}$, where $i = 1, 2, \ldots, N_s$ denotes the samples and $k = x, y, z$.

6.3 Bipartite entanglement: Generation and verification

6.3.1 Magnetic field addressing scheme

We begin by reviewing the seminal work of Polzik *et al* [79] leading to the entanglement of two spatially separated atomic samples, as schematically shown in Fig. 6.2.

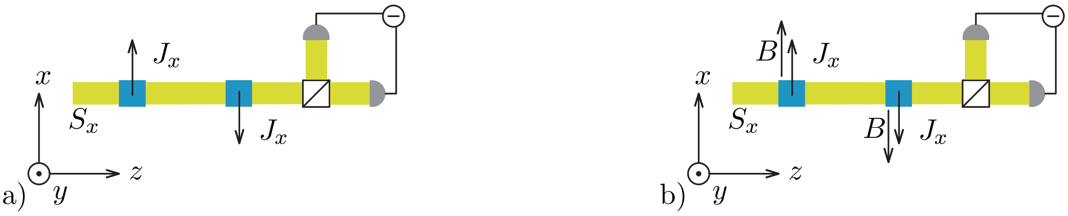

Figure 6.2: Sketch of the experimental setup applied in [79] to generate bipartite entanglement. a) Entangling pulse. b) Verifying pulse followed by homodyne measurement. A local magnetic field is added (parallel to the spin polarization direction) in order to measure two transverse components of the spin with a single light beam.

In the experimental setup, both light and atomic samples were strongly polarized along the x-direction while light propagated along the z-direction ($\alpha = 0$). It is straightforward to generalize the equations of motion of appendix 6.A for two samples. For example, the collective polarization of atoms along the z-direction is still preserved, *i.e.*, $\partial \hat{J}_z^{(i)}/\partial t = 0$ with $i = 1, 2$, and Eq. (6.5) reads now [2]

$$\hat{S}_y^{\text{out}} = \hat{S}_y^{\text{in}} - aS_x \left(\hat{J}_z^{(1)} + \hat{J}_z^{(2)} \right). \tag{6.8}$$

Entanglement between the atomic samples is established *as soon as* the $\hat{S}_y^{\text{out}}$ component of *light is measured.* Moreover, it should be emphasized that entanglement is generated independently of the outcome of the measurement. The real challenge, though, is its experimental verification, since spin entanglement criterium relies on spin variances inequalities of operators of the type $(\hat{J}_y^{(1)} - \hat{J}_y^{(2)})$ and $(\hat{J}_z^{(1)} + \hat{J}_z^{(2)})$. This is so because the maximally entangled EPR state is a co-eigenstate of such operators. This fact, in turn, imposes an upper bound (see theorem 2.6.5) on the

[2] We will omit the superscripts in/out when it is not necessary.

variances of such operators giving rise to a sufficient and necessary condition for separability [22]

$$\left(\Delta\left[|\lambda|\hat{J}_y^{(1)}+\frac{\hat{J}_y^{(2)}}{\lambda}\right]\right)^2+\left(\Delta\left[|\lambda|\hat{J}_z^{(1)}-\frac{\hat{J}_z^{(2)}}{\lambda}\right]\right)^2\geq\left(\lambda^2+\frac{1}{\lambda^2}\right)\hbar J_x, \qquad (6.9)$$

for all $\lambda \in \mathbb{R}$.

The way to experimentally check [79] the above equation with $\lambda = -1$ was to add on each sample an external magnetic field, parallel to the spin polarization direction, x (see also [94]). The magnetic field was local, therefore, it did not affect the generation of entanglement. However, it caused a Larmor precession of the collective atomic momenta, which permitted a simultaneous measurement of the appropriately redefined "canonical variables" $\hat{J}_y^{(1)}+\hat{J}_y^{(2)}$ and $\hat{J}_z^{(1)}+\hat{J}_z^{(2)}$. Notice that this can only be done if the atomic samples are polarized oppositely along the x-direction, so that the commutator $[\hat{J}_z^{(1)}+\hat{J}_z^{(2)},\hat{J}_y^{(1)}+\hat{J}_y^{(2)}] = J_x^{(1)}+J_x^{(2)} = 0$. Therefore, the first light beam was used for creation of EPR-type entanglement, and another one for its verification through Eq. (6.9).

Let us detail how the local magnetic field, if measuring the appropriated observables, enables for checking Eq. (6.9). As in the appendix 6.A, we derive here the complete equation system for observables of light and both samples. As we will see the linearity of the system enables us to, in a easy way, to jump to the CV formalism via symplectic matrices.

If a constant and homogeneous magnetic field is added in the x-direction (parallel to the spin polarization direction) the transverse spin components precess at a Larmor frequency Ω. The magnetic field adds a term [3] $\hat{H} = -\vec{\hat{\mu}}\cdot\vec{B} = +\Omega J_x$ into the Hamiltonian with same field strength and global sign for each one of the two samples. The action of the magnetic field at a fixed time produces a rotation of the spin vector (active view) that can be mimic as a rotation on the system (passive view) via the substitution $\alpha \rightarrow -\Omega t$ on the equations of motion considered in the appendix 6.A *i.e.*

$$\frac{\partial}{\partial t}\hat{j}_y^{(1)}(z,t) = -a\hat{s}_z(t)j_x^{(1)}\cos\Omega t, \qquad (6.10)$$

$$\frac{\partial}{\partial t}\hat{j}_z^{(1)}(z,t) = -a\hat{s}_z(t)j_x^{(1)}\sin\Omega t, \qquad (6.11)$$

$$\frac{\partial}{\partial t}\hat{j}_y^{(2)}(z,t) = -a\hat{s}_z(t)j_x^{(2)}\cos\Omega t, \qquad (6.12)$$

$$\frac{\partial}{\partial t}\hat{j}_z^{(2)}(z,t) = -a\hat{s}_z(t)j_x^{(2)}\sin\Omega t, \qquad (6.13)$$

$$\frac{\partial}{\partial z}\hat{s}_y(z,t) = -\frac{a}{cT}s_x\left(\hat{j}_z^{(1)}\cos\Omega t-\hat{j}_y^{(1)}\sin\Omega t\right), \qquad (6.14)$$

$$\hat{s}_z(z,t) = \hat{s}_z(t), \qquad (6.15)$$

[3] Remember that $\vec{B} = \Omega\frac{m}{e}\vec{i}$ and $\vec{\hat{\mu}} = -\frac{e}{m}\vec{\hat{J}}$.

Grouping the equations (6.10)-(6.13) and using the fact that the two samples are opposite polarized, $J_x^{(1)} = -J_x^{(2)} = J_x > 0$ equations for atoms are

$$\begin{aligned}
\frac{\partial}{\partial t}\left[\hat{j}_y^{(1)}(z,t)+\hat{j}_y^{(2)}(z,t)\right] &= -a\hat{s}_z(t)\left(j_x^{(1)}+j_x^{(2)}\right)\cos\Omega t = 0, && (6.16)\\
\frac{\partial}{\partial t}\left[\hat{j}_z^{(1)}(z,t)+\hat{j}_z^{(2)}(z,t)\right] &= -a\hat{s}_z(t)\left(j_x^{(1)}+j_x^{(2)}\right)\sin\Omega t = 0, && (6.17)\\
\frac{\partial}{\partial t}\left[\hat{j}_y^{(1)}(z,t)-\hat{j}_y^{(2)}(z,t)\right] &= -a\hat{s}_z(t)\left(j_x^{(1)}-j_x^{(2)}\right)\cos\Omega t = \\
&= -a\hat{s}_z(t)2j_x\cos\Omega t, && (6.18)\\
\frac{\partial}{\partial t}\left[\hat{j}_z^{(1)}(z,t)-\hat{j}_z^{(2)}(z,t)\right] &= -a\hat{s}_z(t)\left(j_x^{(1)}-j_x^{(2)}\right)\sin\Omega t = \\
&= -a\hat{s}_z(t)2j_x\sin\Omega t. && (6.19)
\end{aligned}$$

We next integrate in space ($\int_0^L \rho A dz$) and time ($\int_0^T dt$) to introduce the macroscopical variables

$$\begin{aligned}
\hat{J}_y^{(1),\mathrm{in}}+\hat{J}_y^{(2),\mathrm{in}} &= \hat{J}_y^{(1),\mathrm{out}}+\hat{J}_y^{(2),\mathrm{out}}, && (6.20)\\
\hat{J}_z^{(1),\mathrm{in}}+\hat{J}_z^{(2),\mathrm{in}} &= \hat{J}_z^{(1),\mathrm{out}}+\hat{J}_z^{(2),\mathrm{out}}, && (6.21)\\
\hat{J}_y^{(1),\mathrm{out}}-\hat{J}_y^{(2),\mathrm{out}} &= \hat{J}_y^{(1),\mathrm{in}}-\hat{J}_y^{(2),\mathrm{in}}-2aJ_x\int_0^T dt\cos\Omega t\,\hat{s}_z(t), && (6.22)\\
\hat{J}_z^{(1),\mathrm{out}}-\hat{J}_z^{(2),\mathrm{out}} &= \hat{J}_y^{(1),\mathrm{in}}-\hat{J}_y^{(2),\mathrm{in}}-2aJ_x\int_0^T dt\sin\Omega t\,\hat{s}_z(t). && (6.23)
\end{aligned}$$

Eq. (6.15) is also integrated in space ($\int_0^L \rho A dz$) and Eq. (6.14) in space and in time ($\int_0^T dt\cos\Omega t$), ($\int_0^T dt\sin\Omega t$). Using the fact that the observables $\left[\hat{j}_y^{(1)}(z)+\hat{j}_y^{(2)}(z)\right]$ and $\left[\hat{j}_z^{(1)}(z)+\hat{j}_z^{(2)}(z)\right]$ do not evolve, equations for light are

$$\begin{aligned}
\int_0^T dt\cos\Omega t\,\hat{s}_y^{\mathrm{out},2}(t) = \int_0^T dt\cos\Omega t\,\hat{s}_y^{\mathrm{in},1}(t) + \\
-\frac{a}{T}S_x\int_0^T dt\cos\Omega t\left(\left[\hat{J}_z^{(1)}+\hat{J}_z^{(2)}\right]\cos\Omega t-\left[\hat{J}_y^{(1)}+\hat{J}_y^{(2)}\right]\sin\Omega t\right),
\end{aligned} \qquad (6.24)$$

$$\begin{aligned}
\int_0^T dt\sin\Omega t\,\hat{s}_y^{\mathrm{out},2}(t) = \int_0^T dt\sin\Omega t\,\hat{s}_y^{\mathrm{in},1}(t) + \\
-\frac{a}{T}S_x\int_0^T dt\sin\Omega t\left(\left[\hat{J}_z^{(1)}+\hat{J}_z^{(2)}\right]\cos\Omega t-\left[\hat{J}_y^{(1)}+\hat{J}_y^{(2)}\right]\sin\Omega t\right),
\end{aligned} \qquad (6.25)$$

$$\hat{s}_z^{\mathrm{out},2}(t) = \hat{s}_z^{\mathrm{in},2}(t) = \hat{s}_z^{\mathrm{out},1}(t) = \hat{s}_z^{\mathrm{in},1}(t). \qquad (6.26)$$

We introduce here a suitable choice of pairs of macroscopical observables for light and atoms, where the subscript "L" stands for light while "A" for atoms

$$\begin{aligned}
\hat{Q}_{L1}(z) &= \sqrt{\frac{2}{S_x\hbar}}\int_0^T dt\cos\Omega t\,\hat{s}_y(z,t), & \hat{P}_{L1} &= \sqrt{\frac{2}{S_x\hbar}}\int_0^T dt\cos\Omega t\,\hat{s}_z(t),\\
\hat{Q}_{L2}(z) &= \sqrt{\frac{2}{S_x\hbar}}\int_0^T dt\sin\Omega t\,\hat{s}_y(z,t), & \hat{P}_{L2} &= \sqrt{\frac{2}{S_x\hbar}}\int_0^T dt\sin\Omega t\,\hat{s}_z(t),\\
\hat{Q}_{A1}(t) &= \frac{\hat{J}_y^{(1)}-\hat{J}_y^{(2)}}{\sqrt{2J_x\hbar}}, & \hat{P}_{A1} &= \frac{\hat{J}_z^{(1)}+\hat{J}_z^{(2)}}{\sqrt{2J_x\hbar}},\\
\hat{Q}_{A2}(t) &= -\frac{\hat{J}_z^{(1)}-\hat{J}_z^{(2)}}{\sqrt{2J_x\hbar}}, & \hat{P}_{A2} &= \frac{\hat{J}_y^{(1)}+\hat{J}_y^{(2)}}{\sqrt{2J_x\hbar}},
\end{aligned}$$

to finally [4] obtain the solution of the evolution equations for the set of canonical variables before and after interaction (denoted by in/out, respectively)

$$\begin{aligned}
\hat{P}^{\text{out}}_{A1} &= \hat{P}^{\text{in}}_{A1}, && (6.27)\\
\hat{P}^{\text{out}}_{A2} &= \hat{P}^{\text{in}}_{A2}, && (6.28)\\
\hat{Q}^{\text{out}}_{A1} &= \hat{Q}^{\text{in}}_{A1} - \kappa\hat{P}^{\text{in}}_{L1}, && (6.29)\\
\hat{Q}^{\text{out}}_{A2} &= \hat{Q}^{\text{in}}_{A2} - \kappa\hat{P}^{\text{in}}_{L2}, && (6.30)
\end{aligned}$$

$$\begin{aligned}
\hat{Q}^{\text{out}}_{L1} &= \hat{Q}^{\text{in}}_{L1} - \kappa\hat{P}^{\text{in}}_{A1}, && (6.31)\\
\hat{Q}^{\text{out}}_{L2} &= \hat{Q}^{\text{in}}_{L2} - \kappa\hat{P}^{\text{in}}_{A2}, && (6.32)\\
\hat{P}^{\text{out}}_{L1} &= \hat{P}^{\text{in}}_{L1}, && (6.33)\\
\hat{P}^{\text{out}}_{L2} &= \hat{P}^{\text{in}}_{L2}, && (6.34)
\end{aligned}$$

where $\kappa = a\sqrt{S_xJ_x}$ (adimensional) and $\left[\hat{Q}_{Ai},\hat{P}_{Ai}\right] = \mathrm{i}$, $\left[\hat{Q}_{Li},\hat{P}_{Li}\right] = \mathrm{i}$, for $i = 1,2$.

Separability condition (6.9) for $\lambda = -1$

$$\left(\Delta\left[\hat{J}_y^{(1)}-\hat{J}_y^{(2)}\right]\right)^2 + \left(\Delta\left[\hat{J}_z^{(1)}+\hat{J}_z^{(2)}\right]\right)^2 \geq 2\hbar J_x \tag{6.35}$$

translates to

$$\left(\Delta\hat{P}_{A1}\right)^2 + \left(\Delta\hat{P}_{A2}\right)^2 \geq 1 \tag{6.36}$$

taking into account that the sign of the spin y-component flips the sign (sample 1 and 2 are symmetric under a π rotation around z). Thus, checking the inequality can be realized within this scheme by measuring the light quadratures operators $\hat{Q}^{\text{out}}_{L1,2}$ as seen in Eqs. (6.31) and (6.32).

Now, we shall illustrate the power of using a CV phase-space formalism to retrieve the complete covariance matrix of the final states and to detect and quantify the entanglement generation. The variables describing the system after interaction are

[4] Taking into account that $\frac{1}{T}\int_0^T dt\sin^2\Omega t = \frac{1}{T}\int_0^T dt\cos^2\Omega t \simeq \frac{1}{2}$ and $\frac{1}{T}\int_0^T dt\sin\Omega t\cos\Omega t \simeq 0$ if $\Omega T \simeq 2\pi$.

expressed as a linear combination of the initial ones. Let us denote by $\mathcal{O}$ the following linear transformation $\mathcal{O} : \{\hat{Q}^{\text{in}}_{Ai}, \hat{P}^{\text{in}}_{Ai}, \hat{Q}^{\text{in}}_{Li}, \hat{P}^{\text{in}}_{Li}\} \mapsto \{\hat{Q}^{\text{out}}_{Ai}, \hat{P}^{\text{out}}_{Ai}, \hat{Q}^{\text{out}}_{Li}, \hat{P}^{\text{out}}_{Li}\}$, which can be straightforwardly obtained from Eqs. (6.27)-(6.34). Due to the linear coupling between light and matter under consideration, the evolution equations can be directly translated in phase-space as $\zeta^{\text{out}} = O \cdot \zeta^{\text{in}}$ where $\zeta = (Q_{A1}, P_{A1}, Q_{A2}, P_{A2}, Q_{L1}, P_{L1}, Q_{L2}, P_{L2})^T$ is a phase-space vector. There is a symplectic transformation S_{int}, corresponding to the unitary evolution $\mathcal{O}$, relating the state of atoms and light γ, before (in) and after (out) the interaction fulfilling $\gamma_{\text{out}} = S^T_{\text{int}} \gamma_{\text{in}} S_{\text{int}}$ and can be reconstructed in the following way

$$\begin{aligned} \zeta^{\text{out,T}} \cdot \gamma_{\text{in}}^{-1} \cdot \zeta^{\text{out}} &= \zeta^{\text{in},T} O^T \cdot \gamma_{\text{in}}^{-1} \cdot O \zeta^{\text{in}} = \\ &= \zeta^{\text{in,T}} \cdot (O^{-1} \gamma_{\text{in}} (O^T)^{-1})^{-1} \cdot \zeta^{\text{in}} = \\ &= \zeta^{\text{in,T}} \cdot \gamma_{\text{out}}^{-1} \cdot \zeta^{\text{in}}. \end{aligned} \tag{6.37}$$

Therefore the symplectic transformation acting on an initial state with covariance matrix for light and atoms γ_{in} due to the Hamiltonian (6.66) is therefore $S_{\text{int}} = (O^T)^{-1}$ and can be written in a matricial form. If, as we will consider, one prepares the ensemble of atoms in a Gaussian state and Gaussian light is used, the CV formalism enables us not only to measure fluctuations of specific collective spin variables of atoms but the complete covariance matrix and displacement vector after interaction enabling for verification of entanglement amenable with covariance matrix criteria. We derive explicitly the states and the evolution using this formalism in section 6.3.2 presenting a new geometric scheme.

6.3.2 Geometrical scheme

Our aim has been to apply the QND atom-light interface to study genuine multipartite entanglement generation with less restrictive conditions, *i.e.*, we assume that: (i) individual magnetic field addressing of each atomic ensemble is not allowed and, (ii) the number of atomic ensembles can be made arbitrary. Such experimental setups that can be build, for instance, using optical micro-traps [95, 96] which allow for isotropic confinement of 10^4 cold atoms, creating in this way mesoscopic atomic ensembles [5]. In these setups, the preparation of each sample in a different initial magnetic state or the addressing of a sample with individual magnetic fields is out of reach. Despite these limitations, an array of micro-traps offers considerable advantages, ranging from its experimental feasibility to the possibility to generate chains and arrays of atomic samples.

Assuming (i), the verification of entanglement cannot be done anymore by means of local magnetic fields on each sample, thus we assume the two samples to be parallel polarized. The way to overcome this problem is depicted in Fig. 6.3 *i.e.* we mimic the action of local magnetic fields in each sample with light propagating at different angles. As seen in the previous section they are mathematically equivalent

[5] In these experiments with ultra-cold atoms one can reduce the number of atoms up to 10^4 still having the same opacity of the medium.

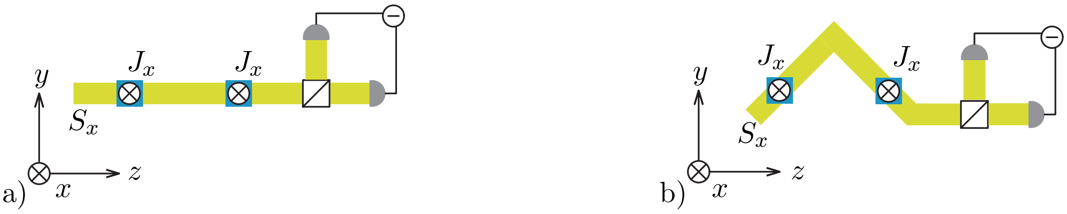

Figure 6.3: The simplest setup for generation and verification of bipartite entanglement between mesoscopic atomic ensembles. a) First light pulse passing through the samples along direction z entangles the samples. b) Second light pulse passing through the samples at angles $\pi/4$ and $-\pi/4$, respectively, allows for verification of entanglement through a variance inequality (see Eq. (6.9)).

local operations. To better understand the dynamics of the interaction in this configuration, we analyze in some detail the setup of Fig. 6.3. In the first shot, light passes through the two sample. As indicated in Eq. (6.8), the light carries information about $\hat{J}_z^{(1)} + \hat{J}_z^{(2)}$ and the measurement of $\hat{S}_y^{\text{out}}$ generates entanglement between the atomic samples. Starting from the evolution equations (6.3),(6.4) and taking into account the light measurements, one can explicitly derive the variances of the atomic spin samples and interpret them in terms of global or non-local squeezings. In the picture, polarized ensembles of atoms in the ground state will be characterized as a vacuum state while light beams will be described as coherent states. In this view, the final bipartite state of the ensembles is characterized by the following variances

$$\left(\Delta[\hat{J}_y^{(1)} + \hat{J}_y^{(2)}]\right)^2 = (1+2\kappa^2)\hbar J_x, \tag{6.38}$$

$$\left(\Delta[\hat{J}_y^{(1)} - \hat{J}_y^{(2)}]\right)^2 = \hbar J_x, \tag{6.39}$$

$$\left(\Delta[\hat{J}_z^{(1)} + \hat{J}_z^{(2)}]\right)^2 = \frac{1}{1+2\kappa^2}\hbar J_x, \tag{6.40}$$

$$\left(\Delta[\hat{J}_z^{(1)} - \hat{J}_z^{(2)}]\right)^2 = \hbar J_x, \tag{6.41}$$

where $\kappa = a\sqrt{S_x J_x}$ is the adimendional coupling interaction. The observables for which the separability criterion (Eq. (6.9)) is violated correspond to $\hat{J}_z^{(1)} + \hat{J}_z^{(2)}$ and $\hat{J}_y^{(1)} - \hat{J}_y^{(2)}$ with $\lambda = -1$. Such a measurement induces squeezing on the variances along the z-direction below the separability limit, as clearly indicated by Eqs. (6.39) and (6.40).

The second part, the verification, it involves a measurement of the sum of the variances corresponding to Eqs. (6.39) and (6.40). In order to do this with a single beam we use light propagating at different angles, as schematically depicted in Fig. 6.3(b). In this case, according to Eq. (6.5) we obtain

$$\hat{S}_y^{\text{out}} = \hat{S}_y^{\text{in}} - \frac{\kappa}{\sqrt{2}}\sqrt{\frac{S_x}{J_x}}\left[\left(\hat{J}_z^{(1)} + \hat{J}_z^{(2)}) + (\hat{J}_y^{(1)} - \hat{J}_y^{(2)}\right)\right]. \tag{6.42}$$

Since within this scheme $<\hat{J}_y^{(i)}\hat{J}_z^{(j)}>=<\hat{J}_y^{(i)}><\hat{J}_z^{(j)}>$, the variance of the output can be written as

$$\begin{aligned}\left(\Delta\hat{S}_y^{\text{out}}\right)^2 &= \left(\Delta\hat{S}_y^{\text{in}}\right)^2 + \\ &+ \frac{\kappa^2}{2}\frac{S_x}{J_x}\left(\left(\Delta[\hat{J}_z^{(1)}+\hat{J}_z^{(2)}]\right)^2+\left(\Delta[\hat{J}_y^{(1)}-\hat{J}_y^{(2)}]\right)^2\right). \qquad (6.43)\end{aligned}$$

For details concerning the experimental measurement of such variances see [97, 98]. This shows that entanglement between two identically polarized atomic ensembles can be generated, irrespectively of the value of the coupling constant κ, and verified using only two beams and no additional magnetic fields, if the second field impinges on the two samples at certain angles.

To increase entanglement between the two samples one should introduce global squeezing in two independent variables. This is schematically depicted in Fig. 6.4(a) and 6.4(b). The first beam introduces squeezing in $\hat{J}_z^{(1)}+\hat{J}_z^{(2)}$ variable. Then, a second beam propagating through the first sample at an angle $\alpha=\pi/2$ and through the second one at an angle $\alpha=-\pi/2$ generates squeezing in $\hat{J}_y^{(1)}-\hat{J}_y^{(2)}$.

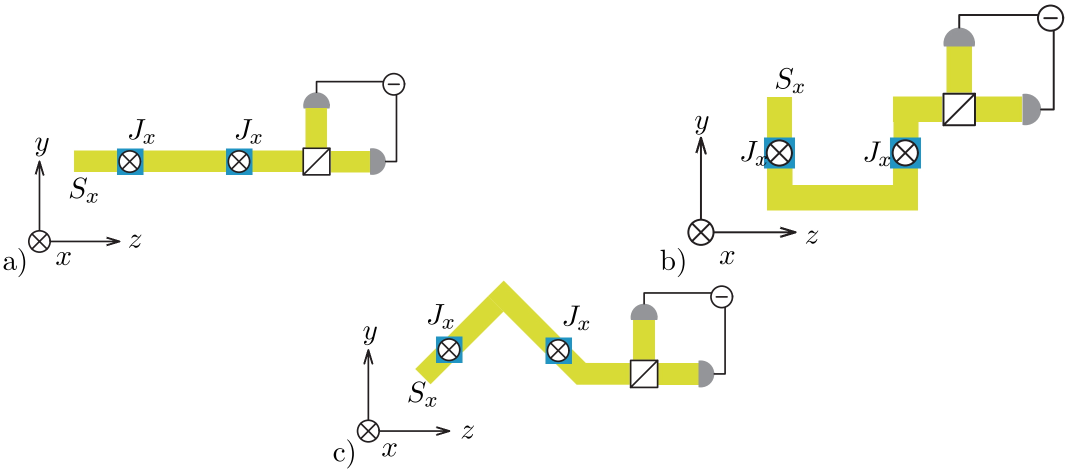

Figure 6.4: The setup for generation and verification of bipartite entanglement between atomic ensembles in which squeezing is introduced in two variables a) $\hat{J}_z^{(1)}+\hat{J}_z^{(2)}$ and b) $\hat{J}_y^{(1)}-\hat{J}_y^{(2)}$ increasing entanglement. The third pulse depicted in figure c) allows for verification of entanglement through a variance inequality. It should be emphasized that the first and last step are exactly the same as in Fig. 6.3.

Note that these are commuting operators, so the second beam would not change the effect of the first one (squeezing of $\hat{J}_z^{(1)}+\hat{J}_z^{(2)}$). The verification of entanglement (see Fig. 6.4(c)) can be done as previously described. Within this scheme one reproduces the results of Julsgaard *et al* [79] without individual addressing *i.e.* EPR entanglement between two atomic samples.

6.3.3 Continuous Variable analysis

We detail here explicitly the setup of Fig. 6.3 at the level of covariance matrix (CM) formalism. The initial state of the two samples and the light is given by the CM for atoms and light $\gamma_{\text{in}}^{A,L} = \mathbb{I}_4^A \oplus \mathbb{I}_2^L$. The symplectic matrix, S_{int}, describing the interaction of light passing through the samples at zero angle is

$$S_{\text{int}} = \left(\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \kappa & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \kappa & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ \kappa & 0 & \kappa & 0 & 0 & 1 \end{array} \right), \tag{6.44}$$

thus, the state after the interaction takes the form

$$\gamma_{\text{out}}^{A,L} = S_{\text{int}}^T \gamma_{\text{in}}^{A,L} S_{\text{int}} = \left(\begin{array}{cccc|cc} 1+\kappa^2 & 0 & \kappa^2 & 0 & 0 & \kappa \\ 0 & 1 & 0 & 0 & \kappa & 0 \\ \kappa^2 & 0 & 1+\kappa^2 & 0 & 0 & \kappa \\ 0 & 0 & 0 & 1 & \kappa & 0 \\ \hline 0 & \kappa & 0 & \kappa^2 & 1+2\kappa^2 & 0 \\ \kappa & 0 & \kappa & 0 & 0 & 1 \end{array} \right). \tag{6.45}$$

Both modes, representing the samples, are entangled with light, however their reduced state is separable as one can check applying NPPT criterium in the CM of the lower-right block matrix. Entanglement between atomic samples is not produced until one measures one quadrature on the light. For this aim, one uses the action of an homodyne measurement on the light mode (see section 2.5.6). The measurement of light leads to the CM describing the final state of the samples.

$$\gamma_{\text{out}}^{A} = \begin{pmatrix} 1+\kappa^2 & 0 & \kappa^2 & 0 \\ 0 & \frac{1+\kappa^2}{1+2\kappa^2} & 0 & -\frac{\kappa^2}{1+2\kappa^2} \\ \kappa^2 & 0 & 1+\kappa^2 & 0 \\ 0 & -\frac{\kappa^2}{1+2\kappa^2} & 0 & \frac{1+\kappa^2}{1+2\kappa^2} \end{pmatrix} \rightarrow \tag{6.46}$$

$$\overset{S_{\tilde r}\oplus S_{\tilde r}}{\longrightarrow} \begin{pmatrix} \frac{1+k^2}{\sqrt{1+2k^2}} & 0 & \frac{k^2}{\sqrt{1+2k^2}} & 0 \\ 0 & \frac{1+k^2}{\sqrt{1+2k^2}} & 0 & -\frac{k^2}{\sqrt{1+2k^2}} \\ \frac{k^2}{\sqrt{1+2k^2}} & 0 & \frac{1+k^2}{\sqrt{1+2k^2}} & 0 \\ 0 & -\frac{k^2}{\sqrt{1+2k^2}} & 0 & \frac{1+k^2}{\sqrt{1+2k^2}} \end{pmatrix}. \tag{6.47}$$

being $\tilde r = \frac{1}{4}\ln(1+2\kappa^2)$ a local squeezing. In this way we write the final state of the two atomic samples in standard form.

The resulting bipartite state of the two samples is pure and parametrized by κ only, thus it can be written as a two mode squeezed state

$$\gamma_{TMS} = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}, \tag{6.48}$$

with squeezing parameter $r = \frac{1}{2}\text{arccosh}(\frac{1+\kappa^2}{\sqrt{1+2\kappa^2}})$ (see lemma 2.5.2) *i.e.* containing pure EPR entanglement with negativity

$$E_N(\gamma_{TMS}) = \cosh^2 r \log_2 \cosh^2 r - \sinh^2 r \log_2 \sinh^2 r. \tag{6.49}$$

6.4 Entanglement eraser

Interesting enough, our geometrical approach also opens the possibility of deleting all the entanglement created by the first light beam, if intensities are appropriately adjusted. The entanglement procedure is intrinsically irreversible because of the projective measurement, so coming "deterministically" back to the initial state is not a trivial task. In [99, 100], a quantum erasing scheme in Continuous Variable systems was proposed. The measurement of the meter coordinate entangled with the quantum system leads to a back-action on it. The authors shown that it is possible to erase the action of the measurement and restore the original state of the system. Here we are interested in deleting the measurement induced entanglement between two atomic samples, exploiting the squeezing and antisqueezing effects produced by the laser beams.

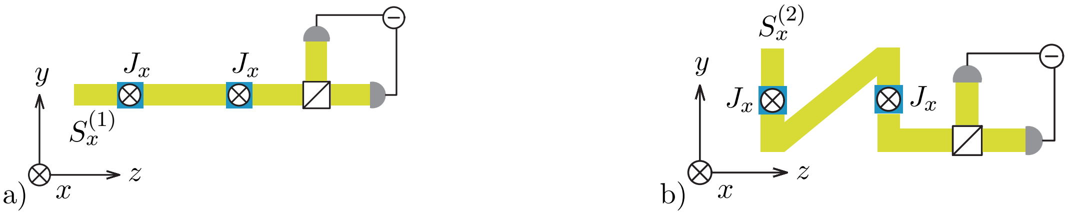

Figure 6.5: Entanglement eraser scheme realized by two pulses of different intensity, $\kappa_1^2 \propto N_{\text{ph}}^{(1)}$ and $\kappa_2^2 \propto N_{\text{ph}}^{(2)}$. See the text for details.

Let us assume that the first entangling beam, characterized by a coupling constant $\kappa_1^2 \propto N_{\text{ph}}^{(1)}$, propagates along the z-direction, exactly as it was described before (see Fig. 6.5(a)). The interaction, followed by the measurement of light, creates squeezing in the observable $\hat{J}_z^{(1)}+\hat{J}_z^{(2)}$ accompanied by antisqueezing in the conjugate variable $\hat{J}_y^{(1)} + \hat{J}_y^{(2)}$ (Eqs. (6.38) and (6.40)). Assume a second beam characterized by a coupling constant $\kappa_2^2 \propto N_{\text{ph}}^{(2)}$ propagates through the samples in an orthogonal direction with respect to the first beam as shown in Fig. 6.5(b). This corresponds to setting $\alpha = \pi/2$ in the Hamiltonian of Eq. (6.2). In this setup the measurement of the variable $\hat{S}_y^{\text{out}}$ introduces antisqueezing in the observable $\hat{J}_z^{(1)} + \hat{J}_z^{(2)}$ while squeezing in the conjugate variable $\hat{J}_y^{(1)} + \hat{J}_y^{(2)}$.

The bipartite state created by propagation and measurement of the first and second beam is characterized by the variances

$$\left(\Delta[J_y^{(1)} + J_y^{(2)}]\right)^2 = \frac{2\kappa_1^2+1}{\left(4\kappa_1^2+2\right)\kappa_2^2+1}\hbar J_x, \tag{6.50}$$

$$\left(\Delta[J_y^{(1)} - J_y^{(2)}]\right)^2 = \hbar J_x, \tag{6.51}$$

$$\left(\Delta[J_z^{(1)} + J_z^{(2)}]\right)^2 = \left(2\kappa_2^2 + \frac{1}{2\kappa_1^2+1}\right)\hbar J_x, \tag{6.52}$$

$$\left(\Delta[J_z^{(1)} - J_z^{(2)}]\right)^2 = \hbar J_x. \tag{6.53}$$

A close look at these equations shows that the second beam can lower or even completely destroy entanglement between the samples. This happens when

$$\kappa_2^2 = \frac{\kappa_1^2}{2\kappa_1^2+1}. \tag{6.54}$$

In such case the atomic ensembles are left in a vacuum (uncorrelated) state, however, displaced. Hence, the overall effect of these two beams is simply a displacement of the initial vacuum state. The value of the displacement depends on the coupling constants $\kappa_{1,2}$ and outputs obtained in the measurement of the light polarization component, $\hat{S}_y^{\text{out}}$, of both beams. Therefore, it will vary run to run.

Using negativity, computed by the symplectic eigenvalues of the partial transpose of the covariance matrix (2.97), one finds that indeed entanglement diminishes continuously or even disappears depending on the value of κ_2, as shown in Fig. 6.6. Notice that for every fixed value of κ_1 there always exists a value of κ_2 for which negativity becomes zero and the state becomes separable even though it was entangled after the first interaction and measurement on the beam.

6.5 Multipartite entanglement

In what follows we generalize our study to the multipartite scenario and we present different strategies to achieve multipartite entanglement without individual addressing. The strategies will not depend on the total number of samples but only if this number is odd or even. For the verification part, we shall adopt the criterium for multipartite entanglement, expressed via generalized inequalities for variances of quadratures, derived by van Loock and Furusawa [92]. We rewrite the inequalities for angular momentum variables as follows. If an N_s-mode state $\hat{\rho}$ is separable, then the sum of variances of the following operators

$$\begin{aligned} \hat{u} &= h_1\hat{J}_y^{(1)} + \ldots + h_{N_s}\hat{J}_y^{(N_s)}, \\ \hat{v} &= g_1\hat{J}_z^{(1)} + \ldots + g_{N_s}\hat{J}_z^{(N_s)}, \end{aligned} \tag{6.55}$$

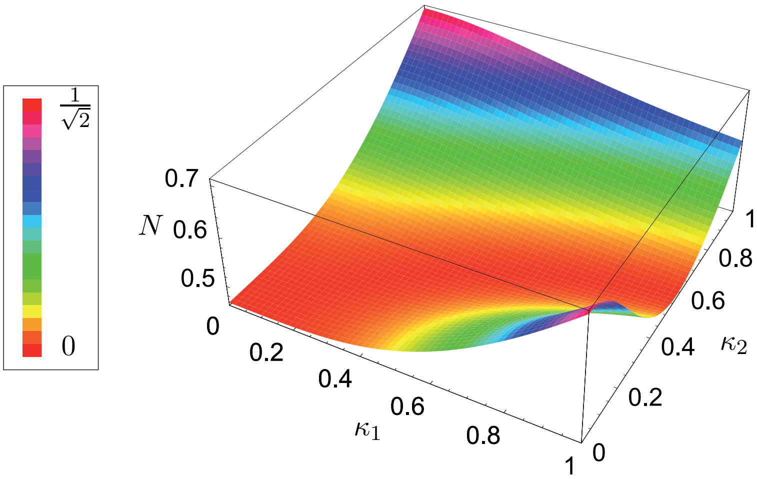

Figure 6.6: The negativity of a bipartite state of atomic ensembles after passage and measurement of two beams of coupling parameters κ_1 and κ_2 (see Fig. 6.5). For specific values of κ_1 and κ_2, *i.e.* fulfilling (6.54), the negativity approaches zero.

is bounded from above by a function of the coefficients $h_1, \ldots, h_{N_s}, g_1, \ldots, g_{N_s}$. Mathematically the inequality is expressed as

$$(\Delta \hat{u})^2 + (\Delta \hat{v})^2 \geq f(h_1, \ldots, h_{N_s}, g_1, \ldots, g_{N_s}) \hbar J_x, \tag{6.56}$$

with

$$f(h_1, \ldots, h_{N_s}, g_1, \ldots, g_{N_s}) = |h_m g_m + \sum_{r \in I} h_r g_r| + |h_n g_n + \sum_{s \in I'} h_s g_s|. \tag{6.57}$$

In the above formula two modes, m and n, are distinguished and the remaining modes are grouped in two disjoint sets I and I'. The criterion (6.56) holds for all bipartite splittings of a state defined by the sets of indices $\{m\} \cup I$ and $\{n\} \cup I'$, and for every choice of parameters $h_1, \ldots, h_{N_s}, g_1, \ldots, g_{N_s}$. For example, in case of three samples we have $f(h_1, h_2, h_3, g_1, g_2, g_3) = (|h_n g_n| + |h_k g_k + h_m g_m|)$, where (n, m, k) is some permutation of the sequence $(1, 2, 3)$, and the coefficients $h_1, h_2, h_3, g_1, g_2, g_3$ are arbitrary real numbers.

6.5.1 GHZ-like states

Genuine multipartite entanglement between any number of equally polarized atomic modes can be obtained with a single beam propagating through all of them followed by a projective measurement of the light. After the measurement, the N_s-mode variable $\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(N_s)}$ is squeezed. This is a trivial extension of the bipartite scheme schematically shown in Fig. 6.3(a).

The phenomenon of destruction of entanglement by squeezing of the conjugate variable, which was discussed in the previous section for two modes, can be also found in the multimode setup. The entanglement prepared with the light beam characterized by the coupling constant κ_1 can be erased by the second orthogonal beam with appropriately adjusted intensity. The relation between the coupling constants for which entanglement is removed from the system is

$$\kappa_2^2 = \frac{\kappa_1^2}{N_s\kappa_1^2 + 1}. \tag{6.58}$$

One can see that with increasing number of samples the value of κ_2 required to delete entanglement decreases.

To generate a maximally entangled GHZ state with N_s-parties, simultaneous squeezing in more independent variables is needed. By independent here we mean commuting linear combinations of atomic spin operators. The most straightforward way to do it is to generate squeezing in the variable $\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(N_s)}$ and in the pairwise differences of angular momenta: $\hat{J}_y^{(i)} - \hat{J}_y^{(j)}$ $(1 \leq i, j \leq N_s,\ i \neq j)$ (see [49, 6]). An entangled state with such properties can be realized by generalization of the bipartite scheme summarized in Figs. 6.4(a) and 6.4(b). Notice, however, that the last step b) should be repeated for all combinations of $i > j$. The final variances characterizing the state would be

$$\left(\Delta[\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(N_s)}]\right)^2 = \frac{N_s}{2 + 2N_s\kappa^2}\hbar J_x, \tag{6.59}$$

$$\left(\Delta[\hat{J}_y^{(i)} - \hat{J}_y^{(j)}]\right)^2 = \frac{1}{1 + N_s\kappa^2}\hbar J_x \quad (i \neq j). \tag{6.60}$$

Thus the samples are in a genuine N_s-mode GHZ state. Within this scheme the number of measurements, $\binom{N_s}{2} + 1 \sim \frac{N_s^2}{2}$, one has to perform in order to create genuine entanglement, grows quadratically with the number of samples. Also verification implies checking all the inequalities of the type

$$\left(\Delta[\hat{J}_y^{(i)} - \hat{J}_y^{(j)}]\right)^2 + \left(\Delta[\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(N_s)}]\right)^2 \geq 2\hbar J_x \quad (i > j).$$

While the above procedure works for an arbitrary number of samples, to optimize it we consider separately even and odd N_s.

For even number of ensembles $N_s = 2M$ the optimal approach generalizes the one proposed for two samples and summarized in Figs. 6.4(a) and 6.4(b). In first step we generate squeezing in $\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(2M)}$. As the second step we squeeze the observable $\hat{J}_y^{(1)} - \hat{J}_y^{(2)} + \ldots + (-1)^{2M-1}\hat{J}_y^{(2M)}$ with the second beam passing through the ith sample at an angle $(-1)^{i-1}\pi/2$. The final state is pure and genuine multipartite entangled. The entanglement can be detected using the criterion (6.56) with the two squeezed observables discussed in this paragraph. The measurement of light propagating through the ith sample at an angle $(-1)^{i-1}\pi/4$ gives at the level of variances

$$\begin{aligned}
&\left(\Delta\hat{S}_y^{\mathrm{out}}\right)^2 = \left(\Delta\hat{S}_y^{\mathrm{in}}\right)^2 + \\
&+\frac{\kappa^2}{2}\frac{S_x}{J_x}\left(\Delta[\hat{J}_y^{(1)} - \hat{J}_y^{(2)} + \ldots + (-1)^{2M-1}\hat{J}_z^{(2M)}]\right)^2 + \\
&+\frac{\kappa^2}{2}\frac{S_x}{J_x}\left(\Delta[\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(2M)}]\right)^2 . \qquad (6.61)
\end{aligned}$$

Therefore, again a single beam can be used for verification of entanglement. The same criterion and the above measurement scheme can be applied not only to detect the entanglement in the above setup but also in those proposed before, *i.e.*, (i) the state with squeezing only in $\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(2M)}$ (after interaction and measurement of only the first beam), and (ii) the state with squeezing in $\hat{J}_z^{(1)} + \ldots + \hat{J}_z^{(2M)}$ and all combinations $\hat{J}_y^{(i)} - \hat{J}_y^{(j)}$ $(i \neq j)$. The reduction in the number of measurements is significant. Moreover, a recently proposed multi-pass technique [101] could lead to a simplification of the geometry.

Optimization of the scheme for odd number of atomic ensembles within this geometric approach is to our knowledge not possible. Even though it is possible to find independent variables involving all the samples, it is not clear what geometry should be applied in order to measure these operators.

A different way to deal with multimode entanglement of odd number of samples is to generalize directly the bipartite scheme of Julsgaard *et al*, *i.e.*, polarize the samples in such a way that the collective polarization $\sum_i J_x^{(i)}$ is zero. Moreover, each sample should experience a different local magnetic field. In such system it is possible to generate squeezing in appropriately redefined (due to Larmor precession) operators $\sum_i \hat{J}_y^{(i)}$ and $\sum_i \hat{J}_z^{(i)}$, using a single light beam. This is possible due to the choice of the initial polarization of the samples making the redefined operators to commute. Analogously to the bipartite case the entanglement test that can be applied involves measurement of variances of the sums of angular momentum components and reads

$$\left(\Delta\sum_i \hat{J}_y^{(i)}\right)^2 + \left(\Delta\sum_i \hat{J}_z^{(i)}\right)^2 \geq N_s\hbar J_x. \qquad (6.62)$$

6.5.2 Cluster-like states

In [102] a class of N-qubit quantum states generated in an arrays of qubits with an Ising-type interaction were presented, the so-called cluster states. While for pure states of bipartite qubit systems there is a single “unit” of entanglement, the one contained in a Bell state, for three or more parties several inequivalent classes exists. Cluster states, generated in optical lattices and similar systems, can be regarded as an entanglement resource since one can generate a family of other multipartite entangled states by simply performing measurement and using classical communication. Using the scalability properties of cluster states, Hans Briegel *et al* presented a scheme for scalable one-way quantum computation [103, 104]. In there, cluster states are the entire resource for quantum computation while computation consists of a sequence of one-qubit projective measurements on them driving the computation. It is an universal quantum computer since any unitary quantum logic network can be simulated on it efficiently.

We detail here, how the analyzed setup allows for generation of Continuous Variable cluster-like states [105]. We associate the modes of the N_s-mode system with the vertices of a graph G. The edges between the vertices define the notion of nearest neighborhood. By N_a we denote the set of nearest neighbors of vertex a. A cluster is a connected graph. For angular momentum variables, cluster states are defined only asymptotically as those with infinite squeezing in the variables

$$\hat{J}_z^{(a)} - \sum_{b\in N_a} \hat{J}_y^{(b)}, \tag{6.63}$$

for all $a \in G$. Cluster-like states are defined when the squeezing is finite. Given a set of N_s atomic ensembles, it is possible to create a chosen cluster-like state by squeezing the required combinations of variables (6.63). Since they commute, it is possible to squeeze them sequentially. Hereafter, we will illustrate the procedure by a simple example. The method is general and can be applied to create any cluster-like state.

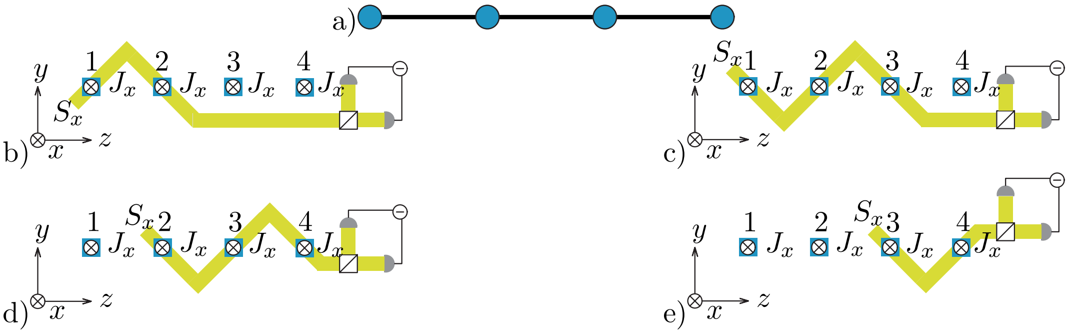

Figure 6.7: Generation of the cluster state schematically depicted in a). The sequence of beams squeeze the following variables: b) $\hat{J}_z^{(1)\prime} - \hat{J}_y^{(2)\prime}$, c) $\hat{J}_z^{(2)\prime} - \hat{J}_y^{(1)\prime} - \hat{J}_y^{(3)\prime}$, d) $\hat{J}_z^{(3)\prime} - \hat{J}_y^{(2)\prime} - \hat{J}_y^{(4)\prime}$, e) $\hat{J}_z^{(4)\prime} - \hat{J}_y^{(3)\prime}$.

In Fig. 6.7 we show how to create the simplest 4-site (linear) cluster state. Let us introduce the new variables for each sample

$$\begin{aligned} \hat{J}_y^{(i)\prime} &= \frac{1}{\sqrt{2}}\left(\hat{J}_y^{(i)} - \hat{J}_z^{(i)}\right), \\ \hat{J}_z^{(i)\prime} &= \frac{1}{\sqrt{2}}\left(\hat{J}_y^{(i)} + \hat{J}_z^{(i)}\right). \end{aligned} \tag{6.64}$$

The squeezing in the combinations of the new variables is produced by passing light as depicted in Figs. 6.7(b)-6.7(e). For example the squeezing in $\hat{J}_z^{(1)\prime} - \hat{J}_y^{(2)\prime}$ is generated when light passes only through samples 1 and 2 at angles $\pm\pi/4$ respectively (see Fig. 6.7(b)). All the other required combinations are squeezed in a similar way.

In order to verify that the state is entangled it is enough to check the set of variance inequalities given in [106]. This can be done, for example, by repetition of each step as first proposed in [79, 97].

6.6 Conclusions

In this chapter, we have studied multipartite mesoscopic entanglement using a quantum atom-light interface in various physical setups, in particular those in which the ensembles cannot be addressed individually. Exploiting a geometric approach in which light beams propagate through the atomic samples at different angles makes it possible to establish and verify EPR bipartite entanglement and GHZ multipartite entanglement with a minimal number of light passages and measurements, so that the quantum non-demolition character of the interface is preserved. We have also shown how to generate cluster-like states by a similar technique.

Furthermore, we have shown that the multipartite entanglement created by the quantum interface of a single light beam can be appropriately tailored and even completely erased by the action of a second pulse with different intensity. This control widens the possibilities offered by measurement induced entanglement to perform quantum information tasks.

6.A Appendix: Detailed atom-light interactions

6.A.1 Interaction Hamiltonian

We detail here the derivation of the effective Hamiltonian (see [13, 80, 93, 107]) coupling atoms and light in the off-resonant limit, neglecting absorption effects and spontaneous emission which is justified if the detuning from the optical transition is large enough. Dispersion effects can change the polarization state of the light if the sample is birefringent *i.e.* the index of refraction is different for orthogonal polarization components. In our scheme, x-polarized light propagates in the z-direction through the atomic samples which is polarized along the x-axis. Thus, x is an optical axis that leaves unchanged the x and y polarizations of light. In what follows, we omit dispersion effects considering that the linear birefringence is zero. We will concentrate more on the continuous description of light and matter since it is convenient for describing the time dynamics of the system.

We consider real cesium atoms with its hyperfine split ground state and excited states, and coupling them off-resonantly to the $6S_{1/2} \rightarrow 6P_{3/2}$ dipole transition (see Fig. 6.8). The interaction Hamiltonian, $\hat{H}_{\text{int}} = -\sum_j \hat{\vec{d}}_j \cdot \hat{\vec{E}}(\vec{r}_j)$, in the rotating wave approximation, eliminating adiabatically the excited states turns in

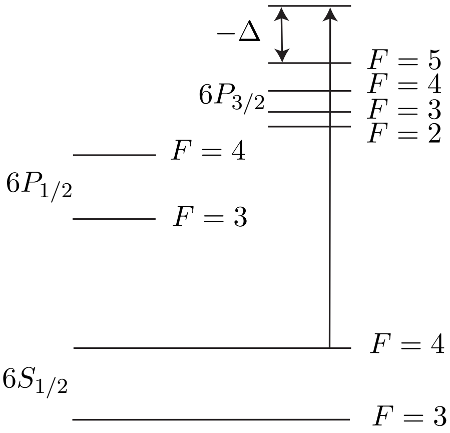

Figure 6.8: Atomic energy levels for the cesium.

$$\begin{aligned}\hat{H}_{\rm int}(t) &= -a\int_0^L (a_0\hbar^2\hat{\phi}(z,t) + a_1\hat{s}_z(z,t)\hat{j}_z(z,t) + \\ &+a_2\left[\hbar\hat{\phi}(z,t)\hat{j}_z(z,t) - \frac{1}{\hbar}\hat{s}_-(z,t)\hat{j}_-^2(z,t) - \frac{1}{\hbar}\hat{s}_+(z,t)\hat{j}_-^2(z,t)\right])\rho A dz = \\ &= \int_0^L \hat{h}_{\rm int}(z,t)\rho A dz \qquad (6.65)\end{aligned}$$

coupling the spin degrees of freedom of atoms and the Stokes vector of light. The parameter $a = \frac{\gamma}{8A\Delta}\frac{\lambda^2}{2\pi}$ is a coupling constant with A being the cross section, λ the wave length of light, Δ the detuning energy and γ the frequency width of the atomic excited states. As one can see from the above expression, the detuning should not be too large for the interaction not to vanish. The first term proportional to a_0 amounts for a Stark shift to all atoms proportional to the photon density $\hat{\phi}(z,t) = \frac{\hbar}{2}(\hat{n}_x + \hat{n}_y) = \frac{\hbar}{2}(\hat{a}_x^\dagger\hat{a}_x + \hat{a}_y^\dagger\hat{a}_y)$. The second term proportional to a_1, known as the Faraday rotation, rotate around the z-axis the spin vector and the Stokes vector. The last terms proportional to a_2 are higher orders coupling light and atoms. All these terms conserve the total angular momentum of light and atoms. As usual we have defined ladder operators for light $\hat{s}_\pm(z,t) = \hat{s}_x \pm \mathrm{i}\hat{s}_y = -\frac{\hbar}{2}\hat{a}_\pm^\dagger\hat{a}_\mp$ and for angular momentum $\hat{j}_\pm(z,t) = \hat{j}_x \pm \mathrm{i}\hat{j}_y$ [6]. For the particular case of Cesium on $F=4$ and large detuning, $a_0 \to 4$, $a_1 \to 1$, $a_2 \to 0$. Additionally the Stark shift term can be suppressed by shifting the energy, thus we restrict ourselves to the linear coupling *i.e.* we can fix the constants to the corresponding values $a_0 = a_2 = 0$ and $a_1 = 1$. Performing a time and space integration to write the Hamiltonian in terms of the macroscopical variables $\hat{S}_k$ and $\hat{J}_k = \int_0^L \hat{j}_k(z,t)\rho A dz$, being ρ the spin density, then

$$\hat{H}_{\rm int}^{\rm eff} = \frac{1}{T}\int_0^T dt\hat{H}_{\rm int}(t) = -\frac{a}{T}\int_0^T dt\int_0^L \hat{s}_z(z,t)\hat{j}_z(z,t)\rho A dz = -\frac{a}{T}\hat{S}_z\hat{J}_z, \qquad (6.66)$$

[6] Choosing z as the axis of quantization, we know from any elementary book on Quantum Me-

and we recover (6.2) for $\alpha = 0$ *i.e.*, when the light propagates along the z-axis while the sample is polarized along x.

6.A.2 Equations of evolution

The total Hamiltonian $\hat{h}_{\text{tot}} = \hat{h}_A + \hat{h}_L + \hat{h}_{\text{int}}$ contains the Hamiltonian for atoms (A), light (L) and the interaction (int). The effective Hamiltonian governs the atomic dynamics and the evolution equations are derived straight through the Heisenberg equations for matter and Maxwell-Bloch equations (neglecting retardation effects) for light. We derive the equations of evolution for light an atoms in the following.

Heisenberg evolution for light can be recasted to a Maxwell-Block evolution for the ladder operators as follows

$$\begin{aligned}
\frac{\partial}{\partial t}\hat{a}(z,t) &= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\frac{\partial}{\partial t}\hat{a}(k,t)e^{\mathrm{i}kz}dk = \\
&= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\frac{1}{\mathrm{i}\hbar}[\hat{a}(k,t),\hat{h}_A+\hat{h}_L+\hat{h}_{\text{int}}]e^{\mathrm{i}kz}dk = \\
&= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\frac{1}{\mathrm{i}\hbar}\left(\int_{-\infty}^{\infty}dk'\hbar ck'[\hat{a}(k,t),\hat{a}^\dagger(k',t)]\hat{a}(k',t)\right)e^{\mathrm{i}kz}dk + \\
&+ \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\frac{1}{\mathrm{i}\hbar}[\hat{a}(k,t),\hat{h}_{\text{int}}]e^{\mathrm{i}kz}dk = \frac{1}{\mathrm{i}\hbar}[\hat{a}(z,t),\hat{h}_{\text{int}}] - \\
&- \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\mathrm{i}ck\hat{a}(k,t)e^{\mathrm{i}kz}dk = \frac{1}{\mathrm{i}\hbar}[\hat{a}(z,t),\hat{h}_{\text{int}}] - c\frac{\partial}{\partial z}\hat{a}(z,t),
\end{aligned}$$

finally $(\frac{\partial}{\partial t}+c\frac{\partial}{\partial z})\hat{a}(z,t) = \frac{1}{\mathrm{i}\hbar}[\hat{a}(z,t),\hat{h}_{\text{int}}]$. As said, we will neglect retardation effects, *i.e.* we do not calculate dynamics on the time scale L/c of propagation across the sample (equivalently we set $c \to \infty$).

In terms of the Stokes components then the evolution for light reads

$$\frac{\partial}{\partial z}\hat{s}_i(z,t) = \frac{1}{\mathrm{i}\hbar c}[\hat{s}_i(z,t),\hat{h}_{\text{int}}(z,t)], \tag{6.67}$$

while for atoms, Heisenberg evolution equations are

$$\frac{\partial}{\partial t}\hat{j}_i(z,t) = \frac{1}{\mathrm{i}\hbar}[\hat{j}_i(z,t),\hat{h}_{\text{int}}(z,t)]. \tag{6.68}$$

chanics that

$$\begin{aligned}
\hat{j}_x &= \frac{1}{2}\sum_{m_F}\sqrt{F(F+1)-m_F(m_F+1)}\left(|m_F+1\rangle\langle m_F| + |m_F\rangle\langle m_F+1|\right), \\
\hat{j}_y &= \frac{1}{2\mathrm{i}}\sum_{m_F}\sqrt{F(F+1)-m_F(m_F+1)}\left(|m_F+1\rangle\langle m_F| - |m_F\rangle\langle m_F+1|\right), \\
\hat{j}_z &= \sum_{m_F}m_F|m_F\rangle\langle m_F|.
\end{aligned}$$

.

Evolution for the ortogonal y and z components using Eqs. (6.67),(6.68), the interacting Hamiltonian (6.65) in the linear regime, *i.e.* setting $a_0 = a_2 = 0$ and $a_1 = 1$ together with the commutation rules [7] gives rise to

$$\frac{\partial}{\partial t}\hat{j}_y(z,t) = -a\hat{s}_z(z,t)\hat{j}_x, \tag{6.69}$$

$$\frac{\partial}{\partial t}\hat{j}_z(z,t) = 0, \tag{6.70}$$

$$\frac{\partial}{\partial z}\hat{s}_y(z,t) = -\frac{a}{c}\hat{s}_x\hat{j}_z(z,t)\delta(t-t'), \tag{6.71}$$

$$\frac{\partial}{\partial z}\hat{s}_z(z,t) = 0. \tag{6.72}$$

Strong x-polarized atoms and light imposes $\hat{j}_x(z,t) = j_x$ and $\hat{s}_x(z,t) = s_x$, thus

$$\hat{j}_x(z,t) = j_x, \tag{6.73}$$

$$\frac{\partial}{\partial t}\hat{j}_y(z,t) = -a\hat{s}_z(t)j_x, \tag{6.74}$$

$$\hat{j}_z(z,t) = \hat{j}_z(z), \tag{6.75}$$

$$\hat{s}_x(z,t) = s_x, \tag{6.76}$$

$$\frac{\partial}{\partial z}\hat{s}_y(z,t) = -\frac{a}{c}s_x\hat{j}_z(z)\delta(t-t'), \tag{6.77}$$

$$\hat{s}_z(z,t) = \hat{s}_z(t). \tag{6.78}$$

Finally, we integrate in space ($\int_0^L \rho A dz$) and time ($\int_0^T dt$) to recover the equations of evolution for the macroscopical variables of atoms and light

$$J_x = \int_0^L \hat{j}_x(z,t)\rho A dz = j_x, \tag{6.79}$$

$$\hat{J}_y(t=T) - \hat{J}_y(t=0) = -a\hat{S}_z J_x, \tag{6.80}$$

$$\hat{J}_z = \int_0^L \hat{j}_z(z)\rho A dz = J_z(t=0) = J_z(t=T), \tag{6.81}$$

$$S_x = \int_0^T \hat{s}_x(z,t)dt = s_x T, \tag{6.82}$$

$$\hat{S}_y(z=L) - \hat{S}_y(z=0) = -aS_x\hat{J}_z, \tag{6.83}$$

$$\hat{S}_z = \int_0^T \hat{s}_z(t)dt = \hat{S}_z(z=0) = \hat{S}_z(z=L). \tag{6.84}$$

[7] For light $[\hat{S}_i, \hat{S}_j] = [\int_0^T \hat{s}_i(t)dt, \int_0^T \hat{s}_j(t')dt'] = i\hbar \int_0^T \int_0^T dtdt'\epsilon_{ijk}\hat{s}_k(t)\delta(t-t') = i\hbar\epsilon_{ijk}\int_0^T \hat{s}_k(t)dt = i\hbar\epsilon_{ijk}\hat{S}_k$ and atoms $[j_i\hat{(z)}, j_j\hat{(z)}] = i\hbar\epsilon_{ijk}\hat{j}_k(z)$.

In the following, it will be useful to think in terms of input/output variables, *i.e.* we define the operators $\hat{S}_k^{\mathrm{in/out}}$ as the Stokes operators characterizing the pulse entering ($z = 0$) and leaving ($z = L$) the atomic sample. Analogously, $\hat{J}_k^{\mathrm{in/out}}$ correspond to initial ($t = 0$) and final state ($t = T$) of the atomic spin. In this way we can write the evolution as a linear equation system

$$\hat{J}_y^{\mathrm{out}} = \hat{J}_y^{\mathrm{in}} - a\hat{S}_z^{\mathrm{in}} J_x, \tag{6.85}$$

$$\hat{J}_z^{\mathrm{out}} = \hat{J}_z^{\mathrm{in}}, \tag{6.86}$$

$$\hat{S}_y^{\mathrm{out}} = \hat{S}_y^{\mathrm{in}} - aS_x\hat{J}_z^{\mathrm{in}}, \tag{6.87}$$

$$\hat{S}_z^{\mathrm{out}} = \hat{S}_z^{\mathrm{in}}, \tag{6.88}$$

recovering Eqs. (6.3)-(6.6) for $\alpha = 0$ *i.e.*, when the light propagates along the z-axis while the sample is polarized along x.

Chapter 7

Conclusions

Summarizing we have studied several quantum protocols with Continuous Variable (CV) systems giving special importance to the efficiency such protocols can achieve when considering current experimental possibilities. Independently of future technological improvements, noise is intrinsically ascribed to any measurement and manipulation. We have taken into account that, but also we have considered non-ideal Gaussian resources and imperfections on the experimental realization. Regarding Gaussian multipartite entanglement, we have used entanglement induced measurement schemes, for the creation and manipulation of multipartite entanglement while proposing a possible candidate physical system for its realization. Finally, motivated by the performance enhancement offered by non-Gaussian states for communication tasks, we have analyzed and proposed a correlation measure based on quadrature correlations. Our measure, provides an excellent quantification of correlations not only for Gaussian states but also for non-Gaussian states, where determination of entanglement is normally not known. Furthermore, our measure has a low computable cost compared to other methods which require a full tomographic analysis of the state.

Specifically, we have first shown that the sharing of entangled Gaussian variables and the use of only Gaussian operations permits efficient Quantum Key Distribution against individual and finite coherent attacks. We have used the fact that all mixed NPPT symmetric states can be used to extract secret bits to design an algorithm, that efficiently succeeds for a secure extraction of a key. Whereas under individual attacks all mixed NPPT symmetric states admit a finite efficiency, for finite coherent attacks an additional condition constrains the parameters of the states. We have introduced a figure of merit (the efficiency E) to quantify the number of classical correlated bits that can be used to distill a key from a sample of M entangled states. We have observed that this quantity grows with the entanglement shared between Alice and Bob.

Secondly, we have proposed a protocol to solve detectable broadcast with entangled Continuous Variable using Gaussian states and Gaussian operations only. Our protocol relies on genuine multipartite entanglement distributed among the three parties, which specifically have to share two copies of a three-mode fully symmetric Gaussian state. Interestingly, we have found that nevertheless not all entangled symmetric Gaussian states can be used to achieve a solution to detectable broadcast: a minimum threshold exists on the required amount of multipartite entanglement. We have moreover analyzed in detail the security of the protocol. In its ideal formulation, our protocol requires that the parties share pure resource states, and that the outcomes of homodyne detections are perfectly coincident and not affected by any uncertainty; this however entails that our protocol achieves a solution with vanishing probability. To overcome such a practical limitation, we have eventually considered a more realistic situation in which firstly the tripartite Gaussian resources are affected by thermal noise, and, more importantly, the homodyne detections are realistically imperfect, and secondly there is a finite range of allowed values for the measurement outcomes obtained by the parties. We have thoroughly investigated the possibility to solve detectable broadcast via our protocol under these relaxed conditions. As a result, we have demonstrated that there exists a broad region in the space of the relevant parameters (noise, entanglement, range of the measurement shift, measurement uncertainty) in which the protocol admits an efficient solution. This region encompasses amounts of the required resources which appear attainable with the current optical technology (with a legitimate trade-off between squeezing and losses). We can thus conclude that a feasible, robust implementation of our protocol to solve detectable broadcast with entangled Gaussian states may be in reach.

Motivated by the relation between the entanglement and the distillation of classically correlated bits we analyzed which is the maximal number of correlated bits (Q) that can be extracted from a CV state via quadrature measurements. We have provided an operational quantification of the entanglement content of several relevant non-Gaussian states (including the useful photon-subtracted states). Crucially, one can experimentally measure Q by direct homodyne detections (of the quadratures displaying optimal correlations only), in contrast to the much more demanding full tomographical state reconstruction. One can then easily invert the (analytic or numeric) monotonic relation between Q and the negativity to achieve a direct entanglement quantification from the measured data. Our analysis demonstrates the rather surprising feature that entanglement in the considered non-Gaussian states can thus be detected and experimentally quantified with the same complexity as if dealing with Gaussian states. In this respect, it is even more striking that the measure considered in this paper, based on (and accessible in terms of) second moments and homodyne detections only, provides such an exact quantification of entanglement in a broad class of pure and mixed non-Gaussian states, whose quantum correlations are encoded nontrivially in higher moments too, and currently represent the preferred resources in CV Quantum Information. We focused on optical realizations of CV systems, but our framework equally applies to collective spin components of atomic ensembles, and radial modes of trapped ions. Finally, it is also surprising that for all these family of states we have studied, the optimization of just one quadrature scales monotonically with the negativity of the state. Although this could be expected for pure Gaussian states, our study demonstrated that the non-Gaussian states obtained either as de-gaussifications of pure Gaussian states or mixings with uncorrelated states preserve this property.

Finally, we have studied multipartite mesoscopic entanglement using a quantum atom-light interface in various physical setups, in particular those in which the ensembles cannot be addressed individually. Exploiting a geometric approach in which light beams propagate through the atomic samples at different angles makes it possible to establish and verify EPR bipartite entanglement and GHZ multipartite entanglement with a minimal number of light passages and measurements, so that the quantum non-demolition character of the interface is preserved. We have also shown how to generate cluster-like states by a similar technique. Furthermore, we have shown that the multipartite entanglement created by the quantum interface of a single light beam can be appropriately tailored and even completely erased by the action of a second pulse with different intensity. This control widens the possibilities offered by measurement induced entanglement to perform quantum information tasks.

Bibliography

[1] C. Rodó, O. Romero-Isart, K. Eckert, and A. Sanpera. Efficiency in quantum key distribution protocols with entangled gaussian states. *Open Sys. Inf. Dyn.*, **14**(69), 2007.

[2] R. Neigovzen, C. Rodó, G. Adesso, and A. Sanpera. Multipartite continuous-variable solution for the byzantine agreement problem. *Phys. Rev. A*, **77**(062307), 2008.

[3] C. Rodó, G. Adesso, and A. Sanpera. Operational quantification of continuous-variable correlations. *Phys. Rev. Lett.*, **100**(110505), 2008.

[4] J. Stasińska, C. Rodó, S. Paganelli, G. Birkl, and A. Sanpera. Manipulating mesoscopic multipartite entanglement with atom-light interfaces. *Phys. Rev. A*, **80**(062304), 2009.

[5] J. Stasińska, S. Paganelli, C. Rodó, and A. Sanpera. A covariance matrix formalism for atom-light interfaces. 2010.

[6] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, **77**(513), 2005.

[7] P. van Loock. Quantum communication with continuous variables. *Fortschr. Phys.*, **12**(1177), 2002.

[8] W.-M. Zhang. Coherent states: Theory and some applications. *Rev. Mod. Phys.*, **62**(867), 1990.

[9] G. Adesso and F. Illuminati. Entanglement in continuous-variable systems: recent advances and current perspectives. *J. Phys. A: Math. Theor.*, **40**(7821), 2007.

[10] A. Ferraro, S. Olivares, and M. G. A. Paris. Gaussian states in continuous variable quantum information. *ArXiv:quant-ph*, **0503.237**, 2005.

[11] M. Hillery, R. F. O'Connell, M. O. Scully, and E. P. Wigner. Distribution functions in physics: Fundamentals. *Phys. Rep.*, **106**(121), 1984.

[12] H.-W. Lee. Theory and application of the quantum phase-space distribution functions. *Phys. Rep.*, **259**(147), 1995.

[13] K. Hammerer, A. S. Sørensen, and E. S. Polzik. Quantum interface between light and atomic ensembles. *ArXiv:quant-ph*, **0807.3358**, 2008.

[14] A. Serafini, A. Retzker, and M. B. Plenio. Manipulating the quantum information of the radial modes of trapped ions: linear phononics, entanglement generation, quantum state transmission and non-locality tests. *New. J. Phys.*, **11**(023007), 2009.

[15] D. F. Styer, M. S. Balkin, K. M. Becker, M. R. Burns, C. E. Dudley, S. T. Forth, J. S. Gaumer, M. A. Kramer, D. C. Oertel, L. H. Park, M. T. Rinkoski, C. T. Smith, and T. D. Wotherspoon. Nine formulations of quantum mechanics. *Am. J. Phys.*, **70**(3), 2002.

[16] G. Giedke and J. I. Cirac. Characterization of gaussian operations and distillation of gaussian states. *Phys. Rev. A*, **66**(032316), 2002.

[17] J. R. Klauder and B.-S. K. Skagerstam. Generalized phase-space representation of operators. *J. Phys. A: Math. Theor.*, **40**(2093), 2007.

[18] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, **77**(1413), 1996.

[19] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, **223**(1), 1996.

[20] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, **84**(2726), 2000.

[21] R. F. Werner and M. M. Wolf. Bound entangled gaussian states. *Phys. Rev. Lett.*, **86**(3658), 2001.

[22] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller. Inseparability criterion for continuous variable systems. *Phys. Rev. Lett.*, **84**(2722), 2000.

[23] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, **65**(032314), 2002.

[24] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signals Processing, Bangalore, India,* **(IEEE, New York)**(page 175), 1984.

[25] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, **67**(661), 1991.

[26] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, **68**(557), 1992.

[27] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, **21**(217903), 2004.

[28] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, **63**(022309), 2001.

[29] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, **88**(057902), 2002.

[30] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, **89**(167901), 2002.

[31] D. Deutsch, A. K. Ekert, R. Jozsa, S. Popescu, C. Macchiavello, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, **77**(2818), 1996.

[32] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett.*, **94**(160502), 2005.

[33] M. Navascués, J. Bae, J. I. Cirac, M. Lewenstein, A. Sanpera, and A. Acín. Quantum key distillation from gaussian states by gaussian operations. *Phys. Rev. Lett.*, **94**(010502), 2005.

[34] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory*, **39**(733), 1993.

[35] A. Acín, Ll. Massanes, and N. Gisin. Equivalence between two-qubit entanglement and secure key distribution. *Phys. Rev. Lett.*, **91**(167901), 2003.

[36] M. Christandl, R. Renner, and A. K. Ekert. A generic security proof for quantum key distribution. *ArXiv:quant-ph*, **0402131**, 2004.

[37] L. Lamport and M. J. Fischer. Byzantine generals and transaction commit protocols. *SRI Interntional*, **62**(unpublished), 1982.

[38] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, **4**(382), 1982.

[39] M. Fitzi, N. Gisin, and U. M. Maurer. Quantum solution to the byzantine agreement problem. *Phys. Rev. Lett.*, **87**(217901), 2001.

[40] M. Fitzi, D. Gottesman, M. Hirt, T. Holenstein, and A. Smith. Detectable byzantine agreement secure against faulty majorities. *Proceedings of the Twenty-first Annual Symposium on Principles of Distributed Computing, Monterey, California*, **3**(118), 2002.

[41] S. Iblisdir and N. Gisin. Byzantine agreement with two quantum-key-distribution setups. *Phys. Rev. A*, **70**(034306), 2004.

[42] A. Cabello. Solving the liar detection problem using the four-qubit singlet state. *Phys. Rev. A*, **68**(012304), 2003.

[43] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter. Experimental demonstration of a quantum protocol for byzantine agreement and liar detection. *Phys. Rev. Lett.*, **100**(070504), 2008.

[44] F. Grosshans, A. Acín, and N. J. Cerf. Continuous variable quantum key distribution. *Imperial College Press, London*, **4** in Quantum Information with Continuous Variables of Atoms and Light(63), 2007.

[45] F. Grosshans, G. van Assche, J. Wenger, R. Brourl, N. J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, **421**(238), 2003.

[46] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, **76**(042305), 2007.

[47] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quantum Inf. Comput.*, **7**(1), 2007.

[48] N. J. Cerf, G. Leuchs, and E. S. Polzik. Quantum information with continuous variables of atoms and light. *Imperial College Press, London*, 2007.

[49] P. van Loock and S. L. Braunstein. Multipartite entanglement for continuous variables: A quantum teleportation network. *Phys. Rev. Lett.*, **84**(3482), 2000.

[50] H. Yonezawa, T. Aoki, and A. Furusawa. Demonstration of a quantum teleportation network for continuous variables. *Nature*, **431**(430), 2004.

[51] G. Adesso and F. Illuminati. Strong monogamy of bipartite and genuine multipartite entanglement: The gaussian case. *Phys. Rev. Lett.*, **99**(150501), 2007.

[52] G. Adesso and F. Illuminati. Continuous variable tangle, monogamy inequality, and entanglement sharing in gaussian states of continuous variable systems. *New. J. Phys.*, **8**(15), 2006.

[53] Y. Lian, C. Xie, and K. Peng. Continuous variable multipartite entanglement and optical implementations of quantum communication networks. *New. J. Phys.*, **9**(314), 2007.

[54] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. *Phys. Rev. Lett.*, **87**(040401), 2001.

[55] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac. Separability properties of three-mode gaussian states. *Phys. Rev. A*, **64**(052303), 2001.

[56] S. L. Braunstein and H. J. Kimble. A posteriori teleportation. *Nature*, **394**(47), 1998.

[57] G. Adesso, A. Serafini, and F. Illuminati. Optical state engineering, quantum communication, and robustness of entanglement promiscuity in three-mode gaussian states. *New. J. Phys.*, **9**(60), 2007.

[58] T. Aoki, N. Takei, H. Yonezawa, K. Wakui, T. Hiraoka, A. Furusawa, and P. van Loock. Experimental creation of a fully inseparable tripartite continuous variable state. *Phys. Rev. Lett.*, **91**(080404), 2003.

[59] S. Suzuki, H. Yonezawa, F. Kannari, M. Sasaki, and A. Furusawa. 7 db quadrature squeezing at 860 nm with periodically poled ktiopo4. *Appl. Phys. Lett.*, **89**(061116), 2006.

[60] Y. Takeno, M. Yukawa, H. Yonezawa, and A. Furusawa. Observation of -9 db quadrature squeezing with improvement of phase stability in homodyne measurement. *Opt. Express*, **15**(4321), 2007.

[61] H. Vahlbruch, S. Chelkowski, K. Danzmann, and R. Schnabel. Quantum engineering of squeezed states for quantum communication and metrology. *New. J. Phys.*, **9**(371), 2007.

[62] M. M. Wolf, G. Giedke, and J. I. Cirac. Extremality of gaussian quantum states. *Phys. Rev. Lett.*, **96**(080502), 2006.

[63] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Phys. Rev. Lett.*, **89**(137903), 2002.

[64] J. Fiurášek. Gaussian transformations and distillation of entangled gaussian states. *Phys. Rev. Lett.*, **89**(137904), 2002.

[65] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen. Universal quantum computation with continuous-variable cluster states. *Phys. Rev. Lett.*, **97**(110501), 2006.

[66] B. Groisman, S. Popescu, and A. Winter. Quantum, classical, and total amount of correlations in a quantum state. *Phys. Rev. A*, **72**(032317), 2005.

[67] W. J. Munro. Optimal states for bell-inequality violations using quadrature-phase homodyne measurements. *Phys. Rev. A*, **59**(4197), 1999.

[68] H. Nha and H. J. Carmichael. Proposed test of quantum nonlocality for continuous variables. *Phys. Rev. Lett.*, **93**(020401), 2004.

[69] R. García-Patrón, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier. Proposal for a loophole-free bell test using homodyne detection. *Phys. Rev. Lett.*, **93**(130409), 2004.

[70] R. García-Patrón, J. Fiurášek, and N. J. Cerf. Loophole-free test of quantum nonlocality using high-efficiency homodyne detectors. *Phys. Rev. A*, **71**(022105), 2005.

[71] E. Shchukin and W. Vogel. Inseparability criteria for continuous bipartite quantum states. *Phys. Rev. Lett.*, **95**(230502), 2005.

[72] A. Ourjoumtsev, A. Danatan, R. Tualle-Brouri, and P. Grangier. Increasing entanglement between gaussian states by coherent photon subtraction. *Phys. Rev. Lett.*, **98**(030502), 2007.

[73] J. S. Neergaard-Nielsen, B. M. Nielsen, C. Hettich, K. Mølmer, and E. S. Polzik. Generation of a superposition of odd photon number states for quantum information networks. *Phys. Rev. Lett.*, **97**(083604), 2006.

[74] K. Wakui, H. Takahashi, A. Furusawa, and M. Sasaki. Photon substracted squeezed states generated with periodically poled ktiopo4. *Opt. Express*, **15**(3568), 2007.

[75] A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles. Entanglement evaluation of non-gaussian states generated by photon subtraction from squeezed states. *Phys. Rev. A*, **73**(042310), 2006.

[76] F. Dell'Anno, S. De Siena, L. Albano, and F. Illuminati. Continuous-variable quantum teleportation with non-gaussian resources. *Phys. Rev. A*, **76**(022301), 2007.

[77] A. P. Lund, T. C. Ralph, and P. van Loock. Non-gaussian, mixed continuous-variable entangled states. *ArXiv:quant-ph*, **0605.247**, 2006.

[78] L. Mišta, R. Filip, and J. Fiurášek. Continuous-variable werner state: Separability, nonlocality, squeezing, and teleportation. *Phys. Rev. A*, **65**(062315), 2002.

[79] B. Julsgaard, A. Kozhekin, and E. S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, **413**(400), 2001.

[80] J. F. Sherson, B. Julsgaard, and E. S. Polzik. Deterministic atom-light quantum interface. *Adv. Atom. Mol. Opt. Phy.*, **54**(81), 2006.

[81] S. Haroche and J.-M. Raimond. Exploring the quantum atoms, cavities, and photons. *Oxford University Press, Oxford*, 2006.

[82] A. Kuzmich, K. Mølmer, and E. S. Polzik. Spin squeezing in an ensemble of atoms illuminated with squeezed light. *Phys. Rev. Lett.*, **79**(4782), 1997.

[83] A. Kuzmich, L. Mandel, and N.P. Bigelow. Generation of spin squeezing via continuous quantum nondemolition measurement. *Phys. Rev. Lett.*, **85**(1594), 2000.

[84] L.-M. Duan, J. I. Cirac, P. Zoller, and E. S. Polzik. Quantum communication between atomic ensembles using coherent light. *Phys. Rev. Lett.*, **85**(5643), 2000.

[85] A. Di Lisi, S. De Siena, and F. Illuminati. Dynamics of entanglement between two atomic samples with spontaneous scattering. *Phys. Rev. A*, **70**(12301), 2004.

[86] A. Di Lisi and K. Mølmer. Entanglement of two atomic samples by quantum-nondemolition measurements. *Phys. Rev. A*, **66**(052303), 2002.

[87] J. L. Sørensen, J. Hald, and E. S. Polzik. Quantum noise of an atomic spin polarization measurement. *Phys. Rev. Lett.*, **80**(3487), 1998.

[88] G. M. Bruun, B. M. Andersen, E. Demler, and A. S. Sørensen. Probing spatial spin correlations of ultracold gases by quantum noise spectroscopy. *Phys. Rev. Lett.*, **102**(030401), 2009.

[89] K. Eckert, O. Romero-Isart, M. Rodríguez, M. Lewenstein, E. S. Polzik, and A. Sanpera. Quantum non-demolition detection of strongly correlated systems. *Nature Physics*, **4**(50), 2008.

[90] T. Roscilde, M. Rodríguez, K. Eckert, O. Romero-Isart, M. Lewenstein, E. S. Polzik, and A. Sanpera. Quantum polarization spectroscopy of correlations in attractive fermionic gases. *New. J. Phys.*, **11**(055041), 2009.

[91] W. Dür, J. I. Cirac, and R. Tarrach. Separability and distillability of multiparticle quantum systems. *Phys. Rev. Lett.*, **83**(3562), 1999.

[92] P. van Loock and A. Furusawa. Detecting genuine multipartite continuous-variable entanglement. *Phys. Rev. A*, **67**(052315), 2003.

[93] B. Julsgaard, J. F. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik. Experimental demonstration of quantum memory for light. *Nature*, **432**(482), 2004.

[94] C. A. Muschik, K. Hammerer, E. S. Polzik, and J. I. Cirac. Efficient quantum memory and entanglement between light and an atomic ensemble using magnetic fields. *Phys. Rev. A*, **73**(062329), 2006.

[95] A. Lengwenus, J. Kruse, M. Volk, W. Ertmer, and G. Birkl. Coherent manipulation of atomic qubits in optical micropotentials. *Appl. Phys. B*, **86**(377), 2007.

[96] R. Dumke, T. Müther, M. Volk, W. Ertmer, and G. Birkl. Interferometer-type structures for guided atoms. *Phys. Rev. Lett.*, **89**(220402), 2002.

[97] B. Julsgaard. Entanglement and quantum interactions with macroscopic gas samples. *PhD*, 2003.

[98] J. F. Sherson, B. Julsgaard, and E. S. Polzik. Distant entanglement of macroscopic gas samples. *NATO Science Series II: Mathematics, Physics and Chemistry*, **189** in Decoherence, entanglement and information protection in complex quantum systems(353), 2005.

[99] R. Filip. Complementarity, entanglement and quantum erasing in continuous-variable quantum nondemolition experiments. *J. Opt. B: Quantum Semiclass. Opt.*, **4**(202), 2002.

[100] R. Filip. Continuous-variable quantum erasing. *Phys. Rev. A*, **67**(042111), 2003.

[101] R. Namiki, T. Takano, S.-I.-R. Tanaka, and Y. Takahashi. Measurement schemes for the spin quadratures on an ensemble of atoms. *ArXiv:quant-ph*, **0905.1197**, 2009.

[102] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, **86**(910), 2001.

[103] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, **86**(5188), 2001.

[104] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, **68**(022312), 2003.

[105] P. van Loock, C. Weedbrook, and M. Gu. Building gaussian cluster states by linear optics. *Phys. Rev. A*, **76**(032321), 2007.

[106] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa. Experimental generation of four-mode continuous-variable cluster states. *Phys. Rev. A*, **78**(012301), 2008.

[107] D. V. Kupriyanov, O. S. Mishina, I. M. Sokolov, B. Julsgaard, and E. S. Polzik. Multimode entanglement of light and atomic ensembles via off-resonant coherent forward scattering. *Phys. Rev. A*, **71**(032348), 2005.