QUANTUM INFORMATION WITH OPTICAL CONTINUOUS VARIABLES:

Nonlocality, Entanglement, and Error Correction

Julien Niset

Thèse présentée en vue de l'obtention du
grade de Docteur en Sciences Appliquées

Année Académique 2007-2008

Promoteur: Nicolas Cerf
Centre for Quantum Information and Communication

Université Libre de Bruxelles

Faculté des Sciences Appliquées

Acknowledgments

My gratitude goes to Nicolas Cerf for introducing me to the fascinating field of quantum information, and for giving me the opportunity to pursue this thesis.

I would also like to thank all of my colleagues at the QuIC, in particular Loïck Magnin who read a preliminary version of this manuscript, and Louis-Philippe Lamoureux who has become a true friend.

Some of the results of this dissertation come from fruitful collaborations. I am very grateful to Antonio Acín and his group at the Institute of Photonic Sciences of Barcelona. My two visits at the ICFO provided me with both inspiration and Sun. I am also grateful to Ulrik L. Andersen of the Technical University of Denmark for his great expertise in quantum optics and outstanding experimental skills. Finally, I would like to thank Jaromir Fiurášek of the University of Palacký for always finding time to answer my questions.

To my friends, to my family, to Veronika.

Contents

List of Figures

1 Introduction

Information is (Quantum) Physical

The 20th century will be remembered, without a doubt, as a century of great technological discoveries. Remarkably, many of these new technologies find their roots in two mathematical theories which completely revolutionized our perception of the world we live in. In 1901, in an attempt to explain the black-body radiation, Max Planck suggested that the energy of the emitted radiation could be described as consisting of discrete packets or *quantas* [87]. His remarkable intuition was soon embraced by Albert Einstein who used this idea of quantization to explain the photoelectric effect [32], and the specific heat of solids at very low temperature [33]. The quantum revolution was on its way. Since its introduction, this theory of the infinitely small has found applications ranging from the invention of the laser to the discovery of superconductivity. Forty-seven years and two world wars later, the need for efficient communication protocols led Claude Shannon to publish an article entitled *"A Mathematical Theory of Communication"* [92]. In this seminal paper, a collection of unpublished results gathered during the war, he addressed the problem of the transmission of information over noisy channels by introducing new mathematical objects such as the entropy of a probability distribution or the capacity of a communication channel. The resulting theory, known as Information theory, radically changed our modern society by providing a mathematical framework for the development of information oriented applications such as the computer, the compact-disk, the internet, i.e. all applications we now label as information technologies (IT).

Interestingly, these two theories, which emerged in different contexts and address different issues, are not as far apart as they seem. On the one hand, information needs a physical support to be transmitted. When we speak, the surrounding molecules of air vibrate according to the sounds we make. The words I am typing now are stored in the hard drive of my computer, and will later be printed on a piece of paper. To quote Rolf Landauer, "Information is physical" [70]. On the other hand, physical objects are, ultimately, made of microscopic particles described by the laws of quantum theory. A bit of information stored on my computer is nothing but a collection of millions of electrons, where each and everyone obey the laws of quantum mechanics. Information should not only be physical then, but quantum physical! Just as classical mechanics is an approximation of quantum mechanics valid for macroscopic objects, the information theory developed by Shannon should be the classical approximation of a quantum information theory which applies when information is stored and manipulated on quantum mechanical systems. At the dawn of the 70's, exploring the possibilities and implications of this quantum version of information theory rapidly gained interest among a small group of pioneer physicists such as Richard Feynman, Charles Bennett, Paul Benioff, and David Deutsch. A new revolution was about to begin.

But let us not go too fast. In parallel of these intellectual considerations, the 60's also witnessed the rise of the computer era. Since the first integration of a transistor in an electronic circuit in 1958, the performances of computing machines had been improving at an amazing pace. This led Gordon Moore, a co-founder of Intel, to conjecture in 1965 that the number of transistors one can place on an integrated circuit was to increase exponentially, approximately doubling every two years [75]. Amazingly enough, his predictions have held true for more than 40 years! However, people soon realized that such a trend could not continue for ever as the size of transistors would ultimately have to reach the size of atoms and enter the quantum regime. As noted by Moore himself in 2005, "It can't continue forever. The nature of exponentials is that you push them out and eventually disaster happens". But is a disaster due to the extreme miniaturization of transistors inevitable? Probably not if one is willing to seriously investigate the capabilities of this extreme quantum regime of computation.

At the beginning of the 80's, both intellectual and economical motivations were present for the rapid development of a new fascinating field of research; Quantum Information Science (QIS) was born.

The promises of Quantum Information

How can one benefit from the association of quantum mechanics with Shannon's theory of information? At first sight, the use of microscopic objects to support information seems to be the source of more problems than solutions.

For example, Heisenberg's uncertainty principle predicts the impossibility to obtain all the information about the spin of a single particle. How can two parties, say Alice and Bob, exchange information if they are unable to read the messages they receive? Interestingly, it is precisely this impossibility to read unknown quantum information which led Stephen Wiesner, then a graduate student at Columbia, to what is considered as the first application of quantum information theory; namely quantum money [105] (ironically, Wiesner proposed this idea in 1970, but had to wait until 1983 to publish it). By integrating a series of two-level quantum systems on a bank note, Wiesner argued that it is possible to create an unforgeable note whose security is guaranteed by the laws of quantum mechanics. Indeed, preparing these systems in well defined non-orthogonal quantum states would force a counterfeiter to measure each of them in a random basis, thereby introducing perturbations in the copies which could be easily detected by the bank. This unpractical but brilliant idea led, a few years later, to the discovery of quantum key distribution [8] and is at the origin of an entire branch of QIS devoted to cryptographic applications and communications.

Asides from the uncertainty principle, quantum mechanics has some other interesting fundamental features with no classical counterparts. Can they be exploited cleverly in order to solve, say, computational problems efficiently? This question was first addressed by David Deutsch, who suggested that, indeed, such quantum computers might have a computational power exceeding that of classical ones [28]. Consider for example a bit, the basic unit of classical information, which has only two possible values "0" or "1". Either a million electrons are stored in a given memory cell of my computer and the bit is interpreted as "one", or they are not and the bit is interpreted as "zero". Now suppose that this memory cell is a two-level quantum system such as the spin of a single electron. The *superposition* principle of quantum mechanics predicts that this quantum bit, or *qubit*, can not only be $|0\rangle$ or $|1\rangle$, but can also be $|0\rangle$ *and* $|1\rangle$ at the same time, i.e. quantum mechanics enables linear superpositions of the form $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. By processing this qubit, one will therefore process "zero" and "one" simultaneously, a feature of quantum computation known as *parallelism*. In 1994, these considerations led Peter Shor to design an efficient algorithm, the so-called Shor algorithm, proving the superiority of quantum over classical computers for the factorization of large numbers [93]. Interestingly, while the uncertainty principle guarantees the security of specific cryptographic tasks, the superposition principle enables parallel quantum computation and is at the origin of the computation and algorithmic branch of QIS.

The power of quantum information lies in its ability to exploit the many possibilities offered by the quantum world. Its development is therefore strongly correlated to our knowledge and understanding of quantum mechanics. Remarkably, the rise of quantum information caused a renewed interest in the foundations of this well established theory. Questions which were left unanswered or considered uninteresting for nearly a century soon became the focus of intensive research. The most striking example of this renewal is a property of quantum mechanics known as *entanglement*. The term entanglement was first coined by Erwin Schrödinger as “the characteristic trait of quantum mechanics” [91]. It was also called “spooky action at the distance” by Albert Einstein, and its implications caused Einstein to dislike the theory he had helped create. He was not the only one puzzled by such a counterintuitive aspect of quantum theory, although for many years questions related to entanglement were mostly considered of philosophical and metaphysical nature. Following the work of John Bell [7], the recent renewal of quantum mechanics has seen our understanding of entanglement change from a controversial property of microscopic entities to a key ressource of quantum information. Entanglement is now used to achieve many tasks such as quantum teleportation [9] or quantum dense coding [10]. An entire branch of QIS, sometimes known as entanglement theory, is now devoted to the study of this fascinating ressource, ranging from its characterization to the exploration of its possible uses.

Continuous Variables

The early investigations of quantum information mostly focused on qubits, i.e. two-level quantum systems such as the spin of an electron or the polarization of a photon, since they are the natural quantum analog of the classical bit. From a theorist’s perspective, these systems are the simplest to manipulate. They also exhibit all the quantum features interesting for quantum information applications. Using qubits, quantum states can be teleported, secret keys can be established, numbers can be factorized, entanglement can be produced, distributed and distilled. Unfortunately, manipulating a single photon (or a single electron) is a difficult experimental task. Single photons are hard to produce *on demand*, and hard to detect efficiently. The same applies to the production and detection of entanglement. These experimental limitations make the implementation of quantum information based on discrete variables both difficult and expensive.

Since 1998, the year of the first experimental demonstration of unconditional quantum teleportation by Furusawa and collaborators [43], a novel approach developed, which relies on canonical observables with continuous spectra. This quantum information with continuous variables (CV) rapidly gained attention as it offers many practical advantages over its discrete variable counterpart. On the one hand, when the quadratures of the electromagnetic field are used to carry the information, many interesting protocols can be implemented by combining passive and active linear optical components (beam splitters, phase shifters and squeezers), supplemented with an efficient detection scheme known as homodyne detection. All these elements are, up to some degree of accuracy, readily accessible in today’s optical labs.

Furthermore, continuous variable entangled states of light can be relatively easily generated in a deterministic way with optical parametric amplifiers [20], while their continuous quantum information is made accessible by the fast and efficient homodyne detection technique. On the other hand, although CV states lie in an infinite dimensional Hilbert space, many of them can be handled by mathematical techniques from finite-dimensional algebra. In particular, operations on the density matrix of the so-called Gaussian states can be achieved by manipulating the finite-dimensional covariance matrix. All these features make the optical continuous variable approach a very promising candidate for quantum information and quantum communications in particular.

Outline of the Thesis

The objective of the present dissertation is to investigate some of the possibilities offered by the continuous variable approach of quantum information, with a focus on optical continuous variables in particular. As often in science, practical applications emerge from purely theoretical considerations. Quantum information is no exception, and many of its remarkable accomplishments are the results of an improved understanding of quantum mechanics and its many mysteries. The first part of this dissertation will therefore be oriented towards fundamental issues. More precisely, we will address various nonlocal aspects of quantum mechanics in the continuous variable regime, and try to gain some insight into the peculiar relation between the two essential ressources of QIS, namely nonlocality and entanglement. The second part of the dissertation will be oriented towards practical applications. In particular, we will focus on an important primitive of quantum information called error correction, and exploit optical continuous variables advantageously in order to design experimentally feasible error-correcting codes.

Quantum information is an interdisciplinary field. In **Chapter 2**, we will introduce some basic concepts and mathematical tools central to quantum mechanics, quantum optics, and information theory. Readers familiar with CV quantum information are free to skip this preliminary chapter.

The next three chapters aim to improve our understanding of quantum nonlocality in the continuous variable regime. In **Chapter 3**, we focus on the standard nonlocality of quantum mechanics, and address the problem of loophole-free Bell inequalities. We will show that Bell tests based on optical continuous variables combined with homodyne detection can benefit from an increased number of parties involved in the experiment. In particular, we will prove that it is always possible to maximally violate the m-partite Mermin-Klyshko inequality based on such quadrature measurements. In **Chapter 4**, we will generalize a bizarre property of quantum mechanics known as Nonlocality Without Entanglement (NWE). This peculiar effect, first identified in 1998 for three-level quantum systems, describes systems that behave in a truly nonlocal manner without being entangled. By introducing a simple quantum circuit, we will generalize the phenomena to arbitrary dimension, and investigate the possibility to witness this effect with CV states. Finally, the first part of this dissertation will be concluded by introducing in **Chapter 5** a third form of nonlocality arising when certain non-entangled states are detected with an entangled measurement. We will name this property Nonlocality Without Squeezing, and experimentally demonstrate its existence based on phase conjugated coherent states.

The second part of the thesis will be devoted to quantum error correction with continuous variables. In **Chapter 6**, we will exploit a known connection between error correction and entanglement distillation to prove that a large class of CV errors, called Gaussian errors, cannot be corrected using the available Gaussian operations (linear optical elements plus homodyne detection). We will nevertheless show in **Chapter 7** that non-Gaussian error patterns can be corrected using Gaussian operations only, and we will present the first continuous-variable quantum erasure-correcting code. The key feature of our code is a nonlocal transmission of information that is made possible by the use of CV entangled states.

In **Chapter 8**, we will summarize our results and look upon future perspectives.

Publications

This dissertation is based on the following publications:

- J. Niset and N. J. Cerf, *Multipartite Nonlocality Without Entanglement in Many Dimensions*, Phys. Rev. A **74**, 052103 (2006).

- J. Niset, A. Acín, U. L. Andersen, N. J. Cerf, R. García-Patrón, M. Navascués, and M. Sabuncu, *Superiority of Entangled Measurements over All Local Strategies for the Estimation of Product Coherent States*, Phys. Rev. Lett. **98**, 260404 (2007).

- J. Niset and N. J. Cerf, *Tight Bounds on the Concurrence of Quantum Superpositions*, Phys. Rev. A **76**, 042328 (2007).

- J. Niset, U.L. Andersen, N.J. Cerf, *Experimentally Feasible Quantum Erasure-Correcting Code for Continuous Variables*, Phys. Rev. Lett. **101**, 130503 (2008).

- A. Acin, N.J. Cerf, A. Ferraro, and J. Niset, *Multimode Quantum Non-Locality Using Homodyne Measurements*, arXiv:0808.2373 (submitted to Phys. Rev. A).

- J. Niset, and N.J. Cerf, *A No-Go Theorem for Gaussian Error Correction*, in preparation.

2 All you Need to Know About...

This chapter

Quantum information is an interdisciplinary field. Fundamentally, it combines aspects of quantum mechanics, information and computation theory. However, going from theory to experiment also requires knowledges of quantum optics, atomic physics, or solid state physics depending on the physical system used to support the information. Good quantum information theorists must therefore combine expertise of some, if not all, of these different fields. The present dissertation being concerned with quantum information based on *optical* continuous variables, we will restrict our attention to quantum mechanics, quantum optics, and information theory. Each of these topics is a field on its own; presenting them in a single chapter is therefore a difficult, if not impossible, task. Nevertheless, the following sections are an attempt to introduce the basic concepts and features of these three theories, together with the associated mathematical formalism. Our goal is to provide an unfamiliar reader with the necessary tools to tackle the problems addressed in this thesis. However, a brief introduction can never replace a good book, and we note that this chapter is mainly a compilation of results found in [78, 101, 20, 26]. Interested readers are strongly encouraged to consult these very instructive references for more details and (probably) better explanations.

2.1 Quantum Mechanics

2.1.1 The postulates of Quantum Mechanics

The aim of quantum information theory is to use microscopic physical systems to store and manipulate information. These systems can be quite different in nature, but irrespective of their differences they can all be described within a common mathematical framework called *quantum mechanics*. This is what makes quantum mechanics both beautiful and powerful. Whether we consider the spin of an electron, the polarization of a photon, or the atomic levels of an atom, the mathematical objects we manipulate are the same. In itself, quantum mechanics is not a theory about which laws a particular physical system must obey, but it provides some general principles from which a mathematical description of these laws can be developed. These general principles can be formulated as a set of basic postulates, which we present here in a form that is particularly suitable for quantum information.

The first postulate of quantum mechanics defines the mathematical entity representing a particular state of a physical system.

Postulate 1 *To any isolated physical system S is associated a Hilbert space (a complex vector space with inner product) $\mathcal{H}_S$. The system state is completely determined by a unit vector $|\psi\rangle$ of that Hilbert space.*

Remarkably, this postulate does not specify what Hilbert space will be associated to a given physical system, that is, it does not give the basis states or even the dimension of the space $\mathcal{H}_S$. In general, this dimension should be adequately chosen to be able to reproduce the physical properties of the system. As we will see, this dimension can be finite or infinite. An important consequence of Postulate 1 is that vectors in a Hilbert space, and therefore quantum states, have the interesting property that if $|\psi_1\rangle$ and $|\psi_2\rangle$ are two states in $\mathcal{H}_S$, so will be any linear combination $|\psi_3\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle$ where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. This property, known as the *superposition principle* of quantum mechanics, is at the origin of the power of quantum information. Finally, the inner product of two states $|\psi_1\rangle$ and $|\psi_2\rangle$ of $\mathcal{H}_S$ is denoted by the *bracket* notation $\langle\psi_1|\psi_2\rangle$.

While the first postulate deals with states at a fixed time, the second postulate tells us how these states evolve in time.

Postulate 2 *The evolution of an isolated quantum system is described by a unitary transformation. That is, the state $|\psi'\rangle$ of the system at time t' is* *related to the state $|\psi\rangle$ of the system at time t by*

$$\left|\psi'\right\rangle = U\left|\psi\right\rangle, \tag{2.1}$$

where U is a unitary operator which depends on the times t and t'.

Just as quantum mechanics does not tell us the state space or quantum state of a particular physical system, it does not tell us which unitary operator describes its evolution. However, it assures us that this evolution may be described in such a way. From the unitarity of the evolution follows the interesting property that quantum processes are always reversible. In practice, systems are never perfectly isolated as required by this second postulate. Nevertheless, there are interesting systems which can be described to a good approximation as being closed, and whose evolution is approximately unitary. In any case, we note that, at least in principle, every open system can be described as part of a larger closed system, the Universe, which is undergoing a unitary evolution.

So far, the postulates have only considered isolated systems. It is however clear that it is necessary to interact with a system at some point if we want to extract some information from it. The process of interacting with a system to extract information is called a measurement, and is the purpose of the following postulate.

Postulate 3 *A quantum measurement on a system S is described by a collection $\{M_m\}$ of measurement operators, defined as operators acting in the Hilbert space $\mathcal{H}_S$ associated with S and satisfying the completeness relation*

$$\sum_m M_m^\dagger M_m = I_S \tag{2.2}$$

where I_S is the identity operator on $\mathcal{H}_S$. The index m refers to the measurement outcomes that may occur in an experiment. The probability $p(m)$ to obtain the outcome m if the system was in the state $|\psi\rangle$ immediately before the measurement is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{2.3}$$

and the state after the measurement becomes

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{p(m)}}. \tag{2.4}$$

Measurements will play an important role in the following chapters, and are central to quantum information. As we will see, they are often the last step of an experiment where one is only interested in the probabilities of getting the different outcomes. In this case, postulate 3 shows that the only relevant mathematical entities are the positive operators $E_m = M_m^\dagger M_m$. The set of operators $\{E_m\}$ is called a *Positive Operator-Valued Measure*, or POVM in short, and the POVM elements E_m satisfy the completeness relation

$$\sum_m E_m = I_S. \tag{2.5}$$

Physicists may not be familiar with this formulation of the measurement postulate. In traditional quantum physics, each physical property that can be measured corresponds to a hermitian operator M, called an *observable*, that has a spectral decomposition $M = \sum_m mP_m$, where the m's are the eigenvalues of M and P_m is the projector to the corresponding eigenspace. These projectors P_m, with $P_m P_{m'} = \delta_{mm'} P_m$, define a particular type of measurement called *projective* or *von Neumann* measurement, and correspond to the special case where the measurement operators E_m are orthogonal projectors. Within this notation, we do recover the measurement postulate as stated in most books on quantum mechanics, i.e. the possible outcomes of a measurement are the eigenvalues m of the corresponding observable M, and the state after the measurement lies within the eigenspace of M associated with the observed outcome m. Let us also mention that we will sometimes refer to "measuring in a basis $|m\rangle$", where $|m\rangle$ forms an orthogonal basis. This simply means that we perform a projective measurement with projectors $P_m = |m\rangle\langle m|$.

Our generalized formulation of the measurement postulate naturally raises two questions. First, one may wonder why we state the postulate in this form. The answer can be found in the development of quantum information theory, which has showed that it is often possible to extract more information from a system by going beyond projective measurements (see for example Chapter 4). Second, one may question the validity of the measurement postulate in this form. As we now see, this formulation is strictly equivalent to the traditional one provided that we add this last postulate

Postulate 4 *The Hilbert space associated with a composite physical system AB, made of two subsystems A and B, is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ associated with A and B. Furthermore, if A is prepared in the state $|\psi_A\rangle$ and B is prepared in the state $|\psi_B\rangle$, the joint state of the composite system AB will be the tensor product state $|\psi_A\rangle \otimes |\psi_B\rangle$, sometimes noted as $|\psi_A\rangle\,|\psi_B\rangle$ for simplicity.*

Suppose for example that we want to realize the generalized measurement $\{M_m\}$ on a system S. We can always extend S by adding an additional system A prepared in a known state, and such that the dimension of $\mathcal{H}_A$ coincides with the number of measurement operators M_m. Associating each M_m with a basis state $|m\rangle$ of A, it is always possible to define a unitary operator U such that $U\left|\psi\right\rangle\left|0\right\rangle = \sum_m M_m \left|\psi\right\rangle\left|m\right\rangle$, where $\left|\psi\right\rangle$ is the unknown state of S and $\left|0\right\rangle$ is some arbitrary fixed state of A known as an *ancilla*. It is now straightforward to check that the generalized measurement $\{M_m\}$ on S can be realized by a projective measurement on SA with projectors $P_m = U^\dagger(I_S \otimes |m\rangle\langle m|)U$, where I_S is the identity on $\mathcal{H}_S$ and $|m\rangle\langle m|$ is the projector on the state $\left|m\right\rangle$ of $\mathcal{H}_A$. This useful correspondence between POVMs and projective measurements in a larger system is known in quantum information as Neumark's theorem [86].

So far, we have formulated quantum mechanics using the language of state vectors. However, it is important to note that there exists an alternate formulation using a tool known as the density operator. This formulation is mathematically equivalent, but much more practical in some commonly encountered scenarios in quantum mechanics. In particular, the density operator provides a convenient means for describing quantum systems whose state is not completely known. For example, if a quantum system can be in one of the states $\{\left|\psi_i\right\rangle\}$ with respectives probabilities p_i, the state of the system is fully characterized by the density operator

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.6}$$

A quantum system whose state $\left|\psi\right\rangle$ is known exactly is said to be *pure*, and its density operator is simply $\rho = |\psi\rangle\langle\psi|$. Otherwise, the state is said to be *mixed* and the density operator has the form of Eq. (2.6). Both formulations will be used interchangeably in the following chapters, and we refer the reader to e.g. [78] for some important properties of the density operator.

2.1.2 Quantum Mechanics and Impossibilities

Remarkably, the simple formalism introduced by these four postulates is sufficient to derive some interesting properties of the quantum theory. For example, it can tell us what is possible and impossible within the framework of quantum mechanics. Interestingly, this is exactly the goal of quantum information; to test the possibilities offered by quantum mechanical systems and see what it implies for the treatment of information. In the following section, we thus present three limitations imposed by quantum mechanics that have been of fundamental importance in the development of QIS. These impossibilities will help us grasp the flavor of the revolutionary concepts introduced by quantum mechanics. They will also introduce the principles which triggered most of the questions addressed in this dissertation.

Distinguishing Quantum States

An important question in quantum information is the problem of distinguishing quantum states. In the classical world, distinct states of an object are usually distinguishable. One can always tell if the result of a coin toss is head or tail for example. In the quantum world however, the situation is more complicated. As we will see in Chapter 4 and 5, it also leads to some very counterintuitive results.

The question of the distinguishability of quantum states is best understood by considering the following simple game between two parties usually called Alice and Bob. Suppose that Alice chooses a state $|\psi_i\rangle$ $(1 \leq i \leq n)$ from a given set known to her and Bob, and sends the state to Bob. Bob's task is to identify the value of the label i.

Let us assume first that the states of the set are orthogonal. Bob can define the n measurement operators $M_i = |\psi_i\rangle\langle\psi_i|$, and an additional measurement operator $M_0 = I - \sum_i M_i$. These operators satisfy the completeness relation, and if the state $|\psi_i\rangle$ is prepared by Alice then $p(i) = \langle\psi_i| M_i |\psi_i\rangle = 1$ so Bob will identify the index i with certainty. It is thus possible to reliably distinguish orthogonal quantum states.

Suppose now that the states of the set are not orthogonal, and let us imagine that there exists a measurement which can distinguish perfectly between the non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$. Bob will apply his measurement described by the measurement operators M_j, and if the outcome j is observed, he guesses that the index is i using some rule $f(j) = i$. If the state $|\psi_1\rangle$ $(|\psi_2\rangle)$ is prepared then the probability of measuring j such that $f(j) = 1$ $(f(j) = 2)$ must be one. Introducing $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$, this translates to

$$\begin{aligned} \langle\psi_1| E_1 |\psi_1\rangle &= 1 \\ \langle\psi_2| E_2 |\psi_2\rangle &= 1. \end{aligned} \tag{2.7}$$

Since $\sum_i E_i = I$, it follows that $\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$, and (2.7) implies $\langle\psi_1| E_2 |\psi_1\rangle = 0$, or equivalently $\sqrt{E_2}\,|\psi_1\rangle = 0$. Now, because the two states are not orthogonal, we can write

$$|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\varphi\rangle\,, \tag{2.8}$$

where $|\varphi\rangle$ is orthogonal to $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$ and $|\beta| < 1$. Then $\sqrt{E_2}\,|\psi_2\rangle = \beta\sqrt{E_2}\,|\varphi\rangle$ which implies

$$\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\varphi| E_2 |\varphi\rangle \leq |\beta|^2 < 1. \tag{2.9}$$

This is in clear contradiction with (2.7), from which we can deduce that there is no quantum measurement capable of distinguishing reliably between non-orthogonal states.

Measuring Non-Commuting Observables

In quantum mechanics, a physical property that can be measured, or observed, is associated with an hermitian operator called an *observable*. Sometimes, these observables correspond to physical properties that are *complementary*, and the order in which these observables are applied to a state matters. If A and B are two such *non-commuting* observables, this property is expressed as

$$[A, B] = AB - BA \neq 0, \tag{2.10}$$

where $[A, B]$ is called the commutator of A and B (we can also define their anti-commutator $\{A, B\} = AB + BA$). In 1926, Werner Heisenberg arrived at the astonishing conclusion that quantum mechanics precludes the perfect knowledge of such non-commuting observables simultaneously. This famous result is known as Heisenberg's uncertainty principle.

Let us consider two non-commuting observables A and B, a quantum state $|\psi\rangle$, and suppose that $\langle\psi| AB |\psi\rangle = x + iy$, where x and y are real. Note that $\langle\psi| AB |\psi\rangle$ is called the average value of AB for the state $|\psi\rangle$, and is sometimes denoted as $\langle AB\rangle$ when it is clear that we refer to the state $|\psi\rangle$. We can calculate the average value of the commutator and anti-commutator of AB,

$$\begin{aligned} \langle\psi| [A, B] |\psi\rangle &= 2iy \\ \langle\psi| \{A, B\} |\psi\rangle &= 2x, \end{aligned} \tag{2.11}$$

which implies

$$| \langle\psi| [A, B] |\psi\rangle |^2 + | \langle\psi| \{A, B\} |\psi\rangle |^2 = 4| \langle\psi| AB |\psi\rangle |^2. \tag{2.12}$$

By the Cauchy-Schwartz inequality, we also know that

$$| \langle\psi| AB |\psi\rangle |^2 \leq \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle , \tag{2.13}$$

from which we deduce

$$| \langle\psi| [A, B] |\psi\rangle |^2 \leq 4| \langle\psi| AB |\psi\rangle |^2 \leq 4 \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle . \tag{2.14}$$

If we now define two new observables C and D such that $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$, we obtain Heisenberg uncertainty principle

$$\Delta C\, \Delta D \geq \frac{|\langle[C, D]\rangle|}{2}, \tag{2.15}$$

where we have introduced the *standard deviation* ΔM of an observable M with

$$\Delta^2 M = \langle(M - \langle M\rangle)^2\rangle \tag{2.16}$$

$$= \langle M^2\rangle - \langle M\rangle^2. \tag{2.17}$$

The conceptual implications of this uncertainty principle are at the origin of the discussion of the standard nonlocality of quantum mechanics addressed in Chapter 3.

Copying Quantum States

Quantum information is carried by quantum states. Unlike classical information, quantum information is not easy to manipulate as it requires the manipulation of quantum objects. For example, a simple task such as perfectly copying an unknown quantum state is precluded by the laws of quantum mechanics. This principle, known as the *no-cloning* theorem, is at the origin of the most advanced application of quantum information called Quantum Key Distribution.

Suppose that we have at hand a device which can copy an arbitrary quantum state. In particular, it can copy the two orthogonal states $|\psi\rangle$ and $|\psi_\perp\rangle$. Without loss of generality, we can associate to our device a unitary operator U acting on the state we want to copy and the "blank" ancilla to which we want the copied state, i.e.

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \tag{2.18}$$

$$U|\psi_\perp\rangle|0\rangle = |\psi_\perp\rangle|\psi_\perp\rangle \tag{2.19}$$

Applying our device to the superposition state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\psi_\perp\rangle)$$

we obtain

$$U|\Psi\rangle|0\rangle = U\frac{1}{\sqrt{2}}(|\psi\rangle + |\psi_\perp\rangle)|0\rangle \tag{2.20}$$

$$= \frac{1}{\sqrt{2}}(|\psi\rangle|\psi\rangle + |\psi_\perp\rangle|\psi_\perp\rangle) \tag{2.21}$$

One can easily check that this state does not correspond to the two copies of $|\Psi\rangle$ that we wished, namely

$$|\Psi\rangle|\Psi\rangle = \frac{1}{2}(|\psi\rangle + |\psi_\perp\rangle)(|\psi\rangle + |\psi_\perp\rangle), \tag{2.22}$$

from which we conclude that there is no universal quantum device that can perfectly copy $|\psi\rangle$, $|\psi_\perp\rangle$ and $|\Psi\rangle$ at the same time.

The impossibility to copy quantum states, and therefore quantum information, is at the origin for the need of cleverly designed quantum error correcting codes that go beyond classical error correcting techniques. This issue will be addressed in chapters 6 and 7.

2.1.3 Entanglement

Definition

As we have just seen, many interesting features of quantum mechanics can be derived from the basic postulates. However, one in particular deserves a special treatment due to its importance in the development of QIS. Suppose for example that we prepare two photons, A and B, with vertical polarization, and that vertical and horizontal polarizations are denoted by $|0\rangle$ and $|1\rangle$ respectively. According to postulate 4, this system is described by the tensorial product $|0\rangle_A |0\rangle_B$. On the other hand, if we choose to prepare two photons with horizontal polarization the quantum state is $|1\rangle_A |1\rangle_B$. Now, recall that quantum mechanics enables linear superpositions. In particular, it enables the superposition state

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B). \tag{2.23}$$

Remarkably, this state can no longer be written as the tensor product of two quantum states, that is there is no description $|a\rangle_A$ and $|b\rangle_B$ of systems A and B such that $|\phi^+\rangle_{AB} = |a\rangle_A |b\rangle_B$ (such a quantum state is called a product state). Even if the system under consideration is still made of two photons, these photons cannot be considered separately as they form one joint entity, i.e., they are *entangled*.

The importance of entanglement in quantum mechanics was first stated by Erwin Schrödinger in 1935, as part of a discussion on Einstein's critique of the quantum theory (see Chapter 3). To quote his own words [91]:

> *When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives [the quantum states] have become entangled. [...] Another way of expressing the peculiar situation is: the best possible knowledge of a whole does not necessarily include the best possible knowledge of all its parts, even though they may be entirely separate and therefore virtually capable of being best possibly known, i.e., of possessing, each of them, a representative of its own. The lack of knowledge is by no means due to the interaction being insufficiently known, at least not in the way that it could possibly be known more completely, it is due to the interaction itself.*

As noted by Schrödinger himself, entanglement is the characteristic feature of quantum mechanics. It has now also become the key ressource of quantum information science. Like every ressource, it can be manipulated and quantified. For example, one can prove that the state (2.23) is not only entangled, but has the maximum entanglement achievable for bipartite two-level systems, i.e., it is *maximally entangled*. However, a complete picture of entanglement is still missing, and, depending of the context, different measures of entanglement have been introduced. Amongst all these measures, the most important one is the von Neumann entropy of the reduced state

$$E[\rho_{AB}] = S(\rho_A) = S(\rho_B), \tag{2.24}$$

(see Sec. 2.3.2 for the definition of the von Neumann entropy S) which completely characterizes the entanglement of bipartite pure states ρ_{AB}. Another important measure that will be used in this thesis is the logarithmic negativity [98]

$$E_N[\rho_{AB}] = \log \|\tilde{\rho}_{AB}\|_1, \tag{2.25}$$

where $\|A\|_1 = \mathrm{Tr}\,|A| = \mathrm{Tr}\,\sqrt{A^\dagger A}$ is the trace norm of an operator A, and the logarithm is in base 2. The logarithmic negativity quantifies by how much the partial transposed $\tilde{\rho}_{AB}$ of a bipartite mixed state ρ_{AB} fails to be positive (fails to be a valid quantum state). Note that partial transposition, i.e., transposing one out of two subsystems, has been proven one of the most useful tool in the study of entanglement as one can show that every separable state must have a positive partial transpose [85]. This result is famously known as the PPT criterion.

Entanglement has many interesting properties. For example, the entanglement of a single bipartite state cannot be increased (on average) by local operations. This is a consequence of the purely quantum nature of entanglement. Nevertheless, from many copies of a weakly entangled state, two collaborating parties can sometimes extract a single highly entangled state by means of local operations only. This process, known as entanglement distillation, is an essential requirement for future quantum communication networks. We will briefly investigate a possible CV distillation protocol in Appendix E.

Finally, let us mention that during these four years of research, we have investigated the connection between entanglement and the superposition principle. This resulted in a publication entitled “Tight bounds on the concurrence of quantum superpositions” [79]. However, this work focuses on discrete variables only, hence it is not included in the present dissertation.

Quantum Teleportation

Let us illustrate the power of entanglement with a simple example; the well-known quantum teleportation protocol. The goal of quantum teleportation is to transmit an unknown quantum state between two distant locations, usually called Alice and Bob, using entanglement and classical communications only.

Suppose Alice and Bob share the maximally entangled state of Eq. (2.23), and Alice wants to communicate the unknown state

$$|\psi\rangle_{in} = \alpha\,|0\rangle_{in} + \beta\,|1\rangle_{in} \tag{2.26}$$

with $|\alpha|^2 + |\beta|^2 = 1$. The state they share is therefore

$$|\psi\rangle_{in}\,|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\big(\alpha\,|0\rangle_{in} + \beta\,|1\rangle_{in}\big)\big(\,|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B\,\big) \tag{2.27}$$

where the modes *in* and A are in Alice's hands, while B is hold by Bob. Grouping the shares of Alice, this input state can be written as

$$\begin{aligned}|\psi\rangle_{in}\,|\phi^+\rangle_{AB} = \frac{1}{2}\Big[\,&|\phi^+\rangle_{in,A}\,(\alpha\,|0\rangle_B + \beta\,|1\rangle_B\,) + |\psi^+\rangle_{in,A}\,(\alpha\,|1\rangle_B + \beta\,|0\rangle_B\,)\\ &+ |\phi^-\rangle_{in,A}\,(\alpha\,|0\rangle_B - \beta\,|1\rangle_B\,) + |\psi^-\rangle_{in,A}\,(\alpha\,|1\rangle_B - \beta\,|0\rangle_B\,)\Big]\end{aligned} \tag{2.28}$$

after the introduction of the four maximally entangled Bell states

$$\begin{aligned}|\phi^\pm\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle\,\big)\\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle\,\big).\end{aligned} \tag{2.29}$$

Remarkably, if Alice measures her two shares in this Bell basis and obtains the result $|\phi^+\rangle$, an operation known as a Bell measurement, she knows that Bob's share is in the state $|\psi\rangle_{in}$. If she obtains one of the other Bell states however, she can inform Bob about her result and he will recover $|\psi\rangle_{in}$ by applying the appropriate unitary transformation.

2.2 Quantum Optics

The present thesis investigates the possibilities offered by optical continuous variables. By optical, we mean that the physical systems used to support the information are quantum states of the electromagnetic field, i.e., quantum states of light. The term continuous variables, on the other hand, refers to the continuous spectra of the observables used to describe the quantum state and support the information. The application of quantum mechanics to characterize and manipulate the quantum properties of light is known as quantum optics.

2.2.1 Quantization of the Electromagnetic Field

In classical mechanics, the electromagnetic field obeys the source-free Maxwell equations

$$\nabla \times \mathbf{E} = -\mu_0 \frac{\partial \mathbf{H}}{\partial t}, \tag{2.30}$$

$$\nabla . E = 0, \tag{2.31}$$

$$\nabla \times \mathbf{H} = \epsilon_0 \frac{\partial \mathbf{E}}{\partial t}, \tag{2.32}$$

$$\nabla . \mathbf{H} = 0, \tag{2.33}$$

where ϵ_0 and μ_0 are the free space permitivity and permeability respectively. The corresponding solution of the electric field is

$$\mathbf{E}(r,t) = \sum_{\mathbf{k},\lambda} E_{\mathbf{k}} \mathbf{e}_{\mathbf{k}}^{(\lambda)} \left[\alpha_{\mathbf{k},\lambda} e^{i(\mathbf{kr}-\omega_k t)} + \alpha_{\mathbf{k},\lambda}^{*} e^{-i(\mathbf{kr}-\omega_k t)} \right] \tag{2.34}$$

where $\mathbf{k}$ is the propagation vector, $\mathbf{e}_{\mathbf{k}}^{(\lambda)}$ is the polarization vector with polarization λ, ω_k is the angular frequency of the mode $\mathbf{k}$, and

$$E_{\mathbf{k}} = \left(\frac{\hbar \omega_k}{2\epsilon_0} \right)^{1/2}. \tag{2.35}$$

The quantization of the electromagnetic field is accomplished by choosing the complex Fourier amplitudes $\alpha_{\mathbf{k},\lambda}$ and $\alpha_{\mathbf{k},\lambda}^{*}$ to be the mutually adjoint annihiliation and creation operators $\hat{a}_{\mathbf{k},\lambda}$ and $\hat{a}_{\mathbf{k},\lambda}^{\dagger}$. Since photons are bosons, they satisfy the boson commutation relations

$$\begin{aligned} [\hat{a}_{\mathbf{k},\lambda}, \hat{a}_{\mathbf{k}',\lambda'}^{\dagger}] &= \delta_{\mathbf{k}\mathbf{k}'}\delta_{\lambda\lambda'}, \\ [\hat{a}_{\mathbf{k},\lambda}, \hat{a}_{\mathbf{k}',\lambda'}] &= 0, \\ [\hat{a}_{\mathbf{k},\lambda}^{\dagger}, \hat{a}_{\mathbf{k}',\lambda'}^{\dagger}] &= 0. \end{aligned} \tag{2.36}$$

2.2.2 The Quadratures Operators

Although the electromagnetic field contains an infinite number of modes, each mode is described by an independent Hilbert space. We can thus, without loss of generality, restrict our attention to a single mode of the field. The definition of the electric field using the single-mode annihilitiation and creation operators $\hat{a}$ and $\hat{a}^{\dagger}$ may be rewritten as

$$\hat{E}(r,t) = E_0 \mathbf{e} \left[\hat{x} \cos(\mathbf{kr} - \omega t) + \hat{p} \sin(\mathbf{kr} - \omega t) \right] \tag{2.37}$$

with E_0 given by (2.35) for the considered mode, and after the introduction of the dimensionless quadrature operators

$$\hat{x} = \frac{1}{\sqrt{2}} (\hat{a} + \hat{a}^{\dagger}), \tag{2.38}$$

$$\hat{p} = \frac{1}{i\sqrt{2}} (\hat{a} - \hat{a}^{\dagger}). \tag{2.39}$$

These operators are formally equivalent to the position and momentum of an harmonic oscillator. Interestingly, unlike $\hat{a}$ and $\hat{a}^\dagger$, they are Hermitian and can therefore be measured. They obey the commutation relation

$$[\hat{x}, \hat{p}] = i\,, \tag{2.40}$$

and satisfy the Heisenberg's uncertainty relation

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{1}{2}. \tag{2.41}$$

The eigenstate of the quadrature operators,

$$\hat{x}\,|x\rangle = x\,|x\rangle \tag{2.42}$$
$$\hat{p}\,|p\rangle = p\,|p\rangle \tag{2.43}$$

form two sets of orthonormal states obeying

$$\langle x|x'\rangle = \delta(x - x') \tag{2.44}$$
$$\langle p|p'\rangle = \delta(p - p'), \tag{2.45}$$

and are related by a Fourier transform, i.e.,

$$|p\rangle = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \mathrm{d}p\, e^{ixp}\,|x\rangle \tag{2.46}$$
$$|x\rangle = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} \mathrm{d}x\, e^{-ixp}\,|p\rangle\,. \tag{2.47}$$

Both ensembles are a resolution of the identity and form complete orthogonal bases. However, their states have infinite energy and are therefore unphysical. The wave function, and its Fourier transform, of a given quantum state $|\psi\rangle$ reads

$$\begin{aligned}\psi(x) &= \langle x|\psi\rangle\\ \tilde{\psi}(p) &= \langle p|\psi\rangle.\end{aligned} \tag{2.48}$$

2.2.3 Representations of the Field

Fock States

The eigenstates of the *number* operator $\hat{n} = \hat{a}^\dagger\hat{a}$ with eigenvalue n

$$\hat{n}\,|n\rangle = n\,|n\rangle \tag{2.49}$$

are called Fock states or photon number states, and they correspond to the presence of n photons in the mode under consideration. The number operator is an Hermitian operator and can be measured. For a mode of frequency ω, the states $|n\rangle$ are also eigenvectors of the Hamiltonian

$$H|n\rangle = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})|n\rangle = E_n|n\rangle \tag{2.50}$$

with energy eigenvalue $E_n = \hbar\omega(n+\frac{1}{2})$. Since Fock states have a well defined energy, their phase is totally random. The state $|0\rangle$ containing no photon is called the vacuum, and from the action of the creation and anihiliation operators on a Fock state

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \tag{2.51}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle\,, \tag{2.52}$$

one finds

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle\,. \tag{2.53}$$

The Fock states form an orthogonal and complete basis

$$\langle n|m\rangle = \delta_{n,m}\,, \tag{2.54}$$

$$\sum_n |n\rangle\langle n| = \mathbb{1}\,, \tag{2.55}$$

hence we can write an arbitrary quantum state of the field as the superposition

$$|\psi\rangle = \sum_n c_n|n\rangle\;, \tag{2.56}$$

with c_n being complex amplitudes obeying $\sum_n |c_n|^2 = 1$.

Note that the coordinate representation of a Fock state $|n\rangle$ is given by

$$\begin{aligned}\phi_n(x) &= \langle x|n\rangle \\ &= \frac{e^{-x^2}}{\pi^{1/4}\sqrt{2^n n!}}H_n(x)\end{aligned} \tag{2.57}$$

where $H_n(x)$ is the Hermite polynomial of order n.

Coherent States

The Fock states only form a useful representation of the field for small number of photons. From a theoretical point of view, manipulating large sums can be a daunting task, while perfect number states are extremely difficult to generate experimentally for $n > 2$. A more appropriate basis for many applications is the coherent states basis, as the field generated by a highly stabilized laser operating well above threshold is a coherent state.

A coherent state $|\alpha\rangle$ is an eigenstate of the annihilation operator

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{2.58}$$

where $\alpha = \frac{1}{\sqrt{2}}(x + ip)$ is a complex number. Introducing the unitary *displacement* operator

$$D(\alpha) = \exp[\alpha\hat{a}^\dagger - \alpha^*\hat{a}], \tag{2.59}$$

we find that the coherent state $|\alpha\rangle$ is generated by displacing the vacuum

$$|\alpha\rangle = D(\alpha)\,|0\rangle\,. \tag{2.60}$$

The displacement operator $D(\alpha)$ will be repeatedly used in this thesis. It satisfies

$$D^\dagger(\alpha) = D^{-1}(\alpha) = D(-\alpha) \tag{2.61}$$

and its action on the creation and annihilation operators reads

$$D^\dagger(\alpha)\hat{a}D(\alpha) = \hat{a} + \alpha \tag{2.62}$$
$$D^\dagger(\alpha)\hat{a}^\dagger D(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{2.63}$$

The coherent states can be expanded in terms of the number states as

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\ , \tag{2.64}$$

which shows that a coherent state has an undefined number of photons. However, this allows them to have better defined phases than the number states. The probability to have n photons in the state $|\alpha\rangle$ is a Poisson distribution with both mean value and variance $\langle n\rangle = \Delta^2(n) = |\alpha|^2$.

Coherent states are not orthogonal

$$|\langle\beta\,|\alpha\rangle\,| = e^{-|\alpha-\beta|^2/2}\,, \tag{2.65}$$

although $|\alpha\rangle$ and $|\beta\rangle$ become orthogonal in the limit $|\alpha - \beta| \gg 1$. They nevertheless satisfy the completeness relation

$$\frac{1}{\pi}\int \mathrm{d}^2\alpha|\alpha\rangle\langle\alpha| = \mathbb{1}. \tag{2.66}$$

and can therefore be used as a (over complete) basis. Finally, we note that coherent states are often called *quasi-classical* states[1] as the uncertainties in the quadrature operators are equal while their product is the minimum allowed by the uncertainty principle (2.41), i.e.,

$$\Delta^2\hat{x} = \Delta^2\hat{p} = \frac{1}{2}. \tag{2.67}$$

Squeezed States

As we have seen, coherent states saturate the uncertainty principle with equal uncertainty in both quadratures. However, one can easily define an entire family of minimum-uncertainty states with unbalanced uncertainties. The corresponding states are called *squeezed* states, and play an important role in continuous variables quantum information. In particular, they provide an approximation to the unphysical eigenstates of the quadrature operators, $|x\rangle$ and $|p\rangle$ respectively.

The squeezed states may be generated by using the unitary *squeezing* operator

$$S(\varepsilon) = \exp[\frac{1}{2}(\varepsilon^*\hat{a}^2 - \varepsilon\hat{a}^{\dagger 2})]. \tag{2.68}$$

where $\varepsilon = re^{2i\phi}$, and r and ϕ are the squeezing factor and squeezing angle respectively. Using this definition, one can define the squeezed vacuum

$$|0,\varepsilon\rangle = S(\varepsilon)\,|0\rangle\,, \tag{2.69}$$

or an arbitrary squeezed state

$$|\alpha,\varepsilon\rangle = D(\alpha)S(\varepsilon)\,|0\rangle\,, \tag{2.70}$$

resulting from first squeezing the vacuum, then displacing it.

2.2.4 Phase Space Representation and the Wigner Function

A continuous variable system of N modes is a canonical quantum system associated with an infinite dimensional Hilbert space

$$\mathcal{H} = \bigotimes_{i=1}^{N}\mathcal{H}_i.$$

[1] The term quasi-classical to describe coherent states also comes from the fact that they behave as classical light in any optical interferometer such as a beam splitter.

To each mode corresponds an Hilbert space $\mathcal{H}_i$ spanned by the infinite dimensional Fock basis $\{|n_i\rangle\}$, and a couple of position-momentum like operators $\hat{x}_i$ and $\hat{p}_i$. The quadrature operators of the N-mode system can be grouped together in the vector

$$\hat{r} = (\hat{r}_1, \ldots, \hat{r}_N) = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_N, \hat{p}_N) \tag{2.71}$$

an must satisfy the canonical commutation relations

$$[\hat{r}_j, \hat{r}_k] = i\Omega_{jk} \tag{2.72}$$

where Ω is the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.73}$$

As already mentioned, the quadrature operators of a mode of the field behave like the position and momentum of an harmonic oscillator. In classical physics, the motion of a particle can be represented in a phase space where the coordinates of a point give its position and momentum respectively. For many particles, one can represent the statistical distribution of position and momentum in this phase space, hence providing a useful mathematical and graphical representation of the system. In quantum optics, it is possible to push further the analogy between the quadrature operators of the field and the position and momentum of a particle by introducing a similar phase-space representation. This representation is provided by the so-called Wigner function. For a single-mode of the field in a quantum state ρ, this function can be written in terms of the eigenvectors of the quadrature operators

$$W(x,p) = \frac{1}{2\pi} \int \mathrm{d}x' \langle x - x'|\rho|x + x'\rangle e^{ix'p}\,. \tag{2.74}$$

Note that the Wigner function completely characterizes the quantum state ρ, and vice versa. Note also that the definition (2.74) easily generalizes to more than one mode. Although the Wigner function has many properties of a probability distribution, it cannot be considered as such since the quantum mechanical position and momentum of a particle cannot be known simultaneously, i.e. points in phase-space are meaningless. In particular, the Wigner function can take negative values. However, it is a *quasi-probability* distribution whose marginals give the real probability distribution of quadrature measurements, i.e.,

$$P(x) = \int \mathrm{d}p W(x,p) \tag{2.75}$$

$$P(p) = \int \mathrm{d}x W(x,p). \tag{2.76}$$

It is sometimes useful to work with the Fourier transform of the Wigner function called the characteristic funtion. For a single-mode quantum state ρ, the characteristic function reads

$$\chi(\xi) = \mathrm{Tr}[\rho\ D(\xi)] \tag{2.77}$$

where $\xi = (\xi_x, \xi_p) \in 2\mathbb{R}$, and

$$D(\xi) = \exp[i(\xi_x \hat{x} - \xi_p \hat{p})] \tag{2.78}$$

is a *Weyl* (or displacement, see Eq. (2.59)) operator. Introducing the N-mode Weyl operator

$$D(\xi) = e^{i\xi^T \Omega \hat{r}} \tag{2.79}$$

with $\xi \in 2\mathbb{R}^N$, the definition of the characteristic function is easily generalizable to multimode settings.

2.2.5 Gaussian States

The Formalism

From a theorist's perspective, most continuous variable states are difficult to manipulate as their full characterization requires the knowledge of an infinite number of amplitude coefficients. However, there exists one well-known exception which, for this reason, plays an essential role in the development of CV quantum information: the *Gaussian states*. The Gaussian states are defined as those states whose characteristic and Wigner functions are Gaussian functions in phase-space. They are thus fully characterized by the first and second moments of their quadrature operators, the *displacement vector* d and *covariance matrix* γ

$$d = \langle \hat{r} \rangle = \mathrm{Tr}[\rho \hat{r}] \tag{2.80}$$

$$\gamma_{ij} = \mathrm{Tr}[\rho\{(\hat{r}_i - d_i), (\hat{r}_j - d_j)\}] \tag{2.81}$$

where $\{.\}$ denotes anti-commutation. For a single-mode state, this is only 5 independent parameters.

The characteristic function of an N-mode Gaussian state is the Gaussian function

$$\chi(\xi) = \exp[-\frac{1}{4}\xi^T \Gamma \xi + iD^T \xi], \tag{2.82}$$

where $D = \Omega d$ and $\Gamma = \Omega\gamma\Omega$. The Wigner function, on the other hand, is given by the Gaussian

$$W(r) = \frac{1}{\pi^N \sqrt{\det \gamma}} \exp[-(r-d)^T \gamma^{-1} (r-d)]. \tag{2.83}$$

Note that not all $2N \times 2N$ real symmetric matrices can be valid covariance matrices as a state must satisfy Heisenberg's uncertainty principle. This is expressed as

$$\gamma + i\Omega \geq 0, \tag{2.84}$$

which is a necessary and sufficient condition for γ to be the covariance matrix of a Gaussian state. More details on how to manipulate the Wigner function of Gaussian states can be found in Appendix D.

Some Examples

In addition to this attractive mathematical framework, Gaussian states also happen to be the states which can (relatively) easily be implemented and manipulated in a laboratory. For example, the vacuum, coherent states, squeezed states and thermal states are all Gaussian states. In the following, we list the properties of some important one-mode and two-mode Gaussian states that we will repeatedly use in this thesis.

Vacuum The vacuum is a state centered at the origin of phase-space, i.e. $d = (0, 0)$, with the covariance matrix $\gamma = \mathbb{1}$. In phase-space, the vacuum is represented by a disk centered at the origin (see Fig.2.1 left).

Coherent state A coherent state being generated by displacing the vacuum, the coherent state $|\alpha\rangle$ with $\alpha = \frac{1}{\sqrt{2}}(x_\alpha + ip_\alpha)$ has $d = (x_\alpha, p_\alpha)$ and $\gamma = \mathbb{1}$. In phase-space, a coherent state is represented by a disk centered on (x_α, p_α) (see Fig.2.1 left).

Squeezed state The squeezed vacuum is centered at the origin with a vanishing vector of first moments. For a squeezing factor r, its covariance matrix reads

$$\gamma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{2.85}$$

When $r > 0$, we say that the state is squeezed in the x quadrature, while $r < 0$ corresponds to an anti-squeezing in x or, equivalently, a squeezing in the p quadrature. A displaced squeezed state has the same covariance matrix but with non-vanishing first moments. As already mentionned, when $r \to \infty$ ($r \to -\infty$), the squeezed state with covariance matrix (2.85) approximates the unphysical position (momentum) eigenstate $|x\rangle$ ($|p\rangle$). In general, a squeezed state is represented by an ellipse centered on the first moments (see Fig.2.1 right).

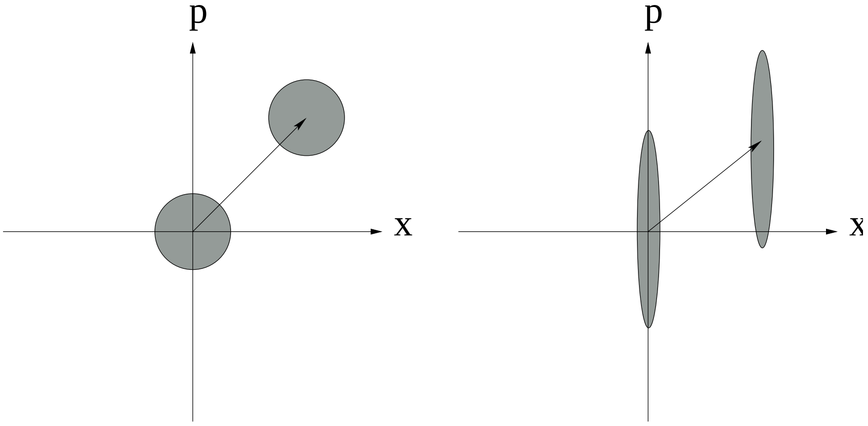

Figure 2.1: *Phase-space representations. Left: Schematic representation of the vacuum and an arbitrary coherent state. Right: Schematic representation of the squeezed vacuum and a displaced squeezed state.*

Thermal state The thermal state has null first moments and a covariance matrix given by

$$\gamma = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}. \tag{2.86}$$

where $V = 2\bar{n} + 1$ and $\bar{n}$ is the average number of photons in the state. It is obtained, for example, by processing the vacuum state in a noisy Gaussian channel with equal noise in x and p.

Two-mode Squeezed vacuum Due to its entanglement properties, the two-mode squeezed vacuum (TMS) is a key ressource in CV quantum information, enabling many protocols such as teleportation [43], dense coding [16], CV quantum key distribution [57], and error correction as we will see in chapter 7. Experimentally, the two-mode squeezed vacuum can be generated by either combining two squeezed states with orthogonal squeezing angles on a balanced beam splitter, or by pumping a Non-degenerate Optical Parametric Amplifier (NOPA). In the Gaussian formalism, the TMS has null first moments and a covariance matrix given by

$$\gamma_{TMS} = \begin{pmatrix} \cosh(2r)\mathbb{1} & \sinh(2r)\Lambda \\ \sinh(2r)\Lambda & \cosh(2r)\mathbb{1} \end{pmatrix}, \tag{2.87}$$

where

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \Lambda = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Interestingly, when $r \to \infty$,

$$\Delta(\hat{x}_1 - \hat{x}_2) = \Delta(\hat{p}_1 + \hat{p}_2) = e^{-2r} \to 0,$$

and the TMS becomes the EPR pair introduced by Einstein, Podolski and Rosen in 1935 to prove the incompleteness of quantum theory [34]. We note that it is sometimes useful to work with the Fock basis description of the TMS,

$$|\psi_{TMS}\rangle = \sqrt{1 - \tanh^2(r)} \sum_n \tanh^n(r) \, |n, n\rangle \, . \tag{2.88}$$

Arbitrary two-mode Gaussian state The covariance matrix of an arbitrary two-mode Gaussian state ρ_{AB} can be decomposed in four blocks

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix}, \tag{2.89}$$

from which we can directly address the properties of systems A and B separately. For example, the covariance matrix of $\rho_A = \mathrm{Tr}_B \, \rho_{AB}$ is given by the upper-left block γ_A (see Appendix D).

2.2.6 Gaussian Operations

Gaussian operations are defined as those that map Gaussian states onto Gaussian states. Interestingly, when dealing with optical continuous variables, the entire set of Gaussian operations can be implemented by combining passive and active linear optical components such as beam splitters, phase shifters and squeezers, with homodyne detection followed by classical communications. All these elements are, up to some degree of accuracy, readily accessible in today's optical labs, which makes Gaussian states and Gaussian operations very attractive for experimental implementation of CV protocols. Note that since Gaussian states are completely characterized by their first and second moments, a Gaussian operation is fully described by its action on d and γ.

Unitary Operations

Gaussian unitary transformations realize the mapping[2]

$$\hat{r} \to \hat{r}' = S\hat{r}, \tag{2.90}$$

[2] Relations which express the transformation as an evolution of the operators correspond to the so-called Heisenberg representation of quantum mechanics. This representation is different, but equivallent, to the traditional representation of quantum mechanics which describes transformations as an evolution of the state itself using the well-known Schrödinger equation. Note that, in quantum information with continuous variables, people are used to switch from one representation to the other depending of the context.

and preserve the canonical commutation relations. This is possible if $S\Omega S^T = \Omega$ which corresponds to the Symplectic operations $S \in Sp(2N, \mathbb{R})$. Note that $\det S = 1$. On the level of covariance matrix, the transformation reads

$$\gamma \to S\gamma S^T. \tag{2.91}$$

A particular subset of the symplectic transformations is formed by the symplectic matrices S that are orthogonal, i.e. $S \in Sp(2N, \mathbb{R}) \cap O(2N)$. These transformations are called passive as they do not change the number of photons, and they include the action of beam splitters and phase shifters with

$$S_{BS} = \begin{pmatrix} \sqrt{T}\mathbb{1} & \sqrt{1-T}\mathbb{1} \\ -\sqrt{1-T}\mathbb{1} & \sqrt{T}\mathbb{1} \end{pmatrix} \tag{2.92}$$

for a beam splitter of transmittance T, and

$$S_{PS} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{2.93}$$

for a rotation of θ in phase-space. Note that every passive transformation of N modes can be realized as a network of beam splitters and phase shifters [89].

The symplectic transformations that are not passive are called active. The most important one is the squeezing operation achieved by pumping an Optical Parametric Amplifier (OPA). Its action is described by

$$S_{Sq} = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}. \tag{2.94}$$

Interestingly, any symplectic transformation of N modes can be realized as a network of beam splitters and phase shifters, followed by squeezers and another set of beam splitters and phase shifters. This is called the Bloch-Messiah reduction theorem (see Fig.2.2 and Chapter 7 for an example).

CP maps

The set of Gaussian unitary operations does not contain all the operations that can be applied to a Gaussian state while maintaining its Gaussian character. One can for example imagine the result of the action of a Gaussian unitary operation U applied to a Gaussian state ρ, together with an environment in a Gaussian state ρ_E, when we do not control the environment, i.e.,

$$\rho \to \mathrm{Tr}_E\, U(\rho \otimes \rho_E)U^\dagger. \tag{2.95}$$

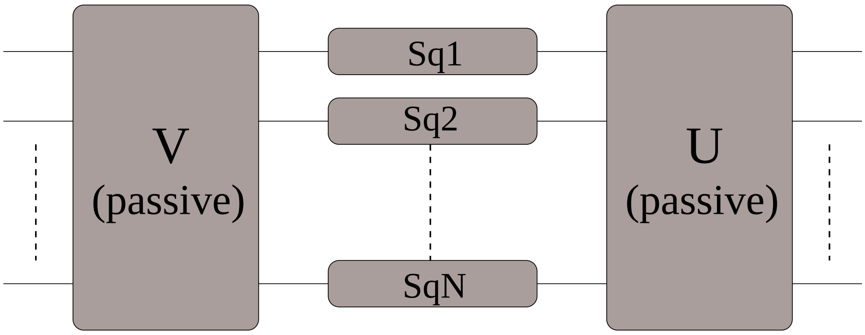

Figure 2.2: *Decomposition of an arbitrary symplectic transformation of N modes as a network of beam splitters, phase shifters and squeezers. U and V are passive linear interferometers.* Sq_i *are single-mode squeezers.*

These transformations, also called Gaussian channels, belong to the general framework of Gaussian completely positive (CP) maps. At the level of covariance matrices, their action is completely characterized by two matrices M and N

$$\gamma \to M\gamma M^T + N \tag{2.96}$$

where M is real and N is real and symmetric. The complete positivity of the map requires that

$$N + i\Omega - iM\Omega M^T \geq 0. \tag{2.97}$$

Instances of Gaussian channels include the transmission through a lossy fiber, or the passive interaction with another mode in a thermal state.

2.2.7 Homodyne Detection

In quantum optics, the way to measure the quadratures of the electromagnetic field is the so-called homodyne detection[3]. The rapidity and high efficiency of this detection technique strongly contributes to the the experimental succes of CV quantum information. Note that from a mathematical point of view, an ideal homodyne detection is a Gaussian operation.

Homodyne detection works as follows. Suppose that we want to measure the position quadrature of a target mode with quadratures $(\hat{x}_t, \hat{p}_t)$. First, this mode is combined at a balanced beam splitter with a strong field ($\sim 10^9$ photons), the so-called local oscillator (LO), used as a phase reference. Denoting by $(X_{LO}, 0)$ the classical quadratures of the local oscillator, the

[3] When both quadratures are measured simultaneously, using a balanced beam splitter and two homodyne detection, the measurement is called an heterodyne measurement.

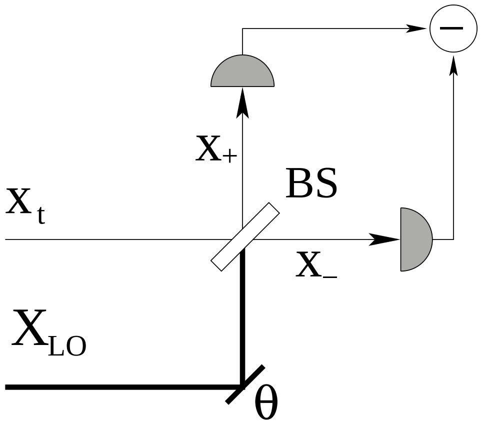

Figure 2.3: *Schematic of an ideal homodyne detection. The quantum target mode (t) is combined with the local oscillator (LO) at a balanced beam splitter (BS). The phase θ of the local oscilator determines the measured quadrature.*

output modes of the beam splitter read

$$\begin{aligned} \hat{x}_+ &= (\hat{x}_t + X_{LO})/\sqrt{2}, \\ \hat{p}_+ &= \hat{p}_t/\sqrt{2}, \\ \hat{x}_- &= (\hat{x}_t - X_{LO})/\sqrt{2}, \\ \hat{p}_- &= \hat{p}_t/\sqrt{2}. \end{aligned} \tag{2.98}$$

Second, the intensities of these two modes are measured using two photodiodes

$$\begin{aligned} I_\pm &\propto \hat{x}_\pm^2 + \hat{p}_\pm^2 \\ &\propto \hat{x}_t^2 + X_{LO}^2 + \hat{p}_t^2 \pm 2X_{LO}\ \hat{x}_t, \end{aligned} \tag{2.99}$$

and the two photocurrents are subtracted and amplified with a low noise amplifier. On can easily check that the difference gives an estimation of the measured quadrature

$$I_+ - I_- \propto X_{LO}\ \hat{x}_t. \tag{2.100}$$

In order to measure the conjugate quadrature $\hat{p}_t$ of the target mode, one simply needs to apply a $\pi/2$ phase shift to the local oscillator. In full generality, one can measure a quadrature $\hat{x}_\theta = \cos\theta\hat{x}_t + \sin\theta\hat{p}_t$ by shifting the phase of the local oscillator by θ, using for example a piezoelectric transducer (PZT). Although technically challenging, the efficiency of a good homodyne detection scheme can easily reach 90% [57, 66].

2.3 Information Theory

Finally, one cannot be called a quantum information scientist without basic knowledge of information theory. As mentionned in the introduction, information theory is a mathematical theory developed by Claude Shannon in 1948 to address the problem of the transmission of information over noisy channels. The most fundamental results of the theory are known as *Shannon's source coding theorem* and *Shannon's channel coding theorem*. The first of these theorems states that, on average, the number of bits needed to represent the result of an uncertain event is given by a quantity called the *entropy*, while the second guarantees that reliable communication is possible over noisy channels provided that the rate of communication is below a certain threshold called the *channel capacity*.

Remarkably, the concepts introduced by Shannon for the manipulation of classical objects can be adapted to the manipulation of quantum states, which gives rise to the theory of quantum information and communication. Quantities such as the entropy or the capacity have their quantum counterpart known as the von Neumann entropy and the quantum channel capacity respectively. The following section will introduce these basic notions, emphasizing on the parallel between the classical versus the quantum version. Let us mention that most of these quantities will not be used directly in the following chapters, but underly the concepts and challenges of quantum information science as a whole.

2.3.1 Classical Information Theory

Suppose that a source emits a sequence of random variables $X_1, X_2, \ldots$ whose values belong to a finite alphabet $A = \{0, 1, \ldots, d\}$. If the variables are independent and identically distributed according to the probability distribution $p(x) = Pr\{X = x\}$, $x \in A$, the *entropy* of the source is defined as

$$H(X) = -\sum_{x \in A} p(x) \log p(x) \,, \tag{2.101}$$

where the logarithm is taken in base 2. The entropy gives a useful measure of the uncertainty one has about X before learning its value. Interestingly, it can also be interpreted as the amount of information one gains by learning the value of X.

Similarly, one can define the *joint entropy* $H(X, Y)$ of a pair of discrete variables (X, Y) which take values in $A_1 = \{0, 1, \ldots, d_1\}$ and $A_2 = \{0, 1, \ldots, d_2\}$, namely

$$H(X, Y) = -\sum_{x \in A_1} \sum_{y \in A_2} p(x, y) \log p(x, y), \tag{2.102}$$

where $p(x,y) = Pr\{X = x, Y = y\}$, $x \in A_1, y \in A_2$, is their joint probability distribution.

Sometimes, the knowledge of the value taken by the variable X provides some information about the possible values of Y and reduces the uncertainty on Y. The average uncertainty we have about Y when X is known is quantified by the *conditional entropy*

$$\begin{aligned} H(Y|X) &= \sum_{x\in A_1} p(x) H(Y|X=x) \\ &= -\sum_{x\in A_1}\sum_{y\in A_2} p(x,y)\log p(y|x). \end{aligned} \tag{2.103}$$

Another useful quantity is the *relative entropy* which quantifies the distance between the two probability distributions $p(x)$ and $q(x)$ on the alphabet A

$$D(p \parallel q) = \sum_{x\in A} p(x)\log\frac{p(x)}{q(x)}. \tag{2.104}$$

Finally, the possibility for the entropy and the conditional entropy of the random variable Y to have different values, i.e. $H(Y) \neq H(Y|X)$, suggests that the variable X contains some information about Y. This common information shared by X and Y can be quantified by the difference $H(Y) - H(Y|X)$ and is known as the *mutual information*

$$I(X:Y) = -\sum_{x\in A_1}\sum_{y\in A_2} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \tag{2.105}$$

$$= D(p(x,y) \parallel p(x)p(y)). \tag{2.106}$$

The mutual information measures in bits the amount of classical correlations between the variables X and Y.

All the quantities introduced in this subsection are closely connected. One can easily verify that they satisfy

$$H(X,Y) = H(X) + H(Y|X) \tag{2.107}$$

$$= H(Y) + H(X|Y), \tag{2.108}$$

$$I(X:Y) = H(X) - H(X|Y) \tag{2.109}$$

$$= H(Y) - H(Y|X) \tag{2.110}$$

$$= H(X) + H(Y) - H(X,Y), \tag{2.111}$$

as graphically illustrated in the Venn diagram of Fig.2.4.

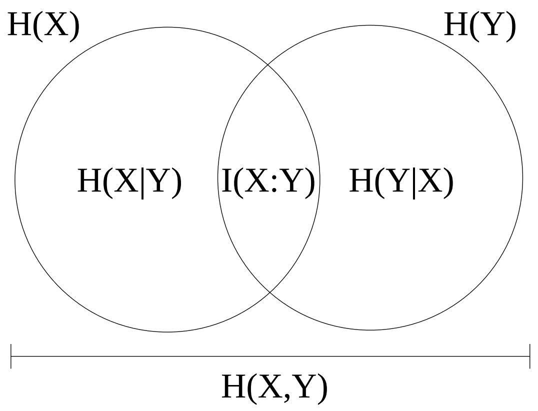

Figure 2.4: *Graphical representation of the various entropies*

The quantities introduced in this subsection can be easilly used to answer questions related to the transmission of information. For example, the maximal rate at which classical information can be reliably transmitted through a noisy channel T is known as the channel capacity $C[T]$, and is given by

$$C[T] = \max_{p(x)} I(X:Y) \tag{2.112}$$

where the maximum is taken over all input distributions $p(x)$ for X, for one use of the channel, and Y is the corresponding induced random variable at the output of the channel.

2.3.2 Quantum Information Theory

Suppose now that the source is no longer classical but emits quantum states chosen from an ensemble $\{|x\rangle\}$ with probability $p(x)$. This can be denoted as $\{|x\rangle, p(x)\}$. The state emitted by the source is described by the mixed state

$$\rho = \sum_x p(x)|x\rangle\langle x|, \tag{2.113}$$

and we can introduce its quantum, or von Neumann, entropy

$$S(\rho) = -\operatorname{Tr}(\rho \log \rho) \tag{2.114}$$

where the logarithm is again taken in base 2. If ρ is diagonal in some eigenbasis $\{|i\rangle\}$, then the von Neumann entropy is the Shannon entropy of the eigenvalues λ_i, i.e. $S(\rho) = H(\lambda)$. As a consequence, the von Neumann entropy of a pure state is null, while it is maximum for a maximally mixed state. This makes the von Neumann entropy an interesting tool for quantum information theory, and for the theory of entanglement in particular.

As an example, consider a bipartite pure state ρ_{AB}. If ρ_{AB} is maximally entangled, then the reduced state $\rho_A = \mathrm{Tr}_B\, \rho_{AB}$ is maximally mixed and $S(\rho_A)$ is maximum. If ρ_{AB} is a product state, however, ρ_A is a pure state and $S(\rho_A) = 0$. As previously mentionned, the entanglement of a bipartite pure state is completely characterized by the von Neumann entropy of any one of its reduced state.

Naturally, for a bipartite quantum system with density matrix ρ_{AB}, one can also define the *joint entropy* $S(A, B)$

$$S(\rho_{AB}) = -\,\mathrm{Tr}(\rho_{AB} \log \rho_{AB}), \tag{2.115}$$

which enables the definition of the *conditional entropy* $S(A|B)$

$$S(A|B) = S(A, B) - S(B). \tag{2.116}$$

In contrary to the classical case, the conditional entropy can be negative [22]. This indicates the presence of entanglement as for systems with $S(A|B) < 0$, the uncertainty about the whole system is less than the uncertainty of one of its constituents.

In analogy with Eq. (2.111), the definition of the joint entropy provides a definition of the quantum *mutual information* [22]

$$S(A : B) = S(A) + S(B) - S(A, B)\,, \tag{2.117}$$

and we can also introduce the *relative entropy*

$$D(\rho \parallel \sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma), \tag{2.118}$$

which provides a useful measure of the distance between the two quantum states ρ and σ.

To conclude this section, we note that there exists various quantum capacities, depending on the information one tries to maximise and the ressources and protocols allowed for. For example, the *classical information capacity* $C[T]$ of a channel T is the asymptotically achievable number of classical bits that can be reliably transmitted per use of the quantum channel. One can also define the *quantum capacity* $Q[T]$, i.e., the number of qubits that can be reliably transmitted through the channel, or the *entanglement-assisted* classical and quantum capacities $C_E[T]$ and $Q_E[T]$, i.e., the rate at which bits or qubits can be transmitted when an infinite amount of entanglement is shared between the sender and receiver [20].

3 Testing Quantum Nonlocality

3.1 Introduction

One of the principal features of quantum mechanics is the impossibility to know simultaneously the value of certain physical quantities with unlimited precision. This limitation does not result from our inability to measure these properties properly, because of the current state of technology for example, but is a consequence of the laws of quantum mechanics themselves. As demonstrated in Sec. 2.1.2, when two quantities are described by non-commuting observables, the perfect knowledge of one precludes the perfect knowledge of the other.

Many physicists of the early days of quantum mechanics were greatly puzzled by such a counterintuitive aspect of the theory. **E**instein, in particular, considered this as a witness of the incompleteness of the theory. In 1935, together with **P**odolski and **R**osen, he advocated his point of view in a seminal paper entitled *"Can Quantum Mechanical Description of Physical Reality Be Considered Complete?"* [34]. Their argument, sometimes referred as the EPR paradox, was the following. In every complete theory, there should be a variable corresponding to an element of reality (a physical quantity that is possible to predict with certainty without disturbing the system). As mentionned above, quantum mechanics precludes the joint knowledge of two non-commuting observables such as the position and momentum of a particle. Hence, either the description of reality given by quantum theory is incomplete, or these two non-commuting observables cannot have simultaneous reality. Considering a special bipartite entangled state known has an EPR pair (equivalent to the maximally entangled two-mode squeezed vacuum of Sec. 2.2.5), and the predictions one can make about the second system of this state based on the measurement of the first, they proved that assuming quantum theory to be complete, i.e., rejecting the first proposition, one could nevertheless assign elements of reality to both non-commuting observables, i.e., one must also reject the second proposition. Their conclusion is thus that one's only choice is to accept the first proposition, and accept that the description of reality given by quantum theory is not complete.

To solve the apparent incompleteness of quantum theory, Einstein, Podolski and Rosen introduced the idea of local hidden variables. Their interpretation of quantum mechanics, known as *Local Realism* or the *Local Hidden Variable* (LHV) model of quantum mechanics, assumes the existence of variables corresponding to all elements of reality, even if some of these variables are inaccessible to measurement. Interestingly, by reintroducing some classical intuition into the description of physical reality, they provided an explanation to the counterintuitive aspects of quantum mechanics such as entanglement and the probabilistic nature of the theory. For many years, depending on their philosophical background or personal beliefs, physicists around the globe argued about the Local Realistic Vs. Quantum Mechanical description of nature.

In 1964, this debate and the EPR argument gained a renewed attention due to the work of John Bell. Assuming local realism to be true, Bell derived his now famous inequality which must be satisfied within the framework of any local realistic theory [7]. Interestingly, this inequality is a relation between conditional probabilities and therefore has *a priori* nothing to do with quantum mechanics. However, Bell predicted a violation of his inequality by considering the probabilities resulting from local measurements on a maximally entangled state. By doing so, he strikingly refuted the possibility to explain quantum mechanics in terms of a local hidden variable model. But the real merit of his work lied somewhere else. After 30 years of philosophical debate, Bell provided a definitive argument in favor of the nonlocal interpretation of quantum mechanics which could be tested in a laboratory. Ironically, Bell's inequality was called *"the most profound discovery of science*" [94] although it is not obeyed by the experimental facts.

Since 1972 and the first experimental violation of a Bell inequality [42], a great variety of Bell tests have been performed based on various quantum systems. In every experiment, a local realistic description of the experimental results is incompatible with the actual observations. Unfortunately, regardless of the success of these experiments, the local description of nature favored by Einstein has not yet been ruled out completely as all the experiments performed to date suffer from so-called loopholes. These conceptual loopholes, exploiting experimental limitations, force us to rely on supplementary assumptions in order to reject local realism, thereby weakening the strength of Bell's argument.

The emergence of quantum information science, and the related discovery that entanglement and nonlocal correlations could be useful ressources [9, 31], naturally triggered the quest for a Bell test free of loopholes. Since Artur Ekert's *"Quantum Cryptography Based on Bell's Theorem"* [31], rejecting local realism and understanding the nonlocal nature of physical reality has left the area of fundamental questions for theoretical physicists, to become an essential ingredient for the development of future technologies and applications. However, the lack of a true loophole free Bell test strongly questions the *operational* use of Bell inequalities in quantum information. If a set of experimental data violates a Bell inequality, can one really conclude that the state under measurement is non local when the detectors are inefficient?

In this chapter, we will contribute to this fascinating quest by considering for the first time m-partite Bell inequalities based on quadrature measurements of the electromagnetic field. Due to the high performances of homodyne detection, such systems are known to possibly close two of the main loopholes simultaneously. In particular, we will prove that it is always possible to maximally violate the m-partite Mermin-Klyshko inequality based on such system, thereby opening a new road towards an experimental test of local realism that could tolerate the inevitable experimental imperfections.

3.2 Bell Tests and Related Loopholes

3.2.1 The CHSH inequality

Let us first introduce an inequality which is, in its spirit, similar to the one initially derived by Bell. There exists infinitely many Bell inequalities, but the well-known CHSH inequality introduced by John **C**lauser, Michael **H**orne, Abner **S**himony and Richard **H**olt in 1969 [24] is certainly the most intuitive one.

To fix the rules of the game, consider the following experiment. Suppose that Alice and Bob, who are spatially separated, receive a box from their friend Charles. They can perform measurements on their box, and each must independently choose between two possible measurements, either A_1 or A_2 for Alice, and B_1 or B_2 for Bob. These measurements have only two possible outcomes ± 1, which are denoted by a_1 or a_2, and b_1 or b_2 respectively. Now assume, as Bell did, that the boxes obey to the local realism of Einstein, Podolski and Rosen. Realism means that the properties measured by Alice and Bob have definite values a_1, a_2, b_1 and b_2 which exist independently of the act of observation. Locality, on the other hand, imposes that Alice's choice of measurement and outcome does not influence the result of Bob's measurement (and vice versa). It follows that the measurement results satisfy

$$a_1(b_1 + b_2) + a_2(b_1 - b_2) = \pm 2 \tag{3.1}$$

This is so because either $b_1 + b_2 = 0$ and $b_1 - b_2 = \pm 2$ or $b_1 - b_2 = 0$ and $b_1 + b_2 = \pm 2$. However, it is important to note that this identity corresponds to four different tests that cannot be performed simultaneously, some of them are *counterfactual* [84]. Nevertheless, the meaning of the identity is guaranteed by the assumptions of realism and locality; realism ensures that all the quantities involved in (3.1) have a simultaneous meaning, while locality is necessary to obtain the value of ±2 on the right hand side. If we now perform many runs of this experiment, we can compute the value of (3.1) on average, which easily leads to the well-known CHSH inequality

$$|\langle a_1 b_1\rangle + \langle a_1 b_2\rangle + \langle a_2 b_1\rangle - \langle a_2 b_2\rangle| \leq 2 \tag{3.2}$$

where $\langle a_i b_j\rangle = P(a_i = b_j) - P(a_i \neq b_j)$ is the average value, or the correlation coefficient, for the measurement of A_i by Alice and B_j by Bob. Recall that (3.2) was derived only assuming locality and realism, i.e., it has to be satisfied by any local realistic theory.

Now suppose that the boxes given to Alice and Bob contain a quantum system. In particular, suppose that the boxes contain each one half of the maximally entangled singlet state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) \tag{3.3}$$

and that the possible measurement settings available to Alice and Bob correspond to

$$\begin{aligned} A_1 &= \sigma_x \\ A_2 &= \sigma_z \\ B_1 &= \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \\ B_2 &= \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z) \end{aligned}$$

where σ_x and σ_z are the standard Pauli operators [78], and $|0\rangle$ and $|1\rangle$ are the eigenvectors of σ_z. Quantum mechanics does not allow the simultaneous consideration of the results of measurements of non-commuting observables, hence for quantum mechanical boxes the identity (3.1) is meaningless. However, quantum mechanics allows the calculation of average values. In particular, we can calculate the average value of the Bell operator

$$S = A_1 \otimes B_1 + A_1 \otimes B_2 + A_2 \otimes B_1 - A_2 \otimes B_2 \tag{3.4}$$

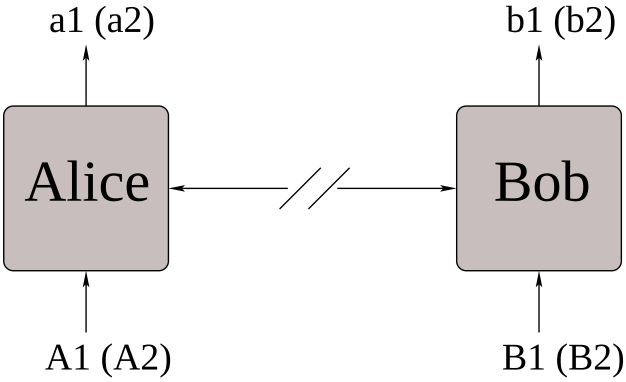

Figure 3.1: *Schematic of a Bell test with two parties and two settings*

for a given quantum state. When the boxes are described by the state $|\Psi^-\rangle$, a few lines of calculation show that the Bell factor

$$\begin{aligned}\mathcal{B} &= |\langle S\rangle| = |\langle A_1 \otimes B_1\rangle + \langle A_1 \otimes B_2\rangle + \langle A_2 \otimes B_1\rangle - \langle A_2 \otimes B_2\rangle| \\ &= 2\sqrt{2} \end{aligned} \tag{3.5}$$

which exceeds the maximum of 2 allowed by Eq. (3.2). Remarkably, quantum mechanics predicts a violation of the CHSH inequality of around 41%.

3.2.2 Detector Efficiency and Locality Loophole

One should not forget that quantum mechanics is a theory about experimental facts. Ultimately, rejecting local realism will have to be done based on experimental data gathered in a laboratory. But experiments are never perfect. They suffer from errors, imperfections, and technological limitations. In order to successfully show that the results of an experiment cannot be explained by a local hidden variable theory, one has to include all these experimental parameters in the local realistic model of the experiment.

Following Freedman and Clauser remarkable experiment in 1972 [42], many Bell tests confirmed the violation of Bell inequalities by quantum mechanics (see e.g. Aspect's experiments [3, 4, 5]). All these early attempts were based on the polarization degree of freedom of photons as it was, for many years, the only known way to generate the necessary entanglement between two distant location. Unfortunately, detecting a photon is a difficult task, and photon detectors are known to suffer from low efficiencies (today typically around 10% [63]). As first noted in [83], this low efficiency can be exploited to explain the observed violation of a Bell inequality with a local hidden variable model. To avoid this problem, one has to make an additional assumption; namely that the registered pairs of photons form a fair sample of the emitted pairs. This is the so-called *detector efficiency loophole*. From a logical point of view, none of the experiments based on photon pairs have successfully succeeded in ruling out local realism.

This loophole was finally closed a few years ago [90, 73], using an entangled pair of trapped ions. The benefit of this novel approach is the high efficiency of the ion state detection. Unfortunately again, entangling ions over large distances is extremely challenging. In the experiments mentioned above, the ions were maintained only several micrometers and one meter apart respectively. So close that the measurement events could not be considered truly space-like separated as required by a local realistic model. This is known as the *locality loophole*.

So far, no experimental test has succeeded in closing both loopholes simultaneously.

3.3 Bell Tests and Continuous Variables

3.3.1 Bell Tests Based on Quadrature Measurements

There is a large variety of quantum systems for which a test of local realism may be envisaged. However, the quest for a loophole free Bell test has recently focused the research towards experiments involving propagating light modes measured with homodyne detectors [76, 102, 44, 45, 77]. The advantage of this approach is twofold. On the one hand, light modes can easily be sent to space-like separated detectors thereby avoiding the locality loophole. On the other hand, the current technology of homodyne detectors achieves a degree of detection efficiency high enough to close the detection efficiency loophole. Unfortunately, the use of continuous variables with homodyne detection also implies drawbacks whose resolution is challenging. The main issue is that the homodyne measurement of a state with a positive Wigner function can always be described with a local hidden variable model. Thus, in order to avoid a local hidden variable description of the measured correlations, one has to perform the test with a state endowed with a non-positive Wigner function. In particular, the easily generated two-mode squeezed state of the EPR argument cannot be directly employed as its positive Wigner function provides a local realistic model explaining all correlations between quadrature measurements.

Several theoretical work have recently demonstrated the possibility to violate a Bell inequality by measuring the quadratures of specifically tailored entangled non-Gaussian states of light. These tests generally involve the following scenario. Two parties perform spacelike separated homodyne measurements by randomly choosing between two settings, thus measuring two quadratures of the incoming electromagnetic fields. The collected data, which are distributed in a (approximately) continuous range, are discretized in a procedure called the *binning process*, and the violation of the CHSH inequality is then tested [24]. Interestingly, these tests can be divided in two categories depending on the magnitude of the predicted violation and the feasibility of the envisioned experimental setup.

Large violation: In [76], Munro identified what ideal correlated photon number state is required to maximally violate the CHSH inequality when homodyne detection is used in combination with a simple binning based on the sign of the measured quadrature. More specifically, he considers the state

$$|\Psi\rangle = \sum_{n=0}^{\infty} c_n |n\rangle |n\rangle \ , \tag{3.6}$$

where $|n\rangle$ is a Fock state, and optimizes over both the quadrature angles of the measurement and the coefficients c_n of the state. This leads to a maximal violation of $\mathcal{B} \approx 2.076$ [1].

Furthermore, it was later shown in [102] that one can even reach the maximal possible value of $\mathcal{B} = 2\sqrt{2}$ by measuring conjugated quadratures of states of the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|f\rangle |f\rangle + e^{i\theta} |g\rangle |g\rangle) \ , \tag{3.7}$$

where f and g are appropriately chosen wave functions, and a special binning based on the roots of the f anf g functions is applied. This will be explained and further extended in Sec. 3.4.2. Unfortunately, the experimental generation of these two types of states is extremely challenging, clearly out of reach of present day technology.

Experimentally feasible: Along a different line of thought, two recent proposals [44, 77] predicted the violation of local realism by considering a state closer to an experimental realization. The state in question is a two-mode squeezed vacuum to which photons have been subtracted. Given the recent sucessful photon subtraction experiments [81, 82], this state is clearly within the reach of present technology. However, the achievable violation with such a photon subtracted squeezed vacuum is so low, around $2,2\%$, that the inevitable experimental imperfections have so far been sufficient to discourage experimentalists from carrying out the experiment.

3.3.2 Multimode Nonlocality

The proposals for loophole free Bell tests relying on homodyne detection have, so far, considered only two parties and the CHSH inequality. This is

[1] If we restrict to positive c_n's as will be seen in Sec. 3.4.1

the simplest scenario, both conceptually and experimentally. However, there exist multipartite Bell inequalities testing the local realism of m-partite entangled states. One such inequality is the Mermin-Klyshko (MK) inequality [74, 67], a generalization to m parties of the CHSH inequality. Interestingly, quantum mechanics predicts an exponentially increasing violation of this inequality with the number of parties involved, i.e., for m parties the maximal violation is [49]

$$\mathcal{B}_m = 2^{(m+1)/2} \tag{3.8}$$

while local realism remains bounded by 2.

We note that multipartite settings with continuous variable states have already been considered, but relying on measurement strategies other than homodyne detection. In Ref. [97] for example, a test based on the measurement of the light field parity is envisaged. It is found that the violation does not increase exponentially, as one would have hoped, but this could be due to the fact that no optimization over the possible measurement settings was performed [37]. In Ref. [23] instead, a maximal violation of the Mermin-Klyshko inequality is found for continuous variable states, considering the measurement of a special class of operators which can be seen as the continuous-variable analogue of the spin operator. However, both of these approaches deal with non-Gaussian measurements described by a non-positive Wigner function. Such measurements are far from the reach of current detection technology.

We note also that very recently, a new approach was introduced which does not rely on the use of inequalities for discrete outcomes, thus avoiding the need of a binning procedure [19]. The authors found that the violation of the local realistic bound is exponential in the number of parties involved, but a possible experimental implementation is still very challenging as it would require at least ten space-like separated homodyne measurements. It is then unclear if such a novel approach can give advantages, from a practical perspective, over the non-locality tests involving binning strategies presented in the next section.

3.4 Multimode Nonlocality using Homodyne Detection

Given this previous work, we ask the following question: Is it possible to have an exponential increase of the violation of local realism in a test involving quadrature measurements of m modes and considering Mermin-Klyshko inequalities?

3.4.1 Correlated Photon Number states

Before we start, let us recall the general form of the Mermin-Klyshko Bell inequalities. As for the CHSH inequality, we consider two dichotomic observables O_t and O'_t for each party t. The Mermin-Klyshko inequalities are then based on the following recursive definition of the Bell operator:

$$B_t \equiv \frac{1}{2}\left[O_t + O'_t\right] \otimes B_{t-1} + \frac{1}{2}\left[O_t - O'_t\right] \otimes B'_{t-1} \ , \tag{3.9}$$

where $B_1 = 2O_1$, $B'_1 = 2O'_1$, and B'_t denotes the same expression as B_t but with all the O_t's and O'_t's exchanged [49]. The Mermin-Klyshko inequality for m parties then reads

$$\mathcal{B}_m \equiv |\langle B_m \rangle| \leq 2 \, . \tag{3.10}$$

Let us now consider a generic photon number correlated state of m bosonic modes

$$|\Psi\rangle = \sum_{n=0}^{\infty} c_n \, |n\rangle_1 \, |n\rangle_2 \ldots |n\rangle_m \ , \tag{3.11}$$

with $\sum_n |c_n|^2 = 1$. This is the generalization to m modes of the state considered in Ref. [76]. There, two quadratures of the electromagnetic field $X(\theta_t)$ and $X(\theta'_t)$ (corresponding to two angles θ and θ') are chosen as the two observable O_t and O'_t to be measured. Recall that the quadrature $X(\theta_t)$ of each mode t can be measured via homodyne detection.

If we introduce the notation X_t (X'_t) for the quadrature $X(\theta_t)$ ($X(\theta'_t)$), and x_t (x'_t) for the outcome of its measurement, the joint probability to obtain the results $x_1, ..., x_m$ by measuring the quadratures $X_1, ..., X_m$ is given by

$$\begin{aligned} \mathcal{P}(x_1, ..., x_m) &= \left| {}_1\langle x_1| \ldots {}_m\langle x_m| \, \Psi\rangle \right|^2 \\ &= \sum_{n,s=0}^{\infty} c_n \, c_s^* \frac{e^{i\phi(n-s)}}{(\pi 2^{n+s} n! s!)^{m/2}} \times \prod_{t=1}^{m} e^{-x_t^2} H_n(x_t) H_s(x_t) \ , \end{aligned}$$

where $\phi = \theta_1 + ... + \theta_m$, $H_t(x)$ is the t-th degree Hermite polynomial, $|x_t\rangle$ are the eigenvectors of the quadrature operator X_t, and we have used the coordinate representation of the Fock states Eq. 2.57.

Consider now a simple binning strategy, the so called *sign binning*: when the result of a quadrature measurement falls in the domain $\mathbb{R}_0^+$, we associate to it the value $+1$, when it is in $\mathbb{R}^-$, we give it the value -1. Based on this binning, we can calculate the probability $\mathcal{P}_{+1,...,+1}$ that a "+1" result is observed in all the measuring sites:

$$\begin{aligned}\mathcal{P}_{+1,...,+1} &= \int_0^\infty \mathrm{d}x_1 ... \int_0^\infty \mathrm{d}x_m \mathcal{P}(x_1,...,x_m) \\ &= \sum_{n,s=0}^{\infty} c_n\, c_s^* \frac{e^{i\phi(n-s)}}{(\pi 2^{n+s} n! s!)^{m/2}} \times \prod_{t=1}^{m} \int_0^\infty \mathrm{d}x_t e^{-x_t^2} H_n(x_t) H_s(x_t)\,. \end{aligned} \tag{3.12}$$

The integrals above can be evaluated recalling the following properties of Hermite polynomials for $n \neq s$,

$$\int_0^\infty \mathrm{d}x_t e^{-x_t^2} H_n(x_t) H_s(x_t) = \frac{\pi 2^{n+s}}{n-s} [F(n,s) - F(s,n)]\,, \tag{3.13}$$

where we defined $F(n,s)$ as

$$F(n,s)^{-1} = \Gamma\left(\frac{1}{2} - \frac{1}{2}n\right) \Gamma\left(-\frac{1}{2}s\right)\,, \tag{3.14}$$

with Γ being the gamma function. For $n = s$ one has instead

$$\int_0^\infty \mathrm{d}x_t e^{-x_t^2} H_n^2(x_t) = 2^{n-1} n! \sqrt{\pi}\,. \tag{3.15}$$

Defining the functions

$$\begin{aligned}\mathcal{G}(\phi,m) &= \sum_{n>s} 2\mathrm{Re}(c_n c_s^*) g_{n,s}(\phi,m)\,, \\ g_{n,s}(\phi,m) &= \left(\frac{\pi 2^{n+s}}{n! s!}\right)^{m/2} \left[\frac{F(n,s) - F(s,n)}{n-s}\right]^m \times \cos[\phi(n-s)]\,, \end{aligned} \tag{3.16}$$

one obtains

$$\mathcal{P}_{+1,...,+1} = \frac{1}{2^m} + \mathcal{G}(\phi,m)\,. \tag{3.17}$$

The other probabilities can be obtained in a similar way. Let us define the multi-index $\mathbf{d} = (d_1,...,d_m)$, with $d_t = \pm 1$ denoting the measurement result obtained for mode t after the binning. Then, the joint probability for a generic collection $\mathbf{d}$ of measurement results will be indicated by $\mathcal{P}_{\mathbf{d}}$ and it can be obtained as above by recalling that an Hermite polynomial of even (odd) degree is an even (odd) function. An explicit formula for the generic probability $\mathcal{P}_{\mathbf{d}}$ can then be calculated:

$$\mathcal{P}_{\mathbf{d}} = \frac{1}{2^m} + \sigma(\mathbf{d}) \mathcal{G}(\phi,m)\,, \tag{3.18}$$

where $\sigma(\mathbf{d}) = \prod_{t=1}^m d_t$.

Now we are in the position to calculate the generic correlation function between the measurement results $E(\phi, m)$. Notice that the correlation depends only on the sum of the angles ϕ. By definition we have that

$$E(\phi, m) = \sum_{\mathbf{d}} \sigma(\mathbf{d}) \mathcal{P}_{\mathbf{d}} \,, \tag{3.19}$$

where the sum goes over all the possible collection of measurement results. Since the number of possible measurement results for which $\sigma(\mathbf{d}) = 1$ is equal to that for which $\sigma(\mathbf{d}) = -1$ one finally has, by substituting Eq. (3.18) into Eq. (3.19), that

$$E(\phi, m) = 2^m \mathcal{G}(\phi, m) \,. \tag{3.20}$$

Let us show that we can reach an exponential violation with a simple analytical manageable example. For the simple case of three parties ($m = 3$), the Mermin-Klyshko inequality then reads $\mathcal{B}_3 \equiv |\langle B_3 \rangle| \leq 2$, with

$$B_3 = O_1 \otimes O_2 \otimes O_3' + O_1 \otimes O_2' \otimes O_3 + O_1' \otimes O_2 \otimes O_3 - O_1' \otimes O_2' \otimes O_3' \,. \tag{3.21}$$

Considering a tripartite GHZ state [55],

$$|\mathrm{GHZ}_3\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \,, \tag{3.22}$$

we have $c_0 = c_1 = 2^{-1/2}$ and $c_{r \geq 2} = 0$, so that

$$\mathcal{G}(\phi, 3) = g_{1,0}(\phi, 3) = (2\pi)^{-3/2} \cos(\phi)$$

and Eq. (3.20) becomes

$$E(\phi, 3) = 2^3 \mathcal{G}(\phi, 3) = \left(\frac{2}{\pi} \right)^{3/2} \cos(\phi). \tag{3.23}$$

The GHZ-like angles ($\theta_1 = 0$, $\theta_2 = \pi/6$, $\theta_3 = 2\pi/6$, and $\theta_i' = \theta_i + \pi/2$), give the maximum violation of the inequality, namely

$$\begin{aligned} \mathcal{B}_3 &= |3\, E(\pi, 3) - E(0, 3)| \\ &= 4 \left(\frac{2}{\pi} \right)^{3/2} \\ &\simeq 2.032 \,. \end{aligned} \tag{3.24}$$

Now, consider the multipartite generalization of the GHZ state

$$|\mathrm{GHZ}_m\rangle = \frac{1}{\sqrt{2}} (|0...0\rangle + |1...1\rangle) \,, \tag{3.25}$$

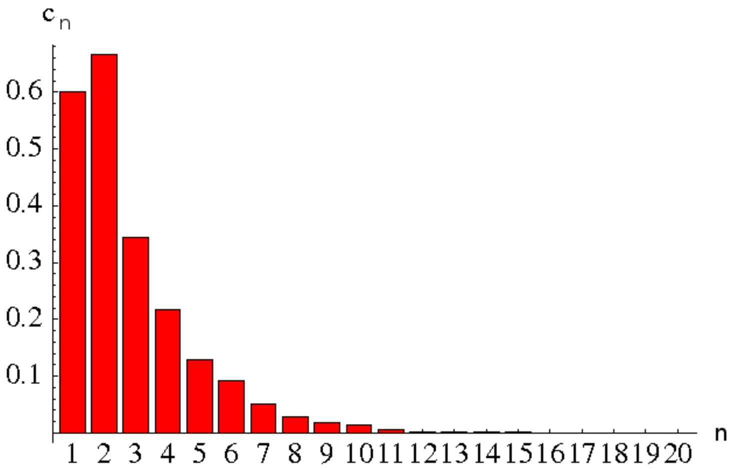

Figure 3.2: *Coefficients c_n for the optimal state $|\Psi\rangle$ in the case of $m = 3$, $d = 20$ (with GHZ-like measurement angles). The Bell factor is $\mathcal{B}_3 \simeq 2.204$.*

and Eq. (3.20) becomes

$$E(\phi, m) = \left(\frac{2}{\pi}\right)^{m/2} \cos\phi\,. \tag{3.26}$$

The dependence on the angle ϕ of the above correlations is the same as the one appearing in a standard spin-like test for a multipartite GHZ state, namely $E(\phi) = \cos(\phi)$. In that case, it is known that the choice of GHZ-like angles

$$\theta_k = (-1)^{m+1}\pi(k-1)/(2m) \tag{3.27}$$

$$\theta'_k = \theta_k + \pi/2, \tag{3.28}$$

gives the highest value of the Bell factor, namely $2^{(m+1)/2}$ [49]. Therefore, using the same angles, the corresponding Bell factor reads

$$\mathcal{B}_m = \sqrt{2}\left(\frac{4}{\pi}\right)^{m/2}, \tag{3.29}$$

giving rise to an exponential violation of local realism.

Apart from this simple analytical example, one can use a numerical approach to show the exponential violation of local realism as the formula (3.20) is easily amenable to perform numerical calculations for a fixed number of parties m. In order to find the state $|\Psi\rangle$ (coefficients c_n's) that maximally violates the Mermin-Klyshko inequality, one has to evaluate the corresponding Bell factor B_m for a given configuration of measuring angles.

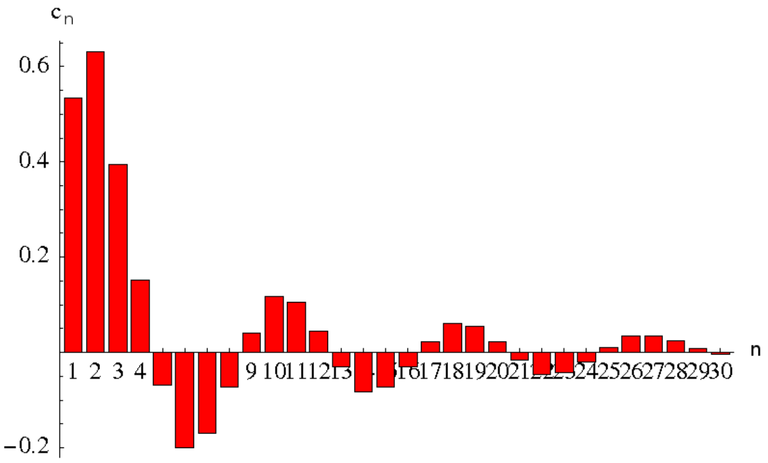

Figure 3.3: *Coefficients c_n for the optimal state $|\Psi\rangle$ in the case of $m = 2$, $d = 30$. The Bell factor is $\mathcal{B}_2 \simeq 2.1$.*

The Bell factors are expressed in general by a linear combination of correlation functions given each by Eq. (3.20), with the prescription given in Eq. (3.9).

Let us search the state which maximizes the violation of the Mermin-Klyshko inequality for the particular GHZ-like choice of angles. For three modes ($m = 3$), defining the (infinite dimensional) real symmetric matrix B_3 as

$$[B_3]_{n,s} = 2^3 \left(3g_{n,s}(\pi, 3) - g_{n,s}(0, 3)\right), \tag{3.30}$$

where the diagonal elements are set to zero, we note that the Bell factor can be re-expressed as $\mathcal{B}_3 = C^\dagger B_3 C$, where the elements of the vector C are given by the coefficients of the input state, *i.e.* $[C]_n = c_n$. Consequently, the maximal violation of the Mermin-Klyshko inequality is simply given by the maximal eigenvalue of the matrix B_3, while the optimal input state is determined by its corresponding eigenvector. In order to perform a numerical analysis, one has to truncate the Hilbert space dimension of $|\Psi\rangle$ to some arbitrary d. For example, for $d = 2$ the optimal choice turns out to be the GHZ state (3.22), giving a violation of $\mathcal{B}_3 = 2.032$. By increasing the dimension d, the asymptotic violation is given by $\mathcal{B}_3 \simeq 2.205$. In Fig. 3.2, we show the coefficients c_n for the optimal state $|\Psi\rangle$ in the case $d = 20$, for which the Bell factor is $\mathcal{B}_3 \simeq 2.204$.

The same procedure can be applied for any number of parties. In the case of two parties ($m = 2$), one recovers the results given by Munro in Ref. [76] provided that the constraint $c_n > 0$ is taken into account, namely $\mathcal{B}_2 \simeq 2.076$. Interestingly, a higher violation can be achieved if we consider negative coefficients for $|\Psi\rangle$. As an example, we report in Fig. 3.3 the coefficients c_n for the optimal state in the case $d = 30$, for which the Bell factor rises up to $\mathcal{B}_2 \simeq 2.100$ (recall that the Bell factor can be written in this case as $\mathcal{B}_2 = 3E(\phi) - E(3\phi)$, where we have chosen $\phi = \pi/4$, as in [76]).

3.4.2 Maximal Violation

Let us now see whether we can find a class of states and a binning strategy that allows for a maximal violation of the Mermin-Klyshko inequality for any number of parties m. Recall that quantum mechanics is bounded by Eq. (3.8). Inspired by the results of Ref. [102], we introduce the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|f\rangle^{\otimes m} + e^{i\theta}|g\rangle^{\otimes m}) \,, \tag{3.31}$$

where f is a real and even function of some quadrature x, while g is real and odd. The two functions are orthogonal and normalized to unity. Note that because $f(x)$ is real and even, it has a real and even Fourier transform $\tilde{f}(p)$, while $g(x)$ has an imaginary Fourier transform $i\tilde{h}(p)$, with $\tilde{h}(p)$ real and odd.

Suppose that each party t chooses to measure one of two conjugated quadrature via homodyne detection, either $X(0) = X$ or $X(\pi/2) = P$, and obtains a continuous variable x_t or p_t depending on his choice of measurement setting. When the k first parties measure the X quadrature, while the remaining $m-k$ measure the conjugate quadrature P, the joint probability that they obtain the results $x_1, ..., x_k, p_{k+1}, ..., p_m$ is given by

$$\begin{aligned}
\mathcal{P}(x_1, ..., x_k, p_{k+1}, ..., p_m) &= |\langle x_1|...\langle x_k|\langle p_{k+1}|...\langle p_m|\Psi\rangle|^2 \\
&= \frac{1}{2}\big(f^2(x_1)...f^2(x_k)\tilde{f}^2(p_{k+1})...\tilde{f}^2(p_m) \\
&\quad + g^2(x_1)...g^2(x_k)\tilde{h}^2(p_{k+1})...\tilde{h}^2(p_m) \\
&\quad + 2\cos(\theta + (m-k)\frac{\pi}{2}) \times f(x_1)g(x_1)...f(x_k)g(x_k) \\
&\quad \times \tilde{f}(p_{k+1})\tilde{h}(p_{k+1})...\tilde{f}(p_m)\tilde{h}(p_m)\big) \,.
\end{aligned} \tag{3.32}$$

To exploit the parity properties of f ang g, we introduce the root binning defined in Ref. [102]. This binning depends on the roots of the known functions f and g. If party t measures the X quadrature, the result will be interpreted as a "+1" if the measured value x_t lies in the interval where $f(x_t)$ and $g(x_t)$ have the same sign, and "−1" if their signs are opposite, i.e., we consider the following domains

$$\begin{aligned}
D_x^+ &= \{x \in \mathbb{R} | f(x)g(x) \geq 0\} \\
D_x^- &= \{x \in \mathbb{R} | f(x)g(x) < 0\} \,.
\end{aligned} \tag{3.33}$$

We can similarly define the domains D_p^+ and D_p^- associated to the measurement of the quadrature P. For the choice of measurement settings defined above, we can thus calculate 2^m probabilities $\mathcal{P}_{\mathbf{d}}$ corresponding to the observation of a given collection $\mathbf{d}$ of binary results. For example, the probability $\mathcal{P}_{+1,\ldots,+1}$ that each party observes a "+1" result reads

$$\begin{aligned}\mathcal{P}_{+1,\ldots,+1} = \int_{D_x^+} \mathrm{d}x_1 \ldots \int_{D_x^+} \mathrm{d}x_k \int_{D_p^+} \mathrm{d}p_{k+1} \ldots \int_{D_p^+} \mathrm{d}p_m \\ \times \mathcal{P}(x_1, \ldots, x_k, p_{k+1}, \ldots, p_m) \,. \qquad (3.34)\end{aligned}$$

We are now in the position to calculate the correlation function $E(X_1, \ldots, X_k, P_{k+1}, \ldots, P_m)$. Note that since f and g ($\tilde{f}$ and $\tilde{h}$) are even and odd respectively, f^2 and g^2 ($\tilde{f}^2$ and $\tilde{h}^2$) are even functions. Hence the first two terms of the right hand side of (3.32) are even functions also, and their contribution to the correlation function will vanish. We thus obtain the remarkably simple expression

$$E(X_1, \ldots, X_k, P_{k+1}, \ldots, P_m) = V^k W^{m-k} \cos\left[\theta + (m-k)\frac{\pi}{2}\right] \,, \qquad (3.35)$$

where

$$V = \int_{-\infty}^{\infty} |f(x)g(x)| dx \qquad (3.36)$$

$$W = \int_{-\infty}^{\infty} |\tilde{f}(p)\tilde{h}(p)| dp \,. \qquad (3.37)$$

Interestingly, the correlation function (3.35) only depends on the number of sites where X and P are measured. One can easily check that all correlation functions corresponding to k measurements of the X quadrature and $m-k$ measurements of the P quadrature are equal. We will denote them $E(k, m-k)$ to emphasize this property.

Let us illustrate the power of this compact notation with an example. For $m = 3$, the Bell factor reads

$$\begin{aligned}\mathcal{B}_3 =& |E(X_1, X_2, P_3) + E(P_1, X_2, X_3) + E(X_1, P_2, X_3) - E(P_1, P_2, P_3)| \\ =& |3E(2,1) - E(0,3)| \\ =& |3V^2 W \cos(\theta + \frac{\pi}{2}) - W^3 \cos(\theta + 3\frac{\pi}{2})| \,. \qquad (3.38)\end{aligned}$$

We see that the maximal violation, i.e. $\mathcal{B}_3^{max} = 4$, can be reached with a state $|\Psi\rangle$ such that $\sin(\theta) = \pm 1$ and $V = W = 1$. Although such a state is quite unrealistic, one can define a family of physical states that approximates it arbitrarily well. The corresponding f ang g functions are trains of gaussians, and $V, W \to 1$ as the number of peaks goes to infinity. We refer the reader to Ref. [102] for their exact analytical expression.

Let us now try to generalize this result for an arbitrary m. First note that the Bell factor (3.10) can be written as

$$\mathcal{B}_m = \frac{1}{2}|\langle X_m B_{m-1}\rangle + \langle P_m B_{m-1}\rangle + \langle X_m B'_{m-1}\rangle - \langle P_m B'_{m-1}\rangle| \,, \tag{3.39}$$

with $B_1 = 2X_1$ and $B'_1 = 2P_1$. In order to benefit from our compact notation, we explicitly develop the expectation values of B_{m-1} and B'_{m-1} in terms of correlation functions

$$\begin{aligned} \langle B_{m-1}\rangle &= \sum_{k=0}^{m-1} \alpha_k E(k, m-1-k) \\ \langle B'_{m-1}\rangle &= \sum_{k=0}^{m-1} \alpha_k E(m-1-k, k) \end{aligned} \tag{3.40}$$

where the α_k's are some known coefficients. When $m-1 = 3$ for example, we have $\alpha_1 = 3$, $\alpha_3 = -1$, and $\alpha_0 = \alpha_2 = 0$. As the correlation functions only depend on the number of X and P measurements, the average values of the four operators of (3.39) can be easily calculated from $\langle B_{m-1}\rangle$ and $\langle B'_{m-1}\rangle$. Suppose B_{m-1} has a term proportional to the $X_1 ... X_k P_{k+1} ... P_{m-1}$ operator, which leads to the correlation function $E(k, m-1-k)$. The operator $X_m B_{m-1}$ will thus have a term proportional to $X_m X_1 ... X_k P_{k+1} ... P_{m-1}$ leading to the correlation function $E(k+1, m-1-k)$, i.e. at the level of correlation functions we only need to replace k by $k+1$ as the X quadrature is measured at one additional site. A similar argument for the expectation values of $P_m B_{m-1}$, $X_m B'_{m-1}$ and $P_m B'_{m-1}$ leads to

$$\begin{aligned} \mathcal{B}_m = \frac{1}{2}| \sum_{k=0}^{m-1} \alpha_k \big(& E(k+1, m-1-k) + E(k, m-k) \\ & + E(m-k, k) - E(m-k-1, k+1) \big)| \end{aligned} \tag{3.41}$$

To maximize this expression, we note that for two and three parties the maximum violation is reached for a state with $V = W = 1$. It is thus reasonable to assume that this property remains true for an arbitrary m. Recall that we know how to choose f and g such as to reach these values. When $V = W = 1$, we have

$$E(k, m-k) = \cos\left[\theta + (m-k)\frac{\pi}{2}\right] \,, \tag{3.42}$$

and (3.40) becomes

$$\langle B_{m-1}\rangle = \sum_{k=0}^{m-1} \alpha_k \cos\left[\theta + (m-1-k)\frac{\pi}{2}\right] \tag{3.43}$$

$$\langle B'_{m-1}\rangle = \sum_{k=0}^{m-1} \alpha_k \cos\left[\theta + k\frac{\pi}{2}\right] \tag{3.44}$$

Introducing Eq. (3.42) in Eq. (3.41), combined with some well known trigonometric formulas, the Bell factor simplifies to

$$\mathcal{B}_m = |\cos(\theta + m\frac{\pi}{4}) + \sin(\theta + m\frac{\pi}{4})| \times |\sum_{k=0}^{m-1} \alpha_k \cos\left[(m-2k)\frac{\pi}{4}\right]|. \quad (3.45)$$

Maximizing the violation of local realism boils down to finding the optimal phase θ_m such that the first factor of the right hand side is maximum. This term achieves its maximum of $\sqrt{2}$ for a value of the phase

$$\theta_m = (1-m)\frac{\pi}{4} \quad (3.46)$$

We also note that

$$(m-2k)\frac{\pi}{4} = \theta_{m-1} + (m-1-k)\frac{\pi}{2} \quad (3.47)$$

hence the maximum value of the Bell factor can be finally written as

$$\begin{aligned} \mathcal{B}_m^{max} &= \sqrt{2}|\sum_{k=0}^{m-1} \alpha_k \cos\left[\theta_{m-1} + (m-1-k)\frac{\pi}{2}\right]| & (3.48) \\ &= \sqrt{2}\ \mathcal{B}_{m-1}^{max} & (3.49) \end{aligned}$$

where we have identified the summation of Eq. (3.48) with Eq. (3.43) at the optimal angle θ_{m-1}. Introducing now the maximum value obtained in Ref. [102] for the two party case, $\mathcal{B}_2^{max} = 2\sqrt{2}$, we obtain by recursion

$$\mathcal{B}_m^{max} = 2^{(m+1)/2} \quad (3.50)$$

which is the known maximal bound imposed by quantum mechanics. Remarkably, the state $|\Psi\rangle$ defined in (3.31) combined with homodyne detection and a binning strategy called *root binning* allows for a maximal violation of the MK inequality. This result shows that even if the binning process discretizing the result of the homodyne detection discards some information, it does not prevent to maximally violate tests of local realism based on discrete variables.

3.4.3 Noise Effects

As shown in the previous sections, the search of loophole-free Bell tests could benefit from an increased number of parties involved in the experiment. The signature of this improvement lies in the exponential increase of the Bell factor with the number of parties m. However, what makes a Bell test challenging in practice is not the magnitude of the violation, but rather the inevitable noise associated with any real experiment. In many cases, this noise is sufficient to hide the nonlocal correlations one tries to observe.

When the number of parties involved in a Bell test increases, so does the fragility of the state used in the experiment. The risk is thus to rescale the violation so that no benefit of a larger m is witnessed *in practice*. One can therefore correctly argue that an increased violation of local realism is only significant if accompanied by a comparable improvement of the robustness to noise of the test. After all, Bell tests have to be verified in a lab, not on paper.

In a discrete variable setting, the question of the tolerance to noise of a Bell test is often investigated introducing the noise fraction [68]. The noise fraction quantifies the maximum amount of depolarizing noise one can add to an entangled state and still detect non-local correlations. The depolarizing noise is characterized by the state $\mathbb{1}/d$, where d is the dimension of the Hilbert space. However, in the continuous variable regime, the Hilbert space under consideration is infinite dimensional and the noise model underlying the noise fraction is irrelevant. Even if we deal with a finite number of photons, such as with the truncated photon number correlated states, the Hilbert space under consideration remains infinite dimensional. Hence the appropriate base is the infinite photon number base and operators proportional to the identity $\mathbb{1}$ have no physical meaning. To adopt an objective measure of the magnitude of the violation of local realism, one must thus introduce an appropriate CV noise model.

The noise we will consider in this section is called *probabilistic erasure*[2]. Consider the following scenario: with a probability p, the system of a random party is erased, otherwise his state is untouched. This noise acts independently on each site and transforms an initial state $|\Psi\rangle$ to

$$\begin{aligned}\rho = (1-p)^m|\Psi\rangle\langle\Psi| + p(1-p)^{m-1}\{\sum_{t=1}^{m} \mathrm{Tr}_t(|\Psi\rangle\langle\Psi|)\otimes|0\rangle_t\langle 0|\} \\ + \ldots + p^m|0\rangle_1\langle 0|\otimes\ldots\otimes|0\rangle_m\langle 0|\,. \qquad (3.51)\end{aligned}$$

Probabilistic erasure is known to appear in, e.g. atmospheric transmissions, and has recently been studied in Ref. [104]. This noise will also be considered in Chapter 7.

Let us first consider the photon number correlated states of subsection 3.4.1, and concentrate on the second term of Eq. (3.51). Each element of the sum corresponds to the erasures of one of the subsystems, so suppose for example that the state of party m has been erased and replaced by vacuum while distributing $|\Psi\rangle$. The corresponding state shared between the

[2] Note that in a real experiment, the most probable sources of noise will be losses and the inefficiency of homodyne detection. Probabilistic erasure is chosen because it can be easily treated analytically.

m parties reads

$$\begin{aligned}\rho_{1,m} &= \mathrm{Tr}_m(|\Psi\rangle\langle\Psi|) \otimes |0\rangle_m\langle 0| \\ &= \sum_{n=0}^{\infty} |c_n|^2 |n\rangle_1\langle n| \otimes ... \otimes |n\rangle_{m-1}\langle n| \otimes |0\rangle_m\langle 0| \,.\end{aligned} \tag{3.52}$$

This state is diagonal in the photon number bases, hence the results of all possible measurements are equiprobable, i.e. $\forall\theta_1, ..., \theta_m$, $P(x(\theta_1), ..., x(\theta_m)) = cst$, and all correlation coefficients vanish. This was to be expected from photon correlated states as their entanglement is truly m-partite; tracing out one subsystem makes the state become separable. Thus, this property also holds for the other noisy terms of (3.51), so that only the erasure-free $|\Psi\rangle\langle\Psi|$ will contribute to the Bell factor. We obtain

$$\mathcal{B}_\rho = (1-p)^m \mathcal{B}_m \tag{3.53}$$

To illustrate this result, consider the m-partite GHZ state (3.25). The noisy Bell factor reads

$$\mathcal{B}_\rho = (1-p)^m \sqrt{2}(\frac{4}{\pi})^{m/2} \,, \tag{3.54}$$

hence the maximum probability of erasure p_{max} such that nonlocal correlations can be detected is

$$p_{max} = 1 - \frac{\sqrt{\pi}}{2} 2^{1/2m} \,. \tag{3.55}$$

This value exponentially tends towards $1 - \sqrt{\pi}/2$ as m goes to infinity, and we observe the desired increased robustness to noise as m becomes large.

Finally, consider now the states of Section 3.4.2. First note that $\langle f|g\rangle = 0$, hence in the $\{|f\rangle, |g\rangle\}$ bases, these states look like GHZ states. We thus expect their robustness to noise to behave like the photon correlated number states. Indeed, going through the calculation, one finds that for every noisy term of (3.51), and for every choice of measurement setting the probability is an even function of the results. For example, if party m looses its mode, the probability $P(x_1, ..., x_m)$ to obtain $x_1, ..., x_m$ given that $X_1, ..., X_m$ is measured is an even function. As a result, none of the noisy terms contribute to the correlation coefficients, and the noisy Bell factor is again given by (3.53) as expected. As a conclusion, with respect to probabilistic erasure, more parties means more robustness.

3.5 A Three-Partite Candidate for a Loophole Free Bell Test

Let us now see how the results of the previous section can be exploited to individuate multipartite states such that, on the one hand, they exhibit a significantly high violation of local realism and, on the other hand, they may be generated with near future technology. In particular, we will focus on a class of three-party state whose generation involves four so-called optical “Schrödinger-cat” states, that is four single mode superpositions of coherent states [81]. We note that a natural candidate to reach our goal could have been the generalization of the photon-subtracted state discussed in Refs. [44, 77]. However, due to symmetry reasons combined with the use of the sign binning, the generalization to three party (actually to any odd number of parties) of the strategy adopted in Refs. [44, 77] is not effective.

In Ref. [102], the authors propose to use a superposition of Gaussians to implement the functions f and g of Eq. (3.31). In particular, in the case of only two Gaussians they considered the family of states defined by

$$f(x) = \langle x| \left[c_+(|\alpha\rangle + |-\alpha\rangle)\right], \tag{3.56a}$$

$$g(x) = \langle x| \left[c_-(|\alpha\rangle - |-\alpha\rangle)\right], \tag{3.56b}$$

where

$$c_\pm^2 = 1/[2(1 \pm e^{-2|\alpha|^2})]. \tag{3.57}$$

Given these functions, one can then calculate the corresponding V and W coefficients using Eq. Eq. (3.36). For large amplitudes $|\alpha| \to \infty$, this gives $V = 1$ and $W \simeq 0.64$. As noticed in Ref. [102], with two parties no violation is possible, i.e $\mathcal{B}_2 \simeq 1.90$.

However, as can be seen in Eq. (3.38), considering three parties already enables a violation as large as $\mathcal{B}_3 \simeq 2.23$. The corresponding state reads

$$|\Psi_3\rangle = \frac{1}{\sqrt{2}}\left[c_-^3(|\alpha\rangle - |-\alpha\rangle)^{\otimes 3} + c_+^3(|\alpha\rangle + |-\alpha\rangle)^{\otimes 3}\right], \tag{3.58}$$

where we have put $\theta = 0$.

Since the maximum violation is achieved for large amplitudes, we consider the following simpler state:

$$\left|\Psi_3'\right\rangle \;=\; c'\left[|\alpha,\alpha,\alpha\rangle + |\alpha,-\alpha,-\alpha\rangle + |-\alpha,\alpha,-\alpha\rangle + |-\alpha,-\alpha,\alpha\rangle\right], \tag{3.59}$$

where

$$c'^2 = 1/[4(1 + 3e^{-4|\alpha|^2})]. \tag{3.60}$$

Notice that $|\Psi_3'\rangle$ coincides with $|\Psi_3\rangle$ when $|\alpha| \to \infty$. In order to obtain the Bell factor $\mathcal{B}_3$ corresponding to such a state, we calculate the probabilities of the binned outcomes using Eq. (3.56) to define the roots, in combination

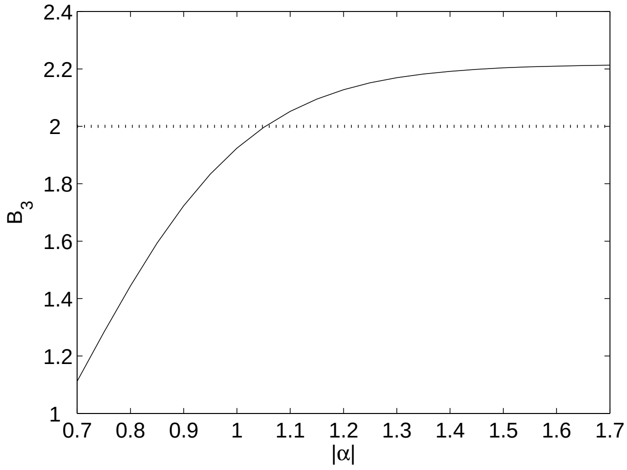

Figure 3.4: *Bell factor $\mathcal{B}_3$ for the state $|\Psi_3'\rangle$ as a function of the amplitude $|\alpha|$.*

with Eqs. (3.32) and (3.34). Specifically, we consider the domains $D_x^{\pm}$ and $D_p^{\pm}$ inherited by the state $|\Psi_3\rangle$:

$$D_x^+ = \{x \in \mathbb{R} | x \geq 0\} \tag{3.61a}$$

$$D_x^- = \{x \in \mathbb{R} | x < 0\} \tag{3.61b}$$

$$D_p^+ = \{p \in \mathbb{R} | -\cos(p\alpha)\sin(p\alpha) \geq 0\} \tag{3.61c}$$

$$D_p^- = \{p \in \mathbb{R} | -\cos(p\alpha)\sin(p\alpha) < 0\} \ . \tag{3.61d}$$

The Bell coefficient $\mathcal{B}_3$ calculated with such a procedure is shown in Fig. 3.4. One can see that for amplitudes as small as $|\alpha| \simeq 1.1$, the state $|\Psi_3'\rangle$ already gives values above the local bound. We note that in this regime of small amplitudes, $|\Psi_3'\rangle \neq |\Psi_3\rangle$ and the domains defined in Eqs. (3.61) might be non-optimal. As α is increased, a violation around 10% of the MK inequality is rapidly achieved.

Now let us describe how the state $|\Psi_3'\rangle$ may be conditionally generated by using linear optics and superpositions of coherent states (SCS) of the form:

$$|\mathrm{SCS}\rangle = c_+(|\alpha\rangle + |-\alpha\rangle). \tag{3.62}$$

Consider the scheme depicted in Fig. 3.5. Two copies of the state $|\mathrm{SCS}\rangle$ in mode a_0 and a_1 are mixed in a balanced beam splitter. The same action is performed on modes a_2 and a_3. Note that mixing two copies of $|\mathrm{SCS}\rangle$ on a balanced beam splitter gives

$$|\mathrm{SCS}\rangle\,|\mathrm{SCS}\rangle \longrightarrow c_+^2[\left|\sqrt{2}\alpha, 0\right\rangle + \left|0, \sqrt{2}\alpha\right\rangle + \left|0, -\sqrt{2}\alpha\right\rangle + \left|-\sqrt{2}\alpha, 0\right\rangle] \tag{3.63}$$

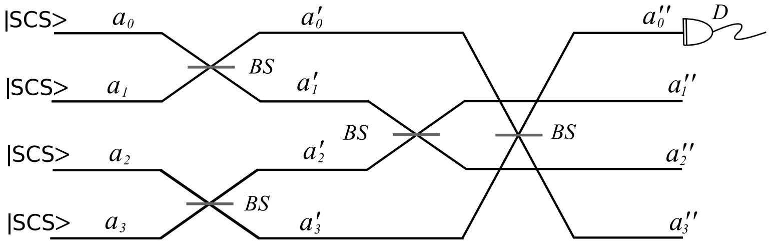

Figure 3.5: *Schematic of a possible way to conditionally generate the state $|\Psi'_3\rangle$ of Eq. (3.59): ($|\mathrm{SCS}\rangle$) superposition of coherent states [see Eq. (3.62)]; (BS) balanced beam splitter; (D) homodyne detector.*

Then modes a'_1 and a'_2, as well as a'_0 and a'_3 are respectively mixed by means of two other beam splitters. As a last step mode a''_0 is measured via a homodyne detector. One can easily show that when the measurement outcome $-\alpha$ is obtained, then the conditional state of the remaining modes coincides (approximately) with $|\Psi'_3\rangle$.

To conclude this section, let us note that generating four states $|\mathrm{SCS}\rangle$ is experimentally demanding. However, the generation in traveling light modes of such Schrödinger-cat state has been recently reported by many groups (see e.g.[81]). One may thus envisage the possibility to implement the whole scheme described in Fig.3.5 in the near future.

3.6 Conclusion

The developpement of QIS has seen an increasing interest towards the characterization and understanding of nonlocal correlations and entanglement. The main tool to verify the existence of such nonlocal correlations between space-like separated locations is to check that the collected data violate a Bell inequality. Unfortunately, technological limitations and imperfections open so-called loopholes, which have to be closed in order to satisfactorily establish the nonlocal nature of quantum mechanics. To date, no experimental Bell test has succeeded in closing these loopholes simultaneously.

Optical continuous variables, combined with the fast and efficient homodyne detection, are an interesting candidate for the experimental implementation of a loophole free Bell test. In theory, they enable to close the detection and locality loophole simultaneously. However, the difficulty to generate non-Gaussian states *efficiently* makes this approach experimentally challenging, and the proposals closer to an experimental realization predict only a small violation of Bell inequalities, whereas the higher violations involve states whose generation is currently out of experimental reach.

In this chapter, we opened a new road in this fascinating quest by investigating the possibility to increase the number of parties involved in a Bell test based on such quadrature measurements of light modes. Our results show that the violation of the m-partite Mermin-Klyshko inequality grows exponentially with the number of parties involved in the test when one uses photon correlated number states combined with a simple binning strategy. Furthermore, by tailoring the state and the binning procedure appropriately, we have proven the possibility to reach maximal violation. The possibility to obtain a maximal violation of the Mermin-Klyshko inequality based on quadrature measurements is non-trivial, since (i) they represent a small subset of all possible measurements and (ii) the binning procedure may cause an irreversible loss of information. As we have shown, such a loss is not crucial if suitable binning procedures are used, properly adapted to the states under investigation.

Our most promising result is illustrated by introducing a three-mode state example achieving 10% violation of the local bound while being, at the same time, implementable with near future technologies.

4 Nonlocality without Entanglement

4.1 Introduction

One of the most intriguing features of quantum mechanics is entanglement. As seen in the previous chapter, entanglement can give rise to nonlocal correlations (or nonlocality), namely the fact that spatially separated systems may behave in a way that cannot be explained by any local theory [34]. This nonlocality, although it does not violate causality, may nevertheless be verified experimentally as one can write a Bell inequality that must be obeyed by any local realistic model but is violated by quantum mechanics.

Interestingly, there also exist other types of nonlocal behaviors which go beyond entanglement. In 1990, Peres and Wootters investigated a set of three correlated product states which required what they called a *combined* measurement, one that interacted with both particles together, to be optimally discriminated [86]. More precisely, they considered two noninteracting spin-1/2 particles prepared with the same polarization, either along the z direction, or in the x-z plane tilted at 120 or -120 degrees from the z axis. Surprisingly, they found that more information could be extracted from this set by considering it as a whole rather than acting on both systems separately, and this in spite of the fact that the systems are in a product state. Inspired by this nonlocal effect manifested by correlated but non-entangled states, Bennett *et al.* discovered in 1998 a set of nine orthogonal product states in $3\otimes3$ dimensions that could not be perfectly distinguished when the two parties are restricted to use a class of operations known as Local Operations and Classical Communications (LOCC) [11]. Yet, as the states are orthogonal and product, they can be perfectly discriminated by a separable operator. They named this bizarre phenomenon *Nonlocality without Entanglement* (NLWE) since it is a truly nonlocal behavior while entanglement is used neither in the preparation of the states, nor in the joint measurement that discriminates them perfectly.

But in what sense exactly is this nonlocality without entanglement nonlocal? Clearly not in the usual sense of being incompatible with a *local hidden variable* (LHV) description. However, as noted in [11], an essential feature of classical mechanics, often omitted in LHV discussions, is the fact that variables corresponding to physical properties are not hidden, but in principle measurable. One could thus say that classical mechanical systems admit a description in terms of *local unhidden variables*. In this chapter, we will see that the sets exhibiting NLWE can be considered nonlocal in the sense that there is no local unhidden variable description of their behavior, i.e., a measurement of the whole reveals more than any sequence of measurement of their parts.

Irrespective of these conceptual issues, the possibility to observe nonlocal effects without the use of entangled states raises some interesting questions. It is a new clear evidence of the nonequivalence between quantum entanglement and quantum nonlocality. Until recently, these two ressources, at the heart of quantum information for the last 25 years, where thought to be two different manifestations of a single characteristic of quantum mechanics. Werner strongly questionned this simple picture by showing that entanglement does not necessarily imply nonlocality in the sense of producing data that are incompatible with local realism [103]. This new type of nonlocality, that should be understood as the advantage of a joint measurement with respect to all LOCC strategies rather than as the incompatibility with local realism, implies that the converse does not hold either. But if

$$\begin{aligned} Entanglement &\not\Rightarrow Nonlocality \\ Entanglement &\not\Leftarrow Nonlocality \end{aligned} \tag{4.1}$$

what is then the nature of the relation between these two essential ressources?

Furthermore, if an operation such as perfectly distinguishing a set of orthogonal product states proves to be impossible when restricted to LOCC, one may wonder what kind of global operations can or cannot be performed using LOCC operations only? This question has attracted a lot of attention over the recent years as it underpins the use of entanglement as a resource in QIS. In particular, this question arises naturally in the hot topic of entanglement distilation, where two parties try to extract a highly entangled state from a collection of weakly entangled mixed states by means of LOCC only (see Appendix E for an example).

4.2 The Domino States

Puzzled by the findings of Peres and Wootters [86], Bennett and co-workers began investigating the distinguishability of unentangled states. Interestingly, the discovery of the well known quantum teleportation [9] grew out of an attempt to identify what ressources, other than actually being in the same place, would enable two parties to make an optimal measurement of the Peres and Wootters states [11]. Besides this famous result, their work also led to the discovery of a set of 9 orthogonal states which exhibited a form of nonlocality qualitatively much stronger than that of Peres and Wootters. While the Peres-Wootters states need an entangled measurement to be optimally distinguished, the discovered set could be perfectly distinguished by a separable operator. They called this set the domino states because of its graphical representation as a set of dominoes (see Fig. 4.1).

The domino states are the following 9 orthogonal product states in $3 \otimes 3$ dimension

$$\begin{aligned}
|\Psi_1\rangle &= |1\rangle_a|1\rangle_b \\
|\Psi_2\rangle &= |0\rangle_a|0+1\rangle_b \\
|\Psi_3\rangle &= |0\rangle_a|0-1\rangle_b \\
|\Psi_4\rangle &= |2\rangle_a|1+2\rangle_b \\
|\Psi_5\rangle &= |2\rangle_a|1-2\rangle_b \qquad (4.2) \\
|\Psi_6\rangle &= |1+2\rangle_a|0\rangle_b \\
|\Psi_7\rangle &= |1-2\rangle_a|0\rangle_b \\
|\Psi_8\rangle &= |0+1\rangle_a|2\rangle_b \\
|\Psi_9\rangle &= |0-1\rangle_a|2\rangle_b
\end{aligned}$$

$$(4.3)$$

To gain some intuition on why this set is special, suppose Alice and Bob, located at A and B, receive one of these 9 states and must determine which one with certainty, i.e., they must return the value of the index i. If they try to achieve this goal using von Neumann (projective) measurements, they will never succeed with unit probability. This can be understood easily by looking at Fig. 4.1. Every measurement, represented by a dotted line, cuts a domino in two hence leaving two states of the set indistinguishable. Suppose for example that Alice tries to discriminate between $\{|0\rangle_a\}$ and $\{|1\rangle_a, |2\rangle_a\}$. Her measurement cuts $|\Psi_8\rangle$ and $|\Psi_9\rangle$, hence it makes these two states indistinguishable by randomly projecting them on either $|0\rangle_a|2\rangle_b$ or $|1\rangle_a|2\rangle_b$. One could imagine that Bob makes a measurement first in order to warn Alice to discriminate rather between $\{|0\rangle_a, |1\rangle_a\}$ and $\{|2\rangle_a\}$ if, for example, he measures $\{|2\rangle_b\}$. But then his measurement will make $|\Psi_4\rangle$ and $|\Psi_5\rangle$ indistinguishable.

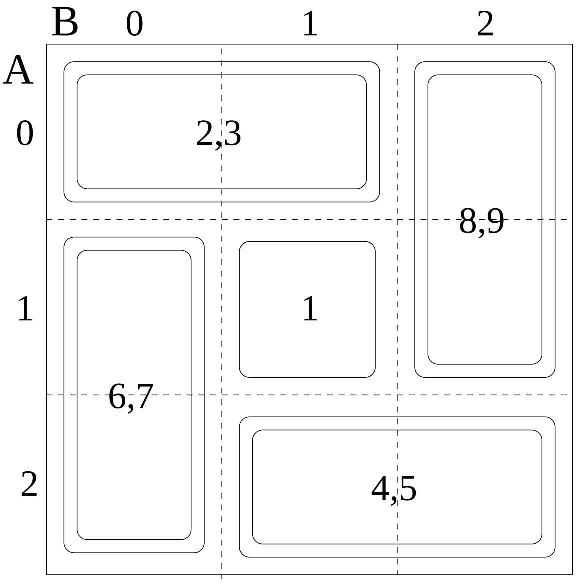

Figure 4.1: *Graphical depiction of the domino states*

Going one step further, because Alice and Bob have access to the entire set of LOCC operations, they can use much more subtle strategies involving many rounds of measurements and POVMs. Nevertheless, as shown in [11], no such strategies will allow to discriminate between the states with certainty. In the language of quantum information theory, this translates into the impossibility to extract all the information from the set. As expected, Bennett and collaborators proved that the maximum mutual information attainable by LOCC was bounded, i.e.

$$I(i : M_{LOCC}) \leq I(i : M_{joint}) - \Delta \tag{4.4}$$

where the deficit Δ is small but finite ($\Delta = 0.00000531$), and M_{LOCC} and M_{Joint} denote the optimal LOCC and joint strategy respectively.

4.3 The Asymmetry of Local Distinguishability

Even if the domino states are orthogonal, they do not appear orthogonal as seen from Alice and Bob alone. Could this simple fact be at the origin of their local indistinguishability? The question of the local distinguishability of a set of states has attracted a lot of attention since the discovery of NLWE. Remember that a set of states, shared between two parties, is exactly locally distinguishable if there exists some sequence of local operations and classical communications that will determine with certainty which state they own. In [100], Walgate *et al.* have shown that any two orthogonal quantum states, entangled or not, can be reliably distinguished using LOCC. Two years later, Walgate and Hardy [99] established the necessary and sufficient conditions for a general set of $2 \otimes 2$ quantum states to be locally distinguishable, and for a general set of $2 \otimes n$ quantum states to be distinguished given that the qubit is measured first. All these results reveal a fundamental *asymmetry* inherent to local distinguishability. To illustrate the asymmetric behavior of local distinguishability, consider the following set

$$\begin{aligned} |\Psi_1\rangle &= |0\rangle_a|0\rangle_b \\ |\Psi_2\rangle &= |0\rangle_a|1\rangle_b \\ |\Psi_3\rangle &= |1\rangle_a|0+1\rangle_b \\ |\Psi_4\rangle &= |1\rangle_a|0-1\rangle_b \end{aligned} \tag{4.5}$$

where $\{|0\rangle, |1\rangle\}$ is called the Computational Basis (CB) while $\{|0 \pm 1\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$ stands for the Dual Basis (DB). This set of bipartite orthogonal product states cannot be reliably distinguished locally if Bob is to go first and only one-way communication from him to Alice is allowed. On the other hand, it can easily be distinguished if Alice performs the first measurement and shares her result with Bob.

As conjectured by Groisman and Vaidman, this asymetry of local distinguishability is at the origin of NLWE. In [56], they studied the *one-way indistinguishability* exhibited by the simple set (4.5), and used it to construct an alternative proof of the NLWE of the domino states. Their key idea was to realize that what is really at issue with NLWE is not the kind of LOCC protocols employed by Alice and Bob, but rather the asymmetric properties of the subsets of the states as seen from Alice and Bob's point of view. In the following section, we will further investigate this close connection between NLWE and one-way indistinguishability. For now, we only note that the set (4.5) can be easily constructed by applying a simple 2-qubit quantum gate to the four states of the computational basis. This quantum gate, called the control-Hadamard (control-H), applies a Hadamard transform to one of the qubits conditioned on the other qubit being in the appropriate state of the CB (in our case $|1\rangle$). Interestingly, it transforms a locally distinguishable set to a one-way indistinguishable one, i.e., it creates asymmetric local indistinguishability.

4.4 The SHIFT Ensemble

4.4.1 A Circuit Based Picture

In addition to the domino states, Bennett and collaborators discovered another set of states conjectured to exhibit nonlocality without entanglement. This less-known set of 8 orthogonal three-qubit product states, called SHIFT, has some interesting features. In particular, it allows for an understanding in term of a simple quantum circuit. The SHIFT ensemble is the following set of states

$$\begin{aligned}
|\Psi_1\rangle &= |0\rangle_a|0\rangle_b|0\rangle_c \\
|\Psi_2\rangle &= |0+1\rangle_a|0\rangle_b|1\rangle_c \\
|\Psi_3\rangle &= |0\rangle_a|1\rangle_b|0+1\rangle_c \\
|\Psi_4\rangle &= |0\rangle_a|1\rangle_b|0-1\rangle_c \\
|\Psi_5\rangle &= |1\rangle_a|0+1\rangle_b|0\rangle_c \\
|\Psi_6\rangle &= |0-1\rangle_a|0\rangle_b|1\rangle_c \\
|\Psi_7\rangle &= |1\rangle_a|0-1\rangle_b|0\rangle_c \\
|\Psi_8\rangle &= |1\rangle_a|1\rangle_b|1\rangle_c
\end{aligned} \tag{4.6}$$

As often with distinguishability issues, the problem is best formulated as a simple game. Suppose an external party randomly chooses a number between 1 and 8, and accordingly prepares the corresponding quantum state $|\Psi_i\rangle$. He then sends the shares of this state to Alice, Bob, and Charles, who are located at A, B, and C respectively. The challenge for them is to identify the state they have received with certainty, i.e. to perfectly determine the value of the label i. Recall that Alice, Bob, and Charles know the precise form of the states of the set but ignore which one has been prepared, and are restricted to LOCC, i.e., they are only allowed to perform sequences of local operations on their respective shares of the state and communicate their results to the other players through a classical channel. In particular, they cannot perform a joint measurement or communicate through a quantum channel. As for the domino states, in such a scenario the players are never able to perfectly distinguish between the 8 possible states [11]. Although the set is made of orthogonal product states, which are distinguishable and can be prepared locally, it has the unexpected property of being *locally indistinguishable*[1].

It is interesting to investigate the implementation of the joint measurement which perfectly discriminates between the states of the set. Formally, it is a projective measurement based on the 8 separable projectors $\Pi_i = |\Psi_i\rangle\langle\Psi_i|$. Consider the 3-qubit unitary operation U, which transforms the 8 states of the CB onto the SHIFT ensemble $\{|\Psi_i\rangle\}$. The knowledge of this joint unitary operation U gives a simple strategy to perform the joint measurement: first apply the joint unitary operation $U^\dagger$ followed by a local measurement by Alice, Bob, and Charles in the computational basis. Interestingly, the unitary U can be implemented by a simple quantum circuit made of 3 identical control-Hadamard gates. As seen in Fig. 4.2, this gate is a tripartite gate which applies a Hadamard transform onto one of the qubits

[1] Throughout this chapter, indistinguishable will mean not perfectly distinguishable. It should not be confused with "indistinguishable" used in the sense that no information at all on the identity of the state can be extracted.

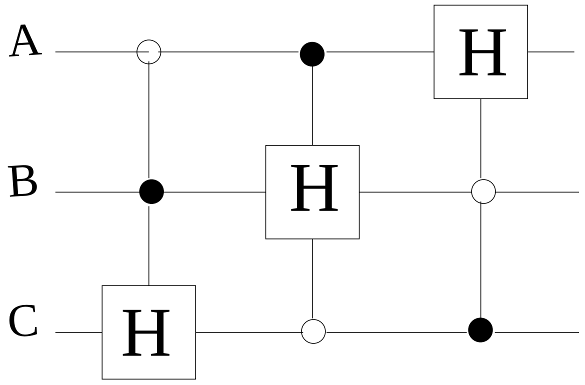

Figure 4.2: *Quantum circuit generating the SHIFT ensemble from the computational basis. The empty and filled circles correspond to a control condition of* $|0\rangle$ *and* $|1\rangle$*, respectively. For example, the first gate applies a Hadamard to Charles' qubit if Alice's qubit is* $|0\rangle$ *and Bob's qubit is* $|1\rangle$*.*

conditioned on the other two being in the appropriate product state $|0\rangle|1\rangle$. More precisely, in case the Hadamard acts on Charles' qubit, this control-H gate performs the operation

$$|i\rangle_a|j\rangle_b|k\rangle_c \longrightarrow \begin{cases} |i\rangle_a|j\rangle_b H|k\rangle_c & \text{if } \ i=0 \wedge j=1 \\ |i\rangle_a|j\rangle_b|k\rangle_c & \text{otherwise} \end{cases}$$

with $H|0\rangle = |0+1\rangle$ and $H|1\rangle = |0-1\rangle$. Because of the cyclic control conditions, the 3 gates appearing in the circuit U are *exclusive*, i.e., one can easily check that if the control conditions are satisfied for one of the gates, they cannot be satisfied for the two others. A direct consequence of this exclusivity property is that the gates are commuting. Consider the first and second gates of the circuit for example. Expressing the Hadamard as $H = \exp(iG)$ with $G = (\pi/2)(\mathbb{1} - H)$, these two gates can be written respectively as $\exp(iA)$ and $\exp(iB)$ with

$$\begin{aligned} A &= \frac{1}{4}\,(\mathbb{1}+\sigma_z)\otimes(\mathbb{1}-\sigma_z)\otimes G \\ B &= \frac{1}{4}\,(\mathbb{1}-\sigma_z)\otimes G\otimes(\mathbb{1}+\sigma_z) \end{aligned}$$

We deduce from these expressions that $AB = BA = 0$ since it contains the product $(\mathbb{1}+\sigma_z)(\mathbb{1}-\sigma_z) = 0$, which translates the exclusivity property. Hence, $[A, B] = 0$, and the Baker-Campbell-Hausdorff formula gives

$$\begin{aligned} \mathrm{e}^{iA}\mathrm{e}^{iB} &= \mathrm{e}^{i(A+B)}\mathrm{e}^{-[A,B]/2} \\ &= \mathrm{e}^{i(A+B)}\mathrm{e}^{[A,B]/2} \\ &= \mathrm{e}^{iB}\mathrm{e}^{iA} \end{aligned}$$

which proves the commutation between the first and second gates of the circuit. The same reasoning trivially holds for any pair of gates.

4.4.2 Understanding the Circuit

Consider first the ensemble constructed by applying only the first control-H (the one that acts on Charles' qubit) on the states of the CB. As shown in [99, 56], this ensemble is indistinguishable if Charles is forced to perform the first non-trivial step of the measurement strategy, or equivalently if he is restricted to one-way classical communication towards Alice and Bob. This is obvious as his share of the state could either be in the computational or in the dual basis, and any non-trivial measurement (one that will gain some information about one of these basis) will always irreversibly loose some information about the conjugate basis. Of course, if Alice and Bob start while Charles is allowed to delay his measurement, then the set appears perfectly distinguishable. Alice and Bob should simply measure in the CB and then inform Charles about the basis he should use. This is the asymmetry of local distinguishability introduced in Sec. 4.3.

Next, let us play the same game but using a quantum circuit made of the first two control-H gates (those acting on Charles' and Bob's qubits). The fact that the two gates are commuting (or exclusive) guarantees that no entanglement will be created when the 8 sates of the CB are processed, i.e., the product states of the CB transform into another set of product states. This time, the ensemble appears indistinguishable to both Charles and Bob as their shares of the states are made of non-orthogonal, hence indistinguishable, states. This is obvious if we adopt a measurement point of view. The second gate tells us that Bob cannot start. But, since the gates commute, the second gate can be interchanged with the first, leading to the similar conclusion that Charles cannot start. Thus, in order to perfectly distinguish the states locally, neither Bob nor Charles may start. Again, if it is Alice who goes first, then the ensemble becomes locally distinguishable. She simply measures her share of the state in the CB: if she gets a $|0\rangle$ she knows that Bob's share should be measured in the CB, and the outcome of Bob's measurement determines which basis Charles should use. A $|1\rangle$ simply interchanges Charles' and Bob's roles. In short, this ensemble is locally indistinguishable if Charles or Bob are forced to start, but distinguishable if Alice goes first.

Finally, consider the entire circuit of Fig. 4.2, that is, the circuit made of the 3 control-H gates and the SHIFT ensemble that it generates. According to the two previous examples, each player now sees an indistinguishable subset created by the Hadamard gate acting on his qubit (this gate can be placed last in the circuit). Consequently, in this last scenario *nobody* wants to start. Because in every LOCC strategy, *someone* has to start,

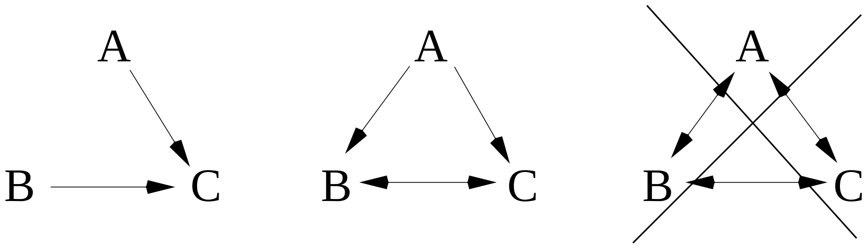

Figure 4.3: *In the first game (left), Charles needs information from both Alice and Bob to make the set distinguishable. In the second game (middle), Bob needs to receive information from Alice and transmit information to Charles, or the reverse, depending on Alice's measurement. In the third scenario (right), even if the players have access to all possible classical communication protocols, the set remains locally indistinguishable (NLWE).*

the ensemble is locally indistinguishable. This simple understanding of the NLWE of the SHIFT ensemble can be summarized as follows:

1. In every LOCC strategy, someone has to start
2. The last gate implies that Alice cannot start
3. The gates commute and can thus be interchanged
4. By (2) and (3), nobody wants to start
5. (1) and (4) are incompatible

The three scenarios presented above and their corresponding LOCC strategies can be nicely illustrated with the diagrams of Fig. 4.3. The arrows represent the minimum amount of communication required to make the ensemble locally distinguishable. This intuitive picture will be translated into a rigorous proof in the next section.

4.5 Multipartite Nonlocality Without Entanglement in Arbitrary Dimension

4.5.1 More Parties and More Dimensions

The intuition gained from the circuit clearly shows that what is really at issue in NLWE is not the kind of LOCC protocols employed by the parties, nor the content of their communication, but rather the asymmetry of local distinguishability encapsulated in the states themselves. Indeed, it is because each player does not know which of the two conjugated basis he should use to measure his share of the state (the set is indistinguishable from his point of view) and because all players are in this same situation (the gates commute) that the ensemble is locally indistinguishable as a whole. Note that, so far, all we have used is the possibility, for each player, to have a state belonging to two conjugate basis. We may therefore extend our construction to systems of arbitrary dimension instead of qubits. Given the central role played by the control-H gate, which creates this local indistinguishability, we may replace it with a d-dimensional quantum Discrete Fourier Transform (DFT_d). This yields a simple strategy to construct an ensemble made of orthogonal tripartite product states of arbitrary dimensions that exhibits NLWE. Note that by changing the control conditions of the gates while maintaining their exclusivity, we can define a whole family of NLWE ensembles with equivalent properties. Furthermore, there is no need to restrict the circuit to a tripartite scenario. Knowing that the key ingredient is a sequence of control-DFT gates that are exclusive (hence commuting), we can further generalize the method and increase the number of parties. The quantum circuit will now be made of n control-DFT gates, one acting on each player, and we require these gates to be exclusive to make sure that the resulting ensemble is made of product states. This imposes some constraint on the dimensions of the players' shares. A simple way to satisfy this exclusivity condition is to require that each player has a Hilbert space large enough to accommodate $n-1$ gates with a different control state. We can therefore state the following sufficient condition

$$d_j \geq n-1\,, \tag{4.7}$$

where d_j is the dimension of $\mathcal{H}_j$, the Hilbert space of player j, and n is the total number of players. We thus have established a generic method to construct some n-partite ensembles of product states exhibiting NLWE using systems of arbitrary dimension. These ideas can be formalized with the following lemma:

Lemma 4.5.1 *If we have $n \geq 3$ parties working in respective Hilbert spaces $\mathcal{H}_j$ of dimension $d_j \geq n-1$, a quantum circuit can be defined, based on n control-DFT gates, which generates a set $\{|\Psi_i\rangle\}$ made of $\prod_j d_j$ orthogonal product states that form a basis of $\bigotimes_j \mathcal{H}_j$ and exhibit Nonlocality Without Entanglement.*

4.5.2 A Lengthy but Generic Proof

Let us denote the CB of player j by $\{|0\rangle, \cdots |d_j-1\rangle\}$. We consider the ensemble generated from the CB of all players by applying the unitary

$$U = \prod_{j=1}^{n} \mathrm{e}^{iA_j} \tag{4.8}$$

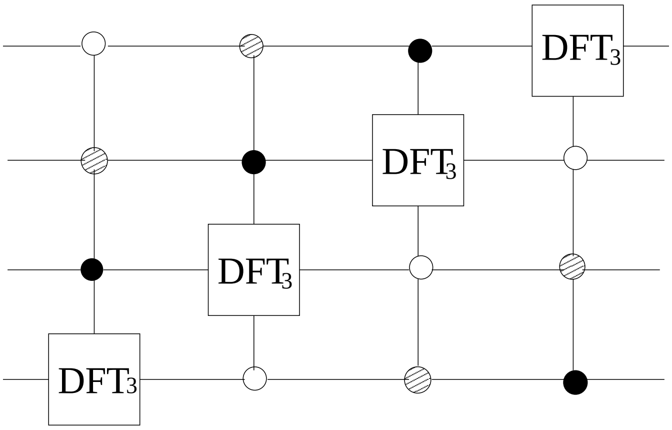

Figure 4.4: *Nonlocality without entanglement in* $3 \otimes 3 \otimes 3 \otimes 3$*. The first gate applies a Discrete Fourier Transform in dimension* 3 *to Damian's qutrit if Alice's state is a* $|0\rangle$*, Bob's state a* $|1\rangle$ *and Charles' state a* $|2\rangle$*.*

with $A_1 = \bigotimes_{j=1}^{n-1} |j-1\rangle\langle j-1| \otimes G$, $A_{2,3,\cdots n}$ are cyclic permutations of A_1, and G is defined so that $\exp[iG]$ applies a Discrete Fourier transform. In the simplest case, each party has a dimension $d_j = n-1$, saturating relation (4.7), but this is not necessary for the proof to hold. As an example, we show in Fig. 4.4 the circuit generating the simplest ensemble exhibiting NLWE for a quadripartite scenario in which all parties hold a qutrit, i.e., in a Hilbert space of total dimension $3 \otimes 3 \otimes 3 \otimes 3$.

Let us prove now that the ensemble generated by the unitary (4.8) exhibits NLWE. Suppose Alice has a share of dimension d and performs the first step of the measurement procedure. We will show that, under the simple constraint of not allowing her operation to lead to a situation in which it has become impossible in principle to perfectly distinguish between the initial states $|\Psi_i\rangle$, then she cannot gain any information. First, let us rewrite the states of the ensemble as $|\Psi_i\rangle = |\phi_i\rangle_A \otimes |\varphi_i\rangle_B$ where $|\phi_i\rangle$ is Alice's share and $|\varphi_i\rangle_B$ is the state held by all the other players. We describe Alice's measurement in two stages: first, her share of the state and the measuring device evolve unitarily under the action of some unitary operator U_A; second, some outcome k is read out. The unitary evolution of Alice's share and the measuring device can be described by:

$$U_A : |\phi_i\rangle_A |A\rangle \longrightarrow \sum_k \alpha_{ik} |\omega_{ik}\rangle \tag{4.9}$$

where $|A\rangle$ is the initial state of the measuring device, and $|\omega_{ik}\rangle$ is the joint state of Alice's share and the measuring device corresponding to a particular outcome k. Without restriction, we can choose α_{ik} to be real and non-negative. Importantly, the states $|\omega_{ik}\rangle$ with different k must be orthogonal as they correspond to different outcomes of the macroscopic measuring device.

Note that Alice only sees $2d$ distinct states $|\phi_i\rangle_A$, the d states of the CB and the d states of the DB. Thus, for each k, it is sufficient to introduce $2d$ couples $\{\alpha_{ik}, |\omega_{ik}\rangle\}$, and we can write the action of the unitary operation U_A on these $2d$ different states $|\phi_i\rangle_A$ as

$$\begin{aligned} |m\rangle_A \otimes |A\rangle \quad &\xrightarrow{U_A} \quad \sum_k \alpha_{mk} |\omega_{mk}\rangle \\ \| m\rangle_A \otimes |A\rangle \quad &\xrightarrow{U_A} \quad \sum_k \alpha'_{mk} |\omega'_{mk}\rangle \end{aligned} \tag{4.10}$$

with k labeling the different outcomes, $m = 0, \ldots, d-1$, and $\|m\rangle$ denoting the states of the DB.

Next, we must impose some constraints on Alice's possible operations. On the one hand, she has to distinguish between the d states that are in the DB at her side since these states appear identical to the other parties. On the other hand, there are also states that are in the CB but are only distinguishable by Alice as they appear nonorthogonal to the other parties [e.g., the states $|\Psi_3\rangle$ and $|\Psi_8\rangle$ of the ensemble (4.6), or the states $|0\rangle_A|2\rangle_B|2\rangle_C|2\rangle_D$ and $|1\rangle_A|2\rangle_B|2\rangle_C|2\rangle_D$ in the example of Fig. 4.4]. For those states, which she sees as orthogonal, she must maintain perfect distinguishability whatever action she performs and for every value of the outcome k. In other words, her measurement must either distinguish these states outright or leave them orthogonal, i.e., we must impose for every k and for all $m \neq n = 0, 1, ..., d-1$

$$\alpha_{mk}\alpha_{nk}\langle\omega_{mk}|\omega_{nk}\rangle \;=\; 0 \tag{4.11a}$$

$$\alpha'_{mk}\alpha'_{nk}\langle\omega'_{mk}|\omega'_{nk}\rangle \;=\; 0 \quad . \tag{4.11b}$$

In addition to these $d(d-1)$ constraints, we also need to consider the relations between the possible initial states at Alice's site. More precisely, we know that the CB and DB are related by the quantum Fourier Transform :

$$\begin{aligned} \|n\rangle &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \exp\left[i\frac{2\pi}{d}nl\right] \; |l\rangle \\ |m\rangle &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \exp\left[-i\frac{2\pi}{d}ml\right] \; \|l\rangle\, . \end{aligned} \tag{4.12}$$

The unitary evolution U_A must conserve these relations, and, since $|\omega_{mk}\rangle$ with different k are orthogonal, we can write $2d$ relations of the form

$$\alpha'_{lk}|\omega'_{lk}\rangle \;=\; \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left[i\frac{2\pi}{d}jl\right] \; \alpha_{jk}|\omega_{jk}\rangle \tag{4.13}$$

$$\alpha_{lk}|\omega_{lk}\rangle \;=\; \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left[-i\frac{2\pi}{d}jl\right] \; \alpha'_{jk}|\omega'_{jk}\rangle\, , \tag{4.14}$$

for each outcome k, with $l = 0, \ldots, d-1$. Consider the d relations of (4.14). If we take the scalar product of two of them and reorganize appropriately the different terms of the sums, we obtain

$$\alpha_{lk}\alpha_{l'k}\langle\omega_{lk}|\omega_{l'k}\rangle = \frac{1}{d}\Big(\sum_{j=0}^{d-1}\exp\left[-i\frac{2\pi}{d}j(l-l')\right]\alpha'^{2}_{jk} + 2\sum_{j=0}^{d-1}\sum_{j'>j}\cos\left[\frac{2\pi}{d}(lj-l'j')\right]\alpha'_{jk}\alpha'_{j'k}\langle\omega'_{j'k}|\omega'_{jk}\rangle\Big) \tag{4.15}$$

If we now choose $l = l'$, it follows

$$\begin{aligned}\alpha^2_{lk} &= \frac{1}{d}\Big(\sum_{j=0}^{d-1}\alpha'^{2}_{jk} \\ &+ 2\sum_{j=0}^{d-1}\sum_{j'>j}\cos\left[\frac{2\pi}{d}l(j-j')\right]\alpha'_{jk}\alpha'_{j'k}\langle\omega'_{j'k}|\omega'_{jk}\rangle\Big) .\end{aligned} \tag{4.16}$$

By the second condition of (4.11), all the terms of the second sum of the right-hand side are trivially equal to zero. Since the remaining term does not depend on the value of l, we conclude that, for each value of the outcome k, all the α_{lk}'s are equal. Similarly, from the d relations of (4.13), we conclude that for all k the α'_{lk}'s must be equal and equal to the α_{lk}'s. It follows that if k is a possible outcome for one particular initial state $|\psi_i\rangle$, then k is a possible outcome for all the initial states (with the same probability). In addition, for all such outcomes k the distinguishability condition (4.11) becomes the true orthogonality condition

$$\langle\omega_{mk}|\omega_{nk}\rangle = 0 \qquad \forall m \neq n \in \{0, 1, \cdots d-1\} \tag{4.17a}$$

$$\langle\omega'_{mk}|\omega'_{nk}\rangle = 0 \qquad \forall m \neq n \in \{0, 1, \cdots d-1\} \tag{4.17b}$$

To summarize, after a measurement procedure which produced the outcome k, the set of possible initial states of Alice's share together with the measuring device have evolved into a set of states which is isomorphic to the initial set, i.e., no information can be gained and communicated to the other players from the value of k. Thus, in order to perfectly distinguish between the states, Alice cannot start. In view of the commutation of the gates, similar arguments can be used to show that the other players face the same dilemma of either gaining some useful information at the cost of irreversibly loosing perfect distinguishability, or not gaining any information at all. This completes the proof. ■

4.5.3 Concluding Remark

First, let us note that the sets we have constructed so far are not the most general ones. Indeed, for $d > 2$ the size of the local Hilbert space allows for

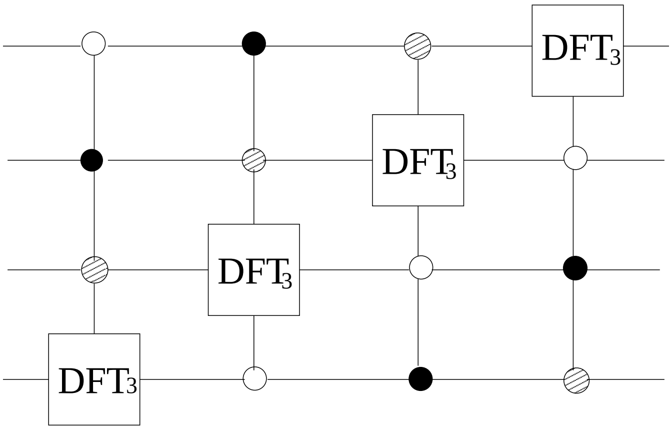

Figure 4.5: *By concatenating this circuit to the one of Fig. 4.4, one gets another ensemble exhibiting NLWE in dimension $3 \otimes 3 \otimes 3 \otimes 3$. The first gate applies a Discrete Fourier Transform in dimension 3 to Damian's qutrit if Alice's state is a $|0\rangle$, Bob's state a $|2\rangle$ and Charles' state a $|1\rangle$.*

the introduction of more gates without loosing the exclusivity (or commutation) condition. For instance, a gate triggered by $|0\rangle_A|2\rangle_B|1\rangle_C$ and acting on Damian's qutrit can be added at the end of the circuit of Fig. 4.4 while conserving the commutation condition. The set constructed with the circuit of Fig. 4.4 supplemented with this gate and its 3 cyclic permutations (as shown on Fig. 4.5) exhibits NLWE while it is qualitatively distinct from the set of Fig. 4.4. In particular, it has more shares in the dual bases, so we conjecture that it should be "more nonlocal" in this respect. Finally, note also that although our method *as it is* fails to create bipartite NLWE, the 9 bipartite domino states of [11] do fit into our picture of commuting control gates. We can associate to this set a quantum circuit made of 4 control-gates, two for each player, where the exclusivity of the gates requires the Fourier Transform to act on 2-dimensional subspaces of $\mathcal{H}_A$ and $\mathcal{H}_B$.

4.6 From Discrete to Continuous Variables

This dissertation is mainly concerned with continuous variables. After all, the reason we investigated the SHIFT ensemble was to understand and extract the mechanisms underlying NLWE, hoping that they could be translated to infinite dimensional Hilbert spaces. This fruitful approach resulted in a simple recipe to create sets of arbitrary dimension exhibiting NLWE. We thus ask the following question: can our recipe be adapted to construct sets of continuous variable product states exhibiting nonlocality without entanglement? We will answer this question by the affirmative, and give the explicit construction of a set of continuous variable product states with the desired property. However, the states of this set are unphysical as they are the eigenstates of the position and momentum operators. We nevertheless recall that they can be approximated as perfectly as needed by the family of squeezed states with finite squeezing (see 2.2.3), and we will briefly discuss the issue of a physical realization of this ensemble at the end of the section.

4.6.1 Unphysical Proof of Principle

The recipe introduced in Sec. 4.5 takes the form of a simple quantum circuit acting on a base of locally distinguishable product states. This circuit has two essential features, or two ingredients: first it creates for each party locally indistinguishable subsets of the states, and second it ensures that no entanglement is produced during this process. Let us now see how these properties translate in the language of continuous variables. To have indistinguishable subsets, we can choose the states to be locally eigenstates of two canonically conjugated observables such as $\hat{x}$ and $\hat{p}$. In analogy with the discrete case, we thus choose our input set to be products of the eigenstates of the position operator $\hat{x}$. Now that we have the structure of the states, we must determine the number of players involved in the game. Our recipe tells us that we can create a set exhibiting NLWE with n players, provided that the local Hilbert space of each party $\mathcal{H}_i$ is large enough to satisfy the exclusivity condition $d_i \geq n-1$ (with n greater or equal to 3). With continuous variables, this condition is always satisfied, hence simplicity suggests to choose $n = 3$. The quantum circuit will therefore be made of three gates, each gate applying a Fourier Transform to one of the modes, locally turning eigenstates of the position operator $|x\rangle$ into eigenstates of the momentum operator $|p\rangle$. Finally, we need to condition this local transformation on the other modes. Because we want a condition which has at least two outcomes, we will locally rotate the states of one mode according to the sign of the other two modes.

Let us summarize our protocol. We have a circuit that takes as input three position eigenstates $|x_a\rangle_A$, $|x_b\rangle_B$ and $|x_c\rangle_C$, and the circuit applies a Fourier Transform (rotation of $\pi/2$ in phase space) to one of these modes according to the following rules:

$$\begin{array}{lll} x_a \geq 0, \quad x_b < 0 & \Rightarrow \; \pi/2 \text{ rotation of} & x_c \\ x_b \geq 0, \quad x_c < 0 & \Rightarrow \; \pi/2 \text{ rotation of} & x_a \\ x_c \geq 0, \quad x_a < 0 & \Rightarrow \; \pi/2 \text{ rotation of} & x_b \end{array} \tag{4.18}$$

This joint operation can be associated to the unitary operator

$$U = U_a \, U_b \, U_c \tag{4.19}$$

where

$$U_j \quad = \quad \exp\left[i\frac{\pi}{2}\;\hat{n}_j\;\theta(x_k)\;\theta(-x_l)\right] \qquad \{j,k,l\} = \{a,b,c\} \tag{4.20}$$

and θ is the Heaviside step function, which is 1 if the argument is positive and null elsewhere. To emphasize the analogy with the SHIFT ensemble of $2\otimes 2\otimes 2$, the set constructed by acting with U on the eigenstates of $\hat{x}_A\hat{x}_B\hat{x}_C$ can be structured in the following 8 different classes:

ψ_1	$\vert x_a^+\rangle_A$	$\vert x_b^+\rangle_B$	$\vert x_c^+\rangle_C$
ψ_2	$\vert x_a^+\rangle_A$	$\vert x_b^-\rangle_B$	$\vert p_c^-\rangle_C$
ψ_3	$\vert x_a^+\rangle_A$	$\vert x_b^-\rangle_B$	$\vert p_c^+\rangle_C$
ψ_4	$\vert x_a^-\rangle_A$	$\vert x_b^-\rangle_B$	$\vert x_c^-\rangle_C$
ψ_5	$\vert x_a^-\rangle_A$	$\vert p_b^-\rangle_B$	$\vert x_c^+\rangle_C$
ψ_6	$\vert x_a^-\rangle_A$	$\vert p_b^+\rangle_B$	$\vert x_c^+\rangle_C$
ψ_7	$\vert p_a^-\rangle_A$	$\vert x_b^+\rangle_B$	$\vert x_c^-\rangle_C$
ψ_8	$\vert p_a^+\rangle_A$	$\vert x_b^+\rangle_B$	$\vert x_c^-\rangle_C$

where $|x^+\rangle$ ($|x^-\rangle$) denotes an eigenstate of the position operator with positive (negative) eigenvalue, and similarly for $|p^\pm\rangle$. To prove that this set exhibits NLWE, we use the same reasoning as in the discrete case, i.e., we show that if we impose on Alice's measurement the constraint that it cannot lead into some irreversible loss of information, then her measurement cannot gain any information at all. Note that this argument strongly relies on the notion of perfect distinguishability which is relevant for the unphysical eigenstates of $\hat{x}$ and $\hat{p}$, but not for their physical approximation the squeezed state of finite variance.

The main steps of the argument are the following: define again Alice's measurement procedure as a unitary evolution U of her state and measuring device followed by a "collapse" (real or virtual) after which an outcome x' is read:

$$U : |\phi_i(x)\rangle|A\rangle \longrightarrow \int \mathrm{d}x' f_i(x,x')|\omega_i(x,x')\rangle \qquad i = x,p \tag{4.21}$$

where $|A\rangle$ is the initial state of Alice's measuring device, $|\omega_i(x,x')\rangle$ is the quantum state of Alice's particle and measuring devices corresponding to a particular outcome x', the coefficients f_i are chosen to be real and nonnegatives and we integrate over all possible outcomes x'. Impose the constraint that the measurement must either distinguish outright the states that she is the only one able to perfectly distinguish, or if it doesn't then it must leave them orthogonal, i.e.,

$$\begin{aligned} f_x(x,x')f_x(y,x')\langle\omega_x(x,x')|\omega_x(y,x')\rangle &= f_x^2(x,x')\delta(x-y) \\ f_p(x,x')f_p(y,x')\langle\omega_p(x,x')|\omega_p(y,x')\rangle &= f_p^2(x,x')\delta(x-y)\,. \end{aligned} \tag{4.22}$$

Remember that the two types of states, (infinitely) squeezed in x and (infinitely) squeezed in p, are related by a Fourier Transform and that the unitary evolution U keeps these relations, in particular for every value of the outcome x'. For example, we can write

$$f_p(x,x')|\omega_p(x,x')\rangle = \frac{1}{\sqrt{2\pi}}\int \mathrm{d}z e^{-ixz} f_x(z,x')|\omega_x(z,x')\rangle\,. \tag{4.23}$$

We have a set of similar conjugated relations linking the x and the p bases. If we take the norm of all such relations we get

$$\begin{aligned} f_p^2(x,x') &= \frac{1}{2\pi}\int\int \mathrm{d}z\mathrm{d}z' e^{-ix(z-z')} f_x(z,x')f_x(z',x')\langle\omega_x(z',x')|\omega_x(z,x')\rangle \\ &= \frac{1}{2\pi}\int \mathrm{d}z f_x^2(z,x') \end{aligned} \tag{4.24}$$

where we have introduced the constraint (4.22) to get the second relation. Because the right hand side is independent of the value of x, it follows that all the f_p coefficients are equal for a given outcome x'. A similar calculation for the conjugated relation imposes that all the f_x coefficients are equal and equal to the f_p coefficients. Hence, as in the case of qudits, we conclude that under the constraint (4.22), no information can be gained by Alice and transmitted to the other players.

4.6.2 Unproved Physical Example

Let us conclude this section by briefly discussing a possible physical realization of the set considered above. The eigenstates of the position and momentum operators can be physically approximated by squeezed states along the x and p quadratures with a finite variance σ^2. The input set will thus be made of product of squeezed states in x whose center are distributed according to a Gaussian distribution of variance $\Sigma^2 = \frac{1}{\sigma^2} - \sigma^2$. This latter condition ensures that each party sees locally a thermal state of variance $\frac{1}{\sigma^2}$. Note that because finitely squeezed states are not orthogonal to each other, our input set is not perfectly distinguishable to start with. It follows that imposing constraints such as (4.22) does not make any sense. On the other hand, those relations reflect some general principle that still applies when the squeezing is finite. What (4.22) really says is that Alice's operations must either gain some information about the x quadrature, or leave the states squeezed in the x quadrature as distinguishable as they where before her measurement. The second relation says the same about the p quadrature. Hence, we could restate these distinguishability conditions as

"the measurement performed by Alice must either gain some information about the x quadrature or leave the accessible information in that quadrature

unaltered, and either gain some information about the p quadrature or leave the accessible information in that quadrature unaltered".

Because x and p do not commute, the only way for Alice to fulfil both requirements simultaneously is by not gaining any information at all. This argument is quite general and suggests that this physically relevant set does exhibit NLWE. However, although intuitive, the argument does not replace a quantitative proof [2]. Finally, we note that even if we turn to physical states with finite squeezing, the unitary operator (4.19) needed to make (or measure) the states requires an Hamiltonian that is cubic in the quadratures, making an experimental realization quite challenging.

4.7 Conclusions

Nonlocality without entanglement is a fascinating phenomenon. It is a striking evidence of the many mysteries quantum mechanics still has to reveal. Our investigation of this recently discovered peculiarity of the quantum theory highlighted the essential role played by a simple quantum gate, the control-Hadamard, as a source of local indistinguishability. The introduction of this gate enables a circuit-based approach of this new form of nonlocality, easily generalizable both in the number of parties and in the dimension of their respective spaces. We therefore presented the first method to construct n-partite d-dimensional product bases which cannot be perfectly distinguished by LOCC. For example, in Fig. 4.4 we display a quantum circuit generating nonlocality without entanglement with 4 qutrits. To our knowledge, this is the first example of this nonlocality in $3 \otimes 3 \otimes 3 \otimes 3$.

Adapting our method to the regime of continuous variables, we derived an infinite set of 3-modal states with the desired behavior. However, this set is unrealistic as it relies on infinitely squeezed states of the position and momentum quadratures. It is nevertheless a valid set, and it can therefore be considered as a *proof of principle* of the existence of nonlocality without entanglement in the continuous variable regime.

The approach developed in this chapter shed some light on the mechanisms underlying the origin of nonlocality without entanglement, and we believe that it is a new tool to improve our understanding of the complex relation between nonlocality and entanglement. However, the benefits of our work go beyond the sole understanding of this new type of nonlocality. It is known for example that nonlocality without entanglement is connected to other recently discovered peculiarities of the quantum world known as unextendible product bases (UPB) and bound entanglement (BE). Understanding and characterizing the latter has been at the center of attention

[2] Note that in the spirit of Bennnett et.al. original paper, we have tried to place a bound on the mutual information obtainable by LOCC but did not succeed.

for the past 5 years, and we show in Appendix A and B that our circuit based approach enables the first generic construction of a large family of unextendible product bases and their related bound entangled states.

Finally, we note that contrary to the original work on the domino states [11], we did not place a bound on the mutual information attainable through LOCC. Instead, we adopted a simpler strategy and proved that such a non-trivial bound necessarily exists[3]. Nonetheless, a method to calculate this bound for a given set is highly desirable as it would enable a quantitative comparison of nonlocality without entanglement.

[3] Strictly speaking, we did not ruled out the possibility that the resulting gap becomes infinitely small as the number of LOCC rounds goes to infinity. However, various reasons suggest that, as proved in [11] for the domino states and the SHIFT ensemble, it is not the case and this gap is always finite.

5

Nonlocality Without Squeezing

5.1 Introduction

Nonlocality is a versatile ressource. One can for example establish useful nonlocal correlations between two distant locations by distributing entangled states. In such a scenario, the nonlocality arises when one performs local measurement on both parts of an entangled state. This is the nonlocality considered in Chapter 3. But nonlocality goes beyond entanglement. The nonlocality without entanglement investigated in Chapter 4 shows that one can also witness a truly nonlocal behavior from a set of orthogonal product states. This weaker form of nonlocality arises when one applies a joint, yet not entangled, measurement to a set of product states. But is this picture complete? Have we characterized all possible manifestations of nonlocality yet? Clearly, these two different types of nonlocal behavior suggest a third and intermediary form of nonlocality, one that would arise from a joint and entangled measurement performed on a set of product states (note that by an entangled measurement, we mean a measurement whose eigenvectors are entangled). Remarkably, this is the nonlocality that was conjectured by Peres and Wootters in [86], and led to the discovery of nonlocality without entanglement. This unexpected property, exhibited by identical particles, has now been rigorously demonstrated. In [72], Massar and Popescu considered a set of N identically prepared spin-1/2 particles pointing in an arbitrary direction, and showed that the optimal strategy to identify that direction required an entangled measurement. In a sense, this third kind of nonlocal behavior can be considered as the dual of that manifested by entangled systems: entangled states must be prepared jointly but exhibit anomalous correlations when measured locally; these sets of identical states can be prepared locally but exhibit anomalous properties when measured jointly with an entangled measurement.

Interestingly, both of these nonlocality illustrate the rich nature of entanglement. In the first one, entanglement, in the form of a state, is used as a medium to establish nonlocal correlations. In the second, entanglement, in the form of a measurement, takes profit of purely classical correlations to provide a better access to the information encoded in a product state. Puzzled by this latter ability of entanglement to exploit classical correlations, Gisin and Popescu discovered yet another surprising property of quantum mechanics. In [50], they surprisingly proved that more information could be extracted from a pair of anti-parallel spins than from a pair of identical ones. Unexpectedly, some classical correlations perform better than others when one uses entanglement to extract information from a set of classically correlated product states.

For us, interested in continuous variables, it is naturally tempting to ask whether similar quantum effects may be observed with CV product states. Although not complete, the previous chapter demonstrated the existence of nonlocality without entanglement in the continuous regime. We are thus tempted to conjecture the existence of nonlocal effects when product states are detected with an entangled measurement. This conjecture will be proven in the following sections. First, we will understand that the difference between pairs of parallel and antiparallel spins observed by Gisin and Popescu lies in an impossibility of quantum mechanics called spin-flipping. The existence of an analog impossibility in the continuous regime, called phase conjugation, will guide us towards the discovery of an ensemble of classically correlated product coherent states that can be better discriminated with an entangled measurement than separately (LOCC). This may be viewed as a nonlocal effect without squeezing, and is in a sense the continuous variable analog of the nonlocality conjectured by Peres and Wootters. We will call this property *Nonlocality Without Squeezing* in reference to the well-known nonlocality without entanglement of Chapter 4. Remarkably, our findings can be experimentally demonstrated, and at the end of this chapter we will briefly report on an experiment performed in collaboration with the group of U.L. Andersen of the Technical University of Denmark[1].

[1] Part of this experimental work was performed at the Max-Planck Institute for Optics, Information and Photonics of the University of Erlangen.

5.2 Parallel and Antiparallel Spins

Consider the following problem. Suppose Alice wants to communicate a direction $\vec{n}$ to Bob, and she can send him two (unentangled) spin-1/2 particles. She has to choose between two possible strategies, she can either send two identical particles polarized along the direction $\vec{n}$ or two particles polarized along the opposite directions $\pm\vec{n}$, i.e., she sends the states $|\vec{n},\vec{n}\rangle$ or $|\vec{n},-\vec{n}\rangle$ where

$$\begin{aligned}|\vec{n}\rangle &= \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \\ |-\vec{n}\rangle &= \sin(\theta/2)|0\rangle - e^{i\phi}\cos(\theta/2)|1\rangle\,. \end{aligned} \tag{5.1}$$

Bob's task is to measure the two spins and make a guess $\vec{n}_g$ of the direction he believes Alice is trying to communicate. Depending on the situation, he has access to two different measuring strategies. He can either measure the two particles separately (the local strategy), or he can act on both particles jointly (the joint strategy).

We thus consider four different protocols, i.e., two encoding strategies for Alice and two measuring strategies for Bob. To compare the performances of these protocols, we introduce the average fidelity

$$F = \int \mathrm{d}\vec{n}\, p(\vec{n}) \sum_g P(\vec{n}_g|\vec{n}) \frac{1+\vec{n}\vec{n}_g}{2}\,, \tag{5.2}$$

where $\vec{n}\vec{n}_g$ is the scalar product between the true and the guessed direction, $p(\vec{n})$ is the probability that Alice chooses the direction $\vec{n}$ and $P(\vec{n}_g|\vec{n})$ is the probability that Bob guesses $\vec{n}_g$ when the true direction is $\vec{n}$. Note that we assume the direction $\vec{n}$ to be chosen at random and uniformly distributed over the unit sphere.

When Alice prepares identical spins, the optimal measurement was found by Massar and Popescu [72]. It is an entangled measurement described by an operator A whose four eigenvectors $|\phi_j\rangle$ are

$$|\phi_j\rangle = \frac{\sqrt{3}}{2}\,|\vec{n}_j,\vec{n}_j\rangle + \frac{1}{2}\,|\Psi^-\rangle\,, \tag{5.3}$$

where $|\Psi^-\rangle$ is the maximally entangled singlet state defined in Eq. (3.3), and the vectors $\vec{n}_j$ point to the vertices of the tetrahedron

$$\begin{aligned}\vec{n}_1 &= (0,0,1),\\ \vec{n}_2 &= (\frac{\sqrt{8}}{3},0,-\frac{1}{3}),\\ \vec{n}_3 &= (\frac{-\sqrt{2}}{3},\sqrt{\frac{2}{3}},-\frac{1}{3}),\\ \vec{n}_4 &= (\frac{-\sqrt{2}}{3},-\sqrt{\frac{2}{3}},-\frac{1}{3}).\end{aligned} \tag{5.4}$$

Note that the phase used in the definition of $|\overrightarrow{n}_j\rangle$ is such that the four states $|\phi_j\rangle$ are orthogonal. When Bob measures $|\phi_j\rangle$, he guesses the direction $\overrightarrow{n}_j$ and this optimal strategy leads to a fidelity of

$$F^{\uparrow\uparrow}_{Joint} = \frac{3}{4} \tag{5.5}$$

Finally, one can prove that no local strategy can reach this value, which is sufficient to prove the conjecture of Peres and Wooters. Note that when Alice sends N identical particles, the optimal joint strategy leads to $F = \frac{N+1}{N+2}$.

When Alice sends antiparallel spins however, Gisin and Popescu proved that the joint measurement whose four eigenvectors are

$$|\varphi_j\rangle = \alpha\,|\overrightarrow{n}_j, -\overrightarrow{n}_j\rangle - \beta \sum_{k\neq j} |\overrightarrow{n}_k, -\overrightarrow{n}_k\rangle\,, \tag{5.6}$$

with $\alpha = 13/(6\sqrt{6} - 2\sqrt{2})$ and $\beta = (5 - 2\sqrt{3})/(6\sqrt{6} - 2\sqrt{2})$, leads to a fidelity of [50]

$$F^{\perp}_{Joint} = \frac{5\sqrt{3} + 33}{3(3\sqrt{3} - 1)^2} \approx 0.789\,. \tag{5.7}$$

This fidelity was later shown to be optimal in connection with cloning transformations [38]. Surprisingly, parallel and antiparallel spins are not equivalent. To conclude this section, let us note that when Bob is restricted to local operations, both parallel and antiparallel spins will lead to the same optimal fidelity. This is so because for every optimal strategy for $|\overrightarrow{n}, \overrightarrow{n}\rangle$, there is a corresponding optimal strategy for $|\overrightarrow{n}, -\overrightarrow{n}\rangle$. One can thus summarize these results as

$$F^{\uparrow\uparrow}_{Local} = F^{\perp}_{Local} < F^{\uparrow\uparrow}_{Joint} < F^{\perp}_{Joint} \tag{5.8}$$

5.3 Spin Flipping and Phase Conjugation

How does quantum mechanics make pairs of parallel and antiparallel spins behave differently? At first sight, it seems that by simply flipping the second spin, we should be able to go from one situation to the other. If, for example, Bob knows how to optimally measure identical particles but receives antiparallel ones, he should just flip the second qubit and then applies his optimal measurement. One would expect these two strategies to give exactly the same fidelity. And indeed, they would... except that quantum mechanics precludes the perfect flipping of an unknown particle [18]. That is, there is no physical operator Θ such that

$$\Theta\,|\overrightarrow{n}\rangle = |-\overrightarrow{n}\rangle \tag{5.9}$$

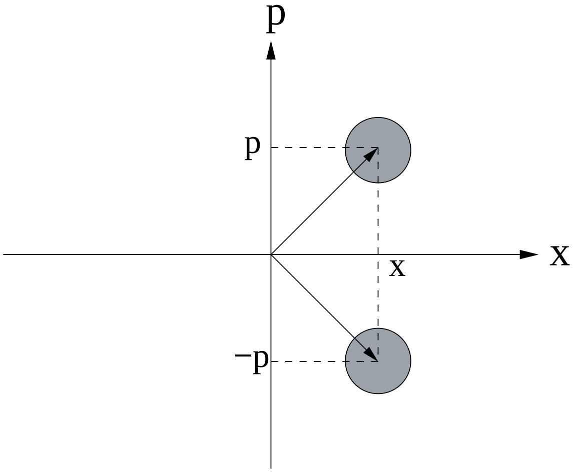

Figure 5.1: *The Phase conjugation operator flips the sign of the $\hat{p}$ quadrature while keeping quadrature $\hat{x}$ unchanged*

The reason behind such an impossibility lies at the very heart of quantum mechanics; the flipping operator Θ is antiunitary while quantum mechanics only allows unitary operations.

Remarkably, this simple impossibility enables the existence of the peculiar effect witnessed by Gisin and Popescu. However, while it explains why parallel and antiparallel particles are not equivalent, it does not give an explanation for the superiority of the antiparallel case. The reason for this superiority can be found by considering the Hilbert spaces in which these two sets belong. Parallel spins lie in the 3-dimensional subspace of symmetric states, while antiparallel spins span the entire 4-dimensional Hilbert space of spin-1/2 particles. One can thus exploit this additional dimension by tuning the measurement and improving the fidelity.

Interestingly, there is a well-known continuous analog of the spin flipping operation, called phase conjugation. The phase conjugation operator flips the sign of the $\hat{p}$ quadrature while keeping quadrature $\hat{x}$ unchanged. It therefore sends a coherent state centered on $\alpha = \frac{1}{\sqrt{2}}(x + ip)$ to a coherent state centered on $\alpha^* = \frac{1}{\sqrt{2}}(x - ip)$, that is

$$|\alpha\rangle = \left|\frac{x+ip}{\sqrt{2}}\right\rangle \longrightarrow |\alpha^*\rangle = \left|\frac{x-ip}{\sqrt{2}}\right\rangle \tag{5.10}$$

Like the spin flip for spin-1/2 particles, the phase conjugation operator is antiunitary. One can easily check that it does not preserve the commutator of the creation and anihiliation operators $\hat{a}$ and $\hat{a}^\dagger$. If $\hat{b} = \hat{a}^\dagger$ is the resulting mode of the conjugation, the new commutator is

$$\begin{aligned}[\hat{b}, \hat{b}^\dagger] &= [\hat{a}^\dagger, \hat{a}] && (5.11)\\ &= -[\hat{a}, \hat{a}^\dagger] && (5.12)\\ &= -1 && (5.13)\end{aligned}$$

instead of 1 as required by quantum mechanics. Nevertheless, one can always approximate the conjugation of coherent states. Interestingly, the corresponding optimal protocol is *classical* as one has to classically conjugate the result of an optimal heterodyne measurement of the $\hat{x}$ and $\hat{p}$ quadrature [21]. This strategy yields a fidelity of 1/2, which is equal to the fidelity of the optimal discrimination of coherent states with an heterodyne measurement.

5.4 Superiority of Entangled Measurement over All Local Strategies for the Estimation of Product Coherent States

We now turn to the main result of this chapter. Inspired by the impossibility to perfectly conjugate an unknown coherent state, we introduce the following two ensembles: according to a bivariate Gaussian probability distribution $P(\alpha)$, a preparator draws a random complex number α and prepares one of two states, either $|\alpha\rangle\,|\alpha\rangle$ or $|\alpha\rangle\,|\alpha^*\rangle$. Depending on the scenario, he thus prepares one of two ensembles denoted by $\mathcal{E}_{(\alpha,\alpha)} = \{P\,(\alpha), |\alpha\rangle|\alpha\rangle\}$ or $\mathcal{E}_{(\alpha,\alpha^*)} = \{P\,(\alpha), |\alpha\rangle|\alpha^*\rangle\}$. This latter ensemble was first introduced in the context of the optimal phase-conjugation transformation [21]. Alice and Bob, who receive the unknown state, agree on some measurement protocol and must return a state ρ as close as possible to $|\alpha\rangle\!\langle\alpha|$. Their action is called a measure-and-prepare strategy, and the relevant figure of merit, used to estimate the quality of a particular scenario, is therefore the average fidelity. When the state prepared is drawn from $\mathcal{E}_{(\alpha,\alpha^*)}$ for example, this fidelity reads

$$F = \sup_{M_y}\sup_{\rho_y}\sum_y \int \mathrm{d}\alpha\, P(\alpha)\, \langle\alpha|\,\langle\alpha^*|\, E_y\,|\alpha\rangle\,|\alpha^*\rangle\,\langle\alpha|\,\rho_y\,|\alpha\rangle\,, \tag{5.14}$$

where E_y are the positive operators defining the measurement applied by Alice and Bob, $\sum_y E_y = 1$, and ρ_y are states prepared according to the measurement results y.

Our aim is to show that Alice and Bob can better discriminate between the states of $\mathcal{E}_{(\alpha,\alpha^*)}$ when they have access to joint, or global, operations than when they are restricted to LOCC, i.e., we want to prove that $F^*_{Local} < F^*_{Joint}$ when F^*_{Local} and F^*_{Joint} denote the optimal fidelities for local and joint measurement on $|\alpha\rangle|\alpha^*\rangle$ respectively. The proof can be decomposed in three steps. We will first show that the optimal LOCC strategies on $|\alpha\rangle|\alpha^*\rangle$ and $|\alpha\rangle|\alpha\rangle$ yield equal fidelities. We will next prove that the optimal measure-and-prepare strategy on identical copies of $|\alpha\rangle$ is achieved by a local strategy. Note that this result shows that identical copies of a coherent state do not show any nonlocality, in contrast with the situation for identical copies of a qubit. Finally, we will exhibit a joint measurement on phase-conjugate states, conjectured to be optimal, which gives a higher fidelity than the optimal strategy on two identical copies. We will thus prove that

$$F^*_{Local} = F_{Local} = F_{Joint} < F^*_{Joint}\,, \tag{5.15}$$

where F_{Joint} and F^*_{Joint} (F_{Local} and F^*_{Local}) denote the optimal fidelities for global (local) measurements on $|\alpha\rangle|\alpha\rangle$ and $|\alpha\rangle|\alpha^*\rangle$ respectively.

5.4.1 The Optimal Local Fidelity for $|\alpha\rangle\,|\alpha^*\rangle$ and $|\alpha\rangle\,|\alpha\rangle$ Are Equal

First recall that any LOCC strategy consists of a sequence of correlated measurements plus a decision strategy depending on the observed statistics. The relevant probabilities after n round of measurements can be written as

$$Pr(\beta) = \mathrm{Tr}\{(A_\beta \otimes B_\beta)\ |\alpha\rangle\langle\alpha| \otimes |\alpha^*\rangle\langle\alpha^*|\}\,, \tag{5.16}$$

with the positive operators A_β and B_β defined as

$$\begin{aligned} A_\beta &= A^n_{r_n}(r_1, r_2, \ldots, r_{n-1}) \times \ldots \times A^3_{r_3}(r_1, r_2) \times A^1_{r_1} \\ B_\beta &= B^{n-1}_{r_{n-1}}(r_1, r_2, \ldots, r_{n-2}) \times \ldots \times B^2_{r_2}(r_1) \end{aligned}$$

In this expression, r_i is the outcome of the i-th measurement, and the upper index stands for its order in the sequence of measurements. These operators depend on the decision strategy, and are constrained by the measurement normalization conditions

$$\begin{gathered} \sum_{r_i} A^i_{r_i}(r_{i-1}, \ldots, r_1) = 1 \\ \sum_{r_i} B^i_{r_i}(r_{i-1}, \ldots, r_1) = 1 \end{gathered} \tag{5.17}$$

Now, suppose that a particular LOCC strategy is optimal for $|\alpha\rangle|\alpha^*\rangle$ and gives the fidelity F^*_{Local}. We can easily map this optimal strategy into an optimal LOCC strategy for $|\alpha\rangle|\alpha\rangle$. Because the trace of Hermitian operators is invariant under complex conjugation, we note that

$$\mathrm{Tr}\{A_\beta|\alpha\rangle\langle\alpha| \otimes B_\beta|\alpha^*\rangle\langle\alpha^*|\} = \mathrm{Tr}\{A_\beta|\alpha\rangle\langle\alpha| \otimes B^*_\beta|\alpha\rangle\langle\alpha|\},$$

hence replacing B_β by B^*_β one defines another LOCC sequence of measurements that achieves the same fidelity F^*_{Local} for $|\alpha\rangle|\alpha\rangle$, i.e. $F^*_{Local} = F_{Local}$.

5.4.2 The Optimal Measure-and-Prepare Strategy on $|\alpha\rangle|\alpha\rangle$ is Local

Next, let us prove that the optimal measure-and-prepare strategy on $|\alpha\rangle|\alpha\rangle$ is a local strategy, i.e., $F_{Joint} = F_{Local}$. We note that this result is already known for a distribution of infinite width [95], using the variances of the estimated quadratures as a figure of merit. Here, however, we prove a much more powerful result: we consider the realistic case of finite distributions, and do not make any assumption on the measurement nor the reconstruction. Actually, we prove the more general result that the optimal measure-and-prepare strategy for the discrimination of N copies of a coherent state distributed according to a Gaussian of variance $1/\lambda$ yields a fidelity F^N satisfying

$$F^N \leq \frac{N+\lambda}{N+\lambda+1}. \tag{5.18}$$

This upper bound is exactly the fidelity achieved by N independent heterodyne measurements and preparation of a coherent state centered on $\frac{1}{N+\lambda}\sum_{i=1}^{N}\alpha_i$ (with α_i being the result of the i-th measurement), hence the optimal strategy is local.

Before we carry on with proving this statement, we may reformulate and simplify the problem. The first simplification comes from noting that without loss of generality, we can restrict our optimization to measurements consisting of projectors $|\Phi_y\rangle\langle\Phi_y|$ and preparation of pure states $|\chi_y\rangle$. This is easily seen by noting that we can always decompose the POVM elements as $E_y = \sum_a |m_{y,a}\rangle\langle m_{y,a}|$ and the states as $\rho_y = \sum_b \lambda_{y,b}^2 |r_{y,b}\rangle\langle r_{y,b}|$. Absorbing the redundant parameter a and b into y, and identifying $\lambda_{y,b}\,|m_{y,a}\rangle$ and $|r_{y,a}\rangle$ with $|\Phi_y\rangle$ and $|\chi_y\rangle$ respectively, one can check that the value of the average fidelity does not change while the strategy has the desired properties. For the input states $|\alpha\rangle^{\otimes N}$ distributed with the Gaussian distribution $P(\alpha) = \frac{\lambda}{\pi}\exp\left[-\lambda|\alpha|^2\right]$, the fidelity we want to optimize therefore reads

$$F = \sum_y \int \mathrm{d}\alpha\ P(\alpha)|\langle\alpha^{\otimes N}|\Phi_y\rangle|^2|\langle\alpha|\chi_y\rangle|^2. \tag{5.19}$$

We can further simplify the problem by noting that the N modes in state $|\alpha\rangle^{\otimes N}$ can be concentrated into one single mode in state $|\sqrt{N}\alpha\rangle$ by mean of beam splitters. This operation is unitary and completely reversible, hence will not change the fidelity. We write

$$F = \sum_y \int \mathrm{d}\alpha P(\alpha)|\langle\sqrt{N}\alpha|\phi_y\rangle|^2|\langle\alpha|\chi_y\rangle|^2\,. \tag{5.20}$$

This expression can be bounded and rewritten more compactly as

$$F_{max} \leq \sup_{\phi_y, \chi_y} \sum_y \langle \chi_y | A_{\phi_y} | \chi_y \rangle \tag{5.21}$$

$$= \sup_{\phi_y} \sum_y \| A_{\phi_y} \|_\infty \tag{5.22}$$

after introduction of the operators

$$A_{\phi_y} = \int \mathrm{d}\alpha P(\alpha) | \langle \sqrt{N} \alpha | \phi_y \rangle |^2 | \alpha \rangle \langle \alpha | \tag{5.23}$$

The last equality (5.22) is trivial as it is indeed best to prepare the eigenstate of A_{ϕ_y} associated to the largest eigenvalue for a given outcome y.

We can now turn to the core of the optimization. The method exploits a trick introduced in the context of the additivity of output purities of bosonic channels [48]. This trick was later used in [58] to calculate the optimal fidelity of all measure-and-prepare strategies on a single copy of a coherent state $|\alpha\rangle$ distributed according to $P(\alpha)$. First, we prove the following theorem for the operator A_{ϕ_y}:

Theorem 5.4.1 *For all states $|\phi\rangle$ and all p-norms $\|A_\phi\|_p = (\mathrm{Tr}\{|A_\phi|^p\})^{1/p}$,*

$$\|A_\phi\|_p \leq \frac{N+\lambda}{[(N+\lambda+1)^p - 1]^{1/p}} \|A_\phi\|_1 \,. \tag{5.24}$$

Proof The properties of the Trace allow us to write

$$\begin{aligned} \|A_\phi\|_p^p = \mathrm{Tr}\{A_\phi^p\} = & \iint \mathrm{d}\alpha_1 \ldots \mathrm{d}\alpha_p \, P(\alpha_1) \ldots P(\alpha_p) \\ & \times |\langle \phi | \sqrt{N} \alpha_1 \rangle|^2 \ldots |\langle \phi | \sqrt{N} \alpha_p \rangle|^2 \\ & \times \mathrm{Tr}\{ |\alpha_1\rangle \langle \alpha_1 | \alpha_2 \rangle \ldots \langle \alpha_{p-1} | \alpha_p \rangle \langle \alpha_p | \} \\ = & \, \mathrm{Tr}\{ |\phi\rangle\langle\phi|^{\otimes p} B \}, \end{aligned} \tag{5.25}$$

$$\|A_\phi\|_1^p = \mathrm{Tr}\{A_\phi\}^p = \mathrm{Tr}\{ |\phi\rangle\langle\phi|^{\otimes p} C \}, \tag{5.26}$$

where we have defined the operators B and C has

$$\begin{aligned} B = & \iint \mathrm{d}\alpha_1 \ldots \mathrm{d}\alpha_p \, P(\alpha_1) \ldots P(\alpha_p) \langle \alpha_1 | \alpha_2 \rangle \ldots \langle \alpha_p | \alpha_1 \rangle \\ & \times |\sqrt{N}\alpha_1\rangle\langle\sqrt{N}\alpha_1| \otimes \ldots \otimes |\sqrt{N}\alpha_p\rangle\langle\sqrt{N}\alpha_p| \,, \\ C = & \bigotimes_{i=1}^{p} \int d\alpha_i P(\alpha_i) |\sqrt{N}\alpha_i\rangle\langle\sqrt{N}\alpha_i| \,. \end{aligned} \tag{5.27}$$

These two operators commute and can be diagonalized in the same basis. A unitary transformation turns them into tensor product of unnormalized thermal states, which are diagonal in the corresponding Fock state basis. One finds

$$B = \frac{\lambda^p}{(N+\lambda+1)^p - 1} \bigotimes_{i=1}^{p} \sum_{n_i=0}^{\infty} \left(\frac{N}{N+\lambda+1-d_i}\right)^{n_i} |n_i\rangle\langle n_i|$$

$$C = \frac{\lambda^p}{(N+\lambda)^p} \bigotimes_{i=1}^{p} \sum_{n_i=0}^{\infty} \left(\frac{N}{N+\lambda}\right)^{n_i} |n_i\rangle\langle n_i| \,, \tag{5.28}$$

where d_i are the eigenvalues of a unitary matrix with $|d_i| = 1$. Next we express the product state $|\phi\rangle^{\otimes p}$ in this Fock state basis, i.e., $|\phi\rangle^{\otimes p} = \sum_{\{n_j\}} c_{\{n_j\}} |n_1, \ldots, n_p\rangle$, and introduce this expression into the traces (5.25) and (5.26). Remembering that $\mathrm{Tr}\{|\phi\rangle\langle\phi|^{\otimes p} B\} \geq 0$, one finds that

$$\begin{aligned}
\mathrm{Tr}\{|\phi\rangle\langle\phi|^{\otimes p} B\} &= \frac{\lambda^p}{(N+\lambda+1)^p - 1} \times \left| \sum_{\{n_j\}=0}^{\infty} |c_{n_1,\ldots,n_p}|^2 \prod_{i=1}^{p} \left(\frac{N}{N+\lambda+1-d_i}\right)^{n_i} \right| \\
&\leq \frac{\lambda^p}{(N+\lambda+1)^p - 1} \times \sum_{\{n_j\}=0}^{\infty} |c_{n_1,\ldots,n_p}|^2 \prod_{i=1}^{p} \left|\frac{N}{N+\lambda+1-d_i}\right|^{n_i} \\
&\leq \frac{\lambda^p}{(N+\lambda+1)^p - 1} \times \sum_{\{n_j\}=0}^{\infty} |c_{n_1,\ldots,n_p}|^2 \prod_{i=1}^{p} \left(\frac{N}{N+\lambda}\right)^{n_i} \\
&\leq \frac{(N+\lambda)^p}{(N+\lambda+1)^p - 1} \times \mathrm{Tr}\{|\phi\rangle\langle\phi|^{\otimes p} C\}
\end{aligned} \tag{5.29}$$

The p-th root of this expression directly gives relation (5.24). ■

Proving Eq. (5.18) is now really easy. First consider the limiting case $p \to \infty$ of Theorem 5.4.1. Next sum over all possible results y and remember that the measurement normalization condition $\sum_y |\phi_y\rangle\langle\phi_y| = 1$ implies $\sum_y \|A_{\phi_y}\|_1 = 1$.

5.4.3 A Better Measurement on Phase-Conjugate Coherent States

To conclude this section, let us prove the existence of a joint measurement on phase-conjugate coherent states that yields a higher fidelity than (5.18) for $N = 2$. One such measurement is already known and was introduced in [21], where it is shown that the $|\alpha\rangle|\alpha^*\rangle$ encoding outperforms $|\alpha\rangle|\alpha\rangle$ in the case $\lambda = 0$. The measurement strategy is the following. First, the two modes are sent on a Beam Splitter (BS), which outputs two coherent states displaced along the x and p axis respectively, i.e.,

$$|\alpha\rangle|\alpha^*\rangle \to |x_\alpha\rangle|ip_\alpha\rangle, \tag{5.30}$$

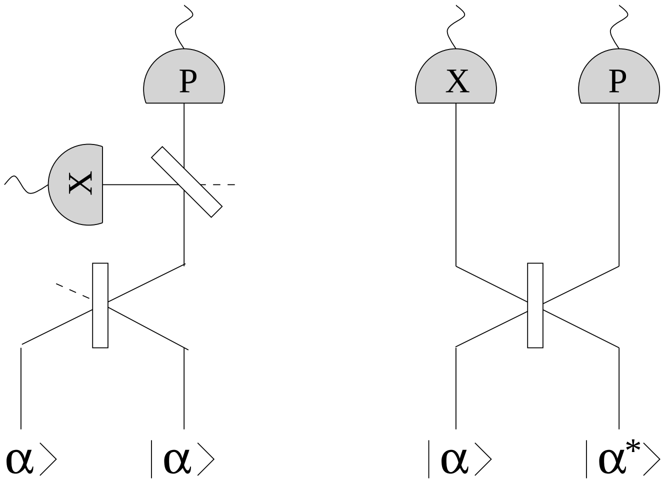

Figure 5.2: *Measurement scheme of the optimal measure-and-prepare strategy for the discrimination of* $|\alpha\rangle\,|\alpha\rangle$ *(left) and* $|\alpha\rangle\,|\alpha^*\rangle$ *(right).*

Recall that $\alpha = (x_\alpha + ip_\alpha)/\sqrt{2}$. Next, the appropriate quadratures are measured on the two output ports, and some state $|f_\beta\rangle$ is reconstructed according to the measurement outcomes (see Fig. 5.2 right).

That this strategy outperforms the optimal measurement on identical copies has an intuitive explanation. Suppose we apply this BS strategy to the $|\alpha\rangle|\alpha\rangle$ case. Then, the two modes are concentrated on one output port, so that only heterodyning can extract information about x and p simultaneously, that is, we need to combine the state with vacuum at another BS, introducing extra noise. Nevertheless, according to the previous section, this strategy is optimal. Applying this same strategy to the $|\alpha\rangle|\alpha^*\rangle$ state, we can directly access the entire information by homodyning each of the two output modes of the BS. Since we do not introduce vacuum in this setup while detecting the same mean signal, we have less noise and can therefore expect a greater fidelity (see Fig. 5.2).

In order to calculate this fidelity and easily compare it with Eq. (5.18), suppose that we have at our disposal N coherent states made of $N/2$ pairs $|\alpha\rangle|\alpha^*\rangle$, or equivalently one pair $|\sqrt{N/2}\;\alpha\rangle|\sqrt{N/2}\;\alpha^*\rangle$. The corresponding fidelity reads

$$F_{BS}^{*N} = \iint \mathrm{d}x\;\mathrm{d}p\;\mathrm{d}\alpha P(\alpha)\;P\big(x,p|x_\alpha,p_\alpha\big)|\langle f_\beta|\alpha\rangle|^2\,,$$

where

$$P(x,p|x_\alpha,p_\alpha) = \frac{1}{\pi}\exp\big[-(x-\sqrt{N}x_\alpha)^2-(p-\sqrt{N}p_\alpha)^2\big] \qquad (5.31)$$

is the probability to measure (x,p) by homodyning on $|\sqrt{N/2}\,x_\alpha\rangle|\sqrt{N/2}\,p_\alpha\rangle$. Introducing $\beta=(x+ip)/\sqrt{2}$ and the positive semi-definite Hermitian operator

$$\hat{O}_\beta=\int \mathrm{d}\alpha\ \exp\big[-(2N+\lambda)|\alpha|^2+4\sqrt{N}\Re(\beta^*\alpha)\big]\,|\alpha\rangle\langle\alpha| \tag{5.32}$$

the fidelity simplifies to

$$F^{*N}_{BS}=2\frac{\lambda}{\pi^2}\int \mathrm{d}\beta e^{-2|\beta|^2}\langle f_\beta|\hat{O}_\beta|f_\beta\rangle\,. \tag{5.33}$$

Optimization of this fidelity with respect to the reconstructed state boils down to finding the largest eigenvalue $\mu_1(\hat{O}_\beta)$ of this operator $\hat{O}_\beta$. To calculate this value, consider the following positive operator and its expansion in the Fock state basis [15]

$$\hat{P}=\int \mathrm{d}\alpha e^{-(2N+\lambda)|\alpha|^2}|\alpha\rangle\langle\alpha| \tag{5.34}$$

$$=\pi\sum_{n=0}^{\infty}(2N+\lambda+1)^{-n-1}|n\rangle\langle n|\,. \tag{5.35}$$

Clearly

$$\mu_1(\hat{P})=\frac{\pi}{2N+\lambda+1}\,. \tag{5.36}$$

Now consider the displaced operator

$$\begin{aligned}\hat{Q}_\beta&=\hat{D}\left(\frac{2\sqrt{N}}{2N+\lambda}\beta\right)\,\hat{P}\,\hat{D}^\dagger\left(\frac{2\sqrt{N}}{2N+\lambda}\beta\right)\\&=\exp[-\frac{4N}{2N+\lambda}|\beta|^2]\,\hat{O}_\beta\,,\end{aligned} \tag{5.37}$$

where $\hat{D}$ is the displacement operator introduced in 2.2.3, from which we deduce

$$\langle f_\beta|\hat{O}_\beta|f_\beta\rangle\leq\exp[+\frac{4N}{2N+\lambda}|\beta|^2]\,\frac{\pi}{2N+\lambda+1}\,. \tag{5.38}$$

Introducing this value in the fidelity, one finds after integration

$$F^{*N}_{BS}\leq\frac{2N+\lambda}{2N+\lambda+1}\,. \tag{5.39}$$

Equality is achieved and the fidelity is optimized by reconstructing the state

$$|f_\beta\rangle=\hat{D}\left(\frac{2\sqrt{N}}{2N+\lambda}\beta\right)|0\rangle=|\frac{2\sqrt{N}}{2N+\lambda}\beta\rangle. \tag{5.40}$$

Clearly, (5.39) is larger than (5.18) for any N. Because the optimal global strategy can only improve this fidelity, we conclude that $F^N < F^{*N}_{BS} \leq F^{*N}$, where F^{*N} is the optimal fidelity of a global strategy on $N/2$ phase-conjugate pairs[2].

Interestingly, $F^{*N}_{BS} = F^{2N}$, that is, this global strategy on $|\alpha\rangle|\alpha^*\rangle$ is exactly as efficient as the optimal strategy on 4 copies of the coherent state $|\alpha\rangle$. Again, this has an intuitive explanation. Consider the input state $|\alpha\rangle^{\otimes 4}$. It can be concentrated using two BS, namely, $|\alpha\rangle^{\otimes 4} \to |\sqrt{2}\alpha\rangle^{\otimes 2}$. Because dual homodyning on $|\sqrt{2}\alpha\rangle|\sqrt{2}\alpha\rangle$ or $|x_\alpha\rangle|p_\alpha\rangle$ gives identical statistics, the corresponding fidelities are equal.

5.5 Experimental Demonstration

Remarkably, the measurement strategies described in the previous sections can be implemented experimentaly. It follows that the nonlocality without squeezing exhibited by the ensemble $\{P(\alpha), |\alpha\rangle|\alpha^*\rangle\}$ can be demonstrated in the lab. The experiment was performed in 2006 at the Technical University of Denmark in collaboration with the group of Professor Ulrik L. Andersen.

5.5.1 Sideband Encoding

In the following experiment, the information will be encoded at a frequency sideband of a carrier frequency. In addition to a high degree of purity, this sideband encoding also holds the advantage of allowing for easy low-voltage control of the amplitudes via simple electro-optic modulators operating at the sideband frequency [1].

The sideband model works as follows. The field mode $\hat{a}$ under consideration is decomposed into a bright carrier component at frequency ω and two sideband modes placed symmetrically around the carrier at frequencies $\omega + \Omega$ and $\omega - \Omega$ respectively, i.e.,

$$\hat{a} = \alpha \exp[i\omega t] + \delta\hat{a}_+ \exp[i(\omega + \Omega)t] + \delta\hat{a}_- \exp[i(\omega - \Omega)t]\,, \tag{5.41}$$

where the amplitude of the carrier α is assumed to be real, and $\delta\hat{a}_\pm$ are the single-mode field operators at the frequencies $\omega \pm \Omega$. It follows that the only significant contribution to the signal at frequency Ω comes from the beating of these three modes. In particular, if we perform a direct photodetection of mode $\hat{a}$

$$\begin{aligned}\hat{n} &= \hat{a}^\dagger \hat{a} \\ &= \alpha^2 + \alpha(\delta\hat{a}_+ \exp[i\Omega t] + \delta\hat{a}_- \exp[-i\Omega t] + \delta\hat{a}_+^\dagger \exp[-i\Omega t] + \delta\hat{a}_-^\dagger \exp[i\Omega t]) \\ &\qquad + (|\delta\hat{a}_+|^2 + |\delta\hat{a}_-|^2 + 2\Re(\delta\hat{a}_+\delta\hat{a}_-^\dagger \exp[2i\Omega t])),\end{aligned} \tag{5.42}$$

[2] Note that if we consider the optimal measurement of $|\alpha\rangle^N |\alpha^*\rangle^N$ with respect to the noise variance, instead of the fidelity, this strategy can be shown to be optimal [21].

a spectral analysis of the resultant photocurrent at the sideband frequency Ω will give information about the amplitude quadrature

$$\delta\hat{X}_a^{\Omega} = \delta\hat{a}_+ \exp[i\Omega t] + \delta\hat{a}_- \exp[-i\Omega t] + \delta\hat{a}_+^{\dagger} \exp[-i\Omega t] + \delta\hat{a}_-^{\dagger} \exp[i\Omega t]. \tag{5.43}$$

Note that $\delta\hat{X}_a^{\Omega}$ contains contributions from both sidebands. As the characterization of an optical CV system requires a pair of canonically conjugated variables, one may also define a phase quadrature by introducing a phase shift of $\pi/2$ between the carrier and the sidebands

$$\hat{a} = \alpha \exp[i\omega t + \pi/2] + \delta\hat{a}_+ \exp[i(\omega + \Omega)t] + \delta\hat{a}_- \exp[i(\omega - \Omega)t]. \tag{5.44}$$

Direct photodetection will then provide information about the phase quadrature

$$\delta\hat{Y}_a^{\Omega} = -\delta\hat{a}_+ \exp[i\Omega t] - \delta\hat{a}_- \exp[-i\Omega t] + \delta\hat{a}_+^{\dagger} \exp[-i\Omega t] + \delta\hat{a}_-^{\dagger} \exp[i\Omega t]. \tag{5.45}$$

5.5.2 The Setup

The laser used in the experiment is a monolithic Nd:YAG laser producing a field at 1064 nm, which is split into two parts and subsequently directed into the coherent state preparation stage (see Fig. 5.3). To ensure that the information is encoded as pure coherent states, the states are assumed to be residing at a radio frequency sideband defined within a certain bandwidth of the laser beam. Note therefore that the two beams are bright although the particular sidebands in question are vacuum states before the encoding. The production of the two phase conjugate coherent states, $|\alpha\rangle$ and $|\alpha^*\rangle$, is then performed by displacing the vacuum sidebands using an amplitude modulator (AM) and a phase modulator (PM) in each arm as shown in Fig. 5.3. The two states are prepared by using the same signal generator, that is by communicating classically correlated information between the two preparation stations. The relative phase shift of π between the phase quadratures was established by adjusting the cable lengths appropriately.

First, the prepared states are characterized by measuring the two copies individually. This is done by successive use of a heterodyne detector yielding information about the amplitude and phase quadratures simultaneously. The coherent state is combined with a phase stabilized auxiliary beam at a 50:50 beam splitter with a $\pi/2$ relative phase shift and balanced intensities. They interfere with a contrast of 99% and the two output beams are detected with high quantum efficiency (95%) photodiodes. Subsequently the photocurrents are subtracted and added which provides information about the phase and amplitude quadratures, respectively. Finally the spectral densities of the quadratures are recorded on a spectrum analyzer. Using the fact

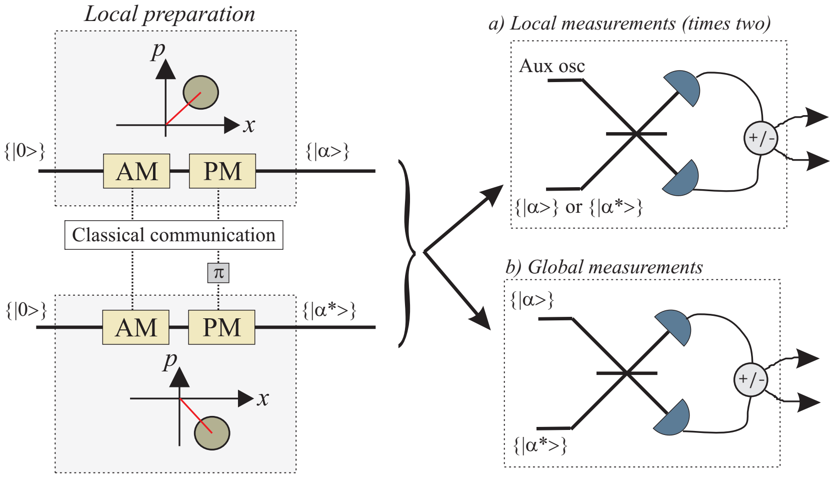

Figure 5.3: *Schematic of the experimental setup. The diagrams show the phase space contours of $|\alpha\rangle$ (upper diagram) and $|\alpha^*\rangle$ (lower diagram). The states are measured using a) a local strategy and b) a joint or global strategy. AM: Amplitude modulator, PM: Phase modulator.*

that the heterodyne detector projects the signal under investigation onto a vacuum state, the spectral densities of the prepared copies is easily infered. Furthermore the measurements have also been corrected to account for the detection losses and electronic dark noise in order to avoid an erroneous underestimation. The inferred results for the spectral densities are shown by the solid horizontal lines in Fig. 5.4.

5.5.3 Local Measurement Strategy

These measurements for characterization of the prepared copies are in fact identical to the measurements associated with an optimal local estimation strategy. However, in contrast to the characterization, for the estimation of unknown coherent states the results are not corrected for detector losses and electronic dark noise. The individual spectral densities for local measurements of $|\alpha\rangle$ and $|\alpha *\rangle$ are shown in column a) and c) of Fig. 5.4. From these measurements the added noise is found to be $\Delta_x = \Delta_p = 1.12 \pm 0.04$ for the amplitude and phase quadratures. Assuming a flat distribution of coherent states, the fidelity is given by

$$F = \frac{2}{\sqrt{(2+\Delta_x)(2+\Delta_p)}} \tag{5.46}$$

and calculated to

$$F_{Local} = 64.0 \pm 1 \tag{5.47}$$

This is close to the theoretical maximum of 2/3.

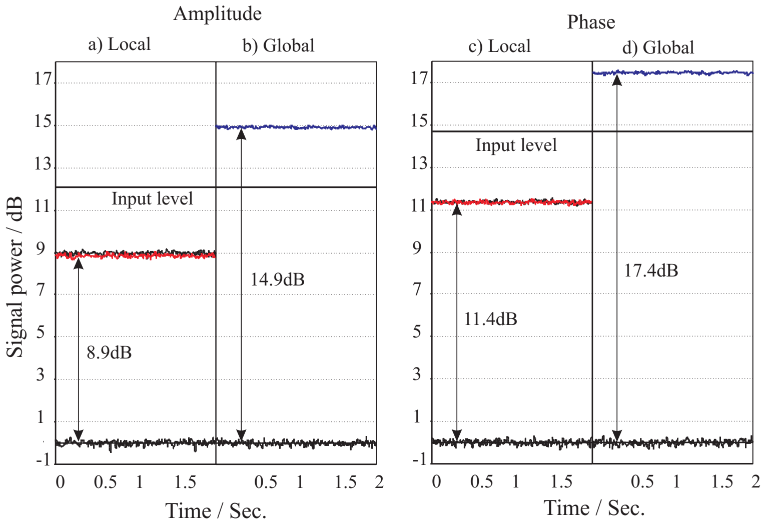

Figure 5.4: *Spectral power densities (normalized to the quantum noise level) of the local and joint strategies. The resolution bandwidth is 100kHz and the video bandwidth is 30Hz.*

5.5.4 Joint Measurement Strategy

Recall that this strategy is to combine the two copies at a 50:50 beam splitter and subsequently measure the amplitude quadrature in one output and the phase quadrature in the other output port of the beam splitter. Such a strategy measures the combinations $\hat{x}_1 + \hat{x}_2$ and $\hat{p}_1 - \hat{p}_2$ where the indices refer to the two input modes. This combination can, however, be accessed using an experimentally simpler approach since the information is encoded onto sidebands of two equally intense bright beams (with the power 60 μW). The two classically correlated copies are carefully mode-matched (∼99%) at a 50:50 beam splitter and actively locked to have balanced intensities at the outputs of the beam splitter. Directly measuring the two outputs yield the quadrature combinations $\hat{i}_1 = (\hat{x}_1 + \hat{x}_2 + \hat{p}_1 - \hat{p}_2)/2$ and $\hat{i}_2 = (\hat{x}_1 + \hat{x}_2 - \hat{p}_1 + \hat{p}_2)/2$, and by adding and subtracting these two contributions we obtain the required combinations $\hat{x}_1 + \hat{x}_2$ and $\hat{p}_1 - \hat{p}_2$. The spectral densities of these measurements are shown in column b) and d) of Fig. 5.4.

The upper traces in Fig. 5.4 correspond to the coherent amplitudes of the input states and of the joint estimates, whereas the lower traces are the powers associated with the noise levels, all of which are at the shot noise level. The signal-to-noise ratio of the estimate is clearly larger than that of the prepared states; the coherent amplitudes of the amplitude and phase quadratures are increased by 3.0 dB and 2.9 dB, respectively, which effectively correspond to noise equivalent power of $\Delta_x = 0.51 \pm 0.02$ and $\Delta_p = 0.52 \pm 0.02$ shot noise units. Using Eq. (5.46), the fidelity is calculated to be

$$F^*_{BS} = 79.5 \pm 0.7 \tag{5.48}$$

thus clearly surpassing the classical local fidelity of 2/3 and close to the theoretical value 4/5.

5.6 Conclusion

In this chapter, we have successfuly investigated a peculiar form of nonlocality which arises when classically correlated product states are measured with an entangled measurement. In particular, we have proven that a set of phase-conjugated pairs of coherent states can be better discriminated with an entangled measurement than with any sequence of local operations and classical communications. This is, to our knowledge, the first example of such a nonlocal behavior based on continuous variables.

Remarkably, the relative simplicity of the preparation and manipulation of coherent states enabled an experimental demonstration of this peculiar property based on the side-band encoding of a modulated laser beam. Because our experimental setup is free of squeezing, we called this nonlocal property of continuous variable product states Nonlocality Without Squeezing. Like nonlocality without entanglement, this new form of nonlocality should not be understood as an incompatibility with local-hidden-variable models (unlike the case of Bell tests), but rather as the manifestation of an inherently global property. We note that the performed experiment nicely illustrates the power of continuous variables when it comes to physically verifying theoretical ideas. Although Peres and Wootters conjectured the existence of a similar nonlocal behavior for qubits in 1991, the superior discrimination of product states of two photons via entangled measurements was verified experimentally only very recently [88, 65].

To conclude this chapter, it is interesting to make a parallel between the different relations proved in Section 5.4 for coherent states, and their counterpart for spin-1/2 particles. For discrete and continuous variables respectively, these relations read

$$\begin{array}{c} F^{\perp}_{Local} = F^{\uparrow\uparrow}_{Local} < F^{\uparrow\uparrow}_{Joint} < F^{\perp}_{Joint} \\ F^{*}_{Local} = F_{Local} = F_{Joint} < F^{*}_{Joint} \end{array}$$

Surprisingly, these two chains of relations are not equivalent. The main difference lies in whether a joint strategy is necessary to optimally discriminate pairs of identical states. While for qubits the optimal strategy is joint and entangled as demonstrated by Massar and Popescu, for coherent states the optimal strategy is local and classical as demonstrated by Eq. (5.18). In a sense, one can thus say that pairs of identical coherent states do not show any quantumness. However, introduce a more powerful correlation, such as phase conjugation, and the quantumness of product coherent states is strikingly revealed again. This is a nice illustration of the particular nature of coherent states that lie at the border of the classical and the quantum world, and justifies their appellation of *quasi-classical* states.

6 Gaussian Error Correction

6.1 Introduction

Quantum information processing based on continuous variables offers many interesting possibilities. One can for example use continuous variables to investigate fundamental issues of the quantum theory. This was the focus of the first part of this dissertation. In Chapters 4 and 5 for example, we considered two special nonlocal effects known for discrete variables and proved their existence in the continuous regime. Interestingly enough, continuous variables are not just a mere equivalent of discrete variables; they are often much easier to implement. This is particularly true when the quadratures of the electromagnetic field are used to carry the information. In Chapter 3 we took advantage of optical continuous variables to derive experimentally feasible loophole free Bell tests. However, the benefit of this experimental simplicity was made strikingly obvious with the nonlocality without squeezing addressed in Chapter 5. While the Peres-Wootters nonlocality waited 14 years for an experimental demonstration, our continuous counterpart could be tested almost immediately!

Interestingly, the reason of this latter success can be summed up in a single word: *Gaussian.* Among all the operations one can apply to an optical CV state, a large class of operations, known as the Gaussian operations, maintain the Gaussian character of Gaussian states. Remarkably, they can all be implemented by combining passive and active linear optical components such as beam splitters, phase shifters and squeezers, supplemented with homodyne detection followed by classical communications, i.e., all elements that are, up to some degree of accuracy, readily accessible in today's optical labs! Recalling that basic Gaussian states can be easily generated with a laser, one notes that Gaussian protocols (Gaussian states + Gaussian operations) are approximately those that can be relatively easily implemented in an optical lab. Indeed, the experiment described in Chapter 5, which involved two coherent states, a beam splitter and homodyne detection, is nothing but a Gaussian protocol. This combination of Gaussian states and Gaussian operations has recently enabled many important quantum information primitives such as teleportation [43], quantum key distribution [57] and quantum cloning [1].

However, manipulating Gaussian states with Gaussian operations has also some theoretical limitations. Probably the most significant is the known impossibility to distill entanglement from Gaussian entangled states with local Gaussian operations and classical communications [35, 39, 46]. It follows that some important quantum primitives, such as quantum repeaters for example, cannot be implemented within the easily accessible Gaussian regime but require the use of hard to achieve non-Gaussian ressources like photon-subtracted states [81] or de-gaussification operations [36]. One may therefore question what are the other tasks central to QIS that are not achievable with Gaussian operations only. Identifying these limitations of the Gaussian regime is of great importance as it underpins the use of optical continuous variables in short term quantum communication and quantum information protocols.

In the remaining part of this dissertation, we will consider one such important primitive called error correction. Clearly, the ability to transmit, store and manipulate quantum information without errors is prerequisite for the realization of most quantum information protocols. However, errors are inherent to any realistic implementation, and Gaussian errors in particular model many physical processes such as the transmission of light through a lossy optical fiber. In this chapter, we will thus try to answer the following question: Can we detect and correct Gaussian errors with Gaussian operations only?

6.2 Preliminaries

Gaussian Error Correction

Building a quantum computer or a quantum communication network is a difficult task. The main obstacle is the coupling of the information carrier with the environment. These effects, known as decoherence or noise, rapidly destroy quantum superpositions and cause information losses. Error correction is therefore a protocol used to suppress and undo the effect of these errors. In classical information theory, the main tool is redundancy

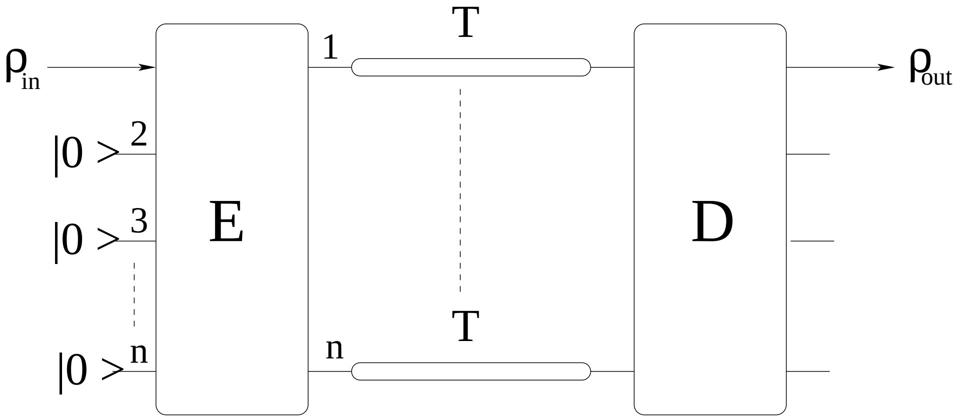

Figure 6.1: *Schematic of a Gaussian error correction protocol $G(n, E, D)$ for a Gaussian channel T. E and D are n-mode unitary Gaussian operations.*

as one can copy the information and transmit a sufficiently large number of copies to enable successful majority voting. In quantum information theory, however, information cannot be copied (see Sec. 2.1.2) but states can be entangled. By cleverly distributing the information over a multipartite entangled state, one can send quantum information "nonlocaly" and protect it from local errors.

Error correction is generally achieved in two steps. An encoding step where the input state is converted into a multipartite entangled state, and a decoding step where the output state is extracted from the received noisy entangled state. In this chapter, we will particularly focus on Gaussian error correction. This means that the coupling to the environment, known as the channel, the encoding and the decoding steps are modeled by Gaussian operations. In particular, we define a Gaussian Error Correcting Code (GECC) for the Gaussian channel T as a finite number $n-1$ of ancillaes in a known quantum state $|0\rangle$, two Gaussian unitary operations E and D acting on n modes, and n use of the channel T as depicted in Fig. 6.1. We denote this code by $G(n, E, D)$ to emphasize its characteristics, and note that its overall effect is to turn the Gaussian channel T with matrices M and N into the Gaussian channel T_{GC} with matrices M_{GC} and N_{GC}.

The Gaussian Formalism

As already mentionned in Chapter 2, Gaussian states and Gaussian operations are not only (relatively) simple to manipulate experimentally, they also benefit from an attractive mathematical framework known as the Gaussian formalism. This formalism is essential for the following sections, hence we briefly recall some of its main elements.

A single-mode Gaussian state ρ with vector of quadratures $\hat{r} = (\hat{x}, \hat{p})$ is fully characterized by its vector of mean values $d_j = \langle \hat{r}_j \rangle$ and the 2×2 covariance matrix $\gamma_{ij} = \langle \hat{r}_i \hat{r}_j + \hat{r}_j \hat{r}_i \rangle - 2 d_i d_j$.

A Gaussian channel, on the other hand, is a trace-preserving completely positive map

$$T : \rho_{in} \rightarrow \rho_{out} = T[\rho_{in}] \, , \tag{6.1}$$

which transforms Gaussian states into Gaussian states. It is completely characterized by its action on d and γ, and at the level of covariance matrices, the channel is represented by two matrices M and N

$$\gamma \rightarrow M \gamma M^T + N \, , \tag{6.2}$$

where M is real and N is real and symmetric. In this chapter, we will only consider single-mode channels. In such cases, the condition of complete positivity (2.97) simplifies to

$$\det N \geq (\det M - 1)^2 , \tag{6.3}$$

i.e., any map $\gamma \rightarrow M \gamma M^T$ can be approximately realized provided that sufficient noise is added.

6.3 On the Impossibility of Gaussian Error Correction

The main result of this chapter takes the form of a no-go theorem. More precisely, we will prove in the following section that a new intrinsic property of Gaussian channels, named the *Entanglement Degradation*, cannot be reduced by Gaussian operations only. Although quite simple, the proof of our theorem is greatly simplified by introducing two convenient lemmas.

6.3.1 Error Correction and Entanglement Distillation

For discrete systems, there is an interesting known connection between error correction and entanglement distillation. In particular, it is proven in [13] that every error correcting code is equivalent to a one-way entanglement distillation protocol. The link between these two protocols is provided by quantum teleportation (see Sec. 2.1.3). Distillation means that one can use the resulting maximally entangled state to perfectly teleport an unknown input state, i.e., effectively accomplishing error correction. Error correction means that one can perfectly distribute a maximally entangled state, i.e., effectively realizing entanglement distillation.

For continuous variables on the other hand, the relation is not as straightforward. The main reason being that CV maximally entangled states are an

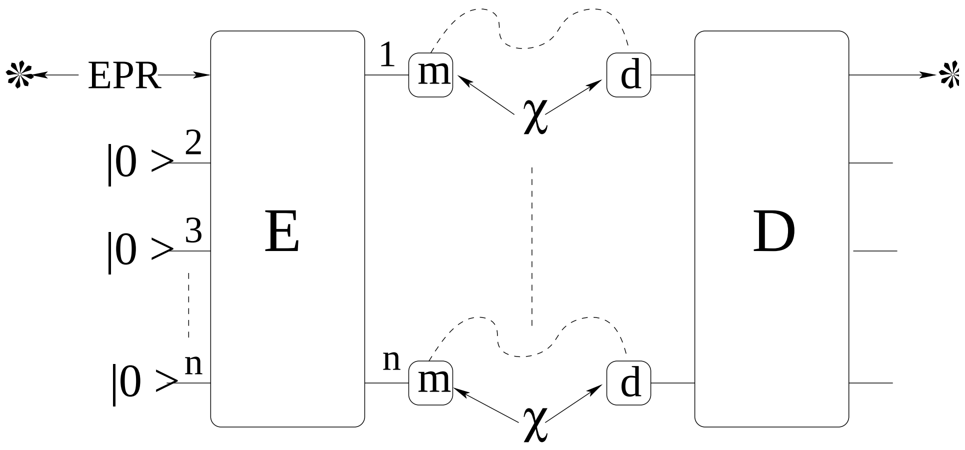

Figure 6.2: *From a GECC to a Gaussian Entanglement Distillation protocol. m: Bell measurement, d: displacement*

unphysical ressource, hence one needs to quantify the entanglement of the physical states involved in the distillation process. Nevertheless, one can use a similar argument to prove the following lemma:

Lemma 6.3.1 *If $|\phi_r\rangle$ is a two-mode squeezed vacuum with squeezing parameter r, the Gaussian error correcting code $G(n, E, D)$ transforming the Gaussian channel T into the Gaussian channel T_{GC} is equivalent to a one-way protocol transforming n copies of the state $\chi = \lim_{r\to\infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ into one copy of the state $\rho_d = \lim_{r\to\infty} \mathbb{1} \otimes T_{GC}(|\phi_r\rangle\langle\phi_r|)$ by local Gaussian operations only.*

Proof Our main tool is the well-known isomorphism between CP maps and positive operators [64]. In particular, to any Gaussian CP map T acting on a one mode Hilbert space $\mathcal{H}$, we can associate a Gaussian positive operator χ on $\mathcal{H} \otimes \mathcal{H}$ defined as

$$\chi = \lim_{r\to\infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|), \tag{6.4}$$

where

$$|\phi_r\rangle = \sqrt{1 - \tanh^2(r)} \sum_n \tanh^n(r)|n, n\rangle$$

is a two mode squeezed vacuum. Acting with map T on a Gaussian state ρ can now be seen as teleporting ρ through the quantum gate defined by the ressource state χ [46]. It follows that the n uses of the channel involved in the GECC can be replaced by n teleportations through the quantum channel χ. Note that the operations involved in the teleportation, that is Bell measurement, one-way classical communications and displacement maintain the overall Gaussian character of the scheme. If the input of the GECC is now chosen to be one-half of a two mode squeezed vacuum, the GECC is turned into a one-way local Gaussian protocol which transforms n copies of the (Gaussian) state χ into one copy of the Gaussian state $\rho_d = \mathbb{1} \otimes T_{GC}(|\phi_r\rangle\langle\phi_r|)$. The protocol is the following: Alice prepares the state $|\phi_r\rangle$ and $n-1$ ancillae, then applies the Gaussian operation E on the ancillae and one half of the entangled state. She next performs n Bell measurements using the n copies of the ressource state χ, and communicates the results to Bob. Bob displaces his n shares of the ressource state accordingly, and applies the Gaussian operation D. Alice and Bob now share one copy of the state ρ_d. In particular, if Alice prepares the maximally entangled state $\lim_{r\to\infty} |\phi_r\rangle\langle\phi_r|$, the state they share is $\rho_d = \lim_{r\to\infty} \mathbb{1} \otimes T_{GC}(|\phi_r\rangle\langle\phi_r|)$. ■

6.3.2 Entanglement Degradation of a Channel

The preceding lemma does not say anything about the entanglement of the ressource sate χ and the *transformed* state ρ_d. This is the reason why we referred to a one-way local protocol and not to a one-way entanglement distillation protocol. For the protocol to truly distill entanglement, one has to show that it increases the entanglement, i.e., that $E[\rho_d] > E[\chi]$ for some entanglement measure E. This is addressed in the following lemma.

Lemma 6.3.2 *Given a Gaussian channel T of matrices M and N, acting on one-half of the maximally entangled state $\rho_{in} = \lim_{r\to\infty} |\phi_r\rangle\langle\phi_r|$, the entanglement of the output state $\rho_{out} = \lim_{r\to\infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ is completely characterized by the Entanglement Degradation of the channel*

$$E_D[T] = \min\{\frac{\det N}{(1+\det M)^2}, 1\}. \tag{6.5}$$

In particular, the logarithmic negativity of ρ_{out} is the decreasing function of E_D

$$E_N[\rho_{out}] = -\frac{1}{2}\log E_D[T]. \tag{6.6}$$

Proof Let us first assume that $\det M \geq 0$. Without restriction, we can choose $M = \eta\mathbb{1}$ with η real. This is so because the channel can always be transformed into another Gaussian channel with $M' = SVMU$ and $N' = SVNV^TS$ by adding two phase shifts of symplectic matrices U and V at the input and output respectively, followed by a single mode squeezer of matrix S at the end. Note that these operations are local, hence they do not change the entanglement properties of the channel. By the Singular Value Decomposition, U and V can be chosen such that VMU is diagonal, and tuning the squeezing appropriately will make M' proportional to the identity, i.e., $M' = \eta\mathbb{1}$. Importantly, the determinant of symplectic matrices being equal to unity, we have $\det M' = \det M$ and $\det N' = \det N$.

Let us now consider the action of the channel T on one-half of a two-mode squeezed vacuum $|\phi_r\rangle\langle\phi_r|$ with covariance matrix $\gamma_{in}^{(r)}$. Recall that covariance matrices of two-mode Gaussian states can be decomposed in four 2×2 blocks. Introducing this decomposition, we easily find the input and output covariance matrices to be

$$\gamma_{in}^{(r)} = \begin{pmatrix} A_r & C_r \\ C_r & A_r \end{pmatrix} \longrightarrow \gamma_{out}^{(r)} = \begin{pmatrix} A_r & \eta C_r \\ \eta C_r & \eta^2 A_r + N \end{pmatrix} \tag{6.7}$$

with

$$A_r = \cosh(2r) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad C_r = \sinh(2r) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Interestingly, the entanglement of a two-mode Gaussian state ρ with covariance matrix

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

is fully characterized by the smallest symplectic eigenvalue ν_- of the partial transposed state $\tilde{\rho}$ [20]. In particular, the logarithmic negativity is the decreasing function

$$E_N = \max\{0, -\log \nu_-\}, \tag{6.8}$$

and ν_- can be calculated from γ according to

$$2\nu_-^2 = \tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4\det\gamma}\,, \tag{6.9}$$

where

$$\tilde{\Delta} = \det A + \det C - 2\det B. \tag{6.10}$$

For the output state $\rho_{out}^{(r)} = \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$ of covariance matrix $\gamma_{out}^{(r)}$, the two symplectic invariants $\tilde{\Delta}$ and $\det \gamma_{out}^{(r)}$ read

$$\begin{aligned}\tilde{\Delta} &= \det A_r + \det(\eta^2 A_r + N) - 2\det \eta C_r \\ &= \cosh^2(2r) + (\eta^4 \cosh^2(2r) + \eta^2 \cosh(2r) \operatorname{Tr} N + \det N) \\ &+ 2\eta^2 \sinh^2(2r) \\ &= \cosh^2(2r)(1+\eta^2)^2 + \cosh(2r)\eta^2 \operatorname{Tr} N + (\det N - 2\eta^2) \end{aligned} \tag{6.11}$$

$$\begin{aligned}\det \gamma_{out}^{(r)} &= \det A_r \det(\eta^2 A_r + N - \eta^2 C_r A_r^{-1} C_r) \\ &= \cosh^2(2r) \det(N + \frac{\eta^2}{\cosh(2r)} \mathbb{1}) \\ &= \cosh^2(2r)(\frac{\eta^4}{\cosh^2(2r)} + \frac{\eta^2}{\cosh(2r)} \operatorname{Tr} N + \det N) \\ &= \cosh^2(2r) \det N + \cosh(2r)\eta^2 \operatorname{Tr} N + \eta^4 \end{aligned} \tag{6.12}$$

where we have used some known rules for the determinant of block matrices, and the relation $\det(A + \lambda\mathbb{1}) = \det A + \lambda \operatorname{Tr} A + \lambda^2$ which is valid for 2×2 matrices.

We are now in the position to characterize the entanglement of $\rho_{out} = \lim_{r\to\infty} \mathbb{1} \otimes T(|\phi_r\rangle\langle\phi_r|)$. We first calculate

$$\begin{aligned}\lim_{r\to\infty} 2\nu_-^2 &= \lim_{r\to\infty} \tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4\det\gamma_{out}^{(r)}} \\ &= \lim_{r\to\infty} \tilde{\Delta}\big(1 - \sqrt{1 - 4\frac{\det\gamma_{out}^{(r)}}{\tilde{\Delta}^2}}\big) \\ &= \lim_{r\to\infty} \tilde{\Delta}\big(1 - (1 - 2\frac{\det\gamma_{out}^{(r)}}{\tilde{\Delta}^2})\big) \\ &= \lim_{r\to\infty} 2\frac{\det\gamma_{out}^{(r)}}{\tilde{\Delta}} \\ &= 2\frac{\det N}{(1+\eta^2)^2} \end{aligned} \tag{6.13}$$

by introduction of (6.11) and (6.12), and using $\sqrt{1-x} \approx 1 - x/2$ when $x \ll 1$. Next we recall that $\det M = \eta^2$ and obtain the logarithmic negativity of ρ_{out}

$$E_N[\rho_{out}] = -\frac{1}{2}\log\big(\min\{\frac{\det N}{(1+\det M)^2}, 1\}\big). \tag{6.14}$$

To conclude this proof, we must also consider channels characterized by $\det M < 0$. An example of such channel is the approximated unphysical phase conjugation map used in Chapter 5. Using the same arguments as before, it is easy to show that we can restrict our attention to $M = \eta\Lambda$, where

$$\Lambda = \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right). \tag{6.15}$$

The two symplectic invariants can again be easily calculated, and while $\det\gamma_{out}$ is the same as in (6.12), now $\tilde{\Delta} = \cosh^2(2r)(1-\eta^2)^2 + O(\cosh(2r))$. Remembering that $\det M = -\eta^2$, the symplectic eigenvalue reads again

$$\lim_{r\to\infty} 2\nu_-^2 = 2\frac{\det N}{(1+\det M)^2}. \tag{6.16}$$

However, combining this expression with the condition of complete positivity (6.3), one finds that for channels with $\det M < 0$, the output state ρ_{out} can never be entangled, i.e.,

$$\begin{aligned} \det M < 0 \Rightarrow \nu_- &\geq 1 \\ &\Rightarrow E_N[\rho_{out}] = 0. \end{aligned} \tag{6.17}$$

These channels are called entanglement breaking channels as it is impossible to use them to distribute entanglement. ■

Let us briefly comment this second Lemma. First, we note that ρ_{out} is entangled provided that $E_D < 1$, i.e.,

$$E_N[\rho_{out}] > 0 \Leftrightarrow \frac{\det N}{(1+\det M)^2} < 1. \tag{6.18}$$

For example, if we consider an attenuating channel ($\eta < 1$), one realizes that for fixed attenuation the noise cannot be too large, while for fixed noise the attenuation cannot be too strong in order to distribute entanglement across the channel. However, for a purely lossy fiber ($M = \eta\mathbb{1}$, $N = (1-\eta^2)\mathbb{1}$), E_D is always less than one and the entanglement never vanishes, i.e. it is always possible to distribute some entanglement across a lossy fiber.

Second, E_D is an intrinsic property of channels which can be used to compare their entanglement properties. As an example, consider two channels T_1 and T_2. The entanglement of their output states $\rho^i_{out} = \lim_{r\to\infty} \mathbb{1} \otimes T_i(|\phi_r\rangle\langle\phi_r|)$ with $i = 1, 2$ relate as

$$E_N[\rho^1_{out}] \geq E_N[\rho^2_{out}] \Leftrightarrow E_D[T_1] \leq E_D[T_2]. \tag{6.19}$$

The latter property will prove very useful in the demonstration of the next theorem.

6.3.3 A No-Go theorem

Theorem 6.3.3 *Given a Gaussian channel T of matrices M and N, it is impossible to find a GECC that will transform T into a Gaussian channel T_{GC} of matrices M_{GC} and N_{GC} with smaller Entanglement Degradation, i.e., such that*

$$\frac{\det N_{GC}}{(1+\det M_{GC})^2} < \min\{\frac{\det N}{(1+\det M)^2}, 1\}\,. \tag{6.20}$$

Proof We will prove the theorem by contradiction. Suppose that there exists the GECC of Fig. 6.1 whose overall effect is to transform T into T_{GC}, and such that the corrected channel satisfies (6.20). By Lemma 6.3.1, there exists the one-way local Gaussian protocol of Fig. 6.2 which transforms n copy of the state χ into the state $\rho_d = \lim_{r\to\infty} \mathbb{1} \otimes T_{GC}(|\phi_r\rangle\langle\phi_r|)$. Lemma 6.3.2 combined with condition (6.20) shows that $E[\rho_d] > E[\chi]$, hence the one-way local protocol is a true entanglement distillation protocol based on Gaussian operations only. This is in clear contradiction with the known impossibility to distill entanglement from Gaussian states with Gaussian operations. We conclude that such a GECC does not exist. ■

6.4 Applications

6.4.1 Important Examples of Gaussian Channels

Lossy channel

The lossy channel T_η is characterized by $M = \eta\mathbb{1}$ and $N = (1-\eta^2)\mathbb{1}$ with $\eta < 1$. It is the prototype for optical communication through a lossy fiber, and can be modelled by a beam splitter of transmittance η. For a given channel, the entanglement degradation

$$E_D[T_\eta] = \frac{(1-\eta^2)^2}{(1+\eta^2)^2} < 1 \tag{6.21}$$

is a decreasing function of η, hence by (6.20) it is impossible to find a GECC that will turn a lossy channel into another lossy channel with less losses. One could nevertheless hope to reduce the attenuation factor into $\eta < \eta_{GC} < 1$, at the expense of an increasing noise N_{GC}. By (6.20), this noise must satisfy

$$\det N_{GC} \geq \frac{(1+\eta_{GC}^2)^2}{(1+\eta^2)^2}(1-\eta^2)^2. \tag{6.22}$$

Amplification channel

The amplification channel is the same as the lossy channel with $\eta > 1$. In particular, (6.21) holds, but now E_D is an increasing function of η, i.e., it is impossible to make $\eta_{GC} < \eta$. Again, one can reduce the amplification, for example by combining the amplification channel with a lossy channel, at the expense of an increased noise.

Classical noise channel

The classical noise channel T_N only adds Gaussian classical noise to a state, i.e., $M = \mathbb{1}$ and $N > 0$. Its entanglement degradation is

$$E_D[T_N] = \min\{\frac{\det N}{4}, 1\}, \tag{6.23}$$

and our theorem states that $\det N_{GC} \geq \min\{\det N, 4\}$, i.e. it is impossible to reduce the noise when $\det N < 4$, or it is impossible to reduce the noise under 4 when $\det N > 4$. Note that this limit of 4 can always be reached as the number of ancilae goes to infinity. The protocol is the following: Alice measures the input state and prepares an infinite number of copies that she sends to Bob. Bob measures the received states and prepares a state centered on the average value of his measurement. This strategy is equivalent to a measure-and-prepare (MP) strategy with $\det N_{MP} = 4$.

Arbitrary channel

Consider a Gaussian channel T with matrices M and N, and entanglement degradation $E_D[T] < 1$. Furthermore, suppose that we wish to transform this channel into a classical noise channel T_{GC}, i.e., we would like $M_{GC} = \mathbb{1}$. The corrected channel will be characterized by a noise matrix N_{GC} satisfying

$$\det N_{GC} \geq \frac{4}{(1 + \det M)^2} \det N, \tag{6.24}$$

and our criteria provides a lower bound on the noise of the accessible channels.

6.4.2 Quantum Capacity

Interestingly, the entanglement degradation is connected to the quantum capacity. Let us recall that the quantum capacity of a channel is defined as the rate at which quantum states, qubits in particular, can be perfectly transmitted through the channel (see 2.3.2). More precisely, the quantum capacity $Q[T]$ of a channel T is the supremum $c \geq 0$ such that for all ϵ, $\delta > 0$ there exist n, m, encoding E and decoding D with

$$\left|\frac{n}{m} - c\right| < \delta, \; \|\mathbb{1}_2^{\otimes n} - DT^{\otimes m}E\|_{cb} < \epsilon\,, \tag{6.25}$$

where the norm of complete boundness $\|.\|_{cb}$ is defined as

$$\|T\|_{cb} = sup_n \|\mathbb{1}_n \otimes T\| \tag{6.26}$$

with $\|T\| = sup_X \|T(X)\|_1/\|X\|_1$. Although the quantum capacity is hard to compute for most channels, Werner and Holevo introduced in [60] a computable upper-bound known as Q_Θ. This capacity-like quantity, defined in terms of the transpose operation, has some remarkable properties. In particular, it is known that $Q_\Theta[T]$ can equivalently be defined as the maximal entanglement, as measured by the logarithmic negativity, of states transmitted through the channel T [60], i.e., states of the form $\mathbb{1} \otimes T[\rho]$. If T is a single-mode Gaussian channel, we therefore deduce the following property of the entanglement degradation

Corollary 6.4.1 *Given a Gaussian channel T with entanglement degradation $E_D[T]$, the quantum capacity $Q[T]$ of the channel is bounded by*

$$Q[T] \leq -\frac{1}{2} \log E_D[T]\,. \tag{6.27}$$

Proof This result directly follows from the definition of Q_Θ and E_D. ■

Given how closely connected E_D and Q are, the hope is now to use Theorem 6.3.3 to prove a similar theorem for the quantum capacity. Such a theorem would, in essence, state that the quantum capacity of a Gaussian channel can never increase by means of Gaussian encoding and decoding operations only. Although we have not succeeded yet, let us note the following interesting comment. Intuitively, the quantum capacity of a channel T gives the maximal rate at which T can be used to simulate the ideal channel $\mathbb{1}$. In particular, if T can never approximate $\mathbb{1}$, i.e., even if an infinite number of instances of T, plus arbitrary encoding and decoding, does not simulate $\mathbb{1}$, the quantum capacity $Q[T]$ is zero. Now, noting that $E_D[\mathbb{1}] = 0$, and recalling that Theorem 6.3.3 states that E_D can never be decreased by Gaussian error-correction, one concludes that for a Gaussian channel T with $E_D[T] > 0$, one will never find a GECC such as to approximate the ideal channel, i.e., the encoding (E) and decoding (D) used in the definition of the quantum capacity Eq. (6.25) are necessarily non-Gaussian.

6.5 Conclusion

The entire set of Gaussian operations can be implemented by combining passive and active linear optical components such as beam splitters, phase shifters and squeezers, with homodyne detection followed by classical communications. This makes the Gaussian operations very attractive, since all these elements can be found in most optical labs.

In this chapter, we investigated the feasibility of Gaussian error-correction, i.e., the possibility to correct Gaussian errors on Gaussian states with Gaussian operations only. Exploiting a connection between error-correction and entanglement distillation, we have proven that an intrinsic quantity of Gaussian channels, called the entanglement degradation, could never be reduced by Gaussian operations only. As a consequence, the encoder and decoder of any efficient error correction scheme must be non-Gaussian when Gaussian states are transmitted through a Gaussian channel. This result, combined with the known impossibility to distil entanglement from Gaussian states with Gaussian operations, shows the limitations of the experimentally feasible Gaussian operations.

Finally, the entanglement degradation is shown to be related to the quantum capacity. In particular, it can be used to easily compute a simple upper-bound for the quantum capacity of a single-mode Gaussian channel. This connection, combined with the demonstrated no-go theorem for the entanglement degradation, opens the possibility of a similar no-go theorem for the quantum capacity of Gaussian channels.

7 Experimentally Feasible Quantum Erasure-Correcting Code

7.1 Introduction

Transmitting, storing or manipulating quantum information without errors is prerequisite to the realization of most quantum information protocols. As seen in the previous chapter, when Gaussian errors affect Gaussian states, the easily accessible Gaussian toolbox made of beam splitters, phase shifters, squeezers and homodyne detection is not sufficient to enable successful error correction. This important result unfortunately shows that one needs non-Gaussian operations to efficiently detect and correct Gaussian errors. These non-Gaussian operations, such as photon subtraction for example [81], are typically hard to achieve experimentally. Are the perspectives of experimental continuous variable error correction doomed yet? Clearly not as one can always escape the Gaussian paradigm of Gaussian error and Gaussian correction by considering non-Gaussian errors corrected by Gaussian operations. Recently, this approach attracted a lot of attention and resulted in the development of several methods to fight non-Gaussian noises in the transmission of continuous variable Gaussian states. These schemes include the purification of coherent states [2] and squeezed states [59, 41] from single or several noisy copies, or the filtering of vacuum noise from an arbitrary set of coherent states [104].

In this chapter, we will attack this problem from a slightly different perspective, considering schemes to eliminate losses instead of noise. More presicely, we will consider the transmission of coherent states through a channel, known as the erasure channel, which either transmits the information perfectly, or erases it completely with a given probability p_e, i.e., the channel acts on a coherent state as

$$|\alpha\rangle \rightarrow T[|\alpha\rangle] = (1-p_e)|\alpha\rangle\langle\alpha| + p_e|0\rangle\langle 0|. \tag{7.1}$$

This non-Gaussian channel is known to occur in realistic situations, e.g., resulting from time jitter or beam pointing noise in atmospheric transmissions [104].

As we will see, if one can detect whether an erasure has occurred, the Gaussian toolbox (beam splitters and a feedforward loop based on homodyne detection in this case) allows one to transmit Gaussian information almost perfectly. Furthermore, we will show that even when errors cannot be probed, replacing feedforward by postselection enables one to filter errors efficiently. The experimental feasibility of the proposed protocols will be addressed at the end of the chapter.

7.2 An Erasure Correcting Code for Discrete Variables

For qubits, the erasure channel was first considered by Grassl, Beth and Pelizzari. In [54], they show how to protect one qubit from erasure by encoding in a four-qubit entangled state. Although the corresponding code is of minimal length, i.e., at least a four-qubit entangled state is needed to efficiently fight one erasure, their code can tolerate an extra input qubit at no cost. The encoding of their two-to-four one-error correcting code is

$$\begin{aligned}
|00\rangle &\rightarrow (|0000\rangle + |1111\rangle)/\sqrt{2} \\
|01\rangle &\rightarrow (|0110\rangle + |1001\rangle)/\sqrt{2} \\
|10\rangle &\rightarrow (|1010\rangle + |0101\rangle)/\sqrt{2} \\
|11\rangle &\rightarrow (|0011\rangle + |1100\rangle)/\sqrt{2},
\end{aligned} \tag{7.2}$$

and it has since then been used in various schemes such as the proposal for an all-optical quantum memory [47].

This encoding can be achieved by the simple circuit depicted in Fig. 7.1, where

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \tag{7.3}$$

is a maximally entangled state, and the control-Not (CNOT) gate is a quantum gate that flips the target qubit if the control qubit is one, i.e.,

$$|i\rangle_c |j\rangle_t \rightarrow |i\rangle_c |j \oplus i\rangle_t \ , \tag{7.4}$$

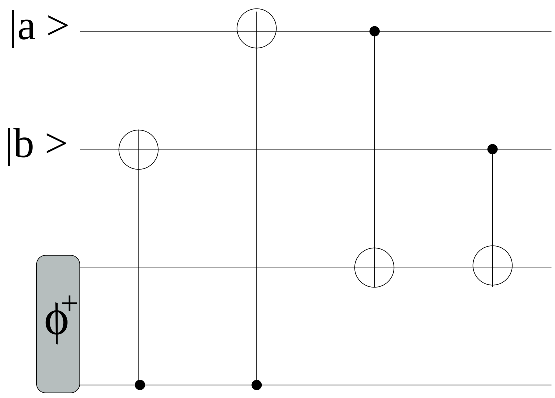

Figure 7.1: *Encoding circuit for the qubit erasure-correcting code. $|a\rangle$, $|b\rangle$: input qubit, $|\phi^+\rangle$: maximally entangled state used as ressource*

with $i, j = 0, 1$ and addition is modulo 2.

Notice that the main ressource of the code is a maximally entangled state used to delocalize the quantum information.

7.3 A Deterministic Protocol: Erasure Correction

7.3.1 The Optical Setup

Protecting the information: the Encoder

Can we adapt the circuit of Fig. 7.1 to the transmission of, e.g., coherent sates? This circuit uses two different elements; a maximally entangled state and four CNOT gates. Clearly, $|\phi^+\rangle$ has a direct continuous analog, namely the EPR pair (a two-mode squeezed vacuum in practice). Furthermore, the CNOT gate can be easily translated to the continuous variable regime. In [6], its action on the canonical position and momentum operators is defined as

$$\begin{aligned} \hat{x}_t &= \hat{x}_t + \hat{x}_c & \hat{x}_c &= \hat{x}_c \\ \hat{p}_t &= \hat{p}_t & \hat{p}_c &= \hat{p}_c - \hat{p}_t\,, \end{aligned} \tag{7.5}$$

where the indices c and t denote the *control* and *target* modes respectively. However, in the continuous regime the CNOT gate is not its own inverse, hence we must also introduce the CNOT† gate

$$\begin{aligned} \hat{x}_t &= \hat{x}_t - \hat{x}_c & \hat{x}_c &= \hat{x}_c \\ \hat{p}_t &= \hat{p}_t & \hat{p}_c &= \hat{p}_c + \hat{p}_t. \end{aligned} \tag{7.6}$$

Combining all these elements leads to the quantum circuit depicted in Fig. 7.2a. Remarkably, one can protect two coherent states from erasure by

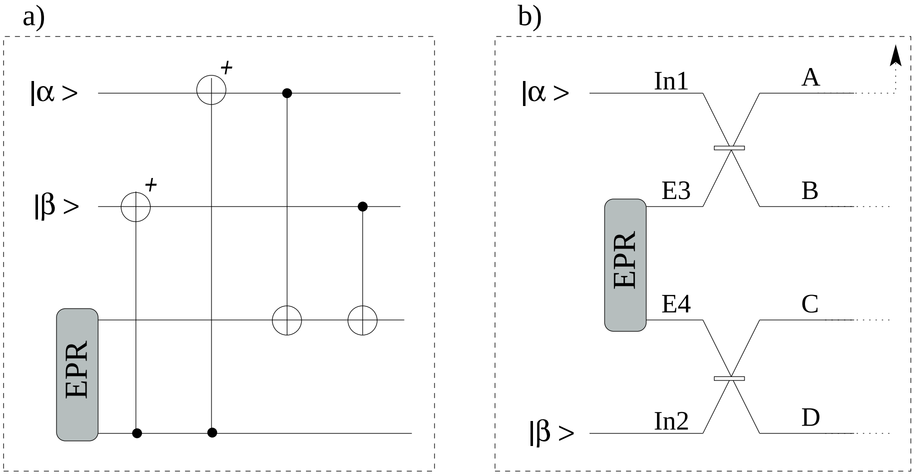

Figure 7.2: *a) Encoding circuit for the CV quantum erasure-correcting code; b) Optical implementation of the encoder using a two-mode squeezed vacuum as ressource (EPR)*

mixing them with an EPR pair through a quantum circuit made of two CNOT and two CNOT† gates.

Unfortunately, there is no physical interaction between light modes which is described by Eqs. (7.5) and (7.6). As a consequence, these two gates cannot be easily implemented optically (see e.g. [106]), and the circuit of Fig. 7.2.a cannot be realized directly. Nevertheless, this circuit can be translated into an experimentally feasible optical setup using Bloch-Messiah reduction theorem. This well known theorem of quantum optics states that a multimode evolution with linear Bogoliubov transformation

$$\hat{b}_j = \sum_k (A_{jk}\hat{a}_k + B_{jk}\hat{a}_k^\dagger) + \beta_j \,, \tag{7.7}$$

where $\hat{a}_j, \hat{b}_j$ are bosonic annihilation operators, may be decomposed into a multi-port linear interferometer, followed by the parallel application of a set of single mode squeezers, followed yet by another multi-port linear interferometer [17]. Recalling that any linear interferometer can be realized as an array of beam splitters and phase shifters [89], one concludes that the encoder of Fig. 7.2.a can be implemented by combining passive and active linear optical components only, i.e. it is a Gaussian operation. A few simplifications leads to the circuit depicted in Fig. 7.2.b. Protecting two coherent states from erasure simply boils down to mixing the two input states with a two-mode squeezed vacuum at two balanced beam splitters.

We note that a subpart of this circuit, where a coherent state is mixed with one-half of an EPR pair, has been introduced in the context of CV quantum secret sharing. This connection between erasure-correction and secret sharing is further explored in Appendix C.

Recovering the information: the Decoder

Let us now prove that we can correct losses provided that we monitor the occurrence of erasures. Depending on the channel, this monitoring may be achieved, e.g., by sending a probe pulse in an orthogonal mode, like another polarization, another spatial, or another frequency mode.

Suppose for example that we loose mode A during the transmission (see Fig. 7.2.b). We can recover the input coherent state $|\beta\rangle$ by mixing modes C and D on a balanced beam splitter, thus effectively completing a Mach-Zehnder interferometer. The other output port of the interferometer yields one half of the EPR pair. The recovery of the other state $|\alpha\rangle$ is a little more demanding as the information has been attenuated and polluted by quantum noise. However, this noise is exactly correlated with the other half of the EPR pair, so that one can partly recover $|\alpha\rangle$ by amplifying mode B in a phase-insensitive amplifier of gain 2, using the second output port of the Mach-Zehnder interferometer as the idler input of the amplifier. Remarkably, such an optical amplifier can be implemented using only linear optics, homodyne detection, and feedforward, as demonstrated in [66]. The decoder that corrects the loss of A based on this amplifier without nonlinearity is depicted in Fig. 7.3.a.

However, to have a practical protocol, the decoding should work regardless the location of the erasure. This is made possible by noticing first that the amplifier of Fig. 7.3.a treats both input ports of BS1 on the same footing. Thus, if we connect A to the empty input of BS1 and adapt the sign of the electronic gains of the feedforward, the circuit can correct both erasures of A or B. Next, notice that BS1 now plays the same role for A and B as BS2 does for C and D. We thus find the decoding optical circuit shown in Fig. 7.3.b.

7.3.2 Performances

Let us characterize our erasure-correction protocol. For two input modes characterized by the conjugate quadrature operators $(\hat{x}_{in1}, \hat{p}_{in1})$ and $(\hat{x}_{in2}, \hat{p}_{in2})$, and an EPR pair corresponding to

$$\Delta\left(\frac{\hat{x}_{E3} - \hat{x}_{E4}}{\sqrt{2}}\right) = \Delta\left(\frac{\hat{p}_{E3} + \hat{p}_{E4}}{\sqrt{2}}\right) = e^{-2r}, \tag{7.8}$$

the two output modes can be written as

$$\begin{aligned} \hat{x}_{out1(2)} &= \hat{x}_{1(2)} + g^x_{1(2)}\, \hat{x}_m\,, \\ \hat{p}_{out1(2)} &= \hat{p}_{1(2)} + g^p_{1(2)}\, \hat{p}_m\,, \end{aligned} \tag{7.9}$$

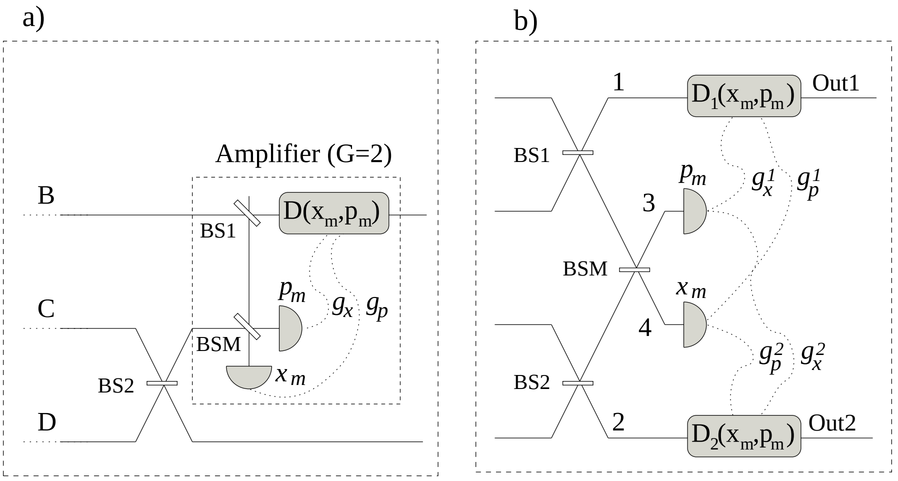

Figure 7.3: *a) Correction of an erasure of mode A via the phase-insensitive amplification of mode B realized with homodyne detection and feedforward; b) Decoding circuit correcting an erasure of any of the four modes.*

where $(\hat{x}_1, \hat{p}_1)$ and $(\hat{x}_2, \hat{p}_2)$ are the upper and lower output modes just before displacement, $(\hat{x}_m, \hat{p}_m)$ are the measured quadratures, and the gains are given in Table 7.1.

	(g_1^x, g_1^p)	(g_2^x, g_2^p)
loss of A	$(-\sqrt{2},-\sqrt{2})$	(0,0)
loss of B	$(\sqrt{2},\sqrt{2})$	(0,0)
loss of C	(0,0)	$(\sqrt{2},-\sqrt{2})$
loss of D	(0,0)	$(-\sqrt{2},\sqrt{2})$

Table 7.1: *Electronic gains for different loss locations.*

To verify these relations, suppose that mode A is lost during the transmission. The upper mode before displacement is given by

$$\begin{aligned}\hat{x}_1 &= \frac{1}{\sqrt{2}}\hat{x}_v + \frac{1}{2}\hat{x}_{in1} - \frac{1}{2}\hat{x}_{E3}\,,\\ \hat{p}_1 &= \frac{1}{\sqrt{2}}\hat{p}_v + \frac{1}{2}\hat{p}_{in1} - \frac{1}{2}\hat{p}_{E3}\,,\end{aligned} \tag{7.10}$$

where $(\hat{x}_v, \hat{p}_v)$ refers to the vacuum mode introduced by the loss of A. The measured quadratures are given by

$$\begin{aligned}\hat{x}_m &= \frac{1}{2}\hat{x}_v - \frac{1}{2\sqrt{2}}\hat{x}_{in1} + \frac{1}{2\sqrt{2}}\hat{x}_{E3} - \frac{1}{\sqrt{2}}\hat{x}_{E4}\,,\\ \hat{p}_m &= \frac{1}{2}\hat{p}_v - \frac{1}{2\sqrt{2}}\hat{p}_{in1} + \frac{1}{2\sqrt{2}}\hat{p}_{E3} + \frac{1}{\sqrt{2}}\hat{p}_{E4}\,,\end{aligned} \tag{7.11}$$

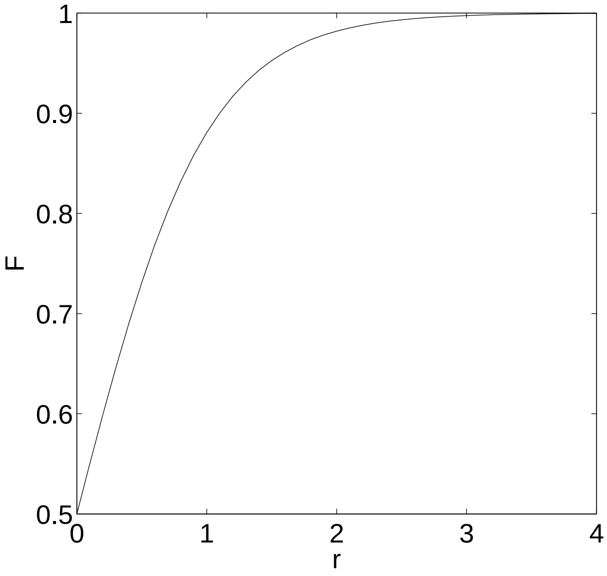

Figure 7.4: *Fidelity of the erasure correcting code as a function of the squeezing factor of the two-mode squeezed state.*

so that Eq. 7.9 yields

$$\begin{aligned}\hat{x}_{out1} &= \hat{x}_1 - \sqrt{2}\,\hat{x}_m = \hat{x}_{in1} - (\hat{x}_{E3} - \hat{x}_{E4})\,,\\ \hat{p}_{out1} &= \hat{p}_1 - \sqrt{2}\,\hat{p}_m = \hat{p}_{in1} - (\hat{p}_{E3} + \hat{p}_{E4})\,. \end{aligned} \tag{7.12}$$

The performances of the protocol can now be easily evaluated using the fidelity. While the lower input is perfectly recovered, i.e.,

$$F_\beta = 1, \tag{7.13}$$

the upper input will be recovered with the fidelity

$$F_\alpha = \frac{1}{1+e^{-2r}}. \tag{7.14}$$

7.3.3 Comments

To conclude this section, let us first note that the two fidelities can be symmetrized by mixing the input modes entering the encoder and unmixing them at the output of the decoder. This will effectively distribute the added noise on both output modes, leading to

$$F_\alpha = F_\beta = \frac{1}{1+\frac{1}{2}e^{-2r}}. \tag{7.15}$$

Second, the fidelity (7.14) – or its symmetrized version – is independent of the input coherent states, hence our erasure-correcting scheme is universal. Finally, as seen on Fig. 7.4, the decoder becomes perfect at the limit of infinite squeezing ($r \to \infty$), and our protocol enables perfect transmission of coherent states over the erasure channel.

7.4 A Probabilistic Protocol: Erasure Filtration

7.4.1 From Feedforward to Postselection

In a realistic experiment, probing erasure without loosing information, a protocol known as a Quantum Non-Demolition (QND) measurement, is a difficult task. While such QND measurement exist for single photons [47], none is explicitly known for optical continuous variable states[1]. Unfortunately, when erasure cannot be probed, we no longer know which set of gains to choose from Table 7.1 and cannot correct errors. In addition, we must consider multiple erasures, a possibility that was implicitly ignored in the previous section. In such a realistic scenario, can we nevertheless use our protocol to improve the transmission of coherent states over the erasure channel?

Surprisingly, the answer turns out to be yes and can be summarized in a single word: *postselection*. The key idea is to note that if the measured quadratures are close to zero, then the output states do not need to be displaced regardless of the location of the erasure, i.e., all 4 lines of Table 7.1 imply the same action. If they are far from zero, we discard the output states, effectively replacing the feedforward loop by postselection.

The scheme is depicted in Fig. 7.5, and its underlying mechanism can be easily understood. Suppose for example that no erasure occurs during the transmission. The two detectors will receive squeezed states centered on zero whose variances depend on the squeezing of the EPR pair, i.e., measuring the appropriate quadrature will give zero on average. In the case of an erasure, however, these squeezed states will be polluted and displaced according to the intensity of the input states, i.e., the measured values will no longer be centered around zero and the error can be detected. This probabilistic protocol can thus be viewed as an erasure filter [51], which excludes the output states that have been affected by an erasure during transmission.

[1] We note that a CV QND measurement was experimentally demonstrated very recently [106].

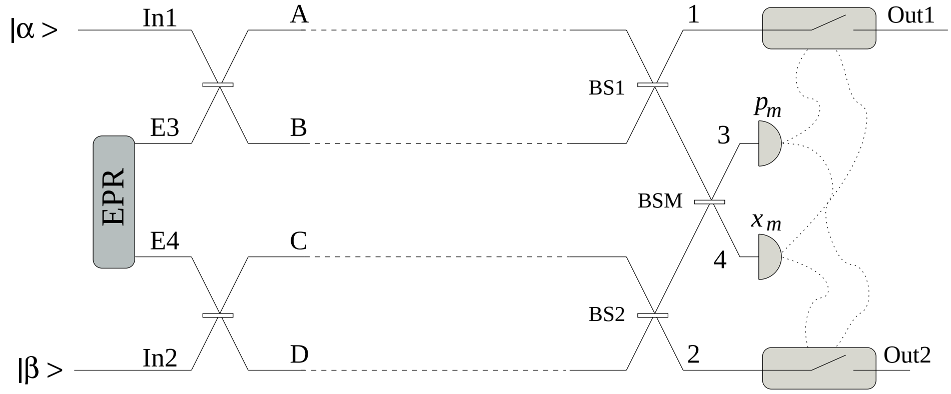

Figure 7.5: *Schematic of the Erasure Filter.*

7.4.2 Evaluating the Performances

In order to investigate our erasure filter, we introduce the Wigner function of the two input modes together with the two modes of the EPR pair,

$$W_{in}(r) = \frac{1}{\pi^4\sqrt{\det\gamma_{in}}}\exp[-(r-d_{in})\gamma_{in}^{-1}(r-d_{in})]\,, \tag{7.16}$$

where $r = (x_1, p_1, ..., x_4, p_4)$ is the vector of quadrature components, d_{in} is the vector of first moments, and γ_{in} is the covariance matrix. According to our protocol, this 4-mode state is processed through two parallel (lossy) Mach-Zehnder interferometers, then modes 3 and 4 are mixed on a balanced beam splitter and measured. Just before measurement, the 4-mode state will have evolved into a non-Gaussian mixture of Gaussian states, whose Wigner function can be written as

$$W_{out}(r) = \sum_{i=1}^{16} p_i W_{out}^{(i)}(r)\,, \tag{7.17}$$

where $W_{out}^{(i)}$ is the output Wigner function corresponding to one of the sixteen events that can occur during transmission. These events range from no erasure, with a probability of $(1-p_e)^4$, to the erasure of all four modes, with a probability of p_e^4. Next, the p quadrature of mode 3 and x quadrature of mode 4 are measured. If the outcomes are (x_m, p_m), the Wigner function of the remaining modes reads

$$\begin{aligned} W_{out}(r'|x_m,p_m) &= \iint_{-\infty}^{-\infty} \mathrm{d}x_3\mathrm{d}p_4 W_{out}(r', x_3, p_m, x_m, p_4) \\ &= \sum_{i=1}^{16} p_i\, W_{out}^{(i)}(r'|x_m,p_m)\,, \end{aligned} \tag{7.18}$$

with $r' = (x_1, p_1, x_2, p_2)$. To calculate these sixteen Wigner functions, we first partition each covariance matrix $\gamma^{(i)},\ i = 1, .., 16$, of the output Wigner functions $W_{out}^{(i)}$ before the measurement (see e.g. [46])

$$\gamma^{(i)} = \begin{pmatrix} \gamma' & A \\ A^T & B \end{pmatrix} \tag{7.19}$$

where B is the covariance matrix of the (traced over) quadratures x_3 and p_4. We further partition the inverse of the covariance submatrix γ' as

$$(\gamma')^{-1} = \begin{pmatrix} (\gamma'')^{-1} & E \\ E^T & D \end{pmatrix}, \tag{7.20}$$

so that its block γ'' contains the second moments of the remaining modes after measurement. After some calculations (see Appendix D for more details), we obtain

$$W_{out}^{(i)}(r'|x_m, p_m) = \frac{1}{\pi^3\sqrt{\det\gamma'}} \exp[-\delta^T F \delta] \times \exp[-(r'-d')^T \gamma''^{-1}(r'-d')] \tag{7.21}$$

where δ is the vector of difference between the measured values (x_m, p_m) in modes 3 and 4 and the corresponding mean values before measurement, d_r is the coherent vector of modes 1 and 2 before displacement, and

$$F = D - E^T \gamma'' E \tag{7.22}$$
$$d' = d_r - \gamma'' E \delta. \tag{7.23}$$

We now introduce the threshold condition. If we decide to keep the output states provided that

$$|x_m| \le X_{th}$$
$$|p_m| \le P_{th}, \tag{7.24}$$

the resulting unnormalized Wigner function reads

$$W_{th}(r') = \sum_{i=1}^{16} p_i \int_{th} \mathrm{d}x_m\, \mathrm{d}p_m\, W_{out}^{(i)}(r'|x_m, p_m)\,, \tag{7.25}$$

and the probability to keep the output state is

$$P_s = \int \mathrm{d}^4 r'\, W_{th}(r')\,, \tag{7.26}$$

where the integration runs over the entire phase space of the two output modes.

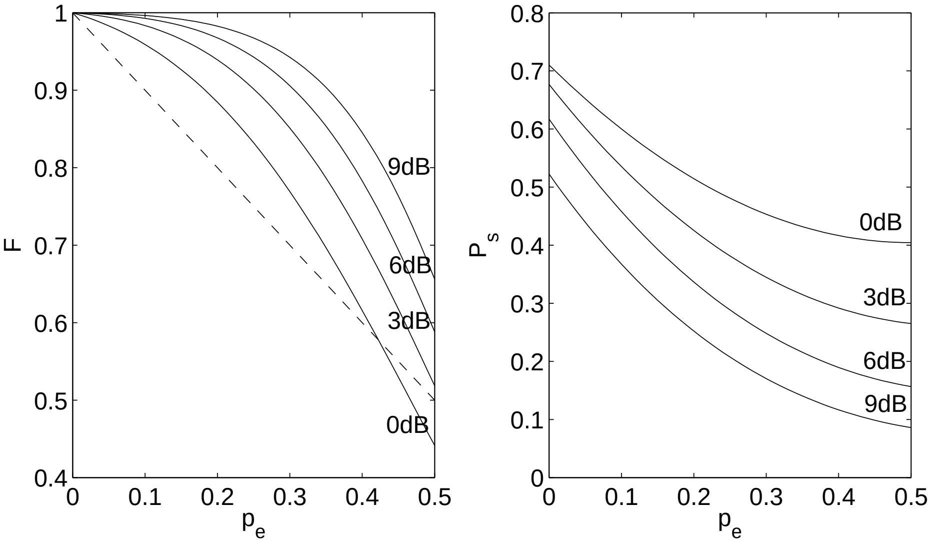

Figure 7.6: *Fidelity F (left) and success probability P_s (right) versus the erasure probability p_e for various degrees of squeezing r and $|\Psi_{in}\rangle = |\frac{4+i4}{\sqrt{2}}\rangle|0\rangle$. The dashed line is the fidelity without erasure filtration. All curves are plotted with $X_{th} = P_{th} = e^{-r}$, $\eta_{HD} = 0.9$ and $n_e = 0$.*

To evaluate the quality of the protocol, we calculate the fidelity of one of the output mode, say for example mode 1,

$$F_{ps} = (2\pi/P_s) \int \mathrm{d}^2 r'_1 \, W^1_{th}(r'_1) \, W_\alpha(r'_1) \,, \tag{7.27}$$

where W_α is the Wigner function of the coherent state at input 1 and

$$W^1_{th}(r'_1) = \int \mathrm{d}^2 r'_2 \, W_{th}(r'). \tag{7.28}$$

We then compare this fidelity to that resulting from the same state being sent directly to the erasure channel, i.e.,

$$F_{ref} = (1 - p_e) + p_e \times 2\pi \int \mathrm{d}^2 r'_1 \, W_0(r'_1) \, W_\alpha(r'_1) \tag{7.29}$$

where W_0 is the Wigner function of the vacuum.

7.4.3 Results

The formulas introduced in the previous section, (7.26) (7.27) and (7.29) in particular, can be evaluated numerically with mathematical softwares like *Matlab*. In order to properly simulate the results of an experiment, one has to model imperfect homodyne detectors. This is achieved by adding a beam splitter with the desired transmitivity in front of a perfect detector.

The performances of the protocol are illustrated in Fig. 7.6 for the input state

$$|\psi_{in}\rangle = |\frac{4+i4}{\sqrt{2}}\rangle|0\rangle \tag{7.30}$$

and various degrees of squeezing. As expected, the fidelity improves with squeezing, and we can achieve high fidelities while maintaining acceptable probabilities of success. For example, with 6dB of squeezing ($r = 0.69$) and an erasure probability of 0.2, we observe a fidelity of 0.97 and a success probability above 33%.

We note that there is a trade-off between the fidelity and the probability of success, tuned by the chosen threshold window. Indeed, a tight condition will filter most errors but also discards acceptable output states, i.e. the fidelity is high but the probability of success is low, while a loose condition will keep most output states but tolerate a large number of errors, i.e. the probability of success is high but the fidelity is low. Numerical simulations suggest to choose $X_{th} = P_{th} \simeq e^{-r}$, which corresponds to one standard-deviation of the Gaussian squeezed state that should be detected in the case of no errors. With perfect detectors and an erasure-free channel, this condition already reject around 30% of the output states.

However, in contrary to the deterministic protocol, the probabilistic error filter is state-dependent since the ability of the protocol to detect an erasure depends on the intensity of the input states. We note that it is also affected by the squeezing parameter r (available entanglement and threshold condition), but in practical applications r will be fixed as one will always chose the maximum available entanglement. The dependence of the fidelity with respect to the input intensities is investigated in Fig. 7.7 for a fixed squeezing parameter. We note that this dependence is only significant at *low* intensities and the protocol can be considered almost universal otherwise. Note that the definition of "low" depends of the chosen r. For example, with $6dB$ of squeezing and an erasure probability of 0.2 as above, increasing the intensity of the first and/or second input of $|\frac{4+i4}{\sqrt{2}}\rangle|0\rangle$ does not change the fidelity by more than 1% (see Fig. 7.7).

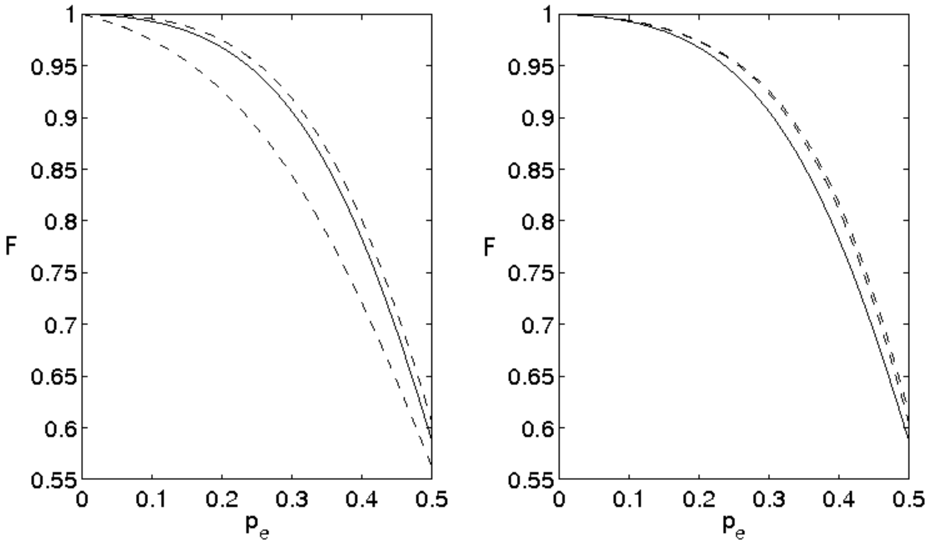

Figure 7.7: *Left: Fidelity F versus the erasure probability p_e for various intensity of the first input state and $r = 6dB$, i.e. $|\psi_{in}\rangle = |\alpha\rangle|0\rangle$ with $\alpha = (2+i2)/\sqrt{2}$(lower dash), $(4+i4)/\sqrt{2}$ (solid), and $(100+i100)/\sqrt{2}$ (upper dash). Right: Fidelity F versus the erasure probability p_e for various intensity of the second input state and $r = 6dB$, i.e. $|\psi_{in}\rangle = \left|(4+i4)/\sqrt{2}\right\rangle|\beta\rangle$ with $\beta = 0$ (solid), $(4+i4)/\sqrt{2}$ (lower dash), and $(100+i100)/\sqrt{2}$ (upper dash).*

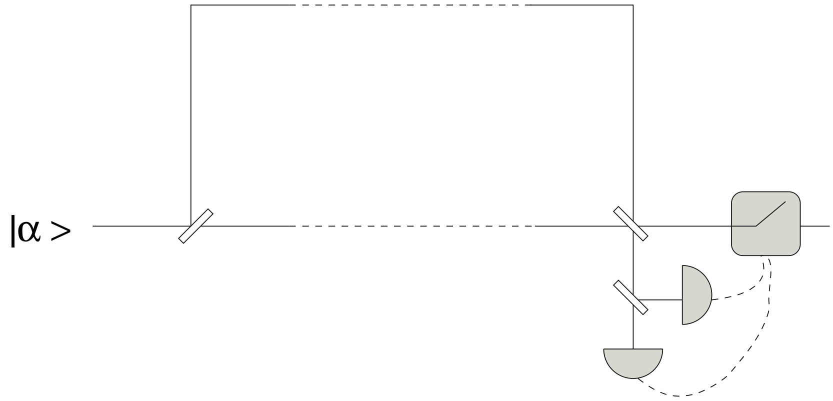

Figure 7.8: *Simple setup to improve the transmission of coherent states over the erasure channel.*

7.4.4 A Simpler Setup

Interestingly, when no squeezing is used and one of the input state is the vacuum, i.e., $r = 0$ and $|\beta\rangle = |0\rangle$, our scheme boils down to a very simple setup: the input coherent state is split on a balanced beam splitter, the two resulting modes are sent through the channel and interfere at the reception station. One of the two output beams is then heterodyne measured, and the other is kept conditionally on the outcomes being close to zero (see Fig. 7.8). As shown by the $0dB$ curve of Fig. 7.6, and further detailed in Fig. 7.9, this strikingly simple protocol is sufficient to improve the transmission of coherent states over the erasure channel.

7.5 Experimental Realization

Remarkably, the simplicity of our protocols allows for an experimental test. This test is currently being implemented by the group of Dr. Ulrik L. Andersen of the Technical University of Denmark, and the first results are expected for september 2008. In the following section, we will briefly foresee this experimental realization and address its feasibility.

The efficiency of our protocols basically falls back on the quality of the entanglement source. Gaussian entanglement can be produced through the interference of two Gaussian, single-mode squeezed states generated either using optical parametric oscillators [14] or single-mode fibers [52]. To enable high efficiency and self-locked interference between the two modes, a system where the two squeezed modes are produced in the same squeezing device but in orthogonal polarization modes is envisaged. By using two orthogonally orientated nonlinear crystals inside a single cavity, the two polarization modes will be independently squeezed, have a relative phase which is inher-

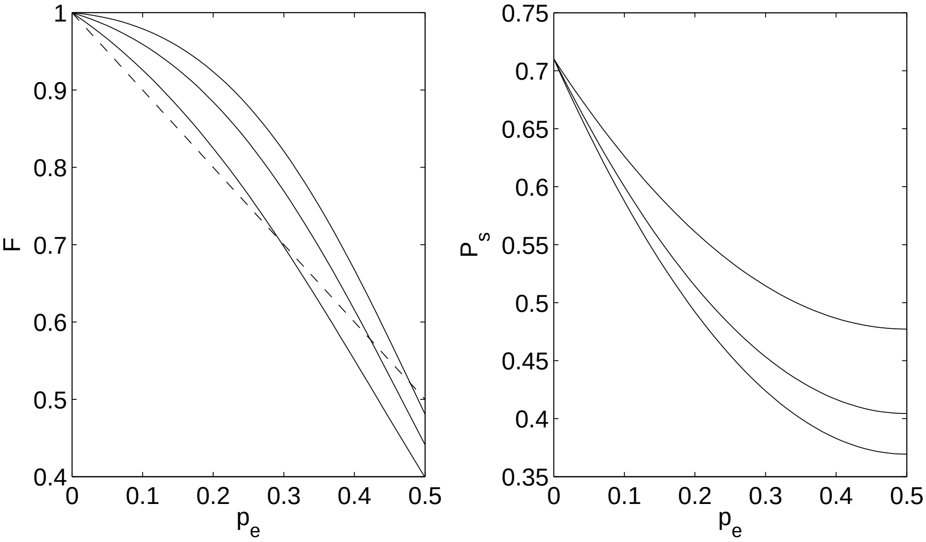

Figure 7.9: *Fidelity F (left) and success probability P_s (right) versus the erasure probability p_e for various intensity of the input state, i.e. $|\psi_{in}\rangle = |\alpha\rangle$ with $\alpha = (3+i3)/\sqrt{2}$, $(4+i4)/\sqrt{2}$, and $(5+i5)/\sqrt{2}$. The dashed line is the fidelity without erasure filtration.*

ently stable, and excite the same spatial mode as supported by the cavity [71]. Using such a scheme, 6dB two-mode squeezing should be feasible. The outputs of the entanglement source must then interfere with two coherent states that can be defined as frequency sideband modes in a frequency range in which the entanglement is most pronounced (see Sec. 5.5.1 for more details about the sideband encoding). The resulting four beams are then mixed on three beam splitters. The spatial and temporal mode overlap at these beam splitters can be almost ideal by using a continuous-wave light source in a single spatial mode and a cavity based squeezing source.

For the measurement of modes 3 and 4, one should use high efficiency and low noise homodyne detectors. To avoid the use of two separate local oscillators (one for each homodyne detector) a simpler scheme relying solely on two high sensitivity detectors can be employed, as discussed in [66]. The measurement efficiency η_{HD} can then easily exceed 90%. Furthermore, the electronic noise n_e of the detectors and the associated feedforward electronics should be kept low. Electronic noise 2-3 orders of magnitude smaller than the shot noise is attainable [66].

In the deterministic scheme, the photocurrents must drive modulators traversed by auxiliary beams which subsequently are mixed with the output states 1 and 2 at very asymmetric beam splitters, thereby accomplishing a clean and near loss free displacement [43, 96, 66]. In the probabilistic scheme, the analog outputs of the measurement devices should be digitized with a high-resolution analog-digital converter, providing fast measurements even when the success rate is low. The resulting outcome (x_m, p_m) is compared with the threshold values and the two output states are either selected or discarded. This selection process can be done electro-optically requiring fast real-time feedforward and fast amplitude modulators or, alternatively, pure electronically by selecting the digitized outcomes of the homodyne detectors used to characterize the scheme.

7.6 Conclusion

In this chapter, we have shown how to exploit the feasible Gaussian operations in order to protect Gaussian states from non-Gaussian errors. In particular, we considered the transmission of coherent states through the erasure channel, and designed a deterministic protocol based on feedforward enabling a recovery of the input states with very high fidelities. The main ingredient of this erasure-correcting code is an entangled state which permits a "nonlocal" transmission of information robust to local erasures. The quality of the scheme only depends on the quality of the entangled ressource. In particular, when highly entangled states are available, our protocol enables the perfect transmission of coherent states over the non-Gaussian erasure channel.

When errors cannot be probed, our erasure-correcting code can be transformed into an efficient probabilistic error filter. To do so, we simply replaced the feedforward loop by postselection. The resulting protocol enables a transmission of coherent states through the erasure channel with high fidelities and at an acceptable rate. Remarkably, entanglement is no longer necessary, and our filter is shown to work when entanglement is not available.

The strength of our two protocols lies in the extreme simplicity of the corresponding optical setup. A few beam splitters, a two-mode squeezed vacuum, and two homodyne detectors are sufficient to implement the entire scheme, thanks to the experimental simplicity of Gaussian operations with optical continuous variables. Our proposed setup is currently being demonstrated experimentally by the group of Dr. Ulrik L. Andersen.

We note that the protocols presented in this chapter are not restricted to complete losses and coherent states. Partial losses can be corrected or filtered as well, and the scheme applies to other Gaussian states, e.g. to the transmission of squeezed states over the erasure channel.

Finally, erasure-correction is connected to other interesting primitives of quantum information theory such as secret sharing and entanglement distillation. In Appendix C, we show how to understand our scheme as the first (3,4)-threshold CV quantum secret sharing protocol, and in Appendix E, we investigate the possibility to use our simple optical setup to distil CV entanglement. We therefore expect our protocol to play an important role in the rapidly developing field of continuous variable quantum information and communication.

8 Conclusion

Nearly a century after its discovery, quantum mechanics continues to be a fascinating theory. Thanks to the introduction of information theoretic aspects, the advent of quantum information science has seen our view of some of the most controversial aspects of quantum mechanics change from bizarre properties of the theory to cherished ressources enabling a variety of protocols. Quantum entanglement and quantum nonlocality are, unarguably, the most emblematic symbols of this renewal. Understanding, characterizing, and, most importantly, exploiting them to achieve e.g. secure communications or efficient computation has been at the center of quantum information science for the past 25 years. In this dissertation, we investigated the possibilities offered by a novel approach of quantum information based on continuous variables of the electromagnetic field. The high performances of homodyne detection, combined with the tractability of the generation of Gaussian states, makes the use of such optical continuous variables particularly suitable for practical applications. Our work can be divided in two complementary parts. In Chapters 3, 4, and 5, oriented towards fundamental issues, we investigated the peculiar relation between entanglement and nonlocality. In Chapters 6 and 7, oriented towards practical applications, we focused on an important primitive of quantum communications, namely quantum error-correction.

Entanglement can give rise to nonlocal correlations. The main tool to verify the existence of such nonlocal correlations between space-like separated locations is to check that the collected data violate a Bell inequality. In **Chapter 3**, we advantageously exploited optical continuous variables in order to design proposals for loophole-free Bell tests. Our main contribution is the proof that it is always possible to maximally violate the multipartie Mermin-Klyshko inequality based on quadrature measurements of light modes. This result is highly non-trivial since the Mermin-Klyshko inequality is in essence discrete. It follows that a Bell test of this kind based on continuous variables requires one to discretize the continuous outcome of the quadrature measurements, thereby discarding some information. Our result shows that this loss is not crucial if one uses a suitable binning procedure, properly adapted to the states under investigation. Furthermore, by allowing for a greater freedom in the search for a feasible multipartite state that can tolerate experimental noise, our work confirms optical continuous variables as a strong candidate for the experimental loophole-free Bell test that physicists have long waited for. However, even if it was proven to be unnecessary in theory, a truly continuous Bell test, i.e., one that does not require a binning process, remains desirable as it would probably enable to fully exploit the potential of optical continuous variables. So far, all proposed Bell tests relying on quadrature measurements of the field suffer from a tradeoff between the magnitude of the violation and the experimental feasibility of the test. One can hope that such a novel approach will not suffer from the same limitations, thereby enabling larger violations with experimentally feasible states. While some preliminary results in that direction have been recently obtained [19], we nevertheless note that, in the present state of knowledge, our proposed noise-resistant multipartite Bell test is probably the best candidate for an experiment based on homodyne detection.

The relation between entanglement and nonlocality is known to be of a complex nature. However, the relative simplicity, both theoretically and experimentally, of the optical continuous variable approach makes it an interesting framework to obtain new insight into these two essential ressources of quantum information. In Chapters 4 and 5, we investigated the possibility to witness nonlocal effects based on continuous-variable product states. In **Chapter 4**, in particular, we focused on nonlocality without entanglement, namely the local indistinguishability that can be sometimes exhibited by a set of locally prepared orthogonal product states. By introducing a circuit-based picture of the phenomenon, we discovered a simple method to generate this peculiar nonlocal effect from the computational basis of a given multipartite d-dimensional Hilbert space. Increasing the dimension towards infinity naturally led to the discovery of a set of continuous variable product states exhibiting the desired behavior. However, the discovered set is unrealistic as it relies on infinitely squeezed states of the electromagnetic field. It is nevertheless a valid set, and can be considered as a proof of principle of the existence of nonlocality without entanglement in the continuous variable regime. In order to show that the sets considered in Chapter 4 exhibit nonlocality without entanglement, we used a practical approach, i.e., we simply proved that they could not be perfectly distinguished locally. We note that a method to compute by how much these states fail to be locally distinguishable, according to some figure of merit such as the mutual information used in [11], is still missing. Such a method would enable an interesting quantitative characterization of nonlocality without entanglement. One could for example rank different sets of product states according to their degree of this new nonlocality. Nonetheless, our work provides new tools to tackle the questions raised by nonlocality without entanglement. For example, one may wonder if this subtle nonlocal effect can be tested in the laboratory, using some operational witness similar to the Bell inequalities for standard nonlocality. Furthermore, since entanglement cannot increase by LOCC, but nonlocality without entanglement proves that some separable superoperators cannot be implemented by LOCC, one can ask whether some separable superoperators can increase entanglement? We believe that our work will help answer these questions in the near future. As an example, in **Appendices A and B** we show how our results can be exploited to tackle the related problems of unextendible product basis and bound entanglement in arbitrary dimensions.

In **Chapter 5**, we considered another peculiar nonlocal behavior exhibited by sets of classically correlated product states. Again, the nonlocality of the states is revealed by the measurement which discriminates them best; although the states are product, this measurement is joint and entangled. This is yet another illustration of the richness of entanglement, as it can be used to efficiently extract information from purely classical correlations. The main result of this chapter is the proof that such a nonlocal effect can be witnessed in the continuous variable regime. The states considered are coherent states of the electromagnetic field, and the classical correlation used is phase-conjugation, i.e., our ensemble is made of pairs of phase-conjugated coherent states. We called this new phenomenon nonlocality without squeezing. Surprisingly, identical copies of coherent states do not exhibit this nonlocality, which is in clear opposition with the similar effect known for discrete variables. Furthermore, since the considered states and the optimal local and joint measurement strategies are all Gaussian, the nonlocality without squeezing exhibited by our product coherent states could be successfully demonstrated experimentally. This nicely illustrates the power of optical continuous variables. While the discrete counterpart of our nonlocality waited 14 years for an experimental demonstration [72, 88], nonlocality without squeezing could be tested immediately. However, we must note that the experiment performed was only a confirmation of the theoretical predictions, not an operational test of nonlocality without squeezing. The existence of such a test remains an interesting open question. Finally, the first part of the dissertation can be concluded by the following comment. The nonlocal behaviors investigated in Chapters 4 and 5 show that the information-theoretic content of some ensembles of product states is larger when considered jointly than locally. Can this benefit be exploited advantageously? Can we, for example, improve quantum communications by using the domino states, or phase-conjugated coherent states? While we do not have the answer, we note that such an application would make our understanding of these two peculiar nonlocal effects change from bizarre properties of quantum mechanics to true ressources that can be used efficiently... a little like entanglement and nonlocality did 40 years ago.

The second part of this dissertation aimed at exploiting the experimental advantages of the optical continuous variable approach. The problem we considered specifically is that of quantum error correction. In **Chapter 6**, we investigated error correction from a Gaussian perspective since, on the one hand many quantum channels can be modeled by a Gaussian operation, and on the other hand the states and the operations that are experimentally feasible are mostly Gaussian. The main result of this chapter, which takes the form of a no-go theorem, is the proof that Gaussian error-correction is, unfortunately, strongly limited. In particular, we introduced a new intrinsic quantity of (single-mode) Gaussian channels, called the Entanglement Degradation, and proved that this quantity can never decrease if one is restricted to Gaussian operations. As a consequence, the encoder and decoder of any efficient error correction scheme must be non-Gaussian when Gaussian states are transmitted through a Gaussian channel. Our new theorem, which nicely complements the known impossibility to distil entanglement from a Gaussian state using local Gaussian operations only, shows the need for efficient and reliable non-Gaussian operations. One such operation has already been experimentally demonstrated, namely photon-subtraction, but remains technically challenging. Although Gaussian operations (beam splitters, phase shifters, squeezers, etc) enable many quantum information protocols such as quantum key distribution, teleportation, or cloning, the future of optical continuous variables strongly relies on our ability to masterize some non-Gaussian operations and their related non-Gaussian states. To conclude, we note that our theorem is based on the newly introduced entanglement degradation. However, a related impossibility based on a well-known quantity could make our theorem a key tool in the study of (single-mode) Gaussian channels. Interestingly, the entanglement degradation can easily be related to the quantum capacity, hence we believe that our theorem can be extended to this widely used quantity. Some preliminary results have already been obtained in this direction.

Despite the limitations demonstrated in the previous chapter, we proved in **Chapter 7** that it is nevertheless possible to exploit the feasibility of optical Gaussian operations in order to achieve efficient error-correction. The trick we used to avoid the necessary non-Gaussian step is to consider the transmission of Gaussian states through a non-Gaussian channel, i.e., the non-Gaussian operation is accomplished by the noisy channel himself. In particular, we considered the erasure channel which either transmits information perfectly or erases it with a given probability. Remarkably, we have shown that coherent states can be perfectly protected from such errors provided that the occurrence of erasure can be probed and highly entangled two-mode squeezed vacuum can be prepared. These two requirements being experimentally challenging, we have also shown how to transform this erasure-correcting code into an erasure-filter based on postselection. Our filter can efficiently detect and discard polluted output states, and is shown to be very performant with currently available two-mode squeezed vacuum. Furthermore, since error-correction is known to be connected with entanglement distillation, we explored in **Appendix E** the possibility to convert our error-filter into an experimentally feasible distillation protocol. The preliminary results are very encouraging, but we have yet to rigorously prove that our proposed protocol increases entanglement. Nevertheless, the introduction of feasible protocols to distribute continuous-variable entanglement over (large) distances, using either error-correction or entanglement distillation, is an important step towards the realization of an efficient quantum communication network based on optical continuous variables. Our results demonstrate that such network can greatly benefit from the experimental simplicity of Gaussian operations. However, many natural decoherence processes are Gaussian, hence restricting communications to non-Gaussian channels is a strong limitation. We thus conclude this second part by noting that the great potential of optical continuous variables will only be fully realized the day we masterize efficiently (and at a low cost) a few key non-Gaussian operations.

Appendices

A

N-Partite Unextendible Product Bases

A.1 From Nonlocality Without Entanglement to Unextendible Product Bases

Consider a n-partite quantum system belonging to $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$, with the local Hilbert spaces of respective dimensions d_i. An Unextendible Product Basis, or UPB in short, is an incomplete orthogonal product basis whose complementary subspace contains no product state (see Fig. A.1).

Interestingly, Unextendible Product Bases are closely connected to nonlocality without entanglement. More precisely, it is shown in [12, 27] that the members of a UPB cannot be perfectly distinguished if one is restricted to LOCC only, i.e. they exhibit nonlocality without entanglement. On the other hand, a necessary and sufficient condition for the extendibility of a product basis is also known, and this condition can be used to construct a UPB from a complete product basis exhibiting NLWE. Starting from the SHIFT ensemble (4.6) for example, one can use this method to construct the following UPB [12, 29]

$$\begin{aligned}
|\Psi_4\rangle &= |0\rangle_a|1\rangle_b|0-1\rangle_c \\
|\Psi_6\rangle &= |0-1\rangle_a|0\rangle_b|1\rangle_c \\
|\Psi_7\rangle &= |1\rangle_a|0-1\rangle_b|0\rangle_c \\
|\Psi_{\mathrm{st}}\rangle &= |0+1\rangle_a|0+1\rangle_b|0+1\rangle_c
\end{aligned} \tag{A.1}$$

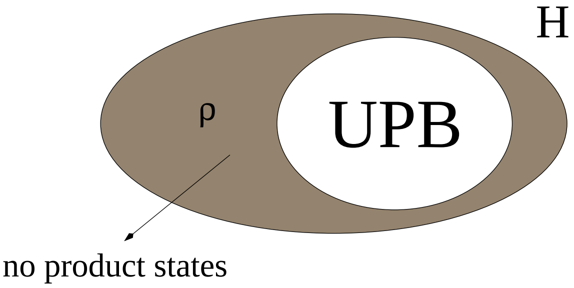

Figure A.1: *Representation of an unextendible product bases in a Hilbert space H, and the associated bound entangled state ρ.*

where the extra state $|\Psi_{st}\rangle$ is the *stopper* state whose role will be explained later on. Interestingly, our systematic method of creating product bases exhibiting NLWE can be easily transformed into a systematic construction of UPBs based on the quantum circuits introduced in Sec. 4.5. This circuit based approach probably does not account for the construction of all possible UPB, but it nevertheless enables the construction of a large family of UPBs in a variety of scenarios.

A.2 Examples

Let us illustrate this construction with a simple example. Consider the quadripartite circuit of Fig. 4.4 and suppose Alice, Bob, Charles, and Damian hold systems of dimension d_a, d_b, d_c, and d_d, respectively. This circuit generates an ensemble $\{|\Psi_i\rangle\}$ made of $d_a d_b d_c d_d$ orthogonal product states exhibiting NLWE. To construct an UPB out of $\{|\Psi_i\rangle\}$, we extract the $d_a - 1$ states in which Alice's share is any state of the DB except the last one, the $d_b - 1$ states in which Bob's share is any state of the DB except the last one, the $d_c - 1$ states in which Charles' share is any state of the DB except the last one, and the $d_d - 1$ states in which Damian's share is any state of the DB except the last one. We complete these $\sum_{i=1}^{4}(d_i - 1)$ states by adding a proper *stopper* state, so as to force the unextendibility of the set. Note that the number of states m in a UPB is known to verify [12]

$$m \geq \sum_{i=1}^{n}(d_i - 1) + 1 \qquad \text{(A.2)}$$

so that the above construction yields a minimal UPB. More specifically, the UPB consists of the following states

$$
\begin{aligned}
|\Psi_1^0\rangle &= |0\rangle_a|1\rangle_b|2\rangle_c F|0\rangle_d \\
&\vdots \\
|\Psi_1^{d_d-2}\rangle &= |0\rangle_a|1\rangle_b|2\rangle_c F|d_d-2\rangle_d \\
\\
|\Psi_2^0\rangle &= |1\rangle_a|2\rangle_b F|0\rangle_c|0\rangle_d \\
&\vdots \\
|\Psi_2^{d_c-2}\rangle &= |1\rangle_a|2\rangle_b F|d_c-2\rangle_c|0\rangle_d \\
\\
|\Psi_3^{0\rangle} &= |2\rangle_a F|0\rangle_b|0\rangle_c|1\rangle_d \\
&\vdots \\
|\Psi_3^{d_b-2}\rangle &= |2\rangle_a F|d_b-2\rangle_b|0\rangle_c|1\rangle_d \\
\\
|\Psi_4^0\rangle &= F|0\rangle_a|0\rangle_b|1\rangle_c|2\rangle_d \qquad\qquad\qquad\qquad (A.3) \\
&\vdots \\
|\Psi_4^{d_a-2}\rangle &= F|d_a-2\rangle_a|0\rangle_b|1\rangle_c|2\rangle_d \\
\\
|\Psi_{\rm st}\rangle &= F|d_a-1\rangle_a F|d_b-1\rangle_b F|d_c-1\rangle F|d_d-1\rangle
\end{aligned}
$$

where $F|i\rangle$ is the Discrete Fourier Transform of $|i\rangle$. To understand why this set is unextendible, suppose we want to add a new product state that is orthogonal to it. Clearly, because of the $d_a - 1$ states that are in the DB for Alice together with the stopper sate, we cannot find a state orthogonal to Alice's share (this subset of d_a states span her entire subspace). So, we should try to look for a product state that is orthogonal to this set within Bob's, Charles' or Damian's subspaces. But the same argument holds for their subspaces too, hence no product state can be found that is orthogonal to all the states, i.e. the set is unextendible.

B

N-partite Bound Entangled States

Interestingly, unextendible product bases are connected to another important quantum property called Bound Entanglement. A Bound Entangled (BE) state is an entangled mixed state from which no pure entanglement can be distilled [61, 62]. The role of bound entanglement in nature, and its yet-to-find possible use for quantum information processing has attracted a lot of attention lately. Although the construction of bound entangled states has proven to be a difficult task, it was recently realized that the state corresponding to the uniform mixture on the subspace orthogonal to an UPB $\{|\tilde{\psi}_i\rangle, i = 1, \cdots m\}$, namely

$$\hat{\rho} = \frac{1}{D-m}\big(1 - \sum_{i=1}^{m} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\big) \tag{B.1}$$

is a bound entangled state [12], where D is the total dimension of the Hilbert space. This is one of the only known generic method to construct bound entangled states. The quantum circuit formalism introduced in Chapter 4 provides a simple strategy to construct a large number of UPBs, hence it also provides a simple method to construct a large number of BE states. As an example, consider the quadripartite UPB defined in Appendix A (Eq. (A.3)). By definition, the space complementary to this UPB contains no product states, hence $\hat{\rho}$ is entangled. We can use the partial transposition to show that every partitioning of the parties is PPT: indeed, the identity is invariant under partial transposition and the product states $|\tilde{\psi}_i\rangle$ of the UPB are mapped onto other product states. Thus, no entanglement can be distilled across any bipartite cut. In addition, note that if some pure global entanglement could nevertheless be distilled, it could be used to create entanglement across a bipartite cut; hence no entanglement at all can be distilled and the state is indeed bound entangled.

In the special case where the exclusivity condition Eq. (4.7) is saturated, i.e., when $n = d+1$ parties hold each a system of dimension d, we can prove the following theorem:

Theorem B.0.1 *When $d+1$ parties each hold a system of dimension d, the BE state produced by our method has zero entanglement across any $d \otimes d^d$ cut.*

Note that this result, already known for the special case of the SHIFT ensemble [12], is stronger than the nondistillability of bipartite entanglement across any $d \otimes d^d$ cut.

Proof We first explicitly separate Alice from the other parties and rewrite the d^2 states of the UPB as

$$\begin{aligned}
|\Psi_{1,i}\rangle &= |0\rangle|a_i\rangle, \qquad |a_i\rangle = |1, 2, \ldots, d-2, F(i)\rangle \\
|\Psi_{2,i}\rangle &= |1\rangle|b_i\rangle, \qquad |b_i\rangle = |2, \ldots, d-2, F(i), 0\rangle \\
&\vdots \\
|\Psi_{d,i}\rangle &= |d-1\rangle|e_i\rangle, \quad |e_i\rangle = |F(i), 0, \ldots, d-3\rangle \\
|\Psi_{d+1,i}\rangle &= |F(i)\rangle|f\rangle, \quad |f\rangle = |0, \ldots, d-1\rangle \\
|\Psi_{st}\rangle &= |F(d-1)\rangle|g\rangle, |g\rangle = |F(d-1), \ldots, F(d-1)\rangle
\end{aligned}$$

where $i = 0, \ldots, d-2$, and $F(i)$ means $F|i\rangle$.

Next, we note that $|f\rangle$ and $|g\rangle$ span a Hilbert space S =span(f,g) of dimension 2, and that all the states in this space are orthogonal to $\{|a_i\rangle, |b_i\rangle, \ldots, |e_i\rangle\}$. We thus define the Hilbert space $S' = \mathcal{H}(d^d)/S$ of dimension $d^d - 2$ such that (i) all the states in this space are, by construction, orthogonal to $|f\rangle$ and $|g\rangle$; and (ii) all the states $\{|a_i\rangle, |b_i\rangle, \ldots, |e_i\rangle\}$ are in S'. We can therefore find an ensemble of $d^d - d - 1$ orthogonal vectors $|a_k^\perp\rangle$ such that every $|a_k^\perp\rangle$ belongs to S' and is orthogonal to all the $|a_i\rangle$, i.e. $\{|a_i\rangle, |a_k^\perp\rangle\}$ is an orthogonal basis of S'. We repeat that procedure for the $\{|b_i\rangle\}$ and define $d^d - d - 1$ vectors $|b_k^\perp\rangle$ in S', until we have defined the last $d^d - d - 1$ vectors $|e_k^\perp\rangle$ associated to the states $\{|e_i\rangle\}$. In addition, we can also define $|f^\perp\rangle$ and $|g^\perp\rangle$ in S, orthogonal to $|f\rangle$ and $|g\rangle$ respectively. We can now use all these new vectors to complete the original UPB and make it a full d^{d+1}-dimensional product basis between A and BC...E. This is done by adding the $d(d^d - d - 1) + (d-1) + 1 = d^{d+1} - d^2$

new states $\{|0\rangle|a_k^{\perp}\rangle, |1\rangle|b_k^{\perp}\rangle, \ldots, |d-1\rangle|e_k^{\perp}\rangle, |F(i)\rangle|f^{\perp}\rangle, |F(d-1)\rangle|g^{\perp}\rangle\}$. This shows that with respect to the cut A and BC...E, the set is completable by product states and the mixed state $\hat{\rho}$ is therefore not entangled. Because the state is symmetric, this argument also applies to the other $d \otimes d^d$ splits which completes the proof, i.e., our generic bound entangled state contains no entanglement across any such cuts. ■

C

CV Secret Sharing

In classical cryptography, secret sharing refers to a method for distributing a secret amongst a group of n players, each of which is allocated a share of the secret. The shares are chosen in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold secret sharing scheme. A typical application of secret sharing consist of a boss and three untrusted employees. The boss wants his employees to access the voucher of the company provided that two or mode collaborate.

The quantum version of secret sharing uses quantum states to encode the message [25, 53]. In contrary to classical secret sharing, quantum secret sharing is constrained by the no-cloning theorem, i.e. in any (t, n)-threshold quantum secret sharing scheme, $t > n/2$. Interestingly, there is a connection between quantum secret sharing an quantum erasure correction. Indeed, any erasure correcting code is a quantum secret sharing protocol where the secret is distributed using the encoder, and can be decoded using the decoder. As an example, consider the erasure-correcting scheme presented in Sec. 7.3. The secret, the input coherent states $|\psi_{sec}\rangle = |\alpha\rangle\,|\beta\rangle$, can be distributed to the four players using the circuit of Fig. 7.2.b . As the protocol can tolerate one erasure, every group of three player can recover the secret using the circuit depicted in Fig. 7.3.b, and our erasure correcting code is the first (3,4)-threshold CV quantum secret sharing protocol. We note that a (2,3)-threshold CV quantum secret sharing protocol which resemble ours was proposed in [96] and later demonstrated experimentally [69]. However, in their implementation, the message was recovered up to an unfeasible unitary operation. As our protocol can be fully implemented with nowadays technology, it is thus the first truly experimentally feasible CV quantum secret sharing protocol.

D

Manipulating Wigner functions

D.1 Partial Trace

Consider a bipartite gaussian state ρ_{AB} of displacement vector and covariance matrix d_{AB} and γ_{AB} respectively. In phase-space representation, tracing mode B corresponds to integrating the Wigner function W_{AB} over the quadratures (x_B, p_B). However, this operation can be achieved much easily at the level of characteristic functions. If ρ_{AB} has a characteristic function $\chi_{AB}(\xi_A, \xi_B)$, $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ has a characteristic function

$$\begin{aligned}
\chi_A(\xi_A) &= \mathrm{Tr}_A[\rho_A D_A(\xi_A)] && \text{(D.1)}\\
&= \mathrm{Tr}_A[\mathrm{Tr}_B(\rho_{AB})\ D_A(\xi_A)] && \text{(D.2)}\\
&= \mathrm{Tr}_A[\mathrm{Tr}_B[\rho_{AB}\ D_A(\xi_A) \otimes \mathbb{1}_B]] && \text{(D.3)}\\
&= \mathrm{Tr}_{AB}[\rho_{AB}\ D_A(\xi_A) \otimes D_B(0)] && \text{(D.4)}\\
&= \chi_{AB}(\xi_A, 0). && \text{(D.5)}
\end{aligned}$$

Using the relation (2.82) for the characteristic function of a gaussian state, one concludes that ρ_A is a gaussian state of covariance matrix γ_A, where γ_A is the diagonal block of γ_{AB} corresponding to mode A

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix} \longrightarrow \gamma_A, \tag{D.6}$$

and displacement vector d_A, with

$$d_{AB} = (d_A, d_B) \longrightarrow d_A. \tag{D.7}$$

D.2 Conditional measurement

Consider a two-mode gaussian state ρ_{AB} with Wigner function $W_{AB}(r_A, r_B)$, and a measurement of the quadrature x_B with an ideal homodyne detector. If the result is x_m, the Wigner function of mode A after the measurement is

$$W_A(r_A|x_m) = \int \mathrm{d}p_B W_{AB}(r_A, x_m, p_B). \tag{D.8}$$

Recalling the result of the previous section, we partition the covariance matrix γ_{AB} with respect to the traced over quadrature p_B

$$\gamma_{AB} = \begin{pmatrix} \gamma' & B \\ B^T & b \end{pmatrix} \tag{D.9}$$

and write the Wigner function as

$$W_A(r_A|x_m) = \frac{\sqrt{\det(\gamma')^{-1}}}{\pi^{3/2}} \exp[-(r'-d')^T(\gamma')^{-1}(r'-d')]\,, \tag{D.10}$$

where $r' = (r_A, x_m)$ and $d' = (d_A, d_{x_B})$. To isolate the quadratures of the remaining mode A, we further partition γ' with respect to the measured quadrature x_B

$$(\gamma')^{-1} = \Gamma' = \begin{pmatrix} \Gamma'' & E \\ E^T & e \end{pmatrix}. \tag{D.11}$$

The Wigner function simplifies to

$$\begin{aligned} W_A(r_A|x_m) = {} & \frac{1}{\pi^{3/2}}\sqrt{\frac{\det\Gamma'}{\det\Gamma''}}\ \exp[-\delta_{x_B} F \delta_{x_B}] \\ & \times \frac{\sqrt{\det\Gamma''}}{\pi} \exp[-(r_A - d'_A)^T\Gamma''(r_A - d'_A)] \end{aligned} \tag{D.12}$$

after the introduction of

$$\delta_{x_B} = x_m - d_{x_B} \tag{D.13}$$

$$F = d - E^T(\Gamma'')^{-1}E \tag{D.14}$$

$$d'_A = d_A - (\Gamma'')^{-1}E\delta_{x_B} \tag{D.15}$$

In other words, mode A is a gaussian state of covariance matrix $\gamma'_A = (\Gamma'')^{-1}$ and displacement vector d'_A. Note that d'_A depends on the measured value x_m, while γ'_A does not, and that the Wigner function (D.12) is not normalized. The probability to measure x_m is

$$P(x_m) = \int \mathrm{d}r_A\ W_A(r_A|x_m). \tag{D.16}$$

D.3 Single-mode Fidelity

Suppose we have two single-mode gaussian states with Wigner functions

$$W_1(r) = \frac{\sqrt{\det \Gamma_1}}{\pi} \exp[-(r-d_1)^t \Gamma_1 (r-d_1)] \tag{D.17}$$

$$W_2(r) = \frac{\sqrt{\det \Gamma_2}}{\pi} \exp[-(r-d_2)^t \Gamma_2 (r-d_2)] \tag{D.18}$$

where $r = (x, p)$, and $\Gamma_i = \gamma_i^{-1}$ is the inverse of the covariance matrix of mode i. Their fidelity reads

$$\begin{aligned} F &= 2\pi \int dr\ W_1(r) W_2(r) & \text{(D.19)} \\ &= \frac{2\sqrt{\det \Gamma_1 \Gamma_2}}{\pi} \int \mathrm{d}r\ \exp[-(r-d_1)^t \Gamma_1 (r-d_1) - (r-d_2)^t \Gamma_2 (r-d_2)] \\ &= \frac{2\sqrt{\det \Gamma_1 \Gamma_2}}{\pi} \exp[\Delta(d_1, \Gamma_1, d_2, \Gamma_2)] \int \mathrm{d}r\ \exp[-(r-d')^t (\Gamma_1 + \Gamma_2)(r-d')] \\ & & \text{(D.20)} \end{aligned}$$

after the introduction of

$$d' = (\Gamma_1 + \Gamma_2)^{-1} (\Gamma_1 d_1 + \Gamma_2 d_2) \tag{D.21}$$

$$\Delta(d_1, \Gamma_1, d_2, \Gamma_2) = d'^t (\Gamma_1 + \Gamma_2) d' - (d_1^t \Gamma_1 d_1 + d_2^t \Gamma_2 d_2). \tag{D.22}$$

Now, remember that Wigner functions are normalized. It follows that the integral of (D.20) yields

$$\int \mathrm{d}r\ \exp[-(r-d')^t (\Gamma_1 + \Gamma_2)(r-d')] = \frac{\pi}{\sqrt{\det(\Gamma_1 + \Gamma_2)}} \tag{D.23}$$

from which we deduce

$$F = 2\sqrt{\frac{\det \Gamma_1 \Gamma_2}{\det(\Gamma_1 + \Gamma_2)}} \exp[\Delta(d_1, \Gamma_1, d_2, \Gamma_2)]. \tag{D.24}$$

Note that $\Delta(d_1, \Gamma_1, d_2, \Gamma_2) = 0$ when $d_1 = d_2$, hence for two gaussian state with same center in phase-space, the fidelity simplifies to

$$F = 2\sqrt{\frac{\det \Gamma_1 \Gamma_2}{\det(\Gamma_1 + \Gamma_2)}}. \tag{D.25}$$

E

Entanglement Distillation

E.1 Introduction

Entanglement is a key ressource for many quantum information protocols. The teleportation of quantum states, for example, requires Alice and Bob to share an entangled state, and the performances of the protocol strongly rely on the quality of this entangled pair. In practice, the transmission channel between Alice and Bob is always noisy and imperfect, hence the entanglement they can share is limited and polluted. Fortunately, fighting these imperfections and nevertheless establish a good entangled pair over the noisy channel is made possible by a technique called entanglement distillation.

The idea of entanglement distillation is to extract from a large number of weakly entangled mixed state a smaller number of highly entangled almost pure states. Recall that Alice and Bob are spatially separated, hence the operations allowed in the protocol are restricted to local operations and classical communications only (LOCC). Regardless of the importance of entanglement distillation for the future of QIS, only a few experimentally feasible protocols are known in the continuous variable regime, and none has been succesfuly demonstrated yet. This is a direct consequence of the famous no-go theorem for Gaussian entanglement distillation. This theorem, established simultaneously in [35, 39, 46], states the impossibility to distil Gaussian entangled states with local Gaussian operations only. Recall that we used this theorem to establish the no-go theorem for gausssian error-

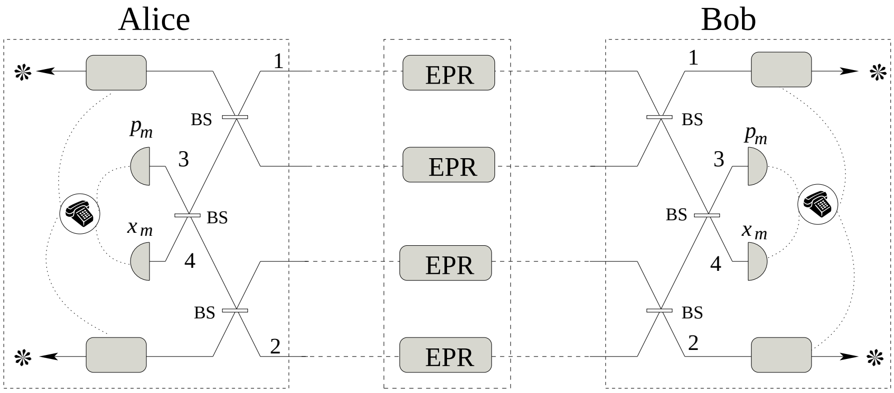

Figure E.1: *Experimentally feasible distillation protocol. BS: Beam splitter, EPR: two-mode squeezed vacuum.*

correction introduced in Chapter 6

To avoid the use of experimentally hard non-Gaussian operations such as in [36], but nevertheless distil entanglement with Gaussian operations only, research has recently focused on non-Gaussian channels. In [41, 40], the authors exploit the known connection between error correction and entanglement distillation to transform a purification protocol for phase-diffused squeezed states into an experimentally feasible entanglement distillation protocol. Inspired by this result, we are tempted to convert the erasure-correcting code presented in chapter 7. In particular, we will concentrate on the probabilistic protocol of Sec. 7.4 as it is closer from a realistic implementation.

E.2 Optical Setup

Let us first note that our erasure-correcting code can improve the distribution of entanglement as one can use it to distribute and protect one-half of an entangled two-mode squeezed state. Second, at least in theory, it can be transformed into an entanglement distillation protocol according to the scheme of Fig. 6.2. However, this latter scheme is far from an experimentally feasible setup.

To obtain a protocol that is feasible with today's technology, we introduce the optical setup of Fig. E.1 which uses four noisy entangled states to possibly produce two more entangled ones. We thus call this protocol a (4 → 2)-entanglement distillation protocol. The distillation works as follows. A preparator, located between Alice and Bob, prepares four two-mode squeezed vacuum and distributes them through the erasure channel. After reception of the modes, Alice and Bob share four weakly entangled non-gaussian states. To distil entanglement, they both mix their four modes

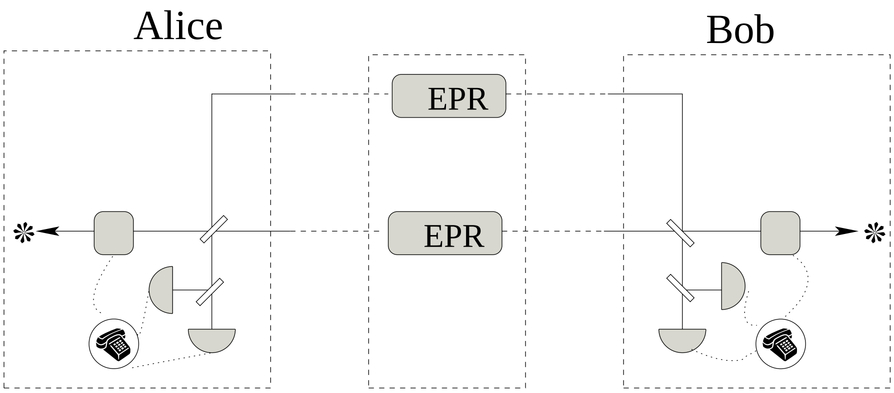

Figure E.2: *Experimentally feasible distillation protocol, a simpler version. BS: Beam splitter, EPR: two-mode squeezed vacuum.*

using three balanced beam splitters, then measure the x and p quadrature of modes 2 and 3 respectively. Next, Alice and Bob compare their values, and keep the two remaining output states according to some threshold condition. When their measurement result is (x_m^A, p_m^A) and (x_m^B, p_m^B) for Alice and Bob respectively, the chosen condition reads

$$\begin{aligned} |x_m^A - x_m^B| &< X_{th} \\ |p_m^A + p_m^B| &< P_{th}. \end{aligned} \tag{E.1}$$

Remarkably, considering the simplified erasure-filter of Fig. 7.8 as our starting point, we can also introduce an even simpler distillation setup in which Alice and Bob receive two noisy entangled states, mix their shares at a balanced beam splitter, measure both conjugate quadratures of one of the output mode (heterodyne detection), and post-select the output state according to the threshold condition (E.1). This (2 → 1)-entanglement distillation protocol is illustrated in Fig. E.2. Interestingly, it is equivalent to the protocol introduced in [40], up to the detection scheme; our protocol uses heterodyne detection, while theirs is based on homodyne detection.

E.3 Performances

The entanglement of the initial Gaussian two-mode squeezed vacuum is fully quantified by the EPR variance

$$\Delta_{EPR} = \langle(\Delta x_-)^2\rangle + \langle(\Delta p_+)^2\rangle \tag{E.2}$$

where

$$x_- = (x_A - x_B)/\sqrt{2} \tag{E.3}$$

$$p_+ = (p_A + p_B)/\sqrt{2} \tag{E.4}$$

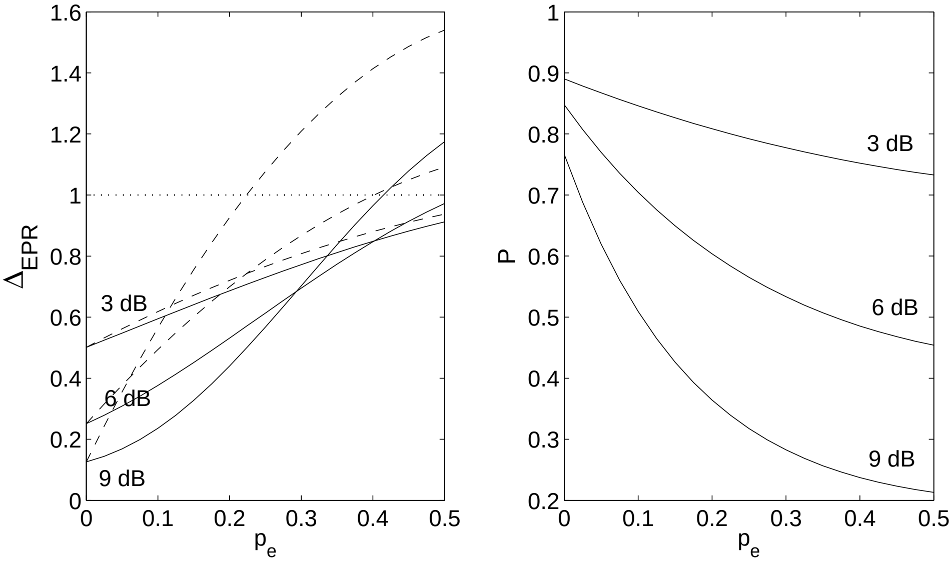

Figure E.3: *Performances of the* $(4 \rightarrow 2)$*-entanglement distillation protocol for various degrees of entanglement of the input two-mode squeezed vacuum. Left: EPR variance as a function of the erasure probability. Right: Probability of success as a function of the erasure probability. All curves are plotted with* $X_{th} = P_{th} = e^{-r}$*,* $\eta_{HD} = 0.9$ *and* $n_e = 0$*.*

are two commuting quadratures of the bipartite state. When the state is entangled, these two quadratures are squeezed and

$$\Delta_{EPR} < 1. \tag{E.5}$$

Strictly speaking, the EPR variance is not an entanglement measure for non-Gaussian states. Nevertheless, the criterion (E.5) is a necessary condition of entanglement [30], which quantifies the amount of nonlocal correlations between the two modes of the state. With respect to a true entanglement measures such as the logarithmic negativity, the EPR variance holds the advantage of being easily measured experimentally, and easily computable theoretically based on the Wigner function.

The performances of the $(4 \rightarrow 2)$-entanglement distillation protocols are illustrated in Fig. E.3. Note that, as for the erasure-filter of chapter 7, imperfect detectors have been simulated by a beam splitter preceding an ideal detector, and the chosen threshold condition is $X_{th} = P_{th} = e^{-r}$ where r is the squeezing parameter of the input two-mode squeezed vacuum. As expected, we clearly observe a decrease of the EPR variance for three different input entanglement. We note that the $(2 \rightarrow 1)$-entanglement distillation protocol exhibits very similar performances, except from a slightly lower probability of success.

However, in order to rigorously prove that our two protocols increase entanglement, the entanglement should be quantified by a proper entanglement measure such as the logarithmic negativity (2.25). Unfortunately, this calculation has to be done based in the Fock state basis as computing the logarithmic negativity of a state requires the knowledge of its spectrum. This makes the numerical simulations much more complicated, and we have not succeeded in this last step yet.

E.4 Conclusion

The erasure-filter introduced in chapter 7 can be easily converted into an experimentally feasible entanglement distillation protocol. According to the EPR variance, the resulting protocol does improve the distribution of entanglement over the erasure-channel. However, the EPR variance is not a proper entanglement measure for non-Gaussian states, hence future work should consider a true entanglement measure such as the logarithmic negativity in order to rigorously demonstrate the benefit of our proposed optical setup. Furthermore, we have not yet considered iterative procedures, neither did we characterized the purity of the output entangled states. All these questions should be addressed in order to seriously evaluate the performances of the proposed entanglement distillation protocols.

Bibliography

[1] U.L. Andersen, V. Josse and G. Leuchs, *Unconditional Quantum Cloning of Coherent States with Linear Optics*, Phys. Rev. Lett. **94**, 240503 (2005).

[2] U.L. Andersen, R. Filip, J. Fiurášek, V. Josse, and G. Leuchs, *Experimental purification of coherent states*, Phys. Rev. A **72**, 060301(R) (2005).

[3] A. Aspect, P. Grangier, and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. **47**, 460 (1981).

[4] A. Aspect, J. Dalibard, and G. Roger, *Experimental Test of Bell's Inequalities Using Time-Varying Analyzers*, Phys. Rev. Lett. **49**, 1804 (1982).

[5] A. Aspect, P. Grangier, and G. Roger, *Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities*, Phys. Rev. Lett. **49**, 91 (1982).

[6] S.D. Bartlett, B.C. Sanders, S.L. braunstein, and K. Nemoto, *Efficient Classical Simulation of Continuous Variable Quantum Information Processes*, Phys. Rev. Lett. **88**, 097904 (2002).

[7] J.S. Bell, *On the Einstein-Podolsky-Rosen Paradox*, Physics **1**, 195-200 (1964).

[8] C. H. Bennett and G. Brassard, *Quantum cryptography: Public-key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, (IEEE Press, 1984), pp. 175-179.

[9] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett. **70**, 1895-1899 (1993).

[10] C.H. Bennett and S.J. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Phys. Rev. Lett. **69**, 2881 (1992).

[11] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, and W.K. Wootters, *Quantum nonlocality without entanglement*, Phys. Rev. A **59**, 1070 (1999).

[12] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B. M. Terhal , *Unextendible Product Bases and Bound Entanglement*, Phys. Rev. Lett. **82**, 5385, (1999).

[13] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54**, 3824 (1996).

[14] W.P. Bowen, N. Treps, R. Schnabel, and P.K. Lam, *Experimental Demonstration of Continuous Variable Polarization Entanglement*, Phys. Rev. Lett. **89**, 253601 (2002).

[15] S.L. Braunstein, C.A. Fuchs, and H.J. Kimble, *Criteria for continuous-variable quantum teleportation*, J. Mod. Opt. **47**, 267 (2000).

[16] S. L. Braunstein and H. J. Kimble, *Dense coding for continuous variables*, Phys. Rev. A **61**, 042302 (2000).

[17] S.L. Braunstein, *Squeezing as an irreducible resource*, quant-ph/9904002 (1999).

[18] V. Buzek, M. Hillery, and R.F. Werner, *Optimal manipulations with qubits: Universal-NOT gate*, Phys. Rev. A **60**, R2626 (1999).

[19] E.G. Cavalcanti, C.J. Foster, M.D. Reid, and P.D. Drummond, *Bell Inequalities for Continuous-Variable Correlations*, Phys. Rev. Lett. **99**, 210405 (2007).

[20] N.J. Cerf, G. Leuchs, and E.S. Polzik, *Quantum Information with Continuous Variables of Atoms and Light*, Imperial College Press (2007).

[21] N.J. Cerf, and S. Iblisdir, *Phase conjugation of continuous quantum variables*, Phys. Rev. A **64**, 032307 (2001).

[22] N. J. Cerf and C. Adami, *Negative Entropy and Information in Quantum Mechanics*, Phys. Rev. Lett. **76**, 5194 (1997).

[23] Z.B. Chen, J.W. Pan, G. Hou, and Y.D. Zhang, *Maximal Violation of Bells Inequalities for Continuous Variable Systems*, Phys. Rev. Lett. **88**, 040406 (2002).

[24] J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett. **23**, 880 (1969).

[25] R. Cleve, D. Gottesman, and H.K. Lo, *How to Share a Quantum Secret*, Phys. Rev. Lett. **83**, 648 (1999).

[26] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, Whiley-Interscience, New York (1991).

[27] S. De Rinaldis, *Distinguishability of complete and unextendible product bases*, Phys. Rev. A **70**, 022309 (2004).

[28] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. London, Ser. A **400**, 97 (1985).

[29] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B. M. Terhal , *Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement*, Comm. Math. Phys. **238**, 379 (2003).

[30] L-M. Duan, G. Giedke, J.I. Cirac, and P. Zoller, *Inseparability Criterion for Continuous Variable Systems*, Phys. Rev. Lett. **84**, 2722 (1999).

[31] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[32] A. Einstein, *Über Einen die Erzeugung und Verwandlung des Lichtes Betreffenden Heuristischen Gesichtpunkt* Ann. D. Phys. **17**, 132 (1905).

[33] A. Einstein, *Die Plancksche Theorie der Strahlung und die Theorie der Spezifischen Wärme*, Ann. D. Phys. **22**, 180 (1907).

[34] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935).

[35] J. Eisert, S. Scheel, and M.B. Plenio, *Distilling Gaussian States with Gaussian Operations is Impossible*, Phys. Rev. Lett. **89**, 137903 (2002).

[36] J. Eisert, D.E. Browne, S. Scheel, and M.B. Plenio, *Distillation of continuous-variable entanglement with optical means*, Ann. Phys. (NY) **311**, 431 (2004).

[37] A. Ferraro and M.G.A. Paris, *Nonlocality of two- and three-mode continuous variable systems*, J. Opt. B **7**, 174 (2005).

[38] J. Fiurášek, S. Iblisdir, S. Massar, and N.J. Cerf, *Quantum cloning of orthogonal qubits*, Phys. Rev. A **65**, 040302(R) (2002).

[39] J. Fiurášek, *Gaussian Transformations and Distillation of Entangled Gaussian States*, Phys. Rev. Lett. **89**, 137904 (2002).

[40] J. Fiurášek, P. Marek, R. Filip, and R. Schnabel, *Experimentally feasible purification of continuous-variable entanglement*, Phys. Rev. A **75**, 050302(R) (2007).

[41] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurášek, and R. Schnabel, *Experimental Demonstration of Continuous Variable Purification of Squeezed States*, Phys. Rev. Lett. **97**, 150505 (2006).

[42] S.J. Freedman and J.F. Clauser, *Experimental test of local hidden-variable theories*, Phys. Rev. Lett. **28**, 938 (1972).

[43] A. Furusawa, J. Sorensen, S.L. Braunstein, C. Fuchs, J. Kimble, and E. Polzik, *Unconditional quantum teleportation*, Science **282**, 706 (1998).

[44] R. García-Patrón Sánchez, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, *Proposal for a Loophole-Free Bell Test Using Homodyne Detection*, Phys. Rev. Lett. **93**, 130409 (2004).

[45] R. García-Patrón Sánchez, J. Fiurášek, and N.J. Cerf, *Loophole-free test of quantum nonlocality using high-efficiency homodyne detectors*, Phys. Rev. A **71** 022105 (2005).

[46] G. Giedke, and J.I. Cirac, *Characterization of Gaussian operations and distillation of Gaussian states*, Phys. Rev. A, **66** 032316 (2002).

[47] R.M. Gingrich, P. Kok, H. Lee, F. Vatan, and J.P. Dowling, *All Optical Quantum Memory based on Quantum Error Correction*, Phys. Rev. Lett. **91**, 217901 (2000).

[48] V. Giovannetti, S. Lloyd, L. Maccone, J.H. Shapiro, and B.J. Yen, *Minimum Rényi and Wehrl entropies at the output of bosonic channels*, Phys. Rev. A **70**, 022328 (2004).

[49] N. Gisin and H. Bechmann-Pasquinucci, *Bell inequality, Bell states and maximally entangled states for n qubits*, Phys. Lett. A **246**, 1 (1998).

[50] N. Gisin, and S. Popescu, *Spin Flips and Quantum Information for Antiparallel Spins*, Phys. Rev. Lett. **82**, 432 (1999).

[51] N. Gisin, N. Linden, S. Massar, and S. Popescu, *Error filtration and entanglement purification for quantum communication*, Phys. Rev. A **72**, 012338 (2005).

[52] O. Glöckl, U.L. Andersen, and G. Leuchs, *Verifying continuous-variable entanglement of intense light pulses*, Phys. Rev. A **73**, 012306 (2006).

[53] D. Gottesman, *Theory of quantum secret sharing*, Phys. Rev. A **61**, 042311 (2000).

[54] M. Grassl, T. Beth, and T. Pellizari, *Codes for the quantum erasure channel*, Phys. Rev. A **56**, 33 (1997).

[55] D.M. Greenberger, M.A. Horne, and A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos (Ed.), Kluwer, Dordrecht, 69-72 (1989).

[56] B. Groisman and L. Vaidman, *Nonlocal variables with product-state eigenstates*, J. Phys. A **34**, 6881 (2001).

[57] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, *Quantum key distribution using Gaussian-modulated coherent states*, Nature **421**, 238 (2003).

[58] K. Hammerer, M.M Wolf, E.S. Polzik, and J.I. Cirac, *Quantum Benchmark for Storage and Transmission of Coherent States*, Phys. Rev. Lett. **94**, 150503 (2005).

[59] J. Heersink, Ch. Marquardt, R.D. Dong, R. Filip, S. Lorenz, G. Leuchs, and U.L. Andersen, *Distillation of Squeezing from Non-Gaussian Quantum States*, Phys. Rev. Lett. **96**, 253601 (2006).

[60] A.S. Holevo and R.F. Werner, *Evaluating capacities of bosonic Gaussian channels* , Phys. Rev. A **63**, 032312 (2001).

[61] P. Horodecki, *Separability criterion and inseparable mixed states with positive partial transposition*, Phys. Lett. A **232**, 333 (1997).

[62] M. Horodecki, P. Horodecki and R. Horodecki, *Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?*, Phys. Rev. Lett. **80**, 5239 (1998).

[63] www.idquantique.com

[64] A. Jamiolkowski, *Linear transformations which preserve trace and positive semidefiniteness of operators*, Rep. Math. Phys. **3**, 275 (1972).

[65] E.R. Jeffrey, J.B. Altepeter, M. Colci, and P.G. Kwiat, *Optical Implementation of Quantum Orienteering*, Phys. Rev. Lett. **96**, 150503 (2006).

[66] V. Josse, M. Sanbuncu, N.J. Cerf, G. Leuchs, and U.L. Andersen, *Universal Optical Amplification without Nonlinearity*, Phys. Rev. Lett. **96**, 163602 (2006).

[67] D.N. Klyshko, Phys. Lett. A **172**, 399 (1993).

[68] D. Kraszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski and A. Zeilinger, *Violations of Local Realism by Two Entangled N-Dimensional Systems Are Stronger than for Two Qubits*, Phys. Rev. Lett. **85**, 4418 (2000).

[69] A. Lance, T. Symul, W. Bowen, B. Sanders, and P. Lam, *Tripartite Quantum State Sharing*, Phys. Rev. lett. **92**, 177903 (2004).

[70] R. Landauer, *Irreversibility and Heat Generation in the Computing Process*, IBM J. Res. Develop. **5**, 3 (1961).

[71] M. Lassen, M. Sabuncu, P. Buchhave, and U.L. Andersen, *Generation of polarization squeezing with periodically poled KTP at 1064 nm*, Opt. Exp. **15**, 5077 (2007).

[72] S. Massar and S. Popescu, *Optimal Extraction of Information from Finite Quantum Ensembles*, Phys. Rev. Lett. **74**, 1259 (1995).

[73] D.N. Matsukevich, P.Maunz, D.L. Moehring, S.Olmschenk, and C. Monroe, *Bell Inequality Violation with Two Remote Atomic Qubits*, Phys. Rev. Lett. **100**, 150404 (2008).

[74] N.D. Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Phys. Rev. Lett. **65**, 1838 (1990).

[75] G.E. Moore, *Cramming more components onto integrated circuits*, Electronics **38**, 8 (1965).

[76] W.J. Munro, *Optimal states for Bell-inequality violations using quadrature-phase homodyne measurements*, Phys. Rev. A **59**, 4197 (1999).

[77] H. Nha, and H.J. Carmichael, *Proposed Test of Quantum Nonlocality for Continuous Variables*, Phys. Rev. Lett. **93**, 020401 (2004).

[78] M.A. Nielsen and I.C. Chuang, *Quantum Computation and Quantum Information* CUP, Cambridge, 2002.

[79] J. Niset and N.J. Cerf, *Tight bounds on the concurrence of quantum superpositions*, Phys. Rev. A **76**, 042328 (2007).

[80] J. Niset, U.L. Andersen and N.J. Cerf, *Experimentally feasible quantum erasure-correcting code for continuous variables*, arxiv:0710.4858 (2007).

[81] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier, *Generation of a Superposition of Odd Photon Number States for Quantum Information Networks*, Science **312**, 83 (2006).

[82] V. Parigi, A. Zavatta, M. Kim, and M. Bellini, *Probing Quantum Commutation Rules by Addition and Subtraction of Single Photons to/from a Light Field*, Science **317**, 1890 (2006).

[83] P. Pearl, *Hidden-Variable Example Based upon Data Rejection*, Phys. Rev. D **2**, 1418 (1970).

[84] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht (1993).

[85] A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett. **77**, 1413 (1996).

[86] A. Peres and W.K. Wootters, *Optimal detection of quantum information*, Phys. Rev. Lett. **66**, 1119 (1991).

[87] M. Planck, *On the law of distribution of energy in the normal spectrum*, Ann. D. Phys. **4**, 553 (1901).

[88] G.J. Pryde, J.L. O'brien, A.G. White, and S.D. Bartlett, *Demonstrating Superior Discrimination of Locally Prepared States Using Nonlocal Measurements*, Phys. Rev. Lett. **94**, 220406 (2005).

[89] M. Reck, A. Zeilinger, H.J. Bernstein, and P. Bertani, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett. **73**, 58 (1994).

[90] M.A. Rowe, D. Ielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland, *Experimental violation of a Bell's inequality with efficient detection*, Nature (London), **409**, 791 (2001).

[91] E. Schrödinger, *Discussion of Probability Relations Between Separated Systems*, Proceedings of the Cambridge Philosophical Society **31**, 555-563 (1935) and **32**, 446-451 (1936).

[92] C.E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal **27**, 379 (1948).

[93] P.W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Sci. Statist. Comput. **26**, 1484 (1997).

[94] H.P. Stapp, Nuovo Cimento B **29**, 270 (1975).

[95] S. Stenholm, *Simultaneous measurement of conjugate variables*, Ann. Phys. (N.Y.) **218**, 233 (1992).

[96] A. Lance, T. Symul, W. Bowen, B. Sanders, T. Tyc, T. Ralph, and P. Lam, *Continuous-variable quantum-state sharing via quantum disentanglement*, Phys. Rev. A **71**, 033814 (2005).

[97] P. van Loock and S.L. Braunstein, *Greenberger-Horne-Zeilinger nonlocality in phase space*, Phys. Rev. A **63**, 022106 (2001).

[98] G. Vidal and R.F. Werner, *Computable measure of entanglement*, Phys. Rev. A **65**, 32314 (2002).

[99] J. Walgate, and L. Hardy, *Nonlocality, Asymmetry, and Distinguishing Bipartite States*, Phys. Rev. Lett. **89**, 147901 (2002).

[100] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, *Local Distinguishability of Multipartite Orthogonal Quantum States*, Phys. Rev. Lett. **85**, 4972 (2000).

[101] D.F. Walls and G.J. Milburn, *Quantum Optics*, Springer Study Edition (1995).

[102] J. Wenger, M. Hafezi, F. Grosshans, R. Tualle-Brouri, and P. Grangier, *Maximal violation of Bell inequalities using continuous-variable measurements*, Phys. Rev. A **67**, 012105 (2003).

[103] R.F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40**, 4277 (1989).

[104] C. Wittmann, D. Elser, U.L. Andersen, R. Filip, P. Marek and G. Leuchs, *Experimental Noiseless Filtering of Continuous-Variable Quantum Information*, quant-ph/07041918 (2007).

[105] S. Wiesner, *Conjugate coding*, ACM SIGACT News, 15(1):7888 (1983).

[106] J. Yoshikawa, Y. Miwa, A. Huck, U.L. Andersen, P. van Loock, and A. Furusawa, *Demonstration of a quantum nondemolition sum gate*, arXiv:0808.0551 (2008).