Quantum Hypothesis Testing: Theory and Applications to Quantum Sensing and Data Readout

Gaetana Spedalieri

PhD

University of York
Computer Science

March 2016

Abstract: In this thesis we investigate the theory of quantum hypothesis testing and its potential applications for the new area of quantum technologies. We first consider the asymmetric formulation of quantum hypothesis testing where the aim is to minimize the probability of false negatives and the main tool is provided by the quantum Hoeffding bound. In this context we provide a general recipe for computing this bound in the most important scenario for continuous variable quantum information, that of Gaussian states. We then study both asymmetric and symmetric quantum hypothesis testing in the context of quantum channel discrimination. Here we show how the use of quantum-correlated light can enhance the detection of small variations of transmissivity in a sample of photodegrabable material, while a classical source of light either cannot retrieve information or would destroy the sample. This non-invasive quantum technique might be useful to realize in-vivo and real-time probing of very fragile biological samples, such as DNA or RNA. We also show that the same principle can be exploited to build next-generation memories for the confidential storage of confidential data, where information can be read only by well-tailored sources of entangled light.

Contents

List of Figures

Acknowledgements

I would like to thank my supervisor Prof Sam Braunstein for his research guidance, encouragement and many helpful discussions. I am grateful to all the quantum information group at York for the help and support during my studentship.

Author's Declaration

This work has not been submitted for any other qualification at this, or any other institution. The work presented is my own except where explicitly indicated and cited. Part of the work in Chapter 3 has been already published in the international journals Physical Review A and Entropy. Another part of Chapter 3 is to be submitted to Physical Review A.

Chapter 1

Introduction

1.1 General scope of the thesis

Quantum technologies represent one of the most exciting fields of investigation, attracting the interest of many research groups all over the world, as well as the interest of research funding bodies and the first big financial investors [11]. Broadly speaking, quantum technology is that vast interdisciplinary area where the unique and powerful features of quantum mechanics [59] are exploited to improve the performance of practical tasks with direct application to technology. From this point of view, quantum information [45] is regarded as a prominent science, for its revolutionary approach to use quantum systems to speed up computing [65], improve the security of communications [28], and allow for new techniques for manipulating and transmitting information [7,8,13,26]. In particular, the latest development has been given by the field of "continuous variable" quantum information, which considers quantum systems with infinite-dimensional Hilbert spaces, as the optical modes of the electromagnetic field, described in terms of position and momentum quadratures. The states of these systems have equivalent phase-space representations and are typically Gaussian [78].

Here we consider one of the central topics in quantum information, which is quantum hypothesis testing (QHT). This topic is first introduced as a problem of quantum state discrimination [5,18], where two (or more) states of a quantum system must be distinguished by means of a quantum measurement. This problem has closed analytical solutions and a series of bounds which are easy to compute. More interesting and advanced is the problem of quantum channel discrimination [1,19,20, 32,58], where we aim to distinguish between two (or more) transformations acting on the states of a quantum system, and the optimal strategy involves an optimization on both input states and output measurements. The general solution of this problem is an open question, therefore representing a rich area of research. The application of this problem to practical examples, as modeling the sensing of far and noisy targets, a protocol known as "quantum illumination" [31,41,64,73,75,81], or the readout of digital memories, a protocol known as "quantum reading" [10, 22, 30, 34, 44, 50, 53], has demonstrated the possibility of non-trivial boosts based on the use of quantum entanglement with respect to classical strategies.

In this thesis we aim to further extend this impact in quantum technology in several aspects. First, we develop a theory of asymmetric quantum state discrimination with Gaussian states. This means that we derive formulas which specifically evaluate the probability of false negatives, corresponding to the worst case scenario where an hypothesis (such as the presence of an illness) is true but the test provides a negative result (i.e., no illness is detected). These formulas are easily computable and represent a basic tool for asymmetric quantum sensing where the role of false positives is less important, such as in biomedical testing.

Second, we exploit this tool and also the approach of symmetric quantum hypothesis testing (where the two hypotheses have the same cost) to show that we can greatly improve the detection of loss at the low photon regime. This is important for non-invasive testing of a bacterial/cell samples. By modeling the probing of biological material as a problem of quantum channel discrimination, we show that the use of quantum entanglement may retrieve all the relevant information from the material while using a negligible amount of energy. This technique would be completely noninvasive, compared to the standard methods used in today's biological instruments (e.g., spectrophotometers), which are based on highly energetic thermal sources. In principle, our approach could pave the way for an in-vivo and real-time testing and analysis of highly photo-degradable material, which would otherwise be destroyed by standard spectroscopic techniques.

Finally, we show how the previous methods can be adapted and exploited to design classical memories where the storage of data is confidential. The use of a well-tailored entanglement source may enable the complete readout of data from an optical memory, while any other approach, e.g., with thermal or coherent state source, would destroy this data. Such a scheme introduces a new layer of technological security to data storage.

1.2 Specific contributions

Our first contribution regards the asymmetric formulation of quantum hypothesis testing, where two quantum hypotheses have different associated costs. In this problem, the aim is to minimize the probability of false negatives and the optimal performance is provided by the quantum Hoeffding bound. Here we show how this bound can be simplified for pure states. Most importantly, we provide a general recipe for its computation in the case of multimode Gaussian states, also showing its connection with other easier-to-compute lower bounds. In particular, we provide analytical formulas and numerical results for important classes of one- and two-mode Gaussian states. This paper has been published in Physical Review A as

"Asymmetric quantum hypothesis testing with Gaussian states" [G. Spedalieri, S. L. Braunstein, Phys. Rev. A 90, 052307 (2014)].

Our second contribution is the study of quantum sensing of loss (or attenuation) by considering both symmetric and asymmetric quantum hypothesis testing, by exploiting the tools of the quantum Chernoff bound and quantum Hoeffding bound, suitably formulated for Gaussian states and continuous variable systems. In both approaches the use of an entangled source, a so called Einstein-Podolsky-Rosen (EPR) state, is able to outperform the classical strategy based on coherent state transmitters, if we assume the regime of low photon numbers. By introducing phenomenological models of bacterial/cell growth and photo-degradability, we show how the quantum advantage can be made extreme for tasks such as the non-destructive testing of biological samples and the readout of classical memories. This paper is under submission to Physical Review A as "Quantum sensing of loss: Implications for biological testing and data storage" [G. Spedalieri et al.]

Our third contribution is related to a central issue in modern cryptography, i.e., the possibility to confidentially store information in a memory for later retrieval. Here we explore this possibility in the setting of quantum reading, which exploits quantum entanglement to efficiently read data from a memory whereas classical strategies (e.g., based on coherent states or their mixtures) cannot retrieve any information. From this point of view, the technique of quantum reading can provide a new form of technological security for data storage. This paper has been published in the journal Entropy as "Cryptographic aspects of quantum reading" [G. Spedalieri, Entropy 17, 2218-2227 (2015)].

1.3 Assumed knowledge

This thesis assume the language of quantum information with Gaussian states. The reader interested in deepening this knowledge may refer to very good reviews in the field, in particular Ref. [78]. In the appendix we also provide some preliminary notions that may be used to better understand the tools and notions used in this thesis.

Chapter 2

Literature review

The general field which is at the basis of this research work is continuous variable quantum information, in particular, its formulation with Gaussian states. These tools are discussed in our Appendix and they are also available in reviews on the field, such as Refs. [14, 78]. In this literature review we just recall some basic notions on Gaussian states and then we focus on the area of quantum hypothesis testing and its various formulations.

2.1 Basics of bosonic systems and Gaussian states

A bosonic system of n modes is a quantum system described by a tensor product Hilbert space $\mathcal{H}^{\otimes n}$ and a vector of quadrature operators [14, 15]

$$\hat{\mathbf{x}}^T := (\hat{q}_1, \hat{p}_1, \dots, \hat{q}_n, \hat{p}_n). \tag{2.1}$$

These operators satisfy the vectorial commutation relations

$$[\hat{\mathbf{x}}, \hat{\mathbf{x}}^T] := \hat{\mathbf{x}}\hat{\mathbf{x}}^T - (\hat{\mathbf{x}}\hat{\mathbf{x}}^T)^T = 2i\mathbf{\Omega} \ , \tag{2.2}$$

where $\mathbf{\Omega}$ is the symplectic form, defined as

$$\mathbf{\Omega} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} . \tag{2.3}$$

Correspondingly, a real matrix $\mathbf{S}$ is called ‘symplectic’ when it preserves $\mathbf{\Omega}$ by congruence, i.e., $\mathbf{S}\mathbf{\Omega}\mathbf{S}^T = \mathbf{\Omega}$.

By definition, we say that a bosonic state ρ is ‘Gaussian’ when its phase-space Wigner representation is Gaussian [78]. In such a case, we can completely describe the state by means of its first- and second-order statistical moments. These are the mean value or displacement vector $\bar{\mathbf{x}} := \mathrm{Tr}(\hat{\mathbf{x}}\rho)$, and the covariance matrix (CM) $\mathbf{V}$ with generic element

$$V_{ij} = \tfrac{1}{2}\mathrm{Tr}(\{\hat{x}_i, \hat{x}_j\}\rho) - \bar{x}_i\bar{x}_j \ , \tag{2.4}$$

where $\{,\}$ denotes the anticommutator. The CM is a $2n \times 2n$ real symmetric matrix, which must satisfy the uncertainty principle [78]

$$\mathbf{V} + i\mathbf{\Omega} \geq 0 \ . \tag{2.5}$$

An important tool in the manipulation of Gaussian states is Williamson's theorem [78]: For any CM $\mathbf{V}$, there is a symplectic matrix $\mathbf{S}$ such that

$$\mathbf{V} = \mathbf{S}\mathbf{W}\mathbf{S}^T \ , \tag{2.6}$$

where

$$\mathbf{W} = \bigoplus_{k=1}^{n} \nu_k \mathbf{I} \ , \ \mathbf{I} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{2.7}$$

The matrix $\mathbf{W}$ is the 'Williamson form' of $\mathbf{V}$, and the set $\{\nu_1, \cdots, \nu_n\}$ is the 'symplectic spectrum' of $\mathbf{V}$. According to the uncertainty principle, each symplectic eigenvalue must satisfy the condition $\nu_k \geq 1$, with $\nu_k = 1$ for all k if and only if the Gaussian state is pure.

2.2 Quantum State Discrimination

Quantum state discrimination [5, 18] is a quantum formulation of the statistical problem of hypothesis testing. The simplest formulation involves the discrimination of two arbitrary quantum states (binary discrimination). The scenario is the following: consider a quantum system which is prepared in some unknown quantum state ρ, which can be ρ_0 with a priori probability p_0 or ρ_1 with a priori probability $p_1 = 1 - p_0$. For instance we can imagine one party, say Alice, who prepares such a system. This system is then passed to Bob, who does not know which choice Alice made. Thus, Bob must solve a test with the following two hypotheses

$$\text{Null hypothesis } H_0 : \rho = \rho_0 \ , \tag{2.8}$$

$$\text{Alternative hypothesis } H_1 : \rho = \rho_1 \ . \tag{2.9}$$

In order to discriminate between these two hypotheses, i.e., distinguish between the two states, Bob applies a quantum measurement to the system, described by a general positive-operator valued measure (POVM) [45]. Without loss of generality, Bob can always reduce his measurement to be a dichotomic POVM $\{\Pi_k\}$ with $k = 0, 1$ [33]. The outcome $k = 0$, with POVM operator Π_0, is associated to the null hypotheses H_0, while the other outcome $k = 1$, with POVM operator $\Pi_1 = I - \Pi_0$, is associated with the alternative hypothesis H_1. Bob's aim is to apply the best possible dichotomic POVM to discriminate the two states, minimizing the probability of making an error. In fact, note that these states may be non-orthogonal, so that no POVM can achieve perfect discrimination.

As an example we may consider a Stern-Gerlach (SG) experiment [59]. If Alice prepares a spin-half particle (qubit) in spin up $|\uparrow\rangle$ or spin down $|\downarrow\rangle$ along the z direction, then Bob can always distinguish the two states using a magnetic field along the z direction. But, if Alice prepares a spin up $|\uparrow\rangle$ along z and spin up $|\rightarrow\rangle$ along x, these states are non-orthogonal and no SG experiment is able to distinguish them perfectly. For instance, using a magnetic field along the z-direction for SG device, the state

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \tag{2.10}$$

will give the same output of $|\uparrow\rangle$ half of the time.

In order to better characterize the discrimination problem and quantify its optimal performance, we first introduce the notions of type-I and type-II errors with their associated conditional error probabilities. By definition, the type-I error, also known as "false-positive", is when Bob accepts the alternative hypothesis H_1 when the null hypothesis H_0 holds. We have a corresponding error probability expressed by

$$\alpha := p(H_1|H_0) = \mathrm{Tr}(\Pi_1\rho_0). \tag{2.11}$$

Note that $p(H_1|H_0)$ is a compact notation for $p(\text{accept } H_1 \mid \text{holds } H_0)$. Then, the type-II error or "false-negative" is when Bob accepts the null hypothesis H_0 when the true hypothesis is the alternative H_1. This error occurs with conditional probability

$$\beta := p(H_0|H_1) = \mathrm{Tr}(\Pi_0\rho_1). \tag{2.12}$$

Note that we can introduce other probabilities, but they are fully determined by α and β. For instance, we may also consider the "specificity" or "true-negativity" of the test with probability

$$\alpha' := p(H_0|H_0) \tag{2.13}$$

which is simply given by

$$\alpha' = 1 - \alpha. \tag{2.14}$$

Then, we may also consider the "sensitivity" or "true-positivity" of the test with probability

$$\beta' := p(H_1|H_1) = 1 - \beta. \tag{2.15}$$

The costs associated with the two types of error can be very different especially in the medical and histological settings. For instance, in a medical test, H_0 is typically associated with no illness, while H_1 with the presence of the disease. It is therefore clear that we would like to have tests where the false negative probability (or rate) β is the lowest possible, so that ill patients are not diagnosed as healthy. For this reason, in a medical setting, hypothesis testing is asymmetric, meaning that we aim to minimize one of the two conditional error probabilities while imposing a constraint on the other.

However, in other settings, the two errors have the same importance, e.g., in the readout of a memory device where H_0 may be associated with the bit-value $u = 0$, and H_1 with the other bit-value $u = 1$. In this case, it makes sense to consider a symmetric test where we aim to jointly minimize the two error probabilities.

Here we start by discussing the general meaning of Bayesian cost in the setting of (quantum) hypothesis testing (Sec. 2.2.1). Then we review the specific case of symmetric testing in Sec. 2.2.2 and asymmetric testing in Sec. 2.2.3.

2.2.1 Bayesian cost

Let us provide a brief survey of the concept of Bayesian cost. We consider binary hypothesis testing, but the notion can easily be generalized and formulated for $N \geq 2$ different hypotheses. As we have seen before, Bob should distinguish between two hypotheses, H_0 (null) and H_1 (alternate), occurring with some a priori probabilities p_0 and p_1, respectively. In the quantum setting, these hypotheses are associated with two possible states, ρ_0 and ρ_1, taken by some quantum system. On this system, Bob performs a dichotomic POVM $\{\Pi_k\}$ with $k = 0, 1$.

Associated with the test, there is the conditional probability of accepting the hypothesis H_k when the actual hypothesis is H_i. In the quantum setting, this is expressed by the Born rule

$$p(H_k|H_i) = \mathrm{Tr}\left(\Pi_k \rho_i\right) \ . \tag{2.16}$$

Then, we can also introduce a "cost" matrix $\mathbf{C}$, whose generic element C_{ki} represents the 'cost' associated with conditional probability $p(H_k|H_i)$. In general, the goal of the binary test is to minimize the following Bayes' cost function

$$\mathcal{C}_{\mathrm{B}} := \sum_{i,k} C_{ki} \ p_i \ p(H_k|H_i) \ , \tag{2.17}$$

where p_0 and $p_1 = 1 - p_0$ are the a priori probabilities associated with the hypotheses H_0 and H_1.

In particular, we may choose

$$\mathbf{C} = \left(\begin{array}{cc} 0 & C_{01} \\ C_{10} & 0 \end{array} \right) \ , \tag{2.18}$$

so that

$$\mathcal{C}_{\mathrm{B}} = C_{10} \ p_0 \ p(H_1|H_0) + C_{01} \ p_1 \ p(H_0|H_1). \tag{2.19}$$

Depending on the cost of the errors, C_{01} and C_{10}, we may prefer symmetric or asymmetric testing. When the costs are the same ($C_{01} = C_{10} = 1$), we adopt symmetric hypothesis testing. Correspondingly, the cost function becomes equivalent to the mean error probability

$$\mathcal{C}_{\mathrm{B}} = P_{err} := p_0\ p(H_1|H_0) + p_1\ p(H_0|H_1). \tag{2.20}$$

By contrast, in case of completely unbalanced costs, such as $C_{01} = 1$ or $C_{10} = 0$, we adopt asymmetric hypothesis testing, with the cost function collapsing into the false-negative error probability, i.e., $\mathcal{C}_{\mathrm{B}} = p(H_0|H_1)$.

2.2.2 Symmetric testing

In symmetric testing type-I and type-II errors are equivalent (but not necessarily equiprobable). For this reason, the optimal performance corresponds to minimizing the average error probability [18]

$$P_{err} = p_0\alpha + p_1\beta = p_0 p(H_1|H_0) + p_1 p(H_0|H_1)\ . \tag{2.21}$$

In quantum state discrimination, this means that Bob's POVM $\{\Pi_0, \Pi_1\}$ must minimize

$$P_{err} = p_0 \operatorname{Tr}(\Pi_1\rho_0) + p_1 \operatorname{Tr}(\Pi_0\rho_1)\ . \tag{2.22}$$

Helstrom Bound

Symmetric state discrimination has a closed solution which is known as the "Helstrom bound" [33]. Given two states ρ_0 (with probability p_0) and ρ_1 (with probability p_1), Bob is able to distinguish them up to a minimum error probability

$$P_{err}^{\min} = \frac{1}{2}(1 - \|\gamma\|_1) \tag{2.23}$$

where

$$\gamma := p_0\rho_0 - p_1\rho_1 \tag{2.24}$$

is a non-positive Hermitian operator called the "Helstrom matrix" and

$$\|\gamma\|_1 := \operatorname{Tr}|\gamma| \tag{2.25}$$

is the trace-norm (providing a real number between 0 and 1).

In particular, Bob's optimal POVM $\{\Pi_0, \Pi_1 = I - \Pi_0\}$ is given by a projector Π_0 onto the positive part γ_+ of the Helstrom matrix γ [33] (we call this optimal detection the "Helstrom POVM"). To construct this detection, we may write the spectral decomposition of the Helstrom matrix as

$$\gamma = \sum_k \gamma_k\, |k\rangle\langle k| \tag{2.26}$$

then Π_0 is the projector

$$P(\gamma_+) = \sum_{\gamma_k^+} |k\rangle\langle k| \tag{2.27}$$

where the sum is limited to the positive eigenvalues γ_+.

From now on we consider the case where $p_0 = p_1 = 1/2$ which means that the two states (quantum hypotheses) are equiprobable

$$H_0 : \rho = \rho_0 \quad p_0 = \frac{1}{2}, \tag{2.28}$$

$$H_1 : \rho = \rho_1 \quad p_1 = \frac{1}{2}. \tag{2.29}$$

In this case the Helstrom matrix is given by

$$\gamma = \frac{1}{2}(\rho_0 - \rho_1) \tag{2.30}$$

and the minimum error probability takes the form

$$P_{err}^{\min} = \frac{1}{2}\left[1 - \frac{1}{2}\left\|\rho_0 - \rho_1\right\|_1\right] = \frac{1}{2}[1 - D(\rho_0, \rho_1)], \tag{2.31}$$

where $D(\rho_0, \rho_1)$ is the "trace-distance" between the two states. For $D = 0$, we have $\rho_0 = \rho_1$ and $P_{err}^{\min} = 1/2$ (random guessing), while for $D = 1$, we have orthogonal states $\rho_0 \perp \rho_1$ and $P_{err}^{\min} = 0$ (perfect discrimination).

A particular example is Peres' formula [48] for discriminating between two equiprobable pure states (kets) $|\varphi_0\rangle$ and $|\varphi_1\rangle$ of a qubit. In this case, the minimum error probability computed using the Helstrom bound provides the formula

$$P_{err}^{\min} = \frac{1 - \sin\frac{x}{2}}{2} \tag{2.32}$$

where x is the angle between the two kets on the Bloch sphere [45]. This angle is related to their fidelity [37], which is a way to quantify the similarity between the two states. In fact, their fidelity is given by

$$F := \left|\langle\varphi_0|\,\varphi_1\rangle\right|^2 = \cos^2\frac{x}{2}. \tag{2.33}$$

State discrimination as bit encoding/decoding

Note that a binary test where Alice prepares two equiprobable states ρ_0 and ρ_1 corresponds to encoding a bit of information $u = 0, 1$ in the quantum system. Correspondingly, Bob's state discrimination corresponds to decoding that bit from the system. Since the process is generally affected by an error-probability, Bob cannot retrieve all the information. There is a simple relation between the minimum error probability $P_{err}^{\min}$ affecting the state discrimination and the maximum amount of information $I_{\max}$ in the bit decoding. This is given by:

$$I_{\max} = 1 - H(P_{err}^{\min}) \in [0,1], \tag{2.34}$$

where

$$H(p) := -p\log_2 p - (1-p)\log_2(1-p) \tag{2.35}$$

is the binary Shannon Entropy. Note that

$$\text{Perfect discrimination: } P_{err}^{\min} = 0 \Rightarrow I_{\max} = 1 \text{ bit (full decoding)} \tag{2.36}$$

$$\text{Random guessing: } P_{err}^{\min} = \frac{1}{2} \Rightarrow I_{\max} = 0 \text{ bit (no decoding).} \tag{2.37}$$

This connection has been used in the protocols of quantum illumination [31, 41, 64, 73,75,81] of targets and quantum reading of digital memories [10,22,30,34,44,50,53].

Quantum Chernoff Bound

In general the Helstrom bound may be difficult to compute but we can use other bounds to provide an estimate of the minimum error probability $P_{err}^{\min}$. The most important one is the quantum Chernoff (QC) bound [3, 4, 46]. This is an upper bound

$$P_{err}^{\min} \leq P_{QC} \ , \tag{2.38}$$

which is defined as [3]

$$P_{QC} := \frac{1}{2} \inf_{s\in[0,1]} C_s \ , \tag{2.39}$$

where the generalized overlap C_s is given by

$$C_s := \mathrm{Tr}(\rho_0^s \rho_1^{1-s}) \leq 1. \tag{2.40}$$

Note that the QC bound is defined using an infimum in $[0,1]$ instead of a minimum because the generalized overlap C_s may have discontinuities at the border points $s = 0, 1$ where $C_0 = C_1 = 1$. Indeed, this happens when one of the two states is pure. For instance, if we have

$$\rho_0 = |\varphi_0\rangle\langle\varphi_0| \tag{2.41}$$

then

$$\inf_s C_s = \lim_{s\to 0^+} C_s. \tag{2.42}$$

Furthermore, in this special case, the QC bound is directly related to the quantum fidelity by the formula

$$P_{QC} = \frac{1}{2} F(|\varphi_0\rangle, \rho_1) \tag{2.43}$$

where

$$F(|\varphi_0\rangle, \rho_1) = \langle\varphi_0|\rho_1|\varphi_0\rangle. \tag{2.44}$$

Quantum Battacharyya Bound

If we ignore the minimization in s and we set $s = 1/2$, we derive a bound which it is easy to compute and helpful in the discrimination of mixed states. This is the quantum Battacharyya (QB) bound [52, 78]

$$P_{QC} \leq P_{QB} := \frac{1}{2}C_{\frac{1}{2}} = \frac{1}{2}\mathrm{Tr}[\sqrt{\rho_0}\sqrt{\rho_1}]. \tag{2.45}$$

This bound has been used to prove quantum illumination [73].

Fidelity Bounds

Additional bounds can be constructed using quantum fidelity, which is defined as [37]

$$F = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}\right)\right]^2 \tag{2.46}$$

for two arbitrary states ρ_0 and ρ_1. Then we may build the upper-bound [25]

$$P_{QB} \leq F_+ := \frac{1}{2}\sqrt{F} \tag{2.47}$$

and the lower-bound [25]

$$F_- := \frac{1-\sqrt{1-F}}{2} \leq P_{err}^{\min}. \tag{2.48}$$

In conclusion, we have a chain of inequalities

$$F_- \leq P_{err}^{\min} \leq P_{QC} \leq P_{QB} \leq F_+. \tag{2.49}$$

Formulas for Gaussian States

Given two equiprobable Gaussian states, ρ_0 and ρ_1, we have a closed formula for the computation of the generalized overlap

$$C_s := \mathrm{Tr}(\rho_0^s \rho_1^{1-s}) \tag{2.50}$$

which is involved in the definitions of the QC bound and QB bound.

Consider the general case of two n-mode Gaussian states $\rho_0(\bar{\mathbf{x}}_0, \mathbf{V}_0)$ and $\rho_1(\bar{\mathbf{x}}_1, \mathbf{V}_1)$ where their CMs can be decomposed as

$$\mathbf{V}_0 = \mathbf{S}_0 \ (\oplus_{k=1}^n \nu_k^0 \mathbf{I}) \ \mathbf{S}_0^T \tag{2.51}$$

$$\mathbf{V}_1 = \mathbf{S}_1 \ (\oplus_{k=1}^n \nu_k^1 \mathbf{I}) \ \mathbf{S}_1^T \tag{2.52}$$

where $\{\nu_k^0\}$ is the symplectic spectrum of $\mathbf{V}_0$, $\{\nu_k^1\}$ is the symplectic spectrum of $\mathbf{V}_1$, and $\mathbf{S}_0$, $\mathbf{S}_1$ are symplectic matrices.

The generalized overlap C_s can be written in terms of the mean values $\bar{\mathbf{x}}_0$ and $\bar{\mathbf{x}}_1$, and the symplectic decompositions $(\mathbf{S}_0, \{\nu_k^0\})$ and $(\mathbf{S}_1, \{\nu_k^1\})$ of the two CMs $\mathbf{V}_0$ and $\mathbf{V}_1$. In order to give this formulation, we first need to introduce the real functions

$$G_s(x) := \frac{2^s}{(x+1)^s - (x-1)^s} \tag{2.53}$$

and

$$\Lambda_s(x) := \frac{(x+1)^s + (x-1)^s}{(x+1)^s - (x-1)^s} \tag{2.54}$$

which are positive for any $x \geq 1$. Then, we also define the "symplectic action" of Λ_s over an arbitrary CM

$$\mathbf{V} = \mathbf{S}\ (\oplus_{k=1}^n \nu_k \mathbf{I})\ \mathbf{S}^T \tag{2.55}$$

as

$$\Lambda_s(\mathbf{V})_* = \mathbf{S}\ [\oplus_{k=1}^n \Lambda_s(\nu_k)\mathbf{I}]\ \mathbf{S}^T\ . \tag{2.56}$$

Given these preliminaries, we can now write the formula. For any $s \in [0,1]$, the generalized overlap has the Gaussian expression [52]

$$C_s = \frac{\Pi_s}{\sqrt{\det \mathbf{\Sigma}_s}} \exp\left[-\frac{\mathbf{d}^T \mathbf{\Sigma}_s^{-1} \mathbf{d}}{2}\right] \tag{2.57}$$

where

$$\mathbf{d} := \bar{\mathbf{x}}_0 - \bar{\mathbf{x}}_1\ , \tag{2.58}$$

$$\mathbf{\Sigma}_s := \Lambda_s(\mathbf{V}_0)_* + \Lambda_{1-s}(\mathbf{V}_1)_*\ , \tag{2.59}$$

and finally

$$\Pi_s := 2^n \Pi_{k=1}^n G_s(\nu_k^0) G_{1-s}(\nu_k^1)\ . \tag{2.60}$$

A particular case is represented by the discrimination of zero-mean Gaussian states ($\bar{\mathbf{x}}_0 = \bar{\mathbf{x}}_1 = \mathbf{0}$), for which the previous formula simplifies to

$$C_s = \frac{\Pi_s}{\sqrt{\det \mathbf{\Sigma}_s}}\ . \tag{2.61}$$

If we also consider single-mode states ($n = 1$), the symplectic spectra are made by a single eigenvalue and we can write the decompositions as

$$\mathbf{V}_0 = \mathbf{S}_0(\nu^0 \mathbf{I})\mathbf{S}_0^T = \nu^0 \mathbf{S}_0 \mathbf{S}_0^T, \tag{2.62}$$

$$\mathbf{V}_1 = \mathbf{S}_1(\nu^1 \mathbf{I})\mathbf{S}_1^T = \nu^1 \mathbf{S}_1 \mathbf{S}_1^T. \tag{2.63}$$

Then, we have

$$\mathbf{\Sigma}_s = \Lambda_s(\nu^0)\mathbf{S}_0\mathbf{S}_0^T + \Lambda_{1-s}(\nu^1)\mathbf{S}_1\mathbf{S}_1^T, \tag{2.64}$$

$$\Pi_s = 2^s G_s(\nu^0) G_{1-s}(\nu^1). \tag{2.65}$$

Finally, another important formula is the fidelity F between two Gaussian states $\rho_0(\bar{\mathbf{x}}_0, \mathbf{V}_0)$ and $\rho_1(\bar{\mathbf{x}}_1, \mathbf{V}_1)$, since the fidelity is used to construct two bounds for the minimum error probability $F_- \leq P_{err}^{\min} \leq F_+$. This formula is known in the case of single-mode Gaussian states, for which we have [60, 61]

$$F(\rho_0, \rho_1) = \frac{2}{\sqrt{\Delta + \delta} - \sqrt{\delta}} \exp\left[-\frac{1}{2}\mathbf{d}^T(\mathbf{V}_0 + \mathbf{V}_1)^{-1}\mathbf{d}\right] \tag{2.66}$$

where $\mathbf{d} := \bar{\mathbf{x}}_1 - \bar{\mathbf{x}}_0$, and

$$\Delta := \det(\mathbf{V}_0 + \mathbf{V}_1), \ \delta := \det(\mathbf{V}_0 - 1)\det(\mathbf{V}_1 - 1). \tag{2.67}$$

Multicopy state discrimination

Until now we have considered the problem of single-copy state discrimination, where a single system is prepared in two possible quantum states. In general we can extend the problem to M-copy discrimination [18]. This means that Alice has M quantum systems which are prepared in two equiprobable multi-copy states

$$\begin{aligned} H_0 : \rho = \rho_0^{\otimes M} = \rho_0 \otimes ... \otimes \rho_0 \ , \\ H_1 : \rho = \rho_1^{\otimes M} = \rho_1 \otimes ... \otimes \rho_1 \ . \end{aligned} \tag{2.68}$$

These systems are passed to Bob who performs a collective measurement on them. This general POVM can be chosen to be dichotomic as before. The optimal POVM is the Helstrom POVM which is a projector onto the positive part of the M-copy Helstrom matrix

$$\gamma = \rho_0^{\otimes M} - \rho_1^{\otimes M}. \tag{2.69}$$

Correspondingly the minimum error probability is given by the Helstrom bound which now takes the multicopy form [33]

$$P_{err}^{\min}(M) = \frac{1}{2}\left[1 - D(\rho_0^{\otimes M}, \rho_1^{\otimes M})\right]. \tag{2.70}$$

It is typical to study the asymptotic behavior for large M. In this limit ($M \gg 1$) we have an exponential decay of the error probability

$$P_{err}^{\min}(M) \simeq \frac{1}{2}e^{-M\kappa} \tag{2.71}$$

where κ is called the "error-rate exponent". Apart from the singular case where the two states are identical $\rho_0 = \rho_1$ (for which $\kappa = 0$), the error-rate exponent κ is strictly positive and therefore the error probability is a decreasing exponential in the number of copies M.

For any number of copies M, we can define the multicopy QC bound which provides an upperbound to $P_{err}^{\min}(M)$. This is defined as [3]

$$P_{QC}(M) = \frac{1}{2}\left[\inf_{s\in[0,1]} C_s\right]^M . \tag{2.72}$$

We may also consider the multicopy QB bound, which is given by [52]

$$P_{QB}(M) = \frac{1}{2}\left(C_{\frac{1}{2}}\right)^M . \tag{2.73}$$

Here it is important to note that these bounds (QC and QB) are easy to compute because the generalized overlap is still computed over the single-copy states, i.e., $C_s = \mathrm{Tr}(\rho_0^s \rho_1^{1-s})$, with the number of copies M only appearing as a power in the formulas.

Similarly we can also extend the fidelity bounds to multicopy discrimination which become [25]

$$F_+(M) = \frac{1}{2}F^{\frac{M}{2}},\ F_-(M) = \frac{1-\sqrt{1-F^M}}{2}, \tag{2.74}$$

where the fidelity F is evaluated over the single-copy states ρ_0 and ρ_1. Thus, we have the following chain of bounds for the multicopy discrimination

$$F_-(M) \leq P_{err}^{\min}(M) \leq P_{QC}(M) \leq P_{QB}(M) \leq F_+(M). \tag{2.75}$$

For large M we find that the QC bound is asymptotically tight, i.e.,

$$P_{err}^{\min}(M) \simeq P_{QC}(M) \text{ for } M \gg 1. \tag{2.76}$$

More precisely, the QC bound has exactly the same error-rate exponent κ which characterizes the asymptotic decay of the error probability. In other words, we have

$$P_{QC}(M) \simeq e^{-M\kappa}, \quad \text{for large } M. \tag{2.77}$$

Explicitly the error-rate exponent can be expressed as

$$\kappa = -\lim_{M\to+\infty} \frac{1}{M} \ln P_{QC}(M) = -\ln\left(\inf_s C_s\right) . \tag{2.78}$$

2.2.3 Asymmetric testing

As we have previously discussed, in asymmetric testing one hypothesis is more important than the other, i.e., false negatives must be avoided. For this reason, we are interested in minimizing the error probability β of false negatives (type-II errors) given some constraint $\alpha < \varepsilon$ for the probability of false positives (type-I errors). We formulate the problem of asymmetric state discrimination directly in the setting of multi-copy states. Consider the following two hypotheses (without a priori probabilities)

$$\begin{aligned} H_0 : \rho = \rho_0^{\otimes M} \ , \\ H_1 : \rho = \rho_1^{\otimes M} \ . \end{aligned} \tag{2.79}$$

The system in the unknown quantum state ρ is detected by a collective dichotomic POVM $\{\Pi_0, \Pi_1 = I - \Pi_0\}$ which provides the correct answer up to conditional error probabilities.

The probability of false positives (type-I errors) is the probability of accepting the alternative hypothesis H_1 despite the null hypothesis H_0 being true

$$\alpha_M = p(H_1|H_0) = \mathrm{Tr}(\Pi_1 \rho_0^{\otimes M}). \tag{2.80}$$

The probability of false negatives (type-II errors) is the probability of accepting the null hypothesis H_0 despite the alternative H_1 being true

$$\beta_M = p(H_0|H_1) = \mathrm{Tr}(\Pi_0 \rho_1^{\otimes M}). \tag{2.81}$$

In the limit of a large number of copies ($M \gg 1$), these probabilities go to zero exponentially. We are then interested in their asymptotic error-rate exponents, also called “rate limits”, which are defined as [4]

$$\alpha_R = - \lim_{M \to +\infty} \frac{1}{M} \ln \alpha_M \ , \tag{2.82}$$

$$\beta_R = - \lim_{M \to +\infty} \frac{1}{M} \ln \beta_M \ . \tag{2.83}$$

Bob’s aim is to maximize the rate-limit β_R, so that the error probability of false negatives β_M has the fastest exponential decay to zero.

Here one of the most important results is the “quantum Stein lemma” [4] which connects β_R with the quantum relative entropy between the single-copy states ρ_0 and ρ_1. For large number of copies M, there is a dichotomic POVM such that the error probability of the false positives is bounded

$$\alpha_M \leq \varepsilon \ \text{ for any } 0 < \varepsilon < 1, \tag{2.84}$$

and the error probability of false negatives goes to zero with error-exponent

$$\beta_R = S(\rho_0 || \rho_1) = \mathrm{Tr}\rho_0(\ln \rho_0 - \ln \rho_1). \tag{2.85}$$

Another important result is the quantum Hoeffding bound [4]. For many copies $M \gg 1$, there is a dichotomic POVM such that the rate-limit of false positives

$$\alpha_R \geq r \text{ for any } r > 0 \tag{2.86}$$

and the rate limit of false negatives satisfies $\beta_R = H(r)$, where

$$H(r) := \sup_{0 \leq s < 1} \frac{-r\ s - \ln C_s}{1 - s} \tag{2.87}$$

with $C_s := \mathrm{Tr}(\rho_0^s \rho_1^{1-s})$ being the usual generalized overlap between the single-copy states ρ_0 and ρ_1. Note that the quantum Hoeffding bound enforces a stronger constraint on the error probability of false-positives.

2.3 Quantum Channel Discrimination

Until now we have considered the problem of quantum state discrimination where a system is prepared in one of two different quantum states by Alice and then subject to a quantum detection by Bob, with the aim of determining the chosen state. The problem was to identify the best quantum measurement and the minimum error probability (average error probability in symmetric testing and false-negative error probability in asymmetric testing).

Quantum channel discrimination [1, 19, 20, 32, 58, 78] is a more complex problem since Alice now chooses between different quantum channels. Recall that a quantum channel is a suitable linear transformation which maps input states into output states (see Appendices for more details). In the case of quantum channel discrimination, finding the optimal strategy involves an optimization on all possible input states of the unknown channel and all possible measurements at its output. In other words, we need to solve a double-optimization problem, by adapting the mathematical tools developed for the theory of quantum state discrimination.

2.3.1 Basic model

The simplest model consists of Alice choosing between two equiprobable quantum channels $\mathcal{E}_0$ and $\mathcal{E}_1$. This is equivalent to encoding a bit of information $k = 0, 1$ into a binary ensemble of channels $\{\mathcal{E}_k\}$. Alice's choice is stored in a input-output black-box which is then passed to Bob (see Fig. 2.1).

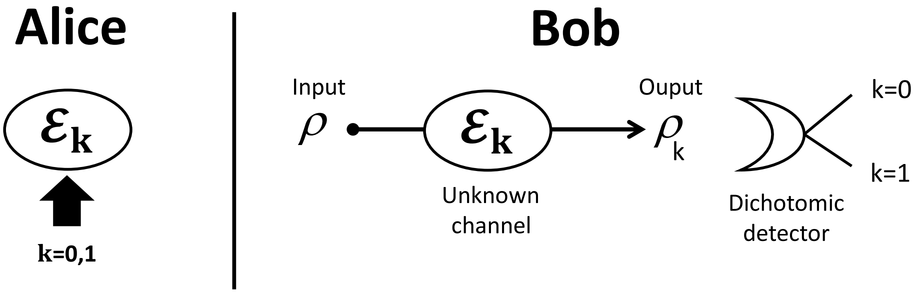

Figure 2.1: Basic model of quantum channel discrimination. (**Left**) Alice encodes a bit k into an ensemble of channels $\{\mathcal{E}_k\}$, i.e., she chooses one of two equiprobable channels $\mathcal{E}_0$ and $\mathcal{E}_1$, storing her choice in a box. (**Right**) Bob use an input state ρ and an output dichotomic detector $\{\Pi_k\}$ to discriminate between the two possible channels in the box. For a given input the ensemble of channels $\{\mathcal{E}_k\}$ is mapped into an ensemble of output states $\{\rho_k\}$ for which the optimal detection is known.

The aim of Bob is to discriminate between the two possible channels present in the box, i.e., to decode Alice's bit $k = 0, 1$. To achieve this, Bob feeds the box with a system prepared in some known quantum state ρ and measures the output by applying a dichotomic POVM $\{\Pi_0, \Pi_1\}$, as shown in Fig. 2.1. The problem is to find the optimal discrimination strategy which means optimizing Bob's decoding strategy on both the input state ρ and the output POVM $\{\Pi_k\}$. For simplicity we can approach this problem in two steps, one step having a closed solution, the other step being an open question.

The first step consists of fixing the input ρ state. In this case, channel discrimination becomes a problem of state discrimination, since the ensemble $\{\mathcal{E}_k\}$ of the two channels is mapped into an ensemble made by two possible output states $\{\rho_k\}$ with $\rho_k = \mathcal{E}_k(\rho)$. This part of the problem has a known solution since the optimal POVM is Helstrom's and the minimum error probability is determined by the trace distance of the output states

$$P_{e,\min}(\rho) = \frac{1}{2}\left[1 - D(\rho_0, \rho_1)\right]. \tag{2.88}$$

Now, the second step is the optimization over the input state ρ. In other words the minimum error probability affecting the channel discrimination $\mathcal{E}_0 \neq \mathcal{E}_1$ is given by minimizing the Eq. (2.88) over all input states ρ, i.e.,

$$P_{e,\min} = \min_{\rho} P_{e,\min}(\rho). \tag{2.89}$$

The open question in channel discrimination is to find this optimal value, as well as the optimal input state ρ_{opt}. Once this question has been answered the optimal output detection is automatically found, since it is the Helstrom POVM relative to the discrimination of the output states $\mathcal{E}_0(\rho_{opt})$ and $\mathcal{E}_1(\rho_{opt})$.

2.3.2 Multicopy channel discrimination

We can extend the process from one-copy to many-copy probing of the box [41,73,78]. This means considering M systems prepared in the M-copy input state

$$\rho^{\otimes M} = \underbrace{\rho \otimes ... \otimes \rho}_{M}. \tag{2.90}$$

Each copy ρ is transformed by the unknown channel $\mathcal{E}_k$, so that the global output state is an M-copy state of the form

$$\rho_k^{\otimes M} = \rho_k \otimes ... \otimes \rho_k, \quad \text{where } \rho_k = \mathcal{E}_k(\rho). \tag{2.91}$$

This multi-copy output is finally detected by a collective measurement, which can be taken to be a dichotomic POVM (see Fig. 2.2).

The minimum error probability will now depend on the number M of copies and is given by the multi-copy Helstrom bound.

$$P^{(M)}_{e,\min}(\rho) = \frac{1}{2}\left[1 - D(\rho_0^{\otimes M}, \rho_1^{\otimes M})\right]. \tag{2.92}$$

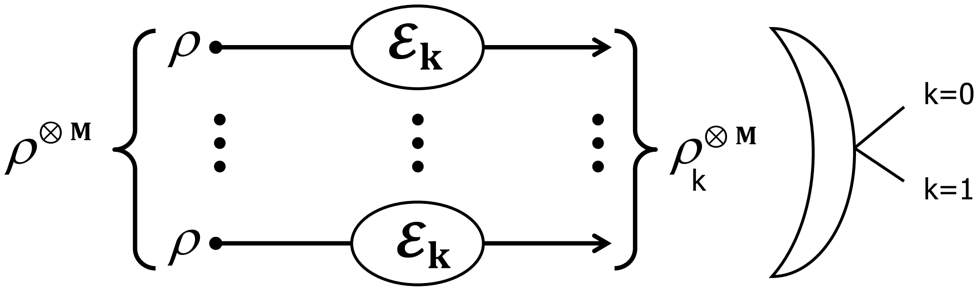

Figure 2.2: Multicopy channel discrimination

In order to achieve the optimal discrimination of the two channels $\{\mathcal{E}_0, \mathcal{E}_1\}$ we must minimize the previous quantity over all input states

$$P_{e,\min}^{(M)} = \min_{\rho} P_{e,\min}^{(M)}(\rho). \tag{2.93}$$

2.3.3 Assisted channel discrimination

The most general formulation of the problem of quantum channel discrimination involves an input state $\rho^{(M,L)}$ consisting of M signal systems (used to probe the box) and additional L idler systems (which are directly sent to assist the output detection) [41, 73, 78]. The output state takes the form

$$\rho_k = (\mathcal{E}_k^{\otimes M} \otimes I^{\otimes L})\rho^{(M,L)} \tag{2.94}$$

where the M signals are transformed by the channel $\mathcal{E}_k^{\otimes M} = \mathcal{E}_k \otimes ... \otimes \mathcal{E}_k$, while the idlers are all subject to the identity. At the output, a dichotomic POVM is collectively applied to all the signal and idler systems. See Fig. 2.3 for a schematic.

For a given input $\rho^{(M,L)}$ we have the conditional error probability

$$P_{e,\min}[\rho^{(M,L)}] = \frac{1}{2}\left[1 - D(\rho_0, \rho_1)\right]. \tag{2.95}$$

The optimal performance of channel discrimination is achieved by optimizing over all the inputs

$$P_{e,\min}^{(M,L)} = \min_{\rho^{(M,L)}} P_{e,\min}[\rho^{(M,L)}]. \tag{2.96}$$

Note that this description is very general and can be specified to various particular cases by fixing the values of M and L. For instance, we have

- Single-copy unassisted strategy for $M = 1$ and $L = 0$,
- Single-copy assisted strategy for $M = L = 1$,
- Multi-copy unassisted strategy for $M > 1$ and $L = 0$, with $\rho^{(M)} = \rho^{\otimes M}$

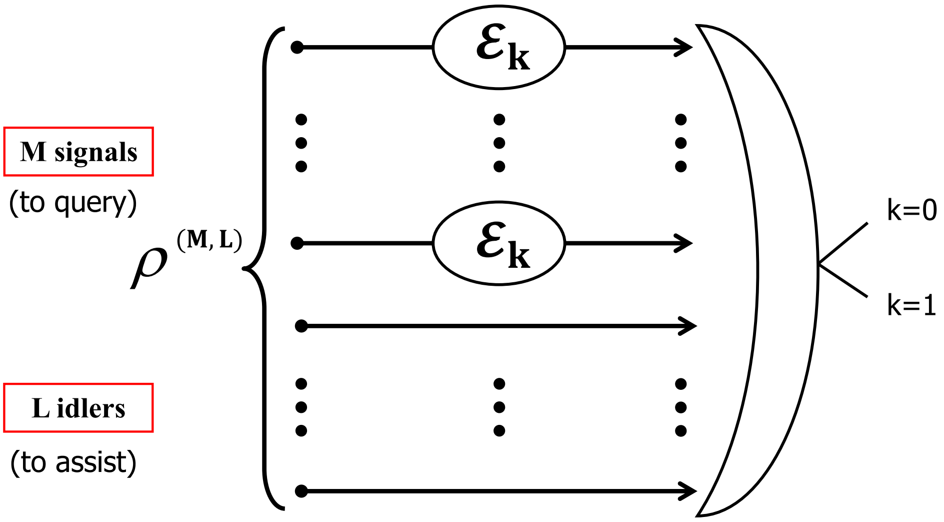

Figure 2.3: Assisted channel discrimination with M signals and L idlers

- Multi-copy assisted strategy for $M = L > 1$ and $\rho^{(M,M)} = \rho_{SI}^{\otimes M} = \rho_{SI} \otimes ... \otimes \rho_{SI}$, where each copy is a bipartite state ρ_{SI} of a signal system S and an idler system I.

2.3.4 Bosonic Channel Discrimination

Now we consider the problem of channel discrimination in the case of bosonic systems where each signal and idler is described by a mode (e.g., an optical wave). In particular, the bosonic channels we seek to discriminate are assumed to be Gaussian channels. The simplest case is the discrimination between the identity channel $\mathcal{E}_0 = I$ and a pure-loss channel $\mathcal{E}_1 = \mathcal{E}_\tau$ with transmissivity $\tau \in [0,1]$ (which is equivalent to a beam-splitter with an environmental vacuum state).

It is important to note that the problem of bosonic channel discrimination is non-trivial only if we impose an energetic constraint on the input to the box. In fact, if we are allowed to use arbitrarily high energy, then we can always perfectly discriminate between two channels $\mathcal{E}_0 \neq \mathcal{E}_1$ by using a single input mode. For instance, in the discrimination of I and $\mathcal{E}_\tau$, we could use a coherent input state $\rho_\alpha = |\alpha\rangle\langle\alpha|$, giving the two possible outputs

$$\rho_0 = I\left(|\alpha\rangle\langle\alpha|\right) = |\alpha\rangle\langle\alpha| \ , \tag{2.97}$$

$$\rho_1 = \mathcal{E}_1\left(|\alpha\rangle\langle\alpha|\right) = \left|\sqrt{\tau}\alpha\rangle\langle\sqrt{\tau}\alpha\right| \ . \tag{2.98}$$

Now even for τ close to 1, we could use a very energetic coherent state with an amplitude α large enough so that the output energies

$$E_0 = |\alpha|^2 \, , \; E_1 = \tau \, |\alpha|^2 \tag{2.99}$$

become very different. It is clear that in the limit of $|\alpha|^2 \to +\infty$ we can perfectly discriminate the two output energies and therefore the two channels in the box.

By contrast the problem becomes highly non-trivial when we impose an energetic constraint on the input. In this case perfect discrimination is generally not possible and we need to identify the optimal input state which satisfies the constraint. From a practical point of view, the energetic constraint is also important when the box to probe is a fragile sample, e.g., highly photo-degradable as is the case of specific biological molecules (RNA etc.). In the following section, we then formulate bosonic channel discrimination as a constrained optimization problem.

General formulation with constrained energy

As shown in Fig. 2.4, we consider an input state which irradiates M signal modes on the box plus additional L modes sent to the output detector. In particular, the total energy of the signal modes is constrained to be equal to $\bar{N}$ average number of photons. This means that each signal mode carries an average of $\bar{N}/M$ mean photons. For a given input state or transmitter $\rho^{(M,L,\bar{N})}$ we have two possible output states $\rho_k = (\mathcal{E}_k^{\otimes M} \otimes I^{\otimes L})[\rho^{(M,L,\bar{N})}]$.

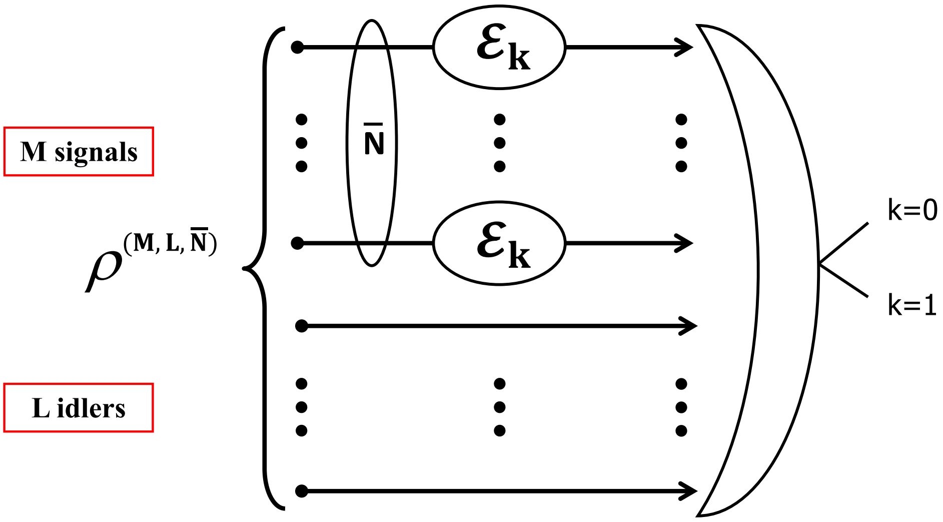

Figure 2.4: Bosonic channel discrimination with energetic constraint on the signal modes.

From the two output states, ρ_0 and ρ_1, we can compute the conditional error probability for a fixed constrained transmitter $\rho^{(M,L,\bar{N})}$, i.e.,

$$P_{e,\min}[\rho^{(M,L,\bar{N})}] = \frac{1}{2}\left[1 - D(\rho_0, \rho_1)\right] \ . \tag{2.100}$$

The optimal performance of channel discrimination now requires a minimization over all constrained transmitters $\rho^{(M,L,\bar{N})}$. In other words, we consider

$$P_{e,\min}^{(M,L,\bar{N})} = \min_{\rho^{(M,L,\bar{N})}} P_{e,\min}[\rho^{(M,L,\bar{N})}]. \tag{2.101}$$

More generally, we can define the optimal performance at fixed input energy $\bar{N}$ by further optimizing over the number of signals M and idlers L, i.e.,

$$P_{e,\min}(\bar{N}) = \min_{M,L} P_{e,\min}^{(M,L,\bar{N})}. \tag{2.102}$$

This is the minimum error probability that we can reach by any type of transmitter with the only constraint given by the number $\bar{N}$ of mean photons hitting the box. This problem is non-trivial for low photon numbers $\bar{N}$, while it is trivial for $\bar{N} \to +\infty$ where $P_{e,\min}(\bar{N}) \to 0$. Note also that we are considering here a "global" constraint [78] where we restrict the total amount of energy hitting the box. Another possibly could be considering a "local" energetic constraint [78] where we restrict the mean number of photons $\bar{n}$ of each signal mode. Assuming a local constraint in multi-copy discrimination would give a total energy of $\bar{N} = M\bar{n}$, clearly going to infinity for $M \to +\infty$.

Finding the solution of Eq. (2.102) for finite energy $\bar{N}$ is an open-problem [78]. This is true even if we restrict the transmitters $\rho^{(M,L,\bar{N})}$ to be M-copy states of the type

$$\rho_{SI}^{\otimes M}(\bar{N}) = \underbrace{\rho_{SI}(\bar{n}) \otimes ... \otimes \rho_{SI}(\bar{n})}_{M} \tag{2.103}$$

where the single-copy $\rho_{SI}(\bar{n})$ is a two-mode entangled state of a signal (with mean energy $\bar{n} = \bar{N}/M$) and an idler (whose energy may be unspecified). For instance we do not know if a single-copy transmitter $\rho_{SI}^{\otimes 1}(\bar{N}) = \rho_{SI}(\bar{N})$ with signal energy $\bar{N}$ may outperform or not a many-copy transmitter $\rho_{SI}^{\otimes\infty}(\bar{N})$ where each signal mode has energy $\bar{n} \to 0$.

Despite it being challenging to find an optimal solution, we can however try to compare the performance of different classes of input states. From this point of view an important comparison is between assisted and unassisted strategies. Given a global energetic constraint $\bar{N}$, we ask if the use of entangled transmitters as in Eq. (2.103) may largely outperform the use of multi-copy transmitters of the form

$$\rho^{\otimes M}(\bar{N}) = \underbrace{\rho(\bar{n}) \otimes ... \otimes \rho(\bar{n})}_{M}, \tag{2.104}$$

which do not exploit any idler system.

The most natural choice is to consider EPR transmitters, expressed by Eq. (2.103) with $\rho_{SI}(\bar{n})$ being an EPR state $|\mu\rangle_{SI}\langle\mu|$ with variance $\mu = 2\bar{n}+1$, compared against coherent-state transmitters, which are expressed by Eq. (2.104) with $\rho(\bar{n}) = |\alpha\rangle\langle\alpha|$ such that $|\alpha|^2 = \bar{n}$. This comparison is depicted in Fig. 2.5.

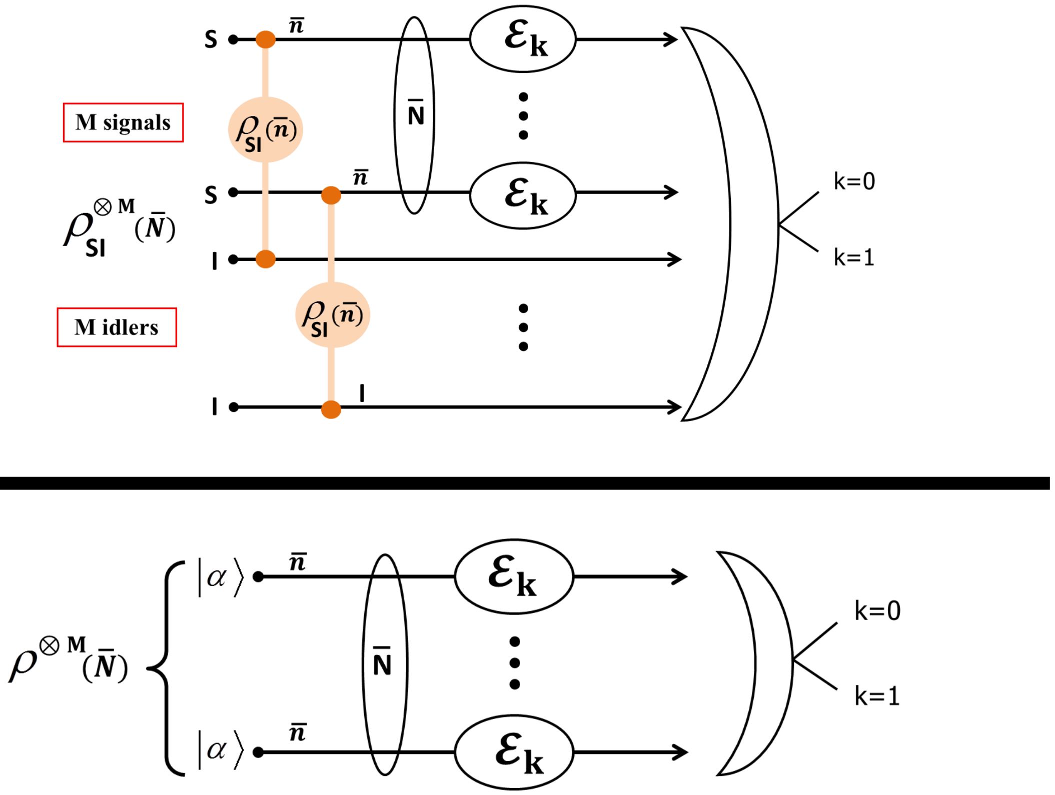

Figure 2.5: (Top) EPR transmitter $\rho_{SI}^{\otimes M}(\bar{N}) = |\mu\rangle_{SI}\langle\mu|^{\otimes M}$ compared to (bottom) coherent-state transmitter $\rho^{\otimes M}(\bar{N}) = |\alpha\rangle\langle\alpha|^{\otimes M}$. Both transmitters irradiate $\bar{N}$ mean photons on the box (i.e., they have equal signal energy).

Note that the two possible outputs of the EPR transmitter are the states

$$\rho_k^{EPR} = [(\mathcal{E}_k \otimes I)(|\mu\rangle_{SI}\langle\mu|)]^{\otimes M} . \tag{2.105}$$

The performance of an EPR transmitter $\rho_{SI}^{\otimes M}(\bar{N}) = |\mu\rangle_{SI}\langle\mu|^{\otimes M}$ with M signals and signal energy $\bar{N}$ is quantified by

$$P_{EPR}(M, \bar{N}) = \frac{1}{2}\left[1 - D(\rho_0^{EPR}, \rho_1^{EPR})\right] . \tag{2.106}$$

The optimal performance achieved by EPR transmitters with signal energy $\bar{N}$ is given by the maximization over M, i.e.,

$$P_{EPR}(\bar{N}) = \min_{M} P_{EPR}(M, \bar{N}) \ . \tag{2.107}$$

For a coherent-state transmitter $\rho^{\otimes M}(\bar{N}) = |\alpha\rangle\langle\alpha|^{\otimes M}$ with M signals and signal energy $\bar{N}$ we have the two possible outputs

$$\rho_k^{coh} = [\mathcal{E}_k(|\alpha\rangle\langle\alpha|)]^{\otimes M}, \tag{2.108}$$

and a discrimination performance given by

$$P_{coh}(M, \bar{N}) = \frac{1}{2}\left[1 - D(\rho_0^{coh}, \rho_0^{coh})\right] \ .$$

The optimal performance achievable by coherent-state transmitters with signal energy $\bar{N}$ is then equal to

$$P_{coh}(\bar{N}) = \min_{M} P_{coh}(M, \bar{N}) \ . \tag{2.109}$$

Now the main task is proving the strict inequality

$$P_{EPR}(\bar{N}) < P_{coh}(\bar{N}), \tag{2.110}$$

for sufficiently low photon numbers $\bar{N}$, so that EPR transmitters outperform standard coherent-state transmitters at low energy. The possibility of having Eq. (2.110) identifies quantum entanglement as a powerful resource to discriminate channels using a small number of photons. This advantage relies in the quantum correlations between signals and idlers which may greatly boost the sensitivity of the discrimination. We note that this kind of advantage has been already found in various other applications, e.g., in quantum illumination [41, 73] or in other problems of quantum metrology [45]. As we explain in the next chapter, we aim to exploit this unique feature of the quantum correlations to probe biological material in a noninvasive way.

Chapter 3

Novel work

Here we present the three main contributions. We start with the asymmetric formulation of quantum hypothesis testing, where two quantum hypotheses have different associated costs. In this problem, the aim is to minimize the probability of false negatives and the optimal performance is provided by the quantum Hoeffding bound. Here we show how this bound can be simplified for pure states and, most importantly, we show how it can be computed for Gaussian states.

The numerical results presented in this chapter are obtained with the help of the software "Mathematica". One of the core procedures is the computation of the symplectic diagonalization of covariance matrices, i.e. their symplectic spectra and, whenever needed, the symplectic matrices involved in their Williamson's decompositions. The formulas for the quantum Chernoff bound and quantum Hoeffding bound not only involve these kinds of diagonalizations but also the general optimization over the real parameter involved in the definition of the generalized overlap between two Gaussian states. The latter problem can often be by-passed by choosing specific values for s (for instance, $s = 1/2$) which however leads to generally larger upper bounds.

3.1 Quantum Hoeffding bound

As we discussed earlier, quantum hypothesis testing (QHT) is a fundamental topic in quantum information theory [45]. It can be formulated as *symmetric testing*, where the quantum hypotheses have the same cost [5,18,33], or *asymmetric testing*, where these hypotheses have different associated costs [5,18,33]. In the latter approach, we focus on minimizing the probability that the alternative hypothesis is confused for the null hypothesis, an error which is known as 'false negative'. This minimization has to be done by suitably constraining the probability of the other type of error ('false positive'), where the null hypothesis is confused for the alternative one. This is clearly the best approach for instance in medical-type testing, where the null hypothesis typically represents absence of a disease, while the alternative corresponds to the presence of a disease.

In the quantum setting, asymmetric QHT is formulated as a multi-copy discrimination problem, where a large number of copies of the two possible states are prepared and subjected to a collective quantum measurement. From this point of view, the aim is to maximize the error-exponent describing the exponential decay of the false negatives, while placing a reasonable constraint on the false positives. For this calculation, we can rely on the recently-introduced quantum Hoeffding bound (QHB) [4].

In this section, we first show how the computation of the QHB simply reduces to that of the quantum fidelity [37] in the presence of pure states. Then, we provide a general recipe for computing the QHB in the case of multimode Gaussian states, for which it can be expressed in terms of their first- and second-order statistical moments. In the general multimode case, we derive a relation between the QHB and other easier-to-compute bounds, which are based on well-known mathematical inequalities. Finally, we derive analytical formulas and numerical results for the most important classes of one-mode and two-mode Gaussian states.

3.1.1 Asymmetric testing with pure states

Asymmetric testing becomes very simple when one of the states (or both) is pure. In this case, we can in fact relate the QHB to the quantum fidelity between the two states. Let us start by considering the case where only one of the states is pure, e.g., $\rho_0 = |\psi_0\rangle \langle\psi_0|$. We can write [70]

$$\inf_s C_s = F(|\psi_0\rangle, \rho_1), \tag{3.1}$$

where F is the fidelity between $|\psi_0\rangle$ and ρ_1. Eq. (3.1) implies $C_s \geq F$. By using the latter inequality in Eq. (2.87), we derive the fidelity-bound

$$H(r) \leq H_F(r) := \sup_{0\leq s<1} \frac{-r\ s - \ln F}{1-s} . \tag{3.2}$$

This bound can be further simplified by explicitly performing the maximization with regard to the parameter s. After a calculation we find

$$H_F(r) = \begin{cases} \ln\frac{1}{F}, & \text{for } r \geq \ln\frac{1}{F} \ , \\ \\ +\infty, & \text{for } r < \ln\frac{1}{F} \ , \end{cases} \tag{3.3}$$

which depends on the comparison between the parameter r and the fidelity F of the two states.

More specifically, in the discrimination of two pure states, we find that the previous fidelity-bound becomes tight

$$H(r) = H_F(r)\ . \tag{3.4}$$

In fact, for pure states $\rho_0 = |\psi_0\rangle\langle\psi_0|$ and $\rho_1 = |\psi_1\rangle\langle\psi_1|$, and for any $0 < s < 1$, we can write

$$\begin{aligned} C_s &= \mathrm{Tr}(|\psi_0\rangle\langle\psi_0|^s|\psi_1\rangle\langle\psi_1|^{1-s}) = \mathrm{Tr}(|\psi_0\rangle\langle\psi_0|\psi_1\rangle\langle\psi_1|) \\ &= |\langle\psi_0|\psi_1\rangle|^2 = F(|\psi_0\rangle, |\psi_1\rangle). \end{aligned} \tag{3.5}$$

Therefore we can replace $\ln C_s = \ln F$ in the QHB of Eq. (2.87), which implies Eq. (3.4).

3.1.2 Asymmetric testing with Gaussian states

Quantum Hoeffding bound for Gaussian states

Our goal is to find a general recipe for the calculation of the QHB for Gaussian states. We start from the general formula in Eq. (2.87) involving the logarithm of the generalized overlap C_s. Given two n-mode Gaussian states, ρ_0 and ρ_1, we can write an explicit Gaussian formula for the generalized overlap in terms of their statistical moments ($\bar{\mathbf{x}}_0$, $\mathbf{V}_0$) and ($\bar{\mathbf{x}}_1$, $\mathbf{V}_0$). This is given by [52, 70]

$$C_s = \frac{\Pi_s}{\sqrt{\det \mathbf{\Sigma}_s}} \exp\left[-\frac{\mathbf{d}^T\mathbf{\Sigma}_s^{-1}\mathbf{d}}{2}\right], \tag{3.6}$$

where $\mathbf{d} := \bar{\mathbf{x}}_0 - \bar{\mathbf{x}}_1$ is the difference between the mean values, while $\mathbf{\Sigma}_s$ and Π_s depends on the CMs $\mathbf{V}_0$ and $\mathbf{V}_1$. See Eqs. (2.59) and (2.60) for their explicit expressions. In particular, these quantities depend on the symplectic decompositions of the two CMs

$$\mathbf{V}_0 = \mathbf{S}_0\ (\oplus_{k=1}^n \nu_k^0 \mathbf{I})\ \mathbf{S}_0^T,\ \ \mathbf{V}_1 = \mathbf{S}_1\ (\oplus_{k=1}^n \nu_k^1 \mathbf{I})\ \mathbf{S}_1^T, \tag{3.7}$$

where $\{\nu_k^0\}$ and $\{\nu_k^1\}$ are the symplectic spectra, with $\mathbf{S}_0$ and $\mathbf{S}_1$ being suitable symplectic matrices.

Substituting Eq. (3.6) into Eq. (2.87), corresponds to explicitly computing the logarithmic term $\ln C_s$, yielding

$$\ln C_s = \ln \Pi_s - \frac{1}{2}\left\{\ln\det \mathbf{\Sigma}_s + \mathbf{d}^T\mathbf{\Sigma}_s^{-1}\mathbf{d}\right\}\ . \tag{3.8}$$

In particular for zero-mean Gaussian states we have $\mathbf{d} = 0$ and the previous expression simplifies to

$$\ln C_s = \ln \Pi_s - \frac{1}{2}\ln\det \mathbf{\Sigma}_s\ . \tag{3.9}$$

Other computable bounds

Note that computing the generalized overlap C_s and its logarithmic form $\ln C_s$ could be difficult due to the presence of the symplectic matrices, $\mathbf{S}_0$ and $\mathbf{S}_1$, in the term $\mathbf{\Sigma}_s$. A possible solution is to compute an upper bound, known as the 'Minkowski bound', which depends only on the two symplectic spectra [9]. Specifically, we have $C_s \leq M_s$, where

$$M_s := 4^n \left[\prod_{k=1}^{n} \Psi_s(\nu_k^0, \nu_k^1) + \prod_{k=1}^{n} \Psi_{1-s}(\nu_k^1, \nu_k^0) \right]^{-n}, \tag{3.10}$$

and

$$\Psi_s(x, y) := \{[(x+1)^s + (x-1)^s][(y+1)^{1-s} - (y-1)^{1-s}]\}^{1/n}. \tag{3.11}$$

Another easy-to-compute upper bound is the 'Young bound' Y_s [80] which satisfies

$$C_s \leq M_s \leq Y_s, \tag{3.12}$$

where [52]

$$Y_s := 2^n \prod_{k=1}^{n} \Gamma_s(\nu_k^0)\Gamma_{1-s}(\nu_k^1) \ , \tag{3.13}$$

and

$$\Gamma_s(x) := \left[(x+1)^{2s} - (x-1)^{2s}\right]^{-\frac{1}{2}} \ . \tag{3.14}$$

Taking the negative logarithm of Eq. (3.12), we can write the following inequality for the QHB

$$H(r) \geq H_M(r) \geq H_Y(r), \tag{3.15}$$

where

$$H_M(r) := \sup_{0 \leq s < 1} \frac{-r\ s - \ln M_s}{1-s}, \tag{3.16}$$

$$H_Y(r) := \sup_{0 \leq s < 1} \frac{-r\ s - \ln Y_s}{1-s}. \tag{3.17}$$

In the specific case where one of the two Gaussian states is pure, we can compute their fidelity F and apply the upper bound given in Eqs. (3.2) and (3.3), which becomes tight when both states are pure [see Eq. (3.4)]. In particular, for two multimode Gaussian states $\rho_0 = |\psi_0\rangle \langle\psi_0|$ and ρ_1, we can easily write their fidelity F in terms of the statistical moments [70]

$$F = \frac{2^n}{\sqrt{\det \mathbf{L}}} \exp\left(-\frac{\mathbf{d}^T \mathbf{L}^{-1} \mathbf{d}}{2}\right), \tag{3.18}$$

where $\mathbf{L} := \mathbf{V}_0 + \mathbf{V}_1$. As a result, we can use Eq. (3.3) with

$$\ln \frac{1}{F} = \frac{1}{2}\left[\ln\left(\frac{\det \mathbf{L}}{4^n}\right) + \mathbf{d}^T\mathbf{L}^{-1}\mathbf{d}\right]. \tag{3.19}$$

3.1.3 Discrimination of one-mode Gaussian states

In this section, we examine the case of one-mode Gaussian states. This means we fix $n = 1$ in the previous formulas of Sec. 3.1.2, with matrices becoming 2×2, vectors becoming 2-dimensional, and symplectic spectra reducing to a single eigenvalue. For instance, the generalized overlap can be more simply computed using the expressions

$$\Pi_s = 2\ G_s(\nu^0)\ G_{1-s}(\nu^1), \tag{3.20}$$

$$\mathbf{\Sigma}_s = \Lambda_s(\nu^0)\ \mathbf{S}_0\mathbf{S}_0^T + \Lambda_{1-s}(\nu^1)\ \mathbf{S}_1\mathbf{S}_1^T, \tag{3.21}$$

where the real functions G_s and Λ_s are given in Eqs. (2.53) and (2.54). In particular, here we derive the analytic formulas for the QHB for two important classes: Coherent states and thermal states.

Asymmetric testing of coherent amplitudes

The expression of the QHB is greatly simplified in the case of one-mode coherent states $\rho_0 = |\alpha_0\rangle\langle\alpha_0|$ and $\rho_1 = |\alpha_1\rangle\langle\alpha_1|$. Since both states are pure, the QHB is equal to the fidelity bound in Eq. (3.3), i.e., $H(r) = H_F(r)$. Therefore, it is sufficient to compute the fidelity between the two coherent states, which is given by

$$F = |\langle\alpha_0|\ \alpha_1\rangle|^2 = e^{-|\alpha_0-\alpha_1|^2}, \tag{3.22}$$

so that $\ln\frac{1}{F} = |\alpha_0 - \alpha_1|^2 := \sigma$, and we can write

$$H(r) = \begin{cases} \sigma\ , & \text{for } r \geq \sigma\ , \\ \\ +\infty\ , & \text{for } r < \sigma\ . \end{cases} \tag{3.23}$$

Assuming that we impose a good control on the rate of false positives (so that $r \geq \sigma$), then the error-exponent for the false negatives is simply given by $H(r) = \sigma$. More explicitly, this corresponds to an asymptotic error rate

$$\beta_M = \frac{1}{2}e^{-M\sigma} = \frac{F^M}{2}\ . \tag{3.24}$$

Note that, if we have poor control on the rate of false positives, i.e., $r < \sigma$, then the QHB $H(r)$ is infinite. This means that the probability of false negatives β_M goes to zero super-exponentially, i.e., more quickly than any decreasing exponential function.

Asymmetric testing of thermal noise

In this section we derive the QHB for one-mode thermal states $\rho_0 = \rho_{\text{th}}(\nu^0)$ and $\rho_1 = \rho_{\text{th}}(\nu^1)$, with variances equal to ν^0 and ν^1, respectively (in our notation, $\nu = 2\bar{n} + 1$, where $\bar{n}$ is the mean number of thermal photons). These Gaussian states have zero mean ($\bar{\mathbf{x}}_0 = \bar{\mathbf{x}}_1 = 0$) and CMs in the Williamson form $\mathbf{V}_0 = \nu^0\mathbf{I}$ and $\mathbf{V}_1 = \nu^1\mathbf{I}$ (so that $\mathbf{S}_0 = \mathbf{S}_1 = \mathbf{I}$). Thus, we can write

$$\mathbf{\Sigma}_s = \varepsilon_s\mathbf{I},\ \varepsilon_s := \Lambda_s(\nu^0) + \Lambda_{1-s}(\nu^1), \tag{3.25}$$

and derive

$$C_s = \frac{\Pi_s}{\varepsilon_s} = \frac{2}{(\nu^0+1)^s(\nu^1+1)^{1-s} - (\nu^0-1)^s(\nu^1-1)^{1-s}}. \tag{3.26}$$

This is the generalized overlap to be used in the QHB of Eq. (2.87).

Given two arbitrary $\nu^0 \geq 1$ and $\nu^1 \geq 1$, the maximization in Eq. (2.87) can be done numerically. The results are shown in Fig. 3.1 for thermal states with variances up to 3 vacuum units (equivalent to 1 mean thermal photon). From the figure we can see an asymmetry with respect to the bisector $\nu^0 = \nu^1$ which is a consequence of the asymmetric nature of the hypothesis test. The bottom-right part of the figure is related to the minimum probability of confusing a nearly-vacuum state ($\nu^1 \simeq 1$) with a thermal state having one average photon ($\nu^0 \simeq 3$). By contrast, the top-left part of the figure is related to the probability of confusing a thermal state having one average photon ($\nu^1 \simeq 3$) with a nearly-vacuum state ($\nu^0 \simeq 1$). These probabilities are clearly different.

We are able to derive a simple analytical result when we compare a thermal state with the vacuum state. Let us start by considering the vacuum state to be the null hypothesis ($\nu^0 = 1$) while the thermal state is the alternative hypothesis ($\nu^1 := \nu > 1$). In this specific case, we find

$$\ln C_s = (1-s)\ln\left(\frac{2}{1+\nu}\right)\,, \tag{3.27}$$

and we get

$$P(r,s) = \ln\left(\frac{1+\nu}{2}\right) - \frac{rs}{1-s}\,. \tag{3.28}$$

Since ν is a constant, the maximization of P over $0 \leq s < 1$ corresponds to minimizing the function $rs(1-s)^{-1}$, whose minimum occurs at $s = 0$. As a result, we have

$$H(r) = P(r,0) = \ln\left(\frac{1+\nu}{2}\right).$$

Since $\nu = 2\bar{n} + 1$, we can write the QHB in terms of the mean number of thermal photons, i.e.,

$$H(r) = \ln(\bar{n}+1). \tag{3.29}$$

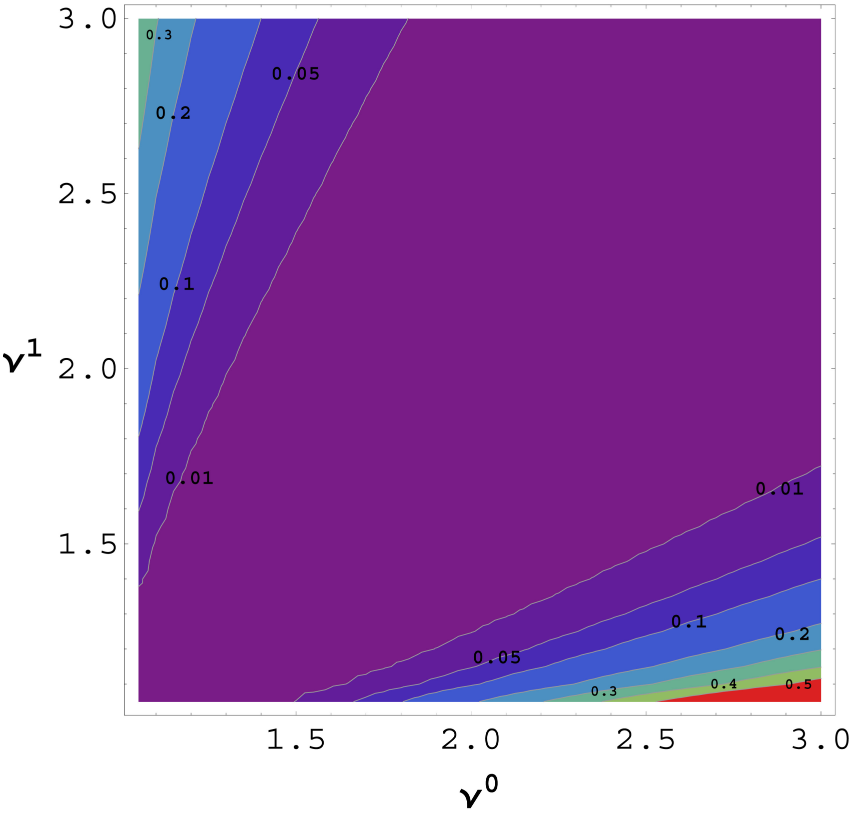

Figure 3.1: We plot the QHB associated with the discrimination of two thermal states: $\rho_{\mathrm{th}}(\nu^0)$ as null hypothesis, and $\rho_{\mathrm{th}}(\nu^1)$ as alternative hypothesis. We consider low thermal variances $1 < \nu^0, \nu^1 \leq 3$ and we have set $r = 0.1$ for the false positives.

This is the optimal error exponent for the asymptotic probability of false negatives, i.e., of confusing a thermal state with the vacuum state.

Let us now consider the thermal state to be the null hypothesis ($\nu^0 := \nu > 1$) while the vacuum state is the alternative hypothesis ($\nu^1 = 1$). In this case, we derive

$$P(r, s) = \frac{s}{1-s}\left[\ln\left(\frac{1+\nu}{2}\right) - r\right], \tag{3.30}$$

which leads to the following expression for the QHB

$$H(r) = \begin{cases} 0 & \text{for } r \geq \ln\left(\frac{1+\nu}{2}\right) \ , \\ \\ +\infty & \text{for } r < \ln\left(\frac{1+\nu}{2}\right) \ . \end{cases} \tag{3.31}$$

This is related to the minimum probability of confusing the vacuum state with a thermal state. Note that this is very different from Eq. (3.29).

3.1.4 Discrimination of two-mode Gaussian states

In this section we consider two important classes of two-mode Gaussian states. The first is the class of Einstein-Podolsky-Rosen (EPR) states, also known as two-mode squeezed vacuum states. The second (broader) class is that of two-mode squeezed thermal (ST) states, for which the computation of the QHB is numerical.

Asymmetric testing of EPR correlations

The expression of the QHB in the case of EPR states is easy to derive. Since EPR states are pure, the QHB $H(r)$ is given by $H_F(r)$ of Eq. (3.3). As a result, we need only compute the fidelity between the two states.

An EPR state has zero mean and CM

$$\mathbf{V}_{\text{EPR}}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \tag{3.32}$$

with $\mu \geq 1$, $\mathbf{I}$ is the 2×2 identity matrix and

$$\mathbf{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.33}$$

Given two EPR states with parameters μ_0 and μ_1, their fidelity is computed via Eq. (3.18), yielding

$$F = \frac{4}{\sqrt{\det \mathbf{L}}}, \tag{3.34}$$

where $\mathbf{L} = \mathbf{V}_{\text{EPR}}(\mu_0) + \mathbf{V}_{\text{EPR}}(\mu_1)$. After simple algebra, we find

$$F = \frac{2}{1 + \mu_0\mu_1 - \sqrt{(\mu_0^2-1)(\mu_1^2-1)}}, \tag{3.35}$$

to be used in Eq. (3.3).

Squeezed thermal states

In this section we consider symmetric ST states $\rho(\mu, c)$, which are Gaussian states with zero mean and CM

$$\mathbf{V}_{\text{ST}}(\mu, c) = \begin{pmatrix} \mu\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \tag{3.36}$$

where $\mu \geq 1$ and $|c| \leq \mu$ [49, 55] (in particular, without loss of generality, we can assume $c \geq 0$). These are called symmetric because they are invariant under permutation of the two modes.

Note that, for $c = 0$, we have no correlations, and the ST state is a tensor-product of thermal states, i.e., $\rho(\mu, 0) = \rho_{\text{th}}(\mu)^{\otimes 2}$. For $c = \sqrt{\mu^2 - 1}$ the correlations are maximal, and the ST state becomes an EPR state, i.e., $\rho(\mu, \sqrt{\mu^2-1}) = \rho_{\mathrm{EPR}}(\mu)$. Finally, for $c = \mu - 1$, we have maximal separable correlations. In other words, $\rho(\mu, \mu-1)$ is the separable ST state with the strongest correlations (e.g., highest discord).

The symplectic decomposition of a symmetric ST state is known. From the CM of Eq. (3.36), one can check that the symplectic spectrum is degenerate and given by the single eigenvalue

$$\nu = \sqrt{\mu^2 - c^2}. \tag{3.37}$$

The symplectic matrix $\mathbf{S}$ which diagonalizes $\mathbf{V}_{\mathrm{ST}}(\mu, c)$ in Williamson form $\nu(\mathbf{I} \oplus \mathbf{I})$ is given by

$$\mathbf{S} = \begin{pmatrix} \omega_+\mathbf{I} & \omega_-\mathbf{Z} \\ \omega_-\mathbf{Z} & \omega_+\mathbf{I} \end{pmatrix}, \tag{3.38}$$

where

$$\omega_\pm := \sqrt{\frac{\mu \pm \nu}{2\nu}}. \tag{3.39}$$

As a result, the generalized overlap between two symmetric ST states, ρ_0 and ρ_1, can be computed using the simplified formulas

$$\Pi_s = 4\; G_s^2(\nu^0)\; G_{1-s}^2(\nu^1), \tag{3.40}$$

$$\mathbf{\Sigma}_s = \Lambda_s(\nu^0)\; \mathbf{S}_0\mathbf{S}_0^T + \Lambda_{1-s}(\nu^1)\; \mathbf{S}_1\mathbf{S}_1^T, \tag{3.41}$$

where ν^0 (ν^1) is the degenerate eigenvalue of ρ_0 (ρ_1), computed according to Eq. (3.37), and $\mathbf{S}_0$ ($\mathbf{S}_1$) is the corresponding diagonalizing symplectic matrix, computed according to Eqs. (3.38) and (3.39).

Let us start with simple cases involving the asymmetric testing of correlations with specific ST states. First we consider the asymmetric discrimination between the uncorrelated thermal state $\rho_0 = \rho(\mu, 0)$ as null hypothesis and the correlated (but separable) ST state $\rho_1 = \rho(\mu, \mu-1)$ as alternative hypothesis. A false negative corresponds to concluding that there are no correlations where they are actually present. It is straightforward to derive their degenerate symplectic eigenvalues which are simply $\nu^0 = \mu$ and $\nu^1 = \sqrt{2\mu - 1}$. Then, we have $\mathbf{S}_0 = \mathbf{I} \oplus \mathbf{I}$, while $\mathbf{S}_1$ can be easily computed from Eqs. (3.38) and (3.39). By substituting these into Eqs. (3.40) and (3.41), we can compute the generalized overlap $C_s = \Pi_s/\sqrt{\det \mathbf{\Sigma}_s}$ and therefore the QHB $H(r)$ via Eq. (2.87). The results are plotted in Fig. 3.2, for values of thermal variance μ up to 3 (i.e., from zero to 1 mean photon) and small values of the parameter r, bounding the rate of false-positives. As expected, the QHB improves for decreasing r and increasing μ.

Now let us consider the asymmetric discrimination between $\rho_0 = \rho(\mu, 0)$ and the EPR state $\rho_1 = \rho_{\mathrm{EPR}}(\mu)$, i.e., the most correlated and entangled ST state. Thanks to the simple symplectic decomposition of the EPR state ($\nu^1 = 1$), we can further

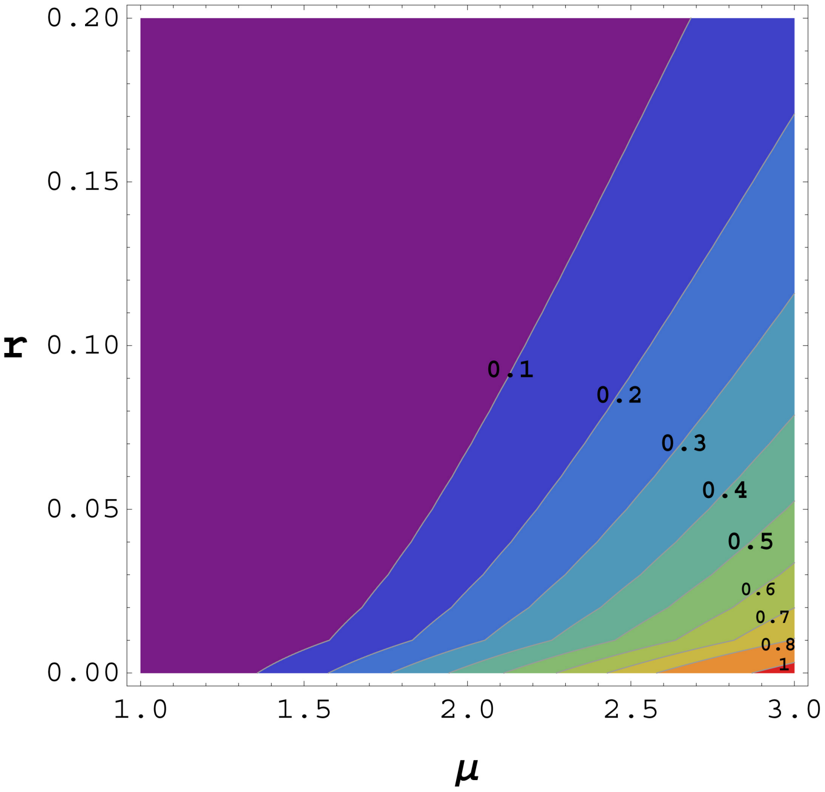

Figure 3.2: (Asymmetric discrimination between the thermal state $\rho_0 = \rho(\mu, 0)$ and the ST state $\rho_1 = \rho(\mu, \mu - 1)$ with maximal separable correlations. We plot the QHB as a function of the thermal variance μ and the false-positive parameter r. As we can see the QHB improves for lower r and for higher μ.

simplify the previous Eqs. (3.40)-(3.41) and write

$$\Pi_s = 4 \; G_s^2(\mu), \;\; \mathbf{\Sigma}_s = \Lambda_s(\mu) \; (\mathbf{I} \oplus \mathbf{I}) + \mathbf{V}_{\text{EPR}}(\mu), \tag{3.42}$$

with $\mathbf{V}_{\text{EPR}}(\mu)$ being given by Eq. (3.32). As before, we compute the QHB which is plotted in Fig. 3.3, for $1 \leq \mu \leq 3$ and $r \leq 2$. As expected the QHB improves for decreasing r and increasing μ. Note a discontinuity identifying two regions, one where the QHB is finite, and the other where it is infinite (white region in the figure).

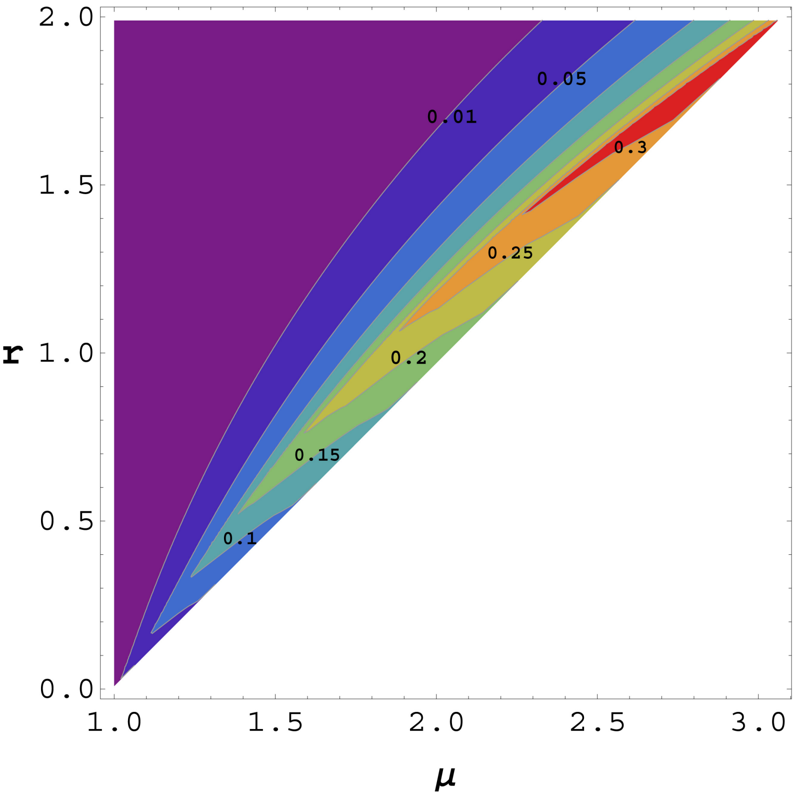

Figure 3.3: Asymmetric discrimination between the thermal state $\rho_0 = \rho(\mu, 0)$ and the EPR state $\rho_1 = \rho_{\text{EPR}}(\mu)$. We plot the QHB as a function of the thermal variance μ and the false-positive parameter r. The QHB improves for lower r and for higher μ. In particular, there is a threshold value after which the QHB becomes infinite (white region).

By expanding the term $P(r, s)$ in Eq. (2.87) for $s \to 1^-$, we find that

$$P(r, s) \simeq \frac{N}{s-1} + O(s-1), \tag{3.43}$$

where

$$N := r - \ln\left(\frac{1+3\mu^2}{4}\right). \tag{3.44}$$

For values of r and μ such that $N > 0$, we find that the term $P(r, s)$ diverges at the border, making the QHB infinite. For a given r, this happens when

$$\mu > \tilde{\mu}(r) := \sqrt{\frac{4e^r - 1}{3}}. \tag{3.45}$$

Finally, we consider the most general scenario in the asymmetric testing of correlations with ST states. We consider two generic ST states, $\rho(\mu, c_0)$ and $\rho(\mu, c_1)$, with the same thermal noise but differing amounts of correlation. For this computation, we use Eqs. (3.37)-(3.39) with $c = c_0$ or c_1, to be replaced in Eqs. (3.40)-(3.41), therefore deriving the generalized overlap and the QHB. At small thermal variance ($\mu = 3$) and for the numerical value $r = 0.1$, we plot the QHB as a function of the correlation parameters c_0 and c_1. As we can see from Fig. 3.4, the QHB is not symmetric with respect to the bisector $c_0 = c_1$ (where it is zero) and increases away from this line.

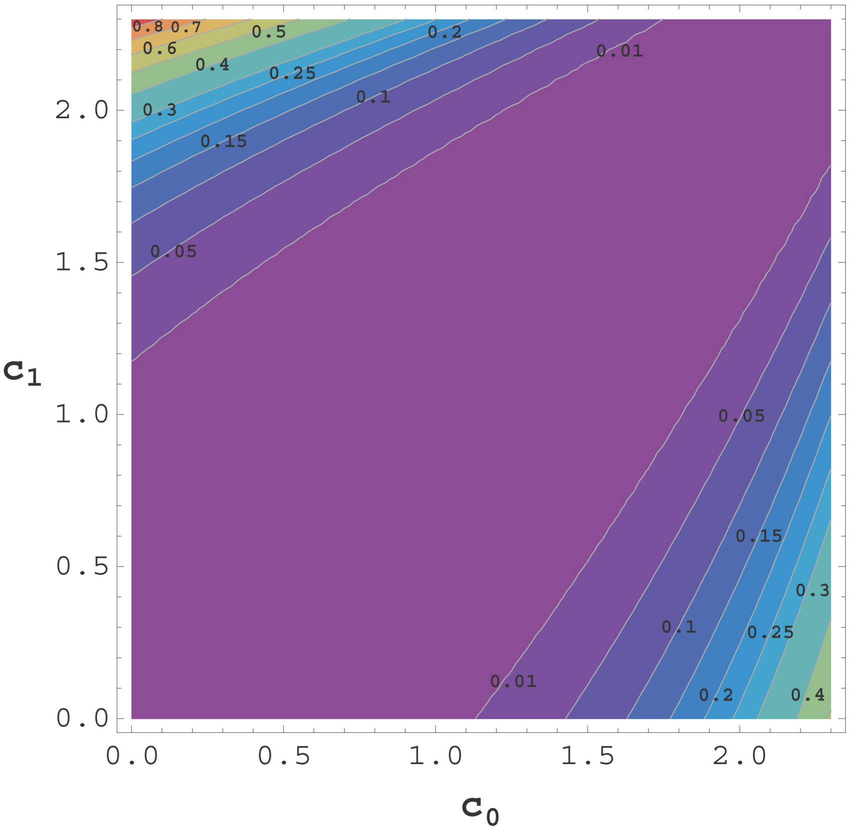

Figure 3.4: Asymmetric discrimination between two ST states with the same thermal variance ($\mu = 3$) but different correlations c_0 and c_1. Setting $r = 0.1$, we plot the QHB as a function of c_0 and c_1. We can see that the QHB increases orthogonally to the bisector $c_0 = c_1$.

3.1.5 Discussion

In this Section 3.1 we have considered the problem of asymmetric quantum hypothesis testing by adopting the recently-developed tool of the quantum Hoeffding bound.

We have shown how the QHB can be simplified in some cases (pure states) and estimated using other easier-to-compute bounds based on simple algebraic inequalities.

In particular, we have applied the theory of asymmetric testing to multimode Gaussian states, providing a general recipe for the computation of the QHB in the Gaussian setting. Using this recipe, we have found analytic formulas and shown numerical results for important classes of one-mode and two-mode Gaussian states. In particular, we have studied the behavior of the QHB in the low energy regime, i.e., considering Gaussian states with a small average number of photons.

Our results could be exploited in protocols of quantum information with continuous variables. In particular, they could be useful for reformulating Gaussian schemes of quantum state discrimination and quantum channel discrimination in such a way as to give more importance to one of the quantum hypotheses. This asymmetric approach could be the most suitable in the development of quantum technology for medical applications.

3.2 Quantum sensing of loss

3.2.1 Introduction

The tools of quantum hypothesis testing can be employed to solve problems of quantum channel discrimination. Here, an unknown quantum channel, $\mathcal{E}_0$ or $\mathcal{E}_1$, is prepared inside an input-output black-box and passed to a reader [42, 50, 53, 69], whose aim is to distinguish the two channels by probing the input port and measuring the output. This problem can be restricted to the bosonic setting with Gaussian channels [78], in particular, lossy channels $\mathcal{E}_\tau$ which are characterized by a single transmissivity parameter $\tau \in [0, 1]$. These channels can be dilated into beam-splitters subject to vacuum noise.

In this section, we are interested in sensing the presence of loss, which corresponds to the discrimination between a lossless channel (i.e., the identity channel $\mathcal{I}$) from a lossy channel with some transmissivity $\tau < 1$. In other words, we consider transmissivity $\tau_0 = 1$ as our null hypothesis H_0, and transmissivity $\tau_1 := \tau < 1$ as our alternative hypothesis H_1. This is relevant in biologically-related problems, such as the detection of small concentrations of cells or bacteria. The connection is established by the Lambert-Beer law [36]. According to this law, the concentration c of species within a sample can be connected with its absorbance or transmissivity τ by the formula

$$\tau = 10^{-\varepsilon l c}, \tag{3.46}$$

where ε is the molar attenuation coefficient of the material at the considered wavelength (measured in m^2/mol or L/mol/cm), l is the optical path length (measured in cm) and, of course, c is the concentration (measured in mol/L also known as molar M). Thus, from an optical point of view, the sample is equivalent to a lossy channel with concentration-dependent transmissivity $\tau = \tau(c)$. Our problem can be mapped into the discrimination between non-growth ($c = 0$) and growth ($c > 0$) within a biological sample.

The values of the various parameters present in Eq. (3.46) may vary widely. To give an idea of possible values, consider that the concentration c may virtually be any number between zero and one molar; l is typically between 1 mm and 1 cm; and ε may be of the order of 120 L/mol /cm for an amino acid like cystine at 280 nm, or equal to much higher values, of the order of 3×10^4 L/mol /cm for bacteria like *E. Coli* at 280 nm [71].

To discuss a potential practical application, consider human serum albumin with $\varepsilon = 32810$ at 280 nm in a cuvette of 1 mm. An extremely small concentration of $c = 10^{-6}$ would provide an optical transmissivity of about $10^{-0.003} \simeq 99\%$ which is where quantum light will be shown to work the best. From this point of view, quantum sensing may reduce the amount of material needed for a diagnosis or, equivalently, it might be used to diagnose a disease in advance, thanks to the better ability to detect extremely small concentrations.

An important issue is related to the amount of energy employed to probe the black-box or, equivalently, the sample in the biological setting just described. First of all, a problem of Gaussian channel discrimination makes sense only if we assume an energetic constraint for the optical mode probing the box, otherwise any two distinct channels can always be perfectly distinguished (using infinite energy). Second, we assume that this constraint imposes an effective regime of a few photons, so that the box is read in a non-invasive way, which fully preserves its content. This is particularly important from a biological point of view, since bacteria may be photodegradable and DNA/RNA extracts in samples can easily be degraded by strong light (especially, at the UV regime).

Thus, in our quantum sensing of loss, we assume a suitable energetic constraints at the input, which may be of two kinds:

(1) Local energetic constraint, where we fix the mean number of photons employed in each single readout of the box; in particular, we are interested in the use of a single readout and in the limit of many readouts (e.g., using a broadband signal).

(2) Global energetic constraint, where we fix the mean number of photons which are used in total, i.e., in all the readouts of the box.

Imposing one of these constraints and a suitable regime of few photons, our work aims to prove the superiority of quantum-correlated sources with respect to classical sources for the non-invasive sensing of loss.

As shown by the setups of Fig. 3.5, we first consider a classical strategy where a single-mode S, prepared in a classical state (in particular, a coherent state), is irradiated through the sample and detected at the output by an optimal dichotomic POVM. Then, we compare this approach with the quantum strategy where two modes, signal S and reference R, are prepared in a quantum correlated state, in particular, an Einstein-Podolsky-Rosen (EPR) state [78]. Only the signal mode is irradiated through the sample, while the reference mode is directly sent to the measurement device where it is subject to an optimal dichotomic POVM jointly with the output mode S' from the sample.

The readout performance of these two setups are compared by constraining the energy of the signal mode S, by fixing the mean number of photon $\bar{n}$ per mode (local constraint), or the total mean number of photons $\bar{N} = M\bar{n}$ in M probings of the sample. The performance is evaluated in terms of minimum error probability considering both symmetric and asymmetric testing.

3.2.2 Classical Benchmark

In the classical setup of Fig. 3.5(a), the input signal mode S is prepared in a coherent state $|\alpha\rangle$ and transmitted through the sample. At the output receiver, one

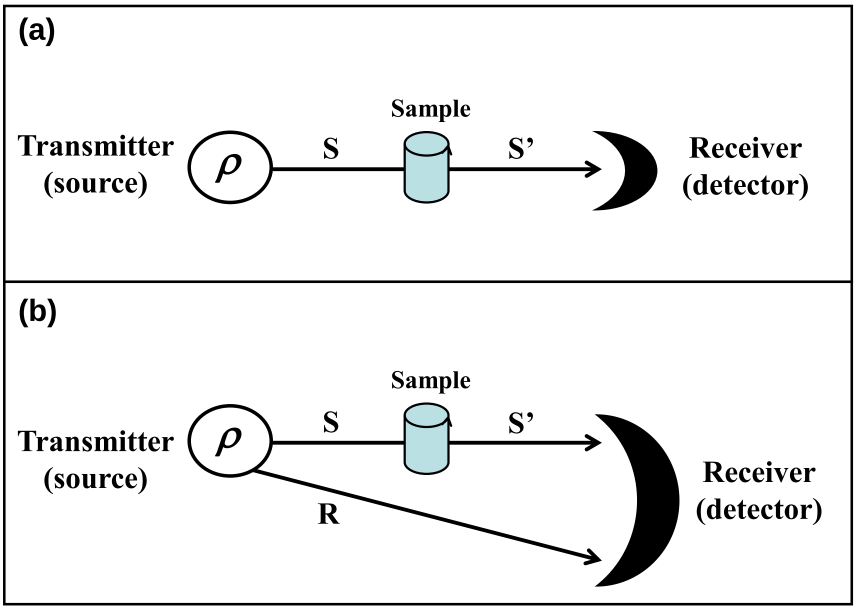

Figure 3.5: Configurations for sensing the presence of loss in a sample via a transmitter (source) and a receiver (detector). **Panel (a)**. In the classical setup, a signal mode S is prepared in a coherent state and irradiated through the sample, with the output mode S' subject to optimal detection. **Panel (b)**. In the quantum setup, the transmitter is composed of two quantum-correlated modes, S and R. Only S is irradiated through the sample. The output S' is combined with R in a joint optimal quantum measurement.

can use a photodetector which counts the number of photons transmitted. This is then followed by digital post-processing, e.g., based on a classical hypothesis test. The performance of this receiver can always be bounded by considering an optimal dichotomic POVM (e.g., the Helstrom POVM [33] in symmetric testing and other suitable dichotomic POVMs in the asymmetric case [4]).

Let us solve this problem in the general multi-copy scenario, where the sample is probed M times, so that the input state is given by the tensor product

$$|\alpha\rangle^{\otimes M} = \underbrace{|\alpha\rangle \otimes \cdots \otimes |\alpha\rangle}_{M} . \tag{3.47}$$

It is clear that the output states will be either $|\alpha\rangle^{\otimes M}$ (under hypothesis H_0) or $|\sqrt{\tau}\alpha\rangle^{\otimes M}$ (under hypothesis H_1).

Since the two possible outputs are pure states, we can easily compute the Helstrom bound (for symmetric testing) and the QHB (for asymmetric testing). In fact, when both the states are pure, i.e., $\sigma_0 = |\varphi_0\rangle\langle\varphi_0|$ and $\sigma_1 = |\varphi_1\rangle\langle\varphi_1|$, we can write the Helstrom bound $P_{err}^{\min} := \bar{p}$ as

$$\bar{p} = \frac{1 - D\left(|\varphi_0\rangle^{\otimes M}, |\varphi_1\rangle^{\otimes M}\right)}{2}, \tag{3.48}$$

where the trace distance D can be here computed from the fidelity as

$$D = \sqrt{1 - F\left(|\varphi_0\rangle^{\otimes M}, |\varphi_1\rangle^{\otimes M}\right)} \tag{3.49}$$

$$= \sqrt{1 - F\left(|\varphi_0\rangle, |\varphi_1\rangle\right)^M}, \tag{3.50}$$

where

$$F(|\varphi_0\rangle, |\varphi_1\rangle) = |\langle\varphi_0 \, |\varphi_1\rangle|^2 \ . \tag{3.51}$$

Then, for the QHB we can write

$$H(r) = H_F(r) = \begin{cases} -\ln F \quad \text{for} \quad r \geq -\ln F \ , \\ \\ +\infty \quad \text{for} \quad r < -\ln F \ , \end{cases} \tag{3.52}$$

depending on our control r on the false positives.

Thus, we just need to compute the fidelity between the single-copy output states. From Eq. (3.53), we obtain

$$F\left(|\alpha\rangle, |\sqrt{\tau}\alpha\rangle\right) = \exp\left(-\left|\alpha - \sqrt{\tau}\alpha\right|^2\right) \tag{3.53}$$

$$= \exp[-\bar{n}(1 - \sqrt{\tau})^2], \tag{3.54}$$

where $\bar{n} = |\alpha|^2$ is the mean number of photons of the single-copy coherent state at the input. Using Eqs. (3.48)-(3.51), we derive the following Helstrom bound for the coherent state transmitter

$$\bar{p}_{\mathrm{coh}} = \frac{1 - \sqrt{1 - e^{-\bar{N}(1-\sqrt{\tau})^2}}}{2}. \tag{3.55}$$

We can see that the minimum error probability depends on the total mean number of photons $\bar{N} = M\bar{n}$. This means that it makes no difference to use: (i) Either M identical faint coherent states each with $\bar{n}$ mean photons, (ii) or a single energetic coherent state with $\bar{N}$ mean photons. Also note that, for $\bar{N}(1-\sqrt{\tau})^2 \ll 1$, we have $\bar{p}_{\mathrm{coh}} \simeq 1/2$, i.e., random guessing. Discrimination becomes therefore challenging at low photon numbers.

Note that it is also easy to compute the quantum Chernoff bound (QCB). Since the two states are pure, we can write it in terms of the quantum fidelity as specified by Eq. (2.43), i.e.,

$$\bar{p}_{\mathrm{QCB}} = \frac{F^M}{2}. \tag{3.56}$$

which here becomes

$$\bar{p}_{\mathrm{coh}}^{\mathrm{QCB}} = \frac{1}{2}\exp[-\bar{N}(1-\sqrt{\tau})^2]. \tag{3.57}$$

This is an upper-bound to the minimum error probability of Eq. (3.55), becoming tight in the limit of large number of copies $M \gg 1$.

In the case of asymmetric quantum discrimination, we aim to minimize the probability of false negatives $p(H_0|H_1)$. In a biological sample, this means to minimize the probability of concluding that there is no growth of bacteria when there actually is. More precisely, we aim to derive the QHB which maximizes the error-rate exponent β_R of $p(H_0|H_1)$ in the regime of many copies M, while constraining the error-rate exponent for the false positives $\alpha_R \geq r$. By using Eq. (3.52), we derive

$$H_{\mathrm{coh}}(r) = \begin{cases} -\ln F = \bar{n}(1-\sqrt{\tau})^2 \quad \text{for} \quad r \geq \bar{n}(1-\sqrt{\tau})^2 \\ \\ +\infty \quad \text{for} \quad r < \bar{n}(1-\sqrt{\tau})^2 \end{cases} \tag{3.58}$$

Here we note that for bad control of the false positives $r < \bar{n}(1-\sqrt{\tau})^2$, the QHB has a super-exponential decay in M. In contrast, for good control of the false positives $r \geq \bar{n}(1-\sqrt{\tau})^2$, the QHB has the following asymptotic exponential decay

$$p_{\mathrm{coh}}(H_0|H_1) \simeq \frac{1}{2}\exp[-M\ H(r)] \tag{3.59}$$

$$\simeq \frac{1}{2}\exp\left[-\bar{N}(1-\sqrt{\tau})^2\right], \tag{3.60}$$

which is the same as the QCB in Eq. (3.57). This an intuitive result because in the case of good control, besides Eq. (2.87), we also have

$$p_{\text{coh}}(H_1|H_0) \simeq \frac{1}{2}\exp[-M\ r] \tag{3.61}$$

$$\leq \frac{1}{2}\exp\left[-\bar{N}(1-\sqrt{\tau})^2\right]. \tag{3.62}$$

Thus, by replacing Eqs. (2.87) and (3.62) in the average error probability of Eq. (2.20), we retrieve

$$\bar{p}_{\text{coh}} \lesssim \frac{1}{2}\exp\left[-\bar{N}(1-\sqrt{\tau})^2\right]. \tag{3.63}$$

3.2.3 Quantum Transmitter

In the quantum setup of Fig. 3.5(b), we consider a transmitter composed of two quantum-correlated modes, the signal S and the reference R. The signal mode, with $\bar{n}$ mean photons, is irradiated through the sample and its output S' is combined with the reference mode in an optimal quantum measurement. For a fixed state ρ_{SR} of the input modes S and R, we get two possible states

$$\sigma_0 = (\mathcal{I}\otimes\mathcal{I})(\rho_{SR}) = \rho_{SR}, \tag{3.64}$$

$$\sigma_1 = (\mathcal{E}_\tau\otimes\mathcal{I})(\rho_{SR}), \tag{3.65}$$

for the output modes S' and R at the receiver. In general, for multi-copy discrimination, the input tensor product $\rho_{SR}^{\otimes M}$ is transformed into either $\sigma_0^{\otimes M}$ or $\sigma_1^{\otimes M}$.

As the single-copy state ρ_{SR} let us consider an EPR state, also known as a two-mode squeezed vacuum state. This is a zero-mean pure Gaussian state $|\mu\rangle_{SR}$ with covariance matrix (CM) [78]

$$\mathbf{V}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \quad \begin{array}{l} \mathbf{Z} := \text{diag}(1,-1), \\ \mathbf{I} := \text{diag}(1,1), \end{array} \tag{3.66}$$

where $\mu \geq 1$ quantifies both the mean number of thermal photons in each mode, given by $\bar{n} = (\mu-1)/2$, and the amount of signal-reference entanglement [78]. Using such a state at the input, we get two possible zero-mean Gaussian states at the output: One is just the input EPR state $\sigma_0 = |\mu\rangle_{SR}\langle\mu|$, while the other state σ_1 is a mixed state with CM.

$$\mathbf{V}_1(\mu,\tau) = \begin{pmatrix} (\tau\mu+1-\tau)\mathbf{I} & \sqrt{\tau(\mu^2-1)}\mathbf{Z} \\ \sqrt{\tau(\mu^2-1)}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}. \tag{3.67}$$

To compute the CM of the output state ρ_1 in Eq. (3.67), we dilate the lossy channel into a beam splitter (with transmissivity τ), mixing the signal mode S with a vacuum mode v. Thus, we have a Gaussian unitary transformation from the input state $\rho_{\text{in}} = |0\rangle_v\langle 0| \otimes |\mu\rangle_{SR}\langle\mu|$ of modes (v, S, R) into the output state ρ_{out} of modes

(v', S', R), i.e.,

$$\rho_{\text{out}} = [\hat{U}_{vS}(\tau) \otimes \hat{I}_R]\rho_{\text{in}}[\hat{U}_{vS}(\tau) \otimes \hat{I}_R]^{\dagger}, \tag{3.68}$$

where $\hat{U}_{vS}(\tau)$ is the beam-splitter unitary [78] applied to modes v and S, while the reference mode R is subject to the identity. In terms of CMs, we have

$$\mathbf{V}_{\text{out}} = [\mathbf{B}_{vS}(\tau) \oplus \mathbf{I}_R]\mathbf{V}_{\text{in}}[\mathbf{B}_{vS}(\tau) \oplus \mathbf{I}_R]^T, \tag{3.69}$$

where $\mathbf{V}_{\text{in}} = \mathbf{I}_v \oplus \mathbf{V}_{SR}(\mu)$ and

$$\mathbf{B}_{vS}(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \tag{3.70}$$

is the symplectic transformation of the beam splitter. After simple algebra, we get an output CM of the form

$$\mathbf{V}_{\text{out}} = \begin{pmatrix} \mathbf{W} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{V}_1(\mu,\tau) \end{pmatrix}, \tag{3.71}$$

where the blocks $\mathbf{W}$ and $\mathbf{C}$ are to be traced out, while $\mathbf{V}_1(\mu,\tau)$ is given in Eq. (3.67).

For symmetric testing we compute the QCB, which can directly be derived from the quantum fidelity, as specified in Eq. (3.56). The multi-copy minimum error probability $\bar{p}_{\text{quant}}$ is upper-bounded by $\bar{p}^{\text{QCB}}_{\text{quant}} = F^M/2$, where the fidelity $F = \langle\mu|\,\sigma_1\,|\mu\rangle$ is determined by the CMs of the two Gaussian states. This fidelity is equal to

$$F = \frac{4}{\sqrt{\det[\mathbf{V}(\mu) + \mathbf{V}_1(\mu,\tau)]}} = \left[1 + \bar{n}\left(1 - \sqrt{\tau}\right)\right]^{-2}. \tag{3.72}$$

Thus, we have

$$\bar{p}_{\text{quant}} \leq \bar{p}^{\text{QCB}}_{\text{quant}} = \frac{1}{2}\left[1 + \bar{n}\left(1 - \sqrt{\tau}\right)\right]^{-2M}. \tag{3.73}$$

For the asymmetric testing we compute the QHB. From

$$H(r) \geq -\ln F\ , \tag{3.74}$$

we may write

$$H_{\text{quant}}(r) \geq 2\ln\left[1 + \bar{n}\left(1 - \sqrt{\tau}\right)\right]. \tag{3.75}$$

More precisely, if control on the false-positives is good, so that $r \geq -\ln F$, then the QHB and the QCB coincide and we have

$$H(r) = -\ln F \quad \text{for} \quad r \geq -\ln F. \tag{3.76}$$

According to Eq. (3.76), we may write

$$H_{\text{quant}}(r) = 2\ln\left[1 + \bar{n}\left(1 - \sqrt{\tau}\right)\right], \tag{3.77}$$

for $r \geq 2\ln[1+\bar{n}(1-\sqrt{\tau})]$. Finally, we have numerically checked that for $r < 2\ln[1+\bar{n}(1-\sqrt{\tau})]$ the QHB $H_{\text{quant}}(r)$ can become infinite.

3.2.4 Comparison and Quantum Advantage

In this section, we perform the comparison between the classical and the quantum strategy for non-invasive sensing of loss, showing how the use of quantum correlations enables us to outperform the classical benchmark achieved with coherent-state inputs. For the symmetric testing, we consider the difference or gain

$$\Delta := \bar{p}_{\text{coh}} - \bar{p}^{\text{QCB}}_{\text{quant}} \leq \bar{p}_{\text{coh}} - \bar{p}_{\text{quant}}, \tag{3.78}$$

using the expressions in Eqs. (3.55) and (3.73). Its positivity is a sufficient condition for the superiority of the quantum transmitter (while $\Delta \leq 0$ corresponds to an inconclusive comparison). In particular, for Δ close to $1/2$, we have that $\bar{p}_{\text{quant}} \simeq 0$ and $\bar{p}_{\text{coh}} \simeq 1/2$, which means that the quantum strategy allows for perfect sensing while the classical strategy is equivalent to random guessing.

We start considering a single probing of the sample, i.e., $M = 1$. Then, we plot $\Delta(\bar{n},\tau)$ considering the regime of small photon numbers ($\bar{n} \leq 10$) and for $0 \leq \tau < 1$. As we can see from Fig. 3.6, the quantum transmitter is better in most of the parameter plane, with very good performances for τ close to 1 (which corresponds to sensing an almost transparent growth). To better explore this region we consider the expansion for $\tau \simeq 1$. By setting $\tau = 1-\varepsilon$, we get the first-order expansion

$$\bar{p}_{\text{coh}} \simeq \frac{1}{2}\left(1+\frac{\sqrt{\bar{n}}}{2}\varepsilon\right), \; \bar{p}^{\text{QCB}}_{\text{quant}} \simeq \frac{1}{2}\left(1-\bar{n}\varepsilon\right), \tag{3.79}$$

so that

$$\Delta \simeq \left(\frac{\sqrt{\bar{n}}+2\bar{n}}{4}\right)\varepsilon \tag{3.80}$$

which is always positive.

We then analyze the multi-probing case where the samples is queries M times where we fix the mean number of photons per signal mode $\bar{n}$ (local energy constraint). We then specify the gain $\Delta(M,\bar{n},\tau)$ for $M = 20$, and we plot the results in Fig. 3.7. We see that the good region where Δ approaches the optimal value of $1/2$ is again for transmissivities $\tau \simeq 1$.

Asymptotic multi-copy behavior

Here we keep the local energy constraint, i.e., we fix the mean number of photons per signal modes $\bar{n}$, and we compare the two transmitters in the limit of large number of copies $M \gg 1$. In this limit the mean error probability in the symmetric test is

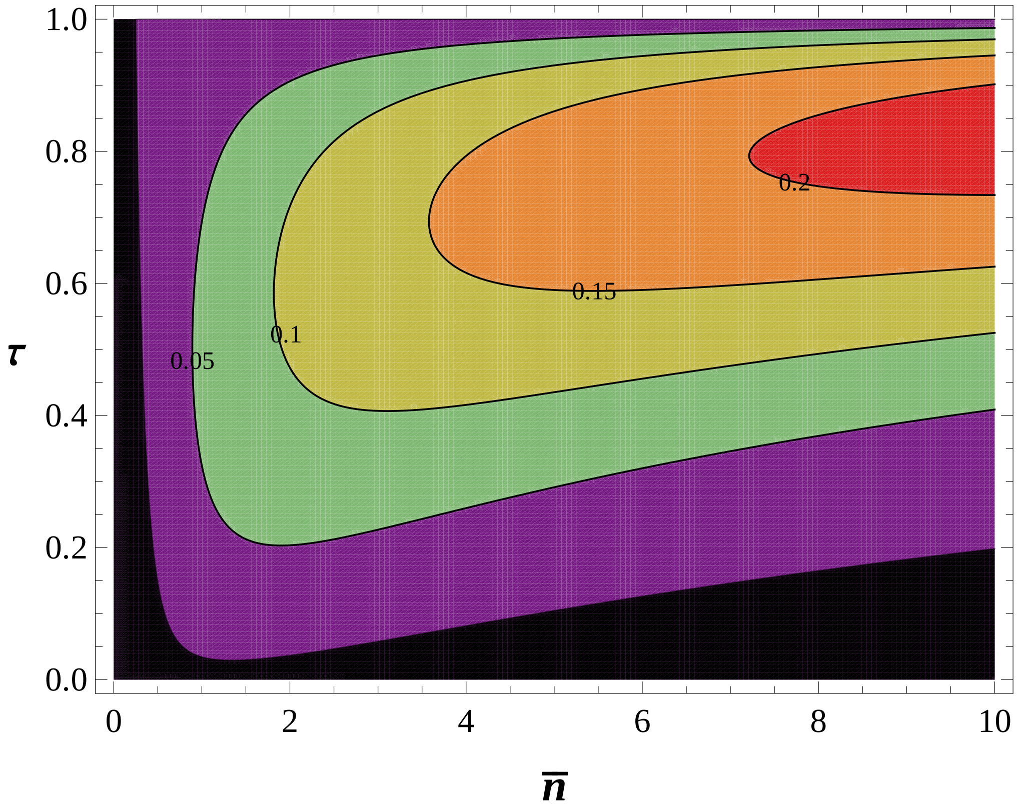

Figure 3.6: Comparison between the quantum transmitter (EPR state) and the classical transmitter (coherent state) for single-copy probing $M = 1$. We plot the gain Δ in the range $0 \leq \tau < 1$ and $\bar{n} \leq 10$. In the black region we have $\Delta \leq 0$ (inconclusive comparison). Outside the black region, we have $\Delta > 0$ proving the superiority of the EPR transmitter, with better performances for $\tau \simeq 1$. Also note that, for increasing $\bar{n}$, the region with quantum advantage tends to shrink towards higher transmissivities.

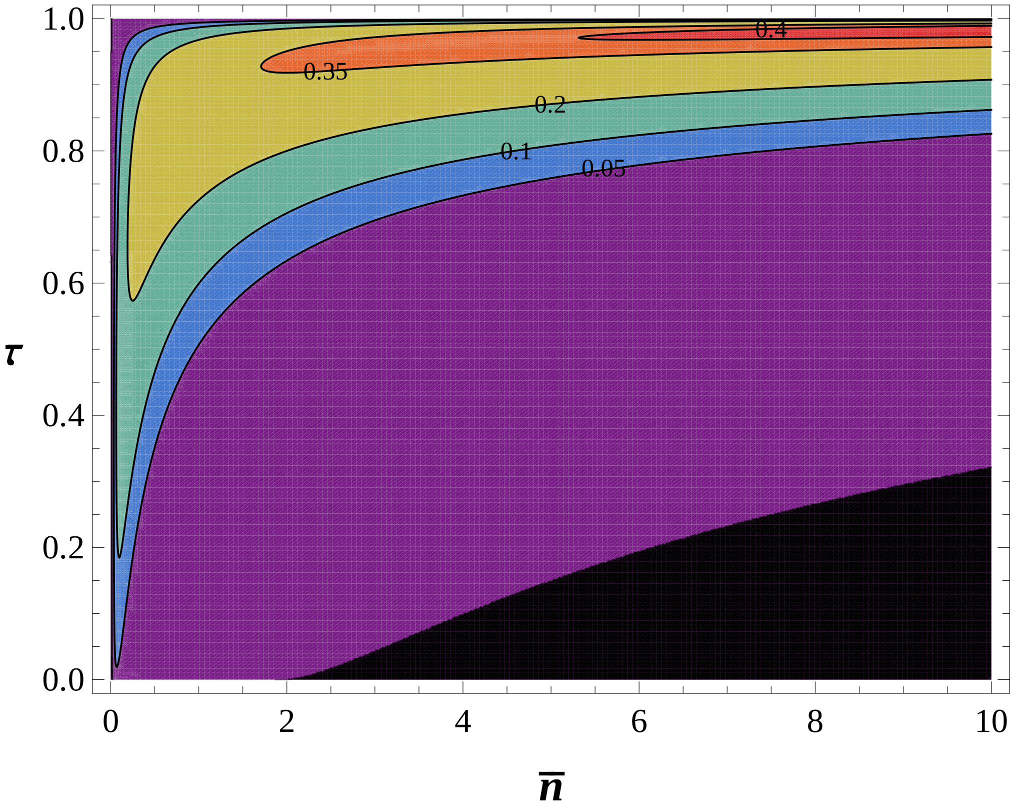

Figure 3.7: Comparison between the quantum transmitter (EPR state) and the classical transmitter (coherent state) for multi-copy probing $M = 20$. We plot the gain Δ in the range $0 \leq \tau < 1$ and $\bar{n} \leq 10$. In the black region we have $\Delta \leq 0$ (inconclusive comparison). Outside the black region, we have $\Delta > 0$ proving the superiority of the EPR transmitter, with better performances for $\tau \simeq 1$. Despite the fact they are not visible in the figure, for $\bar{n} \simeq 0$ we have $\Delta = 0$, as expected. Similarly, we have $\Delta = 0$ at exactly $\tau = 1$.

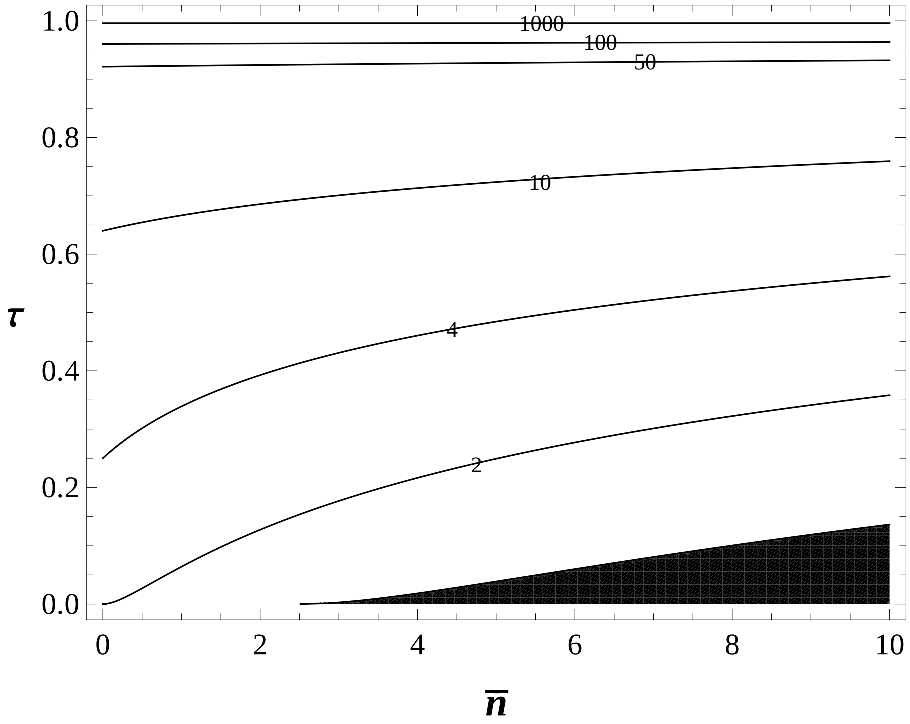

Figure 3.8: We plot the asymptotic ratio $R = \kappa_{\text{quant}}/\kappa_{\text{coh}}$ in terms of transmissivity τ and mean number of photons in the signal mode $\bar{n}$. Note that $R > 1$ in almost all the plane and becomes $O(10^3)$ close to $\tau \simeq 1$ (even though we have a discontinuity at exactly $\tau = 1$, where R must be 1). Black region corresponds to the coherent transmitter outperforming the EPR one ($R \leq 1$).

well approximated by the QCB, so that, from Eqs. (3.57) and (3.73), we can write

$$\bar{p}_{\text{coh}} \simeq \bar{p}_{\text{coh}}^{\text{QCB}} = \frac{1}{2} e^{-M\kappa_{\text{coh}}}, \tag{3.81}$$

where $\kappa_{\text{coh}} := \bar{n}(1 - \sqrt{\tau})^2$, and

$$\bar{p}_{\text{quant}} \simeq \bar{p}_{\text{quant}}^{\text{QCB}} = \frac{1}{2} e^{-M\kappa_{\text{quant}}}, \tag{3.82}$$

where $\kappa_{\text{quant}} := 2\ln[1 + \bar{n}(1 - \sqrt{\tau})]$. Thus, the asymptotic gain can be measured by the ratio

$$R = \frac{\kappa_{\text{quant}}}{\kappa_{\text{coh}}} \ . \tag{3.83}$$

It is clear that for $R > 1$, the error probability of the EPR transmitter goes to zero more rapidly than that of the coherent-state transmitter (while $R \leq 1$ corresponds to the opposite behavior). This ratio is shown in Fig. 3.8. We see that for high values of the transmissivity, the EPR transmitter has an error exponent κ_{quant} which becomes orders of magnitude higher than the classical one κ_{coh}.

Asymptotic multi-copy behavior: Asymmetric testing

Assuming the local energy constraint we now compare the quantum and the classical coherent transmitter from the point of view of asymmetric testing. We consider the ratio between the two QHBs, i.e., for any control r we define

$$R_{\mathrm{QHB}}(r) = \frac{H_{\mathrm{quant}}(r)}{H_{\mathrm{coh}}(r)} \ . \tag{3.84}$$

According to Eqs. (3.58) and (3.75), we have

$$H_{\mathrm{coh}}(r) = \begin{cases} r_{\mathrm{coh}} & \text{for} \quad r \geq r_{\mathrm{coh}} \\ \\ +\infty & \text{for} \quad r < r_{\mathrm{coh}} \end{cases}$$

and

$$\begin{cases} H_{\mathrm{quant}}(r) = r_{\mathrm{quant}} & \text{for} \quad r \geq r_{\mathrm{quant}} \\ \\ H_{\mathrm{quant}}(r) \geq r_{\mathrm{quant}} & \text{for} \quad r < r_{\mathrm{quant}} \end{cases}$$

where

$$r_{\mathrm{coh}} := \bar{n}(1-\sqrt{\tau})^2, \ r_{\mathrm{quant}} := 2 \ln \left[1 + \bar{n}\left(1-\sqrt{\tau}\right)\right] .$$

If we assume a good control on the false positives, i.e., $r \geq \max\{r_{\mathrm{coh}}, r_{\mathrm{quant}}\}$, then we have that the false negative probability is well approximated by the QCB, i.e., $p(H_0|H_1) \simeq \bar{p}_{\mathrm{QCB}}$. As result, the ratio in Eq. (3.84) asymptotically coincides with the previous ratio in Eq. (3.83), i.e., $R_{\mathrm{QHB}}(r) \simeq R$, and the same result shown in Fig. 3.8 also applies to the asymmetric study.

Let us study what happens in the presence of a moderate control on the false positives. Let us consider the case $r_{\mathrm{coh}} < r_{\mathrm{quant}}$ which happens in a delimited region of the plane $(\bar{n}, \tau)$ corresponding to the non-black area in Fig. 3.9. Then, we assume $r = r_{\mathrm{coh}}$, so that $H_{\mathrm{coh}}(r)$ remains finite, while $H_{\mathrm{quant}}(r)$ can become infinite. As we see from Fig. 3.9, there is a wide area where $R_{\mathrm{QHB}}(r) = +\infty$, meaning that the quantum EPR transmitter provides a super-exponential decay for the false-negative probability, while it remains exponential for the classical transmitter.

If we consider the opposite case $r = r_{\mathrm{quant}} < r_{\mathrm{coh}}$, which may only occur in the black area of Fig. 3.9, then we have that $H_{\mathrm{coh}}(r)$ becomes infinite while $H_{\mathrm{quant}}(r)$ remains finite. In other words, we have $R_{\mathrm{QHB}}(r) = 0$ in all the black region. Finally, for $r < \min\{r_{\mathrm{coh}}, r_{\mathrm{quant}}\}$ there are indeterminate forms which do not allow us to provide a simple description of the situation.

From these results it is clear that, for low photon numbers per mode ($\bar{n} \lesssim 10$) and high transmissivities (here $\tau \gtrsim 0.5$), the quantum EPR transmitter greatly outperforms the classical transmitter in the asymmetric quantum discrimination of loss.

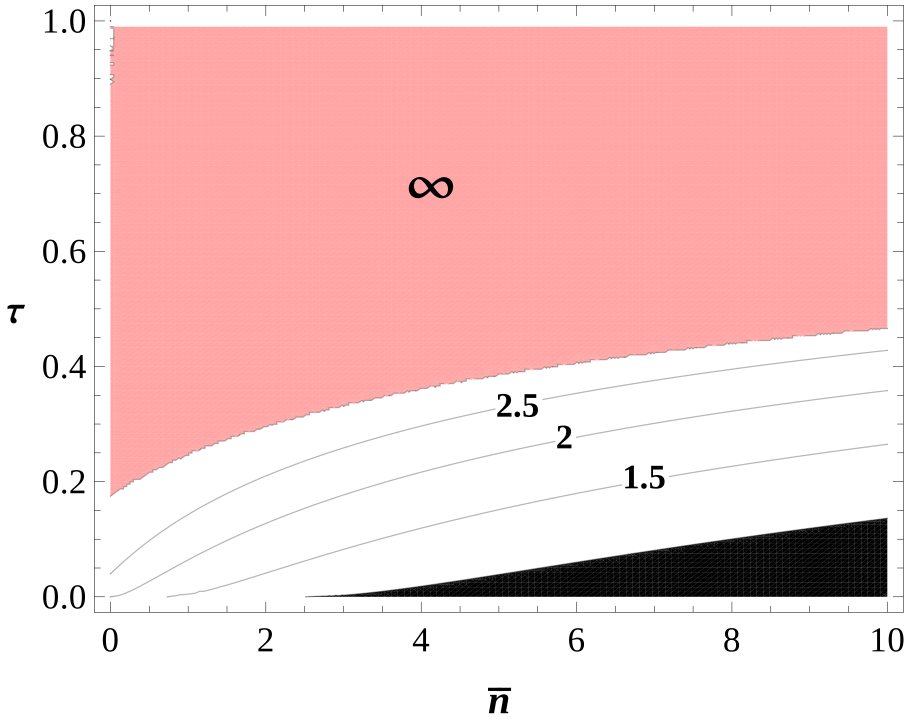

Figure 3.9: Plot of the ratio $R_{\text{QHB}}(r)$ for $r = r_{\text{coh}} < r_{\text{quant}}$ in the plane $(\bar{n}, \tau)$. The black area has to be ignored since it is not compatible with the condition $r_{\text{coh}} < r_{\text{quant}}$. We can see that there is region where the ratio is finite and a wider one where it becomes infinite.

Comparison under the global energy constraint

In order to study the case of the global constraint we set $\bar{n} = \bar{N}/M$ in the QCB in Eq. (3.73), so that it can expressed as $\bar{p}^{\text{QCB}}_{\text{quant}}(\tau, \bar{N}/M, M)$. As we show in Fig. 3.10, the value of $\bar{p}^{\text{QCB}}_{\text{quant}}$ decreases for increasing M, at fixed total energy $\bar{N}$ and transmissivity τ. In other words, it is better to use a large number of copies ($M \gg 1$) of the EPR state with vanishingly small number of photons per copy ($\bar{n} \ll 1$), instead of a single energetic EPR state with $\bar{N}$ mean photons . Remarkably the asymptotic behavior is rapidly reached after a finite number of copies, e.g., $M \simeq 5$ for $\bar{N} = 1$.

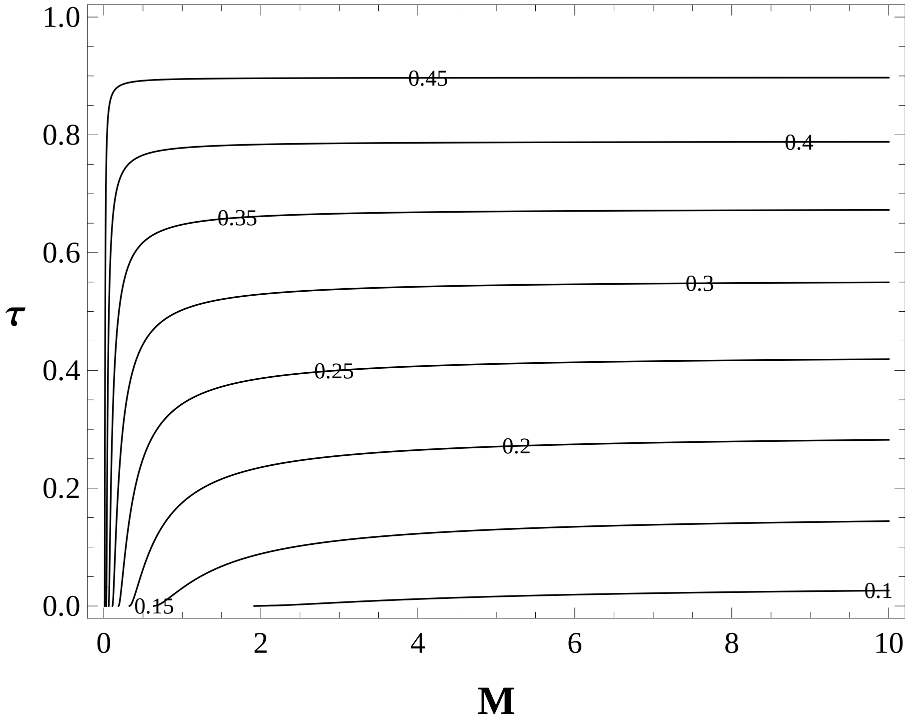

Figure 3.10: Behaviour of $\bar{p}^{\text{QCB}}_{\text{quant}}$ in terms of τ and M at fixed total energy $\bar{N}$. We see that at any fixed transmissivity τ, the QCB of the EPR transmitter is optimized by increasing the number of copies M. This plot refers to $\bar{N} = 1$ but behavior is generic in $\bar{N}$.

For large M, we find the optimal asymptotic expression

$$\lim_{M \to +\infty} \bar{p}^{\text{QCB}}_{\text{quant}}(\tau, \bar{N}/M, M) = \frac{1}{2} \exp\left[-2\bar{N}(1 - \sqrt{\tau})\right], \tag{3.85}$$

and we can study the optimal gain

$$\Delta_{\text{opt}} := \bar{p}_{\text{coh}}(\tau, \bar{N}) - \frac{1}{2} \exp\left[-2\bar{N}(1 - \sqrt{\tau})\right]$$

for values of τ and $\bar{N}$, as shown in Fig. 3.11. We can see that, for relatively small numbers of photons $\bar{N} \leq 50$ globally irradiated over the sample, the EPR transmitter clearly outperforms the classical strategy, especially for high transmissivities $\tau \simeq 1$. In other words, the use of a quantum source has non-trivial advantages for the non-invasive detection of small concentrations.

Luckily, we do not have to consider the limit of $M \to \infty$ for approaching the optimal performance of the EPR transmitter since, as we have already seen in Fig. 3.10, this performance is approximately reached after a small finite M. Indeed this is explicitly check in Fig. 3.12, where we plot $\Delta = \bar{p}_{\mathrm{coh}}(\tau, \bar{N}) - \bar{p}^{\mathrm{QCB}}_{\mathrm{quant}}(\tau, \bar{N}/5, 5)$ and we see that the result is already pretty close to that of Fig. 3.11.

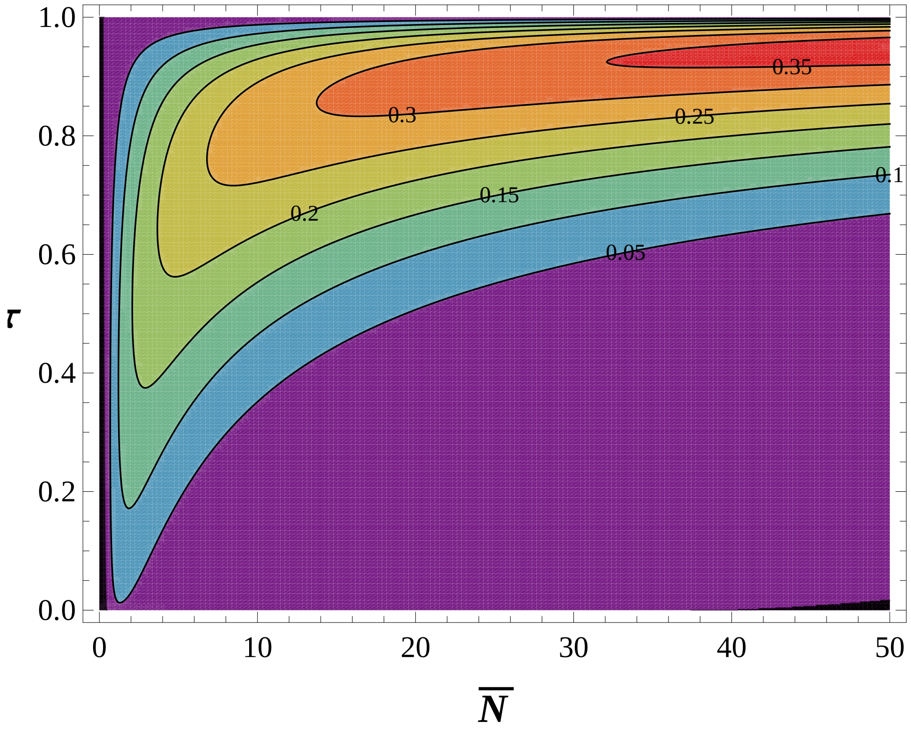

Figure 3.11: Optimal gain Δ_{opt} as a function of τ and $\bar{N}$. Note that Δ_{opt} approaches $1/2$ in the top part of the plot. The small black area at the bottom right corresponds to an inconclusive comparison ($\Delta_{\mathrm{opt}} \leq 0$).

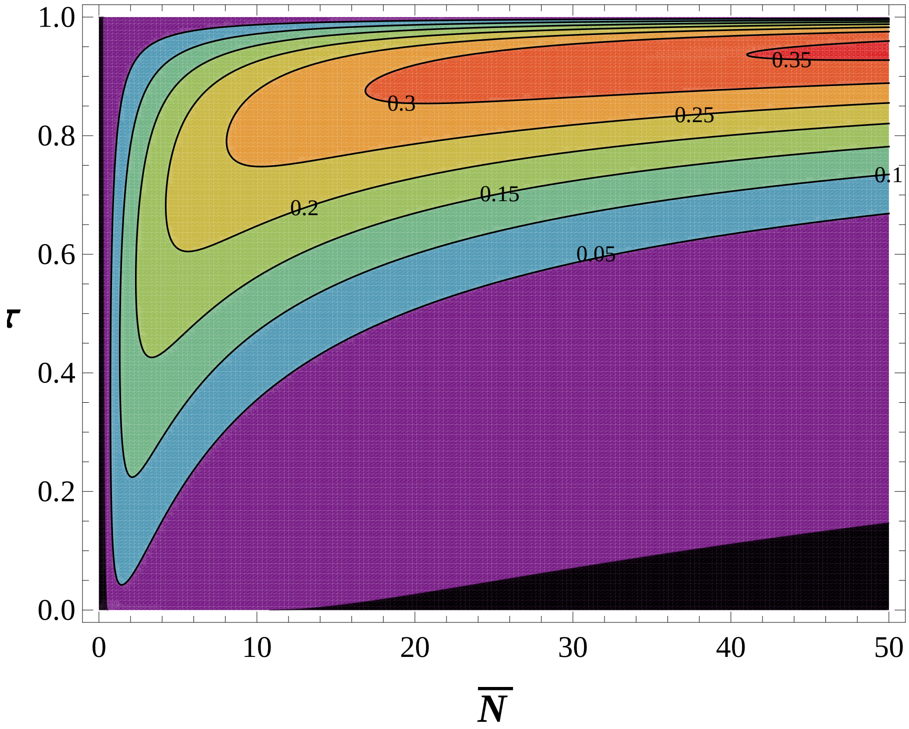

Figure 3.12: Assuming $M = 5$ copies of the EPR state, we plot the gain Δ as a function of τ and $\bar{N}$. Note that the behavior of Δ approximates that of Δ_{opt} in Fig. 3.11. The black area corresponds to an inconclusive comparison ($\Delta \leq 0$).

3.2.5 Phenomenological models of biological growth

As discussed in Sec. 3.2.1, the concentration c of species within a sample can be connected with its transmissivity τ by the formula $\tau(c) = 10^{-\varepsilon l c}$, where ε is an absorption coefficient and l is the path length. Thus, the sample is a lossy channel with concentration-dependent transmissivity $\tau(c)$ and the problem of loss detection can be mapped into the discrimination between non-growth ($c = 0$) and growth ($c > 0$) within the sample. For simplicity, in the following we set $\varepsilon l = 1$, so that $\tau(c) = 10^{-c}$.

We then introduce a phenomenological model of bacterial/cell growth in the sample, so that the concentration depends on time t in a typical exponential law

$$c(t) = c_0 \left[1 - \exp(-gt)\right] , \tag{3.86}$$

where g is a saturation parameter and c_0 is the asymptotic concentration (at infinite time). Using Eq. (3.86) we can write τ as a function of time t as follows

$$\tau(t) = 10^{-c_0[1-\exp(-gt)]} . \tag{3.87}$$

Note that Eq. (3.86) is one of the possible biological growth models that we may consider. It captures an initial linear growth, followed by an exponential growth and ending with an asymptotic saturation. It well describes biological population in a finite habitat. This analytical form has been introduced by Brody [17] and is also known as monomolecular. It also represents a particular case of a Koya-Goshu growth function [38].

Now we can analyze how well we can distinguish between unit transmissivity (no growth) and $\tau(t) < 1$ (growth) at any specified time t. For this aim, we replace $\tau(t)$ in the error probabilities associated with the classical and quantum EPR transmitter. We consider the case of symmetric testing and we assume the global energy constraint, so that we fix the mean total number of photons $\bar{N}$ irradiated over the sample.

We then substitute $\tau(t)$ in the formula of $\bar{p}_{\text{coh}}(\tau, \bar{N})$ of Eq. (3.55) for the classical transmitter, so that we can write $\bar{p}_{\text{coh}}(t, \bar{N})$. Similarly, for the quantum EPR transmitter, we substitute $\tau(t)$ in the formula of $\bar{p}^{\text{QCB}}_{\text{quant}}(\tau, \bar{n}, M)$ of Eq. (3.73) where $\bar{n}M = \bar{N}$. In this case, we can write $\bar{p}^{\text{QCB}}_{\text{quant}}(t, \bar{N}, M)$ and study the two extreme conditions of a single-mode EPR transmitter ($M = 1$) and the broadband EPR transmitter with $M \rightarrow +\infty$ (any other EPR transmitter with arbitrary M will have a performance between these two extremes).

As before we can make the comparison by using the gain $\Delta = \bar{p}_{\text{coh}} - \bar{p}^{\text{QCB}}_{\text{quant}}$ whose maximal value is 1/2. Specifically, we consider the gain given by the single mode EPR transmitter

$$\Delta_1(t, \bar{N}) = \bar{p}_{\text{coh}}(t, \bar{N}) - \bar{p}^{\text{QCB}}_{\text{quant}}(t, \bar{N}, 1),$$

and the optimal gain given by the broadband EPR transmitter, i.e.,

$$\Delta_{\text{opt}}(t, \bar{N}) = \bar{p}_{\text{coh}}(t, \bar{N}) - \bar{p}^{\text{QCB}}_{\text{quant}}(t, \bar{N}, +\infty).$$

We compare the performances of the classical and quantum transmitters plotting $\Delta_1(t, \bar{N})$ and $\Delta_{\text{opt}}(t, \bar{N})$ in Fig. 3.13.

As we can see from Fig. 3.13, the EPR transmitter outperforms the classical strategy at short times, i.e., at low concentrations, when the mean total number of photons $\bar{N}$ is restricted to relatively small values. This means that, in this non-destructive regime, the EPR transmitter is able to provide a much faster detection of bacterial/cell growth in the sample. This is also evident from Fig. 3.14, where we explicitly compare the performances of the transmitters at $\bar{N} = 500$ photons. As we can see, the quantum transmitter allows us to detect the presence or not of a growth in extremely short times (< 0.05 time units in the figure), while we need to wait much more times (at least 0.4 time units) for obtaining the same performance by means of a classical transmitter.

Note that in real world time, the time unit depends on how we express the saturation parameter g in Eq. (3.86). When we account for physical dimensions, we may have g expressed as seconds^{-1} or minutes^{-1} or hours^{-1}. Therefore a unit may be a second or a minute or an hour. In turn, this depends on the material we are

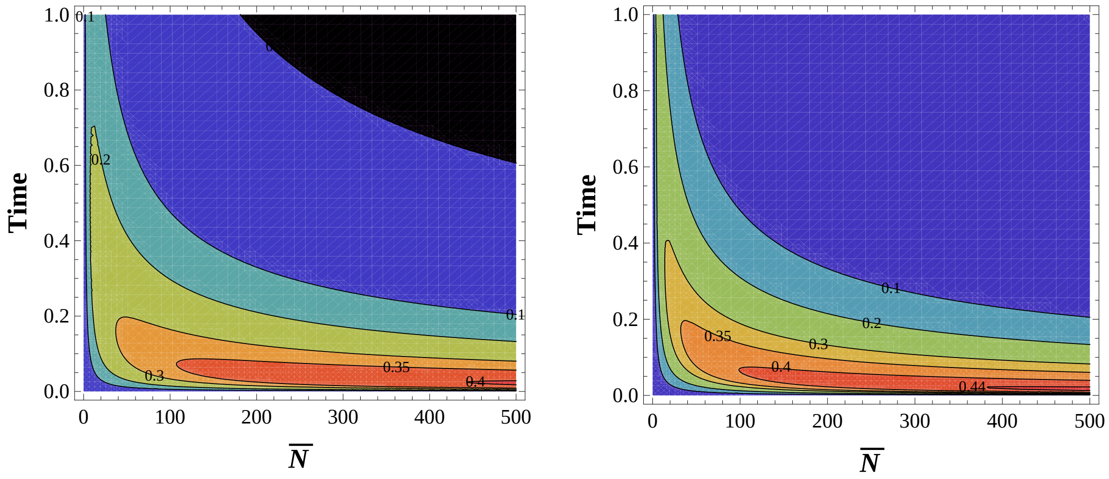

Figure 3.13: Plot of the gains $\Delta_1(t, \bar{N})$ (left panel) and $\Delta_{\text{opt}}(t, \bar{N})$ (right panel) versus mean total energy $\bar{N}$ irradiate over the sample and time t of detection. In the left panel, the black area corresponds to $\Delta_1 \leq 0$ (inconclusive comparison). We can see that the values approach 1/2 at short timescales, corresponding to very low concentrations. Right panel shows a clear improvement of the performance given by the use of a broadband EPR transmitter. In both panels, we have chosen $c_0 = 1$ and $g = 0.2$ for the growth model of Eq. (3.86).

observing. For instance, if we are considering the growth of *E. Coli* in the sample, this is a process which typically takes one day, so that it may be convenient to use hours as basic units.

3.2.6 Photodegradable effects

Here we study the quantum readout of fragile samples in the presence of photodegradability, so that the greater is the input energy (mean number of photons) the greater is the adverse effect on the sample as suitably modeled below. We study the readout mechanism assuming symmetric hypothesis testing and evaluating the number of bits extracted from the sample (since this is a discrimination between two possible hypotheses, the maximum information that can be extracted is equal to one bit).

As before consider a sample which is read in transmission and assume that the two hypotheses are represented by a bit which is encoded in two different transmissivities, τ_0 and τ_1. We design a possible saturation behavior in such a way that the two transmissivities tend to coincide if we increase the amount of energy adopted for readout. Assuming this model, we find wide regions of parameters where the EPR transmitter is able to retrieve the maximum value of 1 bit, while the classical coherent transmitter decodes $\simeq 0$ bits. As we discuss in Sec. 3.3, this striking difference can also be exploited as a cryptographic technique.

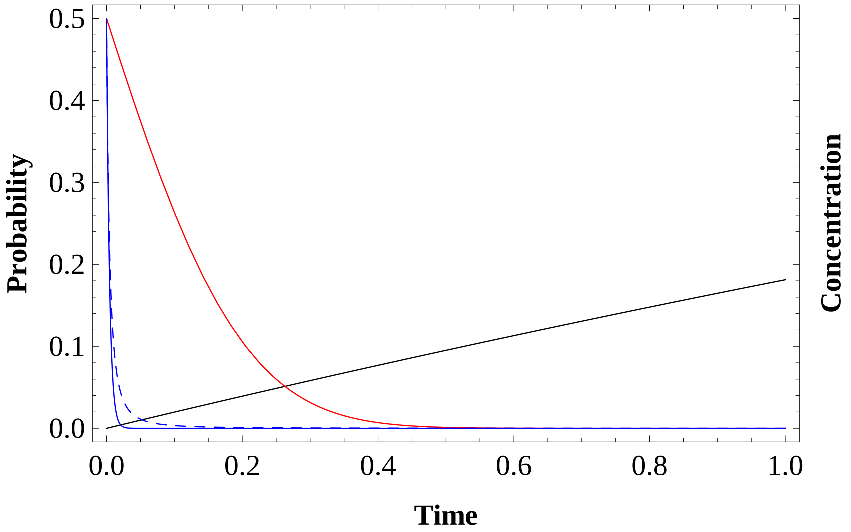

Figure 3.14: Error probabilities of the various transmitters (operated at $\bar{N} = 500$ photons) as a function of time t (abstract units). The red curve refers to the probability of the classical coherent transmitter $\bar{p}_{\text{coh}}$. The Blue curves refer to the quantum EPR transmitter $\bar{p}_{\text{quant}}^{\text{QCB}}$ for single-mode probing $M = 1$ (dashed curve) and broadband probing $M \to +\infty$ (solid curve). We also show the corresponding behavior of the concentration (solid black curve) which increases in time.

Let us start by describing the photodegradable model, assuming, as in the previous sections, that $\tau_0 = 1$ and $\tau_1 := \tau < 1$. We can introduce a simple saturation effect by imposing that the lower transmissivity τ tends to 1 for increasing energies. This may be realized by imposing the exponential law

$$\tau = 1 - \theta_1 \exp(-\theta_2 \bar{N}) \tag{3.88}$$

where $\bar{N}$ is the mean total number of photons employed in the readout, while θ_1 and θ_2 are parameters of the phenomenological model. More specifically, parameter θ_1 provides the value at zero energy (which is $1 - \theta_1$), and parameter θ_2 gives the speed of convergence to 1. Note that the literature on mathematical modeling of photodegradable effects is very limited. Our model corresponds to an inverted Brody model, to be interpreted as a death rate superimposed to the population. See Fig. 3.15 for numerical examples.

In order to evaluate the effects of this saturation behavior, we have to combine the law of Eq. (3.88) with the energy-dependent performances of the quantum and classical transmitters. First of all, we connect the error probability in the channel discrimination $\bar{p}$ with the amount of information retrieved I. This connection is given by the formula

$$I(\bar{p}) = 1 - H(\bar{p}),$$

where $H(\bar{p}) := -\bar{p}\log_2 \bar{p} - (1-\bar{p})\log_2(1-\bar{p})$ is the binary Shannon entropy. Thus, for the coherent transmitter, we have $I_{\text{coh}} := I(\bar{p}_{\text{coh}})$ where $\bar{p}_{\text{coh}}(\tau, \bar{N})$ is given in Eq. (3.55). For the quantum EPR transmitter, we have $I_{\text{quant}} := I(\bar{p}^{\text{QCB}}_{\text{quant}}) \leq I(\bar{p}_{\text{quant}})$, where the QCB $\bar{p}^{\text{QCB}}_{\text{quant}}(\tau, \bar{n}, M)$ is given in Eq. (3.73) and $\bar{n}M = \bar{N}$. Thus, for any fixed choice of the parameters θ_1 and θ_2, we can replace $\tau(\bar{N})$ into the previous information quantities, so to have $I_{\text{coh}} = I_{\text{coh}}(\bar{N})$ and $I_{\text{quant}} = I_{\text{quant}}(\bar{N}, M)$.

At fixed values of the energy $\bar{N}$, we then compare the number of bits retrieved by the classical transmitter $I_{\text{coh}}(\bar{N})$ with those retrieved by the quantum EPR transmitter $I_{\text{quant}}(\bar{N}, M)$ for $M = 1$ (i.e., a single energetic mode with $\bar{N}$ mean photons) and for $M \to +\infty$ (i.e., an infinite number of modes with vanishing mean photons $\bar{N}/M$). The performance of the quantum transmitter for arbitrary M will be bounded by these two extremal curves. This comparison is shown in Fig. 3.16 where we assume several values for the parameters θ_1 and θ_2. From the previous figure it is clear that we can consider photodegradable models such that the classical transmitter is not able to retrieve any information, while the EPR transmitter can retrieve almost all the information in a range of energies, depending on the θ's.

Thus our analysis shows that entanglement can be indeed exploited for non-invasive readout of fragile samples which tend to fade out as a consequence of being irradiated with energy. Our study considers a specific model of photo-degradation. We are currently looking at biological material whose behavior may approximate this law in order to propose an experiment.

Also note that this extreme situation could be exploited for cryptographic tasks. An optical memory could be purposely constructed to be photo-degradable in such a way to hide its encoded classical data from any standard optical drives based on the use of coherent (or thermal) light. Only an advanced laboratory able to engineer a quantum entangled source in the correct window of energy will be able to read out the stored confidential data. From this point of view, quantum reading can provide a potential technological layer of security based on the fact that the generation of entanglement and other non-classical features is only possible in more advanced labs of quantum optics. Furthermore, the range of energy to be used must also be very well-tailored depending on the specific parameters θ_1 and θ_2 employed during data storage, which means that even an eavesdropper with an advanced laboratory is likely to destroy the data. These concepts are clearly preliminary but the basic ideas could further be developed into potential practical applications.

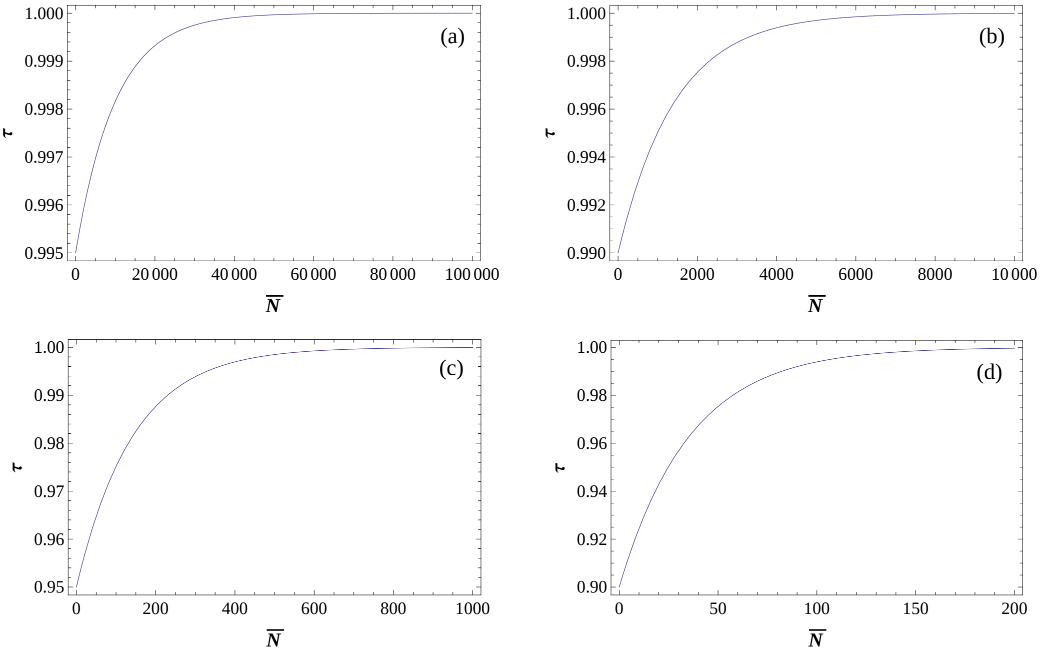

Figure 3.15: Lower transmissivity τ versus mean total number of photons $\bar{N}$ for various choices of the parameters θ_1 and θ_2 in the exponential law of Eq. (3.88). We have $(\theta_1, \theta_2) = (5 \times 10^{-3}, 10^{-4})$ in panel **(a)**; $(\theta_1, \theta_2) = (10^{-2}, 7 \times 10^{-4})$ in panel **(b)**; $(\theta_1, \theta_2) = (5 \times 10^{-2}, 7 \times 10^{-3})$ in panel **(c)** and $(\theta_1, \theta_2) = (10^{-1}, 28 \times 10^{-3})$ in panel **(d)**. As we can see from the panels, we have different types of saturation depending on the chosen values of the θ's. Note that the main difference between these plots is in the different range of values for the axes.

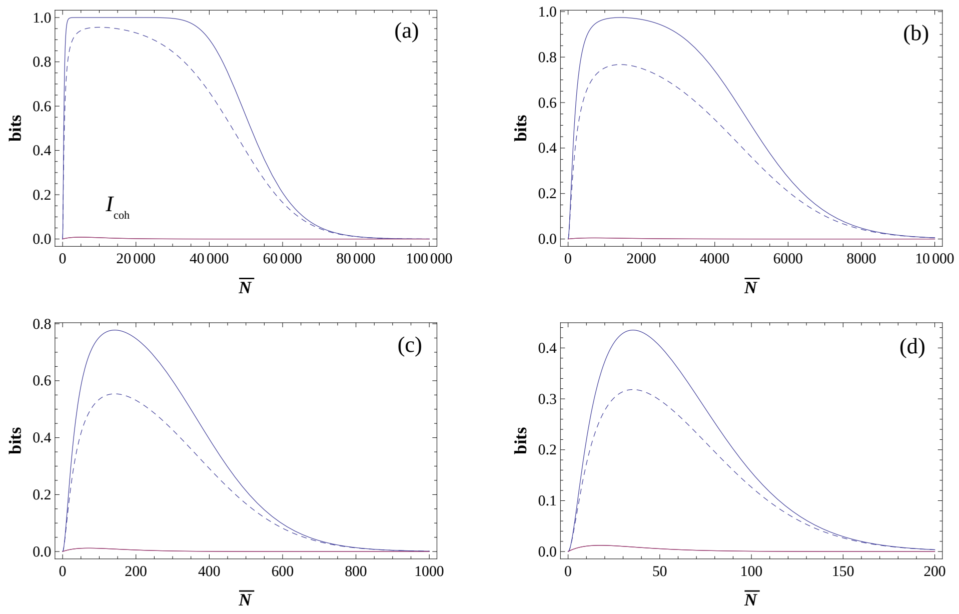

Figure 3.16: Number of bits which are retrieved by irradiating $\bar{N}$ mean total number of photons. In each panel, the red curve close to zero is the performance of the classical coherent transmitter $I_{\text{coh}}(\bar{N})$. The dashed blue curve is the performance of a single-mode EPR transmitter $I_{\text{quant}}(\bar{N}, M = 1)$, while the solid blue curve is the performance of a broadband EPR transmitter $I_{\text{quant}}(\bar{N}, M \to +\infty)$. Any EPR transmitter at fixed energy $\bar{N}$ and arbitrary number of modes M has a performance between the dashed and the solid blue curves. Panels refer to various choices of θ_1 and θ_2 in the exponential law of Eq. (3.88). As in Fig. 3.15 we have $(\theta_1, \theta_2) = (5 \times 10^{-3}, 10^{-4})$ in panel (a); $(\theta_1, \theta_2) = (10^{-2}, 7 \times 10^{-4})$ in panel (b); $(\theta_1, \theta_2) = (5 \times 10^{-2}, 7 \times 10^{-3})$ in panel (c) and $(\theta_1, \theta_2) = (10^{-1}, 28 \times 10^{-3})$ in panel (d).

3.2.7 Model combining growth and photo-degradability

In this section, we combine the two models of growth and photo-degradability into a single model. The simplest way to combine the two models is to consider the multiplication of the two effects described by Eqs. (3.87) and (3.88), so to have

$$\tau(t, \bar{N}) = 10^{-c_0[1-\exp(-gt)]} \left[1 - \theta_1 \exp(-\theta_2 \bar{N})\right]. \qquad (3.89)$$

This law provides the behavior of the transmissivity in terms of time t and input energy $\bar{N}$ for various possible parameters of growth (c_0 and g) and photodegradability (θ_1 and θ_2). In Fig. 3.17 we show how the performance of the quantum and classical transmitters behave in terms of the input energy at different times. The plots show that the quantum transmitter is clearly outperforming the classical benchmark in a very wide range of energies and this property is maintained over time, even if at longer times and higher energies the classical transmitter starts to become comparable in performance.

3.2.8 Discussion

We have shown how the use of quantum sources (in particular, EPR states) greatly outperforms the use of classical strategies (based on coherent state transmitters) for the quantum sensing of loss at low photon numbers, with natural applications to the non-invasive detection of small concentrations in biomedical samples. In our study we consider both the cases of symmetric and asymmetric quantum hypothesis testing, using the recently-developed tools of quantum Chernoff bound and quantum Hoeffding bound.

The advantage of the quantum probe is remarkable at short times, so that a potential application is also related with the fast detection of a slow growing diseases. The strong correlations of quantum light can in fact pick very small changes in the properties of a sample (e.g., a blood sample) well in advance with respect to a standard source, not to mention comparison with the very inefficient thermal sources used in today's labs.

Introducing phenomenological models of bacterial/cell growth and photo-degradability, we have shown how the quantum advantage can be made extreme for tasks such as the non-destructive testing of biological samples. These principles could be exploited to design more advanced types of biological instrumentations, such as non-invasive quantum-enhanced spectro-photometers for concentration detection and measurement.

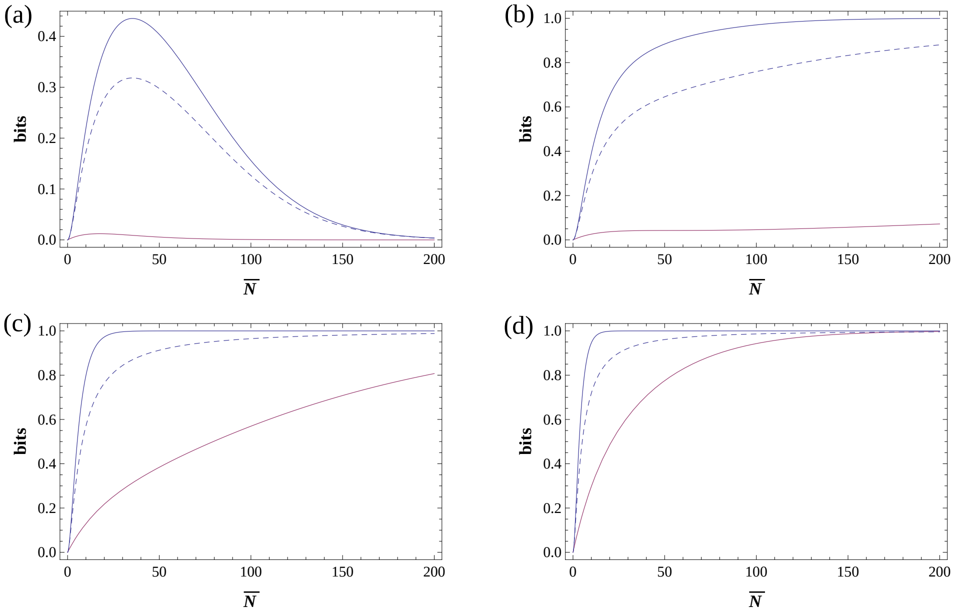

Figure 3.17: Number of bits which are retrieved by irradiating $\bar{N}$ mean total number of photons at different times $t = 0, 1, 5$, and 10 from top left panel (a) to bottom right panel (d). In each panel, the red curve is the performance of the classical coherent transmitter $I_{\text{coh}}(t, \bar{N})$. The dashed blue curve is the performance of a single-mode EPR transmitter $I_{\text{quant}}(t, \bar{N}, M = 1)$, while the solid blue curve is the performance of a broadband EPR transmitter $I_{\text{quant}}(t, \bar{N}, M \to +\infty)$. Any EPR transmitter at fixed energy $\bar{N}$ and arbitrary number of modes M has a performance between the dashed and the solid blue curves. Panels refer to the dynamical model in Eq. (3.89). We have chosen $(\theta_1, \theta_2) = (10^{-1}, 28 \times 10^{-3})$ and $(c_0, g) = (1, 0.02)$.

3.3 Cryptographic quantum reading

A practical scenario where the quantum detection of loss is important is that of quantum reading [50], where the aim is to boost the retrieval of classical data from an optical disk by exploiting quantum entanglement at low photon numbers. A basic setup for quantum reading consists of a series of cells, each one encoding a bit of information. This is physically done by picking two different reflectivities, r_0 and r_1, each encoding a different bit value. A target cell is then read by shining optical modes on it (generated by the transmitter) and detecting their reflection back to a receiver. The use of an entangled source is known to retrieve more information than any classical source (e.g., based on mixture of coherent states). With respect to previous literature [42,50,53,69], we now show that the advantage given by quantum EPR transmitter can be made extreme by introducing a suitable photodegradable model for the memory.

3.3.1 Introduction

Quantum cryptography [78] aims to realize a completely unbreakable scheme for the distribution of a secret key between two remote parties, usually called Alice and Bob. Indeed quantum key distribution (QKD) relies its security on one of the most fundamental physical laws, the uncertainty principle, which is actively exploited for detecting and overcoming the presence of a malicious eavesdropper, usually called Eve. In this scenario, an important role is also played by quantum entanglement, which can be exploited to make QKD protocols device-independent, i.e., more robust to practical flaws (e.g., in the detectors) which may potentially be exploited by Eve. Very recently, quantum discord [43] has also been identified as a useful resource for device-dependent QKD with trusted noise [51], e.g., in scenarios such as measurement-device independent QKD [16,47,54,57].

In this section, we investigate a different but still important problem: The confidential storage of information on a physical device, such as an optical memory. It has recently been proven that quantum entanglement can provide an advantage in the readout of classical data from optical memories, especially in the low-energy regime, i.e., when a few photons are irradiated over the memory cells. This approach is known as quantum reading [42,50,53,69], a notable application of quantum channel discrimination to a practical task as the memory readout.

Here we show how the performance advantage given by quantum reading can be exploited to completely hide classical information in optical memories. The strategy is to design a photo-degradable optical memory whose cells have very close reflectivities (each reflectivity encoding a bit-value). Because of the photodegrable effects, each cell can only be read with a limited number of photons. In these low-energy conditions, we find that only well-tailored quantum sources (in particular, entangled) are able to discriminate two very close reflectivities and, therefore, retrieve the information stored in the cell. Specifically, we derive a simple analytical formula which relates the reflectivities of the memory cell with the mean number of photons to be employed by the quantum source.

This approach would provide a layer of technological security to the stored data, in the sense that only an advanced laboratory equipped with quantum-correlated sources would be able to read the information, whereas any other standard optical reader based on classical states, such as coherent states or even thermal states, can only extract a negligible number of bits.

The discussion is organized as follows. In Sec. 3.3.2, we briefly review the basic setup of quantum reading and we discuss the performances achievable by quantum entanglement and classical (coherent) states. Then, in Sec. 3.3.3 we show how to design memories which are not accessible to classical methods. Finally, Sec. 3.3.4 is for discussions.

3.3.2 Basic setup for quantum reading

For our purpose we consider the simplest version of quantum reading, considering only ideal optical memories, i.e., with high reflectivities, and neglecting decoherence effects. Each memory cell is assumed to be in one of two hypotheses: Non-unit reflectivity $r_0 := r < 1$ (encoding bit-value 0) or unit reflectivity $r_1 = 1$ (encoding bit-value 1). Mathematically, this is equivalent to distinguish between a lossy channel $\mathcal{E}_r$ whose loss parameter is the reflectivity $r < 1$ and an identity channel $\mathcal{I}$.

In symmetric quantum hypothesis testing, these two hypotheses have the same cost, so that we aim to optimize the mean error probability. In other words, we need to minimize $\bar{p} := p(H_1|H_0)p_0 + p(H_0|H_1)p_1$, where p_0 and p_1 are the *a priori* probabilities of the two hypotheses, while $p(H_1|H_0)$ is the probability of a false positive and $p(H_0|H_1)$ is the probability of a false negative. For simplicity, we consider here equiprobable hypotheses, i.e., $p_0 = p_1 = 1/2$, which means that a bit of information is stored per cell. The amount of information which is retrieved in the readout process is therefore given by $I_{\text{read}}(\bar{p}) = 1 - H(\bar{p})$, where $H(\bar{p}) = -\bar{p}\log_2\bar{p} - (1-\bar{p})\log_2(1-\bar{p})$ is the binary formula of the Shannon entropy [21].

To distinguish between the two hypotheses Alice exploits an input source of light (a transmitter) and an output detection scheme (a receiver). In the classical reading setup, the transmitter consists of a single bosonic mode, the signal (S), which is prepared in a coherent state $|\alpha\rangle$ sent to the memory cell. At the output, the receiver is typically a photodetector counting the number of photons reflected, followed by a digital processing based on a classical hypothesis test. The performance of this receiver can be bounded by considering an optimal quantum measurement, constructed from the Helstrom matrix $\rho_0 - \rho_1$ of the two possible output states $\rho_0 = |\sqrt{r}\alpha\rangle\langle\sqrt{r}\alpha|$ and $\rho_1 = |\alpha\rangle\langle\alpha|$.

The minimum error probability is given by the Helstrom bound [33] which is here very simple to compute since the two states are pure. By a simple adaptation of previous derivations we write the mean error probability

$$\bar{p}_{\text{coh}}(\bar{n},r) = \frac{1-\sqrt{1-e^{-\bar{n}(1-\sqrt{r})^2}}}{2}, \tag{3.90}$$

where $\bar{n} = |\alpha|^2$ is the mean number of photons of the input coherent state. Thus, this transmitter is able to read an average of $I_{\text{read}}^{\text{class}} = I_{\text{read}}(\bar{p}_{\text{class}})$ bits per cell.

In the quantum reading setup, we consider a transmitter composed of two entangled modes, the signal (S) and the reference (R). This is taken to be an EPR state, i.e., a two-mode squeezed vacuum state [78]. As already discussed in previous sections, this is a zero-mean pure Gaussian state $|\mu\rangle_{SR}$ with CM

$$\mathbf{V}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \quad \begin{array}{l} \mathbf{Z} := \text{diag}(1,-1), \\ \mathbf{I} := \text{diag}(1,1), \end{array} \tag{3.91}$$

where $\mu \geq 1$ quantifies both the mean number of thermal photons in each mode, given by $\bar{n} = (\mu-1)/2$, and the amount of entanglement between the signal and reference modes.

The signal mode, with $\bar{n}$ mean photons, is sent to read the memory cell and its reflection S' is combined with the reference mode in an optimal quantum measurement. Given the state $\rho_{SR} = |\mu\rangle_{SR}\langle\mu|$ of the input modes S and R, we get two possible states

$$\sigma_0 = (\mathcal{E}_r \otimes \mathcal{I})(\rho_{SR}), \tag{3.92}$$

$$\sigma_1 = (\mathcal{I} \otimes \mathcal{I})(\rho_{SR}) = \rho_{SR}, \tag{3.93}$$

for the output modes S' and R at the receiver. One is just the input EPR state, while the other state σ_0 is a mixed Gaussian state with CM

$$\mathbf{V}_0(\mu,r) = \begin{pmatrix} (r\mu+1-r)\mathbf{I} & \sqrt{r(\mu^2-1)}\mathbf{Z} \\ \sqrt{r(\mu^2-1)}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}. \tag{3.94}$$

The minimum mean error probability is given by the Helstrom bound $\bar{p}_{\text{quantum}} = [1-D(\sigma_0,\sigma_1)]/2$, where $D(\sigma_0,\sigma_1)$ is the trace distance between σ_0 and σ_1. As usual, we resort to the easier-to-compute quantum Chernoff bound (QCB) [3, 4, 46, 52]

$$\bar{p}_{\text{quantum}}^{\text{QCB}} := \frac{C}{2}, \quad C := \inf_{s\in(0,1)} C_s, \tag{3.95}$$

where $C_s := \text{Tr}(\sigma_0^s\sigma_1^{1-s})$ is the generalized overlap between the two states. In the specific case where one of the output states is pure $\sigma_1 = |\varphi\rangle\langle\varphi|$, we may write $C = F$, using the quantum fidelity $F = \langle\varphi|\sigma_0|\varphi\rangle$. For zero-mean Gaussian states, this fidelity can easily be computed in terms of their CMs. In fact, we have

$$F = \frac{4}{\sqrt{\det[\mathbf{V}(\mu) + \mathbf{V}_0(\mu, r)]}} = \left(1 + \bar{n} + \bar{n}\sqrt{r}\right)^{-2} . \tag{3.96}$$

As a result, the mean error probability associated with this quantum transmitter is upperbounded by the QCB as follows

$$\bar{p}_{\text{quantum}} \leq \bar{p}^{\text{QCB}}_{\text{quantum}} = \frac{(1 + \bar{n} + \bar{n}\sqrt{r})^{-2}}{2}. \tag{3.97}$$

Thus, the EPR transmitter is able to read at least $I^{\text{quant}}_{\text{read}} = I_{\text{read}}(\bar{p}^{\text{QCB}}_{\text{quantum}})$ bits per cell.

3.3.3 Data secured by quantum reading

We can compare the readout performances of the two transmitters by considering the information gain $\Delta := I^{\text{quant}}_{\text{read}} - I^{\text{class}}_{\text{read}}$. Its positivity means that quantum reading outperforms the classical readout strategy. In particular, for $\Delta \simeq 1$ bit per cell we have that the EPR transmitter reads all data, while the classical transmitter is not able to retrieve any information. Here we aim to exploit this feature to make the data storage secure in absence of entanglement (and, more generally, quantum resources). As we can see from Fig. 3.18, the value of the gain Δ is close to the maximum value of 1 bit per cell when the memory cell is characterized by very high reflectivities, i.e., $r \simeq 1$. In particular, the good region where $\Delta > 0.95$ is particularly evident at low photon numbers, while it tends to shrink towards $r = 1$ for increasing energy.

We now discuss how we can exploit this advantage of quantum reading for designing a secure classical memory. Let us expand the information quantities $I^{\text{class}}_{\text{read}}$ and $I^{\text{quant}}_{\text{read}}$ at the leading order in $(1 - r) \simeq 0$. We find

$$I^{\text{class}}_{\text{read}} \simeq \frac{\bar{n}(1 - r)^2}{\ln 256}, \quad I^{\text{quant}}_{\text{read}} \simeq \frac{\bar{n}^2(1 - r)^2}{\ln 4}. \tag{3.98}$$

At high reflectivities, there is a different behavior of these quantities in the mean number of photons $\bar{n}$. In particular, we may write

$$I^{\text{quant}}_{\text{read}} \simeq 4\bar{n} I^{\text{class}}_{\text{read}} . \tag{3.99}$$

According to Eq. (3.98), a non-trivial difference between $I^{\text{class}}_{\text{read}}$ and $I^{\text{quant}}_{\text{read}}$ arises by imposing the condition

$$1 - r = \bar{n}^{-1} . \tag{3.100}$$

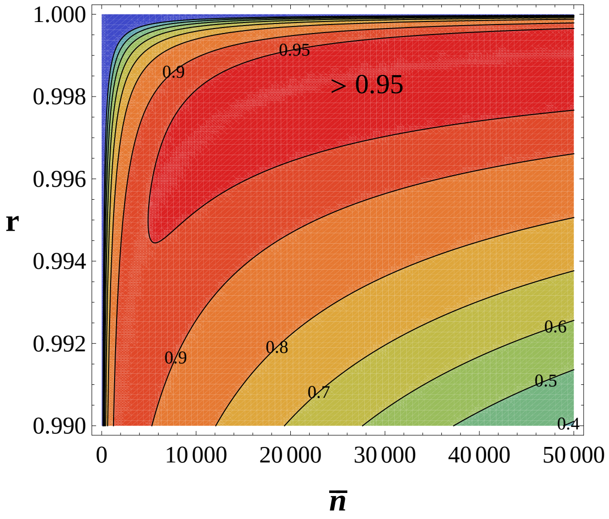

Figure 3.18: We plot $\Delta(\bar{n}, r)$ in the high-reflectivity range $0.99 \leq r < 1$ and wide range of $\bar{n}$ up to 5×10^4. We see how the EPR transmitter is superior for $r \simeq 1$, where Δ becomes close to 1 bit per cell.

This leads to the following behavior for large $\bar{n}$

$$I_{\text{read}}^{\text{class}} \simeq \frac{1}{\bar{n} \ln 256} \rightarrow 0, \quad I_{\text{read}}^{\text{quant}} \simeq \frac{\ln\left(\frac{2048}{81}\right) - 7\ln\left(\frac{9}{7}\right)}{\ln 512} \simeq 0.235. \tag{3.101}$$

From the latter equation we see that only quantum reading enables to retrieve non-zero information from the memory (combining this performance with suitable error correcting codes would enable us to achieve a complete readout of the memory). In the following Fig. 3.19, we show the behavior of the two information quantities $I_{\text{read}}^{\text{class}}$ and $I_{\text{read}}^{\text{quant}}$ in terms of the mean photon number $\bar{n}$ and assuming the condition of Eq. (3.100).

We can see that, at any fixed energy $\bar{n}$ irradiated over the memory cell, there is a memory with reflectivity r satisfying Eq. (3.100) which is readable by using a quantum transmitter with signal energy $\bar{n}$ but unreadable by a classical transmitter with the same irradiated energy $\bar{n}$. More precisely, any classical transmitter with energy up to $\bar{n}$ is inefficient. In fact, let us fix some value $\bar{n}_{\max}$ and consider a memory with $1 - r = \bar{n}_{\max}^{-1}$, then the performance of all classical transmitters with signal energy $\bar{n} \leq \bar{n}_{\max}$ is shown in Fig. 3.20. We see that the optimal classical transmitter is that with the maximal energy $\bar{n}_{\max}$ as clearly expected from the monotonic expression in Eq. (3.90).

Thus, if we construct a theoretical memory which can be irradiated with at most $\bar{n}_{\max}$ photons per cell (otherwise data is lost, e.g., due to photodegrable effects) and having reflectivity r satisfying Eq. (3.100), then this will be unreadable by any classical transmitter based on coherent states while its data can be retrieved by a

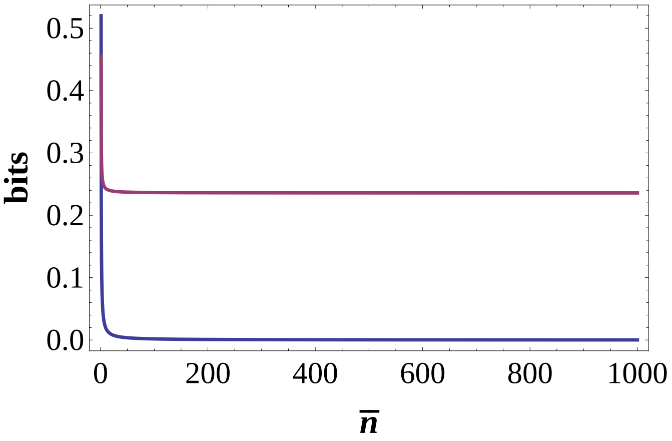

Figure 3.19: We plot $I_{\rm read}^{\rm class}$ (lower curve) and $I_{\rm read}^{\rm quant}$ (upper curve) versus the mean photon number $\bar{n} \geq 1$. We assume a memory with reflectivity r satisfying the condition of Eq. (3.100).

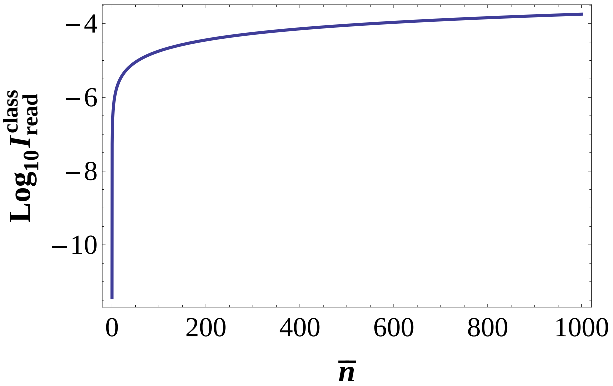

Figure 3.20: We plot the information quantity $I_{\rm read}^{\rm class}$ in log-scale for $\bar{n} \leq \bar{n}_{\max}$. We consider the readout of a memory with $1-r = \bar{n}_{\max}^{-1}$. Here we consider the numerical value $\bar{n}_{\max} = 1000$ but the behavior is generic.

quantum transmitter with signal energy $\simeq \bar{n}_{\max}$.

Note that we can design a memory with reflectivity r such that

$$1 - r = c\bar{n}^{-1}, \tag{3.102}$$

for some constant c. For large $\bar{n}$, we have $I_{\text{read}}^{\text{class}} \to 0$, while $I_{\text{read}}^{\text{quant}}$ tends to a constant ≤ 1 which depends on c. For instance, we have $I_{\text{read}}^{\text{quant}} \to 0.895$ for $c = 0.1$, and $I_{\text{read}}^{\text{quant}} \to 0.997$ for $c = 0.01$. In Fig. 3.21, we show the behavior of the two information quantities $I_{\text{read}}^{\text{class}}$ and $I_{\text{read}}^{\text{quant}}$ assuming Eq. (3.102) with $c = 0.1$. We see how the memories remain unreadable by classical means while the performance of quantum reading approaches 1 bit/cell.

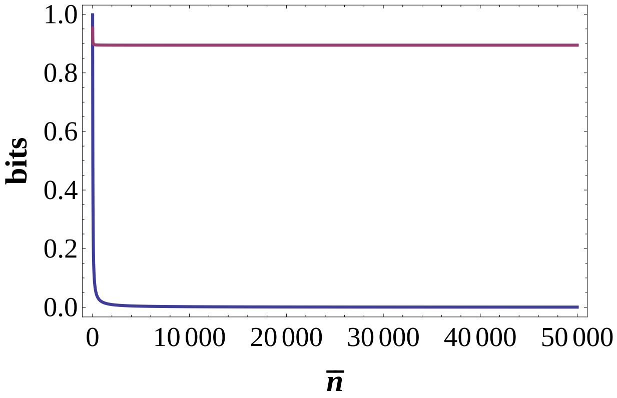

Figure 3.21: We plot the information quantities $I_{\text{read}}^{\text{class}}$ (lower curve) and $I_{\text{read}}^{\text{quant}}$ (upper curve) versus the mean photon number $\bar{n} \geq 1$. We consider memories with reflectivity r satisfying Eq. (3.102) with $c = 0.1$.

3.3.4 Discussion

In this study on the cryptographic aspects of quantum reading, we have shown how it is possible to construct classical memories which cannot be read by classical means, namely coherent states but still they can be read using quantum entanglement. In particular, we have considered an EPR state and we have connected the mean number of photons to be employed by this quantum source with the reflectivities to be used in the memory cells, see Eq. (3.100) and also its generalization in Eq. (3.102). Note that other non-classical states may also provide non-trivial advantages with respect to coherent states and their mixtures. In general, the security provided by the scheme relies on the technological difference between two types of laboratories, one limited to classical sources and the other able to access quantum features, such as entanglement or squeezing.

It is interesting to discuss the connections between our scheme of data-hiding by quantum reading and the traditional technique of quantum data hiding [23, 74].

The latter stores classical information into entangled states, so that it can only be retrieved by joint measurements. It is clearly an application of quantum state discrimination. By contrast, data-hiding by quantum reading is related to the problem of quantum channel discrimination. Classical data is stored in a channel (not a state) and quantum entanglement is used as an input resource to be processed by the channel. This is a crucial difference, also for practical purposes, since data stored in a classical memory does not decohere (like the entangled states typically prepared in quantum data hiding), and quantum entanglement is used a resource on demand, which is needed only for the readout of the information (not for the storage process).

Note that our study can be extended in several ways. We have only considered ideal memories where the cells are addressed individually and have very high reflectivities (in particular, we have assumed unit reflectivity for one of the two bit values stored in the cell). There is no inclusion of additional noise sources in the model, e.g., coming from stray photons scattered during the readout process, neither analysis of diffraction or other optical effects. Finally, we have also assumed that high values of entanglement can be generated. While this is possible theoretically, it is very hard to achieve experimentally. This would not be a problem if we were able to construct memories which are extremely photo-sensitive, so that the maximum values of tolerable energies are of the order of $\bar{n}_{\max} \lesssim 10$ photons per cell.

Chapter 4

Conclusions and future directions

This thesis has contributed to advance research in the field of quantum hypothesis testing in various aspects. First of all we have developed the theory of asymmetric quantum state discrimination in the context of Gaussian states, by deriving a procedure on how to compute the central tool of the quantum Hoeffding bound for these very important states. Our results can be used in quantum optics and continuous variable quantum information whenever one needs to compute the probability of false negatives in an asymmetric test which involves the use of Gaussian sources of light.

Using this approach and also that of the more standard symmetric quantum hypothesis testing, we have investigated practical applications in the context of quantum sensing and data readout, with potential applications in quantum technologies. In general, we have shown how quantum correlations (entanglement) may be used to boost the performance of quantum channel discrimination well-above the standard unassisted and classical strategies. This advantage has been proven at low energies, i.e., for low photon numbers.

In particular, we have discussed how we can model the probing of a biological sample (for retrieving information about a potential growth) as a problem of quantum channel discrimination. Using the Lambert-Beer law we have mapped this problem into a problem of Gaussian channel discrimination, for which we need to enforce an energetic constraint at the input. Imposing the non-invasive regime of few photons, we have proven that the use of entangled states (in particular, EPR states) outperforms any classical strategy which is based on the use of uncorrelated light (in particular, coherent states or thermal states as it happens in today's instruments such as spectrophotometers). This can have potential long-term implications for in-vivo and/or real-time screening of biological samples (e.g. RNA, DNA) and medical tissues.

Next directions involve the analysis of the performance of this non-invasive quantum sensing scheme in the presence of a blank sample which is not necessary an identity operation on the input state, but having some intrinsic transmissivity T_0. This is certainly a further step toward an experimental realization of the idea. Also it is an important step to formulate this more advanced scheme in the context of quantum metrology, where tools as the quantum Fisher information are very well studied in the literature.

A further step towards an experimental implementation is the characterization of biological material for which the photo-degradable effects are more evident. This is certainly true for DNA/RNA at UV frequencies. In today's labs we use spectrophotometers equipped with a UV lamp, UV-transparent cuvettes (depending on the instrument) and a solution of purified DNA. Absorbance readings are performed at 260nm where DNA absorbs light most strongly. Direct DNA damage occurs when the absorption of a UV photon affects thymine base pairs (next to each other in genetic sequences) in such a way that they bond together into pyrimidine dimers. This causes a disruption in the strand, which means that reproductive enzymes cannot copy anymore. RNA is subject to similar problems at roughly the same UV frequencies.

It would also be interesting to identify biological material which is very fragile at optical frequencies (say 400-800nm) where the tools of quantum optics are currently more developed. Besides looking at the literature, this investigation would need a close interaction between a biology lab and a quantum optics lab, so to find the best compromise between potential samples and currently available sources of quantum light. The identification of an extremely photo-degradable material at the optical frequencies will also be useful for implementing the idea of cryptographic quantum reading, where this material would be used to encode confidential data in the cells of a memory.

Appendices

Appendix A

Continuous-variable systems

A.1 Quantization of the electromagnetic field (basic intuition)

By solving Maxwell's equations within an infinite square box, we derive the decomposition of the electromagnetic field into planar waves or bosonic modes [40, 77]. In particular, a single mode of the field is a propagating wave with fixed frequency ν, fixed direction of propagation $\vec{k}$ and fixed polarization $\vec{z}$. Its electric field can be written as

$$\vec{E}(\vec{r},t) = E\ \vec{z}[q\cos(\omega t - \vec{k}\cdot\vec{r}) + p\sin(\omega t - \vec{k}\cdot\vec{r})], \tag{A.1}$$

where E contains all the physical units. For fixed ν, $\vec{k}$ and $\vec{z}$, we have that q and p remain free parameters. In a few words, in classical electromagnetism, the state of the mode is determined by two "classical quadratures" q and p.

According to Eq. (A.1), the quadratures represent two components of the electric field. In particular, the position-quadrature q is the in-phase component of the field with respect to a reference signal $\approx \cos(\omega t - \vec{k}\cdot\vec{r})$, while the momentum-quadrature p is the out-phase component (having a $\pi/2$ dephasing with respect to the reference signal). Note that they are called position and momentum quadratures, because they are similar to the position and momentum of a mechanical oscillator.

The position and momentum quadratures span a bi-dimensional real vector space which is called the "phase-space". In this space, the classical state of a mode corresponds to a single point $x = (q,p)^T$. From an intuitive point of view, the extension from the classical to the quantum description of the field corresponds to the introduction of quantum noise in the phase-space, so that the single point is replaced by a continuum set of points which can be taken with different probabilities.

More precisely, the quantization of a mode corresponds to introducing a quasi-probability distribution, called the "Wigner function" $W(x)$, which is defined over the entire phase space. Mathematically, $W(x)$ is normalized to one, i.e., $\int dx\, W(x) = 1$ (as a probability density), but it can have negative values in the general case $W(x) \ngeq 0$ (contrarily to what happens to probability densities which are positive).

The Wigner function may be used to represent the quantum state of a mode. Its contour identifies the set of the most probable points, an intuitive picture which is particularly appropriate for Gaussian states, i.e., those quantum states having Gaussian Wigner function.

A.2 Bosonic systems and quadrature operators

A more rigorous way to quantize the electromagnetic field is replacing the classical quadratures, q and p, in the expression of the mode of Eq. (A.1), with two non-commuting quantum operators, $\hat{q}$ and $\hat{p}$, with $[\hat{q},\hat{p}]=2i$, so that we have the quantum electric field [40, 77]

$$\hat{E}(\vec{r},t)=E\ \vec{z}[\hat{q}\cos(\omega t-\vec{k}\cdot\vec{r})+\hat{p}\sin(\omega t-\vec{k}\cdot\vec{r})]. \tag{A.2}$$

This procedure transforms the mode from being a classical system to being a bosonic quantum system.

Formally, a bosonic system (or bosonic mode) is a quantum system with an infinite-dimensional Hilbert space $\mathcal{H}$, which is associated with two quadrature operators, $\hat{q}$ and $\hat{p}$, such that $[\hat{q},\hat{p}]=2i$. Given an arbitrary state ρ of the system, the two quadratures have mean values

$$\bar{q}=\langle\hat{q}\rangle_{\rho}=\mathrm{Tr}\left(\hat{q}\rho\right),\quad \bar{p}=\langle\hat{p}\rangle_{\rho}=\mathrm{Tr}(\hat{p}\rho), \tag{A.3}$$

and variances

$$V\left(\hat{q}\right)=\left\langle\hat{q}^{2}\right\rangle_{\rho}-\langle\hat{q}\rangle_{\rho}^{2},\ V\left(\hat{p}\right)=\left\langle\hat{p}^{2}\right\rangle_{\rho}-\langle\hat{p}\rangle_{\rho}^{2}. \tag{A.4}$$

Because of $[\hat{q},\hat{p}]=2i$, we have that the two quadratures must satisfy the uncertainty principle

$$V\left(\hat{q}\right)V\left(\hat{p}\right)\geq 1, \tag{A.5}$$

which expresses the incompressibility of the quantum noise.

A.3 Ladder operators and Fock basis

Besides the two quadratures $\hat{q}$ and $\hat{p}$, a bosonic mode may be characterized by two "ladder operators", known as the annihilation operator

$$\hat{a}=\frac{\hat{q}+i\hat{p}}{2} \tag{A.6}$$

and the creation operator

$$\hat{a}^{\dagger}=\frac{\hat{q}-i\hat{p}}{2}, \tag{A.7}$$

with commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$. Equivalently, we may write

$$\hat{q} = \hat{a} + \hat{a}^\dagger, \ \hat{p} = \frac{\hat{a}^\dagger - \hat{a}}{i}. \tag{A.8}$$

From the ladder operators we define the "number operator"

$$\hat{n} := \hat{a}^\dagger \hat{a} = \frac{\hat{q}^2 \hat{p}^2}{4} - \frac{1}{2}, \tag{A.9}$$

which is an observable representing the number of photons in the bosonic mode. In fact, adopting the procedure of quantization $(q, p) \to (\hat{q}, \hat{p})$, the energy of the mode becomes the following observable

$$E = \frac{1}{2}(q^2 + p^2) \to \hat{E} = \frac{1}{2}(\hat{q}^2 + \hat{p}^2). \tag{A.10}$$

Using Eqs. (A.8) and (A.9) in Eq. (A.10), we obtain

$$\hat{E} = 2\hat{n} + 1 \ , \tag{A.11}$$

so that the energy of the mode is expressed in terms of number of photons $\hat{n}$ plus the energy of the vacuum (equal to 1, in our notation).

Using the number operator $\hat{n}$ we can construct a basis for the Hilbert space of the mode. This corresponds to solving the eigensystem

$$\hat{n}|n\rangle = n|n\rangle \ , \tag{A.12}$$

were $n = 0, 1, ... + \infty$ are the eigenvalues of $\hat{n}$ (representing the number of photons), and $|n\rangle$ are the eigenkets of $\hat{n}$ (representing those states with number of photons exactly equal to n). The eigenset $\{|n\rangle\}_{n=0}^{+\infty}$ provides an orthonormal basis, which is called the "Fock basis" or the "number basis". This is also a basis for the energy, since $\hat{n}$ and $\hat{E}$ are compatible observables.

Thus we have a bosonic mode whose ∞-dimensional Hilbert space $\mathcal{H}$ is spanned by the Fock basis. An arbitrary ket $|\varphi\rangle \in \mathcal{H}$ can be decomposed in this basis as

$$|\varphi\rangle = \sum_{n=0}^{+\infty} \varphi_n |n\rangle \tag{A.13}$$

where the coefficients are given by the inner product $\varphi_n = \langle n \, |\varphi\rangle$. Here $p(n) = |\varphi_n|^2$ is the probability that the state $|\varphi\rangle$ contains n photons. It is the probability that we measure n photons when we detect the mode by using a positive operator-valued measure (POVM) $\{\hat{\Pi}_n\}$ with measurement operator $\hat{\Pi}_n = |n\rangle\langle n|$, i.e., a quantum measurement which projects on the Fock basis.

Finally, we discuss the action of the ladder operators on the Fock states. The annihilation operator $\hat{a}$ destroys one photon. Given a Fock state $|n\rangle$, we have

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad \text{for } n \geq 1, \tag{A.14}$$

$$\hat{a}|0\rangle = 0 \ . \tag{A.15}$$

On the contrary, the creation operator $\hat{a}^\dagger$ generates one photon, i.e., we have

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{A.16}$$

An arbitrary Fock state $|n\rangle$ can be generated by n consecutive applications of the creation operator $\hat{a}^\dagger$ starting from the vacuum state

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle. \tag{A.17}$$

A.4 Coherent states and displacement operator

Coherent states are defined as the eigenkets of the annihilation operator $\hat{a}$ with complex eigenvalues $\alpha \in \mathbb{C}$

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{A.18}$$

Given a coherent state $|\alpha\rangle$ with amplitude α, it can be generated from the vacuum state $|0\rangle$ by applying the so-called "displacement operator" $\hat{D}(\alpha)$, i.e., we have

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle. \tag{A.19}$$

The displacement operator can be defined in terms of the ladder operators as

$$\hat{D}(\alpha) = \exp[\alpha\hat{a}^\dagger - \alpha^*\hat{a}], \tag{A.20}$$

and it is a unitary operator

$$\hat{D}^\dagger(\alpha) = \hat{D}^{-1}(\alpha) = \hat{D}(-\alpha). \tag{A.21}$$

The displacement operator can also be expressed in terms of the quadratures operators $\hat{q}$ and $\hat{p}$. Using Eqs. (A.6) and (A.7) in Eq. (A.20), we derive the Weyl operator

$$\hat{D}(x) = \exp\left[\frac{i}{2}(p\hat{q} - q\hat{p})\right], \tag{A.22}$$

where $x = (q,p)^T$. In particular, we may displace along a specific quadrature, since

$$\hat{D}(q) \equiv \hat{D}(q,0) = \exp^{-\frac{i}{2}(q\hat{p})} \tag{A.23}$$

displaces in position q, while

$$\hat{D}(p) \equiv \hat{D}(0, p) = \exp^{\frac{i}{2}(p\hat{q})} \tag{A.24}$$

displace in momentum p.

Coherent states are correctly normalized $\langle\alpha|\alpha\rangle = 1$, but they are non-orthogonal since they have non-zero overlap

$$\langle\alpha|\beta\rangle = \exp\left(\alpha^*\beta - \frac{|\alpha|^2 + |\beta|^2}{2}\right) \neq 0. \tag{A.25}$$

Despite this, they form a basis for the Hilbert space $\mathcal{H}$, so that an arbitrary ket $|\varphi\rangle \in \mathcal{H}$ can be written as

$$|\varphi\rangle = \int_{\mathbb{C}} d^2\varphi(\alpha)|\alpha\rangle \ .$$

Finally, it is important to note that coherent states are quantum states with minimum uncertainty, since they saturate the uncertainty principle in a symmetric way $V(\hat{q}) = V(\hat{p}) = 1$.

A.5 Squeezed states and squeezing operator

There exist quantum states which are of minimum uncertainty but their quantum noise is distributed asymmetrically between the two quadratures. In other words, they satisfy $V(\hat{q})V(\hat{p}) = 1$ with $V(\hat{q}) \neq V(\hat{p})$. These states can be derived from the vacuum state applying a particular unitary operator called "squeezing operator"

$$|r\rangle = \hat{S}(r)|0\rangle \tag{A.26}$$

where

$$\hat{S}(r) = \exp[\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})], \tag{A.27}$$

with the real number r being the squeezing factor. The pure state $|r\rangle$ is called the "squeezed vacuum" and has quadratures with variances equal to

$$V(\hat{q}) = e^{-2r}, \ V(\hat{p}) = e^{2r} \ . \tag{A.28}$$

Therefore, we see that for $r > 0$ we have squeezing in position, while for $r < 0$ we have squeezing in momentum. In general, we may consider a displaced squeezed state with squeezing r and amplitude α, which is achieved by displacing the squeezed vacuum

$$|\alpha, r\rangle = \hat{D}(\alpha)|r\rangle = \hat{D}(\alpha)\hat{S}(r)|0\rangle. \tag{A.29}$$

A.6 Infinitely-squeezed states

Starting from the squeezed states we can construct the eigenstates of the quadratures, i.e, those states where the quadratures are perfectly defined. These eigenstates are realized in the limit of the infinite squeezing. For instance, from the squeezed vacuum state

$$|0, r\rangle = \hat{S}(r)|0\rangle, \tag{A.30}$$

we can take the two limits $r \to +\infty$ or $r \to -\infty$.In the first case ($r \to +\infty$), we realize an asymptotic state with zero position

$$|q = 0\rangle = \lim_{r \to +\infty} |0, r\rangle. \tag{A.31}$$

In the second case ($r \to -\infty$) we realize an asymptotic state with zero momentum

$$|p = 0\rangle = \lim_{r \to -\infty} |0, r\rangle. \tag{A.32}$$

By using the Weyl operators, we can now displace these states to create all the other states with q and p arbitrary, i.e.,

$$|q\rangle = \hat{D}(q)|q\rangle, \ |p\rangle = \hat{D}(p)|p\rangle \ . \tag{A.33}$$

These asymptotic states represent the eigenkets of the quadratures operators $\hat{q}$ and $\hat{p}$, i.e. we have

$$\hat{q}|q\rangle = q|q\rangle, \ \hat{p}|p\rangle = p|p\rangle \ . \tag{A.34}$$

It is important to note that the asymptotic states $|q\rangle$ and $|p\rangle$ lie outside the Hilbert space of the system. Indeed, they are not normalizable, despite the fact that they form an orthogonal set, i.e., we have

$$\langle q|q'\rangle = \delta(q - q'), \ \langle p|p'\rangle = \delta(p - p') \ , \tag{A.35}$$

where δ is the Dirac-delta defined by

$$\delta(x - x') = \begin{cases} 0 & \text{for } x \neq x' \ , \\ +\infty & \text{for } x = x' \ , \end{cases} \tag{A.36}$$

extending the Kronecker-delta $\delta_{kk'}$ to continuous variables.

Quadrature eigenstates are bases for the Hilbert space $\mathcal{H}$. For any ket $|\varphi\rangle \in \mathcal{H}$, we may write its decomposition in the position basis $\{|q\rangle\}$ as

$$|\varphi\rangle = \int_{-\infty}^{+\infty} dq \ \varphi(q)|q\rangle \ , \tag{A.37}$$

where $\varphi(q) = \langle q\,|\varphi\rangle$ is called the "wave-function" (in position) of the state. Its squared modulus $P(q) = |\varphi(q)|^2$ gives the probability density that we measure the value q of the position. This type of measurement is known as homodyne detection and is described by a POVM $\{\hat{\Pi}_q\}$ with measurement operator $\hat{\Pi}_q = |q\rangle\langle q|$. As one can easily verify, given a ket $|\varphi\rangle$, the outcome q is achieved with probability

$$\begin{aligned} P(q) &= \mathrm{Tr}(\Pi_q \, |\varphi\rangle\langle\varphi|) = \langle\varphi| \, \hat{\Pi}_q \, |\varphi\rangle && \text{(A.38)} \\ &= \langle\varphi| \, q\rangle\langle q \, |\varphi\rangle = |\varphi(q)|^2. && \text{(A.39)} \end{aligned}$$

Equivalently, we may decompose $|\varphi\rangle$ in the momentum basis $\{|p\rangle\}$ as

$$|\varphi\rangle = \int_{-\infty}^{+\infty} dp \; \varphi(p)|p\rangle \tag{A.40}$$

with $\varphi(p) = \langle p \, |\varphi\rangle$ the wave function in the momentum p. Then, $P(p) = |\varphi(p)|^2$ gives the probability density of the momentum. This is the output provided by a homodyne detector $\{\hat{\Pi}_p\}$ with measurement operator $\hat{\Pi}_p = |p\rangle\langle p|$. In general a POVM is a "Homodyne" detection if it realizes a projection on one of the quadratures (position q or momentum p).

A.7 Thermal states

Given the Fock basis $\{|n\rangle\}$, an arbitrary ket (pure state) can be decomposed as

$$|\varphi\rangle = \sum_{n=0}^{+\infty} \varphi_n |n\rangle, \;\; \varphi_n = \langle n|\varphi\rangle. \tag{A.41}$$

More generally, an arbitrary density operator (mixed state) can be decomposed as

$$\rho = \sum_{n,m} \rho_{n,m} \, |n\rangle\langle m| \, , \;\; \rho_{n,m} = \langle n|\rho|m\rangle. \tag{A.42}$$

A thermal state is a particular mixed state which is diagonal in the Fock basis. It is defined as

$$\rho(\bar{n}) = \sum_{n=0}^{+\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{\bar{n}+1}} \, |n\rangle\langle n| \;\; , \tag{A.43}$$

where $\bar{n}$ is a positive parameter ($\bar{n} \geq 0$) and corresponds to the mean number of photons in the mode. It is also called "thermal number" and is related to the temperature T of the environment.

In fact, a bosonic mode with frequency ν, which at thermal equilibrium with an environment at temperature T, is described by thermal state with mean number of photons equal to

$$\bar{n} = \frac{1}{\exp(\frac{h\nu}{KT}) - 1}, \tag{A.44}$$

where K is the Boltzmann constant and h the Plank's constant [59]. This is known as the Planck law of the black-body radiation.

Note that the thermal state has quadrature with variances

$$V(\hat{q}) = V(\hat{p}) = 2\bar{n} + 1 \ , \tag{A.45}$$

which are increasing in $\bar{n}$. Thus, for these states, the parameter $\bar{n}$ describes both the average energy (mean number of photons) and the noise of the state (variance of the quadratures). For $\bar{n} = 0$, the thermal state becomes the vacuum state, i.e., $\rho(0) = |0\rangle\langle 0|$.

Appendix B

Phase-Space Representations

Given a bosonic mode with Hilbert space $\mathcal{H}$ we can associate a corresponding phase-space $\mathcal{K}$. This is a 2-dimensional real vector space ($\backsimeq \mathbb{R}^2$) spanned by the two quadratures q and p, i.e., the eigenvalues of the quadrature operators $\hat{q}$ and $\hat{p}$ (these are "continuous variables" of the mode).

Mathematically, there is a one-to-one correspondence between a density operator ρ, acting on the Hilbert space $\mathcal{H}$, and a real function called the "Wigner function" $W(q,p)$, which is defined over the phase-space $\mathcal{K}$, i.e., $\rho \leftrightarrow W(q,p)$. In other words, a quantum state can equivalently be described by a density operator or by a corresponding Wigner function. The connection between these representations can be realized by means of the Weyl operator

$$\hat{D}(\xi) = \exp\left[i\hat{x}^T \Omega \xi\right] \ , \tag{B.1}$$

where $\xi \in \mathbb{R}^2$, $\hat{x} = (\hat{q}, \hat{p})^T$ and Ω is called the "symplectic form" and defined by

$$\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ . \tag{B.2}$$

As a first step we connect ρ to a "characteristic function" defined by

$$\chi(\xi) = \mathrm{Tr}[\rho \hat{D}(\xi)] \ . \tag{B.3}$$

Then we introduce the Wigner function $W(x)$ as a Fourier transformation of the characteristic function

$$W(x) = \mathrm{FT}\left[\chi(\xi)\right] = \int_{\mathbb{R}^2} \frac{d\xi}{4\pi^2} e^{ix^T \Omega \xi} \chi(\xi), \tag{B.4}$$

where $x = (q,p)^T \in \mathcal{K}$ is the conjugate variable of ξ.

It is important to note that the Wigner function is a quasi-probability distribution meaning that, in general, it can take negative values, even if it is correctly normalized to one

$$\int_{\mathbb{R}^2} d^2x \; W(x) = 1. \tag{B.5}$$

B.1 Single-mode Gaussian States

By definition, the quantum state ρ of a bosonic mode is called Gaussian if its Wigner function $W(x)$ is Gaussian, i.e., taking the form

$$W(x) = \frac{1}{2\pi\sqrt{\det \mathbf{V}}} \exp\left[-\frac{1}{2} (x - \bar{x})^T \mathbf{V}^{-1} (x - \bar{x}) \right]. \tag{B.6}$$

In this case,the Wigner function is positive $W(x) \geq 0$, therefore representing a bona-fide probability density.

As we may see from Eq. (B.6), a Gaussian $W(x)$ is fully characterized by the first- and second-order statistical moments, which are the mean value $\bar{x}$ and the covariance matrix (CM) $\mathbf{V}$. Explicitly, the mean value has components $\bar{x} = (\bar{q}, \bar{p})^T$ with

$$\bar{q} = \mathrm{Tr}(\hat{q}\rho), \; \bar{p} = \mathrm{Tr}(\hat{p}\rho), \tag{B.7}$$

while the CM can be written as

$$\mathbf{V} = \begin{pmatrix} V(\hat{q}) & C(\hat{q}, \hat{p}) \\ C(\hat{q}, \hat{p}) & V(\hat{p}) \end{pmatrix}, \tag{B.8}$$

where $V(\hat{q})$, $V(\hat{p})$ are the variances of the quadratures and

$$C(\hat{q}, \hat{p}) = \frac{\langle \hat{q}\hat{p} + \hat{p}\hat{q} \rangle}{2} - \bar{q}\bar{p} \tag{B.9}$$

is their covariance. The CM has important mathematical properties. It is a 2×2 real and symmetric matrix $\mathbf{V} \in \mathcal{M}(2 \times 2, \mathbb{R})$, $\mathbf{V}^T = \mathbf{V}$. It is positive-definite $\mathbf{V} > 0$ and, more strongly, it must satisfy the uncertainty principle, which is expressed by

$$\mathbf{V} + i\Omega \geq 0 \tag{B.10}$$

where Ω is the symplectic form of Eq. (B.2).

Thus, a Gaussian state is one-to-one with its first- and second-order statistical moments $\{\bar{x}, \mathbf{V}\}$. This is because a density operator ρ is one-to-one with its Wigner function $W(x)$ and, for a Gaussian state, the Wigner function is one-to-one with $\{\bar{x}, \mathbf{V}\}$. Clearly this is not true for a non-Gaussian state, whose non-Gaussian Wigner function generally depends an all the statistical moments. Because of the equivalence

$$\text{Gaussian } \rho \longleftrightarrow \{\bar{x}, \mathbf{V}\} \;, \tag{B.11}$$

we have that a few number of real parameters completely characterize the Gaussian state. In particular, we have 5 real parameters for a single-mode Gaussian state. Afterwards, when we consider multi-mode Gaussian states, we will see that the number of real parameters is still small in the sense that it grows polynomially in the number N of modes, as $2N^2 + 3N$. This efficient description of Gaussian states gives a non-trivial theoretical advantage. Furthermore, Gaussian states are very important experimentally too, since they are the most typical and common states which are generated in quantum optics labs.

B.1.1 Examples of Gaussian states

We review here the phase-space representation of the main Gaussian states of a bosonic mode. Mathematically, it is sufficient to give the expressions of their first two statistical moments $\bar{x}$ and $\mathbf{V}$. Geometrically, we can represent these states by designing their contours in the phase-space $\mathcal{K}$. We first identify a center point, which is given by the mean value $\bar{x}$, and then we design a contour whose shape and size depend on the CM. We may define the contour of a Gaussian Wigner function $W(x)$ as that curve $\mathcal{C}$ of the phase-space where the value of $W(x)$ is constantly equal to $(2\pi\sqrt{e})^{-1}$ (which is the value of the function which corresponds to one-standard deviation). In other words, the contour identifies that region of the phase-space where the quadratures q and p take the most probable values. It is therefore a very intuitive way to represent the quantum noise of the Gaussian state.

Let us review and represent the most important single-mode Gaussian states which are: vacuum state, coherent state, squeezed state and thermal state.

Vacuum State.

The vacuum state $|0\rangle$ is a pure Gaussian state with the simplest statistical moments

$$\bar{x} = 0, \;\; \mathbf{V} = \mathbf{I}, \tag{B.12}$$

where $\mathbf{I}$ is the 2-by-2 identity matrix. In other words, we have symmetric noise in the quadratures $V(\hat{q}) = V(\hat{p}) = 1$, which is the minimal possible allowed by the uncertainty principle (as already discussed). This unit value is the “quantum shot-noise” of the vacuum also known as the “vacuum noise”. In the phase-space, the vacuum state is represented by a circular contour centered in the origin, as shown in Fig. B.1.

Coherent states.

A coherent state corresponds to a displaced vacuum state $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$, with $\alpha = (\bar{q} + i\bar{p})/2$ being its complex amplitude. Its statistical moments are given by

$$\bar{x} = \begin{pmatrix} \bar{q} \\ \bar{p} \end{pmatrix}, \;\; \mathbf{V} = \mathbf{I}. \tag{B.13}$$

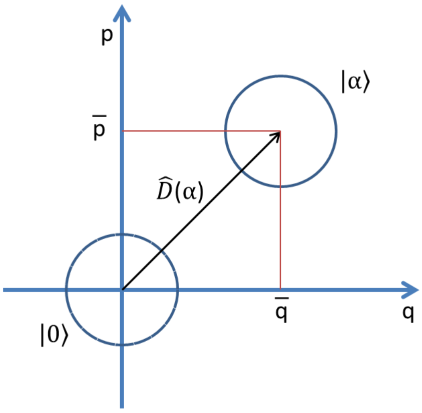

Figure B.1: Phase-space contour of the vacuum state (centered at the origin) and that of a coherent states with amplitude α.

Its phase-space contour is shown in Fig. B.1. Physically, a coherent state represents a semiclassical description for an electromagnetic wave, where the average signal profile of the electric field has superimposed quantum noise. Indeed, in the high-energy limit $\bar{n} = |\alpha|^2 \to +\infty$, a mode in a coherent state well describes a classical electromagnetic wave (with the ratio between the variances of the quadratures and their mean value going to zero).

Squeezed states.

First we consider the squeezed vacuum state, which is achieved by applying the squeezing operator to the vacuum state

$$|0, r\rangle = \hat{S}(r)|0\rangle \tag{B.14}$$

with $r \in \mathbb{R}$ being the squeezing factor. This is a pure Gaussian state with

$$\bar{x} = 0 \tag{B.15}$$

and

$$\mathbf{V} = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{B.16}$$

As we can see from the previous CM and the contours in Fig. B.2, positive squeezing ($r > 0$) shrinks the quantum noise in the position quadrature, while negative squeezing ($r < 0$) shrinks the noise in the other quadrature. In the limit of infinite squeezings ($r \to \pm\infty$), we realize the asymptotic quadrature eigenstates $|q = 0\rangle$ and $|p = 0\rangle$.

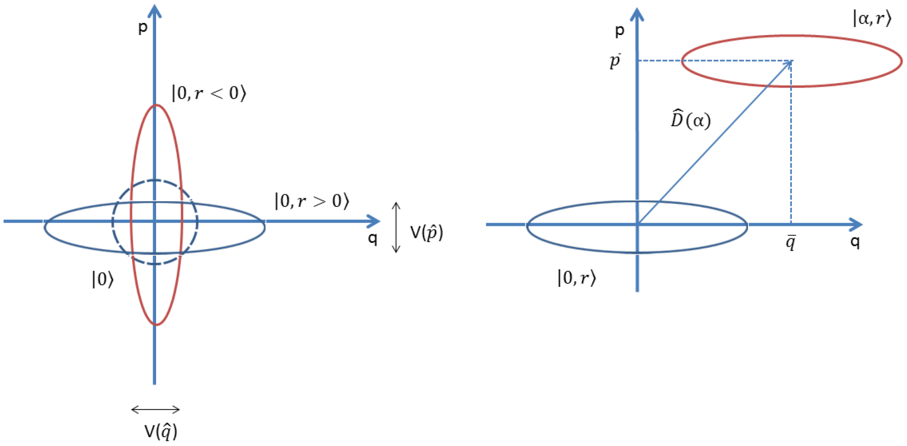

Figure B.2: **Left panel**. Squeezed vacuum states in position $|0, r > 0\rangle$ and momentum $|0, r < 0\rangle$. **Right panel**. Displaced squeezed state $|\alpha, r\rangle$ with amplitude α and squeezing r.

In general, we can have a displaced squeezed state, which obtained by applying the displacement operator to a squeezed vacuum state

$$|\alpha, r\rangle = \hat{D}(\alpha)|0, r\rangle = \hat{D}(\alpha)\hat{S}(r)|0\rangle. \tag{B.17}$$

This has mean value $\bar{x} = (\bar{q}, \bar{p})^T$ with components given by the amplitude of the displacement $\alpha = (\bar{q} + i\bar{p})/2$, and the same CM as before in Eq. (B.16).

Thermal states.

A thermal state is a mixed Gaussian state with density operator $\rho(\bar{n})$ depending on the thermal number $\bar{n} \geq 0$ (mean number of photons). Its statistical moments are

$$\bar{x} = 0, \ \mathbf{V} = \mu\mathbf{I} \tag{B.18}$$

where

$$\mu = 2\bar{n} + 1. \tag{B.19}$$

According to Eq. (B.19), all energy in the state (parameter $\bar{n}$) is in form of quantum noise (variance parameter μ). Clearly, we have the vacuum state for $\bar{n} = 0$. The phase-space contour of the thermal state is shown in Fig. B.3.

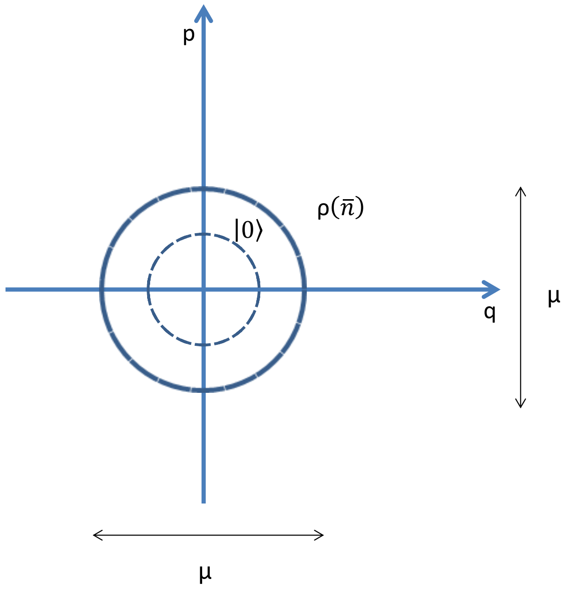

Figure B.3: Contour of a thermal state with variance parameter μ.

B.1.2 Gaussian unitaries or symplectic transformations

Until now we have studied single-mode Gaussian states, discussing some specific examples. We have also seen that pure Gaussian states, as coherent states and squeezed states, can be generated from the vacuum by applying some unitary transformation (displacement and squeezing operators). Such a procedure can be generalized.

By definition, we say that a unitary operator $\hat{U}$ is Gaussian if transforms Gaussian states into Gaussian states, i.e., the output state $\hat{U}|\varphi\rangle$ is Gaussian for any Gaussian state $|\varphi\rangle$ at the input. Using Gaussian unitaries we can generate all the pure Gaussian states starting from the vacuum. In other words, given an arbitrary pure Gaussian state $|\varphi\rangle$ we can write

$$|\varphi\rangle = \hat{U}|0\rangle \tag{B.20}$$

for some suitable Gaussian unitary $\hat{U}$. In particular, the most general single-mode pure Gaussian state can be written as a rotated and displaced squeezed state

$$|\alpha, \theta, r\rangle = \hat{D}(\alpha)\hat{R}(\theta)\hat{S}(r)\ |0\rangle, \tag{B.21}$$

where the vacuum is first squeezed by $\hat{S}(r)$, then rotated by $\hat{R}(\theta) = \exp(-i\hat{n}\theta)$ and finally displaced by $\hat{D}(\alpha)$.

Similarly to Gaussian states, Gaussian unitaries too have simple descriptions in the phase space, in terms of transformations on the two statistical moments $\bar{x}$ and $\mathbf{V}$. In fact, a Gaussian unitary $\hat{U}$ acting on the Hilbert space $\mathcal{H}$ is equivalent to an affine transformation in the phase space $\mathcal{K}$, which transforms the two statistical moments according to the following rules:

$$\bar{x} \to \bar{x}' = \bar{x} + d, \tag{B.22}$$

$$\mathbf{V} \to \mathbf{V}' = \mathbf{S}\mathbf{V}\mathbf{S}^T \ , \tag{B.23}$$

where d is a displacement vector and $\mathbf{S}$ is a symplectic transformation, i.e., a matrix preserving the symplectic form

$$\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \boldsymbol{\Omega} \ . \tag{B.24}$$

Under this correspondence, the displacement operator $\hat{D}(\alpha)$ corresponds to the transformation of the first moments according to Eq. (B.22) with $d = (\mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha)^T$. Squeezing operator $\hat{S}(r)$ corresponds to transforming the CM according to Eq. (B.23) by using the squeezing matrix

$$\mathbf{S}(r) = \begin{pmatrix} e^{-r} & \\ & e^{r} \end{pmatrix} = \begin{pmatrix} \xi^{-1} & \\ & \xi \end{pmatrix}, \ \xi = e^r \ . \tag{B.25}$$

Rotation operator $\hat{R}(\theta)$ corresponds to using the rotation matrix

$$\mathbf{R}(\theta) = \begin{pmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{pmatrix}. \tag{B.26}$$

It is therefore easy to express the most general pure Gaussian state $|\alpha, r, \theta\rangle$ in terms of the pair $\{\bar{x}, \mathbf{V}\}$. Using Eq. (B.21) and the phase-space representation of $\hat{D}$, $\hat{R}$ and $\hat{S}$, we have that $|\alpha, r, \theta\rangle$ has mean value $\bar{x} = (\mathrm{Re}\,\alpha, \mathrm{Im}\,\alpha)^T$ and CM

$$\mathbf{V} = \mathbf{R}(\theta)\mathbf{S}(r)\ \mathbf{I}\ \mathbf{S}(r)^T\mathbf{R}(\theta)^T = \mathbf{R}(\theta)\mathbf{S}^2(r)\mathbf{R}^T(\theta). \tag{B.27}$$

B.2 Two-mode bosonic states

We consider two bosonic modes, labeled as A and B, with joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ and quadratures operators $\hat{x}_A = (\hat{q}_A, \hat{p}_A)^T$ and $\hat{x}_B = (\hat{q}_B, \hat{p}_B)^T$, respectively. The quadrature operators must satisfy the commutation relations

$$[\hat{q}_A, \hat{p}_A] = [\hat{q}_B, \hat{p}_B] = 2i \tag{B.28}$$

and

$$[\hat{q}_A, \hat{q}_B] = [\hat{q}_A, \hat{p}_B] = [\hat{p}_A, \hat{q}_B] = [\hat{p}_A, \hat{p}_B] = 0. \tag{B.29}$$

As a consequence of these commutators we have that we cannot measure position and momentum of the same mode with arbitrary precision, but we can measure these observables if they correspond to different modes. In fact, from Eq. (B.28) we can derive the uncertainty principle

$$V(\hat{q}_k)V(\hat{p}_k) \geq 1, \text{ for } k = A, B \tag{B.30}$$

while Eq. (B.29) do not pose constraints on the other product of variances. Here we have $V(\hat{O}) = \langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2$ with $\langle \hat{O} \rangle := \mathrm{Tr}(\rho_{AB}\hat{O})$.

We can introduce a compact vector notation to describe the quadrature operators of the two modes. We consider a quadrature vector defined as

$$\hat{x} = \begin{pmatrix} \hat{q}_A \\ \hat{p}_A \\ \hat{q}_B \\ \hat{p}_B \end{pmatrix} = \begin{pmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \\ \hat{x}_4 \end{pmatrix}. \tag{B.31}$$

Then the commutation relations take the compact form

$$[\hat{x}_k, \hat{x}_l] = 2i\Omega_{k,l} \quad (k, l = 1, ..., 4), \tag{B.32}$$

where $\Omega_{k,l}$ is the generic element of symplectic form for two modes

$$\Omega = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} = \Omega_A \oplus \Omega_B \tag{B.33}$$

which is achieved by direct sum $\oplus$ of the symplectic forms of each bosonic mode.

The CM of a two-mode state ρ_{AB} can be written in the form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix} \tag{B.34}$$

where the blocks $\mathbf{A}, \mathbf{B}, \mathbf{C}$ are 2×2 real matrices and we have $\mathbf{A} = \mathbf{A}^T$ and $\mathbf{B} = \mathbf{B}^T$. Here $\mathbf{A}$ is the CM of the reduced state $\rho_A = \mathrm{Tr}_B(\rho_{AB})$, $\mathbf{B}$ is the CM of the reduced $\rho_B = \mathrm{Tr}_A(\rho_{AB})$ of mode B, while the off-diagonal block $\mathbf{C}$ accounts for the correlations between the two modes. The generic element V_{kl} of the CM is defined as

$$V_{kl} = \frac{1}{2} \langle \hat{x}_k \hat{x}_l + \hat{x}_l \hat{x}_k \rangle - \langle \hat{x}_k \rangle \langle \hat{x}_l \rangle \tag{B.35}$$

where $k, l = 1, 2, ..., 4$. In terms of the CM, the uncertainty principle takes a very compact form which is expressed by [68]

$$\mathbf{V} + i\Omega \geq 0, \tag{B.36}$$

which means that the matrix $\mathbf{M} \equiv \mathbf{V} + i\Omega$ must have non-negative eigenvalues.

B.2.1 Two-mode Gaussian states

A two-mode Gaussian state ρ_{AB} is equivalent to a Gaussian Wigner function $W(x)$ which, in turn, is completely characterized by its mean value $\bar{x} \in \mathbb{R}^4$ and 4×4 CM as in Eq. (B.34). In particular, zero-mean Gaussian states ($\bar{x} = 0$) are fully equivalent to their CMs.

The most important example of two-mode Gaussian state is the "Einstein-Podolski-Rosen" (EPR) state [78]. This is a pure Gaussian state with zero mean and CM of the form

$$\mathbf{V}_{EPR}(\mu) = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2 - 1}\mathbf{Z} \\ \sqrt{\mu^2 - 1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix} \tag{B.37}$$

where $\mu \geq 1$ and

$$\mathbf{I} = \mathrm{diag}(1, 1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{B.38}$$

$$\mathbf{Z} = \mathrm{diag}\,(1, -1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{B.39}$$

According to the previous CM of Eq. (B.37), we have the following variances and covariances for the quadratures

$$V(\hat{q}_A) = V(\hat{p}_A) = V(\hat{q}_B) = V(\hat{p}_B) = \mu \tag{B.40}$$

and

$$C(\hat{q}_A, \hat{q}_B) = \sqrt{\mu^2 - 1},\ C(\hat{p}_A, \hat{p}_B) = -\sqrt{\mu^2 - 1}. \tag{B.41}$$

The EPR state has maximum correlations between modes A and B. These EPR correlations represent a typical form of entanglement and they are increasing in μ. In the trivial case where $\mu = 1$, we have

$$\mathbf{V}_{EPR}(1) = \mathbf{I} \oplus \mathbf{I} \tag{B.42}$$

which means that we have the tensor product of two vacuum states

$$\rho_{EPR}(1) = |0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B\,. \tag{B.43}$$

This is the only case where the EPR state is separable, being entangled for any $\mu > 1$. In the limit case $\mu \rightarrow +\infty$, we have an ideal EPR state, for which $\hat{q}_A \rightarrow \hat{q}_B$ and $\hat{p}_A \rightarrow -\hat{p}_B$ [24]. In other words, positions become perfectly correlated and momenta become perfectly anti-correlated.

It is important to note that the reduced states of the EPR state $\rho_A = \mathrm{Tr}_B(\rho_{EPR})$ and $\rho_B = \mathrm{Tr}_A(\rho_{EPR})$ are two identical thermal states $\rho_A = \rho_B = \rho_{th}(\mu)$ with CM $\mu\mathbf{I}$. As we can see, the parameter μ also quantifies the mean number of thermal photons in each mode. These thermal numbers are equal $\bar{n}_A = \bar{n}_B = \bar{n}$ and determined by

$$\mu = 2\bar{n} + 1. \tag{B.44}$$

The EPR state is also known as two-mode squeezed vacuum state (TMSV) state. In fact, it is generated by applying the two-mode squeezing operator [77,78] $\hat{S}_{AB}(\mu)$ to a pair of vacuum states. In other words we have $\rho_{EPR} = |\mu\rangle\langle\mu|_{EPR}$, where

$$|\mu\rangle_{EPR} = \hat{S}_{AB}(\mu)(|0\rangle_A \otimes |0\rangle_B) \ . \tag{B.45}$$

In quantum optics labs a two-mode squeezing operator is realized by the process of spontaneous parametric down-conversion (SPDC) which happens when a specific type of optical crystal (BBO-crystal) is pumped by a strong laser [77].

B.2.2 Symplectic decomposition (Williamson's theorem)

Consider an arbitrary two-mode Gaussian state $\rho(\bar{x}, \mathbf{V})$ with mean value $\bar{x}$ and CM $\mathbf{V}$. There is an important decomposition for its CM known as Williamson's theorem [79] (here specified for the two-mode case).

Theorem. *Given the CM V of a two-mode Gaussian state, there is a symplectic matrix S such that*

$$\mathbf{V} = \mathbf{S}\mathbf{W}\mathbf{S}^T \tag{B.46}$$

where

$$\mathbf{W} = \nu_1\mathbf{I} \oplus \nu_2\mathbf{I} = \begin{pmatrix} \nu_1 & 0 & 0 & 0 \\ 0 & \nu_1 & 0 & 0 \\ 0 & 0 & \nu_2 & 0 \\ 0 & 0 & 0 & \nu_2 \end{pmatrix} \tag{B.47}$$

is called Williamson form and the diagonal entries ν_1 and ν_2 are called "symplectic eigenvalues".

The decomposition in Eq. (B.46) is also known as "symplectic decomposition" of the CM $\mathbf{V}$. This is completely specify by the symplectic spectrum $\{\nu_1, \nu_2\}$ and the symplectic matrix $\mathbf{S}$. While $\mathbf{S}$ is not easy to compute in general, we have a standard recipe to compute the symplectic spectrum, which is equal to the standard spectrum of the matrix

$$\mathbf{M} = i\Omega\mathbf{V}. \tag{B.48}$$

In fact, matrix $\mathbf{M}$ is diagonalizable and its eigenvalues turn out to be of the form $\lambda_1 = \nu_1$, $\lambda_2 = -\nu_1$, $\lambda_3 = \nu_2$, and $\lambda_4 = -\nu_2$. Therefore it is sufficient to take the modulus of these eigenvalues to derive the symplectic spectrum of the original CM $\mathbf{V}$. This is a procedure which can be extended to CM of N modes as we will see afterwards.

In the specific case of two-mode CMs, we also have a direct formula to compute the symplectic spectrum. Given a CM $\mathbf{V}$ in block-form of Eq. (B.34), its symplectic eigenvalues $\{\nu_+, \nu_-\}$ are equal to [62,63]

$$\nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det \mathbf{V}}}{2}} \tag{B.49}$$

with

$$\Delta := \det \mathbf{A} + \det \mathbf{B} + 2 \det \mathbf{C}. \tag{B.50}$$

B.2.3 Thermal decomposition

According to Williamson's theorem, we can decompose an arbitrary CM of two modes

$$\mathbf{V} = \mathbf{S}\mathbf{W}\mathbf{S}^T = \mathbf{S}\ (\nu_1 \mathbf{I} \oplus \nu_2 \mathbf{I})\ \mathbf{S}^T, \tag{B.51}$$

for some symplectic matrix $\mathbf{S}$. Note that: (i) the direct sum $\oplus$ in the phase space corresponds to a tensor-product $\otimes$ in the Hilbert space; (ii) A CM of the form $\nu\mathbf{I}$ describes a thermal state $\rho_{th}(\nu)$ with variance $\nu = 2\bar{n}+1$ ($\bar{n}$ being the mean number of photons).

As a result, the diagonal Williamson's form $\mathbf{W}$ corresponds to the tensor-product of two thermal states, whose variances are given by the symplectic eigenvalues ν_1 and ν_2. In other words, we have that $\mathbf{W}$ is associated with the Gaussian state

$$\rho(0, \mathbf{W}) = \rho_{th,A}(\nu_1) \otimes \rho_{th,B}(\nu_2). \tag{B.52}$$

Now, since a symplectic matrix $\mathbf{S}$ corresponds to a Gaussian unitary $\hat{U}_{\mathbf{S}}$ in the Hilbert space, we have that symplectic decomposition of the CM $\mathbf{V}$ corresponds to the following decomposition of the corresponding Gaussian state

$$\rho(0, \mathbf{V}) = \hat{U}_{\mathbf{S}}\ \rho(0, \mathbf{W})\ \hat{U}_{\mathbf{S}}^\dagger\ . \tag{B.53}$$

In general, an arbitrary Gaussian state $\rho(\bar{x}, \mathbf{V})$ with non-zero mean value takes the form of Eq. (B.53) up to a displacement, i.e., we have

$$\rho\ (\bar{x}, \mathbf{V}) = \hat{D}(\bar{x})\ \rho(0, \mathbf{V})\ \hat{D}^\dagger(\bar{x})\ . \tag{B.54}$$

In conclusion, the interpretation of Williamson's theorem in the Hilbert space is the following: An arbitrary Gaussian state $\rho(\bar{x}, \mathbf{V})$ can be decomposed into a tensor product of thermal states up to a Gaussian unitary. In particular, this unitary can be written as

$$\hat{U}(\bar{x}, \mathbf{S}) = \hat{D}(\bar{x})\ \hat{U}_{\mathbf{S}}\ . \tag{B.55}$$

B.2.4 Importance of the symplectic spectrum

It is clear from the previous thermal decomposition that the symplectic eigenvalues quantify the thermal noise present in the two-mode Gaussian state. In fact, ν_1 and

ν_2 represent the variances of the two thermal states in which the original state can be decomposed. For this reason, many quantum properties depend on the symplectic spectrum. For instance, we can easily express the uncertainty principle ($\mathbf{V}+i\Omega \geq 0$) as a simple bona-fide condition for the symplectic eigenvalues, which corresponds to imposing

$$\nu_k \geq 1, \quad \text{for } k = 1,2 \ . \tag{B.56}$$

Then, the von Neumann entropy $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ can be easily given in terms of its symplectic spectrum as

$$S(\rho) = g(\nu_1) + g(\nu_2) \tag{B.57}$$

where

$$g(x) = \left(\frac{x+1}{2}\right)\log_2\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log_2\left(\frac{x-1}{2}\right) \tag{B.58}$$

is defined for any $x \geq 1$ and equal to zero for $x = 1$. As a corollary, we also see that a Gaussian state is pure if and only if $\nu_1 = \nu_2 = 1$, since this latter condition implies $S(\rho) = 0$.

B.2.5 Entanglement criterion for two-mode Gaussian states

For a two-mode Gaussian state $\rho(\bar{x}, \mathbf{V})$ it is easy to decide if it is separable or entangled. From the CM $\mathbf{V}$ of the state, we compute the partially-transposed CM

$$\tilde{\mathbf{V}} = \Lambda \ \mathbf{V} \ \Lambda^T, \tag{B.59}$$

where Λ is the following partial-transposition transformation

$$\Lambda := \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \\ & \mathbf{Z} \end{pmatrix}. \tag{B.60}$$

Then, we derive the symplectic spectrum $\{\tilde{\nu}_-, \tilde{\nu}_+\}$ of the $\tilde{\mathbf{V}}$, where $\tilde{\nu}_- \leq \tilde{\nu}_+$.

Now we can apply the following entanglement criterion [67]: The two-mode Gaussian state ρ is separable if and only if the minimum symplectic eigenvalue $\tilde{\nu}_-$ of the partially-transposed CM is greater than or equal to 1. In other words, we have

$$\rho \text{ separable } \Leftrightarrow \tilde{\nu}_- \geq 1 \ , \tag{B.61}$$

$$\rho \text{ entangled } \Leftrightarrow \tilde{\nu}_- < 1 \ . \tag{B.62}$$

Luckily, there is a simple formula which connects the eigenvalue $\tilde{\nu}_-$ to the blocks of the original CM $\mathbf{V}$ expressed in the block-form of Eq. (B.34). In fact, we can write

$$\tilde{\nu}_- = \sqrt{\frac{\tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4 \det \mathbf{V}}}{2}}, \tag{B.63}$$

where

$$\tilde{\Delta} := \det \mathbf{A} + \det \mathbf{B} - 2 \det \mathbf{C}. \tag{B.64}$$

Entanglement not only can be tested by a criterion but also be quantified by a proper measure. One of the most used is the so called "log-negativity" [76]. For a Gaussian state, this is given by

$$\mathcal{N}\left(\rho\right) = \max\left\{0, -\log \tilde{\nu}_-\right\}. \tag{B.65}$$

We see that for a separable state ($\tilde{\nu}_- \geq 1$) we have $\mathcal{N}\left(\rho\right) = 0$, while for an entangled state ($\tilde{\nu}_- < 1$) we have $\mathcal{N}\left(\rho\right) > 0$, with the value of $\mathcal{N}\left(\rho\right)$ quantifying the amount of entanglement in the state.

As an example, consider an EPR state so that its CM $\mathbf{V}$ has blocks

$$\mathbf{A} = \mathbf{B} = \mu \mathbf{I}, \ \mathbf{C} = \sqrt{\mu^2 - 1}\mathbf{Z}. \tag{B.66}$$

We compute

$$\tilde{\Delta} = 4\mu^2 - 2, \ \det \mathbf{V} = 1, \tag{B.67}$$

which give

$$\tilde{\nu}_-^2 = \frac{4\mu^2 - 2 - \sqrt{4\mu^2 - 6}}{2}. \tag{B.68}$$

Once can verify that $\tilde{\nu}_- < 1$ for any $\mu > 1$. For large μ, we have

$$\tilde{\nu}_- \simeq \frac{1}{2\mu} \tag{B.69}$$

and the log-negativity is equal to

$$\mathcal{N}\left(\rho\right) = 1 + \log_2 \mu. \tag{B.70}$$

B.3 Multimode bosonic system

In general, a bosonic system of n modes is a quantum system associated with a infinite dimensional Hilbert space $\mathcal{H} = \otimes_{j=1}^{n} \mathcal{H}_j$ and a set of $2n$ quadrature operators

$$\hat{x}^T = (\hat{q}_1, \hat{p}_1, ...\hat{q}_n, \hat{p}_n) \tag{B.71}$$

satisfying the commutation relations

$$[\hat{x}_k, \hat{x}_l] = 2i\Omega_{kl}, \quad (k, l = 1, ..., 2n) \tag{B.72}$$

where Ω_{kl} is the generic element of the n-mode symplectic form

$$\Omega = \oplus_{k=1}^{n} \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right). \tag{B.73}$$

An arbitrary density operator ρ is equivalent to a Wigner function $W(x)$, which is a quasi-probability distribution defined over a $2n$-dimensional real vector variable

$$x^T = (q_1, p_1, ..., q_n, p_n) \in \mathbb{R}^{2n}. \tag{B.74}$$

The real vector x represents the continuous variables of the system (eigenvalues of the quadrature operators $\hat{x}$) and spans a $2n$-dimensional vector space which is the phase-space of the n-mode system. Remind that a tensor product of Hilbert spaces $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to a direct sum of phase-spaces $\mathcal{K}_{AB} = \mathcal{K}_A \oplus \mathcal{K}_B$, where dimensions sum up. Therefore, by composing n bosonic modes, we construct a phase space $\mathcal{K} = \oplus_{l=1}^{n} \mathcal{K}_l$ which is $2n$-dimensional.

Given a Wigner function $W(x)$ we can consider all its statistical moments. As we know, the first moment is mean value

$$\bar{x} = \mathrm{Tr}(\hat{x}\rho) \in \mathbb{R}^{2n}, \tag{B.75}$$

and the second moment is the CM $\mathbf{V}$, which is now $2n \times 2n$ real symmetric matrix with generic element

$$V_{kl} = \frac{1}{2} \langle \{\hat{x}_k, \hat{x}_l\} \rangle - \bar{x}_k \bar{x}_l \tag{B.76}$$

where

$$\{\hat{x}_k, \hat{x}_l\} = \hat{x}_k \hat{x}_l + \hat{x}_k \hat{x}_l \tag{B.77}$$

is the anticommutator. In order to be physical, the CM must satisfy the uncertainty principle which takes the form

$$\mathbf{V} + i\Omega \geq 0 \tag{B.78}$$

where Ω is the general symplectic form of Eq. (B.73). Note that Eq. (B.78) implies $\mathbf{V} > 0$.

B.3.1 Multimode Gaussian states

Given a bosonic system of n modes, its state ρ is Gaussian if its Wigner function is Gaussian

$$W(x) = \frac{\exp[-\frac{1}{2}(x - \bar{x})^T \mathbf{V}^{-1} (x - \bar{x})]}{(2\pi)^n \sqrt{\det \mathbf{V}}}. \tag{B.79}$$

Equivalently, we can describe the Gaussian state using the first two statistical moments

$$\rho = \rho(\bar{x}, \mathbf{V}). \tag{B.80}$$

Since $\bar{x} \in \mathbb{R}^{2n}$ and $\mathbf{V}$ is $2n \times 2n$ real matrix, we only need a total of $2n^2 + 3n$ real parameters to fully characterize an n-mode Gaussian state. Since this number of parameters is polynomial in the number of modes n, we have that multimode Gaussian states can be described efficiently.

B.3.2 Multimode Gaussian unitaries

In general, a unitary $\hat{U}$ acting on a n-mode bosonic state $\rho \rightarrow \rho' = \hat{U}\rho\hat{U}^\dagger$ is a Gaussian unitary if transforms Gaussian states into Gaussian states. In the $2n$-dimensional phase-space $\mathcal{K}$, a Gaussian unitary $\hat{U}$ corresponds to an affine map $(\mathbf{S}, d)$ which transforms the statistical moments of the state as

$$\bar{x} \rightarrow \bar{x}' = \mathbf{S}\bar{x} + d \tag{B.81}$$

and

$$\mathbf{V} \rightarrow \mathbf{V}' = \mathbf{S}\mathbf{V}\mathbf{S}^T \tag{B.82}$$

where $d \in \mathbb{R}^{2n}$ is a displacement vector, and $\mathbf{S}$ is a $2n \times 2n$ symplectic matrix $(\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \Omega)$. In general, we can always decompose a Gaussian unitary as

$$\hat{U}_{(\mathbf{S},d)} = \hat{D}(d)\hat{U}_{\mathbf{S}} \tag{B.83}$$

when $\hat{D}(d)$ is the Weyl displacement operator and $\hat{U}_{\mathbf{S}}$ is a canonical unitary which is one-to-one with the symplectic matrix $\mathbf{S}$.

Any Gaussian unitary can be implemented using linear optics in the lab. For instance, a canonical unitary $\hat{U}_{\mathbf{S}}$, i.e., a symplectic transformation $\mathbf{S}$, can be decomposed into n single-mode squeezers, plus an interferometer (i.e., a suitable concatenation of beam-splitters and phase-shifters), and another set of n single-mode squeezers. This is known as Euler-decomposition [2] or Block-Messiah reduction [12]. In other words, any n-mode symplectic matrix can be written as

$$\mathbf{S} = [\oplus_{i=1}^{n}\mathbf{S}(r_i)]\ \mathbf{K}\ [\oplus_{i=1}^{n}\mathbf{S}(r_i')]\ , \tag{B.84}$$

where $\mathbf{S}(r_i)$ and $\mathbf{S}(r_i')$ are single-mode 2×2 squeezing matrices, and $\mathbf{K}$ is the $2n \times 2n$ symplectic matrix describing the interferometer.

B.3.3 Williamson's theorem for n modes

The symplectic decomposition can be extended to CMs of multimode Gaussian states. Given an n-mode Gaussian state with CM $\mathbf{V}$, there is a symplectic matrix $\mathbf{S}$ such that

$$\mathbf{V} = \mathbf{S}\mathbf{W}\mathbf{S}^T \tag{B.85}$$

where

$$\mathbf{W} = \oplus_{k=1}^{n}\nu_k\mathbf{I} \tag{B.86}$$

is the Williamson form and $\{\nu_1, \ldots, \nu_n\}$ is the symplectic spectrum.

Such a symplectic decomposition in phase space corresponds to a thermal decomposition in the Hilbert space. Given a zero-mean Gaussian state $\rho(0, \mathbf{V})$, the decomposition of its CM as in Eqs. (B.85) and (B.86) corresponds to write

$$\rho(0, \mathbf{V}) = \hat{U}_{\mathbf{S}} \rho(0, \mathbf{W}) \hat{U}_{\mathbf{S}}^{\dagger} \tag{B.87}$$

where

$$\rho(0, \mathbf{W}) = \otimes_{k=1}^{n} \rho_{th}(\nu_k) \tag{B.88}$$

is a tensor product of thermal states. In general, for a displaced Gaussian state $\rho(\bar{x}, \mathbf{V})$ we have

$$\rho(\bar{x}, \mathbf{V}) = \hat{D}(\bar{x}) \rho(0, \mathbf{V}) \hat{D}^{\dagger}(\bar{x}) \tag{B.89}$$

where $\hat{D}(\bar{x})$ is the n-mode displacement operator and $\rho(0, \mathbf{V})$ is decomposed in thermal states as in Eqs. (B.87) and (B.88).

As we know, the symplectic spectrum contains all the essential information about the noise of the state. For this reason, it can be used to formulate very important properties of the state. For n modes we can write the uncertainty principle as

$$\nu_k \geq 1 \quad (k = 1, ..., n). \tag{B.90}$$

Then, the von Neumann entropy of a n-mode Gaussian state is given by

$$S(\rho) = \sum_{k=1}^{n} g(\nu_k) \tag{B.91}$$

where $g(x)$ is defined in Eq. (B.58). In particular, a Gaussian state ρ is pure ($S(\rho) = 0$) when $\nu_k = 1$ for any k. In other words, a pure state has a symplectic spectrum which is the minimal possible according to the uncertainty principle Eq. (B.90), such that there is no thermal noise but only quantum vacuum noise. It is also important to note that

$$\det \mathbf{V} = \Pi_{k=1}^{n} \nu_k^2 = \nu_1^2 \nu_2^2 ... \nu_n^2 \ , \tag{B.92}$$

so that Gaussian state is pure if and only if

$$\det \mathbf{V} = 1 \ . \tag{B.93}$$

Appendix C

Gaussian Channels

C.1 Brief review of quantum channels

A quantum channel $\mathcal{E}$ is a linear map transforming density operators into density operators. Mathematically, $\mathcal{E}$ must be a completely positive trace preserving (CPT) map. In fact, density operators are positive $\rho \geq 0$ and unit-trace $\mathrm{Tr}(\rho) = 1$ (properties which mirror those of the probability distributions for which $p_i \geq 0$ and $\sum_i p_i = 1$). Therefore, the map $\mathcal{E}$ must provide an output which is positive $\mathcal{E}(\rho) \geq 0$ and having the same trace of the input. This corresponds to impose $\mathcal{E}$ to be positive and trace-preserving.

More strongly, the map $\mathcal{E}$ must be completely-positive, which means that its output must be positive also when $\mathcal{E}$ is applied locally to one subsystem. In other words, given two systems A and B, prepared in some arbitrary density operator ρ, the application of the map on system B must provide a global state which is positive, i.e., we must have [45]

$$(I \otimes \mathcal{E})\rho_{AB} \geq 0 \ . \tag{C.1}$$

A quantum channel is reversible when it is described by a unitary $\hat{U}$. In this case ($\hat{U}^\dagger = \hat{U}^{-1}$), we have the transformation rule

$$\rho \to \rho' = \mathcal{E}(\rho) = \hat{U}\rho\hat{U}^\dagger \ , \tag{C.2}$$

and the inverse map is given by

$$\rho' \to \rho = \mathcal{E}^{-1}(\rho') = \hat{U}^\dagger\rho'\hat{U} \ . \tag{C.3}$$

C.2 Unitary dilations

A convenient way to represent a quantum channel is to use a unitary defined on a larger Hilbert space describing both the system and the environment. In fact, a quantum channel $\mathcal{E}$ can be dilated into a unitary $\hat{U}$ according to the formula

$$\mathcal{E}(\rho_A) = \mathrm{Tr}_E[\hat{U}_{AE}(\rho_A \otimes \sigma_E)\hat{U}^\dagger_{AE}], \tag{C.4}$$

where the state ρ_A of the system and the state σ_E of the environment are evolved by joint unitary $\hat{U}_{AE}$, after which the environment is traced out. In particular, we can always choose an environment which is large enough to be described by a pure state σ_E. In this case, the dilation is known as "Stinespring dilation" [72]. See Fig. C.1 for a pictorial representation of a quantum channel as a quantum communication process between two parties and the corresponding dilation of the channel into an environment.

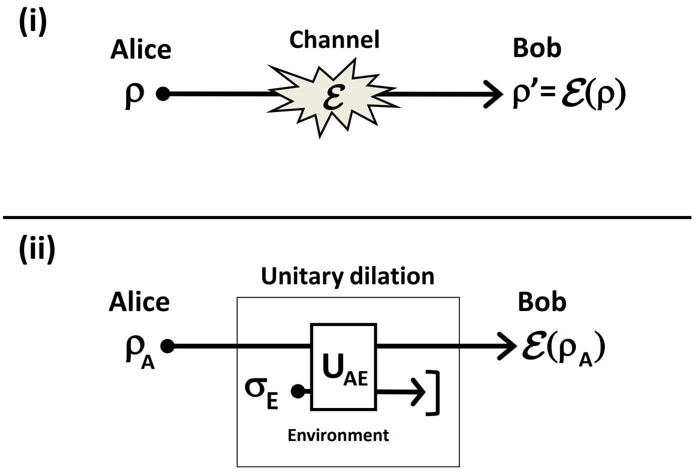

Figure C.1: **(i)**. Quantum channel $\mathcal{E}$ in a communication scenario where the input state ρ of Alice is transformed into an output state $\rho' = \mathcal{E}(\rho)$ for Bob. **(ii)** Unitary dilation of the previous channel. The channel can be described considering a unitary interaction $\hat{U}_{AE}$ between the input state ρ_A and the state σ_E of the environment E. The output of the environment is traced out. If σ_E is pure we have a Stinespring dilation.

Given an arbitrary dilation $\{\sigma_E, \hat{U}_{AE}\}$ of a quantum channel $\mathcal{E}$, we can always construct a Stinespring dilation by purifying the state σ_E of the environment[1]. This means to enlarge the environment to include another system e which, together with E, is described by a pure state $|\Phi\rangle_{Ee}$. See Fig. C.2. The mixed state σ_E represents a reduced state of this global pure state, i.e.,

$$\sigma_E = \mathrm{Tr}_e(|\Phi\rangle_{Ee}\langle\Phi|)\ . \tag{C.5}$$

Then, we can also extend the unitary $\hat{U}_{AE}$ to $\hat{U}_{AE} \otimes \hat{I}_e$, where the identity is applied to the new system e. In a few words, we have constructed a Stinespring dilation

[1] In general, a purification of a mixed state ρ_A means that we find a pure state $\Phi_{AB} = |\Phi\rangle_{AB}\langle\Phi|$ of a larger system AB whose partial trace gives the original state $\rho_A = \mathrm{Tr}_B(\Phi_{AB})$.

$\{|\Phi\rangle_{Ee}, \hat{U}_{AE} \otimes \hat{I}_e\}$ of the channel $\mathcal{E}$. Output states are given by

$$\mathcal{E}(\rho_A) = \mathrm{Tr}_{Ee}(\hat{U}_{AE} \otimes \hat{I}_e)(\rho_A \otimes |\Phi\rangle_{Ee} \langle\Phi|)(\hat{U}^\dagger_{AE} \otimes \hat{I}_e). \tag{C.6}$$

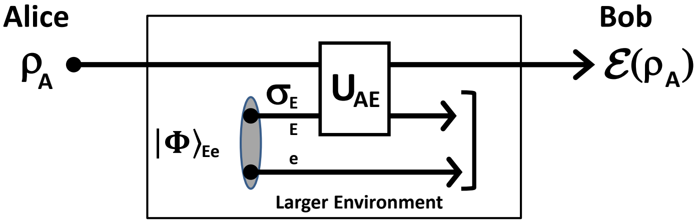

Figure C.2: Purification of the environment. A unitary dilation (with a mixed environmental state σ_E) can always be transformed into a Stinespring dilation involving a large environment Ee in a global pure state $|\Phi\rangle_{Ee}$.

C.3 Bosonic Gaussian Channels

The study of bosonic channels play a central role in the quantum information theory, representing the standard way to model noise in quantum communication protocols. By definition, a quantum channel is "bosonic" when it refers to bosonic modes, i.e., it transforms the quantum states of a bosonic system. In particular, it is a also a "Gaussian channel" when it transforms Gaussian states into Gaussian states.

Given a Gaussian channel transforming the state of n modes (also called n-mode Gaussian channel) we can always construct a Gaussian dilation involving a Gaussian unitary $\hat{U}_{\mathbf{S}}$ combining the n input modes with $n_E \leq 2n$ environmental modes, prepared in a pure Gaussian state $|\varphi\rangle_E$. In particular, this can be chosen to be the multimode vacuum state $|\varphi\rangle_E = \otimes_{k=1}^n |0\rangle_k$.

We can describe the action of an arbitrary Gaussian channel in terms of transformations on the first two statistical moments of the input Gaussian state $\rho(\bar{x}, \mathbf{V})$. In fact, the mean value is transformed according to the rule [78]

$$\bar{x} \longrightarrow \bar{x}' = \mathbf{K}\bar{x} + d \tag{C.7}$$

where $d \in \mathbb{R}^{2n}$ is a displacement vector, and $\mathbf{K}$ is a $2n \times 2n$ real matrix.

At the same time, the CM becomes [78]

$$\mathbf{V} \rightarrow \mathbf{V}' = \mathbf{K}\mathbf{V}\mathbf{K}^T + \mathbf{N} \tag{C.8}$$

where $\mathbf{N} = \mathbf{N}^T$ is a $2n \times 2n$ real symmetric matrix. In particular, the two channel matrices $\mathbf{K}$ and $\mathbf{N}$ must satisfy the condition

$$\mathbf{N} + i\Omega - \mathbf{K}\Omega\mathbf{K}^T \geq 0 \tag{C.9}$$

which is equivalent to enforce the complete-positivity [78].

Therefore an arbitrary Gaussian channel $\mathcal{E}$ is fully characterized by two matrices $\mathbf{K}$ and $\mathbf{N}$ satisfying Eq (C.9), and a displacement vector d

$$\rho \to \rho' = \mathcal{E}(\rho) \Longleftrightarrow \{\bar{x}, \mathbf{V}\} \overset{\mathbf{N},\mathbf{K},d}{\longrightarrow} \{\bar{x}^{'}, \mathbf{V}^{'}\} \ . \tag{C.10}$$

For $\mathbf{N} = \mathbf{0}$ and $\mathbf{K}$ symplectic matrix, the Gaussian channel represents a Gaussian unitary $\hat{U}_{(\mathbf{K},d)}$.

C.4 Single-mode Gaussian channels

In the case of a single bosonic mode ($n = 1$) the description of a Gaussian channel is very easy. In fact, it is equivalent to a bi-dimensional displacement vector $d \in \mathbb{R}^2$ and a pair of 2×2 real matrices $\mathbf{K}$ and $\mathbf{N}$ such that [78]

$$\mathbf{N} = \mathbf{N}^T \geq 0, \ \ \det \mathbf{N} \geq (\det \mathbf{K} - 1)^2. \tag{C.11}$$

According to the Holevo classification [35] we can apply local Gaussian unitaries (at the input and output of the channel) and reduce any single-mode Gaussian channel into a “canonical form” which is a simplified Gaussian channel with $d = 0$ and $\mathbf{K}$, $\mathbf{N}$ being special diagonal matrices.

An example of canonical form is the additive-noise Gaussian channel (also known as B_2 form). It is characterized by $d = 0$, $\mathbf{K} = \mathbf{I}$, and $\mathbf{N} = \varepsilon\mathbf{I}$ with $\varepsilon \geq 0$. For instance, by applying this channel to a coherent state $\rho = |\alpha\rangle\langle\alpha|$ (having CM $\mathbf{V} = \mathbf{I}$) we get a thermalized state ρ' at the output with the same displacement of the input but noisier CM $\mathbf{V}' = (\varepsilon + 1)\mathbf{I}$.

The most important canonical form is the lossy channel which is described by $d = 0$,

$$\mathbf{K} = \sqrt{\tau}\mathbf{I} \text{ and } \mathbf{N} = (1 - \tau)\omega\mathbf{I} \ , \tag{C.12}$$

where $\tau \in [0, 1]$ is the transmissivity and $\omega \geq 1$ quantifies the thermal noise of the channel. By replacing Eq. (C.12) into Eq. (C.8), we get the explicit transformation rules

$$\bar{x} \longrightarrow \bar{x}' = \sqrt{\tau}\bar{x} \ , \tag{C.13}$$

$$\mathbf{V} \to \mathbf{V}^{'} = \tau\mathbf{V} + \omega(1 - \tau)\mathbf{I} \ . \tag{C.14}$$

A lossy channel is therefore characterized by two parameters only, i.e., τ and ω. In particular, it is called "pure-loss channel" when $\omega = 1$ and, therefore, it is completely specified by its transmissivity τ.

As an example the action of a lossy channel $\mathcal{E}_{\tau,\omega}$ on a coherent state $\rho = |\alpha\rangle\langle\alpha|$ (having CM $\mathbf{V} = \mathbf{I}$ and mean value $\bar{x}$) provides a Gaussian state with a contracted mean value $\bar{x}' = \tau\bar{x}$ and thermalized CM $\mathbf{V}' = \mu\mathbf{I}$ with

$$\mu = \tau + (1-\tau)\omega \geq 1. \tag{C.15}$$

(Note that the final state will still be coherent $\mathbf{V}' = \mathbf{I}$ if the channel is pure-loss, i.e., $\omega = 1$).

In a pure-loss channel, the transmissivity τ quantifies the difference in energy (mean number of photons) between the input and output states. In other words τ quantifies how many photons are transmitted and $(1-\tau)$ is the fraction which is lost in the environment.

C.5 Dilation of a lossy channel

Consider a lossy channel $\mathcal{E}_{\tau,\omega}$ with transmissivity $\tau \in [0,1]$ and thermal noise $\omega \geq 1$. This can be dilated into a beam splitter with transmissivity τ which mixes the input state ρ_A with an environmental thermal state $\sigma_E(\omega)$ with variance ω (see Fig. C.3). For a thermal state, the variance is equal to $\omega = 2\bar{n} + 1$, where $\bar{n}$ is the mean number of photons in the state. Thus, the action of the beam splitter is to transmit τ photons of the input, replacing the remaining $1-\tau$ photons with thermal photons coming from the environment.

The beam splitter transformation is a Gaussian unitary $\hat{U}_{AE}(\tau)$ which is equivalent to the following symplectic matrix

$$\mathbf{S}_{AE}(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix}. \tag{C.16}$$

Before the beam splitter the global input state is the tensor product $\rho_A(\bar{x}, \mathbf{V}) \otimes \sigma_E(\omega)$. Then, the global output of transmitted signal (B) and environment (E') is given by

$$\rho_{BE'} = \hat{U}_{AE}(\tau)[\rho_A(\bar{x}, \mathbf{V}) \otimes \sigma_E(\omega)]\hat{U}^{\dagger}_{AE}(\tau). \tag{C.17}$$

This is a Gaussian channel with CM is given by

$$\mathbf{V}_{BE'} = \mathbf{S}_{AE}(\tau)(\mathbf{V} \oplus \omega\mathbf{I})\mathbf{S}^{T}_{AE}(\tau) = \tag{C.18}$$

$$= \begin{pmatrix} \tau\mathbf{V} + \omega(1-\tau)\mathbf{I} & \sqrt{\tau(1-\tau)}(\omega\mathbf{I} - \mathbf{V}) \\ \sqrt{\tau(1-\tau)}(\omega\mathbf{I} - \mathbf{V}) & (1-\tau)\mathbf{V} + \tau\omega\mathbf{I} \end{pmatrix} \tag{C.19}$$

$$= \begin{pmatrix} \mathbf{V}_B & \mathbf{C} \\ \mathbf{C}^T & \mathbf{V}_{E'} \end{pmatrix}. \tag{C.20}$$

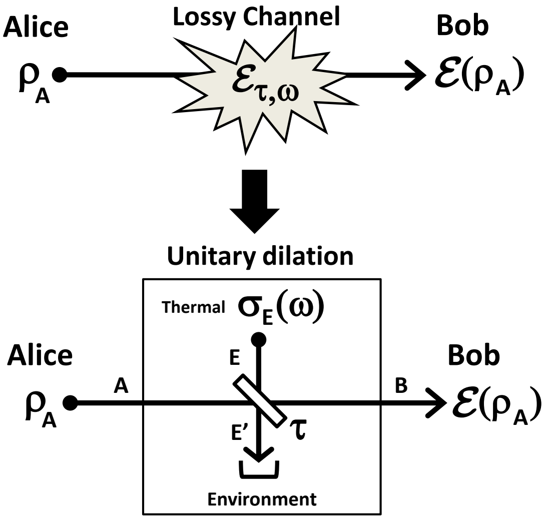

Figure C.3: Dilation of a lossy channel $\mathcal{E}_{\tau,\omega}$ into a beam splitter with transmissivity τ mixing the input state ρ_A with an environmental thermal state σ_E with variance ω.

Now the output state of Bob is the reduced state $\rho_B = \mathrm{Tr}_{E'}(\rho_{BE'})$, obtained by tracing out the output of the environment. Its CM $\mathbf{V}_B$ the top-left diagonal block in the global CM $\mathbf{V}_{BE'}$, i.e., we have

$$\mathbf{V}_B = \tau\mathbf{V} + \omega(1-\tau)\mathbf{I} \ . \tag{C.21}$$

This is exactly the transformation of the input CM under a lossy channel with transmissivity τ and thermal noise ω, as we can check from Eq. (C.14). Similarly, we can derive the transformation of the mean value, specified by Eq. (C.13). By purifying the thermal state of the environment $\sigma_E(\omega) = \mathrm{Tr}_e[\Phi_{Ee}(\omega)]$ into an EPR state $\Phi_{Ee}(\omega)$, we derive a Stinespring dilation of the lossy channel, as we also show in Fig. C.4.

The Stinespring dilation is particularly simple in the case of a pure-loss channels ($\omega = 1$) in which case it only includes a single mode E of the environment prepared in the vacuum state $|0\rangle_E$.

Finally, it is worth to say that the lossy channel is the standard model for noisy quantum communication over optical fibres. Its Stinespring dilation is also called "entangling-cloner" and represents the typical attack considered in continuous variable quantum cryptography, where the environment is identified with an eavesdropper [29].

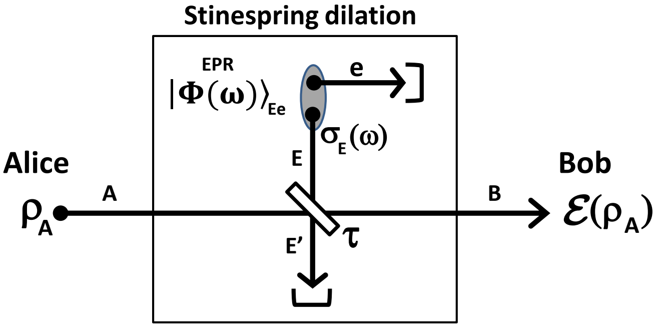

Figure C.4: Stinespring dilation of a lossy channel. The thermal state of the environment $\sigma_E(\omega)$ is purified into an EPR state of modes E and e. Only mode E is mixed with the input mode A via the beam splitter.

Bibliography

[1] A. Acin, *Statistical Distinguishability between Unitary Operations*, Phys. Rev. Lett. **87**, 177901 (2001).

[2] Arvind, B. Dutta, N. Mukunda, and R. Simon, *The Real Symplectic Groups in Quantum Mechanics and Optic*s, Pramana J. Phys. **45**, 471 (1995).

[3] K. M. R. Audenaert, J. Calsamiglia, L. Masanes, R. Munoz-Tapia, A. Acın, E. Bagan, and F. Verstraete, *Discriminating States: The Quantum Chernoff Bound*, Phys. Rev. Lett. **98**, 160501 (2007).

[4] K. M. R. Audenaert, M. Nussbaum, A. Szkola, and F. Verstraete, *Asymptotic Error Rates in Quantum Hypothesis Testing*, Commun. Math. Phys. **279**, 251 (2008).

[5] S. M. Barnett and S. Croke, *Quantum state discrimination*, Advances in Optics and Photonics **1**, 238-278 (2009).

[6] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, Microwave Quantum Illumination, Phys. Rev. Lett. **114**, 080503 (2015).

[7] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).

[8] 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).

[9] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).

[10] A. Bisio, M. Dall'Arno, and G. M. D'Ariano, *Tradeoff between energy and error in the discrimination of quantum-optical devices*, Phys. Rev. A **84**, 012310 (2011).

[11] "Blackberry co-founders start $100M quantum tech fund" on CBC news (accessed online, 19 October 2013). http://www.cbc.ca/news/canada/kitchener-waterloo/blackberry-co-founders-start-100m-quantum-tech-fund-1.1329286

[12] S. L. Braunstein, *Squeezing as an irreducible resource*, Phys. Rev. A **71**, 055801 (2005).

[13] S. L. Braunstein and H. J. Kimble, *Dense coding for continuous variables*, Phys. Rev. A **61** 042302 (2000).

[14] S. L. Braunstein, and P. van Loock, *Quantum information with continuous variables*, Rev. Mod. Phys. **77**, 513 (2005).

[15] S. L. Braunstein, and A. K. Pati, *Quantum Information with Continuous Variables* (Kluwer Academic, Dordrecht, 2003).

[16] S. L. Braunstein, and S. Pirandola, S*ide-Channel-Free Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130502 (2012).

[17] S. Brody, *Bioenergetics and Growth*, (Reinhold Publishing Corporation, New York, 1945)

[18] A. Chefles, *Quantum state discrimination*, Contemp. Phys. **41**, 401 (2000).

[19] A. Childs, J. Preskill, and J. Renes, *Quantum information and precision measurement*, J. Mod. Opt. **47**, 155 (2000).

[20] G. Chiribella, G. D'Ariano, and P. Perinotti, *Memory Effects in Quantum Channel Discrimination*, Phys. Rev. Lett. **101**, 180501 (2008).

[21] T. M. Cover, and J. A. Thomas, *Elements of Information Theory* (Wiley, Hoboken, 2006).

[22] M. Dall'Arno, A. Bisio, G. M. D'Ariano, M. Miková, M. Ježek, and M. Dušek, *Experimental implementation of unambiguous quantum reading*, Phys. Rev. A **85**, 012308 (2012).

[23] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, *Quantum Data Hiding*, IEEE Trans. Inf. Theory **48**, 580–599 (2002).

[24] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935).

[25] C. A. Fuchs, and J.V. de Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[26] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, *Unconditional Quantum Teleportation*, Science **282**, 706 (1998).

[27] C. W. Gardiner, and P. Zoller, *Quantum Noise* (Springer, 2004).

[28] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys. **74**, 145 (2002).

[29] F. Grosshans, , N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables*, Quantum Inf. Comput. **3**, 535 (2003).

[30] S. Guha, Z. Dutton, R. Nair, J. Shapiro, and B. Yen, *Information Capacity of Quantum Reading*, Laser Science, OSA Technical Digest (Optical Society of America, 2011), paper LTuF2.

[31] S. Guha and B. Erkmen, *Gaussian-state quantum-illumination receivers for target detection*, Phys. Rev. A **80**, 052310 (2009).

[32] M. Hayashi, *Discrimination of Two Channels by Adaptive Methods*, IEEE Trans. Inf. Theory **55**, 3807 (2009).

[33] C. W. Helstrom, *Quantum Detection and Estimation Theory*, *Mathematics in Science and Engineering*, Vol. 123 (Academic Press, New York, 1976).

[34] O. Hirota, *Error free Quantum Reading by quasi Bell state of entangled coherent states*, Preprint arXiv:1108.4163 (2011).

[35] A. S. Holevo, *One-mode quantum Gaussian channels: Structure and quantum capacity*, Probl. Inf. Transm. **43**, 1 (2007).

[36] J. D. J Ingle, and S. R. Crouch, *Spectrochemical Analysis* (New Jersey: Prentice Hall, 1988).

[37] R. Jozsa, *Fidelity for Mixed Quantum States*, J. Mod. Opt. **41**, 2315 (1994).

[38] P. R. Koya, and A. T. Goshu, *Generalized Mathematical Model for Biological Growths*, Open Journal of Modelling and Simulation **1**, 42-53 (2013)

[39] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, *No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light*, Phys. Rev. Lett. **95**, 180503 (2005).

[40] U. Leonardt, *Measuring the Quantum State of Light* (Cambridge University Press, 1997).

[41] S. Lloyd, *Enhanced Sensitivity of Photodetection via Quantum Illumination*, Science **321**, 1463 (2008).

[42] C. Lupo, S. Pirandola, V. Giovannetti, and S. Mancini, *Quantum reading capacity under thermal and correlated noise*, Phys. Rev. A **87**, 062310 (2013).

[43] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, *The classical-quantum boundary for correlations: Discord and related measures*, Rev. Mod. Phys. **84**, 1655 (2012).

[44] R. Nair, *Discriminating quantum-optical beam-splitter channels with number-diagonal signal states: Applications to quantum reading and target detection*, Phys. Rev. A **84**, 032312 (2011).

[45] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press 2000).

[46] M. Nussbaum, and A. Szkola, *The Chernoff lower bound for symmetric quantum hypothesis testing*, Ann. Stat. **37**, 1040 (2009).

[47] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, *Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration*, Phys. Rev. A **91**, 022320 (2015).

[48] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Netherlands, 1997).

[49] S. Pirandola, *Entanglement reactivation in separable environments*, New J. Phys. **15**, 113046 (2013).

[50] S. Pirandola, *Quantum Reading of a Classical Digital Memory*, Phys. Rev. Lett. **106**, 090504 (2011).

[51] S. Pirandola, *Quantum discord as a resource for quantum cryptography*, Sci. Rep. **4**, 6956 (2014).

[52] S. Pirandola, and S. Lloyd, *Computable bounds for the discrimination of Gaussian states*, Phys. Rev. A **78**, 012331 (2008).

[53] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, *Quantum Reading Capacity*, New J. Phys. **13**, 113012 (2011).

[54] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L Andersen, *High-rate measurement-device-independent quantum cryptography*, Nature Photonics 9, 397-402 (2015).

[55] S. Pirandola, A. Serafini, and S. Lloyd, *Correlation matrices of two-mode bosonic systems*, Phys. Rev. A **79**, 052327 (2009).

[56] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, *Optimality of Gaussian Discord*, Phys. Rev. Lett. **113**, 140405 (2014).

[57] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, *Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks*, Phys. Rev. Lett. **111**, 130501 (2013).

[58] M. Sacchi, *Entanglement can enhance the distinguishability of entanglement-breaking channels*, Phys. Rev. A **72**, 014305 (2005).

[59] J. J. Sakurai, and J. Napolitano, *Modern Quantum Mechanics,* 2nd edition (Addison-Wesley, San Francisco, 2011).

[60] H. Scutaru, *Fidelity for displaced squeezed thermal states and the oscillator semigroup*, J. Phys. A **31**, 3659 (1998).

[61] L. Banchi, S. L. Braunstein, and S. Pirandola, *Quantum fidelity for arbitrary Gaussian states*, Phys. Rev. Lett. **115**, 260501 (2015).

[62] A. Serafini, F. Illuminati, and S. De Siena, *Symplectic invariants, entropic measures and correlations of Gaussian states*, J. Phys. B **37**, L21 (2004).

[63] A. Serafini, *Multimode Uncertainty Relations and Separability of Continuous Variable States*, Phys. Rev. Lett. **96**, 110402 (2006).

[64] J. H. Shapiro and Seth Lloyd, *Quantum illumination versus coherent-state target detection*, New J. Phys. **11**, 063045 (2009).

[65] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. **26**, 1484 (1997).

[66] C. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, *Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit*, Phys. Rev. Lett. **89**, 167901 (2002).

[67] R. Simon, *Peres-Horodecki Separability Criterion for Continuous Variable Systems*, Phys. Rev. Lett. **84**, 2726 (2000).

[68] R. Simon, N. Mukunda, and B. Dutta, *Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms*, Phys. Rev. A **49**, 1567 (1994).

[69] G. Spedalieri, C. Lupo, S. Mancini, S. L. Braunstein, and S. Pirandola, *Quantum reading under a local energy constraint*, Phys. Rev. A **86**, 012315 (2012).

[70] G. Spedalieri, C. Weedbrook, and S. Pirandola, *A limit formula for the quantum fidelity*, J. Phys. A: Math. Theor. **46**, 025304 (2013).

[71] C. G. Stanley and P. H. von Hippel, *Calculation of Protein Extinction Coefficients from Amino Acid Sequence Data*, Analytical Biochemistry **182**, 319-326 (1989).

[72] W. F. Stinespring, *Positive functions on C * -algebras*, Proc. Am. Math. Soc. **6**, 211 (1955).

[73] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, *Quantum Illumination with Gaussian States*, Phys. Rev. Lett. **101**, 253601 (2008).

[74] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, *Hiding bits in Bell states*, Phys. Rev. Lett. **86**, 5807–5810 (2001).

[75] A. R. Usha Devi and A. K. Rajagopal, *Quantum target detection using entangled photons*, Phys. Rev. A **79**, 062320 (2009).

[76] G. Vidal, and R. F. Werner, *Computable measure of entanglement*, Phys. Rev. A **65**, 032314 (2002).

[77] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, 1994).

[78] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, Rev. Mod. Phys. **84**, 621 (2012).

[79] J. Williamson, *On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems*, Am. J. Math. **58**, 141-163 (1936).

[80] W. H. Young, *On the multiplication of successions of Fourier constants*, Proc. R. Soc. London, Ser. A **87**, 331-339 (1912).

[81] H. P. Yuen, and R. Nair, *Classicalization of nonclassical quantum states in loss and noise: Some no-go theorems*, Phys. Rev. A **80**, 023816 (2009).