Quantum resources in systems with many degrees of freedom

Inaugural Dissertation

for the attainment of the title of

Doctor of natural sciences (Dr. rer. nat.)

in the Faculty of Mathematics and Natural Sciences
at the Heinrich-Heine-Universität Düsseldorf

presented by

Giulio Gianfelici

from Fermo, Italy

Düsseldorf, July 2021

from the Institute for Theoretical Physics III
at the Heinrich-Heine-Universität Düsseldorf

Published by permission of the
Faculty of Mathematics and Natural Sciences at
Heinrich-Heine-Universität Düsseldorf

Supervisor: Prof. Dr. Dagmar Bruß
Co-supervisor: PD Dr. Hermann Kampermann

Date of the oral examination: 15.09.2021

Declaration of Authorship

I declare under oath that I have compiled my dissertation independently and without any undue assistance by third parties under consideration of the "Principles for the Safeguarding of Good Scientific Practice" at Heinrich-Heine-Universität Düsseldorf"

Place, Date	Giulio Gianfelici

To my family

Abstract

In the last three decades, the use of quantum physics in information-processing tasks, such as cryptography or computing, paved the way for the theoretical design of advanced information technologies. The practical implementation of them has been however hindered by the severe fragility of quantum effects at a macroscopic level, due to phenomena such as quantum decoherence. Many quantum features can be thus viewed, in quantum information theory, as precious but limited *resources*, which one needs to study, quantify and detect.
This thesis investigates different aspects of quantum resources in systems with many degrees of freedom. These systems are associated with a great amount of theoretically possible resources, but also with complex mathematical structures and technological limitations.
In the context of cryptographic protocols of secure entity authentication, we study *physical unclonable functions* (PUFs), including extensions to quantum protocols, so-called *quantum readout PUFs* (QR-PUFs). A (QR-) PUF is a physical system that for a given input *challenge* produces a unique *response* that is intended to be hard to simulate. We propose a system-independent theoretical framework to quantitatively characterise the security of entity authentication protocols with (QR-) PUFs in terms of two main properties, the *robustness* and the *unclonability*. Our framework can be used to develop new authentication schemes and to compare different physical implementations of both classical PUFs and QR-PUFs, exploring the possible advantages of using quantum systems.
We then consider the problem of entanglement detection in unknown continuous-variable systems. We develop a scheme that employs random homodyne measurements and a semidefinite program to construct an optimal entanglement witness. We test our method in several cases, in particular with two-mode squeezed vacuum states and with general two-mode states. We show that our scheme can detect entanglement, including bound entanglement, with fewer measurements than in full tomography.
Afterwards, we analyse the connections between different resources in the framework of *quantum resource theories*. Namely, we establish a hierarchy for non-uniformity, coherence, discord and entanglement in continuous-variable systems, in particular Gaussian systems. We introduce the concept of maximal coherence at fixed energy, which is attainable with energy-preserving unitaries, and a resource theory of non-uniformity, in which the purity of a quantum state at fixed energy is identified as a resource. We prove that, by requiring Gaussian states and operations, and by using quantifiers based on the relative entropy, the Gaussian non-uniformity is equal to the maximal Gaussian coherence and can be analytically quantified. We finally show that this quantity provides upper bounds on the discord and entanglement.

Zusammenfassung

Die theoretischen Fortschritte der letzten drei Jahrzehnte, besonders Quantencomputer und Quantenkrypotografie brachten die Möglichkeit, Quantentechnologien für moderne Informationstechnologien zu verwenden. Die praktische Umsetzung dieser Ideen verlangt jedoch sehr präzise Operationen auf Quanten Zuständen, welche durch Dekohärenz meist sehr fragil sind. Aus diesem Grund können Quanten Eigenschaften als eine wertvolle, aber begrenzte *Ressource* angesehen werden, welche studiert, quantifiziert und nachgewiesen werden kann.
Diese Doktorarbeit untersucht verschiedene Aspekte von Quantenressourcen in Systemen mit vielen Freiheitsgraden. Für diese Systeme gibt es viele theoretisch mögliche Ressourcen, häufig mit komplexen mathematischen Strukturen und technologischen Beschränkungen.
Für Kryptografische Protokolle der Entität-Authentisierung, analysieren wir *physisch unklonbare Funktionen* (PUFs), sowie Erweiterungen als Quanten Protokolle, sogenannte *Quanten Auslesung PUFs* (QR-PUFs). Eine (QR-) PUF ist ein physikalisches System, welches für gegebene Eingabe (*challenge*) eine eindeutige Rückgabe (*response*) produziert, welche schwer zu simulieren sein sollte. Wir schlagen ein Systemunabhängiges, theoretisches Konstrukt vor, um die Sicherheit der Entität-Authentisierungsprotokolle mit (QR-) PUFs zu analysieren. Hierfür verwenden wir die zwei Haupteigenschaften *Robustheit* und *Unklonbarkeit*. Unser Konstrukt kann verwendet werden, um neue Authentisierungsverfahren zu entwickeln und um verschiedene physische Implementierungen von sowohl klassischen und QR PUFs zu vergleichen und damit mögliche Vorteile von Quanten Systemen zu erforschen.
Des weiteren schauen wir uns das Problem des Detektierens von Verschränktheit in unbekannten kontinuierlichen Systemen an. Wir entwickeln ein Verfahren, welches zufällige, homodyne Messungen und semidefinite Optimierung verwendet, um ideale Verschränkheitszeugen zu finden. Wir untersuchen unsere Methode für verschiedene Fälle, besonders mit zwei-Moden gequetschten Vakuum Zuständen und generellen zwei-Moden Zuständen. Wir zeigen, dass unser Verfahren Verschränktheit detektieren kann, sogar nicht-destillierbare Verschränktheit, und das mit weniger Messungen als volle Tomografie.
Danach analysieren wir die Verbindungen zwischen verschiedenen Ressourcen innerhalb von Quantenressourcentheorien. Genauer zeigen wir eine Hierarchie für nicht-Uniformität, Koherenz, Quantenzwietracht und Verschränktheit in kontinuierlichen Systemen, besonders Gaußische Systemen. Wir führen das Konzept der maximalen Kohärenz bei konstanter Energie ein, welches die maximal mögliche Kohärenz, optimiert über alle energieerhaltenden Unitären ist, so wie eine Ressourcentheorie von nicht-Uniformität, bei der die Reinheit eines Zustandes bei konstanter Energie als Ressource identifiziert wird. Wir beweisen, dass für Gaußische Zustände und Operationen und auf relativer Entropie basierender Quantifikatoren, die Gaußische nicht-Uniformität genau die maximale Gaußische Kohärenz ist und analytisch quantifiziert werden kann. Ebenso können wir zeigen, dass diese Größe eine obere Schranke an die Zwietracht und Verschränkheit liefert.

Acknowledgments

Throughout these years, I have received a great amount of help and support from many people. I want to take a moment to express my gratitude, knowing that few words cannot be enough and I cannot cite everybody who would deserve to be cited.
First, I would like to thank my supervisor, Dagmar Bruß, and my cosupervisor, Hermann Kampermann, for giving me the privilege of working with them, in the first-rate team that they have put together. Their expertise and scientific rigour have been the most valuable resource in every step of my research. I especially acknowledge them constantly pushing me to aim at excellence, both in terms of scientific content and style of writing. The skills that I learned thanks to them will certainly accompany me throughout my life.
I also wish to thank my present and past colleagues, Felix Bischof, Giacomo Carrara, Sarnava Datta, Federico Grasselli, Timo Holz, Carlo Liorni, Gláucia Murta, Lucas Tendick, Thomas Wagner and Nikolai Wyderka, together with my "quasi-colleagues" Lennart Bittel and Raphael Brieger, and the past Master's students Tatiana Mihaescu and Daniel Miller. Each one of them contributed to making a great working environment and I regret that we could not spend much time together in the last year and a half. I am especially grateful to Giacomo Carrara, Sarnava Datta, Federico Grasselli, Gláucia Murta, Lucas Tendick and Thomas Wagner for proofreading parts of this thesis, and to Lennart Bittel for translating its abstract. Moreover, I would like to thank Tatiana Mihaescu for being an excellent student. It was an honour for me to experience the other side of academia and supervise her.
Moving to Germany has been the most exciting and challenging experience of my life. I wish to express my gratitude to the other wonderful people that made my life easier and enjoyable in this country. I particularly thank Andres, Benedetta, Einar, Juliana, Malte, Nicola P. and V., and all my friends from the PhD meetup.
No fewer thanks are due to my friends in Italy, who always supported me and never allowed my absence to undermine our friendship. I am especially grateful to Cristina, Francesco, Rac, Riccardo and all the people from the University of Camerino. Many thanks also to my friends of Imdi, in particular those of IMDeutschland and Imdi Marche.
I would like to thank my grandparents Andrea and Dalia, my uncle Eliseo, my aunt Fosca and my brother Giorgio for always being on my side. Finally, my greatest gratitude goes to my parents, Ezio and Marinella, for their unconditional love, approval and trust. I truly could not have wished for better parents.

Contents

Declaration of Authorship iii

Abstract vii

Zusammenfassung ix

Acknowledgments xi

Contents xiii

List of Figures xvi

1 Introduction 1

2 Fundamentals of Linear Algebra 4
- 2.1 Vector and Hilbert Spaces . . . 4
  - 2.1.1 Inner Products . . . 6
  - 2.1.2 Dual Vectors . . . 7
  - 2.1.3 Subspaces and Direct Sum . . . 8
- 2.2 Linear Operators . . . 9
  - 2.2.1 Products and Functions of Operators . . . 9
  - 2.2.2 Adjoint Operators . . . 10
  - 2.2.3 Outer Products and Projectors . . . 11
  - 2.2.4 Matrix Representation of a Linear Operator . . . 12
  - 2.2.5 Normal Operators . . . 13
  - 2.2.6 Trace and Determinant . . . 15
  - 2.2.7 Eigenvalues and Eigenvectors . . . 16
- 2.3 Tensor Products . . . 17
- 2.4 Infinite-dimensional Hilbert Spaces . . . 19
- 2.5 Hamming Space . . . 21

3 Quantum Information with Discrete Variables 23
- 3.1 Quantum Mechanics of Closed Systems . . . 23
  - 3.1.1 State Space . . . 23
  - 3.1.2 Quantum Measurements . . . 24
  - 3.1.3 State Evolution . . . 26
  - 3.1.4 Composed Systems . . . 27
- 3.2 Quantum Mechanics of Open Systems . . . 28

3.2.1 Density Operators . . . 28
3.2.2 Postulates of Quantum Mechanics for Density Operators . . . 29
3.2.3 Reduced Density Operator and Purification . . . 31
3.2.4 Quantum Channels . . . 32
3.3 Elements of Quantum Information Theory . . . 34
3.3.1 Entropies . . . 34
3.3.2 Fidelity and Trace Distance . . . 36
3.3.3 Unclonable and Indistinguishable States . . . 37

4 Quantum Information with Continuous Variables 39
4.1 Quantum Light . . . 39
4.1.1 Second Quantisation of the Electromagnetic Field . . . 39
4.1.2 Fock Basis . . . 41
4.1.3 Coherent Basis . . . 42
4.1.4 Phase Space Representations . . . 44
4.2 Gaussian States . . . 47
4.2.1 Notable Gaussian States . . . 49
4.3 Gaussian Unitaries . . . 53
4.3.1 Linear Displacements . . . 54
4.3.2 Phase Shifters and Beam Splitters . . . 54
4.3.3 Squeezing Operators . . . 55
4.3.4 Passive and Active Gaussian Unitaries . . . 56
4.4 Gaussian Channels . . . 57
4.5 Gaussian Measurements . . . 58
4.5.1 Homodyne Detection . . . 58
4.5.2 Heterodyne Detection . . . 59

5 Secure Entity Authentication with (QR-) PUFs 60
5.1 Elements of Cryptography . . . 60
5.1.1 Entity Authentication . . . 61
5.2 Physical Unclonable Functions . . . 62
5.2.1 Types of PUFs . . . 63
5.2.2 Fuzzy Extractors . . . 65
5.2.3 PUF Formalisation Attempts . . . 66
5.3 Quantum Readout of Physical Unclonable Functions . . . 68
5.4 Formalisation of (QR)-PUFs . . . 69
5.4.1 Results . . . 69

6 Entanglement Detection for Unknown Continuous-variable States 73
6.1 Continuous-variable Entanglement . . . 73
6.1.1 Bipartite Entanglement . . . 75
6.2 Entanglement Witnesses . . . 77
6.3 Methods . . . 78
6.3.1 Semidefinite Programming . . . 78
6.3.2 Quantum Tomography via Homodyne Measurements . . . 79
6.4 Detecting Entanglement of Unknown CV States . . . 81
6.4.1 Results . . . 81

7 Hierarchy of Quantum Resource Theories **86**
7.1 Resource Theories 86
7.1.1 Quantifying Resources 88
7.2 Discrete-variable Resource Theories 89
7.2.1 Resource Theory of Coherence 89
7.2.2 Resource Theories of Athermality and Purity (Non-uniformity) 91
7.2.3 Resource Theory of Entanglement 93
7.2.4 Resource Theory of Discord 94
7.2.5 Relations between the Resource Theories 95
7.3 Continuous-variable Resource Theories 96
7.3.1 Resource Theory of (Gaussian) Coherence 97
7.3.2 Resource Theory of (Gaussian) Discord 98
7.4 Hierarchy of Quantum Resource Theories in CV Systems 98
7.4.1 Results 98

8 Conclusions and Outlook **102**

Bibliography **104**

A Theoretical framework for PUFs, including quantum readout **115**

B Detecting entanglement of unknown CV states with random measurements **128**

C Hierarchy of CV quantum resource theories **144**

List of Figures

5.1 Enrollment and verification stage with PUFs 63
5.2 Authentication protocol with (QR-) PUFs 70

6.1 Entanglement witnesses 77
6.2 Quantum tomography using a single homodyne detector 80
6.3 Entanglement detection for two-mode squeezed vacuum states 82
6.4 Entanglement detection for two-mode random states 83
6.5 Entanglement detection for a four-mode bound entangled state 84
6.6 Statistical analysis of the entanglement witness for Gaussian states 85

7.1 A system labeled by spectral and spatial modes 99
7.2 Hierarchy of continuous-variable non-Gaussian resources 101
7.3 Hierarchy of continuous-variable Gaussian resources 101

1 Introduction

Quantum mechanics is the physical theory that describes the behaviour of matter and radiation at the length and energy scales of atoms and subatomic particles. The emergence of quantum mechanics, one century ago, sparked an intense scientific and philosophical debate, which is still ongoing today. Quantum systems exhibit counter-intuitive properties which are often improperly labelled as "paradoxes", such as the wave-particle duality [Boh28; Hei49] or the entanglement [EPR35; Sch35].

A change of paradigm slowly started to take place in the seventies of the last century, with a strong acceleration in the early nineties. Quantum physics has established a symbiotic relationship with *information theory* [Sha48], a field that studies the storage and communication of information in a quantitative way. From an information-theoretic viewpoint, a quantum state is only a mathematical function that encodes *information* about the possible outcomes of a measurement [Per95]. This perspective contributes to clarifying the features of quantum theory that were once considered paradoxical.

Analogously, information theory has benefitted greatly from quantum physics. The use of *quantum resources* generally expands the perimeter of classical information-processing tasks [NC10]. The theoretical and experimental research in *quantum information science* grew in sophistication in the last decades and is starting to produce tangible technological applications [BL19]. However, the practical implementation on a large scale of the theoretical predictions of quantum information theory is technologically and financially challenging, since it requires the complete control of quantum systems and the ability to use them at a macroscopic level. There is thus the necessity of employing quantum resources mindfully, always comparing, in given scenarios, the advantage that they may bring to the costs involved in using them. Moreover, there is the need to develop techniques to efficiently detect and quantify the resources in given quantum systems.

One of the most relevant branches of quantum information is *quantum cryptography*. In 1984, Charles H. Bennett and Gilles Brassard proposed a protocol (today named BB84) that uses quantum states to securely distribute a secret key between two parties [BB84], who can then use this key for the encryption and decryption of private messages. Because quantum

measurements introduce disturbances in a quantum system, an eavesdropper cannot learn the key without being exposed by the legitimate parties. Other *quantum key distribution* (QKD) protocols followed [Eke91; Bru98; Sca+09] and today QKD is perhaps the most celebrated subfield of quantum information science. The interest in quantum cryptography beyond QKD also grew in the last few years.

An important cryptographic task is *entity authentication*, which is the assurance that a given entity can prove its identity and its involvement in the communication session to another entity [Mar12]. *Physical unclonable functions* (PUFs) [Pap01; Pap+02] are a tool to achieve secure entity authentication. They are physical systems, with a complex inner structure, that unpredictably interact with external signals. In an authentication protocol with PUFs, a party sends a determined input signal (called *challenge*) and the other party has to provide the corresponding unique output signal (called *response*) to confirm her/his identity. An extension of PUFs to quantum protocols was proposed by Boris Škorić in 2010, under the name of *quantum read-out PUFs* (QR-PUFs) [Ško12]. QR-PUFs encode challenges and responses in quantum states and are expected to be more secure than classical PUFs. At the time of completing this thesis (July 2021), this possible advantage has not been rigorously quantified for specific experimental implementations.

A significant problem in quantum information theory is to efficiently detect the presence of quantum resources in an unknown quantum state. For instance, many criteria of *entanglement detection* require the knowledge of the density matrix of the system under investigation [Hor+09]. A completely unknown state can be fully reconstructed by *quantum tomography* [DPS03; LR09], which is a very demanding experimental procedure, especially for quantum states with many degrees of freedom. Alternatively, one can use practicable tests that detect entanglement in only a subset of states. A prominent class of tests is that of *entanglement witnesses* [HHH96; Ter00; HE06], which are functionals on the space of quantum states that separate all separable states from some entangled states. Entanglement witnesses may only need partial information about a state to efficiently detect entanglement in it.

The concept of quantum resource has been meticulously formalised by *quantum resource theories* [CG19]. The set of quantum states is partitioned into two subsets, one of *free states*, having no resource, and another of *resource states*. This partition induces an analogous division in the set of quantum operations, where the *free operations* are defined as those which transform any free state into a free state. The sets of free states and operations depend on the specific resource theory. For instance, the states that are diagonal in a certain basis are the free states of the resource theory of *coherence* [Åbe06; BCP14], while the maximally mixed state is the only free state of the resource theory of *purity* [HHO03; Gou+15]. Quantum resource theories provide a way to quantify resources through the so-called *resource monotones*, which are functions that do not increase under free operations. An important class of monotones is that of *distance-based monotones*, where the amount of resource of a quantum state is quantified by its distance with the set of free states. This class also includes some improper distance functions, such as the *relative entropy* [CG19]. The same distance can be used in monotones for different resource theories, thus allowing us to study the relations between different resource theories and the possibility to convert a resource into another. In particular, we can investigate the existence of *hierarchies* of resources [Str+18], i.e. structured relations between the quantities of different resources in given states.

In this thesis, we present our research on quantum resources in systems with many degrees of freedom, namely discrete-variable (QR-) PUFs and continuous-variable multimode systems.

The dissertation is organised as follows.

In Chap. 2, we review basic concepts of linear algebra that are necessary to understand the remainder of the thesis.

In Chap. 3, we introduce the principles of discrete-variable quantum information theory that are used in our work. This chapter includes a discussion of the postulates of quantum mechanics from the viewpoint of quantum information theory.

Chap. 4 is devoted to continuous-variable quantum information theory. In particular, we discuss the representations of continuous-variable quantum systems in the real phase space, and the relevant subset of Gaussian states.

In Chap. 5, we describe the results of our publication [GKB20], where we proposed a theoretical framework to formalise the security of entity authentication protocols with (QR-) PUFs in a quantitative and implementation-independent way. Our results are given with an introduction to the main concepts of entity authentication protocols, PUFs and QR-PUFs.

In Chap. 6, we introduce the results of our publication [Mih+20], where we proposed a scheme to construct an optimal entanglement witness for an unknown continuous-variable state, using a semidefinite program and random homodyne measurements. Together with our results, we review the topic of continuous-variable entanglement and the methods that are used in our publication.

In Chap. 7, we describe the results of our publication [GKB21], where we established a hierarchy of continuous-variable resources. Our results are given with an introduction to quantum resource theories and analogous hierarchies of discrete-variable resources [Str+18].

Finally, in Chap. 8 we conclude and give an outlook for possible future works. The full text of our publications, together with publication details, are contained in the Appendix.

2

Fundamentals of Linear Algebra

Linear algebra is the mathematical backbone of quantum mechanics. This chapter summarises the most important concepts of linear algebra that are used throughout the thesis, employing the Dirac formalism. We include a section on the Hamming space, to formally describe the concept of *bit*. The inexperienced reader may find it useful to carefully read this chapter, while the experienced reader may choose to glance over it. The content is mostly inspired by [Ros11; Sha12; MW20]. All theorems in this chapter are given without proof.

2.1 Vector and Hilbert Spaces

Definition 2.1. A *vector space* $\mathcal{V}$ is a collection of objects $\{|v\rangle, |w\rangle, \dots\}$, called *vectors*, for which there exist two closed operations, an *addition* $+ : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ and a *scalar multiplication* $\cdot : \mathcal{V} \times \mathbb{F} \to \mathcal{V}$, where $\mathbb{F}$ is a field called the *scalar field*. The closure conditions are summarised by requiring $\alpha |v\rangle + \beta |w\rangle \in \mathcal{V}$, for all $|v\rangle, |w\rangle \in \mathcal{V}$ and $\alpha, \beta \in \mathbb{F}$. The addition must satify the following conditions.

1. *Commutative law*: $|v\rangle + |w\rangle = |w\rangle + |v\rangle$, for all $|v\rangle, |w\rangle \in \mathcal{V}$;
2. *Associative law*: $|v\rangle + (|w\rangle + |z\rangle) = (|v\rangle + |w\rangle) + |z\rangle$, for all $|v\rangle, |w\rangle, |z\rangle \in \mathcal{V}$;
3. *Existence of an additive identity*: $\mathcal{V}$ contains a unique vector $\mathbf{0}$, called the *null vector*, such that $\mathbf{0} + |v\rangle = |v\rangle + \mathbf{0}$ for all $|v\rangle \in \mathcal{V}$;
4. *Existence of additive inverses*: for each $|v\rangle \in \mathcal{V}$, there exists a unique inverse vector, denoted by $-|v\rangle$, such that $|v\rangle + (-|v\rangle) = \mathbf{0}$.

The scalar multiplication must satisfy the following conditions:

1. *Distributive law for vectors*: $\alpha \cdot (|v\rangle + |w\rangle) = \alpha \cdot |v\rangle + \alpha \cdot |w\rangle$, for all $|v\rangle, |w\rangle \in \mathcal{V}$ and $\alpha \in \mathbb{F}$;

2. *Distributive law for scalars*: $(\alpha+\beta)\cdot|v\rangle = \alpha\cdot|v\rangle + \beta\cdot|v\rangle$, for all $|v\rangle \in \mathcal{V}$ and $\alpha,\beta\in\mathbb{F}$;
3. *Associative law*: $\alpha\cdot(\beta\cdot|v\rangle) = (\alpha\beta)\cdot|v\rangle$, for all $|v\rangle\in\mathcal{V}$ and $\alpha,\beta\in\mathbb{F}$;
4. *Multiplication by* 0 *and* 1: given the additive identity 0 and the multiplicative identity 1 of $\mathbb{F}$, $0\cdot|v\rangle = \mathbf{0}$ and $1\cdot|v\rangle = |v\rangle$ for all $|v\rangle\in\mathcal{V}$.

In the following, we are going to omit the symbol $\cdot$ in the scalar multiplication, i.e. we will write $\alpha\,|v\rangle$ instead of $\alpha\cdot|v\rangle$.

There are different notations for the vector symbol. In Def. 2.1, we used the *Dirac notation* [Dir39], that is pre-eminent in quantum mechanics. In this notation, vectors $|v\rangle$ are called *kets*, for reasons that will be explained later in the chapter. We preferentially use this notation. Alternatively, vectors can be denoted by bold letters, i.e $\boldsymbol{v}$ in place of $|v\rangle$. In Def. 2.1, we have reserved this notation to the null vector $\mathbf{0}$, since the symbol $|0\rangle$ usually represents a different vector in quantum mechanics. In the following, we are simply going to denote the null vector by 0, since there is no risk of confusion. Moreover, we will use the bold notation in parallel with the Dirac notation when we need to employ two different vector spaces at the same time.

Regarding the scalar field, we are always going to employ the complex field $\mathbb{C}$, unless otherwise specified (see Sec. 2.5).

Definition 2.2. A set of n vectors $|u_i\rangle \neq 0$ in $\mathcal{V}$ is said to be *linearly independent* if there are no scalar solutions $\{\alpha_i\}$ $(i=1,\ldots,n)$ for the equation

$$\sum_{i=1}^{n} \alpha_i\ |u_i\rangle = 0, \tag{2.1}$$

except for the trivial one, with all $\alpha_i = 0$. A vector space is called *n-dimensional*, if it admits at most n linearly independent vectors.

The dimension of a vector space can be finite or infinite. We consider at the moment only finite-dimensional spaces, with dimension n, and delay the extension to infinite dimensions until Sec. 2.4.

Definition 2.3. An ordered set $\{|u_i\rangle\} := \{|u_i\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$ of n linearly independent vectors in a n-dimensional vector space $\mathcal{V}$ is called a *basis* for $\mathcal{V}$.

Theorem 2.4. *Every vector $|v\rangle\in\mathcal{V}$ can be written as a unique* linear combination *of the elements of a basis $\{|u_i\rangle\}$, i.e.*

$$|v\rangle = \sum_{i=1}^{n} v_i\ |u_i\rangle, \tag{2.2}$$

for some $v_i\in\mathbb{C}$, called the components *of $|v\rangle$ in the basis $\{|u_i\rangle\}$. For this reason, we say that $\mathcal{V}$ is* spanned *by $\{|u_i\rangle\}$.*

Therefore, every vector $|v\rangle\in\mathcal{V}$ can be represented by its components $\{v_1, v_2, \ldots, v_n\}$ in a basis $\{|u_i\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$. Mathematically, we say that any n-dimensional vector space $\mathcal{V}$ is *isomorphic* to $\mathbb{C}^n$ since there exists an isomorphism that maps any vector $|v\rangle\in\mathcal{V}$ to a *column vector* in $\mathbb{C}^n$:

$$|v\rangle \Leftrightarrow \boldsymbol{v} := \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \qquad v_j\in\mathbb{C}. \tag{2.3}$$

In the following chapters, we are going to follow the convention of using the same symbol to indicate abstract vectors and their column representation. Here, we use different symbols for clarity.

2.1.1 Inner Products

Definition 2.5. An *inner product* in a vector space $\mathcal{V}$ is an operation that associates to any two vectors $|v\rangle, |w\rangle \in \mathcal{V}$ a complex number $\langle v|w\rangle \in \mathbb{C}$ and satisfies the following axioms:

1. $\langle v|v\rangle \geq 0$ for all $|v\rangle \in \mathcal{V}$, and $\langle v|v\rangle = 0$ if and only if $|v\rangle = 0$;
2. $\langle v|w\rangle = \langle w|v\rangle^*$, for all $|v\rangle, |w\rangle \in \mathcal{V}$;
3. If $|u\rangle = \alpha\ |w\rangle + \beta\,|z\rangle$, then $\langle v|u\rangle = \alpha\,\langle v|w\rangle + \beta\,\langle v|z\rangle$ and $\langle u|v\rangle = \alpha^*\,\langle w|v\rangle + \beta^*\,\langle z|v\rangle$.

The inner product is also called *scalar product* but we avoid this naming to prevent confusion with the scalar multiplication of Def. 2.1.

Definition 2.6. A finite-dimensional vector space equipped with an inner product is called a *Hilbert space* and is denoted by $\mathcal{H}$.

The proper definition of Hilbert space, valid for both finite and infinite dimensions, is more involved (see Sec. 2.4). For the moment, we are going to use Def. 2.6.

Definition 2.7. The *norm* of a vector $|v\rangle \in \mathcal{H}$ is the non-negative real number

$$\|v\| := \sqrt{\langle v|v\rangle}. \tag{2.4}$$

A vector $|v\rangle \in \mathcal{H}$ is called a *unit vector* if $\|v\| = 1$.

Definition 2.8. A *distance* is a function $d : \mathcal{H} \times \mathcal{H} \to \mathbb{R}_{\geq 0}$ that associates to any pair of vectors $|v\rangle, |w\rangle \in \mathcal{H}$ a non-negative real number, $d(v, w)$, and satisfies the following requirements:

1. $d(v, w) = d(w, v)$;
2. $d(v, w) \geq 0$, and $d(v, w) = 0$ if and only if $|v\rangle = |w\rangle$;
3. $d(v, w) \leq d(v, z) + d(w, z)$ (*triangle inequality*).

A vector space that admits a distance is said to be a *metric space*.

Theorem 2.9. *For any pair of vectors $|v\rangle, |w\rangle \in \mathcal{H}$, the norm of $|v\rangle - |w\rangle$, denoted by $\|v - w\|$, is a valid distance for $\mathcal{H}$, i.e. it satisfies the requirements of Def. 2.8.*

The distance induced by the inner product is not the only distance that we will use in this thesis.

Definition 2.10. Two vectors $|v\rangle, |w\rangle \in \mathcal{H}$ are said *orthogonal* if

$$\langle v|w\rangle = 0, \tag{2.5}$$

and *orthonormal* if

$$\langle v|w\rangle = 0, \quad \text{and} \quad \|v\| = \|w\| = 1. \tag{2.6}$$

Theorem 2.11. *Orthogonal vectors are linearly independent. Thus, a set of n orthogonal (orthonormal) vectors $\{|e_i\rangle\}$ in a n-dimensional Hilbert space $\mathcal{H}$ automatically forms a basis, called an* orthogonal (orthonormal) basis.

The orthonormality condition reads:

$$\langle e_i|e_j\rangle = \delta_{ij}, \tag{2.7}$$

where δ_{ij} is the *Kronecker delta*:

$$\delta_{ij} := \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases} \tag{2.8}$$

By using Eqs. (2.2) and (2.7) and Def. 2.5, we obtain a formula for the the inner product $\langle v|w\rangle$ in terms of the components of $|v\rangle$ and $|w\rangle$ in an orthonormal basis $\{|e_i\rangle\}$:

$$\langle v|w\rangle = \sum_i \sum_j v_i^* \, w_j \, \langle e_i|e_j\rangle = \sum_i v_i^* \, w_i. \tag{2.9}$$

Thus, the norm of $|v\rangle$ is the positive square root of

$$\|v\|^2 = \langle v|v\rangle = \sum_i |v_i|^2 . \tag{2.10}$$

The inner product of $|v\rangle$ with the j-th element of a basis $\{|e_i\rangle\}$ is the j-th component of $|v\rangle$ in the basis $\{|e_i\rangle\}$:

$$\langle e_j|v\rangle = \sum_i v_i \, \langle e_j|e_i\rangle = v_j. \tag{2.11}$$

Theorem 2.12. *The result of an inner product does not depend on the basis used to compute it. Namely, for any two orthonormal bases $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ of $\mathcal{H}$ and for any two vectors $|v\rangle, |w\rangle \in \mathcal{H}$:*

$$\sum_i v_i^{(e)\,*} \, w_i^{(e)} = \sum_i v_i^{(f)\,*} \, w_i^{(f)}, \tag{2.12}$$

where $v_i^{(e)}$ and $w_i^{(e)}$ are the i-th components of $|v\rangle$ and $|w\rangle$ in the basis $\{|e_i\rangle\}$, and $v_i^{(f)}$ and $w_i^{(f)}$ are the i-th components of $|v\rangle$ and $|w\rangle$ in the basis $\{|f_i\rangle\}$.

This theorem is consistent with Def 2.5, where the inner product is defined as a unique function from two vectors to a number.

2.1.2 Dual Vectors

Definition 2.13. To each ket $|v\rangle \in \mathcal{H}$, we associate a linear function $\langle\cdot| : \mathcal{H} \to \mathbb{C}$, called *dual vector* (or *bra*), such that

$$\langle v| \left(|w\rangle\right) := \langle v|w\rangle , \qquad \forall \ |w\rangle \in \mathcal{H}. \tag{2.13}$$

The space of all bras acting on $\mathcal{H}$ is called the *dual space* of $\mathcal{H}$, and is denoted by $\mathcal{H}^*$. The isomorphism between $\mathcal{H}$ and $\mathcal{H}^*$ is called the *adjoint* (or *dagger*) *operation*, denoted by $\dagger$. It acts as

$$\left(\alpha \, |v\rangle + \beta \, |w\rangle\right)^\dagger = \alpha^* \, \langle v| + \beta^* \, \langle w| . \tag{2.14}$$

We now understand why Dirac introduced the words "ket" and "bra": in Dirac notation, the inner product ("bra-c-ket") can be thought of as a bra acting on a ket.

We represent a bra $\langle v|$ in terms of the components of $|v\rangle$ by a *row vector*,

$$\langle v| \Leftrightarrow \boldsymbol{v}^\dagger = \begin{pmatrix} v_1^* & v_2^* & \dots & v_n^* \end{pmatrix}, \qquad v_j \in \mathbb{C}. \tag{2.15}$$

Thus, the adjoint performs a *conjugate transposition*,

$$\boldsymbol{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \mapsto \boldsymbol{v}^\dagger = \begin{pmatrix} v_1^* & v_2^* & \dots & v_n^* \end{pmatrix}, \tag{2.16}$$

and the formula in Eq. (2.9) for the inner product in terms of the vector components becomes a *matrix multiplication*:

$$\langle v|w\rangle = \boldsymbol{v}^\dagger \, \boldsymbol{w} = \begin{pmatrix} v_1^* & v_2^* & \dots & v_n^* \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \sum_{i=1}^{n} v_i^* \, w_i. \tag{2.17}$$

2.1.3 Subspaces and Direct Sum

Definition 2.14. A non-empty subset $\mathcal{K}$ of a Hilbert space $\mathcal{H}$ is said to be a *subspace* of $\mathcal{H}$, if it is closed under the same addition and scalar multiplication of $\mathcal{H}$, i.e. if $\alpha\,|v_k\rangle + \beta\,|w_k\rangle \in \mathcal{K}$ for all $|v_k\rangle, |w_k\rangle \in \mathcal{K}$ and $\alpha, \beta \in \mathbb{C}$.

If $\mathcal{H}$ is n-dimensional, then $\mathcal{K}$ is $n_{\mathcal{K}}$-dimensional, with $n_{\mathcal{K}} \leq n$.

Definition 2.15. Two subspaces $\mathcal{K}, \mathcal{K}' \subseteq \mathcal{H}$ of a Hilbert space $\mathcal{H}$ are said to be *orthogonal* if

$$\langle v_k|v_{k'}\rangle = 0, \tag{2.18}$$

for all $|v_k\rangle \in \mathcal{K}$ and $|v_{k'}\rangle \in \mathcal{K}'$. They are denoted by $\mathcal{K} \perp \mathcal{K}'$.

Definition 2.16. Given two orthogonal subspaces $\mathcal{K}$ and $\mathcal{K}'$, we define their *orthogonal direct sum* as:

$$\mathcal{K} \oplus \mathcal{K}' := \{|v_k\rangle + |v_{k'}\rangle : |v_k\rangle \in \mathcal{K}, |v_{k'}\rangle \in \mathcal{K}'\}. \tag{2.19}$$

We write $|v_k\rangle \oplus |v_{k'}\rangle$ instead of $|v_k\rangle + |v_{k'}\rangle$ when we need to emphasise that $|v_k\rangle \in \mathcal{K}$ and $|v_{k'}\rangle \in \mathcal{K}'$.

Definition 2.17. The *orthogonal complement* of a subspace $\mathcal{K} \subseteq \mathcal{H}$ is the unique subspace $\mathcal{K}^\perp$, orthogonal to $\mathcal{K}$, such that $\mathcal{K} \oplus \mathcal{K}^\perp = \mathcal{H}$.

Theorem 2.18. *If $\mathcal{K} \perp \mathcal{K}'$, then the dimension of $\mathcal{K} \oplus \mathcal{K}'$ is the sum of the dimensions of $\mathcal{K}$ and $\mathcal{K}'$.*

For instance, let us consider a 5-dimensional Hilbert space $\mathcal{H}_5$, spanned by an orthonormal basis $\{|e_1\rangle, |e_2\rangle, |e_3\rangle, |e_4\rangle, |e_5\rangle\}$. We can define a 2-dimensional subset $\mathcal{K}_2$, spanned by $\{|e_1\rangle, |e_2\rangle\}$, and a 3-dimensional subset $\mathcal{K}_3$, spanned by $\{|e_3\rangle, |e_4\rangle, |e_5\rangle\}$. Each subset is the orthogonal complement of the other. Given two vectors, $|v\rangle = v_1 |e_1\rangle + v_2 |e_2\rangle \in \mathcal{K}_2$ and $|w\rangle = w_3 |e_3\rangle + w_4 |e_4\rangle + w_5 |e_5\rangle \in \mathcal{K}_3$, we can write their direct sum in terms of the components of $|v\rangle$ and $|w\rangle$ as:

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \oplus \begin{pmatrix} w_3 \\ w_4 \\ w_5 \end{pmatrix} := \begin{pmatrix} v_1 \\ v_2 \\ w_3 \\ w_4 \\ w_5 \end{pmatrix}. \tag{2.20}$$

2.2 Linear Operators

Definition 2.19. A *linear operator* $\hat{A}$ is a map $\hat{A} : \mathcal{H} \to \mathcal{H}$ that associates to any $|v\rangle \in \mathcal{H}$ another vector in $\mathcal{H}$, denoted by $\hat{A}|v\rangle$, with the requirement that

$$\hat{A}(\alpha |v\rangle + \beta |w\rangle) = \alpha \hat{A} |v\rangle + \beta \hat{A} |w\rangle, \tag{2.21}$$

for all $|v\rangle, |w\rangle \in \mathcal{H}$ and for all $\alpha, \beta \in \mathbb{C}$.

We denote by $\mathcal{L}(\mathcal{H})$ the set of linear operators $\hat{A} : \mathcal{H} \to \mathcal{H}$ on the Hilbert space $\mathcal{H}$.
The most basic example is the *identity operator* $\hat{I}$, which leaves every vector unchanged:

$$\hat{I} |v\rangle = |v\rangle, \qquad \forall\ |v\rangle \in \mathcal{H}. \tag{2.22}$$

Another example is the *null operator* $\hat{0}$, which transforms every vector into the null vector:

$$\hat{0} |v\rangle = 0, \qquad \forall\ |v\rangle \in \mathcal{H}. \tag{2.23}$$

Like for the null vector, in the following we will simply denote the null operator by 0.

Definition 2.20. The *inverse* of $\hat{A}$, denoted by $\hat{A}^{-1}$, is the operator that satisfies

$$\hat{A}\hat{A}^{-1} = \hat{A}^{-1}\hat{A} = \hat{I}. \tag{2.24}$$

$\hat{A}$ is said to be *invertible* if its inverse $\hat{A}^{-1}$ exists.

Definition 2.21. If $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}'$, the direct sum of two linear operators, $\hat{A} \in \mathcal{L}(\mathcal{K})$ and $\hat{B} \in \mathcal{L}(\mathcal{K}')$, is the linear operator $\hat{A} \oplus \hat{B} \in \mathcal{L}(\mathcal{H})$ that acts on every $|v\rangle = |v_1\rangle \oplus |v_2\rangle$ as:

$$\left(\hat{A} \oplus \hat{B}\right) |v\rangle = \hat{A} |v_1\rangle \oplus \hat{B} |v_2\rangle. \tag{2.25}$$

2.2.1 Products and Functions of Operators

Definition 2.22. The product $\hat{A}\hat{B}$ of two operators $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H})$ is the operator that corresponds to a sequential action of $\hat{B}$ and $\hat{A}$:

$$\hat{A}\hat{B} |v\rangle = \hat{A}(\hat{B} |v\rangle), \qquad \forall\ |v\rangle \in \mathcal{H}. \tag{2.26}$$

Clearly, $\hat{A}\hat{I} = \hat{I}\hat{A} = \hat{A}$. However, the product of operators is not, in general, commutative.

Definition 2.23. The *commutator* of two operators $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H})$ is defined as:

$$[\hat{A}, \hat{B}] := \hat{A}\hat{B} - \hat{B}\hat{A}. \tag{2.27}$$

When $[\hat{A}, \hat{B}] = 0$, we say that $\hat{A}$ and $\hat{B}$ *commute*.

The following properties hold for the commutator of any three operators $\hat{A}, \hat{B}, \hat{C} \in \mathcal{L}(\mathcal{H})$:

- $[\hat{A}, \hat{B}\hat{C}] = \hat{B}[\hat{A}, \hat{C}] + [\hat{A}, \hat{B}]\hat{C}$;
- $[\hat{A}\hat{B}, \hat{C}] = \hat{A}[\hat{B}, \hat{C}] + [\hat{A}, \hat{C}]\hat{B}$;
- $[\hat{A}, [\hat{B}, \hat{C}]] + [\hat{B}, [\hat{C}, \hat{A}]] + [\hat{C}, [\hat{A}, \hat{B}]] = 0$ (*Jacobi identity*).

Definition 2.24. Let $n \geq 0$. The n-th power of an operator $\hat{A}$ is defined as:

$$\hat{A}^n := \begin{cases} \underbrace{\hat{A}\hat{A}\ldots\hat{A}}_{(n \text{ times})}, & n > 0; \\ \hat{I}, & n = 0. \end{cases} \tag{2.28}$$

Definition 2.25. Let us consider a function $f : \mathbb{C} \to \mathbb{C}$. If f admits a series expansion

$$f(x) = \sum_{n=0}^{\infty} a_n x^n, \qquad x \in \mathbb{C}, \tag{2.29}$$

we define a *function of operators* $f : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ as:

$$f(\hat{A}) = \sum_{n=0}^{\infty} a_n \hat{A}^n, \qquad \hat{A} \in \mathcal{L}(\mathcal{H}). \tag{2.30}$$

In general, $f(\hat{A})$ does not have the same properties of $f(x)$. For instance, the exponential function satisfies $e^x\, e^y = e^{x+y}$ for $x, y \in \mathbb{C}$, whereas this is not true in the case of operators, i.e. $e^{\hat{A}}\, e^{\hat{B}} \neq e^{\hat{A}+\hat{B}}$ for general $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H})$.

Theorem 2.26. *If* $[\hat{A}, [\hat{A}, \hat{B}]] = [\hat{B}, [\hat{A}, \hat{B}]] = \hat{0}$*, then*

$$e^{\hat{A}}\, e^{\hat{B}} = e^{\hat{A}+\hat{B}}\, e^{\frac{1}{2}[\hat{A},\hat{B}]\hat{I}}. \tag{2.31}$$

This formula is called the Baker-Campbell-Hausdorff formula*.*

2.2.2 Adjoint Operators

We can define the action of linear operators on bras. For any $\langle v| \in \mathcal{H}^*$, we define $\langle v|\, \hat{A}$ as the dual vector such that:

$$\left(\langle v|\, \hat{A}\right) |w\rangle := \langle v| \left(\hat{A}\, |w\rangle\right), \qquad \forall\ |w\rangle \in \mathcal{H}. \tag{2.32}$$

We denote this braket by $\langle v|\hat{A}|w\rangle$, signifying that $\hat{A}$ can act either on $|w\rangle$ or on $\langle v|$. The linearity of $\hat{A}$ also applies to bras:

$$\Big(\langle v|\,\alpha + \langle w|\,\beta\Big)\,\hat{A} = \alpha\ \langle v|\,\hat{A} + \beta\,\langle w|\,\hat{A}. \tag{2.33}$$

One may be tempted to assume that $\langle v|\,\hat{A}$ is the dual vector of $\hat{A}\,|v\rangle$. However, by comparing Eq. (2.33) with the fact that the dual vector of $\alpha\,|v\rangle + \beta\,|w\rangle$ is $\langle v|\,\alpha^* + \langle w|\,\beta^*$, we conclude that this is not the case.

Definition 2.27. The *adjoint operator* of $\hat{A}$ is the operator $\hat{A}^\dagger$ such that $\langle v|\,\hat{A}^\dagger$ is the dual vector of $\hat{A}\,|v\rangle$, for any $|v\rangle \in \mathcal{H}$. Alternatively, by employing the property $\langle v|w\rangle = \langle w|v\rangle^*$, we define $A^\dagger$ as the operator that satisfies

$$\langle v|\hat{A}^\dagger|w\rangle = (\langle w|\hat{A}|v\rangle)^*. \tag{2.34}$$

The adjoint is an *idempotent* operation:

$$\left(\hat{A}^\dagger\right)^\dagger = \hat{A}, \qquad \forall\ \hat{A} \in \mathcal{L}(\mathcal{H}). \tag{2.35}$$

Moreover, the adjoint is *anti-linear* and *anti-distributive*, i.e. for all $\hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H})$ and $\alpha, \beta \in \mathbb{C}$,

$$\left(\alpha\hat{A} + \beta\hat{B}\right)^\dagger = \alpha^*\hat{A}^\dagger + \beta^*\hat{B}^\dagger, \tag{2.36}$$

$$\left(\hat{A}\hat{B}\right)^\dagger = \hat{B}^\dagger\hat{A}^\dagger. \tag{2.37}$$

2.2.3 Outer Products and Projectors

Definition 2.28. The *outer product* of $|v\rangle, |w\rangle \in \mathcal{H}$, denoted by $|v\rangle\langle w|$, is the linear operator that acts on every $|z\rangle \in \mathcal{H}$ as follows:

$$(|v\rangle\langle w|)\,|z\rangle := \langle w|z\rangle\ |v\rangle\,. \tag{2.38}$$

The adjoint of $|v\rangle\langle w|$ is $|w\rangle\langle v|$. Let us now consider $|e_j\rangle\langle e_j|$, where $|e_j\rangle$ is an element of an orthonormal basis $\{|e_i\rangle\}$ in $\mathcal{H}$. Its action on a vector $|v\rangle \in \mathcal{H}$ reads:

$$|e_j\rangle\langle e_j|\,|v\rangle = |e_j\rangle\langle e_j| \sum_{i=1}^{n} v_i\,|e_i\rangle = v_j\ |e_j\rangle\,. \tag{2.39}$$

Therefore, it holds:

$$|v\rangle = \sum_{i=1}^{n} v_i\,|e_i\rangle = \sum_{i=1}^{n} \langle e_i|v\rangle\,|e_i\rangle = \left(\sum_{i=1}^{n} |e_i\rangle\langle e_i|\right)|v\rangle\,. \tag{2.40}$$

This implies the following *completeness relation*:

$$\sum_{i=1}^{n} |e_i\rangle\langle e_i| = \hat{I}, \tag{2.41}$$

where $\hat{I}$ is the identity. The operator $|e_j\rangle\langle e_j|$ projects a vector $|v\rangle \in \mathcal{H}$ onto a 1-dimensional subspace $\mathcal{K}_j \subseteq \mathcal{H}$, spanned by $|e_j\rangle$. We say that $|e_j\rangle\langle e_j|$ is an *orthogonal projector*.

Definition 2.29. A *projector* is a linear operator $\hat{\Pi}_{\mathcal{K}} : \mathcal{H} \to \mathcal{K} \subseteq \mathcal{H}$ that is *idempotent*, i.e.

$$\hat{\Pi}_{\mathcal{K}}^2 = \hat{\Pi}_{\mathcal{K}}. \tag{2.42}$$

A projector is said to be *orthogonal* if $\hat{\Pi}_{\mathcal{K}} = \hat{\Pi}_{\mathcal{K}}^\dagger$.

The idempotence of $\hat{\Pi}_{\mathcal{K}}$ implies that $\hat{\Pi}_{\mathcal{K}} |v_k\rangle = |v_k\rangle$ for all $|v_k\rangle \in \mathcal{K}$. Therefore, a projector onto a subspace $\mathcal{K}$ coincides with the identity in the subspace $\mathcal{K}$.

2.2.4 Matrix Representation of a Linear Operator

We have represented kets and bras in terms of their components as columns and rows, respectively. Using the completeness relation in Eq. (2.41) for the projectors onto an orthonormal basis $\{|e_i\rangle\}$, every linear operator $\hat{A} \in \mathcal{L}(\mathcal{H})$ can be written as:

$$\hat{A} = \sum_{i=1}^{n} |e_i\rangle \langle e_i| \; \hat{A} \sum_{j=1}^{n} |e_j\rangle \langle e_j| = \sum_{i,j=1}^{n} \langle e_i|\hat{A}|e_j\rangle \; |e_i\rangle \langle e_j| \,. \tag{2.43}$$

We define $A_{ij} := \langle e_i|\hat{A}|e_j\rangle$ and represent $\hat{A}$ in the basis $\{|e_i\rangle\}$ as a $n \times n$ *matrix*,

$$\hat{A} \Leftrightarrow \boldsymbol{A} = \begin{pmatrix} \langle e_1|\hat{A}|e_1\rangle & \langle e_1|\hat{A}|e_2\rangle & \dots & \langle e_1|\hat{A}|e_n\rangle \\ \langle e_2|\hat{A}|e_1\rangle & \langle e_2|\hat{A}|e_2\rangle & \dots & \langle e_2|\hat{A}|e_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle e_n|\hat{A}|e_1\rangle & \langle e_n|\hat{A}|e_2\rangle & \dots & \langle e_n|\hat{A}|e_n\rangle \end{pmatrix}. \tag{2.44}$$

The identity operator is represented by an *identity matrix*:

$$\hat{I} \Leftrightarrow \boldsymbol{I} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}. \tag{2.45}$$

A product of operators $\hat{A}\hat{B}$ is represented by a product of matrices $\boldsymbol{AB}$, with components:

$$(\boldsymbol{AB})_{ij} = \langle i|\hat{A}\hat{B}|j\rangle = \sum_{k=1}^{n} \langle i|\hat{A}|k\rangle \langle k|\hat{B}|j\rangle = \sum_{k=1}^{n} A_{ik}B_{kj}, \tag{2.46}$$

and the adjoint operator is represented by a conjugate transpose:

$$\left(\boldsymbol{A}^\dagger\right)_{ij} = A_{ji}^*. \tag{2.47}$$

To represent an orthogonal direct sum, we introduce a *block matrix representation*. Let $\mathcal{H} = \mathcal{K} \oplus \mathcal{K}'$, and $\hat{A} \in \mathcal{L}(\mathcal{K})$, $\hat{B} \in \mathcal{L}(\mathcal{K}')$. Then,

$$\boldsymbol{A} \oplus \boldsymbol{B} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{B} \end{pmatrix} := \begin{pmatrix} A_{11} & \dots & A_{1n} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ A_{1n} & \dots & A_{nn} & 0 & \dots & 0 \\ 0 & \dots & 0 & B_{11} & \dots & B_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & B_{1n} & \dots & B_{nn} \end{pmatrix}. \tag{2.48}$$

2.2.5 Normal Operators

Definition 2.30. An operator $\hat{N} \in \mathcal{L}(\mathcal{H})$ is said to be *normal* if

$$\hat{N}\,\hat{N}^\dagger = \hat{N}^\dagger\,\hat{N}. \tag{2.49}$$

We introduce here two classes of normal operators that are central in quantum mechanics: the *Hermitian operators* and the *unitary operators*.

Definition 2.31. A *Hermitian operator* $\hat{H}$ is an operator that is equal to its adjoint,

$$\hat{H} = \hat{H}^\dagger. \tag{2.50}$$

Hermitian operators are normal, since $\hat{H}\hat{H}^\dagger = \hat{H}^2 = \hat{H}^\dagger\hat{H}$. We have already encounted an example of Hermitian operator, the orthogonal projector (see Def. 2.29). Hermitian operators are represented by *Hermitian matrices*,

$$\hat{H} \Leftrightarrow \boldsymbol{H} = \begin{pmatrix} H_{11} & H_{12} & \dots & H_{1n} \\ H_{12}^* & H_{22} & \dots & H_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ H_{1n}^* & H_{2n}^* & \dots & H_{nn} \end{pmatrix}. \tag{2.51}$$

The Hermitian condition reads $\boldsymbol{H} = \boldsymbol{H}^\dagger$, or $H_{ij} = H_{ji}^*$. As a consequence, $H_{ii} \in \mathbb{R}$. When all elements of $\boldsymbol{H}$ are real, the Hermitian condition becomes $\boldsymbol{H} = \boldsymbol{H}^T$, and the matrix is called *symmetric*.

Theorem 2.32. *Any linear operator $\hat{A} \in \mathcal{L}(\mathcal{H})$ can be written as:*

$$\hat{A} = \hat{A}_R + \mathrm{i}\hat{A}_I, \tag{2.52}$$

where i *is the imaginary unit, and $\hat{A}_R$ and $\hat{A}_I$ are Hermitian operators. It holds:*

$$\hat{A} + \hat{A}^\dagger = 2\hat{A}_R, \tag{2.53}$$

$$\hat{A} - \hat{A}^\dagger = 2\mathrm{i}\hat{A}_I. \tag{2.54}$$

Definition 2.33. A Hermitian operator $\hat{H} \in \mathcal{L}(\mathcal{H})$ is said to be *positive-definite* if

$$\langle v|\hat{H}|v\rangle > 0, \qquad \forall\ |v\rangle \in \mathcal{H}\backslash\{0\}; \tag{2.55}$$

$\hat{H}$ is said to be *positive-semidefinite* if

$$\langle v|\hat{H}|v\rangle \geq 0, \qquad \forall\ |v\rangle \in \mathcal{H}. \tag{2.56}$$

The notions of *negative-definite* and *negative-semidefinite* operators are defined analogously.

If a matrix $\boldsymbol{H}$ represents a positive-definite (positive-semidefinite) operator $\hat{H}$, we say that $\boldsymbol{H}$ is a *positive-definite (positive-semidefinite) matrix. Negative-definite (negative-semidefinite) matrices* are defined analogously.

Theorem 2.34. *A Hermitian operator $\hat{H} \in \mathcal{L}(\mathcal{H})$ is positive-semidefinite if and only if there exists an operator $\hat{A} \in \mathcal{L}(\mathcal{H})$ such that:*

$$\hat{H} = \hat{A}^\dagger \hat{A}. \tag{2.57}$$

$\hat{H}$ is positive-definite if and only if this decomposition exists with $\hat{A}$ invertible.

Definition 2.35. An invertible linear operator $\hat{U}$ such that

$$\hat{U}^{-1} = \hat{U}^\dagger, \tag{2.58}$$

is said to be a *unitary operator*. Equivalently, we define the unitary operators as those operators satisfying

$$\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{I}. \tag{2.59}$$

Clearly, Eq. (2.59) implies that unitary operators are normal. Unitary operators satisfy a set of useful properties.

Theorem 2.36. *Unitary operators preserve the inner product between vectors they act on, i.e. given $|v'\rangle = \hat{U}\,|v\rangle$ and $|w'\rangle = \hat{U}\,|w\rangle$,*

$$\langle v'|w'\rangle = \langle v|\hat{U}^\dagger\,\hat{U}|w\rangle = \langle v|w\rangle\,. \tag{2.60}$$

Hence, they preserve the norm $\|v\| = \sqrt{\langle v|v\rangle}$.

Theorem 2.37. *The product of two unitary operators is a unitary operator.*

Since unitary operators preserve the inner product, if $\{|e_i\rangle\}$ is an orthonormal basis, then $\{|f_i\rangle\}$, with elements $|f_i\rangle = \hat{U}\,|e_i\rangle$, is also an orthonormal basis. The matrix representation of $\hat{U}$ in the basis $\{|e_j\rangle\}$, called a *unitary matrix*, reads

$$\hat{U} \Leftrightarrow \boldsymbol{U} = \begin{pmatrix} \langle e_1|\hat{U}|e_1\rangle & \langle e_1|\hat{U}|e_2\rangle & \dots & \langle e_1|\hat{U}|e_n\rangle \\ \langle e_2|\hat{U}|e_1\rangle & \langle e_2|\hat{U}|e_2\rangle & \dots & \langle e_2|\hat{U}|e_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle e_n|\hat{U}|e_1\rangle & \langle e_n|\hat{U}|e_2\rangle & \dots & \langle e_n|\hat{U}|e_n\rangle \end{pmatrix} = \begin{pmatrix} \langle e_1|f_1\rangle & \langle e_1|f_2\rangle & \dots & \langle e_1|f_n\rangle \\ \langle e_2|f_1\rangle & \langle e_2|f_2\rangle & \dots & \langle e_2|f_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle e_n|f_1\rangle & \langle e_n|f_2\rangle & \dots & \langle e_n|f_n\rangle \end{pmatrix}. \tag{2.61}$$

We note that $\langle e_i|f_j\rangle$ is the i-th component of $|f_j\rangle$ in the basis $\{|e_i\rangle\}$.

Theorem 2.38. *The columns of an $n \times n$ unitary matrix are the components of orthonormal vectors.*

On a real Hilbert space, the unitary condition becomes $\boldsymbol{U}^T\boldsymbol{U} = \boldsymbol{U}\boldsymbol{U}^T = \boldsymbol{I}$ and the matrix is said to be *orthogonal*.

Theorem 2.39. *Every unitary operator $\hat{U}$ can be written as:*

$$\hat{U} = e^{\mathrm{i}\hat{H}} := \sum_{j=1}^{\infty} \frac{\left(\mathrm{i}\hat{H}\right)^j}{j!}, \tag{2.62}$$

where $\hat{H}$ is a Hermitian operator.

2.2.6 Trace and Determinant

The components of a linear operator $\hat{A}$ in two orthonormal bases $\{|e_i\rangle\}$ and $\{|f_j\rangle\}$ are different. However, some properties of $\hat{A}$ do not change with the chosen basis and are therefore said *invariants of* $\hat{A}$. Here we present two important invariants, the *trace* and the *determinant*.

Definition 2.40. For any operator $\hat{A} \in \mathcal{H}$, we define as *trace* the sum of its diagonal elements in a certain basis $|e_i\rangle$:

$$\mathrm{Tr}(\hat{A}) := \sum_{i=1}^{n} \langle e_i|\hat{A}|e_i\rangle \,. \tag{2.63}$$

It holds that the trace is invariant under change of basis,

$$\mathrm{Tr}(\hat{A}) = \sum_{i=1}^{n} \langle e_i|\hat{A}|e_i\rangle = \sum_{j=1}^{n} \langle f_j|\hat{A}|f_j\rangle \,. \tag{2.64}$$

The trace is linear,

$$\mathrm{Tr}(\alpha\hat{A} + \beta\hat{B}) = \alpha\mathrm{Tr}\hat{A} + \beta\mathrm{Tr}\hat{B}; \tag{2.65}$$

Moreover, the trace of a product of operators is invariant under *cyclic permutation* of the operators, i.e.

$$\mathrm{Tr}(\hat{A}\hat{B}\hat{C}) = \mathrm{Tr}(\hat{B}\hat{C}\hat{A}) = \mathrm{Tr}(\hat{C}\hat{A}\hat{B}), \tag{2.66}$$

for any $\hat{A}, \hat{B}, \hat{C} \in \mathcal{H}$. However, the trace is not, in general, invariant under non cyclic permutations:

$$\mathrm{Tr}(\hat{A}\hat{B}\hat{C}) \neq \mathrm{Tr}(\hat{B}\hat{A}\hat{C}). \tag{2.67}$$

The cyclic property implies that:

$$\mathrm{Tr}(\hat{U}^\dagger\,\hat{A}\,\hat{U}) = \mathrm{Tr}(\hat{U}\,\hat{U}^\dagger\,\hat{A}) = \mathrm{Tr}(\hat{A}), \tag{2.68}$$

for any unitary operator $\hat{U}$.

Definition 2.41. For any linear operator $\hat{A} \in \mathcal{L}(\mathcal{H})$, we recursively define the *determinant* of $\hat{A}$ as the function:

$$\det(\hat{A}) = \det \boldsymbol{A} := \sum_{j=1}^{n} A_{ij} \det(\boldsymbol{A}_{n-1}^{(i,j)}), \tag{2.69}$$

where $\boldsymbol{A}_{n-1}^{(i,j)}$ is the $(n-1)\times(n-1)$ submatrix obtained by removing the i-th row and the j-th column of $\boldsymbol{A}$, and with the definition:

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc, \qquad \forall\, a, b, c, d \in \mathbb{C}. \tag{2.70}$$

It holds that the determinant is invariant under change of basis.

The determinant is not a linear function. If $\mathcal{H}$ is a n-dimensional Hilbert space, it holds:

$$\det(\hat{A} + \hat{B}) \neq \det\hat{A} + \det\hat{B}, \qquad \text{for general } \hat{A}, \hat{B} \in \mathcal{L}(\mathcal{H}); \tag{2.71}$$

$$\det(\alpha\hat{A}) = \alpha^n \det\hat{A}, \qquad \text{for all } \hat{A} \in \mathcal{L}(\mathcal{H}) \text{ and } \alpha \in \mathbb{C}. \tag{2.72}$$

The determinant of a product of operators is equal to the product of the determinants:

$$\det(\hat{A}\hat{B}) = \det\hat{A}\det\hat{B}. \tag{2.73}$$

This implies that:

$$\det(\hat{U}^\dagger\,\hat{A}\,\hat{U}) = \det\hat{U}^\dagger\,\det\hat{A}\,\det\hat{U} = \det(\hat{U}^\dagger\,\hat{U})\det\hat{A} = \det\hat{A}. \tag{2.74}$$

2.2.7 Eigenvalues and Eigenvectors

Definition 2.42. Let $\hat{A} \in \mathcal{L}(\mathcal{H})$ be a linear operator on a Hilbert space $\mathcal{H}$. If $\lambda \in \mathbb{C}$ and $|\lambda\rangle \in \mathcal{H}\backslash\{0\}$ satisfy

$$\hat{A}\,|\lambda\rangle = \lambda\,|\lambda\rangle\,, \tag{2.75}$$

then we say that λ is an *eigenvalue* of $\hat{A}$ and that $|\lambda\rangle$ is an *eigenvector* (or *eigenket*) of $\hat{A}$ *belonging to the eigenvalue* λ.

Clearly, if $\hat{A}\,|\lambda\rangle = \lambda\,|\lambda\rangle$, then it holds $\hat{A}(\alpha\,|\lambda\rangle) = \lambda(\alpha\,|\lambda\rangle)$, for any $\alpha \in \mathbb{C}$. We usually remove this degree of freedom by normalising the norm of the eigenvectors to 1. If we consider a function $f(\hat{A})$ (see Def. 2.25), it holds:

$$f(\hat{A})\,|\lambda\rangle = f(\lambda)\,|\lambda\rangle\,. \tag{2.76}$$

Theorem 2.43. *The eigenvalues* $\{\lambda_i\}$ *of an operator* $\hat{A} \in \mathcal{L}(\mathcal{H})$ *are the solutions of the* characteristic equation*:*

$$\det\left(\hat{A} - \lambda\,\hat{I}\right) = 0. \tag{2.77}$$

If the Hilbert space $\mathcal{H}$ *is* n*-dimensional, the characteristic equation of* $\hat{A}$ *has* n *solutions, which are not necessarily distinct.*

An eigenvalue is said to be *degenerate* if it is a multiple root of the characteristic equation. From now on, we are going to only consider the nondegenerate case.

Theorem 2.44. *If* $\hat{A} \in \mathcal{L}(\mathcal{H})$ *has* n *distinct eigenvalues* $\{\lambda_i\}$*, then to each* λ_i *belongs a single eigenvector* $|\lambda_i\rangle$*, except for multiplicative constants. Moreover, if the Hilbert space* $\mathcal{H}$ *is* n*-dimensional, a set of* n *eigenvectors* $\{|\lambda_i\rangle\}$ *forms a basis for* $\mathcal{H}$*.*

Theorem 2.45 (Spectral Theorem)**.** *An operator* $\hat{N} \in \mathcal{L}(\mathcal{H})$ *is normal if and only if it admits an orthonormal set of eigenvectors* $\{|\lambda_i\rangle\}$ *that forms a basis for* $\mathcal{H}$*. The matrix representation of* $\hat{N}$ *in this basis is diagonal, with components given by the eigenvalues of* $\hat{N}$*:*

$$\langle\lambda_i|\hat{N}|\lambda_j\rangle = \lambda_i\,\delta_{ij}, \tag{2.78}$$

where δ_{ij} *is the Kronecker's delta. As a consequence, if* $\boldsymbol{N}$ *is the matrix representaton of* $\hat{N}$ *in any basis of* $\mathcal{H}$*, there exists a unitary matrix* $\boldsymbol{U}$ *that* diagonalises $\boldsymbol{N}$*, i.e.*

$$\boldsymbol{U}^\dagger\,\boldsymbol{N}\boldsymbol{U} = \boldsymbol{N}_D := \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}. \tag{2.79}$$

Every normal operator $\hat{N}$ can be written in terms of its eigenvalues and eigenvectors (*spectral representation*):

$$\hat{N} = \sum_i \lambda_i\;|\lambda_i\rangle\,\langle\lambda_i|\,. \tag{2.80}$$

The invariance of the trace and the determinant under change of basis implies that

$$\mathrm{Tr}\hat{A} = \sum_{i=1}^{n} \lambda_i, \qquad \det\hat{A} = \prod_{i=1}^{n} \lambda_i. \tag{2.81}$$

We add some meaningful properties for the eigenvalues of normal operators.

1. If for a normal operator $\hat{N} \in \mathcal{L}(\mathcal{H})$, $\hat{N}\,|\lambda_i\rangle = \lambda_i\,|\lambda_i\rangle$, then $\hat{N}^\dagger\,|\lambda_i\rangle = \lambda_i^*\,|\lambda_i\rangle$;
2. All the eigenvalues of a Hermitian operator are real, $\lambda_i \in \mathbb{R}$;
3. All the eigenvalues of a unitary operator are unimodular, $|\lambda_i| = 1$;
4. All the eigenvalues of a positive (negative)-definite matrix are positive (negative);
5. All the eigenvalues of a positive (negative)-semidefinite matrix are nonnegative (nonpositive).

Moreover, by using Eqs. (2.59) and (2.74), we can prove that any linear operator $\hat{A}$ has the same eigenvalues of $\hat{U}^\dagger\,\hat{A}\,\hat{U}$, for any unitary operator $\hat{U}$, i.e.

$$\det\left(\hat{U}^\dagger\,\hat{A}\,\hat{U} - \lambda\,\hat{I}\right) = \det\left(\hat{U}^\dagger\,(\hat{A} - \lambda\,\hat{I})\,\hat{U}\right) = \det(\hat{A} - \lambda\,\hat{I}). \tag{2.82}$$

Theorem 2.46. *Two normal operators $\hat{N}, \hat{M} \in \mathcal{L}(\mathcal{H})$ commute if and only if they are simoultaneosly diagonalisable, i.e. there exists an orthonormal basis $\{|\lambda_i\rangle\}$ such that both $\hat{N}$ and $\hat{M}$ are diagonal with respect to it. Therefore, they have spectral representations $\hat{N} = \sum_i\, n_i\,|\lambda_i\rangle\,\langle\lambda_i|$ and $\hat{M} = \sum_i\, m_i\,|\lambda_i\rangle\,\langle\lambda_i|$ for some $n_i, m_i \in \mathbb{C}$.*

2.3 Tensor Products

Definition 2.47. A *tensor product* of two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ consists of a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and a function $\otimes : \mathcal{H}_A \times \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$ such that:

1. $(\alpha\,|v_A\rangle) \otimes |v_B\rangle = |v_A\rangle \otimes (\alpha\,|v_B\rangle) = \alpha(|v_A\rangle \otimes |v_B\rangle)$;
2. $(|v_A\rangle + |w_A\rangle) \otimes |v_B\rangle = |v_A\rangle \otimes |v_B\rangle + |w_A\rangle \otimes |v_B\rangle$;
3. $|v_A\rangle \otimes (|v_B\rangle + |w_B\rangle) = |v_A\rangle \otimes |v_B\rangle + |v_A\rangle \otimes |w_B\rangle$,

for any $|v_A\rangle, |w_A\rangle \in \mathcal{H}_A$, $|v_B\rangle, |w_B\rangle \in \mathcal{H}_B$, and $\alpha \in \mathbb{C}$. The space $\mathcal{H}_A \otimes \mathcal{H}_B$ is required to be *minimal*, in the sense that every $|v_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ must be a unique linear combination, i.e.

$$|v_{AB}\rangle = \sum_{i,j=1}^{n} v_{ij}\;|v_i^{(A)}\rangle \otimes |v_j^{(B)}\rangle\,, \tag{2.83}$$

for $|v_i^{(A)}\rangle \in \mathcal{H}_A$, $|v_j^{(B)}\rangle \in \mathcal{H}_B$ and $v_{ij} \in \mathbb{C}$.

Definition 2.48. Let $|v_{AB}\rangle = \sum_{i,j=1}^{n} v_{ij}\;|v_i^{(A)}\rangle \otimes |v_j^{(B)}\rangle$ and $|w_{AB}\rangle = \sum_{i,j=1}^{n} w_{ij}\;|w_i^{(A)}\rangle \otimes |w_j^{(B)}\rangle$ be two vectors in $\mathcal{H}_A \otimes \mathcal{H}_B$, with $v_{ij}, w_{ij} \in \mathbb{C}$, $|v_i^{(A)}\rangle, |w_i^{(A)}\rangle \in \mathcal{H}_A$, $|v_j^{(B)}\rangle, |w_j^{(B)}\rangle \in \mathcal{H}_B$. The inner product $\langle v_{AB}|w_{AB}\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined as:

$$\langle v_{AB}|w_{AB}\rangle := \sum_{i,i',j,j'=1}^{n} v_{ij}^*\,w_{i'j'}\;\langle v_i^{(A)}|w_{i'}^{(A)}\rangle\,\langle v_j^{(B)}|w_{j'}^{(B)}\rangle\,. \tag{2.84}$$

Theorem 2.49. *Let n_A and n_B be the dimensions of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. It holds that the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is $(n_A n_B)$-dimensional. Moreover, if $\{|a_i\rangle\}$ $(i = 1, 2, \ldots, n_A)$ and $\{|b_j\rangle\}$ $(j = 1, 2, \ldots, n_B)$ are orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, then $\{|a_i\rangle \otimes |b_j\rangle\}$ is an orthonormal basis of $\mathcal{H}_A \otimes \mathcal{H}_B$.*

Consider now two linear operators, $\hat{A} \in \mathcal{L}(\mathcal{H}_A)$ and $\hat{B} \in \mathcal{L}(\mathcal{H}_B)$. We define $\hat{A} \otimes \hat{B}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ as:

$$(\hat{A} \otimes \hat{B})(|v_A\rangle \otimes |v_B\rangle) := (\hat{A}\,|v_A\rangle) \otimes (\hat{B}\,|v_B\rangle), \tag{2.85}$$

for all $|v_A\rangle \in \mathcal{H}_A$ and $|v_B\rangle \in H_B$.

Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be the matrix representations of $\hat{A}$ and $\hat{B}$ in some basis of $\mathcal{H}_A$ and $\mathcal{H}_B$. The matrix representation of $\hat{A} \otimes \hat{B}$ is given by the *Kronecker product* of $\boldsymbol{A}$ and $\boldsymbol{B}$,

$$\hat{A} \otimes \hat{B} \;\Leftrightarrow\; \boldsymbol{A} \otimes \boldsymbol{B} := \begin{pmatrix} A_{11}\boldsymbol{B} & A_{12}\boldsymbol{B} & \cdots & A_{1n}\boldsymbol{B} \\ A_{12}\boldsymbol{B} & A_{22}\boldsymbol{B} & \cdots & A_{2n}\boldsymbol{B} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1}\boldsymbol{B} & A_{n2}\boldsymbol{B} & \cdots & A_{nn}\boldsymbol{B} \end{pmatrix}, \tag{2.86}$$

where $A_{ij}\boldsymbol{B}$ is the matrix:

$$A_{ij}\boldsymbol{B} = \begin{pmatrix} A_{ij}B_{11} & A_{ij}B_{12} & \cdots & A_{ij}B_{1n} \\ A_{ij}B_{21} & A_{ij}B_{22} & \cdots & A_{ij}B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{ij}B_{n1} & A_{ij}B_{n2} & \cdots & A_{ij}B_{nn} \end{pmatrix}. \tag{2.87}$$

If we consider a single column or row in Eq. (2.86), the Kronecker product provides a formula for the components of $|v_A\rangle \otimes |v_B\rangle$ or $\langle v_A| \otimes \langle v_B|$, respectively.

When we consider the tensor product of N Hilbert spaces $\mathcal{H}_i$, we use the notation:

$$\bigotimes_{i=1}^{N} \mathcal{H}_i := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N. \tag{2.88}$$

Analogously, we use the symbol $\bigotimes_{i=1}^{N}$ to compactly write the tensor products of many vectors $|v_i\rangle$ and operators $\hat{A}_i$.

In general, there are operators $\hat{X}_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ that cannot be written as $\hat{A} \otimes \hat{B}$, for any $\hat{A} \in \mathcal{L}(\mathcal{H}_A)$ and $\hat{B} \in \mathcal{L}(\mathcal{H}_B)$. In this case, the *partial trace* provides a partial description of the action of $\hat{X}_{AB}$ over either $\mathcal{H}_A$ or $\mathcal{H}_B$.

Definition 2.50. The *partial trace* over $\mathcal{H}_B$ is the operation $\mathrm{Tr}_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A$ defined on any $\hat{X}_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ as follows:

$$\mathrm{Tr}_B\, \hat{X}_{AB} := \sum_i \langle b_i|\, X_{AB}\, |b_i\rangle\,, \tag{2.89}$$

where $\{|b_i\rangle\}$ is any orthonormal basis for $\mathcal{H}_B$. The partial trace over $\mathcal{H}_A$ is analogously defined.

In the jargon of quantum information theory, the action of taking the partial trace over $\mathcal{H}_B$ is usually referred to as "tracing out $\mathcal{H}_B$". The result of tracing out $\mathcal{H}_B$ is an operator on $\mathcal{H}_A$, and viceversa. In particular, for any operator in the form of $\hat{A} \otimes \hat{B}$, it holds:

$$\mathrm{Tr}_B\left(\hat{A} \otimes \hat{B}\right) = \mathrm{Tr}(\hat{B})\,\hat{A}, \qquad \mathrm{Tr}_A\left(\hat{A} \otimes \hat{B}\right) = \mathrm{Tr}(\hat{A})\,\hat{B}. \tag{2.90}$$

The usual trace on $\mathcal{H}_A \otimes \mathcal{H}_B$ is the composition of the partial traces over $\mathcal{H}_A$ and $\mathcal{H}_B$, in any order, i.e.

$$\mathrm{Tr}(\hat{X}_{AB}) = \mathrm{Tr}_A(\mathrm{Tr}_B(\hat{X}_{AB})) = \mathrm{Tr}_B(\mathrm{Tr}_A(\hat{X}_{AB})), \tag{2.91}$$

for any $\hat{X}_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

2.4 Infinite-dimensional Hilbert Spaces

We here extend some of the previously introduced concepts to infinite dimensions, without claiming to be exhaustive. In particular, we choose to partially disregard the high formality associated with infinite-dimensional linear algebra. We refer to specialised textbooks for a more complete introduction to the topic.

We start our discussion by introducing definitions that hold for any dimension.

Definition 2.51. Let $\mathcal{M}$ be a metric space (see Def. 2.8) equipped with a distance d. A sequence of vectors $\{|v_1\rangle, |v_2\rangle, \dots\}$ is said to be a *Cauchy sequence* in (M, d) if for every $\epsilon > 0$ there exists a positive integer $N \in \mathbb{N}$ such that

$$d(v_n, v_m) < \epsilon, \qquad \forall\, n, m > N. \tag{2.92}$$

Definition 2.52. A metric space $\mathcal{M}$ with distance d is said to be *complete* with respect to d if every Cauchy sequence in (M, d) converges to a vector in $\mathcal{M}$ for $n \to \infty$, i.e. if for any Cauchy sequence $\{|v_1\rangle, |v_2\rangle, \dots\}$ in $(\mathcal{M}, d)$, there exists some $|v\rangle \in \mathcal{M}$ such that:

$$\lim_{n\to\infty} d(v_n, v) = 0. \tag{2.93}$$

Definition 2.53. A *Hilbert space* $\mathcal{H}$ is a vector space that is equipped with an inner product and is *complete* with respect to the distance induced by the inner product (see Theorem 2.9).

The completeness of $\mathcal{H}$ ensures that the norm $\|v\|$ of every vector $|v\rangle \in \mathcal{H}$ is finite. It can be proved that every finite-dimensional vector space equipped with an inner product is a Hilbert space, thus justifying our use of Def. 2.6. We now focus on infinite-dimensional spaces.

Definition 2.54. Let $\mathcal{H}$ be an infinite-dimensional Hilbert space. A set of orthonormal vectors $\{|e_i\rangle \in \mathcal{H}\}$ ($\langle e_i|e_j\rangle = \delta_{ij}$, $\||e_i\rangle\| = 1$ for all i, j) is said to be a *complete orthonormal system* for $\mathcal{H}$ if the following equivalent conditions hold:

1. For any $|v\rangle \in \mathcal{H}$,
$$|v\rangle = \sum_{i=1}^{\infty} \langle e_i|v\rangle \; |e_i\rangle\,; \tag{2.94}$$
2. If a vector $|v\rangle \in \mathcal{H}$ satifies $\langle e_i|v\rangle = 0$ for all the vectors $|e_i\rangle$ of the system, then $|v\rangle = 0$.

Complete systems are the natural counterpart to the orthonormal bases in finite-dimensional spaces. Note that Eq. (2.94) implies the completeness relation $\sum_i |e_i\rangle \langle e_i| = \hat{I}$, where $\hat{I}$ is the identity operator on $\mathcal{H}$.

Theorem 2.55. *A complete system $\{|e_i\rangle\}$ of a Hilbert space $\mathcal{H}$ defines an isometry between $\mathcal{H}$ and the space $L^2(\mathbb{R})$ of* square-integrable functions*, i.e. the space of functions $f : \mathbb{R} \to \mathbb{C}$ such that $\int_{\mathbb{R}} |f(x)|^2 < \infty$. Namely, for any two vectors $|f\rangle, |g\rangle \in \mathcal{H}$ there exist functions $f, g \in L^2(\mathbb{R})$ such that*

$$\langle f|g\rangle = \int_{\mathbb{R}} f^*(x)g(x)dx, \qquad \|f\|^2 = \int_{\mathbb{R}} |f(x)|^2 dx. \tag{2.95}$$

So far we have analysed complete systems composed of an infinite, but discrete, number of elements. In quantum mechanics, one may also consider complete systems with continuous elements. Let us define a complete system $\{|x\rangle\}$, with $x \in \mathbb{R}$. The completeness and orthogonality conditions read in this case:

$$\int_{\mathbb{R}} |x\rangle \langle x| = \hat{I}, \qquad \langle x|x'\rangle = \delta(x - x'), \tag{2.96}$$

where $\delta(x - x')$ is the *Dirac delta* function, which is a functional such that:

$$\int_{\mathbb{R}} f(x)\, \delta(x - x')\, dx = f(x'), \qquad \forall\, f \in L^2(\mathbb{R}). \tag{2.97}$$

The Dirac delta is not a function in $L^2(\mathbb{R})$ and thus the states $|x\rangle$ are not properly normalised states in $\mathcal{H}$. However, since the dawn of quantum mechanics [Dir30; Neu32], the space $L^2(\mathbb{R})$ has been enlarged to comprehend the Dirac delta and those functions that are "normalised" to the Dirac delta.

Definition 2.56 (Position operator)**.** The *position operator* $\hat{x}$ (also denoted by $\hat{q}$) is the operator that transforms every vector $|g\rangle \in \mathcal{H}$ into a vector $|xg\rangle \in \mathcal{H}$ such that, in the basis $\{|x\rangle\}$, it holds:

$$\langle f|xg\rangle = \langle f|\hat{x}|g\rangle := \int_{\mathbb{R}} f^*(x)xg(x)dx, \tag{2.98}$$

for every $|g\rangle \in \mathcal{H}$.

The operator $\hat{x}$ is straightforwardly Hermitian ($\hat{x} = \hat{x}^\dagger$), since $\langle f|xg\rangle = \langle xf|g\rangle$.

Theorem 2.57. *The eigenvalues of $\hat{x}$ are the real numbers $x \in \mathbb{R}$ and the corresponding eigenvectors are the elements of the complete system $\{|x\rangle\}$. The components of $\hat{x}$ in the basis of its eigenvectors $\{|x\rangle\}$ reads*

$$\langle x'|\hat{x}|x\rangle = x\delta(x' - x). \tag{2.99}$$

Definition 2.58 (Momentum operator)**.** The *momentum operator* $\hat{p}$ is the operator that transforms every vector $|g\rangle \in \mathcal{H}$ into a vector $-\mathrm{i}\,|dg/dx\rangle \in \mathcal{H}$ such that, in the basis $\{|x\rangle\}$, it holds:

$$-\,\mathrm{i}\,\langle f|dg/dx\rangle = \langle f|\hat{p}|g\rangle := \int_{\mathbb{R}} f^*(x)(-\mathrm{i})\frac{dg(x)}{dx}\, dx, \tag{2.100}$$

for every $|f\rangle \in \mathcal{H}$.

The components of $\hat{p}$ in the $|x\rangle$ basis read:

$$\langle x'|\hat{p}|x\rangle = -\mathrm{i}\delta(x' - x)\frac{d}{dx}. \tag{2.101}$$

By performing an integration by parts and using the property $\lim_{x\to\pm\infty} f(x) = 0$, which holds for any $f \in L^2(\mathbb{R})$, we prove that the momentum operator is Hermitian:

$$\begin{aligned}\langle f| \left(\hat{p}\,|g\rangle\right) &= \int_{\mathbb{R}} f^*(x) \left(-\mathrm{i}\frac{dg(x)}{dx}\right) dx = -\mathrm{i}[f^*(x)g(x)|_{-\infty}^{\infty} + \mathrm{i}\int_{\mathbb{R}} \frac{df^*(x)}{dx}\, g(x)\, dx \\ &= \int_{\mathbb{R}} \left(-\mathrm{i}\frac{df(x)}{dx}\right)^* g(x)\, dx = \left(\hat{p}\,|f\rangle\right)^\dagger |g\rangle\,.\end{aligned} \tag{2.102}$$

Theorem 2.59. *The eigenvalues of $\hat{p}$ are the real numbers $p \in \mathbb{R}$ and the corresponding normalised eigenvectors $|p\rangle$, with*

$$\langle x|p\rangle = \frac{1}{\sqrt{2\pi}}\, e^{\mathrm{i}\,kx}, \tag{2.103}$$

form a complete orthonormal system over $\mathcal{H}$ ($\langle p'|p\rangle = \delta(p'-p)$ and $\int_{\mathbb{R}} |p\rangle\langle p|\, dp = \hat{I}$). The components of $\hat{p}$ in the basis of its eigenvectors $\{|p\rangle\}$ are $\langle p'|\hat{p}|p\rangle = p\,\delta(p'-p)$.

One can also compute the components of $\hat{x}$ and $\hat{p}$ in each other spectral basis, i.e.

$$\langle p'|\hat{x}|p\rangle = \mathrm{i}\,\delta(p'-p), \qquad \langle x'|\hat{p}|x\rangle = \mathrm{i}\delta(x'-x). \tag{2.104}$$

Operators that are related as in Eq. 2.104 are said to be *conjugate* to each other. In particular, the operators $\hat{x}$ and $\hat{p}$ are called the *canonical conjugate operators*.

Theorem 2.60. *The canonical conjugate operators $\hat{x}$ and $\hat{p}$ satisfy the* canonical commutation relation *(CCR):*

$$[\hat{x}, \hat{p}] = \mathrm{i}\hat{I}. \tag{2.105}$$

2.5 Hamming Space

So far, we have always considered vector spaces over the scalar field $\mathbb{C}$. Here we introduce the *Galois field of order* 2.

Definition 2.61. The *Galois field of order* 2, denoted by $\mathbb{F}_2$, is a set of two elements $\{0, 1\}$, together with two binary operations:

1. $+_2 : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$, called the *addition modulus two*, such that:

$$0 +_2 0 = 0, \quad 0 +_2 1 = 1, \quad 1 +_2 0 = 1, \quad 1 +_2 1 = 0; \tag{2.106}$$

2. $\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$, called the *multiplication modulus two* (which in this set is equal to the standard multiplication), such that:

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \tag{2.107}$$

Therefore, the two elements 0 and 1 are the additive and multiplicative identity of the field, respectively. Moreover, for any $x \in \mathbb{F}_2$:

$$x +_2 x = 0, \qquad x^2 = x. \tag{2.108}$$

In information theory, the elements of $\mathbb{F}_2$ are called *bits*, short for **bi**nary digi**ts**.

Definition 2.62. The space $\mathbb{F}_2^n := \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$ (n times) is a vector space over the field $\mathbb{F}_2$ and is called *Hamming space*. The vector addition is defined as:

$$\boldsymbol{u} + \boldsymbol{v} := (u_1 +_2 v_1, u_2 +_2 v_2, \ldots, u_n +_2 v_n), \tag{2.109}$$

and the scalar multiplication as:

$$\alpha \boldsymbol{v} := (\alpha v_1, \alpha v_2, \ldots, \alpha v_n). \tag{2.110}$$

The vectors in $\mathbb{F}_2^n$ are called *(digital) strings*. The *cardinality* of $\mathbb{F}_2^n$, i.e. the number of strings in $\mathbb{F}_2^n$, is 2^n. In information theory, the set $\mathbb{F}_2^n$ can be also improperly referred to as $\{0,1\}^n$.

There is no proper inner product in $\mathbb{F}_2^n$, but a norm and a distance can be still defined.

Definition 2.63. The *Hamming weight* of a string $\boldsymbol{v} \in \mathbb{F}_2^n$ is the function $h : \mathbb{F}_2^n \to \mathbb{N}_0$ that counts the number of ones in $\boldsymbol{v}$. The *Hamming distance* d of two string $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^n$ is defined as the Hamming weigth of $\boldsymbol{u} + \boldsymbol{v}$, i.e.

$$d(\boldsymbol{u}, \boldsymbol{v}) = h(\boldsymbol{u} + \boldsymbol{v}). \tag{2.111}$$

Consider the Hamming space of a single bit, $\mathbb{F}_2$, with elements x. We can define only two operators on this space

1. The identity $\hat{I}$,
$$\hat{I}x = x; \tag{2.112}$$
2. The *bit flip* $\hat{X}$,
$$\hat{X}x = x +_2 1. \tag{2.113}$$

For n bits, all operators are in the form $\hat{A}_1 \oplus \hat{A}_2 \oplus \cdots \oplus \hat{A}_n$, where $\hat{A}_i$ are single-bit operators (i.e. $\hat{A}_i = \hat{I}, \hat{X}$).

Definition 2.64. The *concatenation* of two strings, $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_2^n$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_m) \in \mathbb{F}_2^m$, is the operation $\| : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^{n+m}$ that generates:

$$\boldsymbol{u} \| \boldsymbol{v} = (u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_m). \tag{2.114}$$

3

Quantum Information with Discrete Variables

In this chapter, we introduce quantum mechanics from the point of view of *quantum information theory*, which is the theory that uses quantum mechanics to study, transmit and process information. Here we focus to finite-dimensional (also called *discrete-variable*) systems, postponing the discussion about infinite-dimensional (*continuous-variable*) systems to later chapters. The postulates of quantum mechanics are introduced for closed quantum systems, with emphasis on the two-dimensional ones (*qubits*). Then we broaden our view, considering open quantum systems and studying their dynamics in terms of *density operators* and *quantum channels*. Finally, we introduce specific elements of quantum information theory that are used in the remainder of this thesis. The content of this chapter is mostly inspired from [NC10; MW20; KLM07].

3.1 Quantum Mechanics of Closed Systems

3.1.1 State Space

Postulate 1. *Any isolated quantum system is associated with a complex Hilbert space $\mathcal{H}$, known as* the space state*. Quantum states of the system are completely described by unit vectors $|\psi\rangle \in \mathcal{H}$, with the assumption that $|\psi\rangle$ and $e^{\mathrm{i}\theta}\ |\psi\rangle$ describe the same state, for any $\theta \in \mathbb{R}$.*

Formally speaking, we should say that the state space is a *projective Hilbert space*, defined as the set of all *projective rays* in a Hilbert space $\mathcal{H}$, i.e. all classes of $|\psi\rangle \in \mathcal{H}$, $|\psi\rangle \neq 0$, for the relation:

$$|\psi\rangle \sim |\psi'\rangle \qquad \text{if and only if} \quad |\psi\rangle = \alpha\,|\psi'\rangle\,, \text{ with } \alpha \in \mathbb{C}\backslash\{0\}. \tag{3.1}$$

However, operational definitions of the state space and vector, such as that in Postulate 1, are generally more preferred by physicists than the formal definition.

We illustrate the effects of this postulate with one of the simplest, and yet most important, quantum systems: the *qubit* (short for **qu**antum **bit**).

A qubit is a quantum state $|\psi\rangle$ in a two-dimensional complex Hilbert space $\mathcal{H}_2$. It is the quantum state that represents two-level quantum properties, such as the electron spin (*spin up* and *spin down*) or the photon polarisation (*right* and *left* or *horizontal* and *vertical*).

Qubits are the quantum counterpart to the classical bits (see Sec. 2.5). For this reason, we label as $\{|0\rangle, |1\rangle\}$ the standard basis of $\mathcal{H}_2$, called the *computational basis*, with

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{3.2}$$

The main difference between bits and qubits is that a bit state can be either 0 or 1, whereas a qubit state $|\psi\rangle$ can be any superposition of $|0\rangle$ and $|1\rangle$, i.e.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{3.3}$$

where $\alpha, \beta \in \mathbb{C}$, with the normalisation condition $|a|^2 + |b|^2 = 1$ (it follows from $\langle\psi|\psi\rangle = 1$). Quantum states that differs by a global phase factor are physically equivalent, so we can consider an alternative parameterisation for Eq. (3.3):

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)\,|0\rangle + e^{\mathrm{i}\phi}\sin\left(\frac{\theta}{2}\right)\,|1\rangle\,, \tag{3.4}$$

where $\theta \in [0, \pi]$, $\phi \in [0, 2\pi]$. The angles (θ, ϕ) describe points on the surface of a three-dimensional sphere of unit radius, called the *Bloch sphere*.

3.1.2 Quantum Measurements

Postulate 2. *Quantum measurements are described by a set $\{\hat{M}_m\}$ of* measurement operators *on the state space $\mathcal{H}$, with m labelling a possible outcome of the measurement. The measurement operators must satisfy the* completeness relation

$$\sum_m \hat{M}_m^\dagger\,\hat{M}_m = \hat{I}, \tag{3.5}$$

where $\hat{I}$ is the identity operator on $\mathcal{H}$. If $|\psi\rangle$ is the state of the system immediately prior to the measurement, then the probability of obtaining the outcome m is given by:

$$p_{|\psi\rangle}(m) = \langle\psi|\hat{M}_m^\dagger\,\hat{M}_m|\psi\rangle\,, \tag{3.6}$$

and the measurement transforms $|\psi\rangle$ into:

$$|\psi\rangle \mapsto \frac{1}{\sqrt{p_{|\psi\rangle}(m)}}\,\hat{M}_m\,|\psi\rangle\,. \tag{3.7}$$

The measurement process is therefore a random process: the measurement outcomes m form a classical *random variable*, i.e. a variable taking values over a set $\mathcal{M} = \{m\}$, according to the probability distribution $p_{|\psi\rangle}(m) = p_{|\psi\rangle}(M = m)$ given by Eq. (3.6).

Projective measurements

A projective measurement is described by a Hermitian operator $\hat{M}$ on the state space $\mathcal{H}$, called an *observable*. The spectral decomposition of $\hat{M}$ (see Eq. (2.80)) reads:

$$\hat{M} = \sum_m m\,\hat{\Pi}_m, \tag{3.8}$$

where $m \in \mathbb{R}$ and $\hat{\Pi}_m$ is the orthogonal projector onto the eigenspace of $\hat{M}$ belonging to the eigenvalue m.

If the eigenvalues of $\hat{M}$ are non-degenerate, the corresponding measurement is also called a *von Neumann measurement*. In this case $\hat{\Pi}_m = |m\rangle\langle m|$, where $|m\rangle$ is the eigenstate belonging to the eigenvalue m. The outcome of a von Neumann measurement on a quantum state $|\psi\rangle \in \mathcal{H}$ is given by the eigenvalues m of the observable $\hat{A}$, with probability

$$p_\psi(m) = \langle\psi|\hat{\Pi}_m|\psi\rangle = |\langle\psi|m\rangle|^2. \tag{3.9}$$

As a consequence of the measurement, the state of the system changes to:

$$|\psi\rangle \mapsto \frac{\hat{\Pi}_m\,|\psi\rangle}{\sqrt{p_{|\psi\rangle}(m)}} = \frac{\langle\psi|m\rangle}{|\langle\psi|m\rangle|}\,|m\rangle \sim |m\rangle\,. \tag{3.10}$$

Hence, $|\psi\rangle$ is projected onto the eigenspace of $\hat{A}$ that corresponds to the measurement outcome m. In quantum information jargon, one can "measure in a basis $\{|m\rangle\}$" or "measure $\hat{M}$". Both sentences mean to make a projective measurement on a quantum state $|\psi\rangle$ using the operator $\hat{M} = \sum_m m\,|m\rangle\langle m|$.

Projective measurements are particularly useful to compute the expectation value of the measurement, $E_{|\psi\rangle}(\hat{M})$, since:

$$E_{|\psi\rangle}(\hat{M}) = \sum_m m\,p_{|\psi\rangle}(m) = \sum_m m\,\langle\psi|\hat{\Pi}_m|\psi\rangle = \langle\psi|\hat{M}|\psi\rangle\,. \tag{3.11}$$

We denote $E_{|\psi\rangle}(\hat{M})$ by $\langle\hat{M}\rangle := \langle\psi|\hat{M}|\psi\rangle$, and say that $\langle\hat{M}\rangle$ is the average value of the observable $\hat{M}$. It follows that the variance associated with the measurement of $\hat{M}$ is

$$\left[\Delta(\hat{M})\right]^2 = \langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2\,. \tag{3.12}$$

This leads to one of the most important results of quantum mechanics, which states the impossibility of precisely measuring two non-commuting observable with absolute precision. A proof of the following theorem is given in [NC10].

Theorem 3.1 (Heisenberg uncertainty principle)**.** *For any two observable $\hat{A}, \hat{B}$ over a state space $\mathcal{H}$, it holds:*

$$\Delta(\hat{A})\Delta(\hat{B}) \geq \frac{|\langle\psi|[\hat{A},\hat{B}]|\psi\rangle|}{2}, \tag{3.13}$$

where $|\psi\rangle \in \mathcal{H}$ is the state of the system, $[\hat{A},\hat{B}]$ is the commutator between $\hat{A}$ and $\hat{B}$ (see Def. 2.23) and $\Delta(\hat{A}), \Delta(\hat{B})$ are the standard deviations–the square roots of the variances, as calculated by Eq. (3.12)*–of $\hat{A}$ and $\hat{B}$, respectively.*

Let us now consider a projective measurement of a qubit in a state $|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{\mathrm{i}\phi}\,\sin(\theta/2)\,|1\rangle$. Let $\hat{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ be an observable whose eigenstates are the elements of the computational basis. The eigenvalues of $\hat{Z}$ are ± 1, and they are measured with probability

$$p_{|\psi\rangle}(1) = |\langle\psi|0\rangle|^2 = \cos^2\left(\frac{\theta}{2}\right), \qquad p_{|\psi\rangle}(-1) = |\langle\psi|1\rangle|^2 = \sin^2\left(\frac{\theta}{2}\right). \tag{3.14}$$

We simplify the notation for the outcomes of this projective measurement:

$$+1 \to 0, \qquad -1 \to 1. \tag{3.15}$$

Hence, a measurement of $\hat{Z}$ on a qubit produces a bit. More precisely, the outcome is a *probabilistic bit*, i.e. a random variable over the set of bits $\mathbb{F}_2$ (see Sec. 2.5).

Positive Operator-Valued Measure (POVM)

We now introduce a second class of mesurements, which is particularly useful when the state after the measurement does not matter and only the measurement statistics is relevant. By considering general measurement operators $\{\hat{M}_m\}$ over a Hilbert space $\mathcal{H}$, we define:

$$\hat{E}_m := \hat{M}_m^\dagger \hat{M}_m. \tag{3.16}$$

Each $\hat{E}_m$ is a positive-semidefinite operator (see Theorem 2.34) and $\{\hat{E}_m\}$ satisfies $\sum_m \hat{E}_m = \hat{I}$. The probability of obtaining the outcome m upon measurement on a quantum state $|\psi\rangle \in \mathcal{H}$ becomes:

$$p_{|\psi\rangle}(m) = \langle\psi|\hat{E}_m|\psi\rangle\,. \tag{3.17}$$

The set $\{\hat{E}_m\}$ is called a *positive operator-valued measure* (POVM) and the operators $\hat{E}_m$ are called the *POVM elements* associated with the measurement.

If we set $\hat{E}_m = \hat{M}_m = \hat{\Pi}_m$, we obtain a projective measurement, which can be therefore seen as a particular case of POVM.

3.1.3 State Evolution

Postulate 3. *The state change of an isolated quantum system is described by means of unitary operators. Namely, if $|\psi(t_1)\rangle \in \mathcal{H}$ is the state of a system at time t_1, and $|\psi(t_2)\rangle$ is the state of the system at time t_2, then*

$$|\psi(t_2)\rangle = \hat{U}\,|\psi(t_1)\rangle\,, \tag{3.18}$$

where $\hat{U}$ is a unitary operator over $\mathcal{H}$, i.e. it satisfies $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{I}$, with $\hat{I}$ being the identity operator on $\mathcal{H}$. Moreover,

$$\hat{U} = e^{-\mathrm{i}\frac{(t_2-t_1)}{\hbar}\hat{H}}, \tag{3.19}$$

where $\hbar$ is the reduced Planck constant *and $\hat{H}$ is the* Hamiltonian operator*, i.e. the observable associated with projective measurements of the system's energy.*

A unitary operator $\hat{U}$ corresponds to a deterministic and reversible evolution, with the reverse evolution given by $\hat{U}^\dagger$.

Consider now the time evolution of the expectation value $\langle\hat{A}\rangle$ of an observable $\hat{A}$. It holds:

$$\langle\hat{A}\rangle\,(t_2) = \langle\psi(t_2)|\hat{A}|\psi(t_2)\rangle = \langle\psi(t_1)|\hat{U}^\dagger\hat{A}\hat{U}|\psi(t_1)\rangle\,. \tag{3.20}$$

Then the same measurement statistics $\langle \hat{A} \rangle (t_2)$ is obtained by two equivalent representations of the system's dynamics: a representation in which the state $|\psi\rangle$ evolves according to Eq. (3.18) and the operator $\hat{A}$ remains unchanged, or a representation in which $|\psi\rangle$ remains unchanged and $\hat{A}$ evolves as:

$$\hat{A} \to \hat{U}^\dagger \hat{A} \hat{U}. \tag{3.21}$$

The former representation is called the *Scrödinger picture*, while the latter one is called the *Heisenberg picture*.

Considering again qubits, we introduce the *Pauli operators*, defined as:

$$\hat{X} := |0\rangle\langle 1| + |1\rangle\langle 0|, \quad \hat{Y} := -\mathrm{i}\,|0\rangle\langle 1| + \mathrm{i}\,|1\rangle\langle 0|, \quad \hat{Z} := |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{3.22}$$

They are unitary and Hermitian operators, and act on a generic qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha, \beta \in \mathbb{C}$ as:

$$\hat{X}|\psi\rangle = (\alpha|1\rangle + \beta|0\rangle); \tag{3.23}$$

$$\hat{Y}|\psi\rangle = \mathrm{i}(\alpha|1\rangle - \beta|0\rangle); \tag{3.24}$$

$$\hat{Z}|\psi\rangle = (\alpha|0\rangle - \beta|0\rangle). \tag{3.25}$$

We have already encountered the operator $\hat{Z}$ (also called the *quantum phase flip*) in Sec. 3.1.2, as the Hermitian operator whose eigenstates are the elements of the computational basis $\{|0\rangle, |1\rangle\}$. We also notice that the operator $\hat{X}$ is the quantum counterpart to the classical bit flip (see Sec. 2.5), and is therefore called the *quantum bit flip*. The eigenstates of $\hat{X}$, which form a commonly used basis in quantum information theory, read:

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.26}$$

The operator $\hat{Y}$ is redundant in the description of a qubit's dynamics, since it holds:

$$\hat{Y} = \frac{1}{2\mathrm{i}}[\hat{Z}, \hat{X}]. \tag{3.27}$$

3.1.4 Composed Systems

Postulate 4. *A composite quantum system is related to its subsystems by means of tensor products. Namely, if $\mathcal{H}_i$ ($i = 1, 2, \ldots, n$) is the state space of the i-th subsystem, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ is the state space of the composite system. Morever, if $|\psi_i\rangle$ is the state of the i-th subsystem, $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ is the state of the composite system.*

It naturally follows that if each state $|\psi_i\rangle$ ($i = 1, 2, \ldots, n$) evolves under a unitary operator $\hat{U}_i$, then the composite state $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ evolves under the unitary operator $\hat{U} = \hat{U}_1 \otimes \hat{U}_2 \otimes \cdots \otimes \hat{U}_n$. In the following, we will omit the symbol $\otimes$ in the product states of states, i.e. we write $|\psi_1\rangle|\psi_2\rangle$ instead of $|\psi_1\rangle \otimes |\psi_2\rangle$. However, we will always use the symbol $\otimes$ for the tensor product of operators and Hilbert spaces.

Postulate 4 allows us to introduce the concept of *entanglement*, which in this chapter is presented only for bipartite quantum systems.

Definition 3.2. Let $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$ be the Hilbert space of a bipartite system. A state $|\Psi_{AB}\rangle \in \mathcal{H}_{AB}$ is called *factorable* if there exist $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$ such that $|\Psi_{AB}\rangle = |\psi_A\rangle\,|\psi_B\rangle$. Conversely, states that are not factorable are called *entangled*.

Entangled systems possess definite quantum states only when they are considered as a single global system. They cannot be precisely described in terms of their subsystems.

Theorem 3.3 (Schmidt decomposition)**.** *Let $|\psi_{AB}\rangle$ be a state on a bipartite Hilbert space $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ is d_A-dimensional and $\mathcal{H}_B$ is d_B-dimensional. Then there exist an orthonormal basis $|i_A\rangle$ for $\mathcal{H}_A$, and an orthonormal basis $|i_B\rangle$ for $\mathcal{H}_B$ such that*

$$|\psi_{AB}\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\; |i_A\rangle\; |i_B\rangle\,, \tag{3.28}$$

where $d = \min\{d_A, d_B\}$ and the coefficients λ_i, called the Schmidt coefficients*, satisfy $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$.*

A proof of the theorem is contained in [MW20]. The number of non-zero Schmidt coefficients is called the *Schmidt rank* of $|\psi_{AB}\rangle$. Factorable states $|\psi_A\rangle\,|\psi_B\rangle$ are already in the form of Eq. (3.28) with Schmidt rank equal to one. Hence, a state is entangled if and only if its Schmidt rank is strictly bigger than one. Clearly, the maximum Schmidt rank is $d = \min\{d_A, d_B\}$.

Definition 3.4. A *maximally entangled state* is a composite state $|\Psi_{AB}\rangle$ that possess maximum Schmidt rank and equal Schmidt coefficients, i.e. a state whose Schmidt decomposition reads:

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i_A\rangle\; |i_B\rangle\,, \tag{3.29}$$

where $d = \min\{d_A, d_B\}$.

An example for two qubits is given by the *Bell states*:

$$|\Phi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle), \tag{3.30}$$

$$|\Psi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle). \tag{3.31}$$

3.2 Quantum Mechanics of Open Systems

3.2.1 Density Operators

The postulates given in Sec. 3.1 describe situations in which the state of a system is perfectly determined by a state vector $|\psi\rangle$, called a *pure state*. This is not always the case. In many scenarios, such as open quantum systems that interact with a noisy environment, the state is only known with a certain probability. Hence, we need a more generic description than pure states.

Definition 3.5. A quantum system is said to be in a *statistical ensemble* $\{p_i, |\psi_i\rangle\}$ if the state of the system is one of the pure states in $\{|\psi_i\rangle\}$ according to the probability distribution $\{p_i\}$, where p_i corresponds to the state $|\psi_i\rangle$. Then, the state of the system is said to be a *mixed state* and is described by the following operator, called the *density operator*:

$$\rho := \sum_i p_i \, |\psi_i\rangle \, \langle\psi_i| \, . \tag{3.32}$$

Density operators are always denoted by greek lowercase letters without a circumflex, i.e. we write ρ instead of $\hat{\rho}$. Pure states arise from Eq. (3.32) as the particular case in which a system is in a state $|\psi_i\rangle$ with certainty ($p_i = 1$). Hence, a pure state $|\psi_i\rangle$ can be represented by a density operator $\rho = |\psi_i\rangle \, \langle\psi_i|$.

The set of all density operators on a Hilbert space $\mathcal{H}$ is denoted by $\mathcal{S}(\mathcal{H})$. From Eq. (3.32), it follows that $\mathcal{S}(\mathcal{H})$ is generated by convex combination of all pure density operators $|\psi_i\rangle \, \langle\psi_i|$. Moreover, a convex combination of any density operators, $\rho = \sum_i p_i \rho_i$, is also a density operator and represents a statistical ensemble $\{p_i, \rho_i\}$, where ρ_i may be pure or mixed.

Theorem 3.6. *An operator ρ is a density operator for some ensemble $\{p_i, \rho_i\}$ if and only if*

$$\rho \geq 0, \quad \textit{and} \quad \mathrm{Tr}(\rho) = 1. \tag{3.33}$$

The proof of this theorem is given in [NC10]. Since $\rho \in \mathcal{S}(\mathcal{H})$ is positive-semidefinite, it has a spectral decomposition (see Eq. (2.80)):

$$\rho = \sum_{i=1}^{d} \lambda_j \, |\lambda_j\rangle \, \langle\lambda_j| \, , \tag{3.34}$$

where d is the dimension of $\mathcal{H}$, $\{|\lambda_j\rangle\}$ is an orthonormal set of eigenvectors of ρ and $\{\lambda_j\}$ is a set of real, non-negative eigenvalues that satisfy $\sum_i \lambda_i = 1$. Pure states are the particular case in which the rank of ρ is 1. If the rank of ρ is d, and all eigenvalues are equal, i.e.

$$\rho = \frac{1}{d} \sum_{i=1}^{d} |\lambda_j\rangle \, \langle\lambda_j| = \frac{1}{d} \, \hat{I}, \tag{3.35}$$

where $\hat{I}$ is the identity on $\mathcal{H}$, then ρ is said the *maximally mixed state* of $\mathcal{S}(\mathcal{H})$.

Definition 3.7. The *purity* of a quantum state $\rho \in \mathcal{S}(\mathcal{H})$ is the quantity $\mathrm{Tr}[\rho^2]$. From Eq. (3.34), it follows that:

$$\frac{1}{d} \leq \mathrm{Tr}[\rho^2] \leq 1, \tag{3.36}$$

where d is the dimension of $\mathcal{H}$. In particular, $\mathrm{Tr}[\rho^2] = 1$ is achieved only for pure states, and $\mathrm{Tr}[\rho^2] = 1/d$ is achieved only for the maximally mixed state on $\mathcal{S}(\mathcal{H})$.

3.2.2 Postulates of Quantum Mechanics for Density Operators

Revised Postulate 1. *Any quantum system is associated with a complex Hilbert space $\mathcal{H}$, known as the* space state. *Quantum states of the system are completely described by density operators $\rho \in \mathcal{S}(\mathcal{H})$, i.e. positive operators of trace one on the Hilbert space $\mathcal{H}$. If a quantum system is in a statistical ensemble $\{p_i, \rho_i\}$, the density operator for the system reads:*

$$\rho = \sum_i p_i \, \rho_i. \tag{3.37}$$

The density operator of a generic qubit can be written as a combination of the identity $\hat{I}$ on $\mathcal{H}$, and the Pauli operators $\hat{X}, \hat{Y}$ and $\hat{Z}$ [Pau27]:

$$\rho = \frac{1}{2}\left(\hat{I} + r_x\hat{X} + r_y\hat{Y} + r_z\hat{Z}\right), \tag{3.38}$$

where r_x, r_y, r_z are real coefficients such that $r_x^2 + r_y^2 + r_z^2 \leq 1$. We saw in Eq. (3.4) that pure states are represented by points on the Bloch sphere, which is a three-dimensional sphere of unit radius. From Eq. (3.38), we now see that mixed states are represented by points inside the Bloch sphere, with coordinates (r_x, r_y, r_z). In particular, the maximally mixed state $\rho = \frac{\hat{I}}{2}$ is represented by the center of the sphere $(0, 0, 0)$.

Revised Postulate 2. *Quantum measurements are described by a set* $\{\hat{M}_m\}$ *of* measurement operators *on the state space* $\mathcal{H}$*, with* m *labelling a possible outcome of the measurement. The measurement operators satisfy the completeness relation* $\sum_m \hat{M}_m^\dagger \hat{M}_m = \hat{I}$*, where* $\hat{I}$ *is the identity operator on* $\mathcal{H}$*. If* ρ *is the state of the system immediately prior to the measurement, then the probability of obtaining the outcome* m *is given by:*

$$p_\rho(m) = \mathrm{Tr}(\hat{M}_m\,\rho\,\hat{M}_m^\dagger), \tag{3.39}$$

and the measurement transforms ρ *into:*

$$\rho \mapsto \frac{1}{\sqrt{p_\rho(m)}}\,\hat{M}_m\rho\,\hat{M}_m^\dagger. \tag{3.40}$$

If we consider a von Neumann measurements on an observable $\hat{M} = \sum_m m\,|m\rangle\langle m|$, it follows:

$$p_\rho(m) = \langle m|\rho|m\rangle\,, \tag{3.41}$$

$$\langle\hat{M}\rangle := \mathrm{Tr}\,(\hat{M}\rho). \tag{3.42}$$

Revised Postulate 3. *A deterministic state change of a quantum system is described by means of unitary operators. Namely, if* $\rho(t_1)$ *is the state of a system at time* t_1*, and* $\rho(t_2)$ *is the state of the system at time* t_2*, then*

$$\rho(t_2) = \hat{U}\rho(t_1)\hat{U}^\dagger, \tag{3.43}$$

where $\hat{U}$ *is a unitary operator on* $\mathcal{H}$*, i.e. it satisfies* $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{I}$*, with* $\hat{I}$ *being the identity operator on* $\mathcal{H}$*.*

It is easy to see the emergence of Revised Postulate (3) from Postulate (3). If every state in an ensemble $\{p_i, |\psi_i\rangle\}$ evolves as $|\psi_i\rangle \to \hat{U}\,|\psi_i\rangle$, then

$$\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i| \mapsto \sum_i p_i\,\hat{U}\,|\psi_i\rangle\langle\psi_i|\,\hat{U}^\dagger = \hat{U}\rho\hat{U}^\dagger. \tag{3.44}$$

If we now consider the time evolution of the expectation value of an observable $\hat{A}$, it holds:

$$\langle\hat{A}\rangle\,(t_2) = \mathrm{Tr}[\rho(t_2)\hat{A}] = \mathrm{Tr}[\hat{U}\rho(t_1)\hat{U}^\dagger\hat{A}] = \mathrm{Tr}[\rho(t_1)\hat{U}^\dagger\hat{A}\hat{U}] = \mathrm{Tr}[\rho(t_1)\hat{A}(t_2)], \tag{3.45}$$

with $\hat{A}(t_2) = \hat{U}^\dagger\hat{A}\hat{U}$. Therefore we extend to density operators both the Schrödinger and Heisenberg picture (see Sec.3.1.2).

Revised Postulate 4. *A composite quantum system is related to its subsystems by means of tensor products. Namely, if $\mathcal{H}_i$ ($i = 1, 2, \ldots, n$) is the state space of the i-th subsystem, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ is the state space of the composite system.*

There is a major difference with the case of pure states. If ρ_i is the state of the i-th subsystem, we cannot say that $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$ is the state of the composite system. We will see in Sec. 3.2.3 that the composite state may be a pure entangled state.

The definition of entanglement for bipartite mixed states becomes the following:

Definition 3.8. A *separable* state is a density operator ρ_{AB} on $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$ that can be written as convex combination of states ρ_A^k on $\mathcal{H}_A$ and ρ_B^k on $\mathcal{H}_B$, i.e.

$$\rho_{AB} = \sum_k p_k \, \rho_A^k \otimes \rho_B^k. \tag{3.46}$$

Conversely, all states that are not separable are called *entangled*.

Factorable states, $|\psi_A\rangle \otimes |\psi_B\rangle$ or $\rho_A \otimes \rho_B$, are a particular case of separable states. It is difficult to determine whether a mixed state is entangled since the Schmidt decomposition does not hold for mixed states. We are going to expand on this topic in Chaps. 6 and 7.

3.2.3 Reduced Density Operator and Purification

The formalism of density operators allows us to describe the state of a subsystem knowing the state of the composite system. We consider again a bipartite system AB and, without loss of generality, we focus only on the subsystem A.

Definition 3.9. Let ρ_{AB} be the state of a bipartite system AB with Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Then the state of the subsystem A is described by the corresponding *reduced density operator*, which is defined as:

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{3.47}$$

where Tr_B is the *partial trace* over $\mathcal{H}_B$ (see Def. 2.50).

If $\rho_{AB} = \rho_A \otimes \rho_B$, it immediately follows that $\mathrm{Tr}_B \rho_{AB} = (\mathrm{Tr}\rho_B)\, \rho_A = \rho_A$. Analogously, $\mathrm{Tr}_B(|\psi_A\rangle \langle\psi_A| \otimes |\psi_B\rangle \langle\psi_B|) = |\psi_A\rangle \langle\psi_A|$. For a generic bipartite state ρ_{AB}, it is less evident why the partial trace is the correct way to obtain a state for the subsystem A.

Theorem 3.10. *Let ρ_{AB} be the state of a bipartite system AB with Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Then, the reduced density operator $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ is the unique density operator that provides the correct measurement statistics for any observable $\hat{M}_A$ on the subsystem A, i.e.*

$$\mathrm{Tr}\left(\hat{M}_A \rho_A\right) = \mathrm{Tr}\left((\hat{M}_A \otimes \hat{I}_B)\rho_{AB}\right), \tag{3.48}$$

where $\hat{I}_B$ is the identity operator over $\mathcal{H}_B$.

A proof of the theorem is contained in [NC10].

Let us now consider a pure state $|\psi_{AB}\rangle$ on a bipartite Hilbert space $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$. For simplicity, let the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ be equal to d. The Schmidt decomposition

(see Theorem 3.3) of $|\psi_{AB}\rangle$ is $|\psi_{AB}\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\, |i_A\rangle\, |i_B\rangle$, where $\{|i_A\rangle\}$ and $\{|i_B\rangle\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The reduced density operator of A, ρ_A, reads

$$\rho_A = \mathrm{Tr}_B \left(|\psi_{AB}\rangle \langle\psi_{AB}|\right) = \sum_{i=1}^{d} \lambda_i\, |i_A\rangle \langle i_A|\,. \tag{3.49}$$

A pure state is entangled if and only if there are at least two non-zero coefficients, $\lambda_i, \lambda_j \neq 0$. When this happens, the reduced state ρ_A in Eq. (3.49) is mixed. Therefore, an entangled bipartite system that possesses a precisely determined state (*pure state*) always has statistically uncertain states (*mixed state*) for its subsystems. In particular, the reduced density operator ρ_A of a maximally entangled state (see Eq. (3.29)) $|\Psi_{AB}\rangle$ is the maximally mixed state (see Eq. (3.35)) for $\mathcal{H}_A$:

$$\rho_A = \mathrm{Tr}_B \left(|\Psi_{AB}\rangle \langle\Psi_{AB}|\right) = \frac{1}{d} \sum_{i=1}^{d} |i_A\rangle \langle i_A| = \frac{\hat{I}_A}{d}. \tag{3.50}$$

Remarkably, every mixed state can be considered as the reduced state of a pure entangled state in a larger system. This process is called the *purification* of the system.

Theorem 3.11 (Purification)**.** *For any mixed state ρ_A on a system A, we can introduce a system R, called a* reference system*, and define a pure state $|\psi_{AR}\rangle$ on the joint system AR such that*

$$\rho_A = \mathrm{Tr}_R(|\psi_{AR}\rangle \langle\psi_{AR}|). \tag{3.51}$$

Proof. Let $\{|i_A\rangle\}$ be the basis of $\mathcal{H}_A$ that diagonalises ρ_A, i.e. $\rho_A = \sum_{i=1}^{d_A} \lambda_i\, |i_A\rangle \langle i_A|$, where d_A is the dimension of $\mathcal{H}_A$. If $\{|i_R\rangle\}$ is a basis of a Hilbert space $\mathcal{H}_R$ with dimension $d_R = d_A$, we can define a pure state $|\psi_{AR}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R$ whose Schmidt decomposition (see Theorem 3.3) reads:

$$|\psi_{AR}\rangle := \sum_{i=1}^{d_A} \sqrt{\lambda_i}\, |i_A\rangle\, |i_R\rangle\,. \tag{3.52}$$

We conclude the proof by noting that

$$\mathrm{Tr}_R \left(|\psi_{AR}\rangle \langle\psi_{AR}|\right) = \sum_{i=1}^{d_A} \lambda_i\, |i_A\rangle \langle i_A| = \rho_A. \tag{3.53}$$

□

3.2.4 Quantum Channels

So far, we have considered deterministic and reversible state changes, described by unitary operators. We now introduce *quantum channels*, which are a tool used to characterise the generic evolution of a system, including irreversible and probabilistic state changes that are caused by the interaction of a system with a noisy environment.

Definition 3.12. Let $\mathcal{S}(\mathcal{H})$ denote the set of density operators on a Hilbert space $\mathcal{H}$. A *quantum channel* (or *quantum operation*) is a map $\Lambda : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ that transforms a density operator $\rho \in \mathcal{S}(\mathcal{H}_A)$ on a Hilbert space $\mathcal{H}_A$ into another density operator $\Lambda[\rho] \in \mathcal{S}(\mathcal{H}_A)$, possibly defined on a different Hilbert space $\mathcal{H}_B$.

From now on, we consider for simplicity $\mathcal{H}_A = \mathcal{H}_B$. A quantum channel needs to satisfy a certain set of properties, in order to ensure that $\Lambda[\rho]$ is a valid density operator for any input density ρ. First of all, it must hold

$$\Lambda[\rho] \geq 0, \quad \text{and} \quad \mathrm{Tr}\left[\Lambda[\rho]\right] = 1 = \mathrm{Tr}[\rho]. \tag{3.54}$$

Therefore Λ needs to be *positive* and *trace preserving*. However, positivity is not enough: we have to require the *complete positivity* of Λ, i.e.

$$\left(\Lambda \otimes \mathrm{id}_R\right)[\rho_{AR}] \geq 0, \tag{3.55}$$

for any density operator $\rho_{AR} \in \mathcal{S}(\mathcal{H}_{AR})$ with $\mathcal{H}_{AR} = \mathcal{H}_A \otimes \mathcal{H}_R$, where $\mathcal{H}_R$ is a Hilbert space of arbitrary dimension and id_R is the identity map of $\mathcal{S}(\mathcal{H}_R)$. This requirement ensures that a quantum channel produces a valid density operator also when acting on a subsystem of a larger, possibly entangled, system.

Finally, a quantum channel needs to be convex over the set of density operators, i.e.

$$\Lambda\left[\sum_i p_i \rho_i\right] = \sum_i p_i \Lambda[\rho_i], \tag{3.56}$$

for a set of probabilities $\{\, p_i \,\}$. This is a consequence of Revised Postulate 1: if a system is in an ensemble $\{\, p_i, \rho_i \,\}$, then the state of the system is $\rho = \sum_i p_i \rho_i$. Eq. (3.56) ensures that the evolution of ρ is consistent with the evolutions of the individual ρ_i.

For all these conditions, a quantum channel is also called a *completely positive trace preserving* (CPTP) *map*.

Theorem 3.13 (Kraus theorem)**.** *Let $\mathcal{S}(\mathcal{H})$ be the set of density operators on $\mathcal{H}$. A linear map $\Lambda : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ is completely positive and trace preserving if and only if there exist some linear operators $\{\hat{K}_k\}$, satisfying*

$$\sum_k \hat{K}_k^\dagger \hat{K}_k = \hat{I}, \tag{3.57}$$

such that for any $\rho \in \mathcal{S}(\mathcal{H})$ it holds:

$$\Lambda[\rho] = \sum_k \hat{K}_k \rho \hat{K}_k^\dagger. \tag{3.58}$$

The operators $\hat{K}_k$ are called Kraus operators *and define the* Kraus decomposition *of the channel Λ. It also holds that the number of Kraus operators is no larger than d^2, where d is the dimension of $\mathcal{H}$.*

A proof of the theorem is given in [NC10], where it also showed that the Kraus decomposition is not unique. The Kraus theorem gives us an analytical expression for the action of a generic quantum channel.

An alternative meaningful representation is given by the *Stinespring's dilation*, whose proof is also given in [NC10].

Theorem 3.14 (Stinespring's dilation)**.** *For any quantum channel Λ_S on a Hilbert space $\mathcal{H}_S$, there exists a Hilbert space $\mathcal{H}_E$ and a unitary operator $\hat{U}_{SE}$ on $\mathcal{H}_S \otimes \mathcal{H}_E$ such that*

$$\Lambda_S[\rho_S] = \mathrm{Tr}_E\left[\hat{U}_{SE}(\rho_S \otimes \rho_E)\hat{U}_{SE}^\dagger\right], \tag{3.59}$$

for all $\rho_S \in \mathcal{S}(\mathcal{H}_S)$ and some $\rho_E \in \mathcal{S}(\mathcal{H}_E)$.

This representation interprets quantum channels as interactions between an open system S and an environment E. The composite system SE is closed and evolves unitarily.

Notice that $\rho_E \in \mathcal{H}_E$ in Eq. (3.59) can always be chosen pure, i.e. $\rho_E = |\psi_E\rangle\langle\psi_E|$. We do not have to fix the dimension of $\mathcal{H}_E$, so if $\rho_E \in \mathcal{S}(\mathcal{H}_E)$ is mixed, we can always purify ρ_E in a larger environmental space $\mathcal{H}_E \otimes \mathcal{H}_R$. Then we write:

$$\Lambda_S[\rho_S] = \mathrm{Tr}_E\left[\hat{U}_{SE}(\rho_S \otimes |\psi_E\rangle\langle\psi_E|)\hat{U}_{SE}^\dagger\right] = \sum_k \langle e_K|\,\hat{U}_{SE}\,(\rho_S \otimes |\psi_E\rangle\langle\psi_E|)\,\hat{U}_{SE}^\dagger\,|e_k\rangle\,, \tag{3.60}$$

for some basis $\{|e_k\rangle\}$ of $\mathcal{H}_E$. This allows us to connect the Stinespring's dilation in Eq. (3.59) with the Kraus decomposition in Eq. (3.57), by choosing:

$$\hat{K}_k := \langle e_k|\hat{U}_{SE}|\psi_E\rangle\,. \tag{3.61}$$

3.3 Elements of Quantum Information Theory

3.3.1 Entropies

Claude Shannon, the father of information theory, defined the concept of *information* in relation to the concept of *uncertainty* [Sha48]. A measurement of a system can produce an information gain only if the state of the system before the measurement was uncertain and this uncertainty is reduced by the measurement.

Thus, a key quantity in information theory is the *entropy*, which is a measure of uncertainty. In this subsection, we review the main entropic measures that are used in the remainder of this thesis.

Definition 3.15 (Shannon entropy [Sha48])**.** Let $\mathcal{X}$ be a discrete set of cardinality d and X be a random variable taking values $x \in \mathcal{X}$ with probability $p(x)$. The *Shannon entropy* of X is given by

$$H(X) = -\sum_{x=1}^{d} p(x)\,\log_2\,p(x), \tag{3.62}$$

with the convention $0\log_2 0 = 0$. The Shannon entropy of X can be also indicated as $H(\boldsymbol{p})$, where $\boldsymbol{p} = (p(1), p(2), \ldots, p(d))$.

In the remainder of this thesis, we will always denote by $\log$ the logarithm in base 2 and by $\ln$ the natural logarithm in base e. The base 2 in the logarithm implies that the entropy is expressed in bits, which can be seen as the basic units of information.

The Shannon entropy of X quantifies the average uncertainty on the values of X before a measurement. In Chap. 5, we are going to also use another classical entropy, which quantifies the uncertainty on the values of X in terms of the probability to randomly guess one of them.

Definition 3.16 (min-entropy [Rén+61])**.** Let $\mathcal{X}$ be a discrete set and X be a random variable taking values $x \in \mathcal{X}$ with probability $p(x)$. The *min-entropy* of X is defined as:

$$H_\infty(X) := -\log\left(\max_{x\in\mathcal{X}} p(X = x)\right). \tag{3.63}$$

We now consider quantum entropies.

Definition 3.17 (von Neumann entropy [NC10])**.** The *von Neumann entropy* of a density operator $\rho \in \mathcal{S}(\mathcal{H})$ is defined as:

$$S(\rho) := -\mathrm{Tr}(\rho \log \rho), \tag{3.64}$$

with the assumption $0 \log 0 = 0$.

The von Neumann entropy is the quantum counterpart to the Shannon entropy. In particular, let us consider the spectral representation of $\rho \in \mathcal{S}(\mathcal{H})$, $\rho = \sum_{i=1}^{d} \lambda_i \, |\lambda_i\rangle \langle\lambda_i|$, where d is the dimension of $\mathcal{H}$, and λ_i and $|\lambda_i\rangle$ are the egenvalues and eigenvectors of ρ, respectively. Since ρ is positive-semidefinite and $\mathrm{Tr}\rho = 1$, it follows that $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. Then,

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i = H(\boldsymbol{\lambda}), \tag{3.65}$$

where $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{d-1})$. From Eqs. (3.64) and (3.65), the following properties of ρ follow:

1. $S(\rho) \geq 0$ for every ρ and $S(\rho) = 0$ if and only if ρ is pure.

2. $S(\rho)$ is invariant under unitary operations, i.e. $S(U \, \rho \, U^\dagger) = S(\rho)$. This follows from the fact that the eigenvalues of ρ are invariant under unitary transformations (see Eq. (2.82)).

3. $0 \leq S(\rho) \leq \log \, d$, for every ρ on a d-dimensional Hilbert space $\mathcal{H}$. In particular $S(\rho) = \log d$ if and only if ρ is the maximally mixed state $\hat{I}/d$.

An additional entropy, which will play a major role in Chap. 7, is the *quantum relative entropy*.

Definition 3.18 (Quantum relative entropy [NC10])**.** For any two density operators $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ the *quantum relative entropy* is defined as

$$S(\rho \| \sigma) := \mathrm{Tr}(\rho(\log \rho - \log \sigma)). \tag{3.66}$$

By convention, $S(\rho\|\sigma) = \infty$ if the *support* of ρ, i.e. the vector space spanned by the eigenvectors of ρ belonging to non-zero eigenvalues, is not contained in the support of σ.

Theorem 3.19 (Klein's inequality)**.** *For any $\rho, \sigma \in \mathcal{S}(\mathcal{H})$, the quantum relative entropy $S(\rho\|\sigma)$ is non-negative,*

$$S(\rho\|\sigma) \geq 0, \tag{3.67}$$

and $S(\rho\|\sigma) = 0$ if and only if $\rho = \sigma$.

A proof of this theorem is given in [NC10]. Because of Klein's inquequality, the quantum relative entropy is used as a *pseudo-distance* on the set $\mathcal{S}(\mathcal{H})$ of density operators on $\mathcal{H}$. The relative entropy is not a true distance because it is not symmetric, $S(\rho\|\sigma) \neq S(\sigma\|\rho)$, and does not satisfy the triangle inequality, $S(\rho\|\sigma) \nleq S(\rho\|\tau) + S(\sigma\|\tau)$.

Consider now a state ρ_{AB} on a bipartite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Let $\rho_A = \mathrm{Tr}_B \, \rho_{AB}$ and $\rho_B = \mathrm{Tr}_A \, \rho_{AB}$. We denote the von Neumann entropy (see Eq. (3.64)) of ρ_A and ρ_B by $S(A) := S(\rho_A) = -\mathrm{Tr}(\rho_A \log \rho_A)$ and $S(B) := S(\rho_B) = -\mathrm{Tr}(\rho_B \log \rho_B)$, respectively. We additionally introduce:

- The *quantum joint entropy* of ρ_{AB},

$$S(A,B) := S(\rho_{AB}) = -\mathrm{Tr}\left(\rho_{AB}\log\rho_{AB}\right), \tag{3.68}$$

  which is the von Neumann entropy of the composite system;

- The *quantum conditional entropy* of A with respect to B,

$$S(A|B) = S(A,B) - S(B), \tag{3.69}$$

  which quantifies the uncertainty about the system A after gaining full information about the system B;

- The *quantum mutual information* between A and B,

$$I(A:B) := S(A) + S(B) - S(A,B) \equiv S(A) - S(A|B), \tag{3.70}$$

  which quantifies the information gain on A after gaining full information about the system B.

3.3.2 Fidelity and Trace Distance

Definition 3.20 (Fidelity [NC10])**.** The *fidelity* between two density operators $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ is defined as

$$F(\rho,\sigma) := \mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{3.71}$$

The fidelity satisfies the following properties, which are proven in [NC10]:

1. $F(\rho,\sigma) = F(\sigma,\rho)$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$;
2. $0 \leq F(\rho,\sigma) \leq 1$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ and $F(\rho,\sigma) = 1$ if and only if $\rho = \sigma$;
3. $F(\hat{U}\,\rho\,\hat{U}^\dagger, \hat{U}\,\sigma\,\hat{U}^\dagger) = F(\rho,\sigma)$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ and unitary operator $\hat{U}$;
4. $F(\sum_i p_i\rho_i,\sigma) \geq \sum_i p_i\,F(\rho_i,\sigma)$ and $F(\rho,\sum_i p_i\sigma_i) \geq \sum_i p_i\,F(\rho,\sigma_i)$;
5. $F(|\psi\rangle\langle\psi|,\sigma) = \sqrt{\langle\psi|\sigma|\psi\rangle}$ for any pure state $|\psi\rangle \in \mathcal{H}$ and density $\sigma \in \mathcal{S}(\mathcal{H})$. In particular, if $\sigma = |\phi\rangle\langle\phi|$, then $F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|$.

Although it is not a proper distance, the fidelity is frequently used in quantum information to quantify the "closeness" of two quantum states.

Definition 3.21 (Trace distance [NC10])**.** The *trace distance* between two density operators $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ is defined as:

$$D(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_1, \tag{3.72}$$

where $\|\cdot\|_1$ is the *trace norm* of $\mathcal{S}(\mathcal{H})$, defined as:

$$\|\tau\|_1 := \mathrm{Tr}\left[\sqrt{\tau^\dagger\tau}\right], \qquad \tau \in \mathcal{S}(\mathcal{H}). \tag{3.73}$$

The trace distance is a proper distance for the set $\mathcal{S}(\mathcal{H})$ of density operators, i.e. it satisfies the following requirements (see Def. 2.8) for any $\rho,\sigma,\tau \in \mathcal{S}(\mathcal{H})$:

1. $D(\rho,\sigma) = D(\sigma,\rho)$;
2. $0 \leq D(\rho,\sigma) \leq 1$ for all $\rho,\sigma \in \mathcal{S}(\mathcal{H})$, and $D(\rho,\sigma) = 0$ if and only if $\rho = \sigma$;
3. $D(\rho,\sigma) \leq D(\rho,\tau) + D(\tau,\sigma)$.

These properties are proven in [NC10] together with the following additional ones:

1. $D(\hat{U}\,\rho\,\hat{U}^\dagger, \hat{U}\,\sigma\,\hat{U}^\dagger) = D(\rho,\sigma)$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ and unitary operator $\hat{U}$;
2. $D(\Lambda[\rho],\Lambda[\sigma]) \leq D(\rho,\sigma)$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$ and quantum channel Λ. We say that the trace distance is a *contractive distance*;
3. $D(\sum_i p_i\rho_i,\sigma) \leq \sum_i p_i\, D(\rho_i,\sigma)$ and $D(\rho,\sum_i p_i\sigma_i) \leq \sum_i p_i\, D(\rho,\sigma_i)$;
4. $1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1-F(\rho,\sigma)}$ for any $\rho,\sigma \in \mathcal{S}(\mathcal{H})$, where $F(\rho,\sigma)$ is the fidelity between ρ and σ. The upper-bound inequality is saturated when ρ and σ are pure states.

3.3.3 Unclonable and Indistinguishable States

In this section, we introduce two important results of quantum information theory, which are useful in the remainder of the thesis, especially in Chap. 5.

Theorem 3.22 (No-cloning Theorem [WZ82; Die82])**.** *It is impossible to perfectly copy an unknown pure quantum state $|\psi\rangle$, i.e. there does not exist a universal cloning operator $\hat{U} : \mathcal{H}\otimes\mathcal{H} \to \mathcal{H}\otimes\mathcal{H}$ such that*

$$\hat{U}\,|\psi\rangle\,|\alpha\rangle = |\psi\rangle\,|\psi\rangle\,, \tag{3.74}$$

for every $|\psi\rangle \in \mathcal{H}$ and for some ancillary state $|\alpha\rangle \in \mathcal{H}$.

Proof. The proof follows by contradiction. Suppose there exists the universal cloning operator of Eq. (3.74). Then, for two pure states $|\psi\rangle$ and $|\phi\rangle$, it holds:

$$\hat{U}(|\psi\rangle \otimes |\alpha\rangle) = |\psi\rangle \otimes |\psi\rangle\,, \tag{3.75}$$

$$\hat{U}(|\phi\rangle \otimes |\alpha\rangle) = |\phi\rangle \otimes |\phi\rangle\,. \tag{3.76}$$

We consider the inner product of the elements at the left-hand side of Eqs. (3.75) and (3.76), and equate it to the inner product of the elements at the right-hand side, i.e.

$$\begin{aligned}(\langle\alpha| \otimes \langle\psi|)\,\hat{U}^\dagger\hat{U}\,(|\phi\rangle \otimes |\alpha\rangle) &= \langle\psi|\phi\rangle\,\langle\psi|\phi\rangle\,;\\ \langle\alpha|\alpha\rangle\,\langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2;\\ \langle\psi|\phi\rangle &= (\langle\psi|\phi\rangle)^2.\end{aligned} \tag{3.77}$$

The only solutions for this equation are $\langle\psi|\phi\rangle = 0, 1$, so either $|\psi\rangle = |\phi\rangle$ or $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. Therefore a general quantum cloning device, that works for all quantum states, is impossible. □

We emphasise that the no-cloning theorem forbid *perfect* cloning of an unknown quantum state. Imperfect cloning is always possible, and in certain cases, the cloned states achieve a high fidelity with the original ones [BH96].

Theorem 3.23 (Indistinguishability of non-orthogonal states [NC10])**.** *Any attempt to distinguish between two non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$ introduces disturbance to at least one of them.*

Proof. Let us consider a generic quantum channel Λ, acting on two non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$. By using the Stinespring's dilation of Λ (see Theorem 3.14), we write:

$$\hat{U}(|\psi\rangle \otimes |e\rangle) = |\psi'\rangle \otimes |v_\psi\rangle\,, \tag{3.78}$$

$$\hat{U}(|\phi\rangle \otimes |e\rangle) = |\phi'\rangle \otimes |v_\phi\rangle\,, \tag{3.79}$$

where $\hat{U}$ is a unitary operator acting on a larger Hilbert space and $|e\rangle$ is an environmental ancilla state.

To perfectly distinguish $|\psi\rangle$ and $|\phi\rangle$, $\hat{U}$ would have to satify $|\psi'\rangle = |\psi\rangle$, $|\phi'\rangle = |\phi\rangle$ and $|v_\psi\rangle \neq |v_\phi\rangle$.

However, by considering the inner product of the elements at the left-hand side of Eqs. (3.78) and (3.79), and equating it to the inner product of the elements at the right-hand side, we obtain the equation:

$$\begin{aligned} (\langle e| \otimes \langle\psi|)\, \hat{U}^\dagger \hat{U}\, (|\phi\rangle \otimes |e\rangle) &= \langle\psi'|\phi'\rangle\, \langle v_\psi|v_\phi\rangle\,; \\ \langle\psi|\phi\rangle &= \langle\psi'|\phi'\rangle\, \langle v_\psi|v_\phi\rangle\,. \end{aligned} \tag{3.80}$$

Therefore we can distinguish between $|\psi\rangle$ and $|\phi\rangle$ ($|v_\psi\rangle \neq |v_\phi\rangle$) if and only if we introduce disturbance to at least one of the states ($|\psi'\rangle \neq |\psi\rangle$ or $|\phi'\rangle \neq |\phi\rangle$). □

4

Quantum Information with Continuous Variables

Continuous-variable (CV) systems are characterised by degrees of freedom with a continuous spectrum, such as the position and momentum of a particle (*canonical conjugated coordinates*). They are frequently encountered in *quantum optics*, which is the branch of quantum physics devoted to the study of light photons, and in *continuous-variable quantum information theory*, where the continuous-variable quantum optical states are used to encode and transmit information. Quantum states of CV systems are described by density operators in infinite-dimensional Hilbert spaces but admit alternative representations in the real *phase spaces* of their conjugate coordinates. The most important family of CV quantum states is that of *Gaussian states*, which are represented in the phase space by Gaussian functions.

In this chapter, we introduce the main concepts of CV quantum information theory. We start by introducing the quantum states of the electromagnetic field and the phase space representations (*characteristic functions* and *quasi-probability distributions*). After that, we focus on Gaussian states and study their dynamics in terms of Gaussian operations. We do not discuss here the topic of continuous-variable entanglement, since it will be treated in Chap. 6. The content of this chapter is mostly inspired from [WM07; Oli12; Wee+12; ARL14; Ser17], and we refer to these works for more technical details.

4.1 Quantum Light

This section is devoted to introduce the second quantisation of the electromagnetic field and review the different representations for the quantum states of light.

4.1.1 Second Quantisation of the Electromagnetic Field

Let $\boldsymbol{A}(\boldsymbol{x}, t)$ be the classical vector potential, with $\boldsymbol{x}$ and t being the position vector and the time, respectively. In absence of charges and currents, and by requiring the Coulumb gauge

$\nabla \cdot \boldsymbol{A}(\boldsymbol{r}, t) = 0$, $\boldsymbol{A}$ obeys the wave equation,

$$\nabla^2 \boldsymbol{A}(\boldsymbol{x}, t) = \frac{1}{c^2} \frac{\partial^2 \boldsymbol{A}}{\partial t^2}, \tag{4.1}$$

where c is the speed of light. The solution of this equation in a finite volume V reads [WM07]:

$$\boldsymbol{A}(\boldsymbol{x}, t) = \sum_k \left(\frac{\hbar}{2\omega_k \, \epsilon_0} \right)^{1/2} \left[a_k \, \boldsymbol{u}_k(\boldsymbol{x}) \, e^{-i\omega_k \, t} - a_k^* \, \boldsymbol{u}_k^*(\boldsymbol{x}) \, e^{i\omega_k \, t} \right], \tag{4.2}$$

where $\hbar$ is the reduced Planck's constant, ϵ_0 is the vacuum electric permittivity, $a_k \in \mathbb{C}$, $\omega_k \in \mathbb{R}$, and the vector functions $\{\boldsymbol{u}_k(\boldsymbol{x})\}$ satisfy

$$\int_V \boldsymbol{u}_k^*(\boldsymbol{x}) \cdot \boldsymbol{u}_{k'}(\boldsymbol{x}) \, d\boldsymbol{x} = \delta_{kk'}. \tag{4.3}$$

The explicit form of $\boldsymbol{u}_k(\boldsymbol{x})$ depends on the boundary conditions used in the solution of Eq. (4.1). If we consider a cubical volume of side L, with periodic boundary conditions, $\boldsymbol{u}_k(\boldsymbol{x})$ reads:

$$\boldsymbol{u}_k(\boldsymbol{x}) = L^{-3/2} \, e^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{x}} \, \boldsymbol{e}_\lambda, \tag{4.4}$$

where $\boldsymbol{k} = (2\pi \, n_1/L, \, 2\pi \, n_2/L, \, 2\pi n_3/L)$ is the propagation vector $(n_1, n_2, n_3 = 0, \pm 1, \dots)$ and $\boldsymbol{e}_\lambda$ is the unit polarisation vector ($\lambda = 1, 2$), with $\boldsymbol{k} \cdot \boldsymbol{e}_\lambda = 0$. Hence, the index k describes the four indices n_1, n_2, n_3, λ.

The decomposition in Eq. (4.2) is called the *normal mode decomposition* of the electromagnetic field, and the elements of the sum are called the *normal modes* of the electromagnetic field. Morever, the functions $\{\boldsymbol{u}_k^*(\boldsymbol{x})\}$ are called the *normal mode functions* and the constant ω_k are the *mode frequencies*.

Using the mode decomposition of $\boldsymbol{A}(\boldsymbol{x}, t)$, the electromagnetic energy E can be written as [GAF10]:

$$\begin{aligned} E &= \frac{\epsilon_0}{2} \int \left(\left| \frac{\partial \boldsymbol{A}}{\partial t} \right|^2 + c^2 \, |\nabla \times \boldsymbol{A}|^2 \right) d\boldsymbol{x} \\ &= \sum_k \frac{\hbar}{2} \, (a_k^* \, a_k + a_k \, a_k^*). \end{aligned} \tag{4.5}$$

Theorem 4.1 (Second Quantisation of the electromagnetic field [WM07; GAF10])**.** *The electromagnetic field is quantised by replacing the complex numbers a_k, a_k^* with mutually adjoint operators $\hat{a}_k, \hat{a}_k^\dagger$ that satisfy the* bosonic commutation relations

$$\left[\hat{a}_k, \hat{a}_{k'} \right] = \left[\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger \right] = 0, \qquad \left[\hat{a}_k, \hat{a}_{k'}^\dagger \right] = \delta_{kk'}. \tag{4.6}$$

The energy of the electromagnetic field (see Eq. (4.5)) becomes the Hamiltonian operator

$$\hat{H} = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right). \tag{4.7}$$

This Hamiltonian is formally identical to the Hamiltonian of an ensemble of independent quantum harmonic oscillators [Sha12], each one with frequency ω_k.

Definition 4.2. Let $\{\hat{a}_k, \hat{a}_k^\dagger\}$ be a set of mode operators. For each mode k, we define the corresponding *quadrature operators*, $\hat{q}_k$ and $\hat{p}_k$, as:

$$\hat{q}_k := \frac{\hat{a}_k + \hat{a}_k^\dagger}{\sqrt{2}}, \qquad \hat{p}_k := \frac{\hat{a}_k - \hat{a}_k^\dagger}{\mathrm{i}\sqrt{2}}. \tag{4.8}$$

They obey the following commutation relations, which are a consequence of the CCRs of Eq. (4.6):

$$[\hat{q}_j, \hat{q}_k] = [\hat{p}_j, \hat{p}_k] = 0, \qquad [\hat{q}_j, \hat{p}_k] = \mathrm{i}\,\delta_{jk}. \tag{4.9}$$

The commutation relations of Eq. (4.9) are formally identical to the canonical commutation relations (see Eq. (2.105)) for the position and momentum operators. Hence, the quadrature operators satisfy all the mathematical properties of the canonical conjugate operators.

Each mode is associated with an infinite-dimensional Hilbert space $\mathcal{H}_k$ and the total system is described by a tensor product of single-mode Hilbert spaces,

$$\mathcal{H} = \bigotimes_k \mathcal{H}_k. \tag{4.10}$$

Although in teory the number of modes cannot be bounded, in practice the experimental accessible modes are finite. We thus consider, in the following, a finite number of modes, indicated by M. We then group the quadrature operators in a vector $\hat{\boldsymbol{r}} := (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_M, \hat{p}_M)^T$. This allows us to rewrite the commutation relations of Eq. 4.9 as

$$[\hat{r}_j, \hat{r}_k] = \mathrm{i}\,\Omega_{jk}, \qquad (j, k = 1, \ldots, 2M), \tag{4.11}$$

where Ω_{jk} are the elements of the matrix $\boldsymbol{\Omega}$:

$$\boldsymbol{\Omega} = \bigoplus_{i=1}^{M} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{4.12}$$

which is called the *symplectic form*.

We have seen that the parameterisation of the modes is determined by the boundary conditions in Eq. (4.1), i.e. by the physical conditions of the system (for instance the presence of mirrors or waveguides). We have mentioned that, for a cubical volume with period boundary conditions (see Eq. (4.4)), the index k parameterises four indices, n_1, n_2, n_3 and λ. One could choose a different parameterisation, like one with two indeces n and λ. In that case, we need to substitute the mode operators $\hat{a}_k$ and $\hat{a}_k^\dagger$ with $\hat{a}_{n;\lambda}$ and $\hat{a}_{n;\lambda}^\dagger$, and the commutation relation of Eq. (4.6) with

$$\left[\hat{a}_{n;\lambda}, \hat{a}_{m;\lambda'}\right] = \left[\hat{a}_{n;\lambda}^\dagger, \hat{a}_{m;\lambda'}^\dagger\right] = 0, \qquad \left[\hat{a}_{n;\lambda}, \hat{a}_{m;\lambda'}^\dagger\right] = \delta_{nm}\delta_{\lambda\lambda'}. \tag{4.13}$$

In the following, unless otherwise specified (see Sec. 7.4), we consider only a single index.

4.1.2 Fock Basis

Let us first consider a single mode, with mode operators $\hat{a}$ and $\hat{a}^\dagger$, and define $\hat{N} := \hat{a}^\dagger\hat{a}$. The mode operators are not Hermitian ($\hat{a} \neq \hat{a}^\dagger$) because of the CCRs (see Eq. (4.6)). However, the operator $\hat{N}$ is Hermitian and positive semidefinite, being the product of an operator with its

adjoint (see Theorem 2.34). Therefore, it admits an orthogonal set of eigenstates belonging to non-negative eigenvalues. Moreover, for any eigenstate $|n\rangle$ with eigenvalue n, we see that $\hat{a}\,|n\rangle$ and $\hat{a}^\dagger\,|n\rangle$ are also eigenstates of $\hat{N}$ with eigenvalues $n-1$ and $n+1$, respectively:

$$\hat{a}^\dagger\hat{a}\,(\hat{a}\,|n\rangle) = \left(\hat{a}\hat{a}^\dagger - 1\right)\hat{a}\,|n\rangle = (n-1)\hat{a}\,|n\rangle\,. \tag{4.14}$$

$$\hat{a}^\dagger\hat{a}\left(\hat{a}^\dagger\,|n\rangle\right) = \hat{a}^\dagger\left(\hat{a}\hat{a}^\dagger + 1\right)|n\rangle = (n+1)\hat{a}^\dagger\,|n\rangle\,. \tag{4.15}$$

The eigenvalues of $\hat{N}$ cannot be negative, therefore it must exists a state $|0\rangle$, referred ad *vacuum* or *ground state*, such that $\hat{a}\,|0\rangle = 0$.

Definition 4.3 (Fock states)**.** The eigenstates of $\hat{N} = \hat{a}^\dagger\hat{a}$ are called the *Fock* (*number*) *states* and are denoted by $\{|n\rangle\}$. The Fock states are obtained by repeatedly applying $\hat{a}^\dagger$ to the vacuum state $|0\rangle$ (see Eq. (4.15)), i.e.

$$|n\rangle := \frac{(a^\dagger)^n}{\sqrt{n!}}\,|0\rangle\,. \tag{4.16}$$

Therefore the eigenvalues of $\hat{N}$ are the natural number $n \in \mathbb{N}_0$.

The operators $\hat{a}$ and $\hat{a}^\dagger$ act on the Fock states as

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \quad \text{and} \quad \hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{4.17}$$

Let us now consider a multimode system. By using the rules for the commutator of products of functions (see Def. 2.23), we can prove that any two operators $\hat{N}_j$ and $\hat{N}_k$ commute. Hence, $\hat{N}_k$ also commutes with the M-mode Hamiltonian $\hat{H} = \sum_{k=1}^{M} \hbar\omega\,(\hat{N}_k + 1/2)$. The eigenstates of $\hat{H}$ are therefore tensor products of the Fock states $|n_k\rangle$ over all the M modes, i.e. $|n_1, n_2, \ldots, n_M\rangle := |n_1\rangle\,|n_2\rangle \ldots |n_M\rangle$, and the eigenvalues read:

$$\hat{H}\,|n_1, n_2, \ldots, n_M\rangle = \sum_k \left(n_k + \frac{1}{2}\right)\hbar\omega_k\;|n_1, n_2, \ldots, n_M\rangle\,. \tag{4.18}$$

The ground state of the Hamiltonian, $|0\rangle = |0_1, 0_2, \ldots, 0_M\rangle$ is associated with the minimal vacuum energy $E_V = \sum_{k=1}^{M} \frac{1}{2}\,\hbar\omega_k$. The energy of a Fock state $|n_1, n_2, \ldots, n_M\rangle$ thus reads:

$$E_{n_1,n_2,\ldots,n_M} = E_V + \sum_k n_k\,\hbar\omega_k. \tag{4.19}$$

Therefore, for each mode k the state $|n_k\rangle$ describe a system of n_k particles, called *photons*, each of energy $\hbar\omega_k$. The ground state is called *vacuum* because it contains no particles. The operator $\hat{a}_k$ acts on $|n_k\rangle$ by removing a photon, and is thus called the *annihilation* operator for the mode k. Analogously, $\hat{a}_k^\dagger$ is called the *creation* operator for the mode k because it adds a photon. Finally, the operator $\hat{N}_k$ is the observable associated with the *occupation number in mode* k and $\hat{N} = \sum_k \hat{N}_k$ is associated with the *total number of photons*.

4.1.3 Coherent Basis

Definition 4.4. Let $\mathcal{H}$ be a single-mode Hilbert space, with mode operators $\hat{a}$ and $\hat{a}^\dagger$. The *displacement*, or *Weyl*, *operator* $\hat{D}(\alpha)$ is the operator on $\mathcal{H}$ defined as

$$\hat{D}(\alpha) := \exp[\alpha\,\hat{a}^\dagger - \alpha^*\,\hat{a}], \tag{4.20}$$

for $\alpha \in \mathbb{C}$. The displacement operator is unitary and satifies:

$$\hat{D}^{-1}(\alpha) = \hat{D}^{\dagger}(\alpha) = \hat{D}(-\alpha). \tag{4.21}$$

By using the *Hadamard's lemma* [WM07],

$$e^{\hat{A}}\,\hat{B}\,e^{-\hat{A}} = \hat{B} + [\hat{A},\hat{B}] + \frac{1}{2!}\,[\hat{A},[\hat{A},\hat{B}]] + \ldots \tag{4.22}$$

we can write

$$\hat{D}^{\dagger}(\alpha)\,\hat{a}\,\hat{D}(\alpha) = \hat{a} + \alpha, \quad \text{and} \quad \hat{D}^{\dagger}(\alpha)\,\hat{a}^{\dagger}\,\hat{D}(\alpha) = \hat{a}^{\dagger} + \alpha^{*}. \tag{4.23}$$

As a consequence of Eqs. (4.21) and (4.23), one finds that the state $|\alpha\rangle := \hat{D}(\alpha)\,|0\rangle$ is an eigenstate of the annihilation operator $\hat{a}$ belonging to the the eigenvalue $\alpha \in \mathbb{C}$:

$$\hat{a}\hat{D}(\alpha)\,|0\rangle = \hat{D}(\alpha)\hat{D}^{\dagger}(\alpha)\,\hat{a}\hat{D}(\alpha)\,|0\rangle = \hat{D}(\alpha)(\hat{a}+\alpha)\,|0\rangle = \alpha\hat{D}(\alpha)\,|0\rangle\,. \tag{4.24}$$

The states $|\alpha\rangle := \hat{D}(\alpha)\,|0\rangle$ for $\alpha \in \mathbb{C}$ are called *coherent states*. Their expansion in terms of the number states $|n\rangle$ reads:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{4.25}$$

A proof of Eq. (4.25) is given in [Ser17]. The number of photons in a coherent state is therefore not fixed. The photon number distribution in a coherent state $|\alpha\rangle$, denoted by $p_{\alpha}(n)$ is a *Poisson distribution*,

$$p_{\alpha}(n) = |\,\langle n|\alpha\rangle\,|^2 = \frac{|\alpha|^{2n}\,e^{-|\alpha|^2}}{n!}, \tag{4.26}$$

with mean photon number

$$\bar{n} := \langle\alpha|\hat{a}^{\dagger}\hat{a}|\alpha\rangle = |\alpha|^2. \tag{4.27}$$

From the Baker-Campbell-Hausdorff formula (see Eq. (2.31)), it follows that the coherent states are not orthogonal:

$$\langle\beta|\alpha\rangle = \langle 0|\hat{D}^{\dagger}(\beta)\hat{D}(\alpha)|0\rangle = \exp\left[-\frac{1}{2}\,(|\alpha|^2 + |\beta|^2) + \alpha\beta^{*}\right], \tag{4.28}$$

This result, together with Eq. (4.25), implies that the coherent states form a *overcomplete* system, i.e. a system that is complete and remains complete after removal of any one element [GAF10]:

$$\frac{1}{\pi}\int_{\mathbb{R}^2} d^2\alpha\,|\alpha\rangle\,\langle\alpha| = \sum_{n}\,|n\rangle\,\langle n| = \hat{I}\,, \tag{4.29}$$

with $d^2\alpha = d\,Re[\alpha]\,d\,Im[\alpha]$. A remarkable property of coherent states is that they are *minimum uncertainty states*. The Heisenberg uncertainty relation (see Theorem 3.1) for the quadratures operators $\hat{q}$ and $\hat{p}$ reads:

$$\Delta(\hat{q})\,\Delta(\hat{p}) \geq \frac{|\mathrm{Tr}(\rho\,[\hat{q},\hat{p}])|}{2} = \frac{1}{2}, \tag{4.30}$$

where $\Delta(\hat{q})$ and $\Delta(\hat{p})$ are the standard deviations (see Eq. (3.12)) of $\hat{q}$ and $\hat{p}$, respectively. For a coherent state α, it holds [WM07]:

$$\Delta_\alpha(\hat{q}) = \sqrt{\frac{1}{2}}, \quad \text{and} \quad \Delta_\alpha(\hat{p}) = \sqrt{\frac{1}{2}}. \tag{4.31}$$

Hence, $\Delta_\alpha(\hat{q})\,\Delta_\alpha(\hat{p}) = 1/2$, with $\Delta_\alpha(\hat{q}) = \Delta_\alpha(\hat{p})$.

Let q and p denote the eigenvalues of $\hat{q}$ and $\hat{p}$, respectively. The relation between $\hat{a}$, $\hat{q}$ and $\hat{p}$, $\hat{a} = (\hat{q} + i\hat{p})/\sqrt{2}$ (see Eq. (4.8)) translates into an analougous relation for their eigenvalues:

$$\alpha = \frac{q + \mathrm{i}\, p}{\sqrt{2}}. \tag{4.32}$$

Defining the vector of eigenvalues of $\hat{q}$ and $\hat{p}$, $\boldsymbol{r} := (q, p)^T$ (not to be confused with the vector of operators $\hat{\boldsymbol{r}} = (\hat{q}, \hat{p})^T$), the displacement operator (see Eq. (4.20)) can be rewritten as:

$$\hat{D}(\alpha) = \hat{D}(\boldsymbol{r}) = e^{-\mathrm{i}(q\hat{p} - p\hat{q})} = e^{-i\boldsymbol{r}^T\, \boldsymbol{\Omega}\hat{\boldsymbol{r}}}, \tag{4.33}$$

where $\boldsymbol{\Omega}$ is the symplectic form (see Eq. (4.12)). The form in Eq. (4.33) is sometimes referred to as the *real displacement operator*, in contrast to the *complex displacement operator* of Eq. (4.20).

We conclude this subsection by considering the multimode case. The composite Hilbert space is a tensor product of single-mode Hilbert spaces (see Eq. (4.10)), and the mode operators for different modes j and k, commute (see Eq. (4.6)). Hence, the M-mode displacement operator is defined as a tensor product of single-mode displacement operators, i.e.

$$\hat{D}(\alpha_1, \ldots \alpha_M) := \exp\left[\sum_{j=1}^{M} (\alpha_j\, \hat{a}_j^\dagger - \alpha_j^*\, \hat{a}_j)\right] = \bigotimes_{k=1}^{M} \hat{D}_k(\alpha_k)\,, \tag{4.34}$$

and the M-mode coherent states are defined as tensor products of single-mode coherent states, i.e.

$$|\alpha_1, \ldots, \alpha_M\rangle := |\alpha_1\rangle\, |\alpha_2\rangle \ldots |\alpha_M\rangle\,. \tag{4.35}$$

The real displacement operator is still defined as in Eq. (4.33), by writing $\boldsymbol{r}$ and $\hat{\boldsymbol{r}}$ as vectors of the $2M$ eigenvalues and operators, i.e. $\boldsymbol{r} := (q_1, p_1, q_2, p_2, \ldots, q_M, p_M)^T$ and $\hat{\boldsymbol{r}} := (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_M, \hat{p}_M)^T$.

4.1.4 Phase Space Representations

The study of infinite-dimensional Hilbert spaces can be highly difficult. We shall see, in this subsection, that an M-mode quantum system admits simpler representations in the $2M$-dimensional *phase space*, which is the real space of the eigenvalues r_i of the quadrature operators $\hat{r}_i$ ($i = 1, 2, \ldots 2M$).

Theorem 4.5 (Fourier-Weyl transform)**.** *Let $\hat{D}(\boldsymbol{\alpha})$ and $\hat{D}(\boldsymbol{r})$, with $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_M)^T$ and $\boldsymbol{r} = (q_1, p_1, q_2, p_2 \ldots, q_M, p_M)^T$, be the complex and real displacement operators (see Eqs.* (4.20) *and* (4.33)*) on a Hilbert space $\mathcal{H} = \bigotimes_{k=1}^{M} \mathcal{H}_k$, respectively. Any operator $\hat{A}$ on $\mathcal{H}$ can be expanded as:*

$$\hat{A} = \frac{1}{\pi^M} \int_{\mathbb{R}^{2M}} d^2\boldsymbol{\alpha}\, \mathrm{Tr}\left[\hat{D}(\boldsymbol{\alpha})\hat{A}\right] \hat{D}(-\boldsymbol{\alpha}) = \frac{1}{(2\pi)^M} \int_{\mathbb{R}^{2M}} d\boldsymbol{r}\, \mathrm{Tr}\left[\hat{D}(\boldsymbol{r})\hat{A}\right] \hat{D}(-\boldsymbol{r}), \tag{4.36}$$

where $d^2\boldsymbol{\alpha} = d^2\alpha_1 d^2\alpha_2 \dots d^2\alpha_M$ *and* $d\boldsymbol{r} = d\,q_1, d\,p_1, d\,q_2, d\,p_2, \dots, d\,q_M, d\,p_M$*. This expansion is refered to as the* Fourier-Weyl transform *of* $\hat{A}$*.*

A proof of this theorem is given in [Ser17].

Definition 4.6 (Characteristic function)**.** Let $\hat{D}(\boldsymbol{\alpha})$ and $\hat{D}(\boldsymbol{r})$, with $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_M)^T$ and $\boldsymbol{r} = (q_1, p_1, q_2, p_2 \dots, q_M, p_M)^T$, be the complex and real displacement operators (see Eqs. (4.20) and (4.33)) on a Hilbert space $\mathcal{H} = \bigotimes_{k=1}^{M} \mathcal{H}_k$, respectively. The *characteristic function* of a density operator ρ is a function $\chi(\boldsymbol{\alpha}) = \chi(\boldsymbol{r})$ that is defined as:

$$\chi(\boldsymbol{\alpha}) := \mathrm{Tr}[\hat{D}(\boldsymbol{\alpha})\,\rho] = \mathrm{Tr}[\hat{D}(\boldsymbol{r})\,\rho] =: \chi(\boldsymbol{r}), \tag{4.37}$$

where $\hat{D}(\boldsymbol{\alpha})$ and $\hat{D}(\boldsymbol{r})$ are the complex and real displacement operators (see Eqs. (4.20) and (4.33)), respectively.

Therefore, the Fourier-Weyl transform (see Theorem 4.5) of ρ reads:

$$\rho = \frac{1}{\pi^M} \int_{\mathbb{R}^{2M}} d^2\boldsymbol{\alpha}\, \chi(\boldsymbol{\alpha}) \hat{D}(-\boldsymbol{\alpha}) = \frac{1}{(2\pi)^M} \int_{\mathbb{R}^{2M}} d\boldsymbol{r}\, \chi(\boldsymbol{r}) \hat{D}(-\boldsymbol{r}). \tag{4.38}$$

Hence, both $\chi(\boldsymbol{\alpha})$ and $\chi(\boldsymbol{r})$ provide full information about the state ρ. The conditions $\mathrm{Tr}[\rho] = 1$ and $\rho = \rho^\dagger$ translate into [Ser17]:

$$\chi(0) = 1, \quad \text{and} \quad \chi(\boldsymbol{\alpha}) = \chi^*(-\boldsymbol{\alpha}) = \chi(-\boldsymbol{r}) = \chi(\boldsymbol{r}). \tag{4.39}$$

Definition 4.7 (s-ordered characteristic function)**.** Let $s \in \{-1, 0, 1\}$. The *s-ordered characteristic function* of a quantum state ρ is defined from the characteristic function by:

$$\chi_s(\boldsymbol{\alpha}) := \mathrm{Tr}[\hat{D}(\boldsymbol{\alpha})\,\rho]\, e^{\frac{s}{2}\|\boldsymbol{\alpha}\|^2}. \tag{4.40}$$

The functions $\chi_1(\boldsymbol{\alpha})$ and $\chi_{-1}(\boldsymbol{\alpha})$ are called *normally* and *anti-normally ordered* characteristic functions, respectively. The function $\chi_0(\boldsymbol{\alpha})$, which is nothing but $\chi(\boldsymbol{\alpha})$, may be referred to as the *symmetrically ordered* characteristic function, but it is usually simply called *the* characteristic function. These names are a consequence of the following theorem, whose proof is given in [Ser17].

Theorem 4.8. *Let* $\langle \hat{a}_j^{\dagger m} \hat{a}_k^n \rangle_{\pm 1}$ *denote the expectation values of the product of* $m\ \hat{a}_j^\dagger$ *and* $n\ \hat{a}_k$*, where all the creation operators are on the left and all the annihilation operators are on the right (*normal ordering*) or vice versa (*anti-normal ordering*). Let* $\langle \hat{a}_j^{\dagger m} \hat{a}_k^n \rangle_0$ *denote a sum of all symmetric products of* $m\ \hat{a}_j^\dagger$ *and* $n\ \hat{a}_k$ *in all possible orders (*symmetric ordering*). Then it holds:*

$$\langle \hat{a}_j^{\dagger m} \hat{a}_k^n \rangle_s = \left(\frac{\partial}{\partial \alpha_j} \right)^m \left(-\frac{\partial}{\partial \alpha_k^*} \right)^n \chi_s(\boldsymbol{\alpha})\big|_{\boldsymbol{\alpha}=0}. \tag{4.41}$$

Definition 4.9 (s-ordered quasi-probability distributions)**.** The *s-ordered quasi-probability distribution* of ρ is defined as the Fourier transform of the corresponding s-ordered characteristic function (see Def.4.7):

$$W_s(\boldsymbol{\alpha}) = \frac{1}{\pi^{2M}} \int_{\mathbb{R}^{2M}} d^2\boldsymbol{\beta}\, \chi_s(\boldsymbol{\beta})\, e^{\boldsymbol{\alpha}^T \cdot \boldsymbol{\beta}^* - \boldsymbol{\alpha}^\dagger \boldsymbol{\beta}}. \tag{4.42}$$

They are called quasi-probability distributions because they are normalised to 1:

$$\int_{\mathbb{R}^{2M}} d^2\boldsymbol{\alpha} W_s(\boldsymbol{\alpha}) = \chi_s(0) = \mathrm{Tr}\rho = 1, \tag{4.43}$$

but they are not generally positive. Eq. 4.41 can be expressed in terms of the quasi-probabilities as [Ser17]:

$$\langle \hat{a}_j^{\dagger m} \hat{a}_k^n \rangle_s = \int_{\mathbb{R}^{2M}} d^2\boldsymbol{\alpha} W_s(\boldsymbol{\alpha}) \alpha_j^{*m}\, \alpha_k^n. \tag{4.44}$$

Let us now individually examine $W_s(\alpha)$ for $s = 1, 0, -1$. They were historically introduced in different times for different purposes. Therefore, each one of them has its own name and symbol.

Glauber-Sudarshan P function [Gla63; Sud63]: The normally ordered quasi-probability distribution is called the *Glauber-Sudarshan P function* and is indicated with $P(\boldsymbol{\alpha})$. It coincides with the expansion of ρ over the complete set of coherent states, i.e.

$$\rho = \int_{\mathbb{R}^{2M}} d^2\boldsymbol{\alpha}\, P(\boldsymbol{\alpha})\ |\alpha_1, \alpha_2, \ldots, \alpha_M\rangle \langle \alpha_1, \alpha_2, \ldots, \alpha_M| \,. \tag{4.45}$$

This function can be negative and also highly singular. The non-positivity of the P function has been historically considered as a marker of *non-classicality* [Dod02].

Wigner function [Wig32]: The symmetrically ordered quasi-probability distribution is called the *Wigner function* and is simply denoted by $W(\boldsymbol{\alpha})$. It can be negative, but it is always regular. By substituting α_k with $(q_k + \mathrm{i}\, p_k)/\sqrt{2}$ in Eq. (4.42), we obtain $W(\boldsymbol{r}) = W(\boldsymbol{\alpha})$, which satisfies [Ser17]:

$$W(\boldsymbol{r}) = \left(\frac{2}{\pi}\right)^M \int_{\mathbb{R}^M} d\boldsymbol{z}\, e^{2\mathrm{i}\, \boldsymbol{p}^T \cdot \boldsymbol{z}}\ \langle \boldsymbol{q} + \boldsymbol{z}|\rho|\boldsymbol{q} - \boldsymbol{z}\rangle \,, \tag{4.46}$$

where $|\boldsymbol{q} \pm \boldsymbol{z}\rangle = |q_1 \pm z_1\rangle\, |q_2 \pm z_2\rangle \ldots |q_M \pm z_M\rangle$ and $|q_k \pm z_k\rangle$ is the eigenstate of $\hat{q}_k$ with eigenvalue $q_k \pm z_k \in \mathbb{R}$. Moreover, the Wigner functions allows us to calculate the probability of measuring one of the quadratures [Ser17]:

$$\frac{1}{2^{2M-1}} \int_{\mathbb{R}^{2M-1}} dr_1 \ldots dr_{k-1} dr_{k+1} \ldots dr_M\, W(\boldsymbol{r}) = \langle r_k|\rho|r_k\rangle \,, \tag{4.47}$$

where $|r_k\rangle$ is the eigenstate of $\hat{r}_k$ (which represents either $\hat{q}_k$ or $\hat{p}_k$ depending from k) with the eigenvalue being the k-th component of $\boldsymbol{r}$.

Husimi Q function [Hus40]: The anti-normally ordered quasi-probability distribution is called *Husimi Q function* and is denoted by $Q(\boldsymbol{\alpha})$. It can be written as

$$Q(\boldsymbol{\alpha}) = \frac{1}{\pi^M}\ \langle \alpha_1, \alpha_2, \ldots, \alpha_M|\rho|\alpha_1, \alpha_2, \ldots, \alpha_M\rangle \,. \tag{4.48}$$

Differently from the other two distributions, the Q function is always positive and regular.

4.2 Gaussian States

Definition 4.10 (Gaussian states [Ser17])**.** A *Gaussian state* ρ_G is a quantum state whose characteristic function $\chi_G(\boldsymbol{r})$ is Gaussian, i.e.

$$\chi_G(\boldsymbol{r}) = \exp\left[-\frac{1}{4}\,\mathbf{r}^{\mathrm{T}}\,\mathbf{\Omega}^{\mathbf{T}}\,\mathbf{V}\,\mathbf{\Omega}\,\mathbf{r} + \mathrm{i}\,\mathbf{d}^{\mathrm{T}}\,\mathbf{\Omega}\mathbf{r}\right]. \tag{4.49}$$

Here, $\boldsymbol{d}$ is the real vector of first moments of $\boldsymbol{r}$ in the state ρ_G and is called the *displacement vector* of ρ_G. The k-th component of $\boldsymbol{d}$, denoted by d_k, reads:

$$d_k := \langle \hat{r}_k \rangle = \mathrm{Tr}\,[\hat{r}_k\,\rho], \tag{4.50}$$

The matrix $\boldsymbol{V}$ is the real, symmetric and positive-definite matrix of second moments of of $\boldsymbol{r}$ in the state ρ_G and is called the *covariance matrix* of ρ_G. The (j,k)-th entry of $\boldsymbol{V}$, denoted by V_{jk}, reads:

$$V_{jk} := \langle \hat{r}_j\,\hat{r}_k + \hat{r}_k\,\hat{r}_j \rangle - 2\,d_j\,d_k. \tag{4.51}$$

The displacement vector and covariance matrix are defined for all CV quantum states and are always obtainable from the characteristic function by using Eq. (4.41) and writing $\hat{a}_k = (\hat{q}_k + \mathrm{i}\hat{p}_k)/\sqrt{2}$. We are going to see, in the following, that there are notable properties that only depend on these two moments for all CV quantum states. However Gaussian states are the only states to be fully characterised by their displacement vector and covariance matrix. From Eqs. (4.49) and (4.42), it follows that the Wigner's function of a Gaussian state ρ_G reads [ARL14]:

$$W_G(\boldsymbol{r}) = \left(\frac{2}{\pi}\right)^M \frac{1}{\sqrt{\det \boldsymbol{V}}}\, e^{-(\boldsymbol{r}-\boldsymbol{d})^T\,\boldsymbol{V}^{-1}\,(\boldsymbol{r}-\boldsymbol{d})}. \tag{4.52}$$

Pure Gaussian states are the only pure states with positive Wigner function [Hud74; LB95].

Theorem 4.11 (Robertson-Schrödinger uncertainty relation [SMD94])**.** *The covariance matrix (see Eq.* (4.51)*)* $\boldsymbol{V}$ *of any CV quantum state* ρ *must satisfy*

$$\boldsymbol{V} + \mathrm{i}\mathbf{\Omega} \geq 0, \tag{4.53}$$

where $\mathbf{\Omega}$ *is the symplectic form (see Eq.* (4.12)*). For Gaussian states, this condition is also sufficient [SMD94]. Namely, for any* $2M \times 2M$ *real, symmetric and positive definite matrix* $\boldsymbol{V}$ *that satisfies Eq.* (4.53)*, there exist* M*-mode Gaussian states whose covariance matrix is* $\boldsymbol{V}$*.*

In phase space. the tensor products are replaced by direct sums.

Theorem 4.12 (Composition of Gaussian states)**.** *Let* ρ_A *and* ρ_B *be Gaussian states with displacement vectors (covariance matrices)* $\boldsymbol{d}_A$ *and* $\boldsymbol{d}_B$ *(*$\boldsymbol{V}_A$ *and* $\boldsymbol{V}_B$*), respectively. Then the displacement vector* $\boldsymbol{d}_{AB}$ *and covariance matrix* $\boldsymbol{V}_{AB}$ *of the bipartite state* $\rho_{AB} = \rho_A \otimes \rho_B$ *read:*

$$\boldsymbol{d}_{AB} = \boldsymbol{d}_A \oplus \boldsymbol{d}_B = \begin{pmatrix} \boldsymbol{d}_A \\ \boldsymbol{d}_B \end{pmatrix}, \qquad \boldsymbol{V}_{AB} = \boldsymbol{V}_A \oplus \boldsymbol{V}_B = \begin{pmatrix} \boldsymbol{V}_A & 0 \\ 0 & \boldsymbol{V}_B \end{pmatrix}. \tag{4.54}$$

Theorem 4.13 (Partial trace of Gaussian states)**.** *Let*

$$\boldsymbol{d}_{AB} = \begin{pmatrix} \boldsymbol{d}_A \\ \boldsymbol{d}_B \end{pmatrix}, \qquad \boldsymbol{V}_{AB} = \begin{pmatrix} \boldsymbol{V}_A & \boldsymbol{\Delta}_{AB} \\ \boldsymbol{\Delta}_{AB}^T & \boldsymbol{V}_B \end{pmatrix}, \tag{4.55}$$

be the displacement vector and covariance matrix of a bipartite quantum state ρ_{AB}, respectively. Here $\boldsymbol{d}_{AB}$ and $\boldsymbol{V}_{AB}$ are given in block form, with $\boldsymbol{d}_A, \boldsymbol{d}_B$ being 2-dimensional vectors, and $\boldsymbol{V}_A, \boldsymbol{V}_B, \boldsymbol{\Delta}_{AB}$ being 2×2 real matrices such that $\boldsymbol{V}_{AB}$ is symmetric and satisfies Eq. (4.53)*. Then, $\boldsymbol{d}_A$ and $\boldsymbol{V}_A$ are the displacement vector and covariance matrix of $\rho_A = \mathrm{Tr}_B[\rho_{AB}]$, respectively. Analogously, $\boldsymbol{d}_B$ and $\boldsymbol{V}_B$ are the displacement vector and covariance matrix of $\rho_B = \mathrm{Tr}_B[\rho_{AB}]$, respectively.*

Theorems 4.12 and 4.13 are proven in [Ser17], and follows from the definition of Gaussian characteristic functions (see Eq. (4.49)) and the Fourier-Weyl transform (see Eq. (4.36)). The theorems also hold for any number of modes. An M mode quantum state is a tensor product of single-mode states, therefore we can write the $2M$-dimensional displacement vector and the $2M \times 2M$ covariance matrix of any M-mode Gaussian state as:

$$\boldsymbol{d} = \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \\ \vdots \\ \boldsymbol{d}_M \end{pmatrix}, \qquad \boldsymbol{V} = \begin{pmatrix} \boldsymbol{V}_1 & \boldsymbol{\Delta}_{12} & \dots & \boldsymbol{\Delta}_{1M} \\ \boldsymbol{\Delta}_{12}^T & \boldsymbol{V}_2 & \dots & \boldsymbol{\Delta}_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\Delta}_{1M}^T & \boldsymbol{\Delta}_{2M}^T & \dots & \boldsymbol{V}_M \end{pmatrix}, \tag{4.56}$$

where $\boldsymbol{d}_m$ are 2-dimensional vectors, and $\boldsymbol{V}_m$ and $\boldsymbol{\Delta}_{mm'}$ are 2×2 real matrices. In particular, $\boldsymbol{d}_m$ ($\boldsymbol{V}_m$) corresponds to the displacement vector (the covariance matrix) of the reduced state $\rho_m = \mathrm{Tr}_{\boldsymbol{m}\setminus m}[\,\rho\,]$ after tracing out all modes but the m-th, while $\boldsymbol{\Delta}_{mm'}$ is related to the correlations between the modes m and m'. Using Eq. (4.56), we can derive a formula for the average photon number in an M-mode Gaussian state,

$$\langle \hat{N} \rangle = \sum_{k=1}^{n} \langle \hat{N}_k \rangle = \sum_{k=1}^{M} \frac{1}{4} \left(\mathrm{Tr}[\boldsymbol{V}_k] + 2|\boldsymbol{d}_k|^2 - 2 \right), \tag{4.57}$$

where $\langle \hat{N}_k \rangle$ is the average occupation number of the k-th mode. This expression can be obtained by writing $\mathrm{Tr}[\boldsymbol{V}_k]$ in terms of Eq. (4.51) and the mode operators $\hat{a}_k$ and $\hat{a}_k^\dagger$,

$$\begin{aligned} \mathrm{Tr}[\boldsymbol{V}_k] &= 2\langle \hat{q}_k^2 \rangle + 2\langle \hat{p}_k^2 \rangle - 2\langle \hat{q}_k \rangle^2 - 2\langle \hat{p}_k \rangle^2 = \langle (\hat{a}_k + \hat{a}_k^\dagger)^2 \rangle - \langle (\hat{a}_k - \hat{a}_k^\dagger)^2 \rangle - 2|\boldsymbol{d}_k|^2 \\ &= 2 + 4\langle \hat{a}_k^\dagger \hat{a}_k \rangle - 2|\boldsymbol{d}_k|^2, \end{aligned} \tag{4.58}$$

and then setting $\langle \hat{N} \rangle = \sum_{k=1}^{M} \langle \hat{a}_k^\dagger \hat{a}_k \rangle$. Note that this formula holds regardless of the presence of off-diagonal terms in the covariance matrix. Moreover, Eq. (4.57) remains valid for non-Gaussian states but in this case $\boldsymbol{V}_k$ and $\boldsymbol{d}_k$ are not a reduced covariance matrix and displacement vector.

Theorem 4.14 (Williamson's theorem [Wil36])**.** *Any covariance matrix $\boldsymbol{V}$ (see Eq.* (4.51)*) admits a decomposition:*

$$\boldsymbol{V} = \boldsymbol{S}^T \boldsymbol{D}\, \boldsymbol{S}, \tag{4.59}$$

where $\boldsymbol{S}$ is a symplectic matrix*, i.e. a real matrix that satisfies*

$$\boldsymbol{S}^T \boldsymbol{\Omega}\, \boldsymbol{S} = \boldsymbol{\Omega}, \tag{4.60}$$

with $\boldsymbol{\Omega}$ being the symplectic form (see Eq. (4.12)*), and $\boldsymbol{D}$ being a diagonal matrix,*

$$\boldsymbol{D} = \mathit{diag}\left[\nu_1, \nu_1, \ldots, \nu_M, \nu_M\right]. \tag{4.61}$$

which is called the normal form *of $\boldsymbol{V}$. The variables $\nu_k \geq 1$ are called the* symplectic eigenvalues *of $\boldsymbol{V}$.*

There are notable properties that, for Gaussian states, only depend on the symplectic eigenvalues.

Theorem 4.15 (Uncertainty of a Gaussian state [Wee+12])**.** *For an M-mode Gaussian state ρ_G with covariance matrix $\boldsymbol{V}$ and symplectic eigenvalues $\{\nu_k\}$ ($k = 1, 2, \ldots, M$), the Robertson-Schrödinger uncertainty relation (see Eq.* (4.53)*) can be restated as the following two conditions:*

$$\boldsymbol{V} \geq 0, \quad \textit{and} \quad \nu_k \geq 1 \quad \forall\, k. \tag{4.62}$$

Theorem 4.16 (Purity of a Gaussian state [Ser17])**.** *The purity (see Def. 3.7) $\mathrm{Tr}[\rho_G^2]$ of an M-mode Gaussian state ρ_G with covariance matrix $\boldsymbol{V}$ and symplectic eigenvalues $\{\nu_k\}$ ($k = 1, 2, \ldots, M$) reads:*

$$\mathrm{Tr}[\rho_G^2] = \frac{1}{\sqrt{\det \boldsymbol{V}}} = \frac{1}{\nu_1\, \nu_2 \ldots \nu_M}. \tag{4.63}$$

Pure states satisfy $\mathrm{Tr}[\rho_G^2] = 1$, i.e. $\det \boldsymbol{V} = 1$ and $\nu_k = 1$ for all k. Hence, pure Gaussian states saturate the Robertson-Schrödinger uncertainty relation (4.62)*.*

Theorem 4.17 (Entropy of a Gaussian state [HSH99])**.** *The von Neumann entropy (see Def. 3.17) of an M-mode Gaussian state ρ_G with symplectic eigenvalues $\{\nu_k\}$ ($k = 1, 2, \ldots, M$) reads:*

$$S(\rho_G) = \sum_{k=1}^{M} \left(\frac{\nu_k + 1}{2} \log \frac{\nu_k + 1}{2} - \frac{\nu_k - 1}{2} \log \frac{\nu_k - 1}{2} \right). \tag{4.64}$$

A feature of Gaussian states is that they attain the maximum von-Neumann entropy among all CV states having the same displacement vector and covariance matrix [HSH99].

4.2.1 Notable Gaussian States

Gaussian states are of paramount importance in quantum optics and continuous-variable quantum information. In this subsection, we review some relevant families of Gaussian states and one family of non-Gaussian states.

Fock States

We denote by $W_{|n\rangle}(q, p)$ the Wigner function of a generic single-mode Fock state $|n\rangle$ (see Sec. 4.1.2), which reads [Gro46]:

$$W_{|n\rangle}(q, p) = (-1)^n \frac{2}{\pi} e^{-(q^2+p^2)} L_n\left(2(q^2 + p^2)\right), \tag{4.65}$$

where $L_n(\cdot)$ denotes the n-th *Laguerre polynomial*:

$$L_n(x) := \frac{1}{n!} \left(\frac{d}{dx} - 1 \right)^n x^n. \tag{4.66}$$

For $n > 0$ the Laguerre polynomials are not Gaussian, therefore almost all Fock states $|n\rangle$ are not Gaussian. However, for $n = 0$, $L_0(x) = 1$ and the Wigner function becomes:

$$W_{|0\rangle}(q,p) = \frac{2}{\pi}\, e^{-q^2-p^2}. \tag{4.67}$$

Hence, the vacuum state is Gaussian. Its displacement vector and covariance matrix can be easily calculated by using Eqs. (4.50) and (4.51), respectively:

$$\boldsymbol{d}_{|0\rangle} = 0, \qquad \boldsymbol{V}_{|0\rangle} = \boldsymbol{I}, \tag{4.68}$$

where $\boldsymbol{I}$ is the 2×2 identity matrix. The displacement vector and covariance matrix of the M-mode vacuum state, $|0_1, 0_2, \ldots, 0_M\rangle$, then result by direct summing (see Theorem 4.12) the single-mode displacement vector and covariance matrix of Eq. (4.68).

Coherent States

We denote by $W_{|\alpha_0\rangle}(q,p)$ the Wigner function of a generic single-mode coherent state $|\alpha_0\rangle$, with $\alpha_0 = (q_0 + \mathrm{i}p_0)/\sqrt{2}$ (see Sec. 4.1.3). This function reads [WM07]:

$$W_{|\alpha_0\rangle}(q,p) = \frac{2}{\pi}\, \exp\left[-(q-q_0)^2 - (p-p_0)^2\right]. \tag{4.69}$$

Hence, coherent states are Gaussian. The displacement vector and covariance matrix of a coherent state $|\alpha_0\rangle$ can be calculated by using Eqs. (4.50) and (4.51), respectively:

$$\boldsymbol{d}_{|\alpha_0\rangle} = \begin{pmatrix} \sqrt{2}\,\mathrm{Re}\,\alpha_0 \\ \sqrt{2}\,\mathrm{Im}\,\alpha_0 \end{pmatrix}, \qquad \boldsymbol{V}_{|\alpha_0\rangle} = \boldsymbol{I}. \tag{4.70}$$

We have seen in Sec. 4.1.3 that the coherent states are minimum uncertainty states with equal standard deviation (thus variance) between the quadratures. The covariance matrix of all coherent states being equal to the identity is a restatement of that.

For an M-mode coherent state $|\alpha_1, \alpha_2, \ldots, \alpha_M\rangle$, the displacement vector and covariance matrix result by direct summing (see Theorem 4.12) the single-mode displacement vectors and covariance matrices of Eq. (4.70).

Squeezed States

Definition 4.18 (Single-mode squeezing operator)**.** Let $\xi = r\, e^{2\mathrm{i}\phi}$, with $r, \phi \in \mathbb{R}$. The single-mode *squeezing operator* is defined as:

$$\hat{Z}(\xi) = \exp\left[\frac{1}{2}\left(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2}\right)\right], \tag{4.71}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the mode operators of the system. The parameter $r = |\xi|$ is called the *squeezing parameter* (or *squeezing factor*).

For simplicity of notation, in the following $\phi = 0$ and thus $\xi = r$. The squeezing operator is unitary and satifies:

$$\hat{Z}^\dagger(r) = \hat{Z}^{-1}(r) = \hat{Z}(-r). \tag{4.72}$$

Using the Hadamard's lemma (see Eq. (4.22)), it follows that the action of a squeezing operator on the mode operators $\hat{a}$ and $\hat{a}^\dagger$ reads

$$\hat{Z}^\dagger(r)\hat{a}\hat{Z}(r) = \hat{a}\cosh r - \hat{a}^\dagger \sinh r, \qquad \hat{Z}^\dagger(r)\hat{a}^\dagger\hat{Z}(r) = \hat{a}^\dagger\cosh r - \hat{a}\sinh r. \tag{4.73}$$

The squeezing operator acting on the vacuum state generates a *squeezed (vacuum) state*:

$$|r\rangle := \hat{Z}(r)\,|0\rangle\,. \tag{4.74}$$

A squeezed vacuum state $|r\rangle$ is Gaussian because its Wigner function [WM07] is a Gaussian function:

$$W_{|r\rangle}(q,p) = \frac{2}{\pi}\,\exp\left[-(q\,e^{-r})^2 - (p\,e^{r})^2\right], \tag{4.75}$$

Its displacement vector and covariance matrix can be calculated by using Eqs. (4.50) and (4.51), respectively:

$$\boldsymbol{d}_{|r\rangle} = 0, \qquad \boldsymbol{V}_{|r\rangle} = \begin{pmatrix} e^{2r} & 0 \\ 0 & e^{-2r} \end{pmatrix}. \tag{4.76}$$

We see that $e^{2r}e^{-2r} = 1$, i.e. the squeezed vacuum states are minimum uncertainty states with different variances for $\hat{q}$ and $\hat{p}$.

Definition 4.19 (Two-mode squeezing operator)**.** Let $\xi = r\,e^{2\mathrm{i}\phi}$, with $r, \phi \in \mathbb{R}$. The *two-mode squeezing operator* is defined as

$$\hat{Z}_{AB}(\xi) = \exp\left[\frac{1}{2}\,(\xi^*\hat{a}_A\hat{a}_B - \xi\hat{a}_A^\dagger\hat{a}_B^\dagger)\right], \tag{4.77}$$

where $\hat{a}_A, \hat{a}_A^\dagger$ and $\hat{a}_B, \hat{a}_B^\dagger$ are the mode operators for the first and second mode, labelled by A and B, respectively.

Again, let $\xi = r$. When applied to the two-mode vacuum state, the operator $\hat{Z}_{AB}(r)$ generates the *two-mode squeezed vacuum state* (TMSVS):

$$|r_{AB}\rangle = \hat{Z}_{AB}(r)\,|0_A\rangle\,|0_B\rangle\,, \tag{4.78}$$

with Gaussian Wigner function [BL05]:

$$W_{|r_{AB}\rangle}(\boldsymbol{r}) = \frac{4}{\pi^2}\,\exp\left(-\frac{e^{-2r}}{2}\,[(q_A+q_B)^2 + (p_A-p_B)^2] - \frac{e^{2r}}{2}\,[(q_A-q_B)^2 + (p_A+p_B)^2]\right), \tag{4.79}$$

with $\boldsymbol{r} = (q_A, p_A, q_B, p_B)^T$. Its displacement vector and covariance matrix can be calculated by using Eqs. (4.50) and (4.51), respectively:

$$\boldsymbol{d}_{|r_{AB}\rangle} = 0, \qquad \boldsymbol{V}_{|r_{AB}\rangle} = \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \tag{4.80}$$

We shall see in Chap. 6 that the two-mode squeezed vacuum state is the Gaussian counterpart to the finite dimensional maximally entangled state (see Def. 3.4).

Thermal states

Theorem 4.20 (Thermal equilibrium [Bin+19])**.** *A quantum system with Hamiltonian $\hat{H}$ at thermal equilibrium at the temperature T is described by a quantum state $\tau_\beta(\hat{H})$ in the form:*

$$\tau_\beta(\hat{H}) = \frac{e^{-\beta\hat{H}}}{\mathrm{Tr}\left[e^{-\beta\hat{H}}\right]}, \tag{4.81}$$

where $\beta = 1/\kappa T$, with κ being the Boltzmann constant. The state $\tau_\beta(\hat{H})$ is called the thermal (Gibbs) state *of the system and maximise the von Neumann entropy (see Def. 3.17) $S(\rho)$ under the constraint of fixed average energy $E = \mathrm{Tr}[\rho\hat{H}]$.*

Let us consider a single-mode CV state with Hamiltonian $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + 1/2)$. This Hamiltonian admits a spectral decomposition (see Eq. (2.80)) on the Fock basis, which is the basis of eigenstates of $\hat{H}$ i.e. $\hat{H} = \hbar\omega\sum_n (n + 1/2)\,|n\rangle\langle n|$. Hence, Eq. (4.81) reads for this system:

$$\tau_\beta(\hat{H}) = \frac{e^{-\beta\hbar\omega\sum_n (n+1/2)|n\rangle\langle n|}}{\mathrm{Tr}\left[e^{-\beta\hbar\omega\sum_n (n+1/2)|n\rangle\langle n|}\right]} = \sum_n \frac{1}{(1+\bar{n})}\left(\frac{\bar{n}}{1+\bar{n}}\right)^n |n\rangle\langle n|\,, \tag{4.82}$$

where

$$\bar{n} = \frac{1}{\exp\left(\frac{\hbar\omega}{\kappa T}\right) - 1}, \tag{4.83}$$

is the average photon number for the *Bose-Einstein statistics* [Bos24]. The Gibbs state in Eq. (4.82), which we denote from now on by $\tau(\bar{n})$, is Gaussian since its Wigner function reads: [BL05]:

$$W_\tau(q,p) = \frac{2}{\pi(2\bar{n}+1)}\,\exp\left[-\frac{(q^2+p^2)}{2\bar{n}+1}\right], \tag{4.84}$$

and is therefore called the *Gaussian thermal state*. The displacement vector and covariance matrix of a Gaussian thermal state $\tau(\bar{n})$ read:

$$\boldsymbol{d}_\tau = 0, \qquad \boldsymbol{V}_\tau = (2\bar{n}+1)\boldsymbol{I}. \tag{4.85}$$

We note that the covariance matrix of $\tau(\bar{n})$ is in Williamson's normal form (see Theorem 4.14), with the symplectic eigenvalue being $\nu = (2\bar{n}+1)$. From Eq. (4.64), we obtain that the von Neumann entropy of $\tau(\bar{n})$ is

$$S(\rho) = (\bar{n}+1)\log(\bar{n}+1) - \bar{n}\log\bar{n}. \tag{4.86}$$

Because of Theorem 4.20, this is the maximum entropy that a Gaussian state ρ can have under the constraint of fixed average energy $E = \hbar\omega\bar{n} + 1/2$.

An M-mode thermal state is a tensor product of single-mode thermal states, i.e.

$$\tau_M(\bar{\boldsymbol{n}}) := \bigotimes_{k=1}^{M} \tau(\bar{n}_k), \tag{4.87}$$

where $\bar{\boldsymbol{n}} = (\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_M)$. This is a consequence of the M-mode Hamiltonian being a sum of single-mode Hamiltonians (see Eq. (4.7)).

4.3 Gaussian Unitaries

Let $\hat{U}$ be a unitary operator generated by a Hamiltonian $\hat{H}$ (see Postulate 3). In the following, for simplicity of notation, we set $\frac{(t_2-t_1)}{\hbar} = 1$ in Eq. (3.19) and write $\hat{U} = \exp(-\mathrm{i}\hat{H})$.

Theorem 4.21 (Gaussian unitaries [Sch86])**.** Gaussian unitaries *are unitary operators that preserve the Gaussianity of any Gaussian state. They are generated by Hamiltonians (see Postulate 3) that are at most* quadratic *in the mode operators, i.e.* $\hat{U}_G = \exp(-\mathrm{i}\hat{H}_Q)$ *with*

$$\hat{H}_Q := \sum_{k=1}^{M} \left(f_k \hat{a}_k^\dagger + f_k^* \hat{a}_k \right) + \sum_{k \geq l = 1}^{M} \left(g_{kl} \hat{a}_k^\dagger \hat{a}_l + g_{kl}^* \hat{a}_k \hat{a}_l^\dagger \right) + \sum_{k,l=1}^{M} \left(h_{kl} \hat{a}_k^\dagger \hat{a}_l^\dagger + h_{kl}^* \hat{a}_k \hat{a}_l \right), \tag{4.88}$$

where $f_k, g_k, h_k \in \mathbb{C}$ *and* M *is the number of modes in the system. The zero-th order terms is an unmeasurable global phase factor.*

In the following, we are going, to individually analyse the terms in Eq. (4.88). Before doing so, we consider that, in the Heisenberg picture (see Eq. (3.21)), a Gaussian unitary $\hat{U}_G$ transforms the Hamiltonian of an M-mode system (see Eq. (4.7)) as:

$$\hat{H} \to \hat{U}_G^\dagger \hat{H} \hat{U}_G = \sum_{k=1}^{M} \hbar\omega_k \left[(\hat{U}_G^\dagger \hat{a}_k \hat{U}_G)^\dagger (\hat{U}_G^\dagger \hat{a}_k \hat{U}_G) + \frac{1}{2} \right]. \tag{4.89}$$

Theorem 4.22 (Bogoliubov transformations [Bog58; Val58])**.** *A Gaussian unitary* $\hat{U}_G$*, generated by a Hamiltonian* $\hat{H}_Q$ *in the form of Eq.* (4.88)*, transforms the mode operators in the following way:*

$$\hat{a}_k \to \hat{b}_k := \hat{U}_G^\dagger \, \hat{a}_k \, \hat{U}_G = \sum_j \left(u_{kj} \, \hat{a}_j + v_{kj} \, \hat{a}_j^\dagger \right) + w_k, \tag{4.90}$$

where the coefficients $u_{kj}, v_{kj}, w_k \in \mathbb{C}$ *are called the* Bogoliubov coefficients *of the transformation* $\hat{U}_G$ *and satify:*

$$\sum_j \left(u_{kj} \, v_{k'j} - u_{k'j} \, v_{kj} \right) = 0, \qquad \sum_j \left(u_{kj} \, u_{k'j}^* - v_{kj} v_{k'j}^* \right) = \delta_{kk'}. \tag{4.91}$$

A proof of the theorem is given in [ARL14]. Eq. (4.90) follows from the Hadamard lemma (see Eq. (4.22)) and Eq. (4.91) follows from requiring the new mode operators $\hat{b}_k$ and $\hat{b}_k^\dagger$ to satisfy the bosonic commutation relations (see Eq. (4.6)).

By writing $\hat{a}_k = (\hat{q}_k + \mathrm{i}\,\hat{p}_k)/\sqrt{2}$, the Bogoliubov transformations of Eq. (4.90) induce an *affine transformation* on the vector of quadrature operators $\hat{\boldsymbol{r}} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_M, \hat{p}_M)^T$:

$$\hat{r} \to \boldsymbol{S}\hat{r} + \bar{\boldsymbol{d}}, \tag{4.92}$$

where $\bar{\boldsymbol{d}} \in \mathbb{R}^{2M}$ and $\boldsymbol{S}$ is a $2M \times 2M$ real matrix. The conditions in Eq. (4.91) are equivalent to require the matrix $\boldsymbol{S}$ to be symplectic (see Eq. (4.60)).

By using Eqs. (4.50) and (4.51), Eq. (4.92) is translated into an analogous equation for the displacement vector and the covariance matrix:

$$\begin{aligned} \boldsymbol{d} &\to \boldsymbol{S}\,\boldsymbol{d} + \bar{\boldsymbol{d}}; \\ \boldsymbol{V} &\to \boldsymbol{S}^T \boldsymbol{V}\, \boldsymbol{S}. \end{aligned} \tag{4.93}$$

We now see the physical meaning of the Williamson's theorem 4.14. According to Eq. (4.93), any M-mode Gaussian state ρ_G with displacement vector $\boldsymbol{d}$ and covariance matrix $\boldsymbol{V}$ is unitarily equivalent to an M-mode thermal state τ_M (see Sec. 4.2.1) with zero displacement vector and covariance matrix equal to $\boldsymbol{D} = \bigoplus_{k=1}^{M} \nu_k \boldsymbol{I}_2$, where $\boldsymbol{I}_2$ is the two-dimensional identity and ν_k is the k-th symplectic eigenvalue. The unitary that transforms ρ_G into τ_M is associated with $\bar{\boldsymbol{d}} = -\boldsymbol{d}$ and $\boldsymbol{S}$ being the symplectic matrix that diagonalises $\boldsymbol{V}$. Moreover, the symplectic eigenvalues can be written as $\nu_k = 2\bar{n}_k^{(th)} + 1$, where $\bar{n}_k^{(th)}$ is the number of thermal photons given by Eq. (4.83).

4.3.1 Linear Displacements

Let us now consider the linear term $\hat{H}_L := \sum_{k=1}^{M} \left(f_k \hat{a}_k^\dagger + f_k^* \hat{a}_k \right)$ in the Hamiltonian of Eq. (4.7). If we define $\alpha_k := -\mathrm{i}\, f_k$ and $\boldsymbol{\alpha} := (\alpha_1, \alpha_2, \ldots, \alpha_M)^T$, it is immediate to see that $\hat{D}(\boldsymbol{\alpha}) := \exp[-\mathrm{i}\hat{H}_L]$ is the multimode displacement operator defined in Eqs. (4.34) and (4.20). Comparing Eqs. (4.23) and (4.90), we see that the Bogoliubov coefficients associated with $\hat{D}(\boldsymbol{\alpha})$ read:

$$\begin{aligned} &u_{kj} = 1 \quad \text{and} \quad v_{kj} = 0, \quad \forall k, j; \\ &w_k = \alpha_k. \end{aligned} \tag{4.94}$$

Hence, $\hat{D}(\boldsymbol{\alpha})$ transforms the quadrature operators (see (4.92)) according to the affine transfomation $(\bar{\boldsymbol{d}}_{LD}, \boldsymbol{S}_{LD})$, with

$$\bar{\boldsymbol{d}}_{LD} = \sqrt{2} \begin{pmatrix} \mathrm{Re}(\alpha_1) \\ \mathrm{Im}(\alpha_1) \\ \vdots \\ \mathrm{Re}(\alpha_M) \\ \mathrm{Im}(\alpha_M) \end{pmatrix}, \qquad \boldsymbol{S} = \boldsymbol{I}_{2M}, \tag{4.95}$$

where $\boldsymbol{I}_{2M}$ is the $2M \times 2M$ identity matrix. Note that this result is consistent with the formula for the displacement vector and covariance matrix of a coherent state $|\alpha_k\rangle = \hat{D}_k(\alpha_k)\, |0_k\rangle$ (see Eq. (4.70)).

4.3.2 Phase Shifters and Beam Splitters

Let us now consider the first quadratic term $\hat{H}_{Q1} := \sum_{k \geq l=1}^{M} \left(g_{kl} \hat{a}_k^\dagger \hat{a}_l + g_{kl}^* \hat{a}_k \hat{a}_l^\dagger \right)$ in the Hamiltonian of Eq. (4.7). Depending on whether $k = l$ or $k > l$, this term describe the action of two distinct devices, of great importance in quantum optics: the *phase shifter* and the *beam splitter*.

With $k = l$, the Hamiltonian generates the unitary operator

$$\exp\left[-\mathrm{i} \sum_{k=1}^{M} g_{kk}\, \hat{a}_k^\dagger \hat{a}_k + g_{kl}^* \left(\hat{a}_k^\dagger \hat{a}_k + 1 \right) \right] = \bigotimes_{k=1}^{M} \exp\left(-\mathrm{i}\theta_k \hat{a}_k^\dagger \hat{a}_k \right), \tag{4.96}$$

where $\theta_k = 2\mathrm{Re}[g_{kk}] \in \mathbb{R}$ and we eliminated the unsmeasurable phase factor $e^{-\mathrm{i}\, g_{kl}^*}$. The unitary $\hat{R}_k(\theta_k) := \exp\left(-\mathrm{i}\theta_k \hat{a}_k^\dagger \hat{a}_k \right)$ acts on the k-th mode operator operator as:

$$\hat{R}_k^\dagger(\theta_k)\, \hat{a}_k\, \hat{R}_k(\theta_k) = e^{-\mathrm{i}\theta_k} \hat{a}_k, \tag{4.97}$$

and thus represents the action of a *phase shifter*. The Bogoliubov coefficients associated with $\hat{R}_k(\theta_k)$ read:

$$\begin{aligned} u_{kj} &= e^{-\mathrm{i}\theta_k}\delta_{kj}; \\ v_{kj} &= w_k = 0, \quad \forall k, j. \end{aligned} \tag{4.98}$$

Hence, $\hat{U}_k(\theta_k)$ transforms the quadrature operators (see (4.92)) according to the affine transfomation $(\bar{\boldsymbol{d}}_{PS}, \boldsymbol{S}_{PS})$ with

$$\bar{\boldsymbol{d}}_{PS} = 0, \qquad \boldsymbol{S}_{PS} = \begin{pmatrix} \cos\theta_k & \sin\theta_k \\ -\sin\theta_k & \cos\theta_k \end{pmatrix}. \tag{4.99}$$

The multimode case follows by direct summing the single-mode symplectic matrices $\boldsymbol{S}_{PS}$.

Let us now consider the case $k > l$. For simplicity, we restrict our attention to a system with two modes, labelled by A and B. The Hamiltonian $\hat{H}_{Q1}$ generates the unitary operator

$$\hat{B}_{AB}(\epsilon) := \exp\left[\epsilon \hat{a}_A^\dagger \hat{a}_B - \epsilon^* \hat{a}_A \hat{a}_B^\dagger\right], \tag{4.100}$$

where $\epsilon := -\mathrm{i}\, g_{AB} \in \mathbb{C}$. By defining $\epsilon = \phi\, e^{\mathrm{i}\theta}$, the action of $\hat{B}_{AB}(\epsilon)$ on the mode operators $\hat{a}_A$ and $\hat{a}_B$ reads:

$$\begin{aligned} \hat{B}_{AB}(\epsilon)^\dagger\, \hat{a}_A\, \hat{B}_{AB}(\epsilon) &= \cos\phi\, \hat{a}_A + e^{\mathrm{i}\theta} \sin\phi\, \hat{a}_B; \\ \hat{B}_{AB}(\epsilon)^\dagger\, \hat{a}_B\, \hat{B}_{AB}(\epsilon) &= \cos\phi\, \hat{a}_B - e^{-\mathrm{i}\theta} \sin\phi\, \hat{a}_A. \end{aligned} \tag{4.101}$$

This unitary operator represents the evolution operator associated with the *beam splitter*. In particular, when $\phi = \pi/4$ and $\theta = 0$, $\hat{B}_{AB}(\pi/4)$ is said to be a *balanced beam splitter*, or *50:50 beam splitter*.

Labelling by an index k the outputs modes and by j the input modes, the Bogoliubov coefficients associated with $\hat{B}_{AB}(\epsilon)$ read:

$$\begin{aligned} u_{kj} &= \cos\phi\delta_{kj} \pm (e^{\mathrm{i}\theta}\sin\phi)(1-\delta_{kj}), \\ v_{kj} &= w_k = 0, \quad \forall k, j. \end{aligned} \tag{4.102}$$

Therefore, $\hat{B}_{AB}(\epsilon)$ transforms the quadrature operators (see (4.92)) according to the affine transfomation $(\bar{\boldsymbol{d}}_{BS}, \boldsymbol{S}_{BS})$, with

$$\bar{\boldsymbol{d}}_{BS} = 0, \qquad \boldsymbol{S}_{BS} = \begin{pmatrix} \cos\phi \boldsymbol{I}_2 & \sin\phi \boldsymbol{S}_{PS}(\theta) \\ -\sin\phi \boldsymbol{S}_{PS}(\theta) & \cos\phi \boldsymbol{I}_2 \end{pmatrix}, \tag{4.103}$$

where $\boldsymbol{I}_2$ is the 2×2 identity matrix and $\boldsymbol{S}_{PS}(\theta)$ is the symplectic matrix associated with a phase shifter of angle θ (see Eq. (4.99)).

4.3.3 Squeezing Operators

We now focus on the second quadratic term of Eq. (4.7), i.e. $\hat{H}_{Q2} := \sum_{k,l=1}^{M} (h_{kl}\hat{a}_k^\dagger \hat{a}_l^\dagger + h_{kl}^* \hat{a}_k \hat{a}_l)$. This term also describes to two distinct processes, depending on whether $k = l$ or $k \neq l$.

For $k = l$, the Hamiltonian generates the unitary operator

$$\exp\left[-\mathrm{i}\sum_{k=1}^{M} h_{kk}\hat{a}_k^{\dagger\,2} + h_{kk}^*\hat{a}_k^2\right] = \bigotimes_{k=1}^{M} \hat{Z}_k(\xi_k), \tag{4.104}$$

which is the single-mode squeezing operator $\hat{Z}(\xi_k)$ (see Eq. (4.71)), with $\xi_k = -2\mathrm{i}h_{kk}$. By comparing Eqs. (4.73) and (4.90), and again considering $\xi_k = r_k \in \mathbb{R}$, we see that the Bogoliubov coefficients associated with $\hat{Z}_k(\boldsymbol{r})$ read:

$$\begin{aligned} &u_{kj} = \cosh r_k\, \delta_{kj}; \quad v_{kj} = -\sinh r_k\, \delta_{kj}; \\ &w_k = 0, \quad \forall\, k. \end{aligned} \tag{4.105}$$

Therefore, $\hat{Z}_k(r_k)$ acts on the quadrature operators $\hat{q}_k$, $\hat{p}_k$ (see (4.92)) as an affine transformation $(\bar{\boldsymbol{d}}_{SMS}, \boldsymbol{S}_{SMS})$ with

$$\bar{\boldsymbol{d}}_{SMS} = 0, \qquad \boldsymbol{S}_{SMS} = \begin{pmatrix} e^r & 0 \\ 0 & e^{-r} \end{pmatrix}. \tag{4.106}$$

Let us now consider the case $k > l$. For simplicity, we restrict our attention to a system with two modes, labelled by A and B. We can immediately see that Hamiltonian $\hat{H}_{Q2}$ generates a two-mode squeezing operator (see Eq. (4.77)) $\hat{Z}_{AB}(\xi)$, with $\xi = 2\mathrm{i}\, h_{AB} \in \mathbb{C}$.

By considering again $\xi = r \in \mathbb{R}$, we can derive the action of $\hat{Z}_{AB}(r)$ on the quadrature operators (see (4.92)) as an affine transformation $(\bar{\boldsymbol{d}}_{TMS}, \boldsymbol{S}_{TMS})$, with

$$\bar{\boldsymbol{d}}_{TMS} = 0, \qquad \boldsymbol{S}_{TMS} = \begin{pmatrix} \cosh r & 0 & \sinh r & 0 \\ 0 & \cosh r & 0 & -\sinh r \\ \sinh r & 0 & \cosh r & 0 \\ 0 & -\sinh r & 0 & \cosh r \end{pmatrix}. \tag{4.107}$$

4.3.4 Passive and Active Gaussian Unitaries

We have seen that the most general M-mode Gaussian unitary $\hat{U}_G$ is associated with an affine transformation $(\bar{\boldsymbol{d}}, \boldsymbol{S})$ (see (4.93)). We write $\bar{\boldsymbol{d}} = \sqrt{2}(\mathrm{Re}(\alpha_1), \mathrm{Im}(\alpha_1), \ldots, \mathrm{Re}(\alpha_M), \mathrm{Im}(\alpha_M))^T$ for some $\alpha_k \in \mathbb{C}$ $(k = 1, 2, \ldots, M)$. Then, by considering Eq. (4.95), $\hat{U}_G$ can be decomposed as:

$$\hat{U}_G = \hat{D}(\boldsymbol{\alpha})\, \hat{U}_{\boldsymbol{S}}, \tag{4.108}$$

where $\hat{D}(\boldsymbol{\alpha})$ is an M-mode displacement operator (see Eq. (4.20)), $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_M)$ and $\hat{U}_{\boldsymbol{S}}$ is a Gaussian unitary associated with $(\bar{\boldsymbol{d}} = 0, \boldsymbol{S})$.

For what we have seen in the previous subsections, we understand that $\hat{U}_{\boldsymbol{S}}$ is a combination of phase shifters, beam splitters and squeezing operators. This intuition is formalised by the following theorem.

Theorem 4.23 (Bloch-Messiah theorem [DMS+95])**.** *Any $2M \times 2M$ symplectic matrix can be decomposed as:*

$$\boldsymbol{S} = \boldsymbol{O}_1 \left[\bigoplus_{k=1}^{M} \boldsymbol{S}_{SMS}(r_k)\right] \boldsymbol{O}_2, \tag{4.109}$$

where the $2M \times 2M$ matrices $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are symplectic and orthogonal, and the 2×2 matrix $\boldsymbol{Z}(r_k)$ is a single-mode squeezing operator (see Eq. (4.71)*) with real r_k.*

We have seen that phase shifters and beam splitters are associated with symplectic orthogonal matrices (see Eqs. (4.99) and (4.103), respectively). Any combination of them realises the matrices $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$, since the product of orthogonal matrices is orthogonal.

Definition 4.24. A *passive unitary* [Wee+12; Oli12] is a Gaussian unitary $\hat{U}_{\boldsymbol{O}}$ that is represented in the phase space (Eq. (4.93)) by $(\bar{\boldsymbol{d}} = 0, \boldsymbol{O})$, where $\boldsymbol{O}$ is a symplectic orthogonal matrix. Conversely, any Gaussian unitary that is not passive, is called *active*.

Passive Gaussian unitaries preserve the total average photon number (see Eq. (4.57)):

$$\langle \hat{N} \rangle = \frac{1}{4} \left(\mathrm{Tr}[\boldsymbol{O}\, \boldsymbol{V}\, \boldsymbol{O}^T] + 2|\boldsymbol{O}\boldsymbol{d}|^2 - 2M \right) = \frac{1}{4} \left(\mathrm{Tr}[\boldsymbol{V}] + 2|\boldsymbol{d}|^2 - 2M \right), \tag{4.110}$$

and thus the average energy $E = \langle \hat{H} \rangle$, since $\hat{H}$ commutes with $\hat{N}$(see Eq. (4.7)). Passive Gaussian unitaries are the only energy-preserving Gaussian unitaries [ARL14; Ser17].

Passive Gaussian unitaries induce a linear transformation of the mode operators (see Eqs. (4.97) and (4.101)). For this reason, the experimental implementations of them are called *linear optical components* in quantum optics [WM07]. They are quite commonly used devices in quantum optics laboratories since they are inexpensively available and yet very useful in many applications [GAF10]. In particular, they are used to create correlations between modes with the same frequency [FT20].

We conclude this section by noting that, by combining the most general symplectic matrix (Eq. (4.109)) with the Williamson's theorem 4.14, the most general covariance matrix $\boldsymbol{V}$ can be expressed as:

$$\boldsymbol{V} = \boldsymbol{O}_2^T \left[\bigoplus_{k=1}^{M} \boldsymbol{S}_{SMS}(r_k) \right] \boldsymbol{O}_1^T \left[\bigoplus_{k=1}^{M} \nu_k \boldsymbol{I}_2 \right] \boldsymbol{O}_1 \left[\bigoplus_{k=1}^{M} \boldsymbol{S}_{SMS}(r_k) \right] \boldsymbol{O}_2. \tag{4.111}$$

This expression holds regardless of whether $\boldsymbol{V}$ is the covariance matrix of a Gaussian state or not. This follows from the Williamson's theorem being valid for generic covariance matrices.

4.4 Gaussian Channels

We here extend to CV systems the notion of *quantum channels* (see Def. 3.12). In particular, an M-mode *Gaussian channel* is defined as a completely positive trace-preserving (CPTP) map Λ_G that transforms an M-mode Gaussian state ρ_G into another M-mode Gaussian state $\Lambda_G[\rho_G]$ [Wee+12]. The action of a Gaussian channel on a Gaussian state ρ_G is completely characterised by a transformation on the first and second moments of ρ_G [HW01].

Theorem 4.25. *An M-mode Gaussian channel Λ_G transforms the displacement vector $\boldsymbol{d}$ and covariance matrix $\boldsymbol{V}$ of a generic Gaussian state ρ_G in the following way:*

$$\begin{aligned} \boldsymbol{d} &\to \boldsymbol{T}\, \boldsymbol{d} + \bar{\boldsymbol{d}}, \\ \boldsymbol{V} &\to \boldsymbol{T}^T\, \boldsymbol{V}\, \boldsymbol{T} + \boldsymbol{N}, \end{aligned} \tag{4.112}$$

where $\bar{\boldsymbol{d}}$ is a $2M$-dimensional vector, while $\boldsymbol{T}$ and $\boldsymbol{N} = \boldsymbol{N}^T$ are $2M \times 2M$ real matrices, such that

$$\boldsymbol{N} - i \left(\boldsymbol{\Omega} - \boldsymbol{T}^T\, \boldsymbol{\Omega}\, \boldsymbol{T} \right) \geq 0\,. \tag{4.113}$$

Conversely, any matrices $\boldsymbol{T}$ and $\boldsymbol{N} = \boldsymbol{N}^T$ that satisfy Eq. (4.113) *correspond to a Gaussian channel.*

The Gaussian unitaries are a particular case of Gaussian channels, with $\boldsymbol{T}$ being symplectic and $\boldsymbol{N} = 0$ (see Eq. (4.93)).

Let us consider the Stinespring's dilation (see Theorem 3.14),

$$\Phi_G(\rho) = \mathrm{Tr}_E \left[\hat{U}_{M+M_E} \left(\rho \otimes \rho_E \right) \hat{U}^\dagger_{M+M_E} \right], \tag{4.114}$$

where ρ_E is an environmental state of M_E modes and $\hat{U}_{M+M_E}$ is an $(M + M_E)$-mode Gaussian unitary acting on the system and the environment. Λ_G is a Gaussian channel, because composing and partial tracing Gaussian states are Gaussian operations (see Theorems 4.12 and 4.13, respectively). Remarkably, the converse statement holds (see [Ser17] for the proof): for any M-mode quantum channel Λ_G in the form of Theorem 4.25, a Stinespring's dilation in the form of Eq. (4.114) can be defined. Moreover, we can always choose $\rho_E = |0_E\rangle \langle 0_E|$ and $M_E \leq 2M$ [Car+08; Car+11].

4.5 Gaussian Measurements

Consider quantum measurements, as defined in Sec. 3.1.2. For CV systems, the measurement outcomes usually form a continuous set, therefore the probability of observing an outcome m (see Eq. (3.39)), $p_\rho(m)$, becomes a probability density for $m \in \mathbb{R}$. In this context, *Gaussian measurements* are defined as such measurement operators that transform Gaussian states into Gaussian states [ARL14]. They are associated with a Gaussian probability density $p_{\rho_G}(m)$ for any Gaussian state ρ_G [Wee+12].

Here we introduce the two most commonly used Gaussian measurements: the *homodyne* and *heterodyne detection*. For simplicity, we will consider single-mode systems and measurements.

4.5.1 Homodyne Detection

Definition 4.26 (Homodyne detection)**.** A *homodyne detection* is a projective measurement (see Eq. (3.8)) onto the *generalised quadrature operator*:

$$\hat{x}_\phi = \cos\phi \hat{q} + \sin\phi \hat{p}, \qquad \phi \in [0, \pi], \tag{4.115}$$

which satisfies $[\hat{x}_\phi, \hat{x}_{\phi+\frac{\pi}{2}}] = 1$ for all ϕ.

Denoting by $|x_\phi\rangle$ the improper eigenstates of $\hat{x}_\phi$, the probability of measuring $|x_\phi\rangle$ (see Eq. (3.9)) reads:

$$p_{\rho_G}(x_\phi) = \langle x_\phi | \rho | x_\phi \rangle , \tag{4.116}$$

where ρ_G is the state of the system. By comparing Eq. (4.116) with Eq. (4.47), we see that for a fixed phase ϕ the measurement of $\hat{x}_\phi$ corresponds to the integral of the Wigner function of ρ_G, i.e.

$$\langle x_\phi | \rho | x_\phi \rangle = \frac{1}{2} \int_{\mathbb{R}} dx_{\phi+\frac{\pi}{2}} \, W(q, p). \tag{4.117}$$

For $\hat{q}$ ($\phi = 0$) and $\hat{p}$ ($\phi = \pi/2$), Eq. (4.117) becomes:

$$p_{\rho_G}(q) = \frac{1}{2} \int_{\mathbb{R}} dp \, W(q, p), \qquad P(p) = \frac{1}{2} \int_{\mathbb{R}} dq \, W(q, p). \tag{4.118}$$

The word "homodyne" derives from the Greek roots *homo-* ("same"), and *dyn-* ("power"). In quantum optics, a homodyne detection scheme is realised [BL05] by mixing in a beam splitter the state of the system ρ_G with an ancillary signal, called the *local oscillator*, at same frequency of ρ_G. The local oscillator is a coherent state $|\alpha_{LO}\rangle$, with $\alpha_{LO} = |\alpha_{LO}|\, e^{\mathrm{i}\phi}$ and $|\alpha_{LO}| >> 1$. Because of its large photon number, $|\alpha_{LO}\rangle$ can be associated with a classical complex amplitude α_{LO}, rather than a mode operator $\hat{a}_{LO}$. Denoting by $\hat{a}$ the mode operator associated with ρ_G, a balanced beam splitter mixes $\hat{a}$ and α_{LO}, and generates two new mode operators (see Eq. (4.103)):

$$\hat{a}_1 = (\alpha_{LO} + \hat{a})/\sqrt{2}, \qquad \hat{a}_2 = (\alpha_{LO} - \hat{a})/\sqrt{2}. \tag{4.119}$$

The two mode operators are measured with two *photodetectors*, which are experimental devices that convert the photons into an electric current (*photocurrent*), denoted by $\mathfrak{i}$. It can be assumed [Pau95] that the photocurrent is proportional to the number of photons measured by the photodetector, i.e. $\mathfrak{i} = c\hat{a}^\dagger\hat{a}$. Then the two modes of Eq. (4.119) generate the photocurrents:

$$\begin{aligned} \mathfrak{i}_1 &= \frac{c}{2}\,(\alpha_{LO}^* + \hat{a}^\dagger)(\alpha_{LO} + \hat{a}) = \frac{c}{2}\,(|\alpha_{LO}|^2 + \hat{a}^\dagger\hat{a} + \alpha_{LO}^*\hat{a} + \alpha_{LO}\hat{a}^\dagger); \\ \mathfrak{i}_2 &= \frac{c}{2}\,(\alpha_{LO}^* - \hat{a}^\dagger)(\alpha_{LO} - \hat{a}) = \frac{c}{2}\,(|\alpha_{LO}|^2 + \hat{a}^\dagger\hat{a} - \alpha_{LO}^*\hat{a} - \alpha_{LO}\hat{a}^\dagger). \end{aligned} \tag{4.120}$$

Therefore, the *difference photocurrent* $\delta\mathfrak{i} := \mathfrak{i}_1 - \mathfrak{i}_2$ reads:

$$\delta\mathfrak{i} = c(\alpha_{LO}^*\hat{a} + \alpha_{LO}\hat{a}^\dagger) = c|\alpha_{LO}|\,(e^{-\mathrm{i}\phi}\hat{a} + e^{\mathrm{i}\phi}\hat{a}^\dagger) = c|\alpha_{LO}|\,\hat{x}_\phi. \tag{4.121}$$

Hence, by measuring the difference photocurrent one can measure the quadrature. A more sophisticated and formal analysis of the homodyne detection scheme is given in [Ser17].

4.5.2 Heterodyne Detection

Definition 4.27 (Heterodyne detection)**.** A *heterodyne detection* is a positive operator-valued measure (POVM, see Eq. (3.16)) with POVM elements $\hat{E}_\alpha := |\alpha\rangle\langle\alpha|/\pi$. The operators $\hat{E}_\alpha$ satify:

$$\int_{\mathbb{R}^2} d^2\alpha\, \hat{E}_\alpha = \frac{1}{\pi}\int_{\mathbb{R}^2} d^2\alpha\, |\alpha\rangle\langle\alpha|\,. \tag{4.122}$$

The probability of measuring $\hat{E}_\alpha$ (see Eq. (3.17)) simply reads:

$$p_{\rho_G}(\alpha) = \frac{\langle\alpha|\rho_G|\alpha\rangle}{\pi} = Q_{\rho_G}(\alpha), \tag{4.123}$$

where ρ_G is the state of the system and $Q_{\rho_G}(\alpha)$ is the Husimi Q function of ρ_G (see Eq. (4.48)).

The word "heterodyne" derives from the Greek roots *hetero-* ("different"), and *dyn-* ("power"). A heterodyne detection scheme is traditionally realised [Jac62; Wee+12] as a homodyne scheme but with the frequency of the local oscillator being different from that of the input signal. A suitable photodetector then converts photons at different frequencies into a single photocurrent.

An alternative method to realise heterodyne detection is with a double homodyne scheme: the state of the system ρ_G is first mixed with an ancillary vacuum state by a balanced beam splitter (see Eq. (4.101)). Then the quadrature operators $\hat{q}$ and $\hat{p}$ of the outcome modes are homodyned to obtain $\alpha = (q + \mathrm{i}\,p)/\sqrt{2}$. A proof of the equivalence of this method to the heterodyne detection defined in Def. 4.27 is given in [Ser17].

5

Secure Entity Authentication with (QR-) PUFs

Entity authentication is a cryptographic procedure by which one entity establishes the identity and active participation in a conversation of a second entity. Its objective is to prevent malicious intruders to exploit secure protocols against legitimate users. *Physical unclonable functions* (PUFs) [Pap01; Pap+02] are a precious tool for entity authentication. They are physical objects that, because of a complex inner structure, produce a unique *response* when probed with a *challenge*. An extension of such systems to quantum protocols is called *quantum readout of PUFs (QR-PUFs)* [Ško12].

This chapter is an introduction to our publication [GKB20], which is contained in full in Appendix A. In this article, we developed a generally valid theoretical model of both classical and QR- PUFs and provided a system-independent formalisation of their properties.

This chapter is structured as follows. In Sec. 5.1, we introduce elements of cryptography and the main concepts behind entity authentication protocols. PUFs are presented in Sec. 5.2, and QR-PUFs are introduced in 5.3. Finally in Sec. 5.4, we summarise [GKB20], and discuss possible research outlooks. Besides [GKB20], the content of this chapter is mostly inspired from [SP18; Mar12; McG+19; MV10; Arm+11].

5.1 Elements of Cryptography

The objective of cryptography is to allow two parties, commonly named *Alice* and *Bob*, to securely communicate in presence of an adversary, usually named *Eve* (from *eavesdropping*). There are several features associated with *information security*, such as data confidentiality, authentication and so on. A specific cryptographic protocol, whose elements are called *cryptographic primitives*, can address either a single feature or more than one.

The concept of *security* is formalised in terms of three different aspects [SP18]: an *attack model*, an *adversarial goal*, and a *security level*.

The attack model specifies what kind of information is available to the adversary and what must be kept secret. The adversary is always assumed to know the protocol being used (*Kerckhoffs' Principle*) and is generally allowed to observe all the information being transmitted between Alice and Bob.

The adversarial goal exactly specifies what is the purpose of Eve in attacking the protocol. Hence, it determines what does "successful attack" mean.

The security level quantifies the security of a protocol in terms of the effort required for a successful attack. The usual security levels are the following:

Computational security: a protocol is *computationally secure* if there does not exist an algorithm that efficiently performs a successful attack. The efficiency of an algorithm is quantified in terms of the amount of time required by the algorithm. Computationally secure protocols may become vulnerable due to developments in technology;

Provable security: a protocol is *provably secure* if a successful attack depends on the solution of a difficult mathematical problem. The difficulty of a problem is formalised by the computational complexity theory [SP18]. Provably secure protocols may become vulnerable if an efficient way to solve the underlying mathematical problems is found. Specifically, the emergence of quantum computing poses the biggest security threat to many problems in this class [Sho94; NC10];

Unconditional security: a protocol is *unconditionally secure* if there does not exist a successful attack, even with unlimited computational resources. Unconditional secure protocols base their security on information-theoretic arguments: an adversary does not have enough information to carry out a successful attack. Unconditional secure protocols may still be vulnerable to *side-channel attacks*, i.e. attacks against practical implementations of the protocols.

5.1.1 Entity Authentication

Entity authentication is usually needed in several cryptographic protocols to prevent a *man-in-the-middle-attack* [SP18], where an adversary Eve impersonates one of the legitimate parties (or both). This is a powerful side-channel attack, which Eve could use to accomplish her goal even in the presence of unconditional secure protocols.

As an example, let us consider *quantum key distribution* (QKD) [Sca+09]. This is an unconditional secure protocol that allows two parties, Alice and Bob, to establish a secret key among them, and use it to encrypt and decrypt their conversation. A man-in-the-middle attack may lead to the establishment of two secret keys, one between Eve and Alice, and the other between Eve and Bob. Thus, Eve would become able to read every message exchanged between Alice and Bob, despite the security of QKD.

An entity authentication protocol is said to be *unilateral* when there is only one party (the *verifier*) who needs to verify the identity of the other party (the *claimant*). Otherwise, the authentication is said to be *mutual*. Unilateral entity authentication is particularly used when the verifier is an institution that provides a service and the claimant is a user who wants to access that service. For instance, a client of a bank who wants to withdraw money at an ATM is authenticated by the bank via a unilateral protocol.

There are three main *authentication factors* that are used to verify the identity of the claimant.

1. *Knowledge factor*: the claimant *knows* an authentication key (e.g. a password), and proves this knowledge to the verifier. This factor is very practical in the case of remote online authentication. However, it requires the establishment of a shared key that must be continuously kept secret. Moreover, an adversary could learn the authentication key without being noticed by the legitimate parties;

2. *Ownership factor*: the claimant *has* an authentication token (e.g. an ID card), and show it to the verifier. While this factor requires the distribution of a physical object, it has the advantage to not need secret knowledge from the claimant. This may be a desirable feature when the verifier is an institution and the claimant an untrusted user. The token must be protected from physical theft, which is generally easier to notice than information theft.

3. *Inherence factor*: the claimant *is* something, i.e the authentication is based on some biometric characteristics of the claimant (e.g. a fingerprint). This factor has several practical advantages, such as not requiring secrecy or the distribution of a token. However, it is also controversial for privacy reasons.

The authentication protocol is said to be *single-factor* or *multi-factor*, depending on the number of used factors. An example of multi-factor authentication is the use of a debit card (ownership factor) with a PIN (knowledge factor). Another example is the use of a picture (inherence factor) on identity documents (ownership factor).

An important family of protocols is that of *challenge-response authentication*, in which a party presents a question (*challenge*), based on the authentication factor(s), and another party must provide a valid answer (*response*) to be authenticated. This type of protocol allows establishing in real-time, whenever needed, the identity of the claimant in terms of the authentication factor(s). The attack model does not generally allow the adversary to know the responses for given challenges. In many protocols, the verifier Alice may be required to choose a challenge at random from a given set and to discard it after using it once. In these protocols, a source of randomness is required [SP18].

5.2 Physical Unclonable Functions

In Sec. 5.1, we have discussed the ownership factor in entity authentication protocols. In many applications, an authentication token is *associated* with an identity: for instance, a passport is made by using sophisticate anti-counterfeiting technologies. However, these technologies only serve to distinguish between a valid document and a forgery. The identity of the password is ultimately provided by its serial number and the information contained in it.

The main concept behind *Physical Unclonable Functions* (PUFs) is to directly identify an authentication token in terms of its physical properties, probed by a challenge-response protocol. To have secure authentication, the internal structure of a PUF is required to be hard to counterfeit. Moreover, an adversary should not be able to predict a response from a given challenge. We shall see in Sec. 5.2.2 that postprocessing techniques can be used to enhance the unpredictability of a challenge-response behaviour.

Normally, entity authentication protocols based on PUFs are divided in two phases [ŠTO05]: the *enrollment stage* and the *verification stage* (see fig. 5.1).

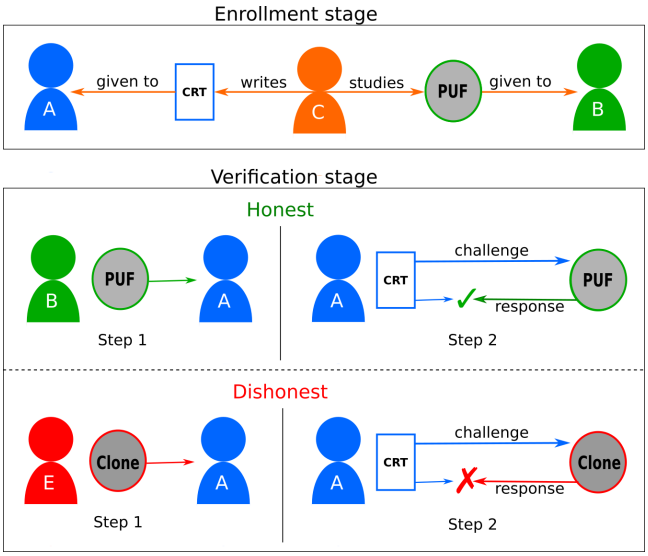

Figure 5.1: A schematic description of the two stages of an authentication protocol with PUFs. **Top:** Enrollment stage. The Certifier (C, orange) studies the PUF's properties and generates the Challenge-Response Table (CRT). Then the CRT is given to Alice (A, blue) and the PUF is given to Bob (B, green).
Bottom: Verification stage. In the honest case, Bob lets Alice interact with his PUF through a terminal and she remotely verifies his identity with the CRT, thus authenticating him. In the dishonest case, an adversary Eve (E, red) claims to be Bob, letting Alice interact with a clone of the PUF, and the protocol should lead to an abortion.
The figure is adapted from our publication [GKB20].

In the enrollment stage, which happens during, or shortly after, the manufacturing of the PUF, a trusted entity, called the *PUF Certifier*, selects a certain number of challenges and records the corresponding responses. The obtained *Challenge-Response Pairs* (CRPs) are stored as a *Challenge-Response Table* (CRT). The Certifier is also allowed to study the PUF's properties and evaluate the parameters needed for an entity authentication protocol. At the end of this stage, the Certifier gives the CRT to the verifier Alice and the PUF to the claimant Bob.

In the verification stage, the verifier checks the identity of the claimant by randomly selecting a challenge from the CRT and sending it to the claimant's PUF. If the response produced by the PUF matches with the one in the CRT, the authentication is successful. This stage can be repeated every time Alice needs to authenticate Bob. The used challenge-response pair needs to be eliminated from the CRT and cannot be used again. Therefore, a PUF can be used a limited number of times.

We mention here that the use of PUFs in cryptography is not limited to entity authentication protocols [Rüh10; RD13; Brz+11] but this topic goes further from the scope of our thesis.

5.2.1 Types of PUFs

Here, we give an overview of some relevant types of PUFs. Extensive discussion can be found in [MV10; McG+19].

Optical PUFs

Optical PUFs were introduced by Pappu [Pap01; Pap+02] as *physical one-way functions* (POWF). This was the first formalisation of the concept of PUF, although the use of complex physical systems for authentication purposes was already established [Bau83; Sim84; Sim91; Tol92; Nat+93; IM94; NF93].

An optical PUF is a transparent medium that is filled, in random positions, with microscopic light-scattering particles. An incident laser that interacts with the PUF is transformed into a unique *speckle pattern*, which is highly dependent on the position of the scatterers and the orientation of the laser. Hence, a laser orientation is used as a challenge and the resulting speckle as the corresponding response.

Pappu showed that any little change in the distribution of the scatterers would produce a drastic change in the challenge-response behaviour. The same effect would be produced in case of any invasive attack on the physical structure (this property has been referred to as *tamper evidence*). Hence, it is very difficult to create a clone for an optical PUF.

Optical PUFs were studied, from an information-theoretic point of view, in [Tuy+04; ŠTO05; Tuy+05; Ign+06]. Since the output speckles are highly sensitive to the input laser orientation, a small error in the implementation of the challenge may produce a high amount of noise. Therefore, a post-processing scheme has to be necessarily used (see Sec. 5.2.2).

Magnetic PUFs

Magnetic PUFs [IM94] are also based on the random distribution of microscopic particles in a homogeneous medium. In this case, a magnetic medium, such as a magnetic swipe card, is filled in an arbitrary position with microscopic ferromagnetic particles of different sizes and shapes. This creates a complex and unique structure. A magnetic reader checks the exact magnetic field intensity in certain positions along the strip: the positions serve as challenges and the corresponding intensities as responses.

Arbiter PUFs

Arbiter PUFs [Lee+04; Lim+05] belong to a family of PUFs embedded on silicon integrated circuits [Del17]. On a chip, two reconfigurable circuits with the same starting point are designed to have the same travel time for an input current. However, the practical manufacture is not perfect, and small random variations are produced. At the end of the circuits, an arbiter component (usually a latch) compares the output signals of the two circuits and generates a bit: the two possible values are associated with the two signals, and the generated bit is that corresponding to the first signal reaching the arbiter. In the initial design, the two circuits are realised by *switch blocks*: they are electric components with two inputs and two outputs, and, based on a parametric bit, they can keep the signals on their original circuit line, or switch them. Thus, the parametric bits on the switch cells is identified as a challenge, while the output bit of the arbiter is the corresponding response. The number of challenge and response bits increase by employing more than one input current, and the number of possible challenges is exponential in the number of switch blocks used.

As soon as they were introduced, arbiter PUFs were found insecure under model-building attacks [Lee+04; Gas+04; Lim+05], i.e. attacks in which the observation of some challenge-

response pairs leads to the creation (by machine-learning techniques) of an accurate mathematical model of the PUF, able to predict the responses to unseen challenges.

Attempts to solve this issue by modifying the PUF's design [MKP09; Lim+05; ÖHS08] were met by more sophisticated machine-learning attacks [MKP08; RSS09; DV14].

Static Random Access Memory (SRAM) PUF

Static random access memory (SRAM) PUFs [Lay+04; Gua+07a; HBF07] are digital memories composed by memory cells, called SRAM cells. A SRAM cell is realised by inverters and transistors and possesses two stable states. When an input electrical power is applied, each cell is stabilised into either state and can be read as a memory storing one bit. The precise state is determined by both the input current and manufacturing variations in the cell, which lead to different states for different cells. Thus, a collection of SRAM cells form a PUF, whose challenge is the "address" of specific cells and the response is the string formed by the bits stored in the cells.

SRAM PUFs were studied, from an information-theoretic point of view, in [Gua+07b] and [Del17]. They were found to be very noisy, thus requiring post-processing.

5.2.2 Fuzzy Extractors

It is not generally reliable or secure to directly use a PUF's output as a response [Del+14; Puc+15]. Because of noise in the physical process, or errors in the practical implementation of the protocol, a single challenge may produce different responses. Therefore an *error correction* scheme is required. Another issue is the existence of correlations between different responses, which could be used by an adversary to simulate the PUF's challenge-response behaviour [Rüh+10; Mer+11; Hel+13; Rüh+13].

A *fuzzy extractor* [DRS04; Dod+08] is frequently used to solve or mitigate both issues [MV10; Arm+11; Del17]. In the following, we assume that PUFs' outputs, including their noisy versions, admit a mathematical representation in terms of a random variable Y on a metric space $\mathcal{Y}$ with distance d. This is a common assumption [Del17], usually with $\mathcal{Y}$ being a subset of the space of n-bits strings $\mathbb{F}_2^n$ and d being the the Hamming distance (see Sec. 2.5). The min-entropy (see Def. 3.16) of Y is then used as a quantifier for the uncertainty on the values of Y since it is related to the probability to randomly guess an outcome. To introduce the concept of fuzzy extractors, we first need some additional mathematical definitions [DRS04].

Definition 5.1 (Kleene star closure)**.** Let $\mathbb{F}_2$ be the Hamming field of bits, and $\mathbb{F}_2^n$ the vector space of n-bits strings (see Sec. 2.5). The *Kleene star closure* of $\mathbb{F}_2$, denoted by $\mathbb{F}_2^\star$, is the set of strings of arbitrary length, i.e.

$$\mathbb{F}_2^\star = \bigcup_{n>0} \mathbb{F}_2^n, \tag{5.1}$$

where $\bigcup$ denotes the union of sets.

Definition 5.2 (Statistical Distance)**.** Let A, B be discrete random variables over the same set $\mathcal{Y}$. Let $p(A)$ and $p(B)$ be probability distributions associated to A and B, respectively. We define the *statistical distance* between p_A and p_B, denoted by $D_S(p_A, p_B)$, as:

$$D_S(p_A, p_B) := \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| Pr(A = y) - Pr(B = y) \right|. \tag{5.2}$$

Definition 5.3 (Fuzzy Extractor [DRS04; Dod+08])**.** Let $\mathcal{Y}$ be a metric space with distance function d. A $(\mathcal{Y}, s, m, t, \epsilon)$-*fuzzy extractor* is a pair of random functions, the *generation function* G and the *reproduction function* R, with the following properties:

- $G : \mathcal{Y} \to \mathbb{F}_2^m \times \mathbb{F}_2^\star$ on input $\boldsymbol{y}_i \in \mathcal{Y}$ outputs an extracted string $\boldsymbol{r}_i \in \mathcal{R} \subseteq \mathbb{F}_2^m$ and a *helper data* $\boldsymbol{h}_i \in \mathcal{H} \subseteq \mathbb{F}_2^\star$. While $\boldsymbol{r}_i$ has to be kept secret, $\boldsymbol{h}_i$ can be made public;
- $R : \mathcal{Y} \times \mathcal{H} \to \mathbb{F}_2^m$ takes an element $\boldsymbol{y}_i' \in \mathcal{Y}$ and a helper string $\boldsymbol{h}_i \in \mathcal{H}$ as inputs. The *correctness property* of a fuzzy extractor guarantees that if $d(\boldsymbol{y}_i, \boldsymbol{y}_i') \leq t$ and $(\boldsymbol{r}_i, \boldsymbol{h}_i) = G(\boldsymbol{y}_i)$, then $R(\boldsymbol{y}_i') = \boldsymbol{r}_i$;
- The *security property* guarantees that for any random variable Y on $\mathcal{Y}$ with min-entropy (see Def. 3.16) $s = H_\infty(Y)$, the string $\boldsymbol{r}_i$ is nearly uniform even for those who observe $\boldsymbol{h}_i$: i.e. if $(\boldsymbol{r}_i, \boldsymbol{h}_i) = G(\boldsymbol{y}_i)$, then

$$D_S(p_{RH}, p_{UH}) \leq \epsilon, \tag{5.3}$$

  where p_{RH} (p_{UH}) is a joint probability distribution for $\boldsymbol{r}_i \in \mathcal{R}$ (for a uniformly distributed variable on m-bit binary strings) and $\boldsymbol{h}_i \in \mathcal{H}$.

A fuzzy extractor is said to be *efficient* if G and R are implemented by an algorithm that runs in an amount of time polynomially dependent on the size of the input.

The generation function G of a fuzzy extractor is used, in the enrollment stage of an entity authentication protocol with PUFs, to transform a PUF's output $\boldsymbol{y}_i$ into a uniformly distributed string $\boldsymbol{r}_i$, which is then used as a response. Afterwards, the reproduction function R is used, in the verification stage of the protocol, on a noisy version of $\boldsymbol{y}_i$ to reproduce the response $\boldsymbol{r}_i$.

As already mentioned, protocols with PUFs generally use fuzzy extractors with $\mathcal{Y}$ being a subset of the n-bits Hamming space $\mathbb{F}_2^n$ (see Sec. 2.5). For instance, the *code-offset construction* [DRS04; Dod+08] has been developed as a method to transform generic error-correcting codes on the Hamming space into fuzzy extractors. In many applications, it is useful to have *reusable fuzzy extractors* [Boy04], i.e. fuzzy extractors that remain secure even when the generation function G of a fuzzy extractor is applied multiple times to noisy versions of the same set $\mathcal{Y}$, producing multiple helper data. For instance, the output of a standard arbiter PUF is a single bit, thus different devices share the same set $\mathcal{Y} = \mathbb{F}_2$. An example of reusable fuzzy extractor is the construction by Canetti et al. [Can+16], which is able to correct up to $t = (l \ln l/m)$ bits, where l is the length of the input strings $\boldsymbol{y}_i$ and m the length of the output strings $\boldsymbol{r}_i$.

5.2.3 PUF Formalisation Attempts

Since there is a large variety of PUF implementations, it is difficult to formalise the intuitive ideas of PUF, agreeing on theoretical assumptions and definitions. However, a common theoretical framework is useful to compare different PUF implementations in terms of security and reliability. In this subsection, we review some attempts to establish this framework.

We have already mentioned that the optical PUFs [Pap01; Pap+02] were introduced as *Physical One-Way Functions* (POWFs). They were characterised as deterministic physical devices with the following properties:

1. POWFs are *easy to evaluate*, i.e. they are evaluable in constant time;

2. POWFs are *hard to invert* (*one-way*), i.e. a probabilistic polynomial algorithm (an algorithm whose running time is polynomially dependent on its input size) can find the challenge that originates a given response only with negligible probability;

3. POWFs are *hard to simulate*, i.e. a probabilistic polynomial algorithm can predict the response for a given challenge only with negligible probability;

4. POWFs are *hard to clone*, i.e. physically cloning them should be financially and technologically unfeasible.

The main problem of this definition is that it considers noiseless PUFs, which is not the case in reality. Another problem is that the one-wayness assumption does not hold for several PUF implementations with a small space of outputs (such as arbiter or SRAM PUFs). Moreover, Rührmair et al. [RSS09] argued that the one-wayness is not a necessary assumption for security.

Gassend et al. [Gas+02; Gas03] proposed the definition of *physical random functions* (PRFs), as deterministic physical devices that contain a mathematical function with the following properties:

1. The function is *easy to evaluate*, i.e. it is evaluable in constant time;

2. The function is *hard to predict*, i.e. a probabilistic polynomial algorithm can simulate the function from a small given set of challenge-response pairs only with negligible probability.

Although this definition continues to consider noiseless PUFs, the unpredictability is a more inclusive assumption than the one-wayness. However, machine-learning attacks reduce the range of validity of this assumption [Lee+04; Rüh+10].

The first definition that accounts for noise was made by Guajardo et al. [Gua+07a]. They described PUFs as physically unclonable systems with a challenge-response behaviour. The unclonability of PUFs was defined as an inherent property caused by their complex inner structure. In [Gua+07a], the following assumptions were made:

1. Different responses are independent of each other;

2. Unknown responses are hard to predict;

3. PUFs are tamper-evident, i.e. the challenge-response behaviour of a PUF is substantially changed by any tampering of the PUF.

It was argued [Arm+11] that some of these assumptions, in particular the tamper-evidence, are too restrictive since they do not hold for several PUF implementations.

Other schemes followed [RSS09; Arm+10; MV10]. A relevant proposal was made by Armknecht et al. [Arm+11]. In their formalism, a *Physical Function* (PF) is defined as the combination of a physical component and a probabilistic algorithm. The physical component interacts with a challenge signal and produces a response signal. The algorithm, which is called the *evaluation procedure*, transforms a digital representation of the challenge signal into a digital representation of the response signal. A *Physical Function System* (PFS) is then defined as the composition of a PF with a fuzzy extractor (see Sec. 5.2.2).

The main merit of [Arm+11] is to explicitly consider fuzzy extractors in the formalisation of PUFs. Another remarkable feature is to separately take into account the digital representation of challenges and responses, and the actual physical interaction. The authors defined the following security properties.

1. *Robustness*: the probability that a PFS outputs the same response when the input is the same challenge. This is quantified by a sample mean over repeated applications to the PUF of the same challenge (*challenge robustness*) or the same set of challenges (*average robustness*);

2. *Selective Physical Clonability*: the probability that a physical clone of a PFS is realised. This is quantified in a specific *security experiment*,i.e. it is quantified by theoretically modelling an attack in which an adversary tries to realise a physical clone of a PFS;

3. *Existential Physical Clonability*: the probability that two PFSs are produced, where one is the clone of the other. This is quantified in a specific security experiment. This property is useful if one takes into account the creation process of a physical function system;

4. *Predictability*: the probability that an adversary predicts the response to an unseen challenge after observing a set of challenge-response pairs. This is also quantified in a specific security experiment.

5.3 Quantum Readout of Physical Unclonable Functions

To enhance the security of Physical Unclonable Functions, Škorić [Ško12] proposed an extension of PUFs to quantum protocols, namely the *quantum readout of physical unclonable functions* (QR-PUFs). They are classical PUFs in which challenges and responses are encoded by non-orthogonal quantum states. An adversary would not be able to clone (see Theorem 3.22) or distinguish (see Theorem 3.23) them without introducing noticeable disturbances.

At the moment, only optical PUFs have been extended to QR-PUFs. In this extension, the challenges represent quantum states associated with some inner degrees of freedom of the laser. In the original article, [Ško12], the challenges are associated with single-qubit states. In the enrollment stage, a Certifier sends a certain number of non-orthogonal challenge states $|x_i\rangle$ to the QR-PUF and characterises the corresponding responses $|y_i\rangle$. To do this, he is free to repeatedly apply the same challenge and perform any measurement. Moreover, he studies the noise level of the system. In the verification stage, the verifier Alice prepares a challenge state consisting of n qubits. She sends each qubit to the QR-PUF belonging to the claimant Bob, and, if the qubit is reflected, performs a measurement onto the expected response state $|y_i\rangle$. If the fraction of returned states and correct responses is consistent with the expected noise level, Alice authenticates Bob.

Škorić examined different protocols, with different assumptions on the ability of Alice of preparing and measuring quantum states. He claimed, without giving formal proof, that the protocols would remain secure even with a public Challenge-Response Table. Moreover, he studied the security of the protocols against specific attacks, such as the random preparation of response states by an adversary Eve.

While having the merit of introducing QR-PUFs, [Ško12] leaves many questions open. Neither the security of QR-PUFs nor their advantage over their classical counterparts are formally proven. Moreover, this formalisation considers noiseless quantum states and assumes the perfect implementation of all quantum operations.

The security of QR-PUFs against other specific attacks was studied in [ŠMP13; Ško16; Yao+16b]. QR-PUFs based on continuous variables were also introduced [ND17; Nik18].

An experimental realisation of QR-PUFs was discussed in [Goo+14]. The challenge states are realised by phase-shaping incoming plane wavefronts via a *spatial light modulator*. In the enrollment stage, a certain number of challenges is sent to the QR-PUF, and the reflected speckles are recorded in a phase-sensitive way. In the verification stage, a challenge state is prepared and sent to the QR-PUF. A second spatial light modulator adds to the reflected beam the conjugate phase pattern of the expected response wavefront. If the pattern is the expected one, the beam of light is transformed into a plane wave, which then is focused by a lens into a single point on an analyser plane. If the speckles are different from the expected ones, this process produces another speckle pattern. Thus, a successful authentication is determined by the distribution of light on the analyser plane.

5.4 Formalisation of (QR)-PUFs

In this section, we introduce the result of our publication [GKB20], in which we proposed a theoretical framework for the quantitative characterisation of both PUFs and QR-PUFs. The original publication, with publication details, can be found in Appendix A.

5.4.1 Results

In [GKB20], we first designed a general, system-independent, authentication scheme, which is applicable to different physical implementations of both classical and QR- PUFs. Then, we characterised as the main security properties of (QR-) PUFs the *robustness* [Arm+11] and the *unclonability*.

Authentication Scheme

We distinguished, in our study of (QR)-PUFs, between two different theoretical levels (*layers*): a *physical layer*, where the actual physical interaction between the (QR-) PUF and an input signal is described, and a *mathematical layer*, where the challenge-response behaviour is represented by digital strings in the Hamming space (see Sec. 2.5). For the sake of clarity, we called *response* only the post-processed uniform key, while we used the term *outcome* for the intermediate raw output of a (QR-) PUF. Moreover, we called *challenges* (*outcomes*, *responses*) the strings in the mathematical layer, and *challenge states* (*outcome states*) the implementations in the physical layer.

Here, we use the vector notation in bold letters to denote the digital strings in the mathematical layer (e.g. $\boldsymbol{x}_i$ for the i-th challenge), and the Dirac notation to denote the (classical or quantum) states in the physical layer (e.g. $|x_i\rangle$ for the i-th challenge state). This notation is slightly different from the notation in [GKB20], but we use it for consistency with the other parts of the thesis.

Let us first consider classical PUFs. In the enrollment stage, the PUF Certifier selects a certain number $N \leq 2^n$ of different challenges $\boldsymbol{x}_i \in \mathcal{X}$ of length n, where $\mathcal{X} \subseteq \mathbb{F}_2^n$ denotes the set of all chosen challenges. Each challenge $\boldsymbol{x}_i \in \mathcal{X}$ represents the information on how to implement a challenge state $|x_i\rangle$. The Certifier studies $\mathcal{X}$ to ensure the lack of correlations (*uniformity*) betweeen the challenges in $\mathcal{X}$, possibly discarding some of them. Then, each challenge state $|x_i\rangle$ interacts with the PUF $\hat{P}$, and produces an *outcome state* $|y_i\rangle = \hat{P}\,|x_i\rangle$.

Inspired by the detection scheme in [Goo+14] (described in Sec. 5.3), we introduced the concept of *shifter*. A shifter is a state-dependent operation $\hat{\Omega}_i$ which maps a specific outcome state $|y_i\rangle$ into a *reference state*, denoted by $|0\rangle$. For N outcome states $|y_i\rangle$, the Certifier designs N shifters $\hat{\Omega}_i$, to have the same reference state for every outcome state. The shifters were introduced to simplify the measurements on the outcome states, with particular regard to the quantum case.

We define $|o_i\rangle := \hat{\Omega}_i \hat{P} |x_i\rangle$. In the enrollment stage, or in a noiseless verification stage, $|o_i\rangle$ is equal to the reference state $|0\rangle$ by definition, whereas in a realistic verification stage $|o_i\rangle$ contains errors. This error is represented by the Hamming weight of a classical string $\boldsymbol{o}_i \in \mathbb{F}_2^{l_o}$ in the mathematical layer, i.e. $\boldsymbol{o}_i = (0, 0, \ldots, 0)$ if and only if $|o_i\rangle = |0\rangle$. The string has a length l_o, which depends on the experimental implementation of the shifter.

Moreover, the information on how to implement a shifter $\hat{\Omega}_i$ is parameterised by a string $\boldsymbol{w}_i \in \mathbb{F}_2^{l_w}$ in the mathematical layer. The length l_w depends on the entropy of the shifters and, consequently, on the outcome states (as they are designed for them).

The string $\boldsymbol{o}_i$ conveys information about the error in the PUF evaluation, whereas $\boldsymbol{w}_i$ conveys information about the uniformity of the outcome states. We defined as *outcome* the combination of $\boldsymbol{o}_i$ and $\boldsymbol{w}_i$, i.e. the outcome is string $\boldsymbol{y}_i$ of length $l = l_w + l_o$, such that $\boldsymbol{y}_i = \boldsymbol{w}_i \,\|\, \boldsymbol{o}_i$, where $\|$ is the concatenation of strings (see Def. 2.64). The outcomes are post-processed by a fuzzy extractor (see Sec. 5.2.2), selected by the Certifier according to the min-entropy of $\mathcal{Y}$. The generation function G of a fuzzy extractor is used to transform the outcome $\boldsymbol{y}_i \in \mathcal{Y}$ into the uniformly distributed response $\boldsymbol{r}_i \in \mathcal{R} \subseteq \mathbb{F}_2^m$. It also generates helper data $\boldsymbol{h}_i \in \mathcal{H} \subseteq \mathbb{F}_2^\star$.

Challenges and responses are stored into the Challenge-Response Table (CRT) together with the strings $\boldsymbol{w}_i$, the helper data and the parameters of the fuzzy extractor. The Challenge-Response Table is given to Alice and the PUF to Bob, concluding the enrollment stage. The entire process is visualised in Fig. 5.2.

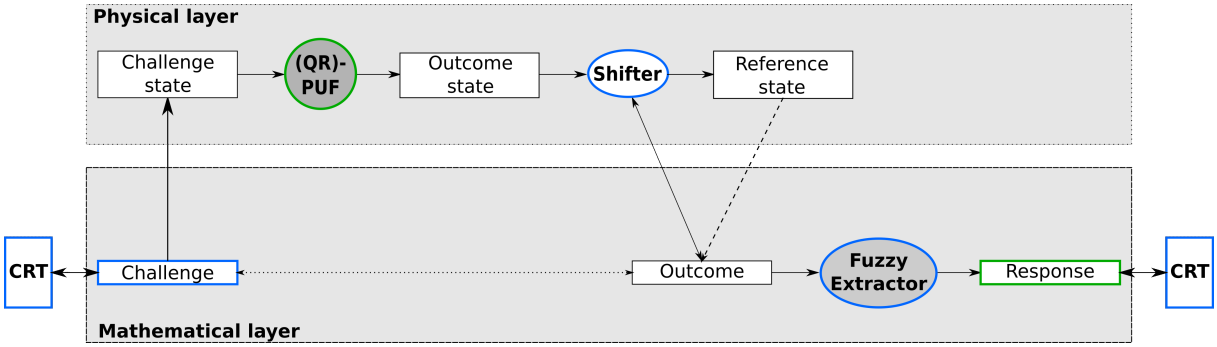

Figure 5.2: A scheme of the described authentication scheme with PUFs. There is a physical layer in which the PUF physically acts and a mathematical layer in which the cryptographic protocol takes place. In the physical layer a challenge state is prepared according to the information of the challenge (mathematical layer) and then the PUF transforms it into an outcome state. The state-dependent shifter maps the outcome state to a reference state. The outcome in the mathematical layer contains the information about the implementation of the shifter and the error in the reference state and is post-processed by the fuzzy extractor to give the response. Challenges and responses are stored into (enrollment stage) or taken from (verification stage) the Challenge-Response Table (CRT). QR-PUFs follows from considering quantum states and operations in the physical layer. The picture is taken from our publication [GKB20].

In the verification stage, Bob declares his identity and allows Alice to interact with his PUF.

Alice picks up a randomly selected challenge $\boldsymbol{x}_j \in \mathcal{X}$, for which she knows the response $\boldsymbol{r}_j \in \mathcal{R}$. She prepares the challenge state $|x_j\rangle$ and sends it to the PUF, which generates the outcome state $\hat{P}\,|x_j\rangle$. At this point, Alice tunes the shifter $\hat{\Omega}_j$, according to the CRT and evaluates $|o_j\rangle := \hat{\Omega}_j\,\hat{P}\,|x_j\rangle$.

She then post-processes the outcome $\boldsymbol{y}_j$ with the reproduction function R of the fuzzy extractor that was used in the enrollment stage, using the helper data $\boldsymbol{h}_j$. She obtain a string $\boldsymbol{z}_j$ that is compared with the response $\boldsymbol{r}_j$ in the CRT: if $\boldsymbol{z}_j = \boldsymbol{r}_j$, Bob is authenticated.

For QR-PUFs the process is analogous. The main difference is that the physical layer employs quantum states and operations. We represented the interactions in an idealised way, as unitary operations acting on pure states. We took into account noise and errors via the string $\boldsymbol{o}_i$, in the transition from the outcome state to the outcome string. In our publication, we considered challenge states formed by λ qubits and single-qubits operations individually acting on the qubits.

Security Properties

We formalised the (QR-) PUFs in terms of two main properties, the *robustness* (connected to false rejection) and the *unclonability* (connected to false acceptance). We took the definition of robustness from [Arm+11], adapting it to our framework. In the following, we denote a (QR-) PUF by $F := (F_E, F_V)$, where $F_E, F_V : \mathcal{X} \to \mathcal{R}$ represent the map from challenges to responses in the enrollment and verification stage, respectively.

Definition 5.4 (Robustness)**.** A (QR-) PUF F is *ϱ-robust* with respect to a set of challenges $\mathcal{X}$ if $\varrho \in [0, 1]$ is the greatest number for which:

$$\frac{1}{N} \sum_{\boldsymbol{x}_i \in \mathcal{X}} Pr\{F_V(\boldsymbol{x}_i) = F_E(\boldsymbol{x}_i)\} \geq \varrho\,. \tag{5.4}$$

ϱ is called the *robustness* of the (QR-) PUF with respect to $\mathcal{X}$.

The robustness quantifies the (QR-) PUF's ability to avoid false rejections and depends on many factors, such as the average noise of the specific implementation and the parameters of the fuzzy extractor.

We then introduced the *physical* and *mathematical unclonability*. A *physical clone* is an experimental reproduction of the (QR-) PUF, with the same physical properties as the original one. A mathematical clone, instead, is an object that *simulates* the challenge-response behaviour of a (QR-) PUF.

Definition 5.5 (Physical Unclonability)**.** A (QR-) PUF is *physically unclonable* if a physical clone is technologically or financially unfeasible at the current state of technology.

Definition 5.6 (Mathematical Clone)**.** Let us suppose that an adversary Eve observes q legitimate authentications of a (QR-) PUF F. With the information she can extract, she prepares a function E_q, with the intent of simulating the PUF. E_q is said to be a (γ, q)*-(mathematical) clone* of F if $\gamma \in [0, 1]$ is the greatest number for which:

$$\frac{1}{N} \sum_{\boldsymbol{x}_i \in \mathcal{X}} Pr(E_q(\boldsymbol{x}_i) = F_E(\boldsymbol{x}_i)) \geq \gamma\,. \tag{5.5}$$

Definition 5.7 (Mathematical Unclonability)**.** A (QR-) PUF F is (γ, q)- *mathematical clonable* if $\gamma \in [0, 1]$ is the smallest number for which it is not possible to generate a $(\bar{\gamma}, q)$ clone of the (QR-) PUF for any $\bar{\gamma} > \gamma$. Conversely, a (QR-) PUF F is (δ, q)- *mathematical unclonable* if it is $(1 - \delta, q)$-clonable.

The unclonability of a (QR-) PUF is therefore related to the average probability of false acceptance. We could expect that an increase of the number of legitimate uses q produces $(1 - \delta, q)$-clones with a lower δ. Therefore, fixing the maximum number of uses $q = q^*$ we fix the minimum $\delta = \delta^*$.

Definition 5.8. A (ϱ, δ^*, q^*)-*secure* (QR-) PUF F is ϱ-robust, physically unclonable and at least (δ^*, q)-mathematically unclonable up to q^* uses.

In [GKB20], we compared classical and QR- PUFs, considering examples. QR-PUFs are expected to have a higher mathematical unclonability than classical PUFs because the quantum challenge and outcome states cannot be copied. Moreover, by choosing non-orthogonal states, we prevent the adversary Eve to distinguish them without introducing detectable errors. Therefore, the amount of information that Eve can extract after observing q interactions is higher for classical PUFs than QR-PUFs.

However, we noticed that the robustness of a QR-PUF could be comparable to or worse than the robustness of a classical PUF. Quantum states are fragile and fuzzy extractors for QR-PUFs need to have a low correctable error threshold, as the noise can originate from a possible interaction of an adversary. In particular, we showed an example in which the correctable error threshold depends on the orthogonality of the challenge states. In this example, the use of highly non-orthogonal states, compared to lowly ones, increases the unclonability of the QR-PUF but also reduces its robustness. Therefore there is a trade-off between the advantages and disadvantages of QR-PUFs, which has to be studied for specific implementations.

6

Entanglement Detection for Unknown Continuous-variable States

Quantum entanglement is a key ingredient for many tasks in quantum information theory, such as quantum cryptography [Sca+09; Pir+20] and quantum communication [Ben+93; Loo02]. Therefore, it is of paramount importance to find efficient criteria for entanglement detection, in particular in unknown quantum states. Entanglement witnesses [HHH96; Ter00; HE06] are experimentally accessible entanglement tests that are based on sufficient conditions for the entanglement. They are quite effective in situations where only partial knowledge about a system is available.

This chapter is an introduction to our publication [Mih+20], which is contained in full in Appendix B. In this article, we developed a scheme for the detection of entanglement in unknown continuous-variable systems. We used random homodyne measurements to gather partial information about the states and semidefinite optimisation for constructing optimal entanglement witnesses. This idea was inspired by an analogous method for discrete-variable entanglement detection [SKB15].

This chapter is structured as follows. In Sec. 6.1, we discuss the topic of continuous-variable entanglement. In Sec. 6.2 we introduce the entanglement witnesses, in particular for continuous-variable systems. In Sec. 6.3 we present the methods that are used in our publication, namely semidefinite programs, and a quantum tomography scheme based on homodyne measurements. Finally in Sec. 6.4, we summarise [Mih+20]. Besides [Mih+20], the content of this chapter is mostly inspired from [HE06; Hor+09; AI07].

6.1 Continuous-variable Entanglement

In Chap. 3, we have introduced the notion of separable and entangled states for bipartite systems AB (see Def. 3.8). We now introduce some basic definitions and properties associated with the general multipartite case.

Definition 6.1 (Full separability [Hor+09])**.** Let $\rho_{A_1\,A_2\,\ldots\,A_M}$ be a state over the M-partite Hilbert space $\mathcal{H}_{A_1\,A_2\,\ldots\,A_M} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_M}$. The state $\rho_{A_1\,A_2\,\ldots\,A_M}$ is said to be *fully M-partite separable* if and only if it can be written as convex combination of tensor product states over $\mathcal{H}_{A_i}$, i.e.

$$\rho_{A_1\,A_2\,\ldots\,A_M} = \sum_i p_i\, \rho^i_{A_1} \otimes \rho^i_{A_2} \otimes \cdots \otimes \rho^i_{A_M}. \tag{6.1}$$

Conversely, $\rho_{A_1\,A_2\,\ldots\,A_M}$ is *entangled* if it is not fully separable.

Fully separable states are the natural extension of the bipartite separable states to the multipartite case. However, we can also introduce a notion of partial separability.

Definition 6.2 (Partial separability [Hor+09])**.** Let $\rho_{A_1\,A_2\,\ldots\,A_M}$ be a state over the M-partite Hilbert space $\mathcal{H}_{A_1\,A_2\,\ldots\,A_M} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \cdots \otimes \mathcal{H}_{A_M}$. Let $\{I_1, \ldots, I_k\}$ be a partition of the set of indeces $I = \{1, \ldots, M\}$, with $\cup_{i=1}^k I_i = I$ and $I_i \cap I_j = \emptyset$ for $i \neq j$. The state $\rho_{A_1\,A_2\,\ldots\,A_M}$ is *separable with respect to the partition* $\{I_1, \ldots, I_k\}$ if and only if it can be written as

$$\rho_{A_1\,A_2\,\ldots\,A_M} = \sum_j p_j\, \rho^j_{I_1} \otimes \rho^j_{I_2} \otimes \cdots \otimes \rho^j_{I_k}, \tag{6.2}$$

where $\rho^j_{I_i}$ is a (possibly composite) quantum state on the subsystems identified by I_i.

Therefore, states that are separable with respect to a partition may be entangled with respect to another one.

For continuous-variable systems, we can characterise the separability of a quantum state in terms of its moments.

Theorem 6.3 (Separable covariance matrices [WW01])**.** *Let $\boldsymbol{V}_{A_1\,A_2\,\ldots\,A_M}$ be the covariance matrix of a separable continuous-variable quantum state $\rho_{A_1\,A_2\,\ldots\,A_M}$. Then there exist covariance matrices $\boldsymbol{V}_{A_1}, \boldsymbol{V}_{A_2}, \ldots, \boldsymbol{V}_{A_M}$ on the subsystems $\{A_i\}$ such that*

$$\boldsymbol{V}_{A_1\,A_2\,\ldots\,A_M} \geq \boldsymbol{V}_{A_1} \oplus \boldsymbol{V}_{A_2} \oplus \cdots \oplus \boldsymbol{V}_{A_M}. \tag{6.3}$$

When $\rho_{A_1\,A_2\,\ldots\,A_M}$ is Gaussian, this condition is also sufficient.

We have not mentioned displacement vectors in Theorem 6.3. We saw in Sec. 4.3.1 that a $2M$-dimensional displacement vector can be arbitrarily modified by an M-mode displacement operator $\hat{D}(\boldsymbol{\alpha})$ (see Eq. (4.34)), which is a tensor product of local unitary operations, i.e. $\hat{D}(\boldsymbol{\alpha}) = \bigotimes_{k=1}^M \hat{D}_k(\alpha_k)$. Hence, no property related to quantum entanglement can depend on the displacement vector, which in the following is always set to zero.

In quantum information jargon, a covariance matrix that satisfies (does not satisfy) Eq. (6.3) is called a *separable* (*entangled*) covariance matrix. A state that possesses an entangled covariance matrix is always entangled, regardless of whether it is Gaussian or not. On the other hand, a separable covariance matrix is a sufficient condition for entanglement only for Gaussian states.

Theorem 6.3 is not a practical criterion, since it is in general hard to find reduced covariance matrices for a separable state or to prove their nonexistence for an entangled state [Hor+09].

6.1.1 Bipartite Entanglement

We temporarily go back to the bipartite case to introduce an important criterion for entanglement detection and expand the topic of continuous-variable entanglement.

Theorem 6.4 (Positive Partial Transpose (PPT) criterion [Per96; HHH96])**.** *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ be a density operator on a bipartite system AB. Let $\rho_{AB}^{T_A}$ denote the* partial transpose *of ρ_{AB} with respect to A, i.e.*

$$\rho_{AB}^{T_A} := (T_A \otimes \mathrm{id}_B)[\rho_{AB}], \tag{6.4}$$

where T_A is the transposition on $\mathcal{S}(\mathcal{H}_A)$ and id_B is the identity map on $\mathcal{S}(\mathcal{H}_B)$. The state ρ_{AB} is separable only if its partial transpose is positive-semidefinite, i.e. $\rho_{AB}^{T_A} \geq 0$.

The PPT criterion is a necessary but not sufficient criterion. If $\rho_{AB}^{T_A} \ngeq 0$, then ρ_{AB} is certainly entangled. On the other hand, there exist entangled states, called *bound entangled states*, for which $\rho_{AB}^{T_A} \geq 0$. However, the PPT criterion has been proven necessary and sufficient for all $1 \times M$ Gaussian states [Sim00; WW01].

Theorem 6.5. *Let $W_{\rho_{AB}}(\boldsymbol{r}_{AB})$ be the Wigner function (see Eq.* (4.46)*) of a bipartite CV state ρ_{AB}, where $\boldsymbol{r}_{AB} = (q_A, p_A, q_B, p_B)$, and A and B are systems of M_A and M_B modes, respectively. The partial transpose over A of ρ_{AB} can be expressed in terms of $W_{\rho_{AB}}$ as:*

$$T_A[W_{\rho_{AB}}(\boldsymbol{r}_{AB})] := W_{\rho_{AB}^{T_A}}(\boldsymbol{r}_{AB}) = W_{\rho_{AB}}((\boldsymbol{T}_A \oplus \boldsymbol{I}_B)\boldsymbol{r}_{AB}), \tag{6.5}$$

where $\boldsymbol{I}_B$ is the M_B-mode identity matrix, and

$$\boldsymbol{T}_A := \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \oplus \dots \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{(M_A \text{ times})}. \tag{6.6}$$

Proof. Consider an M-mode state ρ with Wigner function $W_\rho(\boldsymbol{r})$. By using Eq. (4.46), we write the Wigner function of ρ^T as:

$$\begin{aligned} T[W_\rho(\boldsymbol{r})] = W_{\rho^T}(\boldsymbol{r}) &= \left(\frac{2}{\pi}\right)^M \int_{\mathbb{R}^M} d\boldsymbol{z}\, e^{2\mathrm{i}\,\boldsymbol{p}^T\cdot\boldsymbol{z}}\ \langle \boldsymbol{q} - \boldsymbol{z}|\rho|\boldsymbol{q} + \boldsymbol{z}\rangle \\ &= \left(\frac{2}{\pi}\right)^M \int_{\mathbb{R}^M} d\boldsymbol{z}'\, e^{-2\mathrm{i}\,\boldsymbol{p}^T\cdot\boldsymbol{z}'}\ \langle \boldsymbol{q} + \boldsymbol{z}'|\rho|\boldsymbol{q} - \boldsymbol{z}'\rangle\,, \end{aligned} \tag{6.7}$$

where $\boldsymbol{z}' = -\boldsymbol{z}$. Therefore, the transposition is equal to changing $p_i \to -p_i$ in the components of $\boldsymbol{r}$, i.e.

$$\boldsymbol{r} = \bigoplus_{i=1}^{M} \begin{pmatrix} q_i \\ p_i \end{pmatrix} \to \bigoplus_{i=1}^{M} \begin{pmatrix} q_i \\ -p_i \end{pmatrix} = \bigoplus_{i=1}^{M} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} q_i \\ p_i \end{pmatrix}, \tag{6.8}$$

The proof is concluded by considering the definition of partial transpose (see Eq. (6.4)), $T_A \otimes \mathrm{id}_B$, and identifying the matrix $\bigoplus_{i=1}^{M} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in Eq. (6.8) as the matrix $\boldsymbol{T_A}$ of Eq. (6.6). □

For Gaussian states, with Wigner function given by Eq. (4.52), Eq. (6.5) becomes an equation for the covariance matrix $\boldsymbol{V}_{AB}$:

$$T_A[\boldsymbol{V}_{AB}] = (\boldsymbol{T}_A \oplus \boldsymbol{I}_B)\, \boldsymbol{V}_{AB}\, (\boldsymbol{T}_A \oplus \boldsymbol{I}_B). \tag{6.9}$$

The condition of positivity for the partial transpose is equivalent to require that $T_A[\boldsymbol{V}_{AB}]$ satisfies the Robertson-Schrödinger uncertainty principle (see Theorems 4.11 and 4.15), i.e. one of the two equivalent conditions,

$$T_A[\boldsymbol{V}_{AB}] + \mathrm{i}\,\boldsymbol{\Omega} \geq 0, \quad \text{or} \quad \tilde{\nu}_- \geq 1, \tag{6.10}$$

where $\boldsymbol{\Omega}$ is the symplectic form (see Eq. (4.12)) and $\tilde{\nu}_-$ is the smallest symplectic eigenvalue of $T_A[\boldsymbol{V}_{AB}]$.

Definition 6.6 (Logarithmic negativity [VW02])**.** The *logarithmic negativity* of a bipartite quantum state ρ_{AB} is the non-negative real number

$$E_N(\rho_{AB}) = \log \, \|\rho_{AB}^{T_A}\|_1, \tag{6.11}$$

where $\|\rho_{AB}^{T_A}\|_1$ is the trace norm (see Eq. (3.73)) of $\rho_{AB}^{T_A}$.

This is an example of *entanglement measure*, i.e. a function that *quantifies* the amount of entanglement in a quantum state. We are going to expand on this concept in Chap. 7. If $\rho_{AB}^{T_A} \geq 0$, then

$$\log \, \mathrm{Tr}\left[\sqrt{(\rho_{AB}^{T_A})^\dagger \, (\rho_{AB}^{T_A})}\right] = \log \, \mathrm{Tr}\left[\rho_{AB}^{T_A}\right] = \log 1 = 0. \tag{6.12}$$

Therefore, $E_N(\rho_{AB}) > 0$ always certifies the presence of entanglement, while $E_N(\rho_{AB}) = 0$ certifies its absence only when the PPT criterion is necessary and sufficient.

By using Eq. (6.9), the logarithmic negativity of an $(M_A + M_B)$-mode Gaussian state ρ_{AB}^G can be expressed as [Ser17]:

$$E_{\mathcal{N}}\left(\rho_{AB}^G\right) = \sum_{i=1}^{M_A+M_B} \max\{0, -\log \tilde{\nu}_i\}, \tag{6.13}$$

where $\tilde{\nu}_i$ is the i-th symplectic eigenvalues of $T_A[\boldsymbol{V}_{AB}]$.

Consider now the two-mode squeezed vacuum state (see Eq. (4.78)), $|r_{AB}\rangle = \exp[\frac{r}{2}\,(\hat{a}_A\hat{a}_B - \hat{a}_A^\dagger\hat{a}_B^\dagger)]\,|0\rangle\,|0\rangle$, with $r \in \mathbb{R}_{\geq 0}$. The logarithmic negativity of $|r_{AB}\rangle$, calculated by partial transposing the covariance matrix of Eq. (4.80) and then using Eq. (6.13), is linearly dependent on the squeezing parameter r [Ser17]:

$$E_{\mathcal{N}}(|r_{AB}\rangle\,\langle r_{AB}|) = 2r \, \log \, e, \tag{6.14}$$

where e is the Euler constant. Hence, this state is always entangled for $r > 0$.

For $r \to \infty$, $E_{\mathcal{N}}(|r_{AB}\rangle\,\langle r_{AB}|) \to \infty$. In the same limit, the Wigner function $W_{AB}(\boldsymbol{r}_{AB})$ in Eq. (4.79) becomes proportional to $\delta(q_A - q_B)\delta(p_A + p_B)$. This unphysical state, which is associated with infinite energy, was originally introduced by Einstein, Podolski and Rosen in [EPR35]. The authors used it to argue against the completeness of the quantum theory. However, the *EPR state* was later identified as the prototype of entangled state [Sch35; Bel64] and an ideal continuous-variable maximally entangled state [BW99].

The two-mode squeezed vacuum state for $r > 0$, which is an approximation at finite energy of the EPR state, is also the state that maximises the entanglement at finite energy [MZB06]. Hence, we can consider it a continuous-variable maximally entangled state at finite energy.

6.2 Entanglement Witnesses

Definition 6.7 (Entanglement witnesses [HHH96; Ter00])**.** An *entanglement witness* is a non-negative Hermitian operator $\hat{W}$ such that

$$\mathrm{Tr}(\hat{W}\,\rho^{S}_{A_1\,A_2\,\ldots\,A_M}) \geq 0, \qquad \text{for all (fully) separable states } \rho^{S}_{A_1\,A_2\,\ldots\,A_M}; \tag{6.15}$$

$$\mathrm{Tr}(\hat{W}\,\rho_{A_1\,A_2\,\ldots\,A_M}) < 0, \qquad \text{for some entangled states } \rho_{A_1\,A_2\,\ldots\,A_M}. \tag{6.16}$$

For every entangled state $\rho_{A_1\,A_2\,\ldots\,A_M}$, there exists at least one entanglement witness $\hat{W}$ such that $\mathrm{Tr}(\hat{W}\,\rho_{A_1\,A_2\,\ldots\,A_M}) < 0$. This is a corollary of the *Hahn-Banach theorem* [Roc15], which states the existence of a separating hyperplane between the convex set of separable density matrices on $\mathcal{H}_{A_1\,A_2\,\ldots\,A_M}$ and an entangled density matrix $\rho_{A_1\,A_2\,\ldots\,A_M}$ (see Fig. 6.1).

Definition 6.8. An entanglement witness $\hat{W}_1$ is said *finer* [Lew+00; Lew+01] than another entanglement witness $\hat{W}_2$ if the entanglement detected by $\hat{W}_2$ is also detected by $\hat{W}_1$, i.e.

$$\mathrm{Tr}(\hat{W}_2\,\rho_{A_1\,A_2\,\ldots\,A_M}) < 0 \quad \Rightarrow \quad \mathrm{Tr}(\hat{W}_1\,\rho_{A_1\,A_2\,\ldots\,A_M}) < 0. \tag{6.17}$$

An entanglement witness $\hat{W}$ is called *optimal* if there does not exist a witness finer than it. A *minimal witness* for an entangled state $\rho_{A_1\,A_2\,\ldots\,A_M}$ is the least fine witness that is able to detect entanglement in $\rho_{A_1\,A_2\,\ldots\,A_M}$.

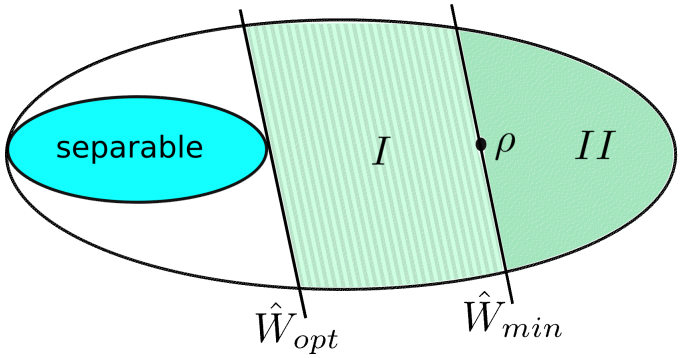

Figure 6.1: A visual representation of the entanglement witnesses (see Def. 6.7) as a separating hyperplane between the set of separable states and an entangled state ρ. The optimal witness (see Def. 6.8) $\hat{W}_{opt}$ detects the entangled states in the regions I and II, while the *minimal witness* $\hat{W}_{min}$ detects entanglement only in the region II. Entanglement witnesses that are less fine than the minimal witness $\hat{W}_{min}$ cannot detect entanglement in ρ.

Entanglement witnesses detect entanglement in both discrete- and continuous-variable systems [HHH96]. For continuous-variable systems, we can consider witnesses that are based on the covariance matrix of the system.

Definition 6.9 (Entanglement witness based on second moments [HE06])**.** An *entanglement witness based on second moments* is a real symmetric matrix $\boldsymbol{Z} \geq 0$ such that

$$\mathrm{Tr}[\boldsymbol{Z}\,\boldsymbol{V}_s] \geq 1, \qquad \text{for all (fully) separable covariance matrices } \boldsymbol{V}_s; \tag{6.18}$$

$$\mathrm{Tr}[\boldsymbol{Z}\,\boldsymbol{V}] < 1, \qquad \text{for some entangled covariance matrices } \boldsymbol{V}. \tag{6.19}$$

As a consequence of Theorem 6.3, a separable state always has a separable covariance matrix, but the vice-versa only holds for Gaussian states. Therefore, the condition $\mathrm{Tr}[\boldsymbol{Z}\,\boldsymbol{V}] < 1$ for some witness $\boldsymbol{Z}$ always implies that $\boldsymbol{V}$ is entangled. The non-existence of such a witness implies the separability of $\boldsymbol{V}$ only when $\boldsymbol{V}$ is Gaussian.

In the cases in which the PPT criterion of separability is necessary and sufficient, entanglement witnesses provide a lower bound for the logarithmic negativity [And06]. Namely, let $w = \mathrm{Tr}[\boldsymbol{Z}\boldsymbol{V}]$, for a covariance matrix $\boldsymbol{V}$ and an entanglement witness $\boldsymbol{Z}$. If $w \in (0, 1)$, then the logarithmic negativity of $\boldsymbol{V}$ obeys:

$$E_{\mathcal{N}}(\boldsymbol{V}) \geq \log \frac{1}{w}. \tag{6.20}$$

In particular, the inequality is saturated for two-mode covariance matrices when one uses the minimal entanglement witness Z_{min}, giving the smallest possible value w_{min} [And06].

Theorem 6.10 ([And06; HE06])**.** *Let $\boldsymbol{V}$ be the covariance matrix of a k-partite system with $\sum_{j=1}^{k} M_j = M$ modes. Then $\boldsymbol{V}$ is entangled with respect to this partition if and only if*

$$\mathrm{Tr}[\boldsymbol{Z}\boldsymbol{V}] < 1 \tag{6.21}$$

for some real, symmetric $2M \times 2M$ matrix $\boldsymbol{Z}$, satisfying

$$\boldsymbol{Z} \geq 0, \quad \sum_{j=1}^{k} \mathrm{str}[\boldsymbol{Z}_j] \geq \frac{1}{2}, \tag{6.22}$$

where $\boldsymbol{Z}_j$ is the block matrix of the diagonal of $\boldsymbol{Z}$ acting on the subsystem j and $\mathrm{str}[\boldsymbol{Z}_j]$ is the symplectic trace *of $\boldsymbol{Z}_j$, i.e. the sum of its symplectic eigenvalues:*

$$\mathrm{str}[\boldsymbol{Z}_j] := \sum_{m=1}^{M_j} \nu_m. \tag{6.23}$$

6.3 Methods

We here introduce two fundamental tools that we used in [Mih+20]: the semidefinite programs and a scheme for the reconstruction of unknown continuous-variable states via random homodyne measurements.

6.3.1 Semidefinite Programming

Definition 6.11 (Semidefinite programs [VB96; Hel02; BV04])**.** A *semidefinite program* (SDP), or *semidefinite problem*, is an optimisation problem in which one minimises a linear function subject to a *semidefinite constraint*, i.e.

$$\begin{aligned} &\underset{\boldsymbol{x}}{\text{minimise}} \quad \boldsymbol{c}^T \cdot \boldsymbol{x}, \\ &\text{subject to} \quad \boldsymbol{F}^{(0)} + \sum_{j=1}^{n} x_j \, \boldsymbol{F}^{(j)} \geq 0, \end{aligned} \tag{6.24}$$

where $\boldsymbol{x}, \boldsymbol{c} \in \mathbb{R}^n$ for a given n, and $\boldsymbol{F}^{(0)}$ and $\boldsymbol{F}^{(j)}$ $(j = 1, 2, \ldots, n)$ are $m \times m$ Hermitian matrices, for a given m.

Once a problem is formulated as an SDP, there are several efficient algorithms to numerically solve it [Löf04], such as the *interior points-methods* [BV04].

Definition 6.12 (Primal and Dual problem)**.** A semidefinite program in the form of Eq. (6.24) is referred to as a *primal problem* and define a corresponding *dual problem*:

$$\begin{aligned} \underset{\boldsymbol{Z}}{\text{maximise}} \quad & -\operatorname{Tr}[\boldsymbol{F}^{(0)}\,\boldsymbol{Z}], \\ \text{subject to} \quad & \boldsymbol{Z} \geq 0, \\ & \operatorname{Tr}[\boldsymbol{F}^{(j)}\,\boldsymbol{Z}] = c_j, \end{aligned} \tag{6.25}$$

where $\boldsymbol{Z}$ is a $m \times m$ Hermitian matrix.

The *weak duality theorem* [BV04] states that the value of the primal problem is lower-bounded by the value of the dual problem, i.e.

$$\boldsymbol{c}^T\,\boldsymbol{x} + \operatorname{Tr}[\boldsymbol{F}^{(0)}\,\boldsymbol{Z}] \geq 0. \tag{6.26}$$

6.3.2 Quantum Tomography via Homodyne Measurements

D'Auria et al. [DAu+05; DAu+09] introduced a method to reconstruct the covariance matrix of a two-mode quantum state using a single homodyne detection (see Def. 4.26).

Consider a two-mode system, with mode operators $\hat{a}_1$ and $\hat{a}_2$ and corresponding quadrature operators $\hat{q}_i = \sqrt{2}\operatorname{Re}\hat{a}_i$ and $\hat{p}_i = \sqrt{2}\operatorname{Im}\hat{a}_i$. The covariance matrix of a state ρ with zero displacement vector is a 4×4 symmetric matrix that reads (see Eq. (4.51)):

$$\boldsymbol{V} = \begin{pmatrix} 2\,\langle\hat{q}_1^2\rangle & \langle\hat{q}_1\,\hat{p}_1 + \hat{p}_1\,\hat{q}_1\rangle & \langle\hat{q}_1\,\hat{q}_2 + \hat{q}_2\,\hat{q}_1\rangle & \langle\hat{q}_1\,\hat{p}_2 + \hat{p}_2\,\hat{q}_1\rangle \\ \langle\hat{q}_1\,\hat{p}_1 + \hat{p}_1\,\hat{q}_1\rangle & 2\,\langle\hat{p}_1^2\rangle & \langle\hat{p}_1\,\hat{q}_2 + \hat{q}_2\,\hat{p}_1\rangle & \langle\hat{p}_1\,\hat{p}_2 + \hat{p}_2\,\hat{p}_1\rangle \\ \langle\hat{q}_1\,\hat{q}_2 + \hat{q}_2\,\hat{q}_1\rangle & \langle\hat{p}_1\,\hat{q}_2 + \hat{q}_2\,\hat{p}_1\rangle & 2\,\langle\hat{q}_2^2\rangle & \langle\hat{q}_2\,\hat{p}_2 + \hat{p}_2\,\hat{q}_2\rangle \\ \langle\hat{q}_1\,\hat{p}_2 + \hat{p}_2\,\hat{q}_1\rangle & \langle\hat{p}_1\,\hat{p}_2 + \hat{p}_2\,\hat{p}_1\rangle & \langle\hat{q}_2\,\hat{p}_2 + \hat{p}_2\,\hat{q}_2\rangle & 2\,\langle\hat{p}_2^2\rangle \end{pmatrix}. \tag{6.27}$$

Since $\boldsymbol{V}$ is symmetric, it admits at most 10 different entries. Introducing

$$\hat{a}_3 := \frac{\hat{a}_1 + \hat{a}_2}{\sqrt{2}}, \quad \hat{a}_4 := \frac{\hat{a}_1 - \hat{a}_2}{\sqrt{2}}, \quad \hat{a}_5 := \frac{\mathrm{i}\hat{a}_1 + \hat{a}_2}{\sqrt{2}}, \quad \hat{a}_6 := \frac{\mathrm{i}\hat{a}_1 - \hat{a}_2}{\sqrt{2}}, \tag{6.28}$$

the off-diagonal elements of $\boldsymbol{V}$ become (with $V_{ij} = V_{ji}$):

$$\begin{aligned} V_{12} &= \langle\hat{z}_1^2\rangle - \langle\hat{t}_1^2\rangle\,, \qquad V_{13} = \langle\hat{q}_3^2\rangle - \langle\hat{q}_4^2\rangle\,, \qquad V_{14} = \langle\hat{p}_5^2\rangle - \langle\hat{p}_6^2\rangle\,, \\ V_{23} &= \langle\hat{q}_6^2\rangle - \langle\hat{q}_5^2\rangle\,, \qquad V_{24} = \langle\hat{p}_3^2\rangle - \langle\hat{p}_4^2\rangle\,, \qquad V_{34} = \langle\hat{z}_2^2\rangle - \langle\hat{t}_2^2\rangle\,, \end{aligned} \tag{6.29}$$

where $\hat{q}_i = \sqrt{2}\operatorname{Re}\hat{a}_i$, $\hat{p}_i = \sqrt{2}\operatorname{Im}\hat{a}_i$, $\hat{z}_i = \sqrt{2}\operatorname{Re}\left(e^{-\mathrm{i}\pi/4}\,\hat{a}_i\right)$ and $\hat{t}_i = \sqrt{2}\operatorname{Re}\left(e^{\mathrm{i}\pi/4}\,\hat{a}_i\right)$.

One can notice that $\langle\hat{q}_6^2\rangle = \langle\hat{q}_2^2\rangle + \langle\hat{p}_1^2\rangle - \langle\hat{q}_5^2\rangle$ and $\langle\hat{p}_6^2\rangle = \langle\hat{q}_1^2\rangle + \langle\hat{p}_2^2\rangle - \langle\hat{p}_5^2\rangle$. Therefore, $\hat{q}_6$ and $\hat{p}_6$ are not necessary to reconstruct $\boldsymbol{V}$, and one needs to measure 10 quadrature operators, $\hat{q}_j$ and $\hat{p}_j$ ($j = 1, 2, 3, 4, 5$).

The homodyne detection is realised by measuring the generalised quadrature

$$\hat{x}_\theta = \frac{e^{-\mathrm{i}\theta}\,\hat{k} + e^{\mathrm{i}\theta}\,\hat{k}^\dagger}{\sqrt{2}}, \tag{6.30}$$

where θ is the phase of the local oscillator, and $\hat{k}$ is a mixture of $\hat{a}_1$ and $\hat{a}_2$,

$$\hat{k} = \cos\phi\,\hat{a}_1 + \exp(\mathrm{i}\psi)\sin\phi\,\hat{a}_2 = \hat{B}_{12}(\phi\,e^{\mathrm{i}\psi})^\dagger\,\hat{a}_1\,\hat{B}_{12}(\phi\,e^{\mathrm{i}\psi}), \tag{6.31}$$

obtained by a beam splitter $\hat{B}_{12}(\phi\,e^{\mathrm{i}\psi})$ (see Eq. (4.101)), selecting only the first of the two output modes. With repeated measurements of $\hat{x}_\theta$ for a set of identical states, the variance of $\hat{x}_\theta$ is given by:

$$[\Delta\hat{x}_\theta]^2 := \langle\hat{x}_\theta^2\rangle - \langle\hat{x}_\theta\rangle^2 = \mathrm{Tr}[\boldsymbol{P}\,\boldsymbol{V}], \tag{6.32}$$

where $\boldsymbol{P}$ is the matrix for the measurement of the quadrature variance of the mode $\hat{k}$, i.e.

$$\begin{aligned}\boldsymbol{P} &:= \boldsymbol{u}\cdot\boldsymbol{u}^T\\ \boldsymbol{u} &:= \begin{pmatrix}\cos\phi\cos(\theta-\psi)\\ \cos\phi\sin(\theta-\psi)\\ \sin\phi\cos\theta\\ \sin\phi\sin\theta\end{pmatrix}.\end{aligned} \tag{6.33}$$

The setting is visualised in Fig. 6.2. By properly choosing the angles ψ, ϕ, θ, it is possible to measure any quadrature. Note that the publication [DAu+05] used a fixed set of angles, since it made assumptions on the polarisation of the modes. Instead, we did not make assumptions in [Mih+20] and thus we used random angles.

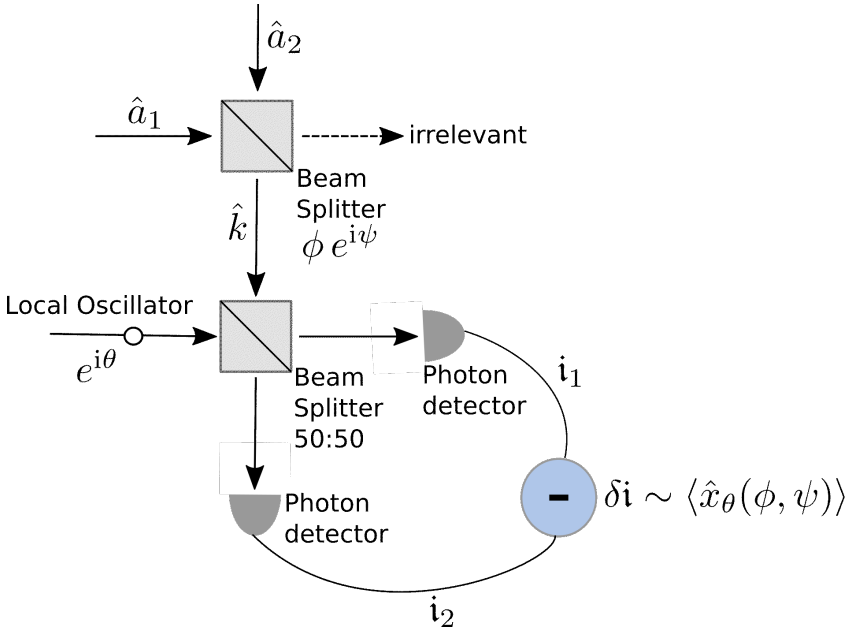

Figure 6.2: A visual depiction of the scheme described in Sec. 6.3.2. The mode operators $\hat{a}_1$ and $\hat{a}_2$ are mixed by a beam splitter $\hat{B}_{12}(\phi\,e^{\mathrm{i}\psi})$ (see Eq. (4.101)). Only one of the outcomes of the beam splitter, denoted by $\hat{k}$, is selected and undergoes a homodyne detection (see Def. 4.26) with a local oscillator of phase θ. The scheme measures the generalised quadrature $\langle\hat{x}_\theta(\phi,\psi)\rangle$ (see Eq. (6.30)).

This detection procedure can be extended to M-mode continuous-variable states by applying the same two-mode beam splitter $M-1$ times among the M modes. An M-mode covariance matrix has $M(M-1)$ parameters.

6.4 Detecting Entanglement of Unknown CV States

In this section, we introduce the results of our publication [Mih+20], in which we proposed a detection scheme for entanglement in unknown continuous-variable states. The original publication, with publication details, can be found in Appendix B.

6.4.1 Results

The idea of [Mih+20] is to find an entanglement witness for a given covariance matrix by using a semidefinite program. The conditions in Theorem 6.10 are not semidefinite constraints, because the symplectic trace is not a linear function. In [Mih+20], we proved the following theorem.

Theorem 6.13. *Theorem 6.10 is satisfied by an entanglement witness $\boldsymbol{Z}$ on a k-partite M-mode system, with $\sum_{j=1}^{k} M_j = M$, if $\boldsymbol{Z}$ fulfills the following conditions:*

$$\boldsymbol{Z} \geq 0, \tag{6.34}$$

$$\boldsymbol{Z}_j + \mathrm{i}\,\frac{x_j}{M_j}\,\boldsymbol{\Omega}_{M_j} \geq 0, \quad x_j \in \mathbb{R}, \quad j = 1, \ldots, k-1, \tag{6.35}$$

$$\boldsymbol{Z}_k + \frac{\mathrm{i}}{M_k}\left(\frac{1}{2} - \sum_{j=1}^{k-1} x_j\right)\boldsymbol{\Omega}_{M_k} \geq 0, \tag{6.36}$$

where $\boldsymbol{Z}_j$ is the block matrix of the diagonal of $\boldsymbol{Z}$ acting on the subsystem j and $\boldsymbol{\Omega}_{M_k} = \bigoplus_{j=1}^{M_k} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is the symplectic form for M_k modes.

These constraints are semidefinite, however they are sufficient but not necessary conditions. Therefore some entanglement witness does not satisfy them.

We then introduced a SDP based on the measurement scheme of Sec. 6.3.2. For simplicity, we describe it for two modes. We have seen in Sec. 6.3.2 that a full reconstruction of the a two-mode covariance matrix $\boldsymbol{V}$ is achieved by 10 measurements. For the generic l-th measurement, the first step is to sample uniformly:

$$0 \leq \theta_l \leq \pi, \tag{6.37}$$

$$0 \leq \phi_l \leq \pi, \tag{6.38}$$

$$0 \leq \psi_l \leq 2\pi, \tag{6.39}$$

and then measure the variance:

$$m_l = \mathrm{Tr}[\boldsymbol{P}_l \boldsymbol{V}], \tag{6.40}$$

where $\boldsymbol{P}_l$ is given by Eq. (6.33). The problem of finding a witness $\boldsymbol{Z}$ for $\boldsymbol{V}$ reduces to finding coefficients c_j such that

$$\mathrm{Tr}[\boldsymbol{Z}\boldsymbol{V}] = \sum_{j=1}^{l} c_j\, m_j \;\Rightarrow\; \boldsymbol{Z} = \sum_{j=1}^{l} c_j\, \boldsymbol{P}_j. \tag{6.41}$$

Hence, we proposed the following semidefinite program:

$$\begin{aligned} \underset{x}{\text{minimise}} \quad & \sum_{j=1}^{l} c_j^x m_j, \\ \text{subject to} \quad & \boldsymbol{Z} = \sum_{j=1}^{l} c_j^x \boldsymbol{P}_j, \\ & \boldsymbol{Z} = \begin{pmatrix} \boldsymbol{Z}_1 & \boldsymbol{Z}_c \\ \boldsymbol{Z}_c^T & \boldsymbol{Z}_2 \end{pmatrix} \geq 0, \\ & \boldsymbol{Z}_1 + \mathrm{i}x\boldsymbol{\Omega} \geq 0, \\ & \boldsymbol{Z}_2 + \mathrm{i}\left(\frac{1}{2} - x\right)\boldsymbol{\Omega} \geq 0. \end{aligned} \tag{6.42}$$

Here, we relabelled the coefficients c_j by c_j^x to emphasise their dependence on the parameter x. If $\mathrm{Tr}[\boldsymbol{Z}_{min}\boldsymbol{V}] = \sum_j c_j^{x_{min}} m_j < 1$, then $\boldsymbol{V}$ is unambiguously entangled. Otherwise one needs to add another measurement and repeat the process. Therefore, the number of required measurements represents a figure of merit for the validity of our method. Since the conditions of Eq. (6.34) are only sufficient, there is a small probability of needing more than 10 measurements to detect the entanglement.

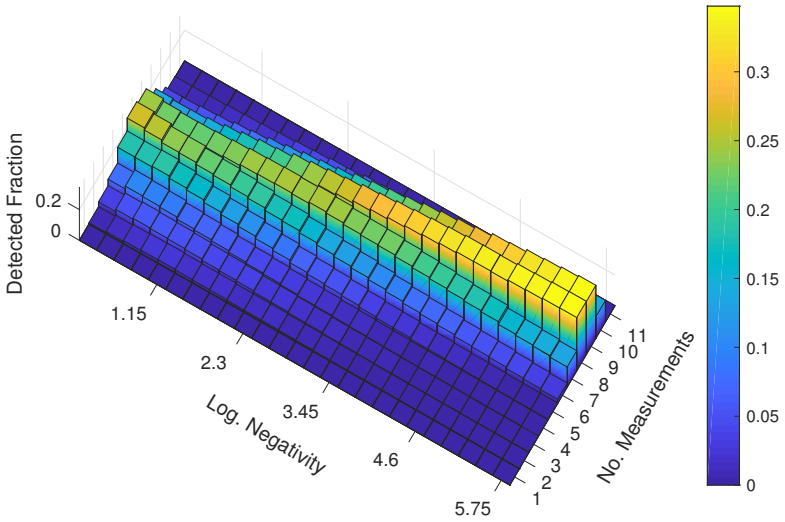

Figure 6.3: 5×10^5 runs of the algorithm on the two-mode squeezed vacuum states with squeezing parameter $r \in [0, 2]$. By successively adding measurements, the witness is evaluated at every round until the presence of entanglement is certified. The data are normalised such that they sum up to one for every value of entanglement. The probability that our method requires more than 10 measurements, in this case, is 0.0094%. The picture is taken from our publication [Mih+20].

We first applied our method to the two-mode squeezed vacuum state, whose logarithmic negativity is proportional to the squeezing parameter r (see Eq. (6.14)). In figure 6.3, we show the fraction of entanglement detection of TMSVSs with squeezing parameter $r \in [0, 2]$ for 5×10^5 runs of the algorithm, as a function of the logarithmic negativity and the number

of measurements. A remarkable result is that lowly entangled states require on average fewer measurements than highly entangled ones. This is due to experimental difficulties [Vah+16] and to the geometry of the squeezed quadrature variances in phase space (see [Mih+20]). The probability that our method needs more than 10 measurements (full tomography) is very low (0.0094%).

We then tested our method for a random two-mode covariance matrix $\boldsymbol{V}$ (see Eq. (4.111)):

$$\boldsymbol{V} = \boldsymbol{O}_2^T \left[\boldsymbol{S}_{SMS}(r_1) \oplus \boldsymbol{S}_{SMS}(r_2)\right] \boldsymbol{O}_1^T \left[\nu_1 \boldsymbol{I} \oplus \nu_2 \boldsymbol{I}\right] \boldsymbol{O}_1 \left[\boldsymbol{S}_{SMS}(r_1) \oplus \boldsymbol{S}_{SMS}(r_2)\right] \boldsymbol{O}_2, \quad (6.43)$$

where $\nu_1, \nu_2 \geq 1$ are symplectic eigenvalues, $\boldsymbol{S}_{SMS}(r_1), \boldsymbol{S}_{SMS}(r_2)$ are single-mode squeezers with parameter r_j, and $\boldsymbol{O}_1, \boldsymbol{O}_2$ are orthogonal symplectic matrices. Therefore, we first generated ν_j and r_j by sampling from uniform distributions in finite real intervals,

$$\nu_j \in [1, t] \quad \text{and} \quad r_j \in [0, s], \quad (6.44)$$

for $t > 1$ and $s > 0$. Then, we sampled $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ from the set of orthogonal symplectic matrices [DMS+95]. In figure 6.4, we show the fraction of entanglement detection of a two-mode random covariance matrix $\boldsymbol{V}$ for 5×10^5 runs of the algorithm, as a function of the logarithmic negativity (calculated by Eq. (6.20)) and the number of measurements. In this case, there is an improvement in the efficiency of entanglement detection for highly entangled states compared to lowly entangled states. The probability that our method needs more than 10 measurements (full tomography) is again very low (0.05%).

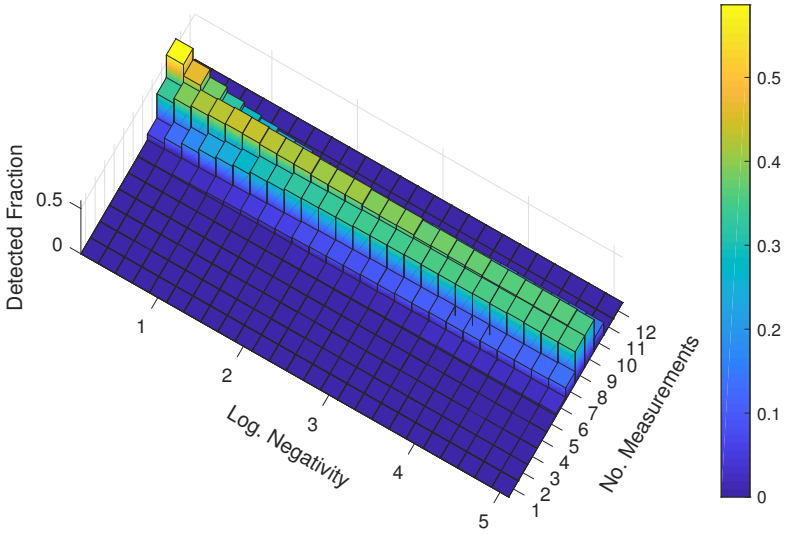

Figure 6.4: 5×10^5 runs of the algorithm on random two-mode CMs for $\nu_i \in [1, 5]$ and $r_i \in [0, 2]$. By successively adding measurements, the EW is evaluated at every round until the presence of entanglement is certified. The data are normalised such that they sum up to one for every value of entanglement. The probability that our method requires more than 10 measurements, in this case, is 0.05%. The picture is taken from our publication [Mih+20].

Our scheme is applicable also to M-mode covariance matrices, with $M > 2$. We considered

the four-mode covariance matrix

$$\boldsymbol{V}_{BE} = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 4 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}, \tag{6.45}$$

which is bound entangled [WW01], i.e. entangled with positive partial transpose. In figure 6.5, we show the fraction of entanglement detection of $\boldsymbol{V}_{BE}$ for 10^4 runs of the algorithm, as a function of the number of measurements. A full tomography corresponds to 36 measurements ($M[2M+1]$ with $M=4$) and our method needs on average 33 random measurements.

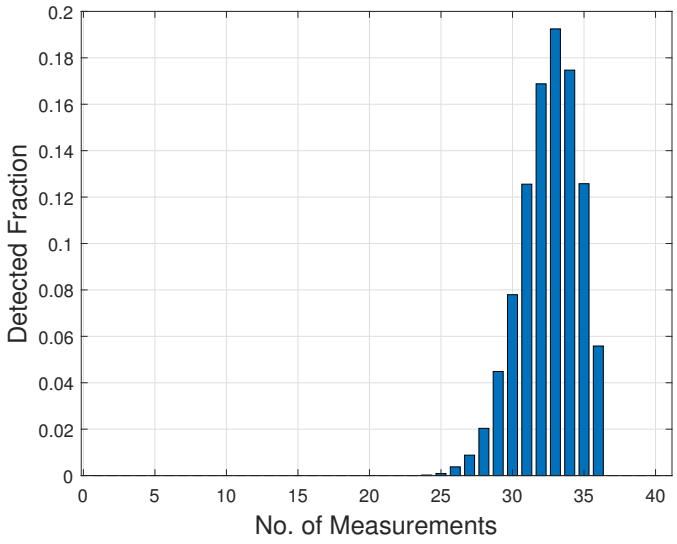

Figure 6.5: 10^4 runs of the algorithm on the four-mode bipartite bound entangled CM in Eq. (6.45). The data are normalised such that they sum up to one. The picture is taken from our publication [Mih+20].

We concluded our analysis by performing statistical analysis, to take into account the statistical fluctuations that are encountered in real experiments. Although our method also detects entanglement in non-Gaussian states, we only considered Gaussian states, for which we can assume that the outcomes of n_i repeated homodyne measurements for a fixed direction θ_i follow a Gaussian distribution. The sample variance $\bar{P}_i$, which estimates the variance $m_i = \Delta(\hat{x}_{\theta_i})^2$, is given by:

$$\bar{P}_i = \frac{1}{n_i - 1} \sum_{j=1}^{n_i} \left(X_{ij} - \bar{X}_i\right)^2, \tag{6.46}$$

where $X_{ij} = \langle \hat{x}_{\theta_i} \rangle_j$ $(j = 1, \ldots, N_i)$ and $\bar{X}_i$ is the sample mean,

$$\bar{X}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} X_{ij}. \tag{6.47}$$

The estimated value of $\mathrm{Tr}[\boldsymbol{z}\boldsymbol{V}]$, denoted by $\bar{Z}$, is given by:

$$\bar{Z} = \sum_i c_i \bar{P}_i, \tag{6.48}$$

where i labels a measuring setting and c_i is the coefficient that we get from solving the SDP of Eq. (6.42). Since the data follows a Gaussian distribution, the sample variance for n_I repetitions of the measurement follows the $\chi^2_{n_i-1}$ distribution [Kni00] for $n_i - 1$ degrees of freedom, i.e.

$$\frac{n_i - 1}{m_i} \bar{P}_i \sim \chi^2_{n_i-1}. \tag{6.49}$$

By considering that number of measurement repetitions equal for every measurement direction, i.e. $n_i = n$ for every i, and using the error propagation formula we showed that the uncertainty of $\bar{Z}$ reads:

$$\Delta(\bar{Z}) = \sqrt{\frac{2}{n}} \sqrt{\sum_i c_i^2 m_i^2}. \tag{6.50}$$

In figure 6.6, we consider the single detection of an entangled CM $\boldsymbol{V}$, with $\mathrm{Tr}[\boldsymbol{Z}_{min}\boldsymbol{V}] = 0.852$, and plot the 3σ confidence of $\mathrm{Tr}[\boldsymbol{Z}\boldsymbol{V}]$ as a function of the number n of measurement repetitions. A certification of $\mathrm{Tr}[\boldsymbol{Z}\boldsymbol{V}] < 1$ with 99.7%-confidence is possible for 6 measurements requiring a high number of repetitions of the measurements. This number significantly decreases with additional measuring settings, thus confirming the validity of our method also in realistic scenarios.

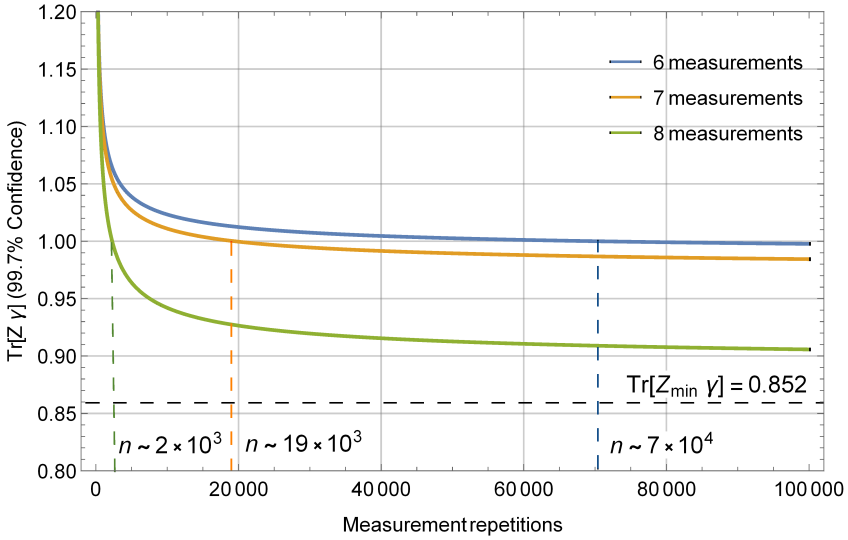

Figure 6.6: The value of the witness with 95%-confidence for Gaussian states, as obtained by the statistical estimate according to Eq. (6.50). The picture is taken from our publication [Mih+20].

7

Hierarchy of Quantum Resource Theories

Quantum resource theories (QRTs) [CG19] provide a framework for quantitatively studying different quantum phenomena. The set of quantum states is partitioned into two groups, the *free states* and *resource states*. Consequently, quantum operations are called *free* when they transform any free state into a free state. The set of free states and operations are identified by given theoretical or practical constraints, for which only some operations can be (easily) implemented or only some states can be (easily) prepared. Quantum resource theories provide meaningful ways to quantify given physical resources, through *resource monotones*.

This chapter is an introduction to our publication [GKB21], which is contained in full in Appendix C. In this article, we established a hierarchy of continuous-variable resources, namely purity, coherence, discord and entanglement. Our results represent the continuous-variable counterpart to an analogous hierarchy of discrete-variable resources [Str+18].

This chapter is structured as follows. In Sec. 7.1, the general formalism associated with quantum resource theories is introduced. The discrete-variable resource theories of coherence, purity, entanglement and discord are discussed in Sec. 7.2, while their extensions to continuous variables are addressed in Sec. 7.3. Finally, in Sec. 7.4, we summarise [GKB21], and discuss possible research outlooks. Besides [GKB21], the content of this chapter is mostly inspired from [CG19; Str+18; SAP17; Gou+15].

7.1 Resource Theories

In this section, we introduce basic definitions and properties of general quantum resource theories. In the following, the set of density operators over a Hilbert space $\mathcal{H}$ is denoted by $\mathcal{S}(\mathcal{H})$ and the set of quantum operations (channels) from $\mathcal{S}(\mathcal{H})$ to itself is denoted by $\mathcal{Q}(\mathcal{H})$.

Definition 7.1 (Quantum resource theory [CG19])**.** Let $\mathcal{O}(\mathcal{H}) \subset \mathcal{Q}(\mathcal{H})$ and $\mathcal{F}(\mathcal{H}) \subset \mathcal{S}(\mathcal{H})$ be non-empty subsets of the sets of quantum channels $\mathcal{Q}(\mathcal{H})$ and densities $\mathcal{S}(\mathcal{H})$, respectively. A *quantum resource theory* (QRT) is a tuple $(\mathcal{O}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$ that satisfies the following conditions:

1. $\mathcal{O}(\mathcal{H})$ contains the identity map $\mathrm{id}_{\mathcal{H}}$ over $\mathcal{S}(\mathcal{H})$;

2. The composition of channels in $\mathcal{O}(\mathcal{H})$ is closed in $\mathcal{O}(\mathcal{H})$, i.e. $\Phi \circ \Lambda \in \mathcal{O}(\mathcal{H})$ for any $\Phi, \Lambda \in \mathcal{O}(\mathcal{H})$;

3. Channels in $\mathcal{O}(\mathcal{H})$ map $\mathcal{F}(\mathcal{H})$ to itself, i.e. $\Lambda[\rho] \in \mathcal{F}(\mathcal{H})$ for any $\Lambda \in \mathcal{O}(\mathcal{H})$ and $\rho \in \mathcal{F}(\mathcal{H})$.

$\mathcal{F}(\mathcal{H})$ and $\mathcal{O}(\mathcal{H})$ are called the sets of *free states* and *free operations*, respectively. Conversely, any $\sigma \in \mathcal{S}(\mathcal{H}) \backslash \mathcal{F}(\mathcal{H})$ is called a *resource state*.

The conditions in Def. 7.1 formalise intuitive ideas of what "free" and "resourceful" mean for quantum states and operations. The identity map has always to be free in every resource theory, as it represents the action of doing nothing. The second condition guarantees that different free operations can be freely applied multiple times and in any possible combination. The third condition finally ensures that resource states cannot be created "for free", i.e. by applying free operations on free states. The set of free states $\mathcal{F}(\mathcal{H})$ has to be strictly included in $\mathcal{S}(\mathcal{H})$, i.e. $\mathcal{F}(\mathcal{H}) \neq \mathcal{S}(\mathcal{H})$, otherwise the resource theory would be trivial. Analogously, $\mathcal{O}(\mathcal{H}) \neq \mathcal{Q}(\mathcal{H})$.

Def. 7.1 provides a minimal set of requirements for defining a quantum resource theory. Depending on the theory, more assumptions may be needed. We here present some of the most relevant ones [CG19].

Definition 7.2. A QRT $(\mathcal{O}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$ admits a *tensor-product structure* if the following conditions are met:

- The free operations are *completely free*, i.e. for any free operation $\Lambda_A \in \mathcal{O}(\mathcal{H}_A)$, $\Lambda_A \otimes \mathrm{id}_B \in \mathcal{O}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where id_B is the identity map for density operators acting on an arbitrary Hilbert space $\mathcal{H}_B$;

- The tensor product of free states is a free state, i.e. $\rho_A \otimes \sigma_B \in \mathcal{F}(\mathcal{H}_A \otimes \mathcal{H}_B)$ for any $\rho_A \in \mathcal{F}(\mathcal{H}_A)$ and $\sigma_B \in \mathcal{F}(\mathcal{H}_B)$, and for any $\mathcal{H}_A, \mathcal{H}_B$;

- The trace and partial trace are free operations. Consequently, $\rho_A = \mathrm{Tr}_B[\rho_{AB}] \in \mathcal{F}(\mathcal{H}_A)$ for any $\rho_{AB} \in \mathcal{F}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

Definition 7.3. A QRT $(\mathcal{O}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$ is a *convex resource theory* if the sets $\mathcal{O}(\mathcal{H})$ and $\mathcal{F}(\mathcal{H})$ are convex, i.e. for a probability distribution $\{p_i\}$, with $p_i \geq 0$ and $\sum_i p_i = 1$, it holds:

$$\sum_i p_i \Lambda_i \in \mathcal{O}(\mathcal{H}), \qquad \forall\, \Lambda_i \in \mathcal{O}(\mathcal{H}), \tag{7.1}$$

$$\sum_i p_i \rho_i \in \mathcal{F}(\mathcal{H}), \qquad \forall\, \rho_i \in \mathcal{F}(\mathcal{H}). \tag{7.2}$$

Usually, the sets of free states and operations are not selected simultaneously. In many resource theories (e.g coherence, see Sec. 7.2.1), a set of free states $\mathcal{F}(\mathcal{H}) \subset \mathcal{S}(\mathcal{H})$ is identified by properties related to the resource. Afterwards, the operations that transform any free state into a free state are defined as free operations.

Definition 7.4. Let $\mathcal{F}(\mathcal{H}) \subset \mathcal{S}(\mathcal{H})$ be a set of free free states. A set $\mathcal{O}_{max}(\mathcal{H}) \subset \mathcal{Q}(\mathcal{H})$ of quantum operations is said to be the set of *maximally free operation* if it contains all the operations Λ such that

$$\Lambda[\rho] \in \mathcal{F}(\mathcal{H}), \qquad \forall\, \rho \in \mathcal{F}(\mathcal{H}). \tag{7.3}$$

The set $\mathcal{O}_{max}(\mathcal{H})$ is convex if and only if $\mathcal{F}(\mathcal{H})$ is convex [CG19].

7.1.1 Quantifying Resources

Definition 7.5. Let $(\mathcal{O}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$ be a quantum resource theory (see Def. 7.1). A function $f : \mathcal{F}(\mathcal{H}) \to \mathbb{R}_{\geq 0}$ is called a *resource monotone* if:

$$\rho \in \mathcal{F}(\mathcal{H}) \Rightarrow f(\rho) = 0; \tag{7.4}$$

$$f\left(\Lambda[\rho]\right) \leq f(\rho), \qquad \forall\, \Lambda \in \mathcal{O}(\mathcal{H}). \tag{7.5}$$

Resource monotones are used to quantify the amount of resource in a quantum states. Depending on the specific resource theory, *resource measures* are defined as resource monotones with additional properties, which may be:

(Sub) additivity. A resource monotone f is *subadditive* if, for all $\rho, \sigma \in \mathcal{S}(\mathcal{H})$,

$$f(\rho \otimes \sigma) \leq f(\rho) + f(\sigma). \tag{7.6}$$

When the equality holds in Eq. (7.6) for all states, the function is *additive*.

Convexity. A resource monotone f is *convex* if:

$$f\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i\, f(\rho_i), \tag{7.7}$$

for any collection of states $\rho_i \in \mathcal{S}(\mathcal{H})$ and probability distribution $\{p_i\}$, with $p_i \geq 0$ and $\sum_i p_i = 1$.

A relevant class of resource monotone are based on *contractive distances*, i.e. distances $d : \mathcal{S}(\mathcal{H}) \times \mathcal{S}(\mathcal{H}) \to \mathbb{R}_{\geq 0}$ such that:

$$d\left(\Lambda[\rho], \Lambda[\sigma]\right) \;\leq\; d(\rho, \sigma), \tag{7.8}$$

for any $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ and $\Lambda \in \mathcal{Q}(\mathcal{H})$.

Theorem 7.6. *Let $\mathcal{F}(\mathcal{H})$ be a set of free states and d be a contractive distance (see Eq.* (7.8)*). Then,*

$$\mathcal{R}_d(\rho) = \inf_{\sigma \in \mathcal{F}(\mathcal{H})} d(\rho, \sigma). \tag{7.9}$$

is a resource monotone for the quantum resource theory $(\mathcal{O}_{max}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$, where $\mathcal{O}_{max}(\mathcal{H})$ is the set of maximally free operations (see Def. 7.4) for $\mathcal{F}(\mathcal{H})$.

It is immediate to verify that $\mathcal{R}_d(\rho) = 0$ for any $\rho \in \mathcal{F}(\mathcal{H})$. The monotonicity follows from the contractivity of d and from the fact that $\Lambda[\sigma] \in \mathcal{F}(\mathcal{H})$ for all $\sigma \in \mathcal{F}(\mathcal{H})$ and $\Lambda \in \mathcal{O}_{max}(\mathcal{H})$:

$$\mathcal{R}_d\left(\rho\right) = \inf_{\sigma \in \mathcal{F}(\mathcal{H})} d(\rho, \sigma) \geq \inf_{\sigma \in \mathcal{F}(\mathcal{H})} d\left(\Lambda[\rho], \lambda[\sigma]\right) = \inf_{\tau \in \mathcal{F}(\mathcal{H})} d\left(\Lambda[\rho], \tau\right) = \mathcal{R}_d\left(\Lambda[\rho]\right). \tag{7.10}$$

Note that the monotonocity under $\mathcal{O}_{max}(\mathcal{H})$ implies the monotonicity under any set of free operations $\mathcal{O}(\mathcal{H}) \subseteq \mathcal{O}_{max}(\mathcal{H})$.

It is possible to include in this family resources measures based on entropic pseudo-distances, such as the relative entropy (see Def. 3.18).

Definition 7.7. For a quantum resouce theory $(\mathcal{O}(\mathcal{H}), \mathcal{F}(\mathcal{H}))$, the *relative entropy* of resource is the quantity

$$\mathcal{R}_{rel}(\rho) = \inf_{\sigma \in \mathcal{F}(\mathcal{H})} S(\rho \| \sigma), \tag{7.11}$$

where $S(\rho\|\sigma) := -S(\rho) + \mathrm{Tr}[\rho \log \sigma]$ is the quantum relative entropy of ρ and σ.

7.2 Discrete-variable Resource Theories

We here introduce a selection of resource theories that are relevant to this thesis. Namely, we address the resource theories of coherence (see Sec. 7.2.1), athermality and purity (see Sec. 7.2.2), entanglement (see Sec. 7.2.3) and discord (see Sec. 7.2.4). We conclude this section by showing their connection in Sec. 7.2.5.

7.2.1 Resource Theory of Coherence

When we introduced qubits (see Sec. 3.1.1), we discussed that their main advantage with respect to classical bits is the possibility of having superpositions of the basis states $|0\rangle$ and $|1\rangle$. This property is quantified by the resource theory of *quantum coherence* [Åbe06; BCP14; LM14; WY16].

Definition 7.8 (Incoherent states [SAP17])**.** Let $\{|i\rangle\}$ be an orthonormal basis for a d-dimensional Hilbert space $\mathcal{H}$. A state $\rho_I \in \mathcal{S}(\mathcal{H})$ is said to be *incoherent* in the basis $\{|i\rangle\}$ if it is diagonal in such basis, i.e.

$$\rho_I = \sum_{i=0}^{d-1} p_i \, |i\rangle \langle i| \,, \tag{7.12}$$

where $\{p_i\}$ is a probability distribution, with $p_i \geq 0$ and $\sum_i p_i = 1$.

The set of incoherent states, denoted by $\mathcal{I}$, is the set of free states for the resouce theory of coherence. From Def. 7.8, we see that $\mathcal{I}$ is a convex set, therefore the resource theory of coherence is convex.

Definition 7.9 (Dephasing operator [SAP17])**.** Let $\{|i\rangle\}$ be an orthonormal basis for a Hilbert space $\mathcal{H}$ of dimension d and $\mathcal{I} \subset \mathcal{S}(\mathcal{H})$ be the set of incoherent states in the basis $\{|i\rangle\}$. The *dephasing operator* is the channel $\Delta : \mathcal{S}(\mathcal{H}) \to \mathcal{I}$ that is defined as:

$$\Delta[\rho] := \sum_{i=0}^{d-1} |i\rangle \langle i| \, \rho \, |i\rangle \langle i| \,. \tag{7.13}$$

Any quantum state $\rho = \sum_{j,k} p_{jk} \, |j\rangle \langle k| \in \mathcal{S}(\mathcal{H})$ is mapped by Δ to an incoherent state:

$$\Delta[\rho] = \sum_{i=0}^{d-1} |i\rangle \langle i| \, \rho \, |i\rangle \langle i| = \sum_{i=0}^{d-1} |i\rangle \langle i| \left(\sum_{j,k=0}^{d-1} p_{jk} \, |j\rangle \langle k| \right) |i\rangle \langle i| = \sum_{i=0}^{d-1} p_{ii} \, |i\rangle \langle i| \,. \tag{7.14}$$

For an incoherent state ρ_I, $p_{jk} = p_j \delta_{jk}$. By inserting this condition in Eq. (7.14), we see that

$$\Delta[\rho_I] = \rho_I \;\Leftrightarrow\; \rho_I \in \mathcal{I}. \tag{7.15}$$

The maximal set of free operations (see Def. 7.4) in the resource theory of coherence is called the set of *maximally incoherent operations* (MIO) [Åbe06]. It contains all channels $\Lambda_{MIO} \in \mathcal{Q}(\mathcal{H})$ such that:

$$\Lambda_{MIO}[\rho_I] \in \mathcal{I}, \quad \forall \, \rho_I \in \mathcal{I}. \tag{7.16}$$

A smaller subset of free states is the set of *incoherent operations* (IO) [BCP14], which is formed by those operations Λ_{IO} that admit a Kraus decomposition (see Theorem 3.13) in terms of incoherent Kraus operators. Namely, $\Lambda_{IO}[\rho] = \sum_i \hat{K}_i \rho \hat{K}_i^\dagger$, with

$$\frac{\hat{K}_i \, \rho_I \, \hat{K}_i^\dagger}{\mathrm{Tr}[\hat{K}_i \, \rho_I \, \hat{K}_i^\dagger]} \in \mathcal{I}, \qquad \forall \, \rho_I \in \mathcal{I}. \tag{7.17}$$

This definition ensures that IOs cannot generate coherence probabilistically. It holds that IO is a strict subset of MIO [WY16; CG16a; CG16b],

$$IO \subset MIO. \tag{7.18}$$

We refer to [SAP17] for a detailed review of other relevant subsets of free operations.

Definition 7.10. A *coherence measure* (see Sec. 7.1.1) is a function $\mathcal{C}$ that is required to satisfy the following axioms [Åbe06; BCP14].

(C1) Non-negativity: $\mathcal{C}(\rho) \geq 0$ for any density operator $\rho \in \mathcal{S}(\mathcal{H})$ and $\mathcal{C}(\rho) = 0$ if and only if $\rho \in \mathcal{I}$;

(C2) Monotonicity under a given sets of free operations, e.g. MIO: $\mathcal{C}(\rho) \geq \mathcal{C}(\Lambda_{MIO}[\rho])$ for any $\Lambda_{MIO} \in MIO$;

(C3) Convexity: $\sum_i p_i \, \mathcal{C}(\rho_i) \geq \mathcal{C}\left(\sum_i p_i \, \rho_i\right)$ for any set of probabilities $\{p_i\}$.

The condition (C2) is often replaced by the following stronger condition.

(C2') Strong monotonicity: $\mathcal{C}$ does not increase on average under selective incoherent operations, i.e.

$$\sum_i q_i \, \mathcal{C}(\sigma_i) \leq \mathcal{C}(\rho), \tag{7.19}$$

where $q_i = \mathrm{Tr}(\hat{K}_i \rho \hat{K}_i^\dagger)$, $\sigma_i = \hat{K}_i \rho \hat{K}_i^\dagger / p_i$ and $\{\hat{K}_i\}$ is a set of incoherent Kraus operators (see Eq. (7.17)).

Indeed, the conditions (C2') and (C3) together imply (C2) for the set IO [BCP14].

Among distance-based coherence measures (see Theorem 7.6), the *relative entropy of coherence* (see Eq. (7.11)),

$$\mathcal{C}_{rel}(\rho) := \min_{\sigma \in \mathcal{I}} S(\rho \| \sigma), \tag{7.20}$$

is particularly relevant, because it admits a simple closed expression [Åbe06; BCP14]:

$$\mathcal{C}_{rel}(\rho) = S(\Delta[\rho]) - S(\rho), \tag{7.21}$$

where Δ is the dephasing operator (see Def. 7.9).

Since coherence is a basis-dependent concept, unitary operations are not, in general, free operations.

Definition 7.11 (Maximally coherent mixed state [Sin+15; Yao+16a])**.** A state $\rho_{max} \in \mathcal{S}(\mathcal{H})$ is a *maximally coherent mixed state* (MCMS) with respect to a coherence monotone $\mathcal{C}$ (see Def. 7.10) if ρ_{max} maximises, via unitary operations, the coherence of a given $\rho \in \mathcal{S}(\mathcal{H})$ with respect to a coherence measure $\mathcal{C}$, i.e.

$$\mathcal{C}(\rho_{max}) = \mathcal{C}_{max}(\rho) := \sup_{\hat{U}} \mathcal{C}(\hat{U} \rho \hat{U}^\dagger). \tag{7.22}$$

Relevant results for the MCMS were found in [Str+18].

Theorem 7.12. *Let* $\{|n_+\rangle\}$ *be a* mutually unbiased basis *with respect to the incoherent basis* $\{|i\rangle\}$*, i.e. a basis such that for any* $|n_+\rangle$ *and* $|i\rangle$ *it holds:*

$$|\langle i|n_+\rangle|^2 = \frac{1}{d}, \tag{7.23}$$

where d *is the dimension of the Hilbert space. Among all the states* ρ *with a fixed spectrum* $\{p_n\}$*, the state*

$$\rho_{max} = \sum_{n=1}^{d} p_n \, |n_+\rangle\langle n_+| \tag{7.24}$$

is the maximally coherent mixed state with respect to any MIO monotone.

Theorem 7.13. *Let* $\mathcal{C}_d$ *be the coherence monotone based on a contractive distance* d *(see Theorem 7.6). The maximal coherence of a state* ρ *with respect to* $\mathcal{C}_d$ *is given by:*

$$\mathcal{C}_{d;max}(\rho) = \mathcal{C}_d(\rho_{max}) = d(\rho, \hat{I}/d), \tag{7.25}$$

where $\hat{I}/d$ *is the maximally mixed state for the dimension* d*.*

We conclude this section by noting that, for a composite M-partite system, the incoherent states are in the form [BCA15; Str+15]:

$$\rho_I = \sum_{i_1,\ldots,i_M} p_{i_1,\ldots,i_M} |i_1\rangle\langle i_1| \otimes \cdots \otimes |i_M\rangle\langle i_M|, \tag{7.26}$$

where $\{p_{i_1,\ldots,i_M}\}$ is a M-partite probability distribution, and $\{|i_j\rangle\langle i_j|\}$ is a local orthonormal basis for the j-th system. The results of this section straightforwardly extend to multipartite systems, considering $\{|\boldsymbol{i}\rangle\} := \{|i_1\rangle \otimes \cdots \otimes |i_M\rangle\}$ as the incoherent basis.

7.2.2 Resource Theories of Athermality and Purity (Non-uniformity)

The formalism of quantum resource theories has been recognised as an important tool for quantum thermodynamics [Bra+13; Bra+15; MO17; NW18; Los19]. For instance, the *resource theory of athermality* has been formulated to study the interactions between a system and a thermal bath at temperature T under the condition of global energy conservation.

The free states of this resource theory are those in thermal equilibrium with the bath, i.e Gibbs states (see Theorem 4.20) $\tau_\beta(\hat{H}) = e^{-\beta\hat{H}}/\mathrm{Tr}\left[e^{-\beta\hat{H}}\right]$, where $\hat{H}$ is the Hamiltonian of the system and $\beta = 1/\kappa T$, with κ being the Boltzmann's constant.

Definition 7.14 (Gibbs-preserving operations [NW18])**.** The maximal set of free operations (see Def. 7.4) in the resource theory of athermality is called the set of *Gibbs-preserving operations* (GP), i.e. the set of all operation Λ_{GP} such that:

$$\Lambda_{GP}[\tau_\beta(\hat{H})] = \tau_\beta(\hat{H}), \tag{7.27}$$

where $\tau_\beta(\hat{H})$ is the Gibbs state for the Hamiltonian $\hat{H}$ and the inverse temperature β of the system.

Definition 7.15 (Thermal operations [Jan+00; Bra+13; NW18])**.** Let S be a system with Hamiltonian $\hat{H}_S$. A quantum channel Λ_{TO} is called a *β-thermal operation* (TO) if and only if admits a Stinespring dilation (see Theorem 3.14) in the form:

$$\Lambda_{TO}[\rho] = \mathrm{Tr}_E \left[\hat{U}_{SE} \left(\rho \otimes \tau_\beta(\hat{H}_E)\right) \hat{U}_{SE}^\dagger\right], \tag{7.28}$$

where $\tau_\beta(\hat{H}_E)$ is the Gibbs state for an environmental system E with Hamiltonian $\hat{H}_E$ and $\hat{U}_{SE}$ is an *energy-preserving unitary operation* on the composite system SE, i.e. $[\hat{U}_{SE}, \hat{H}_{tot}] = 0$, with $\hat{H}_{tot} := \hat{H}_S \otimes \hat{I}_E + \hat{I}_S \otimes \hat{H}_E$.

Thermal operations are a more physically relevant set of free operations since they have a clear physical interpretation in terms of energy exchanges between the system S and an environment E.

A special case of this resource theory, which is relevant in quantum information theory, emerges when the Hamiltonian of the system has a fully degenerate spectrum, i.e. the Hamiltonian is in the form $\hat{H} = E\hat{I}_d$, where $\hat{I}_d$ is the d-dimensional identity operator and $E \in \mathbb{R}$. We can easily see that the Gibbs state for this system at any temperature is the d-dimensional maximally mixed state:

$$\frac{e^{-\beta E \hat{I}_d}}{\mathrm{Tr}\left[e^{-\beta E \hat{I}_d}\right]} = \frac{e^{-\beta E}\hat{I}_d}{e^{-\beta E}\mathrm{Tr}\left[\hat{I}_d\right]} = \frac{\hat{I}_d}{d}, \tag{7.29}$$

and any unitary operator commutes with the Hamiltonian. Therefore the system cannot exchange energy with the environment, but only entropy.

This resource theory has been called *resource theory of purity* or of *non-uniformity* [Gou+15]. The latter term is preferred when there is the need to stress the dimensional dependence in the theory since pure states with different dimensions generally have a different resource content.

The Gibbs-preserving channels are replaced by the *unital operations* [MW09], i.e. the operations Λ_U that preserve the maximally mixed state:

$$\Lambda_U\left[\frac{\hat{I}}{d}\right] = \frac{\hat{I}}{d}, \tag{7.30}$$

and the thermal operations are replaced by the *noisy operations* (NO) [HHO03; Hor+03], i.e. the operations that admit a Stinespring dilation (see Theorem 3.14) in the form:

$$\Lambda_{NO}[\rho] = \mathrm{Tr}_E \left[\hat{U}_{SE} \left(\rho \otimes \frac{\hat{I}_{d_E}}{d_E}\right) \hat{U}_{SE}^\dagger\right], \tag{7.31}$$

where $\hat{I}_{d_E}/d_E$ is the maximally mixed state for an environmental d_E-dimensional system E and $\hat{U}_{SE}$ is a unitary operation on the composite system SE.

Definition 7.16. A *purity measure* (see Sec. 7.1.1) is a function $\mathcal{P}$ that satisfies the following requirements [Gou+15; Str+18].

(P1) Non-negativity: $\mathcal{P}(\rho) \geq 0$ for any density operator $\rho \in \mathcal{S}(\mathcal{H})$ and $\mathcal{P}(\rho) = 0$ if and only if $\rho = \hat{I}_d/d$;

(P2) Monotonicity under unital operations: $\mathcal{P}(\rho) \geq \mathcal{P}(\Lambda_U[\rho])$ for any unital operation Λ_U;

(P3) Additivity: $\mathcal{P}(\rho \otimes \sigma) = \mathcal{P}(\rho) + \mathcal{P}(\sigma)$ for any two states ρ and σ;

(P4) Maximal value for pure states: $\mathcal{P}(|\psi\rangle \langle\psi|) = \log d$ for any pure state $|\psi\rangle$ on a system of dimension d.

7.2.3 Resource Theory of Entanglement

We have already seen, in the previous chapters, that quantum entanglement is one of the most important phenomena in quantum information theory. Not surprisingly, the resource theory of entanglement is one of the oldest and most developed resource theories [PV07; Hor+09].

For simplicity of notation, we only consider bipartite entanglement in this subsection. The set of free states $\mathfrak{S}$ is then the convex set of bipartite separable states (see Def. 3.8) $\rho_{AB} = \sum_k p_k \rho_A^k \otimes \rho_B^k$, where $p_i \geq 0$ and $\sum_i p_i = 1$. The extension to the multipartite case is achieved by letting $\mathfrak{S}$ be the set of fully separable multipartite states (see Def. 6.1).

Definition 7.17 (Separable operations [Ved+97; Rai01])**.** The maximal set of free operations (see Def. 7.4) associated to the set $\mathfrak{S}$ of bipartite separable states of a system AB is called the set of *separable operations*. It contains all channels $\Lambda_{sep} \in \mathcal{Q}(\mathcal{H}_{AB})$ that admit a Kraus decomposition (see Theorem 3.13) in terms of tensor product Kraus operators:

$$\Lambda_{sep}[\rho] = \sum_k \left(\hat{A}_k \otimes \hat{B}_k\right) \rho \left(\hat{A}_k \otimes \hat{B}_k\right)^\dagger, \tag{7.32}$$

where $\hat{A}_k$ and $\hat{B}_k$ act on the subsystems A and B, respectively.

An important subset of free operations is the set of *local operations and classical communications* (LOCC) [Ben+96a; Ben+96b; Ved+97]. This set describes the realistic physical scenarios in which two distant parties, Alice and Bob, are freely allowed to exchange classical information and perform arbitrary local quantum operations on their individual subsystems. The parties are not allowed to transfer quantum information or perform non-product operations on the composite system. Despite its adherence to the experimental reality, this set is characterised by a very complex mathematical structure [Gru+08; Hor+09; Chi+14].

There are several types of *entanglement measures* [Hor+09], with different properties. Any measure $\mathcal{E}$ has to be an *entanglement monotone* (see Def. 7.5), i.e. $\mathcal{E}$ needs to satisfy the following requirements.

(E1) Non-negativity: $\mathcal{E}(\rho) \geq 0$ for any $\rho \in \mathcal{S}(\mathcal{H})$ and $\mathcal{E}(\rho_S) = 0$ for any $\rho_S \in \mathfrak{S}$;

(E2) Monotonicity under separable operations Λ_{sep} or smaller subsets of free operations, i.e. $\mathcal{E}(\rho) \geq \mathcal{E}(\Lambda_{sep}(\rho))$ for any separable operation Λ_{sep}.

We have seen an example of entanglement measure, the logarithmic negativity (see Def. 6.6), which was shown to be a monotone under LOCC [VW02]]. Distance-based entanglement measures (see Theorem 7.6), such as the *relative entropy of entanglement*,

$$\mathcal{E}_{rel}(\rho) := \inf_{\sigma \in \mathfrak{S}} S(\rho \| \sigma), \tag{7.33}$$

were introduced in [Ved+97; VP98].

7.2.4 Resource Theory of Discord

Two systems A and B are correlated if together they contain more information than taken separately. The correlations between A and B may be classical or quantum, and are quantified by the quantum mutual information (see Eq. (3.70)) $I(A:B) = S(A) - S(A|B)$.

Definition 7.18 (Quantum Discord [Zur00; HV01; OZ01])**.** The *quantum discord* $D(B|A)$ of a bipartite state ρ_{AB} is defined as the difference between total correlations and classical correlations. Mathematically,

$$D(B|A) = I(A:B) - \max_{\{\hat{M}_a\}} I(B|A'), \tag{7.34}$$

where $I(A:B)$ is the mutual information between A and B (see Eq. (3.70)), the maximisation is performed over all measurements (see Eq. (3.16)) $\{\hat{M}_a\}$ on the system A, and $I(B|A')$ denote the mutual information calculated in the state ρ'_{AB}, which is the state produced by the measurement $\hat{M}_a$ on ρ_{AB}, i.e.

$$\rho'_{AB} := \sum_a \frac{(\hat{M}_a \otimes \hat{I}_B)\,\rho_{AB}\,(\hat{M}_a^\dagger \otimes \hat{I}_B)}{\mathrm{Tr}\left[(\hat{M}_a \otimes \hat{I}_B)\,\rho_{AB}\,(\hat{M}_a^\dagger \otimes \hat{I}_B)\right]}, \tag{7.35}$$

where $\hat{I}_B$ is the identity over the system B.

Quantum discord has the following properties [Mod+12].

1. Asymmetry: $D(B|A) \neq D(A|B)$ in general;
2. Non-negativity: $D(B|A) \geq 0$ for all states ρ_{AB} and $D(B|A) = 0$ if and only if ρ_{AB} is a *classical-quantum state* [OZ01; Dat08]:

$$\rho_{AB} = \sum_i p_i\, \hat{\Pi}_i^A \otimes \rho_i^B, \tag{7.36}$$

   where $\hat{\Pi}_i^A := \left|e_i^A\right\rangle \left\langle e_i^A\right|$ is a projector onto the i-th element of any basis of A;
3. Upper-boundness [LL11]: $D(B|A) \leq S(A)$;
4. Invariance under under local-unitary transformations: $D(B|A)$ is the same for ρ_{AB} and $(\hat{U}_A \otimes \hat{U}_B)\rho_{AB}(\hat{U}_A \otimes \hat{U}_B)^\dagger$.

A resource theory of quantum discord is designed by considering the set $\mathcal{Z}$ of classical-quantum states (see Eq. (7.36)) as the set of free states. Note that this set is not convex, so this is an example of non-convex resource theory. Distance-based discord monotones (see Theorem 7.6), such as the relative entropy of discord,

$$\mathcal{D}_{rel}(\rho) := \inf_{\sigma \in \mathcal{Z}} S(\rho\|\sigma), \tag{7.37}$$

are established in the literature [Mod+10].

A related measure of quantum correlations is the *symmetric discord* [PHH08; WPM09; GPA11], which removes the asymmetry between the systems A and B in Def. 7.18.

Definition 7.19 (Symmetric Discord)**.** The *symmetric discord* $D_S(A,B)$ of a bipartite state ρ_{AB} is defined as

$$D(A,B) = I(A:B) - \max_{\{\hat{M}_a \otimes \hat{M}_b\}} I(A':B'), \tag{7.38}$$

where $I(A:B)$ is the mutual information between A and B (see Eq. (3.70)), the maximisation is performed over all measurements $\{\hat{M}_a\}$ on the system A and $\{\hat{M}_b\}$ on the system B, and $I(A':B') = I(\rho'_{AB})$ with

$$\rho'_{AB} := \sum_{a,b} \frac{(\hat{M}_a \otimes \hat{M}_b)\,\rho_{AB}\,(\hat{M}_a^\dagger \otimes \hat{M}_b^\dagger)}{\mathrm{Tr}\left[(\hat{M}_a \otimes \hat{M}_b)\,\rho_{AB}\,(\hat{M}_a^\dagger \otimes \hat{M}_b^\dagger)\right]}. \tag{7.39}$$

The symmetric discord satisfies $D_S(A,B) = D_S(B,A)$. Moreover, $D_S(A,B) = 0$ if and only if ρ_{AB} is a *classical state* [Opp+02; PHH08]:

$$\rho_{AB} = \sum_{a,b} p_{ab}\,\hat{\Pi}_a \otimes \hat{\Pi}_b, \tag{7.40}$$

where $\hat{\Pi}_a$ and $\hat{\Pi}_b$ are projectors onto any basis of A and B, respectively. The set of classical states, denoted by $\mathcal{Z}_S$, is a subset of that of classical-quantum states (see Eq. (7.36)), $\mathcal{Z}$. A resource theory of symmetric discord is established by using $\mathcal{Z}_S$ as the set of free states.

Both asymmetric and symmetric discord can be extended to the multipartite case [Mod+12]. In the following, we will only consider multipartite symmetric discord, which is naturally defined from Eq. (7.38) by considering a tensor product of more than two elements.

7.2.5 Relations between the Resource Theories

The general framework of quantum resource theories allows us to explore the relations between different resources.

Let us consider a multipartite system $\mathcal{A}_1\mathcal{A}_2\ldots\mathcal{A}_M$ of total dimension $d_{tot} = \sum_i d_i$, with d_i being the dimension of the subsystem $\mathcal{A}_i$. In this scenario, we consider the following resource monotones based on the same contractive distance d (see Theorem 7.6):

$$\begin{aligned} \mathcal{C}_d(\rho) &:= \inf_{\sigma\in\mathcal{I}} d(\rho,\sigma), \qquad & \mathcal{P}_d(\rho) &:= d(\rho, \hat{I}/d_{tot}), \\ \mathcal{E}_d(\rho) &:= \inf_{\sigma\in\mathfrak{S}} d(\rho,\sigma), \qquad & \mathcal{D}_d(\rho) &:= \inf_{\sigma\in\mathcal{Z}_S} d(\rho,\sigma), \end{aligned} \tag{7.41}$$

where

- $\mathcal{C}_d$ is a distance-based coherence measure and $\mathcal{I}$ is the set of incoherent states (see Def. 7.8) in some product basis $\{|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_M\rangle\}$;
- $\mathcal{P}_d$ is a distance-based purity measure and $\hat{I}/d$ is the d_{tot}-dimensional maximally mixed state, which is the only free state in the resource theory of purity;
- $\mathcal{E}_d$ is a distance-based entanglement measure and $\mathfrak{S}$ is the set of fully separable states (see Def. 6.1);
- $\mathcal{D}_d$ is a distance-based symmetric discord measure and $\mathcal{Z}_S$ is the set of multipartite classical states (see Eq. 7.40).

Streltsov et al. [Str+18] derived the following result.

Theorem 7.20. *There exist a hierarchy of purity, coherence, symmetric discord and entanglement, i.e. for any $\mathcal{C}_d$, $\mathcal{P}_d$, $\mathcal{E}_d$ and $\mathcal{D}_d$ given by Eq.* (7.41) *for the same contractive distance d, it holds:*

$$\mathcal{P}(\rho) \geq \mathcal{C}(\rho) \geq \mathcal{D}(\rho) \geq \mathcal{E}(\rho), \tag{7.42}$$

for any $\rho \in \mathcal{S}(\mathcal{H})$. In particular, introducing

$$\mathcal{C}_{max}(\rho) := \sup_{\hat{U}} \mathcal{C}(\hat{U}\rho\hat{U}^\dagger), \quad \mathcal{D}_{max}(\rho) := \sup_{\hat{U}} \mathcal{D}(\hat{U}\rho\hat{U}^\dagger), \quad \mathcal{E}_{max}(\rho) := \sup_{\hat{U}} \mathcal{E}(\hat{U}\rho\hat{U}^\dagger), \tag{7.43}$$

it holds:

$$\mathcal{P}(\rho) = \mathcal{C}_{max}(\rho) \geq \mathcal{D}_{max}(\rho) \geq \mathcal{E}_{max}(\rho). \tag{7.44}$$

Therefore any amount of purity can be converted into coherence through unitary operations. Moreover, any purity measure on a quantum state ρ upper-bounds the amount of coherence, symmetric discord and entanglement in ρ. We shall see in the following how we extended in [GKB21] this relation to continuous-variable systems.

7.3 Continuous-variable Resource Theories

The extension of the resource theories of Sec. 7.2 to continuous variables is not trivial, because of mathematical properties associated with infinite-dimensional Hilbert spaces. Consider for instance the relative entropy $S(\rho\|\sigma) := \mathrm{Tr}(\rho(\log\rho - \log\sigma))$. For finite-dimensional systems, the following theorem holds [Weh78].

Theorem 7.21. *Let $\mathcal{S}(\mathcal{H})$ denote the set of density operators on a Hilbert space $\mathcal{H}$, and $\|\cdot\|_1$ denote the trace norm (see Eq.* (3.73)*) of $\mathcal{S}(\mathcal{H})$. If $\mathcal{H}$ is finite-dimensional, then the relative entropy $S : \mathcal{S}(\mathcal{H}) \times \mathcal{S}(\mathcal{H}) \to \mathbb{R}_{\geq 0}$ is* trace norm continuous*. Namely, if a sequence of density operators $\{\sigma_n\} \subseteq \mathcal{S}(\mathcal{H})$ satisfies*

$$\lim_{n\to\infty} \|\sigma_n - \sigma\|_1 = 0, \tag{7.45}$$

for a given state σ, then

$$\lim_{n\to\infty} S(\sigma_n\|\sigma) = 0. \tag{7.46}$$

This theorem does not hold for infinite-dimensional Hilbert spaces, and this prevents the use of the relative entropy as a resource monotone (see Def. 7.7) for general continuous-variable states. However, the relative entropy becomes trace-norm continuous if one considers a subset of states with finite mean energy [Weh78]. More precisely, one needs to require that the Hamiltonian $\hat{H}$ of the system satisfies

$$\mathrm{Tr}[e^{-\beta\hat{H}}] < \infty, \tag{7.47}$$

for all $\beta > 0$. This condition ensures that a Gibbs state (see Eq. (4.81)) exists and that the mean energy, which is given by the formula [Bin+19]

$$\langle\hat{H}\rangle = -\frac{\partial}{\partial\beta}\mathrm{Tr}[e^{-\beta\hat{H}}], \tag{7.48}$$

is finite.

In the context of the resource theory of entanglement, Eisert et al. [ESP02] proved that the relative entropy of entanglement (see Eq. (7.33)) and other entanglement measures are trace-norm continuous when Eq. (7.47) is satisfied. Since then, the assumption of finite mean energy has been used also in other continuous-variable resource theories, such as that of coherence [Zha+16].

In the following, we are going to introduce the resource theories of continuous-variable coherence and discord. Continuous-variable entanglement was already treated in Sec. 6.1, while the resource theory of continuous-variable non-uniformity will be introduced in Sec. 7.4.

7.3.1 Resource Theory of (Gaussian) Coherence

Zhang et al. [Zha+16] introduced a resource theory of coherence for continuous-variable systems, where the set $\mathcal{I}$ of incoherent states is formed by states that are diagonal in the infinite-dimensional Fock basis (see Sec. 4.1.2). In this theory, a coherence monotone $\mathcal{C}$ has to satisfy the same conditions of Def. 7.10 and, in addition,

(C4) Finite coherence for systems with finite mean energy: $\mathcal{C}(\rho) < \infty$ for all $\rho \in \mathcal{S}(\mathcal{H})$ such that $\mathrm{Tr}[\rho \hat{H}] < \infty$.

The authors proved that the relative entropy of coherence $\mathcal{C}_{rel}(\cdot) := \min_{\tau \in \mathcal{I}} S(\cdot \| \tau)$ satisfies the condition (C4), thus being a valid measure of coherence also in the infinite-dimensional case.

The difficulties associated with infinite-dimensional Hilbert spaces prevented a detailed study of coherence for general continuous-variable states. However, some relevant results were found by focusing on the relevant Gaussian subclass, in which all states and operations are Gaussian.

Theorem 7.22 (Incoherent Gaussian states [Xu16])**.** *An M-mode Gaussian state is incoherent in the product Fock basis $|n_1\rangle |n_2\rangle \dots |n_M\rangle$ if and only if it is a Gaussian thermal state (see Eq.* (4.82)*).*

We denote the subset of all incoherent Gaussian states by $\mathcal{I}_G$. The free operations of the resource theory of Gaussian coherence are the *incoherent Gaussian operations* (IG) [Xu16], which are defined as all quantum channels that map thermal states into thermal states. The mathematical expression of IG is given in [Xu16] and, in an alternative formulation, in [GKB21].

Gaussian coherence measures are defined as coherence measures with respect to $\mathcal{I}_G$ as free states and IG as free operations. They quantify the Gaussian coherence, which is an upper-bound of the proper coherence, since $\mathcal{I}_G \subset \mathcal{I}$. Xu [Xu16] derived the following formula for the *relative entropy of Gaussian coherence* of a generic M-mode Gaussian state ρ:

$$\mathcal{C}^G_{rel}(\rho) := S(\rho \| \tau_M(\bar{\boldsymbol{n}}_\rho)) = -S(\rho) + \sum_{m=1}^{M} \left[(\bar{n}_m + 1) \log(\bar{n}_m + 1) - \bar{n}_m \log \bar{n}_m \right], \qquad (7.49)$$

where $\bar{n}_m$ is the average occupation number of the m-th mode of ρ (see Eq. (4.57)), $\tau_M(\bar{\boldsymbol{n}}_\rho)$ represents the thermal state with the same $\bar{n}_m$ of ρ and the von-Neumann entropy $S(\rho)$ is given by Eq. (4.64).

7.3.2 Resource Theory of (Gaussian) Discord

Many concepts from the finite-dimensional resource theory of discord can be extended to continuous-variable systems [Tat+12; BLA19]. The definitions of asymmetric and symmetric discord are still given by Defs. 7.18 and 7.19, respectively. Analogously, classical-quantum states are defined by Eq.(7.36) and classical states are defined by Eq. (7.40). To our knowledge, an extensive study of discord in non-Gaussian continuous-variable systems has not been carried out so far.

For Gaussian states ρ_{AB}, quantum discord is defined as in Def. 7.18,

$$D(B|A) = I(A:B) - \max_{\{\hat{M}_a^G\}} I(B|A'), \tag{7.50}$$

where the maximisation can be limited to the Gaussian measurements $\{\hat{M}_a^G\}$ [Pir+14].

Gaussian discord was studied in [AD10; GP10] for the asymmetric case and in [Miš+11] for the symmetric case. The extension to the multipartite case was considered in [BLA19], both in the asymmetric and symmetric cases.

A remarkable result found in [AD10] and [Miš+11] is that all non-product Gaussian states have non-zero (asymmetric or symmetric) discord. This means that Gaussian states are either not correlated at all or possess both classical and quantum correlations. A resource theory of Gaussian discord is then established by considering the set of Gaussian product states,

$$\mathcal{Z}_G = \{\rho \quad s.t. \quad \rho = \rho_A \otimes \rho_B, \quad \rho_A, \rho_B \text{ Gaussian } \}, \tag{7.51}$$

as the set of free states.

7.4 Hierarchy of Quantum Resource Theories in CV Systems

In this section, we introduce the results of our publication [GKB21], in which we established a hierarchy of quantum resources for non-uniformity, coherence, discord and entanglement in continuous-variable systems. The original publication, with publication details, can be found in Appendix C.

7.4.1 Results

In [GKB21], we considered a system with a finite number M of discrete *spectral* and *spatial* modes, which refer to the frequency and location of the mode, respectively. The different frequencies were labeled by an index $\omega = \omega_1, \omega_2, \ldots, \omega_{M_f}$ and the spatial degrees of freedom were labelled by an index $j = 1, 2, \ldots, M_s$. We cataloged our modes first in term of frequency and then in terms of their spatial label (see Fig. 7.1).

Maximal Coherence at Fixed Energy

We defined a *maximally coherent mixed state* (MCMS) *at fixed energy* with respect to a coherence monotone $\mathcal{C}$ (see Def. 7.10) as a state ρ_{max} that satisfies

$$\mathcal{C}(\rho_{max}) = \mathcal{C}_{max}(\rho) := \sup_{\hat{U}_{EP}} \mathcal{C}(\hat{U}_{EP}\, \rho\, \hat{U}_{EP}^\dagger), \tag{7.52}$$

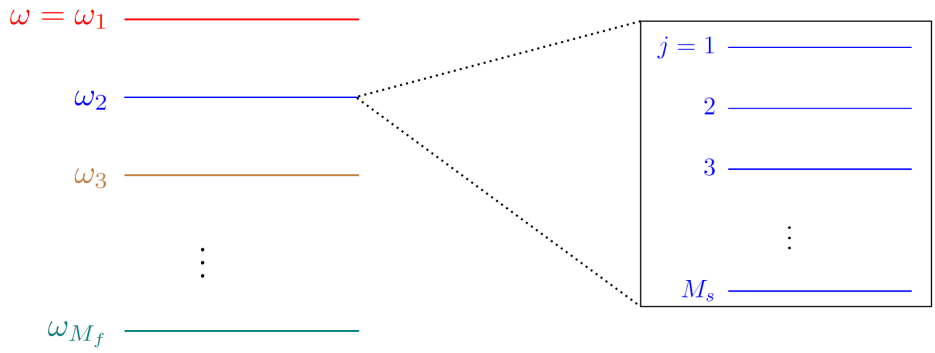

Figure 7.1: Graphical depiction of the labeling of the spectral and spatial modes. The modes are cataloged first in terms of their frequency $\omega = \omega_1, \omega_2, \ldots, \omega_{M_f}$ (represented by a distinct colour) and then in terms of their spatial label $j = 1, 2, \ldots, M_s$. The picture is taken from our publication [GKB21].

where $\hat{U}_{EP}$ are energy-preserving unitaries. When Gaussian states and operations are considered in Eq. (7.22), we called ρ_{max} the *maximally coherent mixed Gaussian state* (MCMGS) *at fixed energy* with respect to $\mathcal{C}$. We considered the behiavour at fixed energy because the coherence depends on the energy of the system and can in principle be increased indefinitely by energy non-preserving unitaries.

Consider an arbitrary Gaussian state ρ with mean occupation number

$$N = \sum_{\omega=\omega_1}^{\omega_{M_f}} N_\omega, \qquad N_\omega = \sum_j \bar{n}_{\omega;j}, \tag{7.53}$$

where $\bar{n}_{\omega;j} = \langle \hat{a}^\dagger_{\omega;j} \hat{a}_{\omega;j} \rangle_\rho$ is the single mode occupation number (see Eq. (4.57)) for the mode with frequency ω and spatial label j. We derived that the maximal relative entropy of Gaussian coherence (see (7.49)) at fixed energy $\mathcal{C}^G_{rel;\,max}(\rho)$ of ρ can be expressed as:

$$\mathcal{C}^G_{rel;\,max}(\rho) = \sum_{\omega=\omega_1}^{\omega_{M_f}} S\left(\rho_\omega \,\middle\|\, \tau_{M_s}\left(\frac{N_\omega}{M_s}, \ldots, \frac{N_\omega}{M_s}\right)\right), \tag{7.54}$$

where $\tau_{M_s}(N_\omega/M_s, \ldots, N_\omega/M_s)$ is an M_s-mode thermal state (see Eq. (4.82)) at frequency ω with equal single-mode occupation numbers, i.e. $\bar{n}_{\omega;j} = N_\omega/M_s$ for all $j = 1, 2, \ldots M_s$. This result was the main step that allowed us to establish the hierarchy of resources.

Resource theory of (Gaussian) non-uniformity

We introduced a continuous-variable *resource theory of non-uniformity* by considering purity at given energy as a resource. For an M-mode system with M_f frequencies and M_s spatial labels, we found that the following Gaussian thermal state (see Eq. (4.82)), which we named *uniform state*, is the CV counterpart at finite energy to the DV maximally mixed state:

$$\tau_M(\boldsymbol{\delta}) = \bigotimes_{\omega=\omega_1}^{\omega_{M_f}} \tau_{M_s}(\boldsymbol{\delta}_\omega), \qquad \tau_{M_s}(\boldsymbol{\delta}_\omega) := \underbrace{\tau(\delta_\omega) \otimes \tau(\delta_\omega) \otimes \cdots \otimes \tau(\delta_\omega)}_{(M_s \text{ times})}, \tag{7.55}$$

where $\boldsymbol{\delta}_\omega = (\delta_\omega, \delta_\omega, \ldots, \delta_\omega)$ is a collection of equal elements $\delta_\omega := N_\omega/M_s$, and N_ω is the total occupation number for all spatial modes with frequency ω. The covariance matrix of $\tau_M(\boldsymbol{\delta})$ reads:

$$\boldsymbol{V}\left[\tau_M(\boldsymbol{\delta})\right] = \bigoplus_{\omega=\omega_1}^{\omega_{M_f}} (2\delta_\omega + 1)\ \boldsymbol{I}_{2M_s}. \tag{7.56}$$

Both the general and Gaussian version of this resource theory have the same set of free states. We introduced the set of *uniformity-preserving operations* (UP) as the set of all maps that preserve the uniform state $\tau_M(\boldsymbol{\delta})$ (see Eq. (7.55)), i.e.

$$\Lambda_{UP}\left[\tau_M(\boldsymbol{\delta})\right] = \tau_M(\boldsymbol{\delta}). \tag{7.57}$$

The Gaussian channels in UP form the subset of *uniformity-preserving Gaussian operations* (UPG). Among Gaussian channels in UPG, we defined the *Gaussian noisy operations* (GN) as those Gaussian channels Λ_{GN} that admit the following decomposition:

$$\Lambda_{GN}[\rho] = \mathrm{Tr}_{M_E}\left[\hat{U}_{\boldsymbol{O}}^{(M+M_E)}\ \left(\rho \otimes \tau_{M_E}(\boldsymbol{\delta})\right)\ \hat{U}_{\boldsymbol{O}}^{(M+M_E)\,\dagger}\right], \tag{7.58}$$

where $\tau_{M_E}(\boldsymbol{\delta})$ is the uniform state (see Eq. (7.55)) for M_E environmental modes and with the same $\boldsymbol{\delta}$ of the system, and $\hat{U}_{PG}^{(M+M_E)}$ is an $(M + M_E)$-mode energy-preserving Gaussian unitary, i.e. a passive Gaussian unitary (see Def. 4.24). We do not know whether the inclusions $GN \subseteq UPG \subseteq UP$ are strict or not.

We introduced the *relative entropy of non-uniformity*,

$$\mathcal{P}_{rel}(\rho) := S\left(\rho \| \tau_M(\boldsymbol{\delta})\right), \tag{7.59}$$

and proved it to be a valid non-uniformity measure. Restricting ourselves to Gaussian states and operations, we found that the relative entropy of Gaussian non-uniformity $\mathcal{P}^G_{rel}(\rho)$ (that is the relative entropy of non-uniformity for Gaussian states) of a Gaussian state ρ is equal to its maximal coherence at fixed energy (see Eq. (7.54)):

$$\mathcal{P}^G_{rel}(\rho) = \mathcal{C}^G_{rel;\,max}(\rho). \tag{7.60}$$

Hierarchy

Using quantifiers based on the relative entropy (see Def. 7.7), we extended the ordering of resources for discrete variables (see Theorem 7.20) to continuous-variable systems.

Theorem 7.23. *There exist a hierarchy for the relative entropy of non-uniformity $\mathcal{P}_{rel}$ (see Eq. (7.59)), coherence $\mathcal{C}_{rel}$ (see Eq. (7.49)), symmetric discord $\mathcal{D}_{rel}$ (see Eqs. (7.37) and (7.40)) and entanglement $\mathcal{E}_{rel}$ (see Eq. (7.33)), i.e. it holds:*

$$\mathcal{P}_{rel}(\rho) \geq \mathcal{C}_{rel}(\rho) \geq \mathcal{D}_{rel}(\rho) \geq \mathcal{E}_{rel}(\rho), \tag{7.61}$$

for any $\rho \in \mathcal{S}(\mathcal{H})$. In particular, considering Gaussian states and operations and introducing

$$\begin{aligned} \mathcal{C}^G_{rel;\,max}(\rho) &:= \sup_{\hat{U}_{PG}} \mathcal{C}^G(\hat{U}_{PG}\rho\hat{U}_{PG}^\dagger), \qquad \mathcal{D}^G_{rel;\,max}(\rho) := \sup_{\hat{U}_{PG}} \mathcal{D}^G(\hat{U}_{PG}\rho\hat{U}_{PG}^\dagger), \\ \mathcal{E}^G_{rel;\,max}(\rho) &:= \sup_{\hat{U}_{PG}} \mathcal{E}^G(\hat{U}_{PG}\rho\hat{U}_{PG}^\dagger), \end{aligned} \tag{7.62}$$

where $\hat{U}_{PG}$ are passive Gaussian unitaries (see Def. 4.24), it holds:

$$\mathcal{P}^G_{rel}(\rho) = \mathcal{C}^G_{rel;\,max}(\rho) \geq \mathcal{D}^G_{rel;\,max}(\rho) \geq \mathcal{E}^G_{rel;\,max}(\rho). \tag{7.63}$$

Eqs. (7.61) and (7.63) are visualised in Figs. 7.2 and 7.3, respectively.

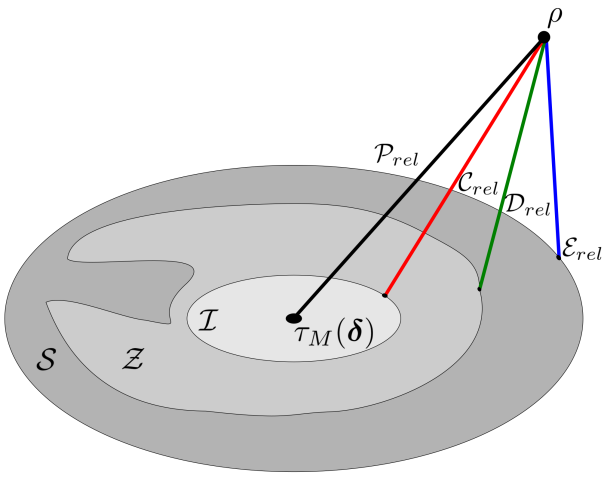

Figure 7.2: Graphical depiction of the relative entropy of non-uniformity $\mathcal{P}_{rel}$ (black line), coherence $\mathcal{C}_{rel}$ (red line), symmetric quantum discord $\mathcal{D}_{rel}$ (green line) and entanglement $\mathcal{E}_{rel}$ (blue line) for a quantum state ρ. The uniform state $\tau_M(\boldsymbol{\delta})$ is an element of the incoherent set $\mathcal{I}$, which is a convex subset of the zero-discord set $\mathcal{Z}$, which in turn is a non-convex subset of the separable set $\mathcal{S}$. The picture is taken from our publication [GKB21].

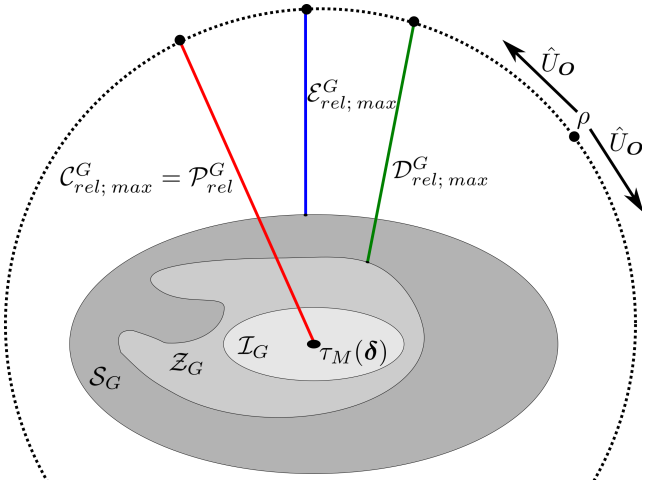

Figure 7.3: Graphical depiction of Eq. (7.63). The dotted circle represents all the states that can be obtained from ρ via passive unitaries $\hat{U}_{\boldsymbol{O}}$. The red line, connecting the uniform state $\tau_M(\boldsymbol{\delta})$ to the MCMGS, is the maximal Gaussian coherence $\mathcal{C}^G_{rel;\,max}(\rho) = \mathcal{P}^G_{rel}(\rho)$. The green and blue lines are the maximal Gaussian discord $\mathcal{D}^G_{rel;\,max}$ and entanglement $\mathcal{E}^G_{rel;\,max}$, respectively. The uniform state $\tau_M(\boldsymbol{\delta})$ is an element of the Gaussian incoherent set $\mathcal{I}_G$, which is a convex subset of the Gaussian zero-discord set $\mathcal{Z}_G$, which in turn is a non-convex subset of the Gaussian separable set $\mathcal{S}_G$. The picture is taken from our publication [GKB21].

8

Conclusions and Outlook

In this thesis, we presented results on three projects related to the use of quantum resources in systems with many degrees of freedom.

In [GKB20], we presented a theoretical model for the formalisation and comparison of classical and quantum readout (QR-) physical unclonable functions (PUFs). We introduced an authentication protocol that is valid for both typologies and independent from the specific (QR-) PUF implementation. We then quantitatively characterised the security of (QR-) PUFs in terms of two properties, the robustness and the unclonability. The former property is connected to the probability that a legitimate user is not authenticated, due to noise or disturbances by an adversary, while the latter one is connected to the probability that an adversary successfully impersonates a legitimate user, by cloning or simulating the (QR-) PUF.

Our work could be the starting point of theoretical and experimental research on (QR-) PUFs since it allows the comparison of different implementations and the development of new authentication protocols. In particular, future research could verify the supposed supremacy of QR-PUFs over classical PUFs and examine, in given scenarios, whether the technological challenges and financial costs connected to the use of quantum resources are compensated by the possible security gain. Moreover, our framework could be used to explore the security of using (QR-) PUFs in other classical or quantum cryptographic protocols. For instance, a (QR-) PUF could be employed in quantum key distribution to generate an authentication key and reduce the number of preshared key bits. This application would require the development of (QR)-PUFs with a very high security level.

In [Mih+20], we introduced a scheme for entanglement detection in unknown continuous-variable states. We derived semidefinite constraints for the entanglement witnesses based on the second moments and used them as a sufficient condition for a state to be entangled. We implemented the constraints by using a semidefinite program and partial information about the state, which we obtained through random homodyne measurements. We tested our method and showed that it requires, with high probability, fewer measurements than a full tomography. For two-mode squeezed vacuum states (TMSVSs), we showed good performance of our scheme for states with a low amount of entanglement. The performance declines for highly entangled

states, due to the geometric shape in the phase space of the variance of the TMSVSs. We found that our method is more convenient than full tomography also for randomly generated two-mode states. In this case, highly entangled states require fewer measurements on average. We also tested our method on a four-mode bound entangled state, again finding an efficient detection. We finally verified that our scheme has good robustness to statistical errors.

Our method is easily implementable in a laboratory since it only requires linear optical components and homodyne detectors. It can be adapted to many experimental situations, in which there is little or no information about quantum states. The ability to detect entanglement affordably also paves the way to a more practical use of this resource in large-scale technological applications.

In [GKB21], we established a hierarchy of continuous-variable quantum resources, under the condition of fixed energy. First, we defined the maximal coherence at fixed energy, as the coherence that is obtainable by energy-preserving unitaries. Then, we introduced a resource theory of non-uniformity for continuous-variable systems, in which the purity at fixed energy is the resource. By using quantifiers based on the relative entropy, we proved that the non-uniformity of a quantum state always upper-bounds its coherence, discord and entanglement. In particular, when we consider Gaussian states and operations, the Gaussian non-uniformity is exactly equal to the maximal Gaussian coherence, and we derived an analytical formula for this quantity. Our results extend to continuous variable an analogous hierarchy for discrete-variable resources [Str+18].

Future works may investigate whether the same hierarchy holds by considering the action of energy non-preserving unitaries, under the constraint of finite maximum energy. Another open question is whether the non-uniformity is equal to the maximal coherence also for non-Gaussian states and operations.

In conclusion, the achievement of a high level of control and understanding of quantum resources is a necessary precondition to concretely implement quantum technologies in industrial scenarios. We hope that our doctoral research has supported this process and will stimulate further new scientific studies.

Bibliography

[Åbe06] J. Åberg, "Quantifying superposition", *arXiv:quant-ph/0612146*, 2006.

[AD10] G. Adesso and A. Datta, "Quantum versus classical correlations in Gaussian states", *Phys. Rev. Lett.* 105.3, 030501, 2010.

[AI07] G. Adesso and F. Illuminati, "Entanglement in continuous-variable systems: recent advances and current perspectives", *J. Phys. A: Math. Theor.* 40.28, 7821, 2007.

[ARL14] G. Adesso, S. Ragy, and A. R. Lee, "Continuous variable quantum information: Gaussian states and beyond", *Open Systems & Information Dynamics* 21.01n02, 1440001, 2014.

[And06] J. Anders, "Estimating the degree of entanglement of unknown Gaussian states", *arXiv:quant-ph/0610263*, 2006.

[Arm+10] F. Armknecht et al., "Memory leakage-resilient encryption based on physically unclonable functions", *Towards Hardware-Intrinsic Security*, Springer, 135–164, 2010.

[Arm+11] F. Armknecht et al., "A formalization of the security features of physical functions", *2011 IEEE Symposium on Security and Privacy*, 397–412, 2011.

[BW99] K. Banaszek and K. Wódkiewicz, "Nonlocality of the Einstein-Podolsky-Rosen state in the phase space", *arXiv:quant-ph/9904071*, 1999.

[Bau83] D. W. Bauder, "An anti-counterfeiting concept for currency systems", *Sandia National Labs, Tech. Rep. PTK-11990*, 1983.

[BCP14] T. Baumgratz, M. Cramer, and M. B. Plenio, "Quantifying coherence", *Phys. Rev. Lett.* 113.14, 140401, 2014.

[Bel64] J. S. Bell, "On the Einstein Podolsky Rosen paradox", *Physics* 1.3, 195–200, 1964.

[BB84] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179, 1984.

[Ben+93] C. H. Bennett et al., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.* 70.13, 1895, 1993.

[Ben+96a] C. H. Bennett et al., "Concentrating partial entanglement by local operations", *Phys. Rev. A* 53.4, 2046, 1996.

[Ben+96b] C. H. Bennett et al., "Mixed-state entanglement and quantum error correction", *Phys. Rev. A* 54.5, 3824, 1996.

[Bin+19] F. Binder et al., *Thermodynamics in the Quantum Regime: Fundamental Aspects and New Directions*, Springer, 2019.

[Bog58] N. N. Bogoliubov, "On a new method in the theory of superconductivity", *Il Nuovo Cimento (1955-1965)* 7.6, 794–805, 1958.

[Boh28] N. Bohr, "The quantum postulate and the recent development of atomic theory", *Nature* 121, 580–590, 1928.

[Bos24] S. N. Bose, "Plancks gesetz und lichtquantenhypothese", *Zeitschrift für Physik* 26, 178–181, 1924.

[BV04] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge university press, 2004.

[Boy04] X. Boyen, "Reusable cryptographic fuzzy extractors", *Proceedings of the 11th ACM conference on Computer and Communications Security*, 82–91, 2004.

[BLA19] M. Bradshaw, P. K. Lam, and S. M. Assad, "Gaussian multipartite quantum discord from classical mutual information", *J. Phys. B: At. Mol. Opt. Phys.* 52.24, 245501, 2019.

[Bra+13] F. G. S. L. Brandão et al., "Resource theory of quantum states out of thermal equilibrium", *Phys. Rev. Lett.* 111.25, 250404, 2013.

[Bra+15] F. G. S. L. Brandão et al., "The second laws of quantum thermodynamics", *Proceedings of the National Academy of Sciences* 112.11, 3275–3279, 2015.

[BL05] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables", *Rev. Mod. Phys.* 77.2, 513, 2005.

[BCA15] T. R. Bromley, M. Cianciaruso, and G. Adesso, "Frozen quantum coherence", *Phys. Rev. Lett.* 114.21, 210401, 2015.

[Bru98] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states", *Phys. Rev. Lett.* 81.14, 3018, 1998.

[BL19] D. Bruß and G. Leuchs, *Quantum Information: From Foundations to Quantum Technology Applications*, John Wiley & Sons, 2019.

[Brz+11] C. Brzuska et al., "Physically uncloneable functions in the universal composition framework", *Annual Cryptology Conference*, Springer, 51–70, 2011.

[BH96] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem", *Phys. Rev. A* 54.3, 1844, 1996.

[Can+16] R. Canetti et al., "Reusable fuzzy extractors for low-entropy distributions", *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 117–146, 2016.

[Car+08] F. Caruso et al., "Multi-mode bosonic Gaussian channels", *New J. Phys.* 10.8, 083030, 2008.

[Car+11] F. Caruso et al., "Optimal unitary dilation for bosonic Gaussian channels", *Phys. Rev. A* 84.2, 022306, 2011.

[CG16a] E. Chitambar and G. Gour, "Comparison of incoherent operations and measures of coherence", *Phys. Rev. A* 94.5, 052336, 2016.

[CG16b] E. Chitambar and G. Gour, "Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence", *Phys. Rev. Lett.* 117.3, 030401, 2016.

[CG19] E. Chitambar and G. Gour, "Quantum resource theories", *Rev. Mod. Phys.* 91.2, 025001, 2019.

[Chi+14] E. Chitambar et al., "Everything you always wanted to know about LOCC (but were afraid to ask)", *Communications in Mathematical Physics* 328.1, 303–326, 2014.

[DPS03] G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, "Quantum tomography", *Advances in Imaging and Electron Physics* 128, 206–309, 2003.

[DAu+05] V. D'Auria et al., "Characterization of bipartite states using a single homodyne detector", *J. Opt. B: Quantum Semiclass. Opt.* 7.12, S750, 2005.

[DAu+09] V. D'Auria et al., "Full characterization of Gaussian bipartite entangled states by a single homodyne detector", *Phys. Rev. Lett.* 102.2, 020502, 2009.

[Dat08] A. Datta, "Studies on the role of entanglement in mixed-state quantum computation", PhD thesis, University of New Mexico, 2008.

[Del17] J. Delvaux, "Security analysis of PUF-based key generation and entity authentication", PhD thesis, Shanghai Jiao Tong University, 2017.

[DV14] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65 nm arbiter and RO sum PUFs via environmental changes", *IEEE Transactions on Circuits and Systems I: Regular Papers* 61.6, 1701–1713, 2014.

[Del+14] J. Delvaux et al., "Helper data algorithms for PUF-based key generation: Overview and analysis", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34.6, 889–902, 2014.

[Die82] D. Dieks, "Communication by EPR devices", *Phys. Lett. A* 92.6, 271–272, 1982.

[Dir30] P. A. M. Dirac, *Principles of quantum mechanics*, Clarendon Press, 1930.

[Dir39] P. A. M. Dirac, "A new notation for quantum mechanics", *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35.3, 416–418, 1939.

[DRS04] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", *International conference on the theory and applications of cryptographic techniques*, Springer, 523–540, 2004.

[Dod+08] Y. Dodis et al., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", *SIAM J. Comput.* 38.1, 97–139, 2008.

[Dod02] V. V. Dodonov, "Nonclassical states in quantum optics: a squeezed review of the first 75 years", *J. Opt. B: Quantum Semiclass. Opt.* 4.1, 2002.

[DMS+95] B. Dutta, N. Mukunda, R. Simon, et al., "The real symplectic groups in quantum mechanics and optics", *Pramana* 45.6, 471–497, 1995.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Phys. Rev.* 47.10, 777, 1935.

[ESP02] J. Eisert, C. Simon, and M. B. Plenio, "On the quantification of entanglement in infinite-dimensional quantum systems", *J. Phys. A Math. Gen.* 35.17, 3911, 2002.

[Eke91] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* 67.6, 661, 1991.

[FT20] C. Fabre and N. Treps, "Modes and states in quantum optics", *Rev. Mod. Phys.* 92.3, 035005, 2020.

[Gas03] B. Gassend, "Physical random functions", PhD thesis, Massachusetts Institute of Technology, 2003.

[Gas+02] B. Gassend et al., "Silicon physical random functions", *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 148–160, 2002.

[Gas+04] B. Gassend et al., "Identification and authentication of integrated circuits", *Concurrency and Computation: Practice and Experience* 16.11, 1077–1098, 2004.

[GKB20] G. Gianfelici, H. Kampermann, and D. Bruß, "Theoretical framework for physical unclonable functions, including quantum readout", *Phys. Rev. A* 101.4, 042337, 2020.

[GKB21] G. Gianfelici, H. Kampermann, and D. Bruß, "Hierarchy of continuous-variable quantum resource theories", *arXiv:quant-ph/2106.11334*, 2021.

[GP10] P. Giorda and M. G. A. Paris, "Gaussian quantum discord", *Phys. Rev. Lett.* 105.2, 020503, 2010.

[GPA11] D. Girolami, M. Paternostro, and G. Adesso, "Faithful nonclassicality indicators and extremal quantum correlations in two-qubit states", *J. Phys. A: Math. Theor.* 44.35, 352002, 2011.

[Gla63] R. J. Glauber, "Coherent and incoherent states of the radiation field", *Phys. Rev.* 131.6, 2766, 1963.

[Goo+14] S. A. Goorden et al., "Quantum-secure authentication of a physical unclonable key", *Optica* 1.6, 421–424, 2014.

[Gou+15] G. Gour et al., "The resource theory of informational nonequilibrium in thermodynamics", *Phys. Rep.* 583, 1–58, 2015.

[Gro46] H. J. Groenewold, *On the principles of elementary quantum mechanics*, Springer, 1946.

[Gru+08] A. Grudka et al., "Entanglement-swapping boxes and their communication properties", *Phys. Rev. A* 77.6, 060307, 2008.

[GAF10] G. Grynberg, A. Aspect, and C. Fabre, *Introduction to quantum optics: from the semi-classical approach to quantized light*, Cambridge university press, 2010.

[Gua+07a] J. Guajardo et al., "FPGA intrinsic PUFs and their use for IP protection", *International workshop on cryptographic hardware and embedded systems*, Springer, 63–80, 2007.

[Gua+07b] J. Guajardo et al., "Physical unclonable functions and public-key crypto for FPGA IP protection", *2007 International Conference on Field Programmable Logic and Applications*, IEEE, 189–195, 2007.

[Hei49] W. Heisenberg, *The physical principles of the quantum theory*, Courier Corporation, 1949.

[Hel+13] C. Helfmeier et al., "Cloning physically unclonable functions", *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, IEEE, 1–6, 2013.

[Hel02] C. Helmberg, "Semidefinite programming", *European Journal of Operational Research* 137.3, 461–482, 2002.

[HV01] L. Henderson and V. Vedral, "Classical, quantum and total correlations", *J. Phys. A: Math. Gen.* 34.35, 6899, 2001.

[HBF07] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags", *Proceedings of the Conference on RFID Security*, vol. 7.2, 1, 2007.

[HSH99] A. S. Holevo, M. Sohma, and O. Hirota, "Capacity of quantum Gaussian channels", *Phys. Rev. A* 59.3, 1820, 1999.

[HW01] A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic Gaussian channels", *Phys. Rev. A* 63.3, 032312, 2001.

[HHO03] M. Horodecki, P. Horodecki, and J. Oppenheim, "Reversible transformations from pure to mixed states and the unique measure of information", *Phys. Rev. A* 67.6, 062104, 2003.

[Hor+03] M. Horodecki et al., "Local information as a resource in distributed quantum systems", *Phys. Rev. Lett.* 90.10, 100402, 2003.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions", *Phys. Lett. A* 223.1, 1–8, 1996.

[Hor+09] R. Horodecki et al., "Quantum entanglement", *Rev. Mod. Phys.* 81.2, 865, 2009.

[Hud74] R. L. Hudson, "When is the Wigner quasi-probability density non-negative?", *Rep. Math. Phys.* 6.2, 249–252, 1974.

[Hus40] K. Husimi, "Some formal properties of the density matrix", *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series* 22.4, 264–314, 1940.

[HE06] P. Hyllus and J. Eisert, "Optimal entanglement witnesses for continuous-variable systems", *New J. Phys.* 8.4, 51, 2006.

[Ign+06] T. Ignatenko et al., "Estimating the secrecy-rate of physical unclonable functions with the context-tree weighting method", *2006 IEEE International Symposium on Information Theory*, IEEE, 499–503, 2006.

[IM94] R. S. Indeck and M. W. Muller, *Method and apparatus for fingerprinting magnetic media*, US Patent 5365586A, 1994.

[Jac62] S. Jacobs, "Technical Note on Heterodyne Detection in Optical Communications", *Technical Research Group*, 1962.

[Jan+00] D. Janzing et al., "Thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the second law", *Int. J. Theor. Phys.* 39.12, 2717–2753, 2000.

[KLM07] P. Kaye, R. Laflamme, and M. Mosca, *An introduction to quantum computing*, Oxford University Press, 2007.

[Kni00] K. Knight, *Mathematical Statistics*, Chapmann and Hall, 2000.

[Lay+04] P. A. Layman et al., *Electronic fingerprinting of semiconductor integrated circuits*, US Patent 6738294B2, 2004.

[Lee+04] J. W. Lee et al., "A technique to build a secret key in integrated circuits for identification and authentication applications", *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*, IEEE, 176–179, 2004.

[LM14] F. Levi and F. Mintert, "A quantitative theory of coherent delocalization", *New J. Phys.* 16.3, 033007, 2014.

[Lew+00] M. Lewenstein et al., "Optimization of entanglement witnesses", *Phys. Rev. A* 62.5, 052310, 2000.

[Lew+01] M. Lewenstein et al., "Characterization of separable states and entanglement witnesses", *Phys. Rev. A* 63.4, 044304, 2001.

[LL11] N. Li and S. Luo, "Classical and quantum correlative capacities of quantum systems", *Phys. Rev. A* 84.4, 042124, 2011.

[Lim+05] D. Lim et al., "Extracting secret keys from integrated circuits", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 13.10, 1200–1205, 2005.

[Löf04] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB", *2004 IEEE international conference on robotics and automation (IEEE Cat. No. 04CH37508)*, IEEE, 284–289, 2004.

[Loo02] P. van Loock, "Quantum communication with continuous variables", *Fortschritte der Physik: Progress of Physics* 50.12, 1177–1372, 2002.

[Los19] M. Lostaglio, "An introductory review of the resource theory approach to thermodynamics", *Rep. Prog. Phys.* 82.11, 114001, 2019.

[LB95] N. Lütkenhaus and S. M. Barnett, "Nonclassical effects in phase space", *Phys. Rev. A* 51.4, 3340, 1995.

[LR09] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography", *Rev. Mod. Phys.* 81.1, 299, 2009.

[MV10] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions", *Towards Hardware-Intrinsic Security*, Springer, 3–37, 2010.

[MKP08] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing techniques for hardware security", *2008 IEEE International Test Conference*, IEEE, 1–10, 2008.

[MKP09] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs", *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* 2.1, 1–33, 2009.

[MW20] S. Mancini and A. Winter, *A Quantum Leap in Information Theory*, World Scientific, 2020.

[Mar12] K. M. Martin, *Everyday Cryptography: Fundamental Principles and Applications*, OUP Oxford, 2012.

[MO17] L. Masanes and J. Oppenheim, "A general derivation and quantification of the third law of thermodynamics", *Nature communications* 8.1, 14538, 2017.

[McG+19] T. McGrath et al., "A PUF taxonomy", *Appl. Phys. Rev.* 6.1, 011303, 2019.

[MZB06] D. McHugh, M. Ziman, and V. Bužek, "Entanglement, purity, and energy: Two qubits versus two modes", *Phys. Rev. A* 74.4, 042303, 2006.

[MW09] C. B. Mendl and M. M. Wolf, "Unital quantum channels–convex structure and revivals of Birkhoff's theorem", *Comm. Math. Phys.* 289.3, 1057–1086, 2009.

[Mer+11] D. Merli et al., "Side-Channel Analysis of PUFs and Fuzzy Extractors", *International Conference on Trust and Trustworthy Computing*, Springer, 33–47, 2011.

[Mih+20] T. Mihaescu et al., "Detecting entanglement of unknown continuous variable states with random measurements", *New J. Phys.* 22.12, 123041, 2020.

[Miš+11] L. Mišta Jr et al., "Measurement-induced disturbances and nonclassical correlations of Gaussian states", *Phys. Rev. A* 83.4, 042325, 2011.

[Mod+10] K. Modi et al., "Unified View of Quantum and Classical Correlations", *Phys. Rev. Lett.* 104.8, 080501, 2010.

[Mod+12] K. Modi et al., "The classical-quantum boundary for correlations: Discord and related measures", *Rev. Mod. Phys.* 84.4, 1655, 2012.

[NF93] D. Naccache and P. Fremanteau, *Unforgeable identification device, identification device reader and method of identification*, US Patent US5434917A, 1993.

[Nat+93] National Research Council et al., *Counterfeit Deterrent Features for the Next-Generation Currency Design*, National Academies Press, 1993.

[Neu32] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, 1932.

[NW18] N. Ng and M. P. Woods, "Resource theory of quantum thermodynamics: Thermal operations and Second Laws", *arXiv:quant-ph/1805.09564*, 2018.

[NC10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2010.

[Nik18] G. M. Nikolopoulos, "Continuous-variable quantum authentication of physical unclonable keys: Security against an emulation attack", *Phys. Rev. A* 97.1, 012324, 2018.

[ND17] G. M. Nikolopoulos and E. Diamanti, "Continuous-variable quantum authentication of physical unclonable keys", *Scientific Reports* 7, 46047, 2017.

[Oli12] S. Olivares, "Quantum optics in the phase space", *Eur. Phys. J. Special Topics* 203.1, 3–24, 2012.

[OZ01] H. Ollivier and W. H. Zurek, "Quantum discord: a measure of the quantumness of correlations", *Phys. Rev. Lett.* 88.1, 017901, 2001.

[Opp+02] J. Oppenheim et al., "Thermodynamical approach to quantifying quantum correlations", *Phys. Rev. Lett.* 89.18, 180402, 2002.

[ÖHS08] E. Öztürk, G. Hammouri, and B. Sunar, "Towards robust low cost authentication for pervasive devices", *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, IEEE, 170–178, 2008.

[Pap01] R. Pappu, "Physical one-way functions", PhD thesis, Massachusetts Institute of Technology, 2001.

[Pap+02] R. Pappu et al., "Physical one-way functions", *Science* 297.5589, 2026–2030, 2002.

[Pau95] H. Paul, *Photonen: eine Einführung in die Quantenoptik*, Springer-Verlag, 1995.

[Pau27] W. Pauli, "Zur Quantenmechanik des magnetischen Elektrons", *Zeitschrift für Physik* 43.9, 601–623, 1927.

[Per95] A. Peres, *Quantum Theory: Concepts and Methods*, Springer Science & Business Media, 1995.

[Per96] A. Peres, "Separability criterion for density matrices", *Phys. Rev. Lett.* 77.8, 1413, 1996.

[PHH08] M. Piani, P. Horodecki, and R. Horodecki, "No-local-broadcasting theorem for multipartite quantum correlations", *Phys. Rev. Lett.* 100.9, 090502, 2008.

[Pir+14] S. Pirandola et al., "Optimality of Gaussian discord", *Phys. Rev. Lett.* 113.14, 140405, 2014.

[Pir+20] S. Pirandola et al., "Advances in quantum cryptography", *Advances in Optics and Photonics* 12.4, 1012–1236, 2020.

[PV07] M. B. Plenio and S. S. Virmani, "An introduction to entanglement theory", *Quant. Inf. Comp.* 7.1, 1–51, 2007.

[Puc+15] S. Puchinger et al., "On error correction for physical unclonable functions", *SCC 2015; 10th International ITG Conference on Systems, Communications and Coding*, VDE, 1–6, 2015.

[Rai01] E. M. Rains, "A semidefinite program for distillable entanglement", *IEEE Transactions on Information Theory* 47.7, 2921–2933, 2001.

[Rén+61] A. Rényi et al., "On measures of entropy and information", *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, vol. 4, 1, 547–561, 1961.

[Roc15] R. T. Rockafellar, *Convex analysis*, Princeton university press, 2015.

[Ros11] C. Rossetti, *Metodi matematici per la Fisica*, Libreria editrice universitaria Levrotto & Bella, 2011.

[Rüh10] U. Rührmair, "Oblivious transfer based on physical unclonable functions", *International Conference on Trust and Trustworthy Computing*, Springer, 430–440, 2010.

[RD13] U. Rührmair and M. van Dijk, "On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols", *J. Cryptogr. Eng.* 3.1, 17–28, 2013.

[RSS09] U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable functions", *IACR Cryptol. ePrint arch: 2009/277*, 2009.

[Rüh+10] U. Rührmair et al., "Modeling attacks on physical unclonable functions", *Proceedings of the 17th ACM conference on Computer and communications security*, ACM, 237–249, 2010.

[Rüh+13] U. Rührmair et al., "PUF modeling attacks on simulated and silicon data", *IEEE Transactions on Information Forensics and Security* 8.11, 1876–1891, 2013.

[Sca+09] V. Scarani et al., "The security of practical quantum key distribution", *Rev. Mod. Phys.* 81.3, 1301, 2009.

[Sch35] E. Schrödinger, "Discussion of probability relations between separated systems", *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, 4, 555–563, 1935.

[Sch86] B. L. Schumaker, "Quantum mechanical pure states with Gaussian wave functions", *Phys. Rep.* 135.6, 317–408, 1986.

[Ser17] A. Serafini, *Quantum continuous variables: a primer of theoretical methods*, CRC press, 2017.

[Sha12] R. Shankar, *Principles of quantum mechanics*, Springer Science & Business Media, 2012.

[Sha48] C. E. Shannon, "A mathematical theory of communication", *Bell system technical journal* 27.3, 379–423, 1948.

[Sho94] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", *Proceedings 35th annual symposium on foundations of computer science*, IEEE, 124–134, 1994.

[Sim84] G. J. Simmons, "A system for verifying user identity and authorization at the point-of sale or access", *Cryptologia* 8.1, 1–21, 1984.

[Sim91] G. J. Simmons, "Identification of data, devices, documents and individuals", *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security technology*, IEEE, 197–218, 1991.

[SMD94] R. Simon, N. Mukunda, and B. Dutta, "Quantum-noise matrix for multimode systems: U (n) invariance, squeezing, and normal forms", *Phys. Rev. A* 49.3, 1567, 1994.

[Sim00] R. Simon, "Peres-Horodecki separability criterion for continuous variable systems", *Phys. Rev. Lett.* 84.12, 2726, 2000.

[Sin+15] U. Singh et al., "Maximally coherent mixed states: Complementarity between maximal coherence and mixedness", *Phys. Rev. A* 91.5, 052115, 2015.

[Ško12] B. Škorić, "Quantum readout of physical unclonable functions", *Int. J. Quantum Inf.* 10.01, 1250001, 2012.

[Ško16] B. Škorić, "Security analysis of quantum-readout PUFs in the case of challenge-estimation attacks", *Quantum Inf. Comput* 16, 50–60, 2016.

[ŠMP13] B. Škorić, A. P. Mosk, and P. W. H. Pinkse, "Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks", *International journal of quantum information* 11.04, 1350041, 2013.

[ŠTO05] B. Škorić, P. Tuyls, and W. Ophey, "Robust key extraction from physical uncloneable functions", *International Conference on Applied Cryptography and Network Security*, Springer, 407–422, 2005.

[SP18] D. R. Stinson and M. Paterson, *Cryptography: theory and practice-4th Edition*, CRC press, 2018.

[SAP17] A. Streltsov, G. Adesso, and M. B. Plenio, "Colloquium: Quantum coherence as a resource", *Rev. Mod. Phys.* 89.4, 041003, 2017.

[Str+15] A. Streltsov et al., "Measuring quantum coherence with entanglement", *Phys. Rev. Lett.* 115.2, 020403, 2015.

[Str+18] A. Streltsov et al., "Maximal coherence and the resource theory of purity", *New J. Phys.* 20.5, 053058, 2018.

[Sud63] E. C. G. Sudarshan, "Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams", *Phys. Rev. Lett.* 10.7, 277, 1963.

[SKB15] J. Szangolies, H. Kampermann, and D. Bruß, "Detecting entanglement of unknown quantum states with random measurements", *New J. Phys.* 17.11, 113051, 2015.

[Tat+12] R. Tatham et al., "Nonclassical correlations in continuous-variable non-Gaussian Werner states", *Phys. Rev. A* 85.2, 022326, 2012.

[Ter00] B. M. Terhal, "Bell inequalities and the separability criterion", *Phys. Lett. A* 271.5, 319–326, 2000.

[Tol92] K. M. Tolk, *Reflective particle technology for identification of critical components*, Sandia National Labs. technical reports, 1992.

[Tuy+04] P. Tuyls et al., "An information theoretic model for physical uncloneable functions", *Proceedings of the 2004 International Symposium on Information Theory*, IEEE, 141, 2004.

[Tuy+05] P. Tuyls et al., "Information-theoretic security analysis of physical uncloneable functions", *International Conference on Financial Cryptography and Data Security*, Springer, 141–155, 2005.

[Vah+16] H. Vahlbruch et al., "Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency", *Phys. Rev. Lett.* 117.11, 110801, 2016.

[Val58] J. Valatin, "Comments on the theory of superconductivity", *Il Nuovo Cimento (1955-1965)* 7.6, 843–857, 1958.

[VB96] L. Vandenberghe and S. Boyd, "Semidefinite programming", *SIAM review* 38.1, 49–95, 1996.

[VP98] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures", *Phys. Rev. A* 57.3, 1619–1633, 1998.

[Ved+97] V. Vedral et al., "Quantifying entanglement", *Phys. Rev. Lett.* 78.12, 2275, 1997.

[VW02] G. Vidal and R. F. Werner, "Computable measure of entanglement", *Phys. Rev. A* 65.3, 032314, 2002.

[WM07] D. F. Walls and G. J. Milburn, *Quantum optics*, Springer Science & Business Media, 2007.

[Wee+12] C. Weedbrook et al., "Gaussian quantum information", *Rev. Mod. Phys.* 84.2, 621, 2012.

[Weh78] A. Wehrl, "General properties of entropy", *Rev. Mod. Phys.* 50.2, 221, 1978.

[WW01] R. F. Werner and M. M. Wolf, "Bound entangled Gaussian states", *Phys. Rev. Lett.* 86.16, 3658, 2001.

[Wig32] E. Wigner, "On the Quantum Correction For Thermodynamic Equilibrium", *Phys. Rev.* 40.5, 749, 1932.

[Wil36] J. Williamson, "On the algebraic problem concerning the normal forms of linear dynamical systems", *Am. J. Math.* 58.1, 141–163, 1936.

[WY16] A. Winter and D. Yang, "Operational resource theory of coherence", *Phys. Rev. Lett.* 116.12, 120404, 2016.

[WZ82] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature* 299.5886, 802–803, 1982.

[WPM09] S. Wu, U. V. Poulsen, and K. Mølmer, "Correlations in local measurements on a quantum state, and complementarity as an explanation of nonclassicality", *Phys. Rev. A* 80.3, 032319, 2009.

[Xu16] J. Xu, "Quantifying coherence of Gaussian states", *Phys. Rev. A* 93.3, 032111, 2016.

[Yao+16a] Y. Yao et al., "Maximal coherence in a generic basis", *Phys. Rev. A* 94.6, 062339, 2016.

[Yao+16b] Y. Yao et al., "Quantum cloning attacks against PUF-based quantum authentication systems", *Quantum Inf. Process.* 15.8, 3311–3325, 2016.

[Zha+16] Y.-R. Zhang et al., "Quantifying coherence in infinite-dimensional systems", *Phys. Rev. A* 93.1, 012334, 2016.

[Zur00] W. H. Zurek, "Einselection and decoherence from an information theory perspective", *Annalen der Physik* 9.11-12, 855–864, 2000.

A

Theoretical framework for physical unclonable functions, including quantum readout

Title:	Theoretical framework for physical unclonable functions, including quantum readout
Authors:	Giulio Gianfelici, Hermann Kampermann and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	3.140 (2020)
Date of submission:	18 November 2019
Publication status:	Published
Contribution by GG:	First author (input approx. 75%)

This publication corresponds to the reference [GKB20]. A summary of the results is presented in Chap. 5. The original research objectives consisted in the study of authentication protocols with QR-PUFs and were set by my coauthors before my work started. These objectives were subsequently reworked by all authors to include classical PUFs and focus on the establishment of a system-independent security framework. I regularly discussed the project with my coauthors, and they repeatedly gave me valuable inputs. In particular, HK guided me to the introduction of the shifters and DB suggested to me to study the examples in Sec. VII of the article. I identified robustness and unclonability as the two properties that quantitatively characterise the security of (QR-) PUFs. I performed all analytical calculations and created all figures in the article. I wrote the whole manuscript which was then proofread by my coauthors and greatly improved thanks to their comments.

Theoretical framework for physical unclonable functions, including quantum readout

Giulio Gianfelici,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

(Received 18 November 2019; accepted 24 March 2020; published 29 April 2020)

We propose a theoretical framework to quantitatively describe physical unclonable functions (PUFs), including extensions to quantum protocols, so-called quantum readout PUFs (QR-PUFs). (QR-) PUFs are physical systems with challenge-response behavior intended to be hard to clone or simulate. Their use has been proposed in several cryptographic protocols, with particular emphasis on authentication. Here, we provide theoretical assumptions and definitions behind the intuitive ideas of (QR-) PUFs. This allows us to quantitatively characterize the security of such devices in cryptographic protocols. First, by generalizing previous ideas, we design a general authentication scheme which is applicable to different physical implementations of both classical PUFs and (QR-) PUFs. Then, we define the *robustness* and the *unclonability*, which allows us to derive security thresholds for (QR-) PUF authentication and paves the way to develop further new authentication protocols.

DOI: 10.1103/PhysRevA.101.042337

I. INTRODUCTION

Authentication is a major task of both classical and quantum cryptography. To achieve secure communication between two parties Alice and Bob, it is necessary to ensure that no intruder may participate in the communication, pretending to be one of the legitimate parties, e.g., by a so-called *man-in-the-middle attack* [1]. Authentication is ultimately classical, even in quantum protocols like quantum key distribution (QKD) [2].

The main ingredient of an authentication protocol is a shared secret between the legitimate parties: during any authenticated communication Alice and Bob must prove the possession of this secret to confirm their identity. One has to distinguish two types of authentication [1]. *Message authentication* is the assurance that a given entity was the original source of the received data. This type of authentication can be achieved by unconditionally secure protocols [3]. *Entity authentication* is the assurance that a given entity can prove its identity and its involvement in the communication session to another entity.

Entity authentication is particularly important if there is an asymmetry between the parties, e.g., when one party, namely, Alice, is a trusted institution and the other one, namely, Bob, is an untrusted user. The communication between Alice and Bob may happen on an authenticated channel owned by Alice, where Bob interacts through a remote terminal. In that case, a one-way entity authentication protocol will be used by Alice to authenticate Bob and to allow him to use her channel. Such protocols are usually based on a *challenge-response authentication*, a type of authentication where Alice presents a *challenge* and Bob provides a valid *response*, based on the common secret, to be authenticated. For instance, Alice can ask for a password (challenge) and Bob will provide the correct one (response).

In the case of asymmetric communication, it is useful to design authentication protocols based on something the parties possess. The trusted Alice can still be required to have secret knowledge since she is able to conceal information from an adversary, but Bob is required only to protect a given token from theft. A crucial condition of this approach is that the object has to be unique and an adversary, namely, Eve, should not be able to copy it easily.

A *physical unclonable function* (PUF) [4] is a physical system which can interact in a very complex way with an external signal (which can serve as a challenge) to give an unpredictable output (which can serve as a response). Its internal disorder is exploited to make it unique, hard to clone, or simulate. PUFs are particularly suited for entity authentication because their internal structure plays the role of the shared secret. They can also be used in other protocols, like oblivious transfer [5], bit commitment [6], or classical key distribution [7]. There is a large variety of PUFs, such as the *optical PUF* [8], the *arbiter PUF* [9], the *SRAM PUF* [10], the *coating PUF* [11], the *magnetic PUF* [12], the *ring oscillator PUF* [13], and so on. A more detailed description of the whole family of PUFs is given in [14] and in [15].

To ensure reliability and security it is required to post-process the PUFs' outputs [16,17]. The most common way to do it is by using the so-called *fuzzy extractor* [18], a tool which combines error correction and privacy amplification. Error correction is necessary because the PUF's output can be different each time the PUF interacts with the same challenge, even when the authentication involves the real Bob with the original PUF. This can be due to an erroneous implementation of the challenge or to noise in the physical process. Privacy amplification is important since the outcomes of a PUF are generally nonuniform, i.e., there exist correlations between different responses that can be used by an adversary to undermine the PUF's security. Furthermore, the response, once it is mapped into a uniform key, can, in principle, be used in different protocols other than entity authentication.

*giulio.gianfelici@uni-duesseldorf.de

However, even when dealing with noise and nonuniformity, there are some issues with PUFs because it has been shown that many of them can be actually cloned or simulated [19–21], compromising their use in secure authentication schemes.

To solve these problems, an extension of PUFs to quantum protocols was suggested, the so-called *quantum readout PUFs* (QR-PUFs) [22]. Such PUFs encode challenges and responses in quantum states, and thus they are expected to be more secure and reliable than classical PUFs, as they add a layer of complexity given by the unclonability of the involved quantum states [23]. Moreover, if such quantum states are nonorthogonal, an adversary cannot perfectly distinguish them, and an attempt to do it would introduce disturbances, thus exposing the presence of an intruder to the legitimate parties.

It is desirable to establish a theoretical framework in which one can perform a rigorous, quantitative analysis of the security properties of (QR-) PUFs. Several efforts have been made to formalize the intuitive ideas of PUF [24–28], and they all capture some aspects of them, but a well-defined agreement about theoretical assumptions and definitions is still lacking. Moreover, the previous approaches are devoted to classical PUFs only.

In this article we propose a common theoretical framework by quantitatively characterizing the (QR-) PUF properties, particularly the *robustness* [25] against noise and the *unclonability*. This is done by generalizing ideas from previous approaches (in particular from [25]) to encompass both classical and QR-PUFs. Moreover, we introduce a generic scheme for authentication protocols with (QR-) PUFs, for which security thresholds can be calculated once an experimental implementation is specified. This scheme provides an abstract formalization of existing protocols, together with ideas such as the difference between a *physical layer* and a *mathematical layer* (see Sec. II) or the concept of the *shifter* (see Secs. IV A and V A). This framework is designed to be independent of the specific experimental implementation such that a comparison of different types of PUFs and QR-PUFs becomes possible. In particular, all implementations use a fuzzy extractor for postprocessing. We expect that this analysis supports both theoretical and experimental research on (QR-) PUFs by promoting the implementation of such devices in existing and new secure authentication schemes.

The paper is organized as follows. In Sec. II we give an introduction on entity authentication protocols with (QR-) PUFs. Section III contains the notation we will use in the paper, in Sec. IV we describe a protocol with a generic classical PUF, and in Sec. V we generalize this to a generic QR-PUF. The shared formalization of the theoretical properties of (QR-) PUFs is stated in Sec. VI and the formalism is applied in some examples in Sec. VII. Some final remarks and the outlook of the work are given in the Conclusion.

II. AUTHENTICATION PROTOCOLS

In the following, we will always call Alice the party that has to authenticate Bob. Mutual authentication can be achieved by repeating the protocol swapping the roles of Alice and Bob. Moreover, we stated in the Introduction that the raw output of a (QR-) PUF has to be postprocessed to be used in secure cryptographic protocols. Therefore, for the sake of clarity, we call *outcome* the raw output while we mean with *response* only the postprocessed uniform key.

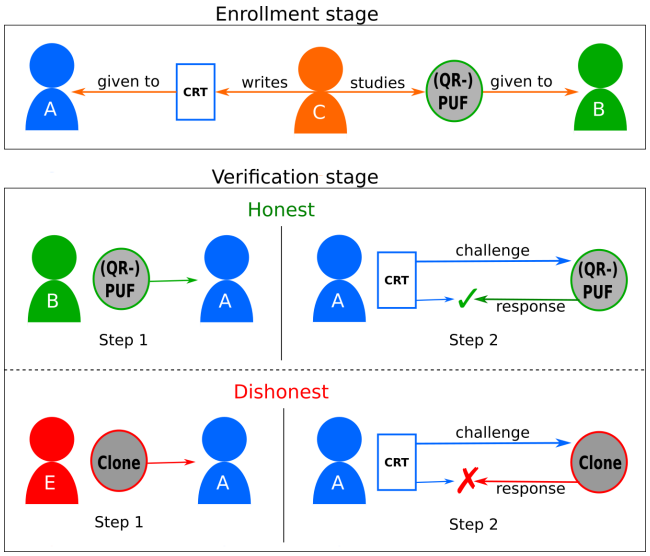

FIG. 1. A schematic description of the authentication scheme. Top: Enrollment stage. The certifier (C, orange) studies the (QR-) PUF's properties and generates the challenge-response table (CRT). Then the CRT is given to Alice (A, blue) and the (QR-) PUF is given to Bob (B, green). Bottom: Verification stage. In the honest case, Bob lets Alice interact with his (QR-) PUF through a terminal and she remotely verifies his identity with the CRT, thus authenticating him. In the dishonest case, an adversary Eve (E, red) claims to be Bob, letting Alice interact with a clone of the (QR-) PUF, and the protocol should lead to an abortion.

Entity authentication protocols with (QR-) PUFs consist of two phases [29], the *enrollment stage* and the *verification stage* (see Fig. 1).

The enrollment stage is a part of the protocol which happens only once at the beginning, after the manufacture of the (QR-) PUF and before any communications between Alice and Bob. An entity or group of entities called the *(QR-) PUF certifier* [which may be the (QR-) PUF manufacturer, Alice itself, a third trusted party, or a combination of all of them] studies the (QR-) PUF's properties and evaluates the parameters needed for the implementation and postprocessing. In particular, the certifier selects a certain number N of challenges and records the corresponding responses. Challenges and responses form the so-called challenge-response pairs (CRPs) and they are stored as a challenge-response table (CRT), together with additional information needed in the remaining part of the protocol. After the end of this stage, the certifier gives the CRT to Alice (which then *knows* the secret) and the (QR-) PUF to Bob (which then *has* the secret).

The verification stage is the part of the protocol where communication between Alice and Bob is necessary. In this stage, Bob declares his identity to Alice with his (QR-) PUF, remotely interacting with her through her terminal. To authenticate Bob, Alice sends randomly one challenge from the CRT to the (QR-) PUF and collects the outcome, which is

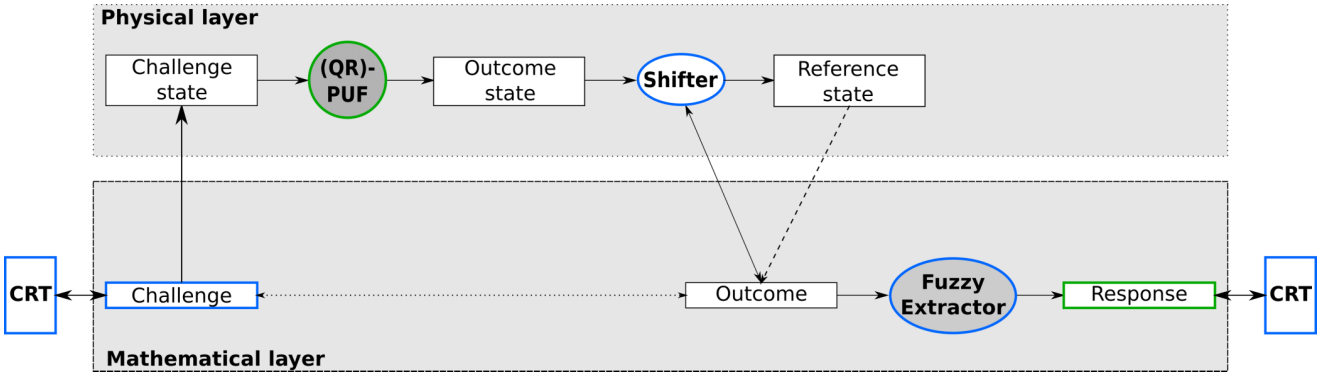

FIG. 2. A scheme of the two layers, the mathematical one (where the cryptographic protocol takes place) and the physical one (where the (QR-) PUF acts). In the physical layer a challenge state is prepared according to the information of the challenge (mathematical layer) and then the (QR-) PUF transforms it into an outcome state. The state-dependent shifter (see Secs. IV A and V A) maps the outcome state to a reference state. The outcome in the mathematical layer contains information about the implementation of the shifter and the error in the reference state and is postprocessed by the fuzzy extractor to give the response. Challenges and responses are stored into (enrollment stage) or taken from (verification stage) the challenge-response table (CRT). See Secs. IV and V for a more detailed description.

then postprocessed. The calculated response is compared with the one in the CRT, i.e., the one obtained in the enrollment stage. If they match, Alice authenticates Bob. This stage can be repeated every time Alice needs to authenticate Bob. After every round, however, the used challenge-response pair has to be eliminated from the CRT and cannot be used again.[1]

Depending on the different types of (QR-) PUFs, the challenges could be different types of physical quantities. For instance, optical PUFs are transparent materials filled with light scattering particles: a laser that interacts with one of them is turned into a unique speckle pattern. For a classical optical PUF, the challenge is the laser orientation and the outcome is the intensity of some points in the speckle pattern [8]. For a QR-PUF, the challenges and the outcomes are quantum states [22]. In both cases, however, challenges, outcomes, and responses are stored in the CRT as digital binary strings, and the responses are used as authentication keys.

There are two different layers involved in this protocol: a physical one, where the actual (QR-) PUF acts as a physical evolution from input systems to output systems, and a mathematical one, where a binary challenge string (which should represent the information on how to implement the input system) is mapped into an outcome string which is postprocessed into a response string.

To deal with the two different layers, we denote as *challenges* (*outcomes*, *responses*) the strings in the mathematical layer and as *challenge states*[2] (*outcome states*, *response states*) the implementations in the physical layer.

This configuration is schematized in Fig. 2.

[1]It was argued [22] that in the QR-PUF case, challenge-response pairs could be used again because an adversary is not able to gain full information about their state. Such claims need to be quantitatively proven; here we continue as if any reused CRP is insecure.

[2]This term clearly comes from quantum physics, where it is used to describe a vector in a Hilbert space. We will use the term *classical state* in this article, meaning a classical physical quantity, either scalar or vectorial.

III. NOTATION

In the article we will use the following conventions:

(i) Digital strings, like the challenges and the responses, are denoted by lowercase bold letters, for instance, $\mathbf{x_i}$ and $\mathbf{r_j}$ for the ith challenge and the jth response, respectively;

(ii) Sets of digital strings are denoted by the calligraphic uppercase letters, e.g., $\mathcal{X}$ and $\mathcal{R}$ for the set of challenges and responses, respectively;

(iii) Random variables which take values from given sets are denoted by uppercase italic letters, e.g., X and R for challenges and responses, respectively;

(iv) The physical classical states are denoted by the vector symbol (right arrow), for instance, $\vec{x}_i$ and $\vec{r}_j$ for the ith challenge state and the jth response state, respectively;

(v) The physical quantum states are denoted by the usual ket notation, for instance, $|x_i\rangle$ and $|r_j\rangle$, for the ith challenge state and the jth response state, respectively;

(vi) Maps are denoted by uppercase letters with a circumflex accent, e.g., $\hat{P}$ or $\hat{\Pi}$. In particular, the Latin letters are used for maps between strings and the Greek ones for maps between states.

IV. CLASSICAL PUF

The realization of a challenge state may involve several different steps, each of them with different experimental complexity. Each step involves devices with a limited, even though possibly large, number of different configurations, and such configurations can be used to parametrize the experimental system, resulting in our ability to formalize the challenges through discrete variables. A challenge is therefore defined as the binary string $\mathbf{x_i}$ of length n representing the configuration which realizes a given challenge state $\vec{x}_i$.

A. Enrollment

At the start of the enrollment stage, the PUF certifier selects $N \leqslant 2^n$ different challenges $\mathbf{x_i} \in \mathcal{X} \subseteq \{0,1\}^n$, where $\mathcal{X} \subseteq \{0,1\}^n$ is the set of all chosen challenges and $|\mathcal{X}| = N$. In fact, if a challenge consists of n bits, the total possible

number of challenges is 2^n. However, in practice, certain challenges could represent states which are impossible or hard to implement or they do not lead to a set of distinguishable responses.

For security purposes, the set of challenges $\mathcal{X}$ has to be uniform, i.e., $\hat{S}(X) = |\mathcal{X}|$, where X is the random variable defined on the set $\mathcal{X}$ and $\hat{S}(X)$ is the Shannon entropy of X. An adversary should not be able to characterize the set of challenges by studying some of them. The certifier is free to discard some challenges from $\mathcal{X}$ if he finds correlations in them. This affects the number N of challenges and has to be quantified for given experimental implementations.

Each $\mathbf{x_i} \in \mathcal{X}$ represents a challenge state $\vec{x}_i$ which can be experimentally realized and sent to the PUF, which acts as a deterministic function $\hat{\Pi}$. Due to its complex structure, any attempt to give a full description of it should be unfeasible, even for the certifier itself. For a given challenge state $\vec{x}_i$, $\hat{\Pi}(\vec{x}_i) = \vec{y}_i$, where $\vec{y}_i$ is denoted as an outcome state.

The certifier needs to map the outcome state into an outcome string, taking into account both the distribution of the outcome states and any error which may have occurred due to noise or wrong implementation of the experimental system. To do this, we introduce the notion of a shifter.

For each outcome state $\vec{y}_i$, let $\hat{\Omega}_i$ be a state-dependent operation which maps $\vec{y}_i$ into a reference state, denoted by $\vec{0}$, equal for all outcome states. For N outcome states $\vec{y}_i$ we obtain a set of N shifters $\hat{\Omega}_i$. The importance of using the shifters will be more clear when we discuss QR-PUFs. The shifters simplify the error verification process, as each expected outcome is identical.

Some devices ascribable to shifters have been used in some PUF implementations: consider, for instance, the optical PUF [8], where a laser beam (challenge state) is transformed into a complex speckle pattern (outcome state). In this scenario, it has been proposed [30] to use spatial light modulators to transform every speckle pattern into a plane wave, which then is focused into a single point (the reference state). Only if the pattern is the expected one does this happen; otherwise, the outcome state is mapped into another speckle pattern. Shifters can be designed also for other PUFs, depending on which physical quantities are implied in the outcome states. If the outcome state is already a binary value (like in the SRAM PUF [10]) the reference state can be the bit 0 and the shifters can be realized by a gate implementing either the identity or a bit-flip operation, depending on the expected outcome state. Whenever an outcome is determined by the frequency of a signal (like in a ring oscillator PUF [13]), the shifters can be passband filters.

The certifier can implement the corresponding shifter for every outcome state, since he can characterize $\hat{\Pi}(\vec{x}_i)$, possibly repeating the PUF evaluation for the same challenge state $\vec{x}_i$, to find a $\hat{\Omega}_i$ such that $\hat{\Omega}_i[\hat{\Pi}(\vec{x}_i)] = \vec{0}$.

We define $\vec{o}_i := \hat{\Omega}_i[\hat{\Pi}(\vec{x}_i)]$. While in the enrollment stage, or in a noiseless verification stage, $\vec{o}_i = \vec{0}$ by definition, in reality $\vec{o}_i$ will contain errors. This error is mapped into the Hamming weight, i.e., the number of bits that are different from 0, of a classical string $\mathbf{o_i}$, i.e., $\mathbf{o_i} = \mathbf{0}_{l_o} = 00\ldots0$ if and only if $\vec{o}_i = \vec{0}$. The string has a length l_o, dependent on the experimental implementation of the shifter. In the aforementioned example of an optical PUF, the plane wave is focused onto an analyzer plane with a pinhole. If $\vec{o}_i = \vec{0}$ the light passes through this pinhole and a detector will click. Therefore the intensity of the light on the analyzer plane outside the pinhole can be used to find $\mathbf{o_i}$, and the resolution of the analyzer plane determines the length l_o.

The shifters convey information about the distribution of the outcome states (as they are designed on them) and therefore indirectly about the PUF. We can represent this information in terms of binary strings in the mathematical layer, just as we did for challenge states. The shifters are implemented by an experimental device (or a collection of them) with a limited number of configurations, each one of them implementing a different $\hat{\Omega}_i$. Parametrizing such configurations, we map each shifter $\hat{\Omega}_i$ in a string $\mathbf{w_i} \in \mathcal{W} \subseteq \{0,1\}^{l_w}$. This string is exact, because it represents only the correct implementation of the shifter, without taking into account any noise. The length l_w depends on the entropy of the shifters and, consequently, on the outcome states (for some implementations, methods to analyze such an entropy have been derived [31,32]). The entropy of $\mathcal{W}$ has to be studied also to verify the presence of nonuniformity, i.e., correlations between different outcomes or between challenges and corresponding outcomes. This entropy affects the unclonability of the PUF (see Sec. VI).

The two strings $\mathbf{o_i}$ and $\mathbf{w_i}$ convey two different aspects of the outcome state. In fact, $\mathbf{o_i}$ gives information about the error only, without distinguishing different outcomes. Instead, $\mathbf{w_i}$ gives information about the distribution of the outcome states but not about errors (even a single bit-flip of $\mathbf{w_i}$ changes it into $\mathbf{w_{j\neq i}}$).

We combine $\mathbf{o_i}$ and $\mathbf{w_i}$ by defining as *outcome* a string $\mathbf{y_i}$ of length $l = l_w + l_o$, such that

$$\mathbf{y_i} = \mathbf{w_i} \,\|\, \mathbf{o_i}, \tag{1}$$

where $\|$ is the concatenation of strings. We designate $\mathcal{Y} \subseteq \{0,1\}^l$ as the set of all outcomes, including all possible noisy versions. Explicitly,

$$\mathcal{Y} = \{\mathbf{y_i} = \mathbf{w_i} \,\|\, \mathbf{o_i},\ \mathbf{w_i} \in \mathcal{W},\ \mathbf{o_i} \in \{0,1\}^{l_o}\}, \tag{2}$$

and $|\mathcal{Y}| = 2^{l_o} N$ (see Fig. 3 for a graphic representation of the set $\mathcal{Y}$). Moreover, we define a function $\hat{P} : \mathcal{X} \to \mathcal{Y}$, associating each challenge with the corresponding outcome, i.e., $\hat{P}(\mathbf{x_i}) = \mathbf{y_i}$.

The outcome string, being noisy and not uniformly distributed, cannot be used directly as a response. The most common way to postprocess it is through a *fuzzy extractor* [18], which is a combined error correction and privacy amplification scheme.

Definition IV.1. Let $\{0,1\}^\star$ be the *star closure* of $\{0,1\}$, i.e., the set of strings of arbitrary length:

$$\{0,1\}^\star = \bigcup_{i \geqslant 0} \{0,1\}^i, \tag{3}$$

where $\{0,1\}^0 = \emptyset$ is the empty set. Let $\hat{H}(\mathbf{y_i}, \mathbf{y_i'})$ be the Hamming distance between $\mathbf{y_i}$ and $\mathbf{y_i'}$, i.e., the Hamming weight of $\mathbf{y_i} + \mathbf{y_i'}$, and $s := -\log_2(\max_k p_k)$ be the min-entropy of a probability distribution $p = \{p_k\}$. Furthermore, given two probability distributions p_A, p_B, associated to discrete random variables A, B with the same domain $\mathcal{C}$, let $\hat{D}_S(p_A, p_B)$ be the

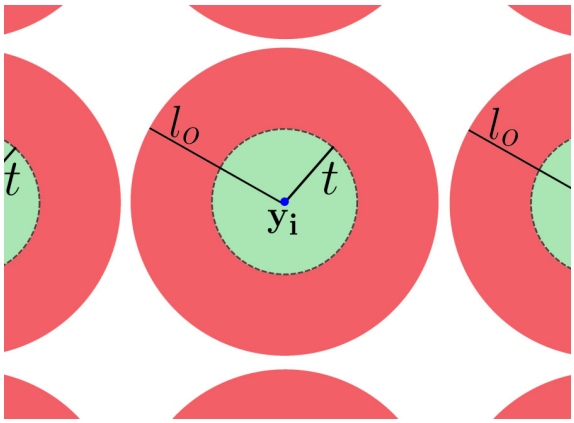

FIG. 3. Graphic representation of the set $\mathcal{Y}$, according to Eq. (2). The centers of the circles represent the noiseless outcomes $\mathbf{y_i} = \mathbf{w_i}\|\mathbf{0}_{l_o}$ for different $\mathbf{w_i} \in \mathcal{W}$, while every point in the corresponding outer circles, of radius l_o, represents a noisy version of them. Between different outcomes, including the noisy versions, there is no overlap, because $\mathbf{w_i} \neq \mathbf{w_j}$ for $i \neq j$. A fuzzy extractor can correct $t < l_o$ bit errors, i.e., the outcomes inside the inner circles.

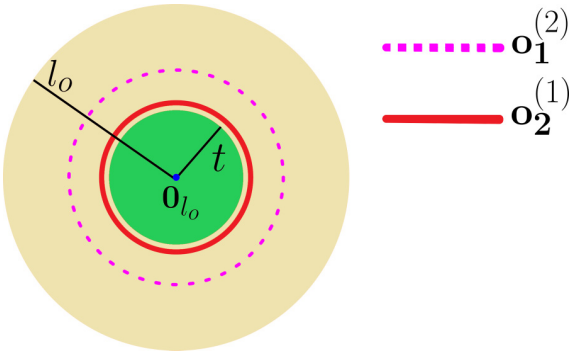

FIG. 4. Graphic representation of the choice of t for $N = 2$ challenge-response pairs. The circle represents both $\mathbf{o_1}$ and $\mathbf{o_2}$, independently from $\mathbf{w_1}$ and $\mathbf{w_2}$. The center of the circle represent the noiseless cases $\mathbf{o_1} = \mathbf{o_2} = \mathbf{0}_{l_o}$, and all the noisy cases lie in a circle of radius l_o. The errors $\mathbf{o}_1^{(2)}$ and $\mathbf{o}_2^{(1)}$ define two rings, and t is chosen smaller than the radius of the smaller one (in our case $\mathbf{o}_2^{(1)}$).

statistical distance between p_A and p_B, i.e.,

$$\hat{D}_S(p_A, p_B) := \frac{1}{2} \sum_{c \in \mathcal{C}} |P(A = c) - P(B = c)|. \tag{4}$$

A $(\mathcal{Y}, s, m, t, \epsilon)$ fuzzy extractor is a pair of random functions, the generation function $\hat{G}$, and the reproduction function $\hat{R}$, with the following properties:

(i) $\hat{G} : \mathcal{Y} \to \{0,1\}^m \times \{0,1\}^\star$ on input $\mathbf{y_i} \in \mathcal{Y}$ outputs an extracted string $\mathbf{r_i} \in \mathcal{R} \subseteq \{0,1\}^m$ and a *helper data* $\mathbf{h_i} \in \mathcal{H} \subseteq \{0,1\}^\star$. While $\mathbf{r_i}$ has to be kept secret, $\mathbf{h_i}$ can be made public (it can even be physically attached to the PUF);

(ii) $\hat{R} : \mathcal{Y} \times \mathcal{H} \to \{0,1\}^m$ takes an element $\mathbf{y}'_\mathbf{i} \in \mathcal{Y}$ and a helper string $\mathbf{h_i} \in \mathcal{H}$ as inputs. The *correctness property* of a fuzzy extractor guarantees that if $\hat{H}(\mathbf{y_i}, \mathbf{y}'_\mathbf{i}) \leqslant t$ and $(\mathbf{r_i}, \mathbf{h_i}) = \hat{G}(\mathbf{y_i})$, then $\hat{R}(\mathbf{y}'_\mathbf{i}) = \mathbf{r_i}$;

(iii) The *security property* guarantees that for any probability distribution on $\mathcal{Y}$ of min-entropy s, the string $\mathbf{r_i}$ is nearly uniform even for those who observe $\mathbf{h_i}$: i.e., if $(\mathbf{r_i}, \mathbf{h_i}) = \hat{G}(\mathbf{y_i})$, then

$$\hat{D}_S(p_{RH}, p_{UH}) \leqslant \epsilon, \tag{5}$$

where p_{RH} (p_{UH}) is a joint probability distribution for $\mathbf{r_i} \in \mathcal{R}$ (for a uniformly distributed variable on m-bit binary strings) and $\mathbf{h_i} \in \mathcal{H}$.

The generation function of a fuzzy extractor is used, in the enrollment stage, to transform the outcome $\mathbf{y_j}$ into the uniformly distributed $\mathbf{r_i}$, that is the final response. We will see later that, in the verification stage, the reproduction function is used on a noisy version of the outcome to generate the same response.

The certifier selects a fuzzy extractor by knowing $\mathcal{Y}$ and its min-entropy s, and choosing t such that the fuzzy extractor uniquely maps a given outcome into a response, without collisions: due to noise or an erroneous experimental setup, a challenge state $\vec{x}_i$ can be implemented as a state which is closer to $\vec{x}_j$ for $i \neq j$. The error $\mathbf{o}_\mathbf{i}^{(j)}$ associated to $\hat{\Omega}_i[\hat{\Pi}(\vec{x}_j)]$ for $i \neq j$ must be uncorrectable; the certifier has to choose a maximum allowed error $t < l_o$ smaller than the minimum Hamming weight of $\mathbf{o}_\mathbf{i}^{(j)}$, over all $i \neq j$ (see Fig. 4).

There is a tradeoff between t and the entropy of the shifters: a high entropy, associated to a longer length l_w of $\mathbf{w_i}$, is equivalent to similar states with a small error in case of a wrong implementation, and t has to be chosen low. The certifier may decide to delete challenge-response pairs from the challenge-response table in order to choose a higher t and increase the resistance of the PUF against the noise.

For practical purposes we define two functions $\hat{G}_R$ and $\hat{G}_H$ such that

$$\hat{G}(\cdot) = (\hat{G}_R(\cdot), \hat{G}_H(\cdot)), \tag{6}$$

and therefore $\mathbf{r_i} = \hat{G}_R(\mathbf{y_i})$ and $\mathbf{h_i} = \hat{G}_H(\mathbf{y_i})$ for $\mathbf{y_i} \in \mathcal{Y}$. Moreover, we define the function $\hat{F}_E$ to be the function mapping each challenge to the respective response in the enrollment stage, i.e.,

$$\hat{F}_E(\cdot) := \hat{G}_R(\hat{P}(\cdot)), \tag{7}$$

for $\mathbf{x_i} \in \mathcal{X}$ and therefore $\mathbf{r_i} = \hat{F}_E(\mathbf{x_i})$.

Summarizing, during the enrollment stage the certifier creates a set of N challenges $\mathcal{X} \in \{0,1\}^n$ and a set of N responses $\mathcal{R} \subseteq \{0,1\}^m$:

$$\mathcal{R} = \{\, \mathbf{r_i} \in \{0,1\}^m \mid \mathbf{r_i} = \hat{F}_E(\mathbf{x_i}); \quad \mathbf{x_i} \in \mathcal{X} \,\}. \tag{8}$$

They are stored into the CRT together with

(i) the set of N strings $\mathbf{w_i}$ representing how to set the shifter operator to get the correct outcome;

(ii) the parameters of the fuzzy extractor;

(iii) the (possibly public) set of helper data $\mathcal{H} \subseteq \{0,1\}^\star$, i.e.,

$$\mathcal{H} = \{\, \mathbf{h_i} \in \{0,1\}^\star \mid \mathbf{h_i} = \hat{G}_H[\hat{P}(\mathbf{x_i})]; \quad \mathbf{x_i} \in \mathcal{X} \,\}. \tag{9}$$

The CRT is given to Alice and the PUF to Bob, concluding the enrollment stage.

B. Verification

In the verification stage, Bob declares his identity and allows Alice to (remotely) interact with his PUF. Alice, equipped with the CRT, retraces the steps made by the certifier in the enrollment stage.

She picks up a randomly selected challenge $\mathbf{x_j} \in \mathcal{X}$ [for which she knows the response $\mathbf{r_j} = \hat{F}_E(\mathbf{x_j})$] and prepares the challenge state $\vec{x}_j$. The PUF transforms $\vec{x}_j$ into the outcome state $\hat{\Pi}(\vec{x}_j)$. At this point, Alice tunes the shifter $\hat{\Omega}_j$, according to the CRT and evaluates $\hat{\Omega}_j[\hat{\Pi}(\vec{x}_j)]$.

After the use of the PUF and the shifter, she may obtain a noisy version of $\vec{y}_j$ because of noise or a wrong preparation of the challenge state. Moreover, the noise could come from the PUF not being the original one if an adversary Eve is impersonating Bob.

We call this noisy version $\vec{y'}_j = \hat{\Pi}^{(e)}(\vec{x}_j)$. In that case $\hat{\Omega}_j(\vec{y'}_j) \neq \vec{0}$, which leads to $\mathbf{o'_j} \neq \mathbf{0}_{l_o}$ such that $\mathbf{y'_j} = \mathbf{w_j} \parallel \mathbf{o'_j} = \hat{P}^{(e)}(\mathbf{x_j})$ is different from the $\mathbf{y_j}$ obtained by the certifier in the enrollment stage.

The outcome is then postprocessed by the reproduction function of the fuzzy extractor that was used in the enrollment stage, so Alice collects $\mathbf{z_j} := \hat{F}_V(\mathbf{x_j})$, where the function $\hat{F}_V$ represents the map between the challenges and the corresponding responses in the verification stage, i.e.,

$$\hat{F}_V := \hat{R}[\hat{P}^{(e)}(\cdot), \hat{G}_H(\hat{P}(\cdot))], \tag{10}$$

for $\mathbf{x_j} \in \mathcal{X}$.

The claimed response $\mathbf{z_j}$ is compared with the one in the CRT: if $\mathbf{z_j} = \mathbf{r_j}$, Bob is authenticated, otherwise the protocol fails.

V. QR-PUF

The authentication scheme for quantum readout PUFs follows the structure of the classical scheme (see Sec. IV) and still uses classical challenges, responses, and fuzzy extractors in the mathematical layer. However, the implementation of the challenge states and outcome states in the physical layer is done via quantum states. At the moment, the only classical PUF which was extended to a QR-PUF is an optical PUF [22,30], for which there are some studies on side-channel attacks [33–35].

In this work we study discrete qubit states, but our approach could also be generalized to continuous-variable (QR-) PUFs [36,37]. Let us assume to work with λ qubits, so challenge states are elements of the Hilbert space $\mathbb{C}^{2^\lambda}$. We also assume that each qubit can be in a finite number of states. Like in the classical case, we can parametrize the configurations of the experimental system that implements the challenge states to obtain a set $\mathcal{X}$ of classical challenges. Let us denote the length of such strings by n to match the case of classical PUFs.

Here the challenge states are quantum; therefore challenge states will be represented by $|x_i\rangle$. Our QR-PUF will be described in an idealized way, as a unitary operation acting on a pure state to produce another pure state. In reality, this process will introduce noise: in our framework, this will be taken into account in the transition from the outcome state to the outcome string.

A. Enrollment

Since not all states are implementable, or they do not lead to distinguishable responses, the certifier selects $N \leqslant 2^n$ challenges $\mathbf{x_i} \in \mathcal{X} \subseteq \{0,1\}^n$, where $\mathcal{X}$ is implemented by a set of nonorthogonal states $\{ |x_1\rangle, \ldots, |x_N\rangle \} \in \mathbb{C}^{2^\lambda}$.

The nonorthogonality is expected to be a crucial condition, since, as a consequence of the no-cloning theorem [23], there does not exist a measurement which perfectly distinguishes nonorthogonal states. We expect that this enhances the security of QR-PUFs compared to classical PUFs, since an adversary could gain only a limited amount of information about the challenge and the outcome states.

In this work we consider separable challenge states $|x_i\rangle$, so $|x_i\rangle = \bigotimes_{k=1}^{\lambda} |x_{ik}\rangle$ and we can deal with single-qubit states $|x_{ik}\rangle$. The procedure can be generalized to other challenge states. The qubit states can be written in terms of some complete orthonormal basis, which we denote as $\{ |0\rangle, |1\rangle \}$

$$|x_{ik}\rangle = \cos\theta_{ik} \; |0\rangle + e^{i\varphi_{ik}} \sin\theta_{ik} \; |1\rangle \,, \tag{11}$$

where $\theta_{ik} \in [0, \pi]$ and $\varphi_{ik} \in [0, 2\pi]$.

The certifier sends all states to the QR-PUF, collecting the outcome states. The QR-PUF is formalized as a λ-fold tensor product of single-qubit unitary gates $\hat{\Phi} = \bigotimes_{k=1}^{\lambda} \hat{\Phi}_k$. Despite its form being unknown, it can be parametrized by [38]

$$\hat{\Phi}_k(\omega_k, \psi_k, \chi_k) = \begin{pmatrix} e^{i\psi_k}\cos\omega_k & e^{i\chi_k}\sin\omega_k \\ -e^{-i\chi_k}\sin\omega_k & e^{-i\psi_k}\cos\omega_k \end{pmatrix}, \tag{12}$$

with random parameters $\psi_k, \chi_k \in [0, 2\pi]$ and $\omega_k \in [0, \frac{\pi}{2}]$. The outcome state is then $|y_i\rangle = \bigotimes_{k=1}^{\lambda} |y_{ik}\rangle$, where

$$\begin{aligned} |y_{ik}\rangle &= \hat{\Phi}_k \, |x_{ik}\rangle \\ &= \begin{pmatrix} e^{i\psi_k}\cos\omega_k\cos\theta_{ik} + e^{i(\chi_k+\varphi_{ik})}\sin\omega_k\sin\theta_{ik} \\ -e^{-i\chi_k}\sin\omega_k\cos\theta_{ik} + e^{i(\varphi_{ik}-\psi_k)}\cos\omega_k\sin\theta_{ik} \end{pmatrix}. \end{aligned} \tag{13}$$

Like in the classical case, the certifier can design a state-dependent shifter that performs a tensor product of unitary transformations, $\hat{\Omega}_i = \bigotimes_{k=1}^{\lambda} \hat{\Omega}_{ik}$, each one of them mapping a specific qubit state to the reference state $|0\rangle = (1,0)^T$. This operation is indeed unitary, because for $|y_{ik}\rangle = \cos\alpha_{ik}|0\rangle + e^{i\beta_{ik}} \sin\alpha_{ik} \, |1\rangle$, it holds that $\hat{\Omega}_{ik} \, |y_{ik}\rangle = |0\rangle$ for

$$\hat{\Omega}_{ik} = \begin{pmatrix} \cos\alpha_{ik} & e^{-i\beta_{ik}}\sin\alpha_{ik} \\ e^{i\beta_{ik}}\sin\alpha_{ik} & -\cos\alpha_{ik} \end{pmatrix}, \tag{14}$$

which verifies $\hat{\Omega}_{ik}\,\hat{\Omega}_{ik}^\dagger = \hat{\Omega}_{ik}^\dagger\,\hat{\Omega}_{ik} = \mathbb{I}$, where $\mathbb{I}$ is the identity operator. The certifier can implement $\hat{\Omega}_i$ for each $\hat{\Phi}|x_i\rangle$ because he can repeat the experiment and characterize each outcome state by performing quantum state tomography or, as we work with pure states, compressed sensing [39].

Instead of having to change the single-qubit measurement basis for each qubit and each challenge, by applying the suitable shifter it is now possible to use the basis $\{ |0\rangle, |1\rangle \}$ for all qubits of all challenges.

By definition of $\hat{\Omega}_{ik}$, if there is no error, we will measure for every qubit the state $|0\rangle$, and the results of the measurement form a string of length λ made by all zeros, $\mathbf{o_i} = \mathbf{0} = 00\ldots0$. If there is some error, which in the quantum case is introduced

by either the environment or an adversary, the Hamming weight of $\mathbf{o_i}$ will give us an estimate of it.

Like in the classical case, we can parametrize the experimental system that implements the shifters in terms of the (discrete) configuration it must assume to implement a specific $\hat{\Omega}_i$. Therefore, a given $\hat{\Omega}_i$ is represented by a classical string $\mathbf{w_i} \in \mathcal{W}$ of length l_w.

We again define as *outcome* a classical string $\mathbf{y_i}$ of length $l = l_w + \lambda$, given by

$$\mathbf{y_i} = \mathbf{w_i} \,\|\, \mathbf{o_i}, \tag{15}$$

where $\|$ is the concatenation of strings.

We also define a set $\mathcal{Y}$ like in Eq. (2) and a function $\hat{P} : \mathcal{X} \to \mathcal{Y}$ mapping every challenge to the corresponding outcome. At this point, like for classical PUFs, the certifier fixes the correctable amount of noise $t < l_o$ and selects a fuzzy extractor $(\hat{G}, \hat{R})$, able to correct t errors and to generate a uniformly distributed response, according to the distribution of the outcome states and the entropy of the set of outcomes. The nonorthogonality of the challenge states affects t: when a wrong challenge state is implemented, its *fidelity* with the correct one is preserved by the QR-PUF and the shifter, since they are unitary maps, and influences the results of the measurement. The maximum correctable error t has to be chosen lower than the error produced by wrong implementations, which becomes small for highly nonorthogonal challenges. The certifier may decide to delete challenge-response pairs from the challenge-response table in order to choose a higher t and increase the resistance of the QR-PUF against the noise. However, this reduces the overall nonorthogonality of the quantum states, thus improving Eve's ability to distinguish them. Such a tradeoff will be discussed again in the following sections.

The generation function of a fuzzy extractor generates a uniformly distributed response $\mathbf{r_i} \in \mathcal{R}$, together with a public helper data $\mathbf{h_i} \in \mathcal{H}$. Again, we have

$$\hat{G}(\cdot) = (\hat{G}_R(\cdot), \hat{G}_H(\cdot)), \tag{16}$$

and

$$\mathbf{r_i} = \hat{G}_R(\mathbf{y_i}), \quad \forall\, \mathbf{y_i} \in \mathcal{Y}. \tag{17}$$

We define a function $\hat{F}_E(\cdot) := \hat{G}_R(\hat{P}(\cdot)) : \mathcal{X} \to \mathcal{R}$, mapping each challenge to the corresponding response, representing the action of the QR-PUF in the enrollment stage. Like for classical PUFs, challenges, responses, and other information are stored in the challenge-response table, which is given to Alice, while the QR-PUF is given to Bob.

B. Verification

In the verification stage Bob allows Alice to (remotely) interact with his QR-PUF. She selects randomly a challenge $\mathbf{x_j} \in \mathcal{X}$ and prepares $|x_j\rangle$.

Using the QR-PUF with the challenge state $|x_j\rangle$, Alice may obtain $|y'_j\rangle$, different from the expected $|y_j\rangle$, because of noise or an erroneous implementation of the system or the action of a malicious intruder. Then Alice applies $\hat{\Omega}_j$ and measures each qubit state in the basis $\{\,|0\rangle, |1\rangle\,\}$, obtaining $\mathbf{o'_j}$ and hence the outcome $\mathbf{y'_j} = \mathbf{w_j} \,\|\, \mathbf{o'_j}$. While in the ideal noiseless case $\mathbf{o'_j} = \mathbf{0}_{l_o}$, here we may measure some state $|1\rangle$ for some qubits; therefore $\mathbf{y'_j}$ could be different from the $\mathbf{y_j}$ obtained by the certifier in the enrollment stage.

The outcome is then postprocessed by the reproduction function of the fuzzy extractor that was used in the enrollment stage, so Alice collects $\mathbf{z_j} := \hat{F}_V(\mathbf{x_j})$, where the function $\hat{F}_V$ is defined like in the classical case, $\hat{F}_V(\cdot) := \hat{R}[\hat{P}^{(e)}(\cdot), \hat{G}_H(\hat{P}(\cdot))]$. Authentication succeeds if $F_E(\mathbf{x_j}) = F_V(\mathbf{x_j})$. The verification stage is schematized in Fig. 5.

VI. PROPERTIES AND FORMALIZATION

In this section, we will analyze the properties of (QR-) PUFs. As we have seen, both PUFs and QR-PUFs can be represented by a classical pair of functions $\hat{F} = (\hat{F}_E, \hat{F}_V)$ that describe the map between challenges and responses in the enrollment [$\hat{F}_E$, see Eq. (7)] or verification [$\hat{F}_V$, see Eq. (10)] stage. We will keep the same formalism for both PUFs and QR-PUFs to allow our framework to compare them, but we will also specify the practical differences.

We have seen that the noise can be a problem which can lead to false rejection in the protocols. Therefore it is important to characterize and quantify the amount of noise of a (QR-) PUF which is connected to the *robustness* of a (QR-) PUF. We take the definition of this concept from [25], adapting it to our framework and our formalism.

Definition VI.1. Let us consider a (QR-) PUF $\hat{F}$ with a set of challenges $\mathcal{X}$, where $|\mathcal{X}| = N$. $\hat{F}$ is *ρ-robust* with respect to $\mathcal{X}$ if $\rho \in [0, 1]$ is the greatest number for which

$$\frac{1}{N} \sum_{i=1}^{N} P\{\hat{F}_V(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})\} \geqslant \rho, \tag{18}$$

where ρ is called the *robustness* of the (QR-) PUF with respect to $\mathcal{X}$.

The robustness represents the average probability that the (QR-) PUF in the verification stage outputs the correct response such that the authentication succeeds. So it represents the (QR-) PUF's ability to avoid false rejections and depends on many factors, e.g., on the average noise of the specific implementation and the parameters of the fuzzy extractor.

Regarding the robustness, we do not expect a significant advantage of QR-PUFs compared to classical PUFs. Actually, there is the possibility to have a disadvantage, because of the fragility of quantum states and of the necessity of having a low error threshold t, as the noise can originate from a possible interaction of an adversary. Any implementation with QR-PUFs has to pay special care to this issue.

Now we will discuss unclonability, which is the main parameter involved in attacks from an adversary Eve. This concept is also mildly inspired by [25] but with marked differences, mainly caused by the need of taking into account QR-PUFs. In the context of entity authentication with (QR-) PUF, the purpose of an adversary Eve is to create a clone of a (QR-) PUF such that Alice can verify with it a challenge-response pair, falsely authenticating her as Bob.

When we say *clone*, we need to specify whether we are talking of a physical or a mathematical one. A *physical clone* is an experimental reproduction of the (QR-) PUF. It will have the same physical properties as the original one, even in contexts not involved with the authentication protocol. The requirement of *physical unclonability* means that a physical

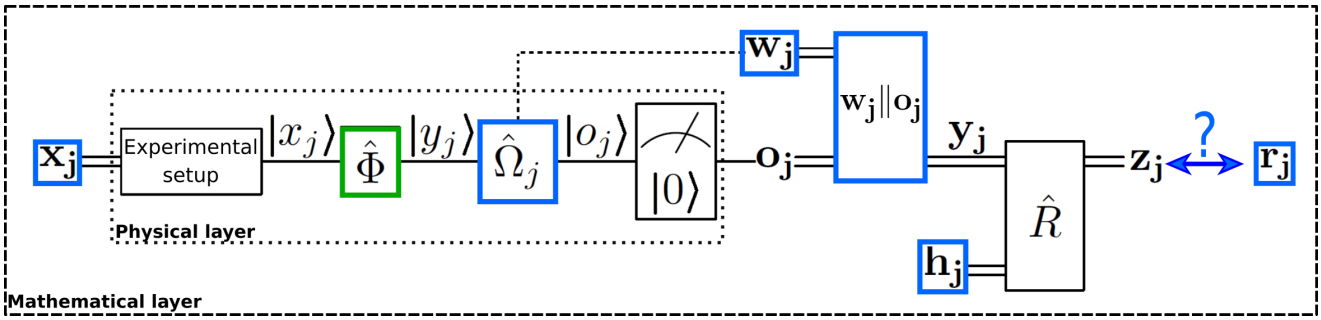

FIG. 5. A scheme for the verification stage for QR-PUFs, as described in Sec. V B. Bob provides the QR-PUF ($\hat{\Phi}$, here enclosed in a green box), and Alice uses quantities stored in the challenge-response table (here enclosed in blue boxes) to evaluate a response $\mathbf{z_j}$ for a challenge $\mathbf{x_j}$. Authentication succeeds if $\mathbf{z_j} = \mathbf{r_j}$, where $\mathbf{r_j}$ is the response stored in the CRT. The verification stage for classical PUFs (as described in Sec. IV B) can be obtained by substituting in the physical layer (the inner box) quantum states and operators with classical states and operators, and by leaving the mathematical layer (outer box) unchanged.

clone is technologically or financially unfeasible at the current state of technology.

A mathematical clone, instead, is an object that *simulates* the challenge-response behavior of a (QR-) PUF. In this case, we cannot just state that a mathematical clone is unfeasible, because if there are some correlations between the outcome states, in principle they can be exploited to predict new challenge-response pairs. As mentioned in the Introduction, several PUFs have been successfully mathematically cloned. We need to formalize this notion in order to quantify it for different (QR-) PUFs.

We assume that Eve cannot directly access the internal structure of the (QR-) PUF [24,40] but only interact with the challenge and the outcome states. An attack consists of two phases, both carried out during the verification stage of the protocol. We require that the enrollment stage is inaccessible to Eve, since this part is performed in the certifier's laboratory and it involves the study of the inner structure of the (QR-) PUF. During the *passive phase*, Eve observes a certain number of successful authentications with the real (QR-) PUF, collecting as much information as she can. Then, during the *active phase* she designs a clone and gives it to Alice, claiming to be Bob. The attack succeeds if she is authenticated as Bob.

Each interaction affects one challenge-response pair. In this context, there is a crucial difference between PUFs and QR-PUFs. Classical states can be measured without introducing disturbances and can be copied perfectly. Therefore for $q \leqslant N$ interactions, we can assume that Eve would know exactly q challenge and outcome states, possibly using this information to create a mathematical clone of the PUF.

Instead, a quantum state cannot be copied. Moreover, a quantum measurement cannot perfectly distinguish the states (since they are nonorthogonal), and any measurement can in principle introduce errors, thus potentially making a passive eavesdrop a detectable action. After q interactions, Eve would know less than q challenge and outcome states. This is the main reason for which QR-PUFs have been introduced: we expect that, concerning unclonability, they can be superior, even far superior, than classical PUFs.[3]

Definition VI.2. Let $\hat{F}$ be a (QR-) PUF with a set of challenges $\mathcal{X}$, where $|\mathcal{X}| = N$. Let us suppose that an adversary Eve has q interactions with a (QR-) PUF in the passive stage of an attack, by observing an authentication protocol between Alice and Bob. With the information she can extract, she prepares a clone $\hat{E}_q$, defined as [see Eq. (10) for a comparison]

$$\hat{E}_q(\cdot) := \hat{R}[\hat{P}_E(\cdot), \hat{G}_H(\hat{P}(\cdot))]\,, \tag{19}$$

and gives it to Alice, who selects a challenge $\mathbf{x_i} \in \mathcal{X}$ and evaluates $\hat{E}_q(\mathbf{x_i})$.

Then $\hat{E}_q$ is a (γ, q)-*(mathematical) clone* of $\hat{F}$ if $\gamma \in [0, 1]$ is the greatest number for which

$$\frac{1}{N}\sum_{i=1}^{N} P[\hat{E}_q(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})] \geqslant \gamma\,. \tag{20}$$

Definition VI.3. A (QR-) PUF $\hat{F}$ is called (γ, q)-*(mathematical) clonable* if $\gamma \in [0, 1]$ is the smallest number for which it is not possible to generate a $(\bar{\gamma}, q)$ clone of the (QR-) PUF for any $\bar{\gamma} > \gamma$. Conversely, a (QR-) PUF $\hat{F}$ is denoted as (δ, q)-*(mathematical) unclonable* if it is $(1 - \delta, q)$ clonable.

The unclonability of a (QR-) PUF is therefore related to the average probability of false acceptance. We could expect to find a relation between the number of interactions q and the unclonability; with a higher knowledge of CRP, it could be expected that Eve will be able to build a more and more sophisticated reproduction of the (QR-) PUF. Increasing q increases the know-how for making $(1 - \delta, q)$ clones with a lower δ. Therefore, fixing the maximum number of uses $q = q^*$ we fix the minimum $\delta = \delta^*$. So we ensure that for $q < q^*$, the (QR-) PUF is at least (δ^*, q) unclonable.

Definition VI.4. A (ρ, δ^*, q^*)-*secure* (QR-) PUF $\hat{F}$ is ρ-robust, physically unclonable, and at least (δ^*, q)-mathematically unclonable up to q^* uses.

When manufacturing (QR-) PUFs, several properties, that are typically implementation dependent, are important [15]. We believe that the above theoretical definitions of robustness

[3]As we mentioned in Sec. V A, highly nonorthogonal challenge states require a fuzzy extractor with a low correctable error, undermining the robustness of the QR-PUF. Therefore this feature of QR-PUFs must be used carefully, balancing robustness and unclonability.

and unclonability are, from a theoretical point of view, the main and most general properties involved in a (QR-) PUF. They are directly related to the probabilities of false rejection and false acceptance, hence describing the efficiency and the security of the entity authentication protocol. They also describe all (QR-) PUFs independently from their implementation.

VII. EXAMPLES

Explicit calculation of the robustness and the unclonability for particular (QR-) PUFs strongly depends on its implementation. In this section, we illustrate the analysis for simplified examples, starting from idealized, extreme cases.

(i) Consider a physically unclonable device implementing a true random number generator. An example of that is a QR-PUF based on the shot noise of an integrated circuit. This device is extremely difficult to simulate (Eve has to try a random guess), but also not robust at all (since it will not generate the same number in the enrollment and the verification). For this device, it holds that

$$\begin{aligned}\frac{1}{N}\sum_{i=1}^{N} P\{\hat{F}_V(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})\} &= \frac{1}{N}\,;\\ \frac{1}{N}\sum_{i=1}^{N} P\{\hat{E}_{q^*}(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})\} &= \frac{1}{N}.\end{aligned} \tag{21}$$

Therefore it is a $(1/N, 1-1/N, q^*)$ (QR-) PUF for any q^*.

(ii) Consider a physically unclonable device that outputs a fixed signal ($\vec{0}$ for classical PUFs or $|0\rangle$ for QR-PUFs) for any input. An example is an optical QR-PUF, based on the polarization of light for which a fixed polarizer is used as a shifter: for all outcome states only light waves of a specific polarization would pass though. This device is perfectly robust, but also clonable. It holds that

$$\begin{aligned}\frac{1}{N}\sum_{i=1}^{N} P\{\hat{F}_V(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})\} &= 1\,;\\ \frac{1}{N}\sum_{i=1}^{N} P\{\hat{E}_{q^*}(\mathbf{x_i}) = \hat{F}_E(\mathbf{x_i})\} &= 1.\end{aligned} \tag{22}$$

Therefore the (QR-) PUF is a $(1, 0, q^*)$ (QR-) PUF, for any q^*.

These examples are extreme cases, while all (QR-) PUFs will be somewhere in between. We now focus on an example of QR-PUF to point out some features of QR-PUFs and some open points.

Let $\hat{F}$ be a QR-PUF implemented by a unitary transformation $\hat{\Phi}$, acting on λ qubits, parametrized according to Eq. (12), with $\psi_k = \chi_k = 0$, i.e.,

$$\hat{\Phi} = \bigotimes_{k=1}^{\lambda} \hat{\Phi}_k = \bigotimes_{k=1}^{\lambda} \begin{pmatrix} \cos\omega_k & \sin\omega_k \\ -\sin\omega_k & \cos\omega_k \end{pmatrix}. \tag{23}$$

Consider a scenario in which each challenge state is a separable state of λ qubits, $|x_i\rangle = \bigotimes_{k=1}^{\lambda} |x_{ik}\rangle$, and each qubit is in one of four possible states:

$$|x_{ik}\rangle = \left|x_{ik}^{(\ell)}\right\rangle := \cos\left(\frac{\phi^{(\ell)}}{2}\right)|0\rangle + \sin\left(\frac{\phi^{(\ell)}}{2}\right)|1\rangle, \tag{24}$$

where

$$\begin{aligned}\phi^{(1)} &= \phi, \quad \phi^{(2)} = -\phi,\\ \phi^{(3)} &= \phi - \pi, \quad \phi^{(4)} = \pi - \phi,\end{aligned} \tag{25}$$

for a fixed angle ϕ. Such challenge states can be parametrized by challenge strings of length $n = 2\lambda$; for each qubit, the four possibilities are represented by two bits.

For simplicity of notation, from now on, we drop the indices i and k, e.g., we write $|x^{(\ell)}\rangle := |x_{ik}^{(\ell)}\rangle$. The pairs $\{|x^{(1)}\rangle, |x^{(3)}\rangle\}$ and $\{|x^{(2)}\rangle, |x^{(4)}\rangle\}$ are orthogonal, but the overall set is nonorthogonal.

We assume that the noise can be parametrized as a depolarizing channel, associated to a probability of error $\tilde{p}$ and equal for all qubits. The noisy challenge state reads

$$\begin{aligned}\tilde{\rho}_x &:= (1-\tilde{p})|x\rangle\langle x| + \tilde{p}\,\frac{\hat{I}}{2}\\ &= \left[(1-\tilde{p})\cos^2\left(\frac{\phi^{(\ell)}}{2}\right) + \frac{\tilde{p}}{2}\right]|0\rangle\langle 0|\\ &\quad + \left[(1-\tilde{p})\sin\left(\frac{\phi^{(\ell)}}{2}\right)\cos\left(\frac{\phi^{(\ell)}}{2}\right)\right](|0\rangle\langle 1| + |1\rangle\langle 0|)\\ &\quad + \left[(1-\tilde{p})\sin^2\left(\frac{\phi^{(\ell)}}{2}\right) + \frac{\tilde{p}}{2}\right]|1\rangle\langle 1|.\end{aligned} \tag{26}$$

The shifter needs to map the noiseless outcome state to $|0\rangle\ldots|0\rangle$. According to Eq. (14) it can be chosen to be a λ-fold tensor product of single-qubit gates,

$$\begin{aligned}\hat{\Omega} &= \cos\left(\frac{\phi^{(\ell)}}{2} - \omega\right)|0\rangle\langle 0| + \sin\left(\frac{\phi^{(\ell)}}{2} - \omega\right)|0\rangle\langle 1|\\ &\quad + \sin\left(\frac{\phi^{(\ell)}}{2} - \omega\right)|1\rangle\langle 0| - \cos\left(\frac{\phi^{(\ell)}}{2} - \omega\right)|1\rangle\langle 1|,\end{aligned} \tag{27}$$

and it follows that

$$\tilde{\rho}_o := \hat{\Omega}\,\tilde{\rho}_y\,\hat{\Omega}^\dagger = \left(1 - \frac{\tilde{p}}{2}\right)|0\rangle\langle 0| + \left(\frac{\tilde{p}}{2}\right)|1\rangle\langle 1|. \tag{28}$$

For a single qubit, therefore, the probability of measuring $|1\rangle$ is $\tilde{p}/2$. For a challenge state of λ qubits, the average Hamming weight of the string $\mathbf{o_i}$ is $\lambda\,\tilde{p}/2$.

Any fuzzy extractor is defined in terms of the maximum number of errors t it can correct. With our error model, we can choose to correct the average error of the system, i.e., $t = \lceil \lambda\,\tilde{p}/2 \rceil$, where $\lceil \lambda\,\tilde{p}/2 \rceil$ is the least integer greater than or equal to $\lambda\,\tilde{p}/2$. However, t and the number N of challenge-response pairs are related since the fuzzy extractor has to uniquely map a given outcome into a unique response, without collisions.

Consider $|x^{(\ell)}\rangle$ and $|x^{(\ell')}\rangle$ ($\ell, \ell' \in \{1,2,3,4\}$ and $\ell \neq \ell'$) and estimate the error if $|x^{(\ell)}\rangle$ is implemented as the state

TABLE I. Error induced by implementing the wrong challenge state. The entry in row ℓ and column ℓ' of the table is the probability of error when applying shifter ℓ to state ℓ'. The parameter ϕ is defined in Eq. (25).

	$\lvert x^{(1)}\rangle$	$\lvert x^{(2)}\rangle$	$\lvert x^{(3)}\rangle$	$\lvert x^{(4)}\rangle$
$\lvert x^{(1)}\rangle$	0	$\sin^2\phi$	1	$\cos^2\phi$
$\lvert x^{(2)}\rangle$	$\sin^2\phi$	0	$\cos^2\phi$	1
$\lvert x^{(3)}\rangle$	1	$\cos^2\phi$	0	$\sin^2\phi$
$\lvert x^{(4)}\rangle$	$\cos^2\phi$	1	$\sin^2\phi$	0

$|x^{(\ell')}\rangle$, by evaluating $\hat{\Omega}_\ell\,\hat{\Phi}|x^{(\ell')}\rangle$. From

$$|x^{(\ell)}\rangle = \cos\left(\frac{\phi^{(\ell)}}{2}\right)|0\rangle + \sin\left(\frac{\phi^{(\ell)}}{2}\right)|1\rangle,$$
$$|x^{(\ell')}\rangle = \cos\left(\frac{\phi^{(\ell')}}{2}\right)|0\rangle + \sin\left(\frac{\phi^{(\ell')}}{2}\right)|1\rangle, \tag{29}$$

it follows that

$$\hat{\Omega}_\ell\,\hat{\Phi}|x^{(\ell')}\rangle = \cos\left(\frac{\phi^{(\ell)}-\phi^{(\ell')}}{2}\right)|0\rangle + \sin\left(\frac{\phi^{(\ell)}-\phi^{(\ell')}}{2}\right)|1\rangle. \tag{30}$$

Therefore, for this case the probability of measuring $|1\rangle$ is $\sin^2[(\phi^{(\ell)}-\phi^{(\ell')})/2]$.

In Table I, the explicit values for all the combinations of the four-qubit states are listed. In case of wrong implementation, challenges with a large overlap lead to small error weights, while orthogonal challenges lead to big ones. Thus there is a tradeoff between the robustness of the QR-PUF and the quantum advantage of using indistinguishable nonorthogonal states. For any pair of possible challenge states $|x_i\rangle = \bigotimes_{k=1}^{\lambda}|x_{ik}\rangle$ and $|x_j\rangle = \bigotimes_{k=1}^{\lambda}|x_{jk}\rangle$, the average Hamming weight of the error string $\mathbf{o_i}$, obtained by the aforementioned process, is

$$\mathrm{err}_{i,j} := (n_{12}+n_{34})\sin^2\phi + (n_{13}+n_{24}) + (n_{14}+n_{23})\cos^2\phi, \tag{31}$$

where n_{ab} counts how many times $|x_{ik}\rangle = |x^{(\ell)}\rangle$ when $|x_{jk}\rangle = |x^{(\ell')}\rangle$ (or vice versa).

If $\mathrm{err}_{i,j} < \lceil\lambda\,\tilde{p}/2\rceil$, then the certifier should discard one of the two challenges, either $\mathbf{x_i}$ or $\mathbf{x_j}$, thus reducing the number N of possible challenge-response pairs. After this selection is repeated for all pairs of challenges, the certifier studies the entropy of the set of shifters, determining the strings $\mathbf{w_i}$ and the outcomes $\mathbf{y_i} = \mathbf{w_i} \,\|\, \mathbf{o_i}$.

The *Canetti's reusable fuzzy extractor* [41] is able to correct up to $t = (l \ln l/m)$ bits, where l is the length of the outcomes and m the length of the responses. As $l = \lambda + l_w$ is fixed, m has to be adapted to the noise level $\lceil\lambda\,\tilde{p}/2\rceil$. The correctness property of this fuzzy extractor guarantees that an error smaller than t is corrected with probability $1-\tilde{\varrho}$, where

$$\tilde{\varrho} = \left[1-\left(1-\frac{t}{l}\right)^m\right]^{\xi_1} + \xi_1\xi_2, \tag{32}$$

with ξ_1 and ξ_2 being computational parameters of the fuzzy extractor (in [41], to which we refer for a precise explanation, they are called ℓ and γ, respectively). Then the robustness of this QR-PUF is $1-\tilde{\varrho}$.

Concerning the unclonability, one should relate the amount of information Eve obtains from the (possibly correlated) challenge-response pairs to her ability to create a mathematical clone of the QR-PUF. Unfortunately, there is no general method known to provide this relation. We expect that, for some QR-PUFs, quantum unitary gate discrimination methods [42] could be used, but this line of research goes beyond the purposes of our work. Here, we can show that QR-PUFs prevent Eve to gain too much information about challenges and responses, thus strongly hindering her ability to learn the challenge-response table.

As the optimal global attack on the challenge states is unknown, unless knowing all challenge states, here we consider an attack that acts individually on qubits. In particular, we consider the case for which, on each qubit, Eve can apply a $1\to 2$ cloning operator, i.e., she can intercept each qubit of a challenge state during an authentication round to produce two (imperfect) copies, one of which is given back to the legitimate parties and the other is kept for herself.

For such a set of states, the optimal cloning transformation, i.e., the transformation who keeps the highest possible fidelity between the copies and the original states, has been derived [43] and for any challenge state $|x_i\rangle$ and its optimal copy ρ_i^E holds:

$$F\left(|x_i\rangle\langle x_i|, \varrho_i^E\right) := \prod_{k=1}^{\lambda}\langle x_{ik}\,|\,\varrho_{ik}^E\,|\,x_{ik}\rangle = \left[\frac{1}{2}\left(1+\sqrt{\sin^4\phi+\cos^4\phi}\right)\right]^{\lambda}. \tag{33}$$

For fixed λ, the minimum value of the fidelity is reached for $\phi = \pi/4$, for which, considering a single qubit, $F = (0.85)$. Already for 10 qubits the fidelity drops to $F = (0.20)$, and for 20 qubits, $F = (0.04)$.

Thus, Eve is not able to successfully simulate the challenge-response behavior, as she cannot even reconstruct the challenge and outcome states. Moreover, as the fidelity is preserved by unitary matrices, this result holds also for the expected outcome state $|y_i\rangle$ and the actual outcome state Alice obtains after challenging the QR-PUF with her (unwittingly altered by the cloning process) challenge state. The noise is too high to be corrected by the fuzzy extractor, thus aborting the authentication protocol and exposing the presence of an intruder.

For classical PUFs, instead, Eve could perfectly read the challenge and outcome states, without being noticed. This provides an advantage of QR-PUFs compared to classical PUFs in terms of unclonability. However, we also noticed that a high nonorthogonality of the challenges can, in principle, undermine the robustness. The tradeoff between the advantages and disadvantages of QR-PUFs (see Table II) has to be studied in order to find secure applications of them.

TABLE II. Advantages and disadvantages of QR-PUFs compared to classical PUFs.

Advantages of QR-PUFs	Disadvantages of QR-PUFs
An adversary cannot copy or distinguish nonorthogonal states.	Highly nonorthogonal states reduce the robustness.
Adversarial measurements on the states introduce detectable disturbances.	Quantum states are more fragile than classical states.

VIII. CONCLUSION

In this article we proposed a theoretical framework for the quantitative characterization of both PUFs and QR-PUFs. After developing an authentication protocol common to both typologies, with the same error correction and privacy amplification scheme, we formalized the (QR-) PUFs in term of two main properties, the *robustness* (connected to false rejection) and the *unclonability* (connected to false acceptance). Finally, we studied some examples, motivating the possible advantages and disadvantages of QR-PUFs compared to classical PUFs.

Our framework is useful to study and to compare different implementations of (QR-) PUFs and to develop new authentication schemes. An important application would be to strictly prove the superiority of QR-PUFs over classical PUFs. The next step towards that goal would be the development of new methods to estimate the unclonability of (QR-) PUFs for different implementations. This could open an interesting line of theoretical and experimental research about (QR-) PUFs. Furthermore, our framework can be employed to determine the level of security of using (QR-) PUFs in other cryptographic protocols, like QKD, where a quantitatively secure (QR-) PUF can be used as authentication and reduces the number of necessary preshared key bits.

Note added. Recently we became aware of a preprint on a related topic [44].

ACKNOWLEDGMENTS

The authors thank U. Rührmair for helpful discussions. This project has received funding from the German Federal Ministry of Education and Research (BMBF) within the Hardware-Based Quantum Security (HQS) project.

[1] K. M. Martin, *Everyday Cryptography: Fundamental Principles and Applications* (Oxford University Press, Oxford, England, 2012).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, J. Comput. Syst. Sci. **22**, 265 (1981).

[4] R. Pappu, Physical one-way functions, Ph.D. thesis, Massachusetts Institute of Technology, 2001.

[5] U. Rührmair, Oblivious transfer based on physical unclonable functions, in *International Conference on Trust and Trustworthy Computing* (Springer, New York, 2010), pp. 430–440.

[6] U. Rührmair and M. van Dijk, On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols, J. Cryptogr. Eng. **3**, 17 (2013).

[7] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, Physically uncloneable functions in the universal composition framework, in *Annual Cryptology Conference* (Springer, New York, 2011), pp. 51–70.

[8] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical one-way functions, Science **297**, 2026 (2002).

[9] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, A technique to build a secret key in integrated circuits for identification and authentication applications, in *2004 Symposium on VLSI Circuits, Digest of Technical Papers (IEEE Cat. No. 04CH37525)* (IEEE, New York, 2004), pp. 176–179.

[10] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, FPGA intrinsic PUFs and their use for IP protection, in *International Workshop on Cryptographic Hardware and Embedded Systems* (Springer, New York, 2007), pp. 63–80.

[11] P. Tuyls, G.-J. Schrijen, B. Škorić, J. Van Geloven, N. Verhaegh, and R. Wolters, Read-proof hardware from protective coatings, in *International Workshop on Cryptographic Hardware and Embedded Systems* (Springer, New York, 2006), pp. 369–383.

[12] R. S. Indeck and M. W. Muller, Method and apparatus for fingerprinting magnetic media. US Patent 5,365,586 (1994).

[13] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon, IEEE Trans. Emerg. Topics Comput. **2**, 30 (2013).

[14] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, A PUF taxonomy, Appl. Phys. Rev. **6**, 011303 (2019).

[15] R. Maes and I. Verbauwhede, Physically unclonable functions: A study on the state of the art and future research directions, in *Towards Hardware-Intrinsic Security* (Springer, New York, 2010), pp. 3–37.

[16] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, Helper data algorithms for PUF-based key generation: Overview and analysis, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. **34**, 889 (2014).

[17] S. Puchinger, S. Müelich, M. Bossert, M. Hiller, and G. Sigl, On error correction for physical unclonable functions, in *SCC 2015, 10th International ITG Conference on Systems, Communications and Coding* (VDE, German Society for Biomedical Engineering, 2015), pp. 1–6.

[18] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, SIAM J. Comput. **38**, 97 (2008).

[19] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, Cloning physically unclonable functions, in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (IEEE, New York, 2013), pp. 1–6.

[20] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, Modeling attacks on physical unclonable functions, in *Proceedings of the 17th ACM Conference on Computer and Communications Security* (Association for Computing Machinery, New York, 2010), pp. 237–249.

[21] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, PUF modeling attacks on simulated and silicon data, IEEE Trans. Inf. Forensics Secur. **8**, 1876 (2013).

[22] B. Škorić, Quantum readout of physical unclonable functions, Int. J. Quantum Inf. **10**, 1250001 (2012).

[23] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[24] U. Rührmair, J. Sölter, and F. Sehnke, On the foundations of physical unclonable functions, IACR Cryptology ePrint Archive **2009**, 277 (2009).

[25] F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, and C. Wachsmann, A formalization of the security features of physical functions, in *2011 IEEE Symposium on Security and Privacy* (IEEE, New York, 2011), pp. 397–412.

[26] R. Plaga and F. Koob, A formal definition and a new security mechanism of physical unclonable functions, in *International GI/ITG Conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance* (Springer, New York, 2012), pp. 288–301.

[27] R. Plaga and D. Merli, A new definition and classification of physical unclonable functions, in *Proceedings of the Second Workshop on Cryptography and Security in Computing Systems* (Association for Computing Machinery, New York, 2015), p. 7.

[28] J. Delvaux, Security analysis of PUF-based key generation and entity authentication, Ph.D. thesis, Katholieke Universiteit Leuven, Belgium, 2017.

[29] B. Škorić, P. Tuyls, and W. Ophey, Robust key extraction from physical uncloneable functions, in *International Conference on Applied Cryptography and Network Security* (Springer, New York, 2005), pp. 407–422.

[30] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. Pinkse, Quantum-secure authentication of a physical unclonable key, Optica **1**, 421 (2014).

[31] P. Tuyls, B. Škorić, S. Stallinga, A. H. Akkermans, and W. Ophey, Information-theoretic security analysis of physical uncloneable functions, in *International Conference on Financial Cryptography and Data Security* (Springer, New York, 2005), pp. 141–155.

[32] O. Rioul, P. Solé, S. Guilley, and J.-L. Danger, On the entropy of physically unclonable functions, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, New York, 2016), pp. 2928–2932.

[33] B. Škorić, A. P. Mosk, and P. W. Pinkse, Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks, Int. J. Quantum Inf. **11**, 1350041 (2013).

[34] B. Škoric, Security analysis of quantum-readout PUFs in the case of challenge-estimation attacks, Quantum Inf. Comput. **16**, 50 (2016).

[35] Y. Yao, M. Gao, M. Li, and J. Zhang, Quantum cloning attacks against PUF-based quantum authentication systems, Quantum Inf. Process. **15**, 3311 (2016).

[36] G. M. Nikolopoulos and E. Diamanti, Continuous-variable quantum authentication of physical unclonable keys, Sci. Rep. **7**, 46047 (2017).

[37] G. M. Nikolopoulos, Continuous-variable quantum authentication of physical unclonable keys: Security against an emulation attack, Phys. Rev. A **97**, 012324 (2018).

[38] K. Zyczkowski and M. Kus, Random unitary matrices, J. Phys. A: Math. Gen. **27**, 4235 (1994).

[39] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum State Tomography Via Compressed Sensing, Phys. Rev. Lett. **105**, 150401 (2010).

[40] U. Rührmair, H. Busch, and S. Katzenbeisser, Strong PUFs: Models, constructions, and security proofs, in *Towards Hardware-Intrinsic Security* (Springer, New York, 2010), pp. 79–96.

[41] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, Reusable fuzzy extractors for low-entropy distributions, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 2016), pp. 117–146.

[42] C. W. Helstrom, Quantum detection and estimation theory, J. Stat. Phys. **1**, 231 (1969).

[43] D. Bruß and C. Macchiavello, Optimal cloning for two pairs of orthogonal states, J. Phys. A: Math. Gen. **34**, 6815 (2001).

[44] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, Quantum physical unclonable functions: Possibilities and impossibilities, arXiv:1910.02126v1.

B

Detecting entanglement of unknown continuous variable states with random measurements

Title:	Detecting entanglement of unknown continuous variable states with random measurements,
Authors:	Tatiana Mihaescu, Hermann Kampermann, Giulio Gianfelici, Aurelian Isar and Dagmar Bruß
Journal:	New Journal of Physics
Impact factor:	3.729 (2020)
Date of submission:	1 July 2020
Publication status:	Published
Contribution by GG:	Third author (input approx. 7%)

This publication corresponds to the reference [Mih+20]. A summary of the results is presented in Chap. 6. The research objectives were identified by my coauthors before I was involved in the project. I regularly discussed the article with my coauthors, in particular TM. I helped to physically motivate the results related to the detection of entanglement in two-mode squeezed vacuum states. Furthermore, I assisted TM in developing the statistical analysis presented in Sec. 6 of the article. Finally, I helped to proofread and improve the entire manuscript.

PAPER • OPEN ACCESS

Detecting entanglement of unknown continuous variable states with random measurements

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
1 July 2020

REVISED
24 November 2020

ACCEPTED FOR PUBLICATION
8 December 2020

PUBLISHED
23 December 2020

PAPER

Detecting entanglement of unknown continuous variable states with random measurements

Tatiana Mihaescu[1,2,*], Hermann Kampermann[1], Giulio Gianfelici[1], Aurelian Isar[2,3] and Dagmar Bruß[1]

[1] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany
[2] Department of Theoretical Physics, National Institute of Physics and Nuclear Engineering, RO-077125 Bucharest-Magurele, Romania
[3] Faculty of Physics, University of Bucharest, RO-077125 Bucharest-Magurele, Romania
[*] Author to whom any correspondence should be addressed.

E-mail: mihaescu.tatiana@theory.nipne.ro

Keywords: quantum entanglement, continuous variable systems, entanglement witnesses, covariance matrices

Abstract

We develop a scheme for the detection of entanglement in any continuous variable system, by constructing an optimal entanglement witness from random homodyne measurements. To this end, we introduce a set of linear constraints that guarantee the necessary properties of a witness and allow for its optimisation via a semidefinite program. We test our method on the class of squeezed vacuum states and study the efficiency of entanglement detection in general unknown covariance matrices. The results show that we can detect entanglement, including bound entanglement, in arbitrary continuous variable states with fewer measurements than in full tomography. The statistical analysis of our method shows a good robustness to statistical errors in experiments.

1. Introduction

The most valuable characteristics of quantum systems are quantum correlations such as entanglement, which represents a useful resource for applications unattainable in the framework of classical theory, such as quantum teleportation, quantum cryptography and dense coding [1, 2]. In the last two decades, the use of continuous variable (CV) systems became a very powerful approach to quantum information processing and communication [3–5], opening the way to various protocols and tasks, like quantum cryptography [6], quantum teleportation [7], quantum dense coding [8]. CV quantum systems provide the quantum description of the propagating electromagnetic field, and therefore manifest particular relevance for quantum communication and quantum techniques like detection, imaging and sensing [9].

A significant problem in quantum information theory and any application is to efficiently reveal the properties of an unknown quantum state, in particular to certify the presence of entanglement in a given unknown state. Usual entanglement criteria for CV systems consist in certain operations on the second moments, or uncertainties, of quantum states, such as the positive partial transpose (PPT) criterion [10, 11]. Therefore, first a full tomography is required for completely unknown states, in order to reconstruct the entire covariance matrix (CM). However, this method may be a very resource-consuming and demanding experimental procedure, especially for quantum states with a high number of modes. In addition, the full information about the second moments of the state can be excessive for the characterisation of entanglement present in the state. Instead, one can choose to measure certain fixed combinations of second moments, giving rise to a specific test, which detects entanglement in some states and does not detect it in others [12–14].

Entanglement witnesses (EWs) represent another commonly used entanglement test, being directly accessible in experiments through measurable observables [15]. A Hermitian observable W is an EW if for all separable states ρ_s, $\mathrm{Tr}[W\rho_s] \geqslant 0$ holds, while for some entangled state ρ we have that $\mathrm{Tr}[W\rho] < 0$ [15]. For CV systems a special instance of EWs can be defined, which embodies the entanglement criterion in

terms of the variances of the canonical observables of the state [16–19]. This is possible because all the relevant information on the quantum entanglement of a CV system is encoded in its CM, specifically in its symplectic spectrum [20]. Typically, EWs are employed when certain knowledge about the state is available.

Given an unknown quantum state, however, the complexity of the state and the absence of any information about it deprive us of a specific experimental strategy in tackling the problem of efficient entanglement detection. Therefore, the best strategy in this case would be to perform random measurements, serving as building blocks for the construction of an EW by means of a semidefinite optimization algorithm. In this context, one has the opportunity to represent the performance of entanglement detection in terms of the number of measurements required for this task.

We introduce new linear constraints for EWs and use them to build a semidefinite program (SDP). Our method based on EWs is applicable to arbitrary unknown CV states, and can be easily adjusted to detect any type of entanglement encoded in the second moments, including bound entanglement. Important is that we find a high probability of success in detecting entanglement with fewer measurements than in a tomographically complete set. Our method presents a clear advantage over entanglement criteria subjected to specific measurement directions on the CM, or to full information about the CM [11, 12]. As this is of high interest for experimental applications, we also provide a statistical analysis showing the robustness of this method to statistical errors. This idea is inspired by an analogous method for the discrete-variable case, which was developed in [21].

The paper is organized as follows. In section 2 we present the theoretical framework of CV states, mainly based on the second moments description of the state. In section 3 we introduce the EWs based on the CM of the state, as presented in references [16, 17], and propose a set of stronger linear semidefinite constraints in order to characterize the EWs. Then, we simulate random homodyne measurements for two-mode CMs in section 4 and formulate a SDP optimizing the witness constructible from given experimental data. We present the results of the efficiency of entanglement detection for random two-mode CMs and, in particular, for the class of squeezed vacuum states in section 5, and illustrate an example of bipartite bound EW. A statistical analysis of our method is provided in section 6, and a summary and conclusions are presented in section 7.

2. Continuous variable systems

A CV system of N canonical bosonic modes, like the quantized electromagnetic field with a Hamiltonian of a system of N harmonic oscillators (modes), is defined in a Hilbert space $\mathcal{H} = \bigoplus_{k=1}^{N} \mathcal{H}_k$, each one with an infinite-dimensional space $\mathcal{H}_k = L^2(\mathbb{R})$ and two canonical observables $\hat{x}_k$ and $\hat{p}_k$, with the corresponding phase space variables of position x_k and momentum p_k [3–5]. One can define a vector of quadrature operators $\hat{R}^{\mathrm{T}} \equiv (\hat{R}_1, \ldots, \hat{R}_{2N}) = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_N, \hat{p}_N)$ satisfying the bosonic commutation relations

$$[\hat{R}_i, \hat{R}_j] = \mathrm{i}\Omega_{ij}\hat{\mathrm{I}}, \quad i,j = 1, \ldots, 2N, \tag{1}$$

where $\hat{\mathrm{I}}$ is the identity matrix, and Ω_{ij} are the elements of the fundamental symplectic matrix (we assume $\hbar = 1$)

$$\Omega_N = \bigoplus_{1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2}$$

The primary role in this study is played by the statistical moments of the quadrature operators, that characterize the state with density operator ρ [3, 4], up to the second order: the displacement vector, which is the real vector d of first order moments $d_i = \langle \hat{R}_i \rangle_\rho = \mathrm{Tr}[\hat{R}_i \rho]$, and the CM, which is the real, symmetric matrix γ whose entries are the second order moments in symmetrized form (the variances) of the quadrature operators, defined as [5, 22]:

$$\gamma_{ij} = \langle \{\hat{R}_i - \langle \hat{R}_i \rangle, \hat{R}_j - \langle \hat{R}_j \rangle\}_+ \rangle_\rho, \tag{3}$$

where $\{,\}_+$ represents the anticommutator. The Robertson–Schrödinger uncertainty relation in terms of the CM reads

$$\gamma + \mathrm{i}\Omega_N \geqslant 0, \tag{4}$$

assuring that it is a CM of a physical quantum state. Gaussian states represent the class of CV states which are completely characterized by their first and second moments. The entanglement criteria discussed in this paper can also detect entanglement of non-Gaussian states.

A quantum state of a bipartite system is entangled if it cannot be prepared by means of operations acting locally on the subsystems. In the case of separable states correlations are attributed to possible

classical communication between subsystems, and hence are of classical origin. This reasoning carries over to CV systems, where a separability criterion can be defined in terms of CMs. If a CM γ of a state of N modes is fully separable, then there exist CMs γ_i, $i = 1, \ldots, N$, corresponding to N subsystems, such that [23]

$$\gamma \geqslant \bigoplus_{i=1}^{N} \gamma_i. \tag{5}$$

Conversely, if this holds, then Gaussian states with CM γ are separable. Therefore, if this criterion is violated, then the corresponding state is entangled, irrespective of whether it is Gaussian or not. If it is not violated, then a Gaussian state is separable, while a non-Gaussian state might be entangled.

In the following, we will refer to the situation of a k-partition of an N-mode system as the splitting or distribution of an N-mode system into k subsystems, where every subsystem j ($j = 1, \ldots, k$) is composed of N_j modes, such that $\sum_{j=1}^{k} N_j = N$.

2.1. Symplectic transformations

Unitary operators acting on the quantum state space are equivalent to symplectic transformations which preserve the commutation relations of canonical variables. The real symplectic group is defined by [24]:

$$Sp(2N, \mathbb{R}) = \{S \in \mathcal{M}(2N, \mathbb{R}) : S\Omega_N S^{\mathrm{T}} = \Omega_N\}, \tag{6}$$

where S is a symplectic transformation acting in phase space as $\hat{R} \to \hat{R}' = S\hat{R}$, and $\mathcal{M}(2N, \mathbb{R})$ denotes the set of $2N \times 2N$ real matrices. Symplectic transformations act by congruence on CMs: $\gamma' = S\gamma S^{\mathrm{T}}$.

Every symplectic transformation can be decomposed using the Euler decomposition, which represents the singular value decomposition for real symplectic matrices [24]:

$$S = K \left[\bigoplus_{i=1}^{N} S(r_i)\right] L, \tag{7}$$

where K, L are symplectic and orthogonal matrices, while

$$S(r_i) = \begin{pmatrix} \mathrm{e}^{-r_i} & 0 \\ 0 & \mathrm{e}^{r_i} \end{pmatrix} \tag{8}$$

are one-mode squeezing matrices (symplectic and nonorthogonal) with r_i the squeezing parameter. The symplectic and orthogonal matrices form the maximal compact subgroup $K(N)$ within the noncompact group $Sp(2N, \mathbb{R})$ [24]. The group $K(N)$ is isomorphic to the group $U(N)$ of $N \times N$ complex unitary matrices:

$$K(N) = \{S(X, Y) | X - \mathrm{i}Y \in U(N)\}, \tag{9}$$

where the corresponding symplectic matrices are of the following form:

$$S(X, Y) = \begin{pmatrix} X & Y \\ -Y & X \end{pmatrix} \in Sp(2N, \mathbb{R}). \tag{10}$$

Such transformations describe multiport interferometers and are called passive canonical unitaries, which preserve the photon number [4]. The active canonical unitaries correspond to nonorthogonal symplectic transformations, such as one-mode squeezers.

In the following we will use the theorem by Williamson [20], according to which every matrix $M \in \mathcal{M}(2N, \mathbb{R})$, $M \geqslant 0$ can be brought to a diagonal form through symplectic transformations:

$$SMS^{\mathrm{T}} = \mathrm{diag}(s_1, s_1, \ldots, s_N, s_N), \tag{11}$$

where $s_1, \ldots, s_N \geqslant 0$ are called symplectic eigenvalues of M. By

$$\mathrm{str}[M] := \sum_{i=1}^{N} s_i \tag{12}$$

we will denote the symplectic trace of M.

3. Entanglement witnesses for covariance matrices

An EW based on CMs is characterised by a real symmetric matrix $Z \geqslant 0$ such that [17]

$$\mathrm{Tr}[Z\gamma_{\mathrm{s}}] \geqslant 1, \quad \text{for all separable CMs} \quad \gamma_{\mathrm{s}}, \tag{13a}$$

$$\mathrm{Tr}[Z\gamma] < 1, \quad \text{for some entangled CM} \quad \gamma. \tag{13b}$$

The EWs based on second moments defined in equations (13a) and (13b) represent hyperplanes in the space of CMs that separate some entangled states from the set of separable CMs. If there exists Z which fulfills conditions (13b), then the state with CM γ is entangled, irrespective of whether it is Gaussian or not, while if this test does not detect entanglement in a given non-Gaussian state, then the result is inconclusive. The following theorem fully characterises the EWs for multimode CV states defined in equations (13a) and (13b) for different entanglement classes.

Theorem . *(Taken from [16, 17]) A CM γ of a k-partite system with $\sum_{j=1}^{k} N_j = N$ modes is entangled with respect to this partition iff there exists Z such that*

$$\mathrm{Tr}[Z\gamma] < 1, \tag{14}$$

where Z is a real, symmetric $2N \times 2N$ matrix satisfying

$$Z \geqslant 0, \quad \sum_{j=1}^{k} \mathrm{str}[Z_j] \geqslant \frac{1}{2}, \tag{15}$$

where Z_j is the block matrix on the diagonal of Z acting on the subsystem j. Matrices Z are called EWs based on second moments.

Due to the convexity of the set of separable CMs there always exists an EW Z giving the result of equation (14) for an entangled CM γ. In reference [17] the authors formulated the above theorem in a slightly different way: in addition to equation (15) it is stated that such an EW has to satisfy also $\mathrm{str}[Z] < \frac{1}{2}$, instead of condition $\mathrm{Tr}[Z\gamma] < 1$. Note that there is no contradiction between the conditions (15) and $\mathrm{str}[Z] < \frac{1}{2}$ that an EW has to satisfy, since the relation $\mathrm{str}[Z] \leqslant \sum_{i=1}^{N} \mathrm{str}[Z_i]$ holds [16].

Nevertheless, the two formulations of the theorem above are equivalent. In order to show this we will use the results from reference [16] where it is proven that $\mathrm{Tr}[Z\gamma] \geqslant 1$ for all separable CMs γ if and only if $Z \geqslant 0$ and $\sum_{j=1}^{k} \mathrm{str}[Z_j] \geqslant \frac{1}{2}$. In addition, it is shown that $\mathrm{Tr}[Z\gamma] \geqslant 1$ for all CMs γ if and only if $Z \geqslant 0$ and $\mathrm{str}[Z] \geqslant \frac{1}{2}$. As $Z \ngeqslant 0$ would contradict $\mathrm{Tr}[Z\gamma] \geqslant 1$ for all separable CMs γ, it follows that if $\mathrm{Tr}[Z\gamma] < 1$ for some CM γ then $\mathrm{str}[Z] < \frac{1}{2}$. Conversely, if $\mathrm{str}[Z] < \frac{1}{2}$ then there exists some CM γ such that $\mathrm{Tr}[Z\gamma] < 1$.

The problem of finding an EW that most robustly detects entanglement in a given CM arises as a SDP (see reference [17] where the authors provide also numerical routines performing this task). Here we consider the situation when no information about the state is available, and we aim at constructing the EWs from given random measurements. For this purpose, the description of EWs given in the theorem above can serve as constraints in our optimization program.

However, the inequality (15) cannot be used in this form as a semidefinite constraint in an SDP, because its left-hand side cannot be regarded as a linear function since the symplectic eigenvalues of a matrix $M \geqslant 0$ are given by the eigenvalues of the matrix $M^{\frac{1}{2}}(\mathrm{i}\Omega_N)M^{\frac{1}{2}}$ [5]. In the following, we propose a set of linear semidefinite constraints for EWs, which are stronger than conditions (15).

Proposition . *For the EW Z of a k-partite entangled N-mode CM with $\sum_{j=1}^{k} N_j = N$, the inequalities (15) are satisfied if the following conditions are fulfilled:*

$$\begin{aligned} &Z \geqslant 0, \\ &Z_j + \mathrm{i}\frac{x_j}{N_j}\Omega_{N_j} \geqslant 0, \quad x_j \in \mathbb{R}, \quad j = 1, \ldots, k-1, \\ &Z_k + \mathrm{i}\frac{1}{N_k}\left(\frac{1}{2} - \sum_{j=1}^{k-1} x_j\right)\Omega_{N_k} \geqslant 0. \end{aligned} \tag{16}$$

Proof

(a) In the first part we prove the proposition for $k = N$. First, we prove this for $N = 2$, i.e. for a two-mode witness with the following block form:

$$Z = \begin{pmatrix} Z_1 & Z_c \\ Z_c^{\mathrm{T}} & Z_2 \end{pmatrix}, \tag{17}$$

where Z_1, Z_2 and Z_c are 2×2 matrices. Since Z is a positive semidefinite matrix, also the principal submatrices Z_1 and Z_2 are positive semidefinite. Let us assume the following inequality:

$$Z_1 + \mathrm{i}x\Omega_1 \geqslant 0, \quad \text{where} \quad \Omega_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad x \in \mathbb{R}. \tag{18}$$

By symplectic transformation S the positive matrix above can be brought to the Williamson normal form as follows[4]:

$$S(Z_1 + \mathrm{i}x\Omega_1)S^{\mathrm{T}} = Z_1^w + \mathrm{i}x\Omega_1 = \begin{pmatrix} z_1 & x\mathrm{i} \\ -x\mathrm{i} & z_1 \end{pmatrix}, \tag{19}$$

where $Z_1^w = \mathrm{diag}(z_1, z_1)$, with z_1 the positive symplectic eigenvalue of Z_1. The eigenvalues α of matrix (19) are determined from the equation:

$$(z_1 - \alpha)^2 - x^2 = (z_1 - \alpha - x)(z_1 - \alpha + x) = 0, \tag{20}$$

and hence

$$z_1 \pm x = \alpha \geqslant 0. \tag{21}$$

Thus, the symplectic eigenvalue z_1 fulfills the inequality $z_1 \geqslant \pm x$, or $z_1 \geqslant |x|$. A similar inequality can be formulated for the block matrix Z_2:

$$Z_2 + \mathrm{i}(\frac{1}{2} - x)\Omega_1 \geqslant 0, \tag{22}$$

from which we obtain the following condition for the symplectic eigenvalue z_2:

$$z_2 \geqslant \left| \frac{1}{2} - x \right|. \tag{23}$$

Now, the sum of symplectic eigenvalues gives:

$$z_1 + z_2 \geqslant |x| + \left| \frac{1}{2} - x \right| \geqslant \left| x + \frac{1}{2} - x \right| = \frac{1}{2}. \tag{24}$$

The above inequality assures that the condition (15) is always fulfilled. The generalization to more modes is straightforward. For instance, consider a three-mode CM and we want an EW detecting three-partite entanglement. Then, according to the proposition, we need to impose constraints on the three block diagonal matrices of the witness, which amount to the following inequalities for the corresponding symplectic eigenvalues:

$$\begin{aligned} z_1 &\geqslant |x_1|, \quad x_1 \in \mathbb{R}, \\ z_2 &\geqslant |x_2|, \quad x_2 \in \mathbb{R}, \\ z_3 &\geqslant \left| \frac{1}{2} - x_1 - x_2 \right|. \end{aligned} \tag{25}$$

These inequalities imply the constraint (15).

(b) In the second part, we present the generalization of the proof for k-partite entanglement of N-mode CMs, with $k < N$. Consider, for simplicity, a three-mode state and the bipartition between the first and the other two modes. The witness Z is a 6×6 matrix where Z_1 is the 2×2 block diagonal matrix of Z acting on the first mode, and we denote by Z' the 4×4 block matrix acting on the other two modes. Then the corresponding constraints on the witness are:

$$\begin{aligned} Z &\geqslant 0, \\ Z_1 + \mathrm{i}x\Omega_1 &\geqslant 0, \quad x \in \mathbb{R}, \\ Z' + \mathrm{i}\frac{1}{2}\left(\frac{1}{2} - x\right)\Omega_2 &\geqslant 0. \end{aligned} \tag{26}$$

If we denote by z_1 the symplectic eigenvalue of Z_1, and by z_1', z_2' the two symplectic eigenvalues of Z', then the conditions above are equivalent to:

$$z_1 \geqslant |x|, \quad x \in \mathbb{R},$$

[4] Any symplectic transformation preserves the symplectic eigenvalues, and since we know that $\mathrm{Tr}[M] \geqslant 2\,\mathrm{str}[M]$ holds for any positive matrix M [25], then we may say that symplectic transformations preserve also the positivity.

$$z_1' \geqslant \frac{1}{2}\left|\frac{1}{2} - x\right|,$$
$$z_2' \geqslant \frac{1}{2}\left|\frac{1}{2} - x\right|, \tag{27}$$

which satisfy the condition (15). Since this is a bipartite state, the lower bounds for the three symplectic eigenvalues depend on a single parameter x, while, according to the proposition, the detection of three-partite entanglement in a three-mode state would require two optimization parameters, x_1 and x_2 (see equation (25)). The generalization of the proof to N modes and k parties is straightforward. Note that the conditions in the proposition are stronger for k-partite entanglement (with $k < N$) than for genuine multipartite entanglement (i.e. $k = N$), where the optimization for every symplectic eigenvalue is done independently.

□

While the semidefinite inequalities proposed in the previous proposition present the advantage of being linear, the drawback of these constraints is that they are stronger than those required by the theorem characterizing the EWs based on second moments, and therefore some EWs will not satisfy conditions (16).

4. Entanglement witnesses from random measurements

Here we will shortly present the physical set-up of the homodyne detection, that encodes the experimental settings measuring the variances of the state. Homodyne measurements are phase sensitive measurements which allow the detection of the moments of quadratures up to the second order [3, 4]. We denote by $\hat{k}$ and $\hat{k}^\dagger$ the mode operators of our state. A simple scheme for balanced homodyne measurements is composed of a balanced beam splitter superposing the signal mode to be measured $\hat{k}$ with a strong local oscillator field $\alpha_{\rm LO} = |\alpha_{\rm LO}|e^{i\theta}$ with phase θ, and two photon detectors, converting the electromagnetic modes into two output photon currents, i_1 and i_2. The actual quantity to be measured is the difference in the photon currents, given by:

$$\delta i = i_1 - i_2 = q|\alpha_{\rm LO}|\ \langle \hat{x}_\theta \rangle, \tag{28}$$

with q being a constant, and $\hat{x}_\theta$ is the generalized quadrature operator of mode $\hat{k}$ defined as:

$$\hat{x}_\theta = \frac{\exp(-i\theta)\hat{k} + \exp(i\theta)\hat{k}^\dagger}{\sqrt{2}}, \tag{29}$$

which covers the whole continuum of quadratures for $\theta \in [0, \pi]$. It was shown in reference [26] that in the strong local oscillator limit the homodyne detection performs projective measurements corresponding to the positive operator valued measure $\{|x_\theta\rangle\langle x_\theta|\}$, where $|x_\theta\rangle$ is the eigenstate of the quadrature phase operator $\hat{x}_\theta$.

In two-mode homodyne detection, we rely on the detection scheme proposed in reference [27], where the two-mode states are characterized by a single homodyne detector. By denoting with $\hat{a}$ and $\hat{b}$ the initial modes to be detected, the mode $\hat{k}$ arriving at the detector can be expressed as [27]

$$\hat{k} = \exp(i\varphi)\cos\phi\,\hat{a} + \sin\phi\,\hat{b}, \tag{30}$$

which corresponds to applying a phase shift of angle φ between the horizontal and vertical polarization components, a polarization rotator of angle ϕ, and a polarizing beam splitter (PBS) reflecting the vertically polarized component of the beam toward the detector [27]. Using repeated measurements of the quadratures for a set of identical states, the homodyne data are collected for which a probability distribution can be assigned with the variance given by:

$$\langle \hat{x}_\theta^2 \rangle - \langle \hat{x}_\theta \rangle^2 = \mathrm{Tr}[P\gamma], \tag{31}$$

where P is the matrix for the measurement of the quadrature variance of the mode $\hat{k}$:

$$P = uu^{\rm T}, \quad u^{\rm T} = \left(\cos\phi\cos(\theta-\varphi),\ \cos\phi\sin(\theta-\varphi),\ \sin\phi\cos\theta,\ \sin\phi\sin\theta\right). \tag{32}$$

As P is a symmetric, real 4×4 matrix we can see that for 10 different combinations of angles θ, ϕ and φ the entire two-mode CM can be reconstructed (the number of unknown independent parameters in an N-mode CM is $N(2N+1)$).

The extension of detection to N-mode CV states by a single homodyne detector can be achieved by applying the same two-mode combination scheme $N-1$ times. For example, for the initial modes $\hat{a}$, $\hat{b}$ and $\hat{c}$, the generalized mode arriving at the detector is:

$$\hat{k} = \exp(\mathrm{i}\varphi_1)\cos\phi\,\hat{a} + \exp(\mathrm{i}\varphi_2)\sin\phi\,\cos\psi\,\hat{b} + \sin\phi\,\sin\psi\,\hat{c}, \tag{33}$$

from where we can see that for $\psi = 0$ and $\varphi_2 = 0$ the two-mode case in equation (30) is obtained. We denote by P_j the matrix of the jth measurement.

4.1. Constructing witnesses

Random measurement directions in the case of two modes are given by random angles θ, ϕ, φ that are drawn from a uniform distribution in an interval:

$$0 \leqslant \theta \leqslant \pi, \tag{34}$$

$$0 \leqslant \phi \leqslant \pi, \tag{35}$$

$$0 \leqslant \varphi < 2\pi. \tag{36}$$

The problem of finding a witness operator Z, given the repeated independent measurements P_j on the CM, reduces to finding the coefficients c_j such that $Z = \sum_j c_j P_j$. Therefore, we apply the proposition in order to find the best witness for two-mode CMs, and propose the following SDP:

$$\begin{aligned} &\underset{x}{\text{minimize}}\ \mathbf{c}\cdot\mathbf{m} \\ &\text{subject to } Z = \sum_j c_j P_j \\ &Z = \begin{pmatrix} Z_1 & Z_c \\ Z_c^{\mathrm{T}} & Z_2 \end{pmatrix} \geqslant 0 \\ &Z_1 + \mathrm{i}x\Omega_1 \geqslant 0 \\ &Z_2 + \mathrm{i}(\frac{1}{2} - x)\Omega_1 \geqslant 0, \end{aligned} \tag{37}$$

where $\mathbf{m} = \mathrm{Tr}(\boldsymbol{P}\gamma)$, with $\mathbf{P}$ being the vector of measurement matrices P_j. This SDP finds the matrix Z, given the experimentally obtained data, such that

$$\mathbf{c}\cdot\mathbf{m} = \mathrm{Tr}[Z\gamma] \tag{38}$$

takes its minimal value, while being an EW as defined in theorem above. If the obtained value in equation (38) is smaller than one, then the CV state with CM γ can be unambiguously identified as being entangled.

This SDP also allows for the identification of the minimal number of measurements that are required for entanglement assessment in arbitrary states. The number of measurements in a tomographically complete setting is given by $N(2N+1)$, where N is the number of modes. This is the maximal number of measurement settings required to detect entanglement. However, the set of EWs described in the proposition is more restrictive than the set of all EWs. The consequences will be discussed later.

5. Detection of non-PPT entanglement and bound entanglement

The proposed SDP has the immediate advantage that it does not require any information about the state, except the number of modes N. We will now test the performance of this method by simulating its implementation on random two-mode entangled CV states, and on four-mode bipartite bound entangled states.

The entanglement of two-mode CMs with block structure given by:

$$\gamma = \begin{pmatrix} \gamma_1 & \varepsilon_{1,2} \\ \varepsilon_{1,2}^{\mathrm{T}} & \gamma_2 \end{pmatrix} \tag{39}$$

is quantified by means of the logarithmic negativity [28]:

$$E = \max\left\{0, -\frac{1}{2}\log_2 f\right\}, \tag{40}$$

where

$$f = \frac{1}{2}(\det \gamma_1 + \det \gamma_2) - \det \varepsilon_{1,2} - \left(\left[\frac{1}{2}(\det \gamma_1 + \det \gamma_2) - \det \varepsilon_{1,2}\right]^2 - \det \gamma\right)^{1/2}. \quad (41)$$

An EW provides a lower bound for the logarithmic negativity measure when the PPT criterion of separability is necessary and sufficient [16]:

$$E \geqslant \log_2 \frac{1}{w}, \quad (42)$$

where $w \in (0, 1)$ is the outcome of measuring an EW on CM γ: $\mathrm{Tr}[Z\gamma] = w$. For two-mode CMs the logarithmic negativity corresponds to the minimal[5] EW $Z_{\min}$ giving the smallest possible value $w_{\min}$.

In the following we investigate the efficiency of our method for detecting entanglement of arbitrary CV states, with respect to the minimal number of measurements required to accomplish this task. Thus, given an arbitrary unknown CM our algorithm first computes the variances of the generalized quadrature (31) for one random measurement direction in phase space and then carries out the SDP optimization to check if the state is entangled. If entanglement is not detected, additional random measurements are successively simulated and the optimization algorithm is executed each time until the entanglement is detected. At least two measurement settings are required in order to detect entanglement.

5.1. Detecting entanglement in squeezed vacuum states

The CMs of squeezed vacuum states have the form:

$$\gamma = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}, \quad (43)$$

where r is the squeezing parameter. For such states the logarithmic negativity can be calculated using (40), obtaining a linear dependence on the squeezing parameter:

$$E = 2r \log_2 e, \quad (44)$$

where e is the Euler constant. Squeezed vacuum states are Gaussian states, which are naturally accessible in many experimental situations where spontaneous down conversion is involved, being also useful in many quantum optics applications [3, 4].[6]

In figure 1 we show the fraction of entanglement detection of squeezed vacuum states, using random EWs. Contrary to intuition, states with less entanglement are more easily detected, i.e. they require on average fewer measurements than states with higher entanglement. This is due to the fact that in this case the amount of entanglement is linked to the strength of quadrature squeezing. It is well known that it is difficult to measure high squeezing in CV states [29] (see also the explanation given in figure 2). The full tomography for two-mode CMs is reached by 10 independent measurements. The CM (43) of the squeezed vacuum state has some zero elements, and with this knowledge about the state one would need only 6 measurements to reconstruct the CM entirely. However, our method may require more than 6 measurements to assess entanglement since we assumed no information about the states, except the dimension of the CM. As a consequence of the stronger constraints imposed on the EWs in equation (16) our method requires, with very low probability (0.0094% in our example), more than 10 measurements, which correspond to full tomography.

In figure 2 we show the variance of the generalized quadrature $\mathrm{Tr}[P\gamma]$, see (31), for $\theta = 0$, as a function of $\varphi \in [-\pi, \pi]$ and $\phi \in [-\pi, \pi]$, for different values of the squeezing parameter, $r = 0.2$ (left) and $r = 1$ (right), of the squeezed vacuum state. The outcomes of the random measurements are represented by the points on this surface. The horizontal plane is given by $\mathrm{Tr}[P\gamma] = 1$, which holds for a separable vacuum state with $r = 0$. The areas below this plane, where $\mathrm{Tr}[P\gamma] < 1$, correspond to the region of parameters φ and ϕ for which entanglement is detected. We observe that the areas of the regions of entanglement detection are decreasing with increasing the squeezing. This corresponds to the fact that highly squeezed

[5] Compared to the optimal EW in state space, the minimal EW based on second moments gives the best estimate of the degree of entanglement the considered state has, but it is not necessarily the finest witness [16].

[6] Recent experiments report the achievement in measuring 15 dB of squeezed light [29], which corresponds to $r \approx 1.73$ according to the formula [30]: $\#\mathrm{dB} = 10 \log_{10} e^{2r}$.

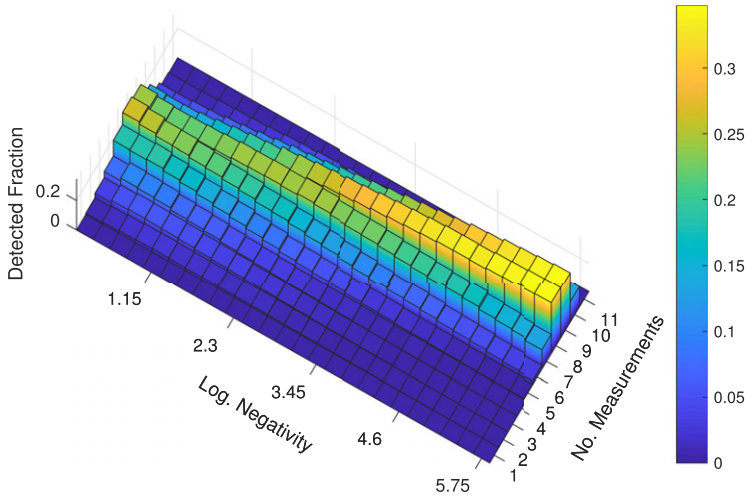

Figure 1. Fraction of entanglement detection of squeezed vacuum states: 5×10^5 runs of the algorithm on the two-mode squeezed vacuum states (43) with squeezing parameter $r \in [0, 2]$. The logarithmic negativity is given by $E = 2r \log_2 e$ (see equation (44)). By successively adding measurement directions, the EW is evaluated at every round until the presence of entanglement is certified. The data are normalized such that they sum up to 1 for every value of entanglement.

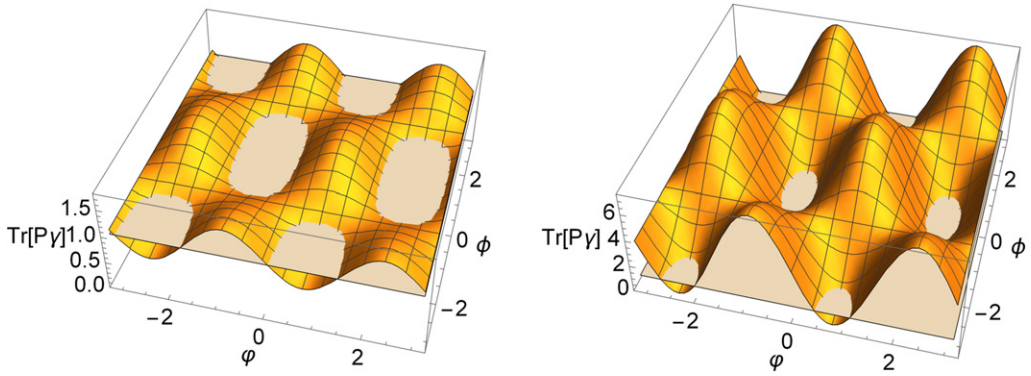

Figure 2. The variance of the generalized quadrature $\mathrm{Tr}[P\gamma]$, see equation (31), of the squeezed vacuum CM, as a function of $\varphi \in [-\pi, \pi]$ and $\phi \in [-\pi, \pi]$, for $\theta = 0$ and squeezing parameter $r = 0.2$ (left) and $r = 1$ (right). The horizontal plane represents $\mathrm{Tr}[P\gamma] = 1$, which is the case of the squeezed vacuum states with $r = 0$ (separable states). In the regions below this plane entanglement is detected.

states occupy a smaller region in phase space in terms of the angles ϕ, φ. Thus, more random measurements are needed to detect the entanglement.

5.2. Detecting entanglement in random covariance matrices

Random CMs are produced as follows. Starting with a CM in diagonal form, with symplectic eigenvalues $\nu_i \geqslant 1$ $(i = 1, \ldots, N)$ randomly generated from a uniform distribution in a finite real interval $[1, t]$, $t > 1$:

$$\gamma_{\mathrm{th}} = \bigoplus_{i=1}^{N} \begin{pmatrix} \nu_i & 0 \\ 0 & \nu_i \end{pmatrix}, \tag{45}$$

the general random CMs γ are created by applying random symplectic transformations $S \in Sp(2N, \mathbb{R})$, as follows [5]:

$$\gamma = S\gamma_{\mathrm{th}}S^{\mathrm{T}}. \tag{46}$$

The matrix (45) is the CM of thermal states, with the symplectic eigenvalue of every mode i related to the thermal photon number n_i as follows: $\nu_i = 2n_i + 1$ [5]. Random symplectic matrices are generated using the Euler decomposition (7). First, unitary matrices X and Y in equation (9) are generated from the Haar distribution [24], and the symplectic orthogonal matrices K and L are formed as in equation (10). The one-mode squeezers defined in equation (8) are created by randomly choosing parameters r_i via a uniform distribution in a finite interval. For this purpose we implemented the Matlab code presented in reference [31].

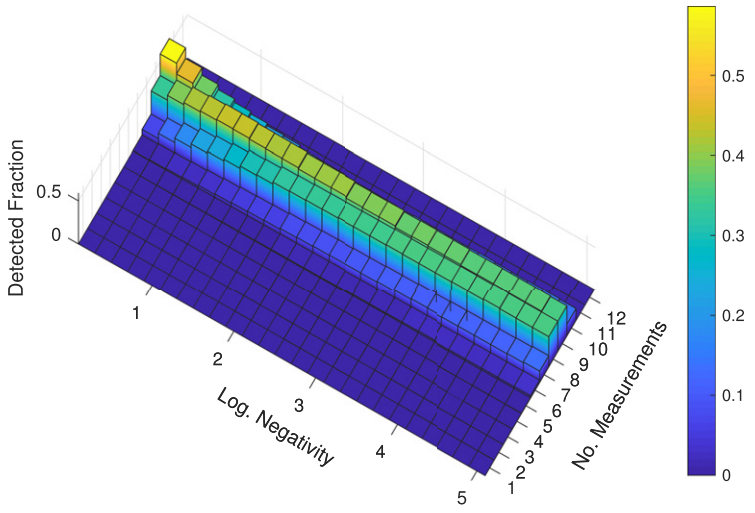

Figure 3. Fraction of entanglement detection for random two-mode states: 5×10^5 runs of the algorithm on random two-mode CMs for $\nu_i \in [0, 5]$ and $r_i \in [0, 2]$. By successively adding measurement directions, the EW is evaluated at every round until the presence of entanglement is certified. The data are normalized such that they sum up to 1 for every value of entanglement.

In figure 3 we illustrate the efficiency of entanglement detection for general random two-mode CMs, created from thermal state CMs (45) with random symplectic eigenvalues $\nu_i \in [0, 5]$, by random symplectic transformations (7) with squeezing parameters $r_i \in [0, 2]$. Our method shows a slight improvement in the efficiency of entanglement detection for highly entangled states compared to less entangled states, and most of the time it does not require full tomography. However, because of the strength of our proposed linear constraints, we may need, with very low probability, more measurements than in the full tomography in order to detect entanglement in random two-mode states. The probability that entanglement is detected by 11–12 measurements in this case, is 0.05%.

The evident difference in the efficiency of entanglement detection in random CMs compared to squeezed vacuum states may reside in the fact that highly squeezed states look classical in random measurement directions, which does not have to be the case for random states. In addition, squeezed vacuum states are a special class of states for which the logarithmic negativity has a linear dependence on the squeezing parameter alone (see equation (44)), while for a general two-mode CM the logarithmic negativity depends also on thermal photon number of the modes, and the simulation of entanglement detection shows a different behaviour.

In general, it is unlikely to draw randomly an entangled state with high logarithmic negativity, especially for states with a high number of modes. However, for the two-mode CMs, with the range of entanglement considered in figure 3, a substantial fraction of randomly generated CMs is entangled, which allowed us to perform the simulation.

5.3. Detecting bipartite bound entanglement

Since the proposed SDP algorithm can be easily generalized to multi-mode CV states, we provide an example of a four-mode CM with 12 independent parameters, mentioned in reference [32], which has bipartite bound entanglement:

$$\gamma = \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 4 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}. \tag{47}$$

The detection of bound entanglement by our method proves that the EWs defined in the theorem above, goes beyond the criteria which detect entanglement only in states with non-PPT. A general N-mode CM has $N(2N + 1)$ independent variables, and for the four-mode CM in equation (47) by performing 36 measurements our algorithm provides the best estimate of entanglement, $\mathrm{Tr}[Z_{\min}\gamma] = 0.8966$, which is in agreement with the results of reference [17]. In figure 4 we depict the frequency of entanglement detection

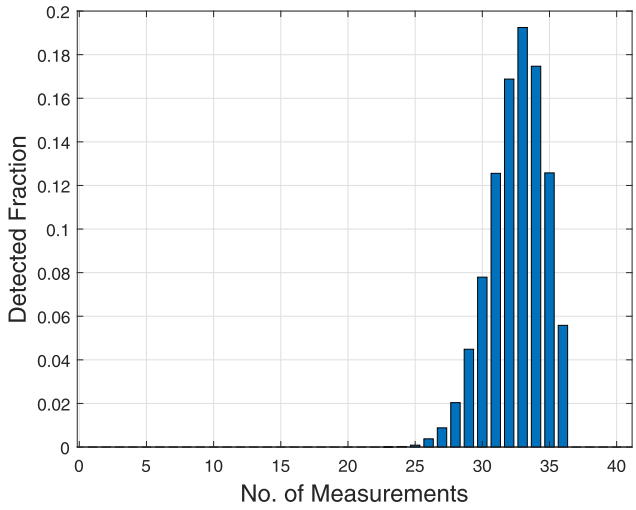

Figure 4. Fraction of entanglement detection for 4-mode bipartite bound entangled state, see equation (47): 10^4 runs of the algorithm. The data are normalized such that they sum up to 1.

as a function of the number of random measurements composing the witness. The CM in equation (47) is of a rather simple form, however, the construction of the EW detecting bound entanglement requires 33 random measurements on average, since our SDP considers the number of modes of the state as the only available information.

6. Statistical analysis

Until now we have considered only ideal measurements, where we used the exact variances $m_i = \mathrm{Tr}[P_i\gamma] = (\Delta\hat{x}_{\theta_i})^2$ (see section 4) in order to construct the EW. In real experiments the accessible data are subject to statistical fluctuations. In the following we perform the statistical analysis for the case of Gaussian states, that is, we assume that the data obtained in homodyning, which represent the collection of outcomes $X_{ij} = \langle\hat{x}_{\theta_i}\rangle_j$, $(j = 1, \ldots, n_i)$, from n_i repetitions of the measurement with the measurement direction given by θ_i, are governed by the normal probability distribution $\mathcal{N}_i(\mu_i, m_i)$ with the mean μ_i, and variance $m_i = (\Delta\hat{x}_{\theta_i})^2$. Given the homodyne data from n_i measurements for a fixed measurement direction θ_i, the sample variance denoted as $\bar{P}_i$, which estimates the variance m_i, is given by[7]:

$$\bar{P}_i = \frac{1}{n_i - 1}\sum_{j=1}^{n_i}(X_{ij} - \bar{X}_i)^2, \tag{48}$$

where $\bar{X}_i$ is the sample mean:

$$\bar{X}_i = \frac{1}{n}\sum_{j=1}^{n_i} X_{ij}. \tag{49}$$

In this case, the estimated value of our witness $\mathrm{Tr}[Z\gamma]$, denoted as $\bar{Z}$, is given by:

$$\bar{Z} = \sum_i c_i\bar{P}_i, \tag{50}$$

where the index i is used to denote different measurement settings, and the coefficients c_i were introduced in equation (37). In the case when the data comes from a Gaussian probability distribution, the distribution of the sample variance follows the $\chi^2_{n_i-1}$ distribution [33]:

$$\frac{n_i - 1}{m_i}\bar{P}_i \sim \chi^2_{n_i-1}, \tag{51}$$

where $\chi^2_{n_i-1}$ is the chi-square distribution with $n_i - 1$ degrees of freedom, which by definition represents the distribution of sum of squares of $n_i - 1$ independent, standard normal random variables. The statistical

[7] Using $n_i - 1$ instead of n_i corrects the bias in the estimation of the population variance, and is called Bessel's correction [34]. This method is necessary when the population mean μ_i is unknown, but is estimated by the sample mean $\bar{X}_i$.

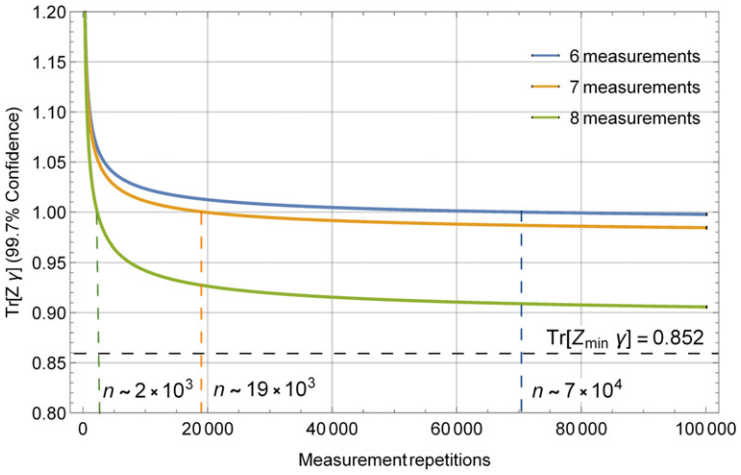

Figure 5. The maximum of the 3σ confidence interval for the witness Z of a Gaussian CM γ, as obtained by the statistical estimate according to equation (54). The horizontal dashed line indicates the minimal value of the witness for the considered CM $\mathrm{Tr}[Z_{\min}\gamma] = 0.852$. The vertical dashed lines indicate the number of measurement repetitions required to detect entanglement with 6 (blue), 7 (orange) and 8 (green) measurement settings.

error carried by $\chi^2_{n_i-1}$ is given by:

$$\Delta\chi^2_{n_i-1} = \sqrt{\mathrm{Var}(\chi^2_{n_i-1})} = \sqrt{2(n_i-1)}, \tag{52}$$

where $\mathrm{Var}(\chi^2_{n_i-1}) = 2(n_i-1)$ is the variance of the chi-square distribution [33]. Using the error propagation formula the uncertainty of $\bar{P}_i$ satisfies:

$$\Delta\bar{P}_i = \frac{\mathrm{d}\bar{P}_i}{\mathrm{d}\chi^2_{n_i-1}}\Delta\chi^2_{n_i-1} = \frac{m_i}{n_i-1}\Delta\chi^2_{n_i-1} = m_i\sqrt{\frac{2}{n_i-1}}. \tag{53}$$

Using again standard error propagation and considering that the number of measurement repetitions is equal for every measurement direction, i.e., $n = n_i$ for every i, we obtain that the resulting error of $\bar{Z}$ defined in equation (50) has the following expression:

$$\Delta\bar{Z} = \sqrt{\sum_i \left(\frac{\mathrm{d}\bar{Z}}{\mathrm{d}\bar{P}_i}\right)^2 (\Delta\bar{P}_i)^2} = \sqrt{\frac{2}{n-1}}\sqrt{\sum_i c_i^2 m_i^2}. \tag{54}$$

We stress the fact that, although by our method we can also detect entanglement in non-Gaussian states, this formula for the error of the value of the witness is valid only for Gaussian states. If the X_{ij} are not normally distributed, then the statistical analysis of EWs based on second moments will require also higher moments of the distribution.

In our method the coefficients c_i are derived from the variances m_i (see equation (37)), while equation (54) neglects the fact that they are not independent. To solve this difficulty one has to divide the homodyne data into two sets. First, one of them is used to derive the coefficients c_i, and then this witness is evaluated using the variances obtained from the other set of data [35]. In this way, the coefficients can be regarded as independent from the errors in the variances of the second set of data. With the quantity in equation (54) it is possible to decide whether it is better to perform additional repetitions of the measurements, or to add new measurements to detect entanglement. For example, consider the single detection of a low entanglement CM with $\mathrm{Tr}[Z_{\min}\gamma] = 0.852$. In figure 5 the 3σ-confidence of $\mathrm{Tr}[Z\gamma]$ is plotted as a function of the number n of measurement repetitions. It shows that a certification of $\mathrm{Tr}[Z\gamma] < 1$ with 99.7%-confidence is possible for 6 measurements, which requires a high number of repetitions of the measurements. However, this number significantly decreases when adding another measurement setting.

7. Summary and conclusions

We have proposed a method to detect entanglement of unknown CV states, given only the dimension of their covariance matrices, using random homodyne measurements. Our method provides an alternative for

performing full tomography. We characterize the EWs based on second moments using stronger semidefinite constraints than those presented in reference [17], and which account for obtaining a valid witness at all times. Therefore, a quantum state can be clearly considered entangled if it is detected by this criterion. As these constraints are linear, they can be implemented in an SDP. We studied the feasibility of this method in experimental situations, where the figure of merit is considered the number of measurements required to detect entanglement.

First, we tested the proposed algorithm for two-mode squeezed vacuum states, for which the logarithmic negativity linearly depends on the squeezing. We showed that the number of necessary random measurements is very likely to be smaller than for full tomography. We observed an increasing number of measurements required to detect highly entangled states, which is explained by the well-known difficulties in detecting high squeezing.

Our primary objective was to simulate the performance of this method for uniformly drawn random two-mode covariance matrices. Without adding any information about the states, we still found a reduction in the number of measurements needed to certify the presence of entanglement. The phenomenology of entanglement detection in random CV states is very similar to the case of decomposable witnesses for discrete systems [21]. Hence, a higher entanglement is easier to detect, but in our case this improvement is not as significant as in the discrete case. Only with very low probability our method needs more than a tomographically complete set of measurements in order to detect entanglement in random two-mode states.

Bound entangled CV states can also efficiently be detected by a random EW. Similarly to the previous cases entanglement is detected with less than a tomographically complete set of measurements.

As we provide a method of efficient entanglement detection in CV systems which does not require specific measurements, nor necessarily the full information about the CM, it is of high relevance for any experimental application which relies on the valuable resource of entanglement. The experimental scheme implementing our method for two-mode CV states consists of a phase shift in polarization basis, a rotator of polarization, a PBS and a homodyne detector, as e.g. presented in reference [27]. We also extended this scheme to multimode CV states. Our semidefinite optimisation program can easily be adapted to different experimental situations, like making specific measurements or including some additional information about the CM to be measured. Likewise, our method is also applicable to any experimental scheme measuring the quadrature variances, by directly inserting the results of the experiment into the optimisation program we provided. We investigated the statistical robustness of the method, and showed that it has a good robustness to statistical errors.

Acknowledgments

The authors thank Jochen Szangolies, Thomas Wagner and Matteo Paris for helpful discussions. Giulio Gianfelici has received funding from the German Federal Ministry of Education and Research (BMBF), within the Hardware-based Quantum Security (HQS) project.

ORCID iDs

Aurelian Isar https://orcid.org/0000-0003-3033-7045

References

[1] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865
[2] Bruß D and Leuchs G (ed) 2019 *Quantum Information: From Foundations to Quantum Technology Applications* 2nd edn (New York: Wiley)
[3] Braunstein S L and van Loock P 2005 Quantum information with continuous variables *Rev. Mod. Phys.* **77** 513
[4] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Gaussian quantum information *Rev. Mod. Phys.* **84** 621
[5] Serafini A 2017 *Quantum Continuous Variables: A Primer of Theoretical Methods* (Boca Raton, FL: CRC Press)
[6] Shi J, Chen S, Lu Y, Feng Y, Shi R, Yang Y and Li J 2020 An approach to cryptography based on continuous-variable quantum neural network *Sci. Rep.* **10** 2107
[7] Qureshi H S, Ullah S and Ghafoor F 2020 Continuous variable quantum teleportation via entangled Gaussian state generated by a linear beam splitter *J. Phys. B: At. Mol. Opt. Phys.* **53** 135501
[8] Guo Y, Liu B H, Li C F and Guo G C 2019 Advances in quantum dense coding *Adv. Quantum Technol.* **2** 1900011
[9] Mukamel S *et al* 2020 Roadmap on quantum light spectroscopy *J. Phys. B: At. Mol. Opt. Phys.* **53** 072002
[10] Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* **77** 1413
[11] Simon R 2000 Peres–Horodecki separability criterion for continuous variable systems *Phys. Rev. Lett.* **84** 2726
[12] Duan L-M, Giedke G, Cirac J I and Zoller P 2000 Inseparability criterion for continuous variable systems *Phys. Rev. Lett.* **84** 2722

[13] Aoki T, Takei N, Yonezawa H, Wakui K, Hiraoka T, Furusawa A and van Loock P 2003 Experimental creation of a fully inseparable tripartite continuous-variable state *Phys. Rev. Lett.* **91** 080404
[14] van Loock P and Furusawa A 2003 Detecting genuine multipartite continuous-variable entanglement *Phys. Rev.* A **67** 052315
[15] Gühne O and Tóth G 2009 Entanglement detection *Phys. Rep.* **474** 1
[16] Anders J 2003 Estimating the degree of entanglement of unknown Gaussian states *Diploma Thesis* Potsdam University
[17] Hyllus P and Eisert J 2006 Optimal entanglement witnesses for continuous-variable systems *New J. Phys.* **8** 51
[18] Shahandeh F, Sperling J and Vogel W 2013 Operational Gaussian Schmidt-number witnesses *Phys. Rev.* A **88** 062323
[19] Shchukin E and van Loock P 2015 Generalized conditions for genuine multipartite continuous variable entanglement *Phys. Rev.* A **92** 042328
[20] Williamson J 1936 On the algebraic problem concerning the normal forms of linear dynamical systems *Am. J. Math.* **58** 141
[21] Szangolies J, Kampermann H and Bruß D 2015 Detecting entanglement of unknown quantum states with random measurements *New J. Phys.* **17** 113051
[22] Simon R, Mukunda N and Dutta B 1994 Quantum-noise matrix for multimode systems: $U(n)$ invariance, squeezing, and normal forms *Phys. Rev.* A **49** 1567
[23] Werner R F and Wolf M M 2001 Bound entangled Gaussian states *Phys. Rev. Lett.* **86** 3658
[24] Dutta A B, Mukunda N and Simon R 1995 The real symplectic groups in quantum mechanics and optics *Pramana* **45** 471
[25] Bhatia R and Jain T 2015 On symplectic eigenvalues of positive definite matrices *J. Math. Phys.* **56** 112201
[26] Tyc T and Sanders B C 2004 Operational formulation of homodyne detection *J. Phys. A: Math. Gen.* **37** 7341
[27] D'Auria V, Porzio A, Solimeno S, Olivares S and Paris M G A 2005 Characterization of bipartite states using a single homodyne detector *J. Opt. B: Quantum Semiclass. Opt.* **7** S750
[28] Adesso G, Serafini A and Illuminati F 2004 Extremal entanglement and mixedness in continuous variable systems *Phys. Rev.* A **70** 022318
[29] Vahlbruch H, Mehmet M, Danzmann K and Schnabel R 2016 Detection of 15 dB squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency *Phys. Rev. Lett.* **117** 110801
[30] Adesso G, Ragy S and Lee A R 2014 Continuous variable quantum information: Gaussian states and beyond *Open Syst. Inf. Dyn.* **21** 1440001
[31] Jagger D P 2003 MATLAB toolbox for classical matrix groups *MSc Thesis* University of Manchester
[32] Werner R F and Wolf M M 2001 Bound entangled Gaussian states *Phys. Rev. Lett.* **86** 3658
[33] Knight K 2000 *Mathematical Statistics* (London: Chapman and Hall)
[34] Kenney J F and Keeping E S 1951 *Mathematics of Statistics* 2nd edn vol 2 (Princeton, NJ: Van Nostrand)
[35] Moroder T, Kleinmann M, Schindler P, Monz T, Gühne O and Blatt R 2013 Certifying experimental errors in quantum experiments *Phys. Rev. Lett.* **110** 180401

C

Hierarchy of continuous-variable quantum resource theories

Title:	Hierarchy of continuous-variable quantum resource theories
Authors:	Giulio Gianfelici, Hermann Kampermann and Dagmar Bruß
Journal:	New Journal of Physics
Impact factor:	3.729 (2020)
Date of submission:	30 June 2021
Publication status:	Submitted
Contribution by GG:	First author (input approx. 85%)

This publication corresponds to the reference [GKB21]. A summary of the results is presented in Chap. 7. The research objectives were initially suggested by DB and then regularly discussed and defined among all authors. I independently identified the requirement of finite mean energy as the key assumption to extend the hierarchy of discrete-variable resources of [Str+18] to continuous variables. I devised, with valuable inputs from HK, the continuous-variable version of the resource theory of non-uniformity. Together with HK, I adapted our analysis to a system composed of spectral and spatial modes. I performed all analytical calculations and created all figures in the article. I wrote the whole manuscript which was then proofread by my coauthors and greatly improved thanks to their comments.

Hierarchy of continuous-variable quantum resource theories

Giulio Gianfelici , Hermann Kampermann, and Dagmar Bruß

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

Email: giulio.gianfelici@uni-duesseldorf.de

Abstract

Connections between the resource theories of coherence and purity (or non-uniformity) are well known for discrete-variable, finite-dimensional, quantum systems. We establish analogous results for continuous-variable systems, in particular Gaussian systems. To this end, we define the concept of maximal coherence at fixed energy, which is achievable with energy-preserving unitaries. We show that the maximal Gaussian coherence (where states and operations are required to be Gaussian) can be quantified analytically by the relative entropy. We then propose a resource theory of non-uniformity, by considering the purity of a quantum state at fixed energy as resource, and by defining non-uniformity monotones. In the Gaussian case, we prove the equality of Gaussian non-uniformity and maximal Gaussian coherence. Finally, we show a hierarchy for non-uniformity, coherence, discord and entanglement in continuous-variable systems.

Keywords: continuous-variable systems, resource theories, quantum coherence, purity

1 Introduction

Quantum resource theories [1] describe the resources of quantum states in a quantitative way. The set of states is divided into *free states* (having no resource) and *resource states*. Quantum operations are called *free* when they transform any free state into a free state, i.e. free operations cannot increase the resources.

Different resource theories have different sets of free states and operations. For instance, the resource theory of coherence [2–7] identifies states that are diagonal in a certain basis as free, while the resource theory of purity [8–10] considers the maximally mixed state as the only free state. The resourcefulness of a quantum state can be quantified by a resource monotone, which is a function that is non-increasing under free operations. In particular, relevant monotones for several resource theories are based on the relative entropy [2, 9, 11, 12].

For discrete-variable (DV) systems, an important connection between coherence, purity, entanglement and discord was found in [10]. Here, it was shown that the purity of a quantum state is — for an appropriate resource monotone — equal to the maximal coherence that can be obtained by applying unitary operations to the state. This quantity then upper-bounds the maximal quantum discord and entanglement of the state.

This result cannot be straightforwardly extended to continuous-variable (CV) systems. Infinite-dimensional Hilbert spaces are structurally different from their finite-dimensional counterpart [13–16], and this difference influences the mathematical definition of the physical quantities themselves and their resource theories [17]. In particular, infinite-dimensional Hilbert spaces allow the generation of infinite resources via unitary operations [18, 19].

A common strategy to replicate DV results is to introduce valid physically and experimentally motivated constraints. The first restriction is to consider finite energy [18, 20, 21] and to explore the use of energy-preserving unitaries, as those operations are easily available in laboratories. The second restriction is to focus on Gaussian states and operations, as most of the relevant phenomena in quantum information and quantum optics can be described by at most quadratic Hamiltonians.

Equipped with these assumptions, we investigate the resource theories of CV coherence [6, 7]. We discuss both general and Gaussian coherence, the latter by restricting the set of quantum states and operations to be Gaussian. We define the concept of maximal coherence of a quantum state at fixed energy, as the coherence that can be obtained via applying energy-preserving unitaries. In the case of Gaussian coherence, we find the structure of the states with maximal coherence and discuss the form of the maximizing unitary in some specific cases. We derive an analytical expression for the relative entropy of the maximal Gaussian coherence. We then propose a resource theory of non-uniformity, to describe purity at fixed energy as resource, considering states that maximise the entropy at fixed energy as free. However, our resource theory studies the interactions of a quantum system with a noisy thermal environment, therefore it is connected to the resource theories of a-thermality [22, 23], where states out of thermal equilibrium are identified as resources. Our theory emphasises the entropic exchanges between the system and the environment, rather than the energetic ones.

Finally, we establish a connection between non-uniformity, coherence, quantum discord and entanglement, by identifying a hierarchy between them. In particular, the maximal Gaussian coherence is bounded by the Gaussian non-uniformity and both upper-bound the maximal discord and the entanglement. Our results represent an extension to infinite dimensions of the hierarchy found in [10].

We begin our work by introducing our setting together with the basic notions of CV quantum information in Sec. 2. We review coherence and Gaussian coherence in Sec. 3. In Sec. 4, we define the maximally coherent mixed state at fixed energy and derive its properties for the Gaussian case. We assemble the resource theory of non-uniformity in Sec. 5 and illustrate the connections between non-uniformity, coherence, discord and entanglement in Sec. 6. Finally, we summarise our results in Sec. 7.

2 Notation and preliminaries

In the following, we will indicate vectors and matrices as bold lowercase and uppercase letters, respectively. We shall consider systems with a finite number of discrete *spectral* and *spatial* modes, which refer to the frequency and location of the mode, respectively. We label the mode operators of a mode with two indices: an index ω for the spectral degrees of freedom and an index j for the spatial degrees of freedom.

We sort our mode operators by gathering all mode operators with the same frequency, i.e.

$$\{\, \hat{\boldsymbol{a}}_{\omega_1}, \hat{\boldsymbol{a}}_{\omega_2}, \dots \hat{\boldsymbol{a}}_{\omega_{M_f}} \,\}\,, \tag{1}$$

where M_f is the number of different frequencies, and for each frequency ω

$$\hat{\boldsymbol{a}}_\omega = (\hat{a}_{\omega;1}, \hat{a}_{\omega;2}, \ldots, \hat{a}_{\omega;M_s})^T, \tag{2}$$

with $\hat{a}_{\omega;j}$ being the annihilation operator for a mode with spectral label ω and spatial label j, and M_s being the total number of spatial labels. Without loss of generality, we assume that M_s is the same for all frequencies. A graphical depiction of our mode labeling is drawn in Fig. 1.

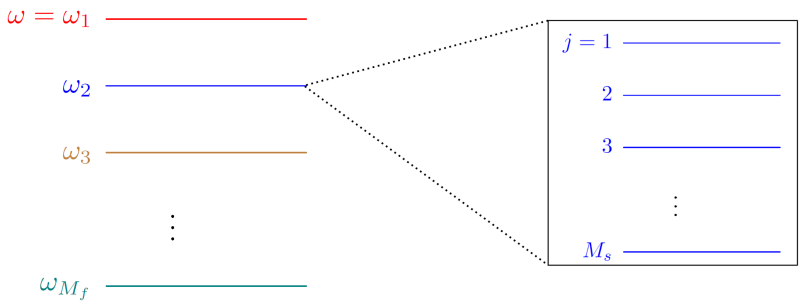

Figure 1: Graphical depiction of the labeling of the spectral and spatial modes. The modes are cataloged first in terms of their frequency $\omega = \omega_1, \omega_2, \ldots \omega_{M_f}$ (represented by a distinct colour) and then in terms of their spatial label $j = 1, 2, \ldots M_s$.

The operators satify the usual bosonic commutation relations

$$\left[\hat{a}_{\omega;j}, \hat{a}_{\omega';j'}\right] = \left[\hat{a}^\dagger_{\omega;j}, \hat{a}^\dagger_{\omega';j'}\right] = 0, \tag{3}$$

$$\left[\hat{a}_{\omega;j}, \hat{a}^\dagger_{\omega';j'}\right] = \delta_{\omega\omega'}\delta_{jj'}. \tag{4}$$

Using the notation of Eqs. (1) and (2), the free Hamiltonian of the system reads

$$\hat{H} = \sum_{\omega=\omega_1}^{\omega_{M_f}} \hbar\omega \left[\sum_{j=1}^{M_s} \left(\hat{a}^\dagger_{\omega;j}\, \hat{a}_{\omega;j} + \frac{1}{2}\right)\right]. \tag{5}$$

In the following, we will always assume that the system has finite mean energy, i.e. that the Hamiltonian satisfies $\langle \hat{H} \rangle < \infty$. This is a natural and physically reasonable assumption, and a mathematically necessary precondition for the trace-norm continuity of many functionals [18, 20, 21].

The total number of modes is $M = M_f M_s$. We shall label the modes with the index $m \equiv \omega; j$ whenever there is no need to distinguish between spectral and spatial modes. We use the order $m = (\omega_1; 1), (\omega_1; 2), \ldots, (\omega_1; M_s), (\omega_2; 1), \ldots, (\omega_{M_f}; M_s)$.

We now recall basic concepts of Gaussian quantum information, inspired from [13–16] and written according to our notation.

For each mode m, we define the canonical conjugate operators $\hat{q}_m := (\hat{a}_m + \hat{a}^\dagger_m)/\sqrt{2}$ and $\hat{p}_m := (\hat{a}_m - \hat{a}^\dagger_m)/(i\sqrt{2})$. We group them in a vector $\hat{\boldsymbol{r}} := (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_M, \hat{p}_M)^T$.

The first and second moment of a state ρ is the *displacement vector* $\boldsymbol{d}$ and the *covariance matrix* $\boldsymbol{V}$, respectively. Their components d_m and $V_{mm'}$ read in terms of components $\hat{r}_m$ of $\hat{\boldsymbol{r}}$

as [15]:

$$d_m := \langle \hat{r}_m \rangle = \mathrm{Tr}\,[\hat{r}_m\,\rho], \tag{6}$$

$$V_{mm'} := \langle \hat{r}_m\,\hat{r}_{m'} + \hat{r}_{m'}\,\hat{r}_m \rangle - 2\,d_m\,d_{m'}. \tag{7}$$

Both moments are real, and $\boldsymbol{V}$ is symmetric and positive definite. Gaussian states are represented by a Gaussian quasi-probability distribution in the phase space and are fully characterised by the first and second moments. The $2M$-dimensional displacement vector and the $2M \times 2M$ covariance matrix of any Gaussian state can be written in the following block form:

$$\boldsymbol{d} = \begin{pmatrix} \boldsymbol{d}_1 \\ \boldsymbol{d}_2 \\ \vdots \\ \boldsymbol{d}_M \end{pmatrix}, \qquad \boldsymbol{V} = \begin{pmatrix} \boldsymbol{V}_1 & \boldsymbol{\Delta}_{12} & \dots & \boldsymbol{\Delta}_{1M} \\ \boldsymbol{\Delta}_{12}^T & \boldsymbol{V}_2 & \dots & \boldsymbol{\Delta}_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\Delta}_{1M}^T & \boldsymbol{\Delta}_{2M}^T & \dots & \boldsymbol{V}_M \end{pmatrix}, \tag{8}$$

where $\boldsymbol{d}_m$ are 2-dimensional vectors, and $\boldsymbol{V}_m$ and $\boldsymbol{\Delta}_{mm'}$ are 2×2 real matrices. In particular, $\boldsymbol{d}_m$ ($\boldsymbol{V}_m$) corresponds to the displacement vector (the covariance matrix) of the reduced state $\rho_m = \mathrm{Tr}_{\boldsymbol{m}\setminus m}\,[\,\rho\,]$ after partial trace of all modes but the m-th, while $\boldsymbol{\Delta}_{mm'}$ is related to the correlations between the modes m and m' [13].

The total average occupation number can be derived as

$$\langle \hat{N} \rangle = \sum_{m=1}^{M} \bar{n}_m = \sum_{m=1}^{M} \frac{1}{4}\,(\mathrm{Tr}[\boldsymbol{V}_m] + 2|\boldsymbol{d}_m|^2 - 2), \tag{9}$$

where $\bar{n}_m$ is the average occupation number of the m-th mode. This expression can be obtained by writing $\mathrm{Tr}[\boldsymbol{V}_m]$ in terms of Eq. (7) and the mode operators $\hat{a}_m$ and $\hat{a}_m^\dagger$

$$\begin{aligned} \mathrm{Tr}[\boldsymbol{V}_m] &= 2\,\langle \hat{q}_m^2 \rangle + 2\,\langle \hat{p}_m^2 \rangle - 2\,\langle \hat{q}_m \rangle^2 - 2\,\langle \hat{p}_m \rangle^2 = \langle (\hat{a}_m + \hat{a}_m^\dagger)^2 \rangle - \langle (\hat{a}_m - \hat{a}_m^\dagger)^2 \rangle - 2|\boldsymbol{d}_m|^2 \\ &= 2 + 4\,\langle \hat{a}_m^\dagger \hat{a}_m \rangle - 2|\boldsymbol{d}_m|^2. \end{aligned} \tag{10}$$

Eq. (9) follows by setting $\langle \hat{N} \rangle = \sum_{m=1}^{M} \langle \hat{a}_m^\dagger \hat{a}_m \rangle$. Notice that this formula holds regardless of the presence of correlations between different modes, for both Gaussian and non-Gaussian states.

By Williamson's theorem [24], any covariance matrix $\boldsymbol{V}$ can be brought into a diagonal form:

$$\boldsymbol{V} = \boldsymbol{S}\,\boldsymbol{D}\,\boldsymbol{S}^T, \tag{11}$$

where $\boldsymbol{D}$ is a diagonal matrix

$$\boldsymbol{D} = \mathrm{diag}\,[\nu_1, \nu_1, \dots, \nu_M, \nu_M]\,, \tag{12}$$

and $\boldsymbol{S}$ is a *symplectic matrix*, i.e. a real matrix that satisfies

$$\boldsymbol{S}\boldsymbol{\Omega}\boldsymbol{S}^T = \boldsymbol{\Omega}, \qquad \boldsymbol{\Omega} = \bigoplus_{m=1}^{M} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{13}$$

The variables $\nu_m \geq 1$ are called *symplectic eigenvalues* and obey the Bose-Einstein statistics:

$$\nu_m = \nu_{\omega;j} = \frac{1}{2}\,\left[\exp\left(\frac{\hbar\omega}{\kappa\,T_{\omega;j}}\right) - 1\right]^{-1} - \frac{1}{2}, \tag{14}$$

where κ is the Boltzmann constant and $T_{\omega;j}$ is the temperature of the m-th mode, with $m = (\omega; j)$. The symplectic eigenvalues are used to express several properties of Gaussian states. For instance, the von-Neumann entropy of a Gaussian state reads [25]:

$$S(\rho) = \sum_{m=1}^{M} \left(\frac{\nu_m + 1}{2} \log \frac{\nu_m + 1}{2} - \frac{\nu_m - 1}{2} \log \frac{\nu_m - 1}{2} \right). \tag{15}$$

Any unitary that preserves the Gaussianity of quantum states is called *Gaussian unitary*. In terms of the moments, a Gaussian unitary acts as [16]

$$\begin{aligned} \boldsymbol{d} &\to \boldsymbol{S} \cdot \boldsymbol{d} + \boldsymbol{v}, \\ \boldsymbol{V} &\to \boldsymbol{S} \cdot \boldsymbol{V} \cdot \boldsymbol{S}^T, \end{aligned} \tag{16}$$

where $\boldsymbol{v}$ is a $2M$-dimensional vector and $\boldsymbol{S}$ is a $2M \times 2M$ symplectic matrix.

Theorem 2.1 (*Bloch-Messiah decomposition* [26])**.** *Any $2M \times 2M$ symplectic matrix can be decomposed as*

$$\boldsymbol{S} = \boldsymbol{O}_1 \left[\bigoplus_{m=1}^{M} \boldsymbol{Z}(r_m) \right] \boldsymbol{O}_2, \tag{17}$$

where the $2M \times 2M$ matrices $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are symplectic and orthogonal (we generally denote symplectic orthogonal matrices as $\boldsymbol{O}$), and the 2×2 matrix $\boldsymbol{Z}(r_m)$ is a single-mode squeezer with squeezing parameter r_m, that is

$$\boldsymbol{Z}(r_m) := \begin{pmatrix} e^{-r_m} & 0 \\ 0 & e^{r_m} \end{pmatrix}. \tag{18}$$

For $r_m = 0$ (absence of squeezing), $\boldsymbol{Z}(r_m)$ becomes the identity $\boldsymbol{I}$. Therefore, in Eq. (17), $\boldsymbol{S} = \boldsymbol{O}_1 \boldsymbol{O}_2$ is orthogonal, being the product of two orthogonal matrices.

Definition 2.2. A *passive unitary* [13, 14] is a Gaussian unitary $\hat{U}_{\boldsymbol{O}}$ that is represented in the phase space (Eq. (16)) by $\boldsymbol{v} = \boldsymbol{0}$ and a symplectic orthogonal matrix $\boldsymbol{O}$ in the form of

$$\boldsymbol{O} = \bigoplus_{\omega=\omega_1}^{\omega_{M_f}} \boldsymbol{O}_\omega, \tag{19}$$

where $\boldsymbol{O}_\omega$ are $2M_s \times 2M_s$ symplectic orthogonal matrices acting on the subset of modes with frequency ω. Conversely, any Gaussian unitary that is not passive, is called *active*.

Active unitaries are associated with linear displacements and squeezing. Passive unitaries are realised by linear-optics circuits, that is any multiport interferometer made of beam splitters and phase shifters. They preserve the total average occupation number (see Eq. (9)):

$$\langle \hat{N} \rangle = \frac{1}{4} \left(\mathrm{Tr}[\boldsymbol{O}\,\boldsymbol{V}\,\boldsymbol{O}^T] + 2|\boldsymbol{O}\boldsymbol{d}|^2 - 2M \right) = \frac{1}{4} \left(\mathrm{Tr}[\boldsymbol{V}] + 2|\boldsymbol{d}|^2 - 2M \right). \tag{20}$$

Since $\hat{N}$ commutes with the Hamiltonian $\hat{H}$ of the system, passive Gaussian unitaries preserve the average energy, too. Passive Gaussian unitaries are the only energy-preserving Gaussian unitaries [15, 16]. They create correlations between spatial modes with the same frequency ω.

They do not allow interactions between modes with different frequencies (see Eq. (19), and [27]).

Gaussian unitaries are not the only operations that preserve the Gaussianity of a quantum state. A *Gaussian channel* is a completely positive trace-preserving (CPTP) operation that maps Gaussian states into Gaussian states. In terms of the moments, a Gaussian channel acts as [28]

$$\begin{aligned} \boldsymbol{d} &\to \boldsymbol{T} \cdot \boldsymbol{d} + \boldsymbol{v}, \\ \boldsymbol{V} &\to \boldsymbol{T} \cdot \boldsymbol{V} \cdot \boldsymbol{T}^T + \boldsymbol{N}, \end{aligned} \tag{21}$$

where $\boldsymbol{T}$, $\boldsymbol{N}$ are $2M \times 2M$ real matrices, $\boldsymbol{N} \geq 0$, and $\boldsymbol{v}$ is a $2M$-dimensional vector.

3 Resource theory of (Gaussian) coherence

A state ρ of M bosonic modes is said to be *incoherent* if it is diagonal in the M-mode Fock basis [6], i.e.

$$\rho = \sum_{n_1 \ldots n_M = 0}^{\infty} p_{n_1 \ldots n_M} \left| n_1 \right\rangle \left\langle n_1 \right| \otimes \cdots \otimes \left| n_M \right\rangle \left\langle n_M \right|, \tag{22}$$

for an arbitrary set of non-negative probabilities $\{ p_{n_1 \ldots n_M} \}$.

We denote the set of all incoherent states by $\mathcal{I}$. The resource theory of coherence admits different sets of free operations. The maximal set of free operations for $\mathcal{I}$ are called *maximally incoherent operations* (MIO) [2]. These are all maps that cannot create coherence, i.e.,

$$\Lambda_{MIO}(\rho) \in \mathcal{I}, \qquad \forall\, \rho \in \mathcal{I}. \tag{23}$$

An extensive study of MIO in infinite-dimensional Hilbert spaces has not been carried out so far. We shall not investigate this here, referring to [5] for a general review of coherence and to [6] for the CV case.

Definition 3.1. For continuous-variable systems, a function $\mathcal{C}(\rho)$ is a suitable measure of coherence with respect to a chosen set of free operations, e.g. MIO (see Eq.(23)), if it satisfies the following properties [3, 6, 7]:

(C1) Positivity: $\mathcal{C}(\rho) \geq 0$ for any density operator ρ and $\mathcal{C}(\rho) = 0$ iff $\rho \in \mathcal{I}$;

(C2) Monotonicity under the chosen set of free operations, e.g. for MIO:

$$\mathcal{C}(\rho) \geq \mathcal{C}(\Lambda_{MIO}(\rho)); \tag{24}$$

(C3) Convexity:

$$\sum_n p_n \, \mathcal{C}(\rho_n) \geq \mathcal{C}\left(\sum_n p_n \, \rho_n \right); \tag{25}$$

(C4) Finite coherence for systems with finite energy:

$$\langle \hat{H} \rangle < \infty \Rightarrow \mathcal{C}(\rho) < \infty. \tag{26}$$

The condition (C4) is specific for CV systems. Denoting with $S(\rho\|\tau)$ the quantum relative entropy between ρ and τ,

$$S(\rho\|\tau) := \mathrm{Tr}[\rho\log\rho] - \mathrm{Tr}[\rho\log\tau], \tag{27}$$

the *relative entropy of coherence* is defined as:

$$\mathcal{C}_{rel}(\rho) := \min_{\tau\in\mathcal{I}} S(\rho\|\tau). \tag{28}$$

This measure satisfies all conditions of Def. 3.1 [6].

The generic CV coherence has not been deeply studied, mainly because of theoretical and experimental difficulties associated with general bosonic Hilbert spaces. We shall therefore address now the relevant Gaussian subclass, in which all states and operations are Gaussian [1].

In the realm of Gaussian states, a state is diagonal in the Fock basis if and only if it is a thermal state [7], defined as

$$\begin{aligned}\tau_M(\bar{\boldsymbol{n}}) &:= \bigotimes_{m=1}^{M}\tau(\bar{n}_m);\\ \tau(\bar{n}_m) &:= \sum_{n_m=0}^{\infty}\frac{\bar{n}_m^{n_m}}{(\bar{n}_m+1)^{n_m+1}}\,|n_m\rangle\langle n_m|\,,\end{aligned} \tag{29}$$

where $\bar{\boldsymbol{n}} = (\bar{n}_1,\ldots,\bar{n}_M)$ and $\bar{n}_m$ is the average occupation number of the m-th mode (see Eq. (9)). The subscript M in τ_M denotes the number of modes of τ_M, and is omitted for single-mode thermal states. Thermal states have a zero displacement vector and a diagonal covariance matrix

$$\boldsymbol{V}\left[\tau_M(\bar{\boldsymbol{n}})\right] = \bigoplus_{m=1}^{M}(2\bar{n}_m+1)\boldsymbol{I}. \tag{30}$$

We denote the subset of all incoherent Gaussian states by $\mathcal{I}_G$. Xu [7] introduced *incoherent Gaussian operations* (IG).

Definition 3.2. Incoherent Gaussian operations (IG) are defined as all Gaussian channels Λ_{IG} that map thermal states (Eq. (29)) into thermal states, i.e. the maximal set of free operations in this scenario. A generic IG can be written in the form of Eq. (21), where

- $\boldsymbol{v}_{IG} = 0$;
- $\boldsymbol{N}_{IG}$ is diagonal,
$$\boldsymbol{N}_{IG} = \mathrm{diag}\left\{w_1\,\boldsymbol{I}_2,\ldots,w_M\,\boldsymbol{I}_2\right\}, \tag{31}$$
with $\omega_m \geq 0$;
- $\boldsymbol{T}_{IG}$ is composed of M_f submatrices $\boldsymbol{T}_\omega$ that act on single frequency sectors, namely:
$$\boldsymbol{T}_{IG} = \bigoplus_{\omega=\omega_1}^{\omega_{M_f}}\boldsymbol{T}_\omega, \tag{32}$$
and each $\boldsymbol{T}_\omega$ can be generated as follows:

[1] In principle, one could consider mixed scenarios, e.g. with Gaussian states and general operations, or vice versa. This goes beyond the scope of our work.

1. Take M_s real coefficients $t_{\omega;j} \in \mathbb{R}$;
2. Take M_s 2×2 orthogonal matrices $\boldsymbol{\mathcal{O}}_{\omega;j}$, which do not need to be symplectic;
3. $\boldsymbol{T}_\omega$ is given by a permutation of the columns of $\bigoplus_{j=1}^{M_s} t_{\omega;j} \boldsymbol{\mathcal{O}}_{\omega;j}$.

Definition 3.3. A function $\mathcal{C}^G(\rho)$ is a suitable measure of Gaussian coherence with respect to IG ($\mathcal{I}_G$) as free operations (free states), if it satisfies the properties (C1)-(C4) of Def. 3.1. Here, IG are defined in Def. 3.2 and states in $\mathcal{I}_G$ are defined by Eq. (29). This function quantifies the Gaussian coherence, which is, in general, an upper bound for the general coherence (since $\mathcal{I}_G \subset \mathcal{I}$).

In particular, the *relative entropy of Gaussian coherence* $\mathcal{C}^G_{rel}(\rho)$ can be defined as the relative entropy of coherence (see Eq. (28)) by performing the minimization over $\mathcal{I}_G$. For M-mode Gaussian systems, it reads [7]:

$$\mathcal{C}^G_{rel}(\rho) := S(\rho \| \tau_M(\bar{\boldsymbol{n}}_\rho)) = -S(\rho) + \sum_{m=1}^{M} \left[(\bar{n}_m + 1)\log(\bar{n}_m + 1) - \bar{n}_m \log \bar{n}_m\right], \tag{33}$$

where $\bar{n}_m$ is the reduced average occupation number of ρ (see Eq. (9)), $\tau_M(\bar{\boldsymbol{n}}_\rho)$ represents the thermal state with the same $\bar{n}_m$ of ρ and the von-Neumann entropy $S(\rho)$ is given by Eq. (15).

4 Maximally coherent mixed states at fixed energy

Coherence is a basis-dependent quantity, therefore it is affected by unitary operations. For a given DV state ρ, the *maximally coherent mixed state* (MCMS) [29, 30] is defined as $\rho_{max} = V \rho V^\dagger$, where V is the unitary that maximises the coherence of ρ.

For CV systems, this definition is not applicable, since the coherence depends on the energy of the system. This can be seen, for instance, in Eq. (33) for the relative entropy of Gaussian coherence. Therefore, energy non-preserving unitaries can in principle increase the coherence indefinitely.

From an experimental point of view, energy-preserving unitaries are easier to realise and do not require interaction with an external source of energy.

This is the motivation to define a family of *maximally coherent mixed states at fixed energy*:

Definition 4.1. A state ρ_{max} is a *maximally coherent mixed state* (MCMS) *at fixed energy* with respect to a coherence monotone $\mathcal{C}$ (see Def. 3.1) if

$$\mathcal{C}(\rho_{max}) = \mathcal{C}_{max}(\rho) := \sup_{\hat{U}_{EP}} \mathcal{C}(\hat{U}_{EP}\, \rho\, \hat{U}^\dagger_{EP}), \tag{34}$$

where $\hat{U}_{EP}$ are energy-preserving unitaries. If we consider Gaussian states and operations in Eq. (34), then ρ_{max} is the *maximally coherent mixed Gaussian state* (MCMGS) *at fixed energy* with respect to $\mathcal{C}$.

Let us now focus on the Gaussian case. Passive Gaussian unitaries $\hat{U}_{\boldsymbol{O}}$ (see Def. 2.2) are the only energy-preserving Gaussian unitaries, i.e. they preserve $N_\omega = \sum_j \bar{n}_{\omega;j}$, and thus $N = \sum_\omega N_\omega$. However, the interaction between modes with the same frequency ω results in a redistribution of $\bar{n}_{\omega;j}$.

Let us consider a generic Gaussian state ρ and call $\rho_\omega = \mathrm{Tr}_{\boldsymbol{\omega}\setminus\omega}(\rho)$ the state obtained by tracing out all modes with any frequency but ω. From its definition in Eq. (28), the relative entropy of Gaussian coherence of ρ can be written as the sum of the relative entropies for all ρ_ω:

$$\mathcal{C}^G_{rel}(\rho) = \sum_{\omega=\omega_1}^{\omega_{M_f}} \mathcal{C}^G_{rel}(\rho_\omega). \tag{35}$$

Therefore, the maximal Gaussian coherence can be obtained by maximizing the Gaussian coherence for each ρ_ω.

Theorem 4.2. *Among all Gaussian states ρ_ω with a given symplectic spectrum $\{\nu_1, \ldots, \nu_{M_s}\}$ and a given average occupation number $N_\omega = \sum_j \bar{n}_{\omega;j}$, the states with equidistributed reduced average occupation numbers, i.e. $\bar{n}_{\omega;j} = N_\omega/M_s$, $\forall\, j$, are the maximally coherent mixed Gaussian states with respect to the relative entropy of Gaussian coherence $\mathcal{C}^G_{rel}(\rho_\omega)$ (see Eq. (33)).*

The proof is given in Appendix A, using Lagrange multipliers. Combining this result with Eq. (33), it follows that the maximal relative entropy of Gaussian coherence of a Gaussian state ρ reads

$$\begin{aligned}\mathcal{C}^G_{rel;\,max}(\rho) :=& S(\rho_{max}\|\tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})) \\ =& -S(\rho) + \sum_{\omega=\omega_1}^{\omega_{M_f}} \left[(N_\omega + M_s)\log\left(\frac{N_\omega + M_s}{M_s}\right) - N_\omega \log\left(\frac{N_\omega}{M_s}\right)\right],\end{aligned} \tag{36}$$

where $\tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})$ is the M-mode thermal state with occupation numbers $\bar{\boldsymbol{n}}_{\rho_{max}}$ (see Eq. (29)). In Appendix B, we provide an alternative analytical expression for $\mathcal{C}^G_{rel;\,max}$ (see Theorem 4.3), that will play a pivotal role in the next sections.

Theorem 4.3. *The maximal relative entropy of Gaussian coherence $\mathcal{C}^G_{rel;\,max}(\rho)$ of any Gaussian state ρ can be expressed as:*

$$\mathcal{C}^G_{rel;\,max}(\rho) = \sum_{\omega=\omega_1}^{\omega_{M_f}} S\left(\rho_\omega \,\middle\|\, \tau_{M_s}\left(\frac{N_\omega}{M_s}, \ldots, \frac{N_\omega}{M_s}\right)\right), \tag{37}$$

where $\tau_{M_s}(N_\omega/M_s, \ldots, N_\omega/M_s)$ is the thermal state (see Eq. (29)) with $\bar{n}_{\omega;j} = N_\omega/M_s$ for all $j = 1, 2, \ldots M_s$.

Finally, in Appendix C, we provide examples of passive unitaries that maximise the Gaussian coherence for two generic classes of Gaussian states.

5 Resource theory of (Gaussian) non-uniformity

The resource theory of purity (or non-uniformity) [9] belongs to a family of resource theories of quantum thermodynamics in which states out of some form of equilibrium are considered as resources [31–34]. Usually, this equilibrium is given by assuming the environment at a certain background temperature T: the free states are thermal states at the same temperature and the free operations are those which are generated by an energy-preserving unitary acting on the system and the environment.

For DV systems, the resource theory of purity arises when the Hamiltonian is fully degenerate at any temperature. Then all unitaries become energy preserving (hence free operations) and the exchanges between the system and the environment are purely entropic [9]. The state representing informational equilibrium becomes the maximally mixed state (MMS) $\boldsymbol{I}/d$, where d is the dimension of the system. The MMS is the only free state, as every other state possesses some non-uniformity.

The DV theory cannot be straightforwardly extended to Gaussian systems, because a proper MMS is nonphysical, as it is associated with infinite energy in infinite-dimensional Hilbert spaces [16].

While several resource theories of Gaussian states out of thermal equilibrium exist [22, 23, 35], we choose a different approach, that emphasises the informational aspects of the interactions between the system and the environment over the energetic ones. We consider purity at given energy as a resource and we refer to this resource theory as *non-uniformity*: with a similar argument as given by Gour et al [9], we use this term in place of "purity" because we shall consider pure states at different energy as states with different resource content.

Consider an M-mode state ρ, with M_f frequencies and M_s spatial labels (see Sec. 2). Consider also a Hamiltonian $\hat{H}$ in the form of Eq. (5). In terms of the frequencies its mean energy can be written as

$$\langle \hat{H} \rangle = \sum_{\omega=\omega_1}^{\omega_{M_f}} E_\omega, \tag{38}$$

where $E_\omega = \hbar\omega N_\omega$ (see Eq.(5)) and any other contribution is set to zero by a suitable choice for the zero-point energy. In the DV resource theory of purity, a dimension d for the set of all states was fixed. In our resource theory, we fix a set of frequencies $\omega = \omega_1, \omega_2, \ldots, \omega_{M_f}$ and the energy in each frequency mode E_ω, thus fixing $\langle \hat{H} \rangle$ as in Eq. (38). The states and modes can have any temperature that is compatible with E_ω, i.e. the thermal component of the energy cannot be higher than E_ω for any frequency sector.

For a single frequency ω, the state that maximises the entropy is the natural CV counterpart of the maximally mixed state in the DV case. We call it the *uniform state at frequency* ω. In our setting, with M_f different frequencies, we consider as free state the tensor product of all uniform states at frequency ω over all frequencies. We call it the *uniform state*.

From Eq. (9), we see that the average energy $E_\omega = \hbar\omega\, N_\omega$ is a function of the first and second moments of ρ, for both Gaussian and non-Gaussian states. It is well known that Gaussian states attain the maximum von-Neumann entropy among all states having the same displacement vector and covariance matrix [25]. Therefore, even if we consider the set of all CV states, we can search for the uniform state in the subset of Gaussian states.

For single-mode Gaussian systems at a fixed energy $E_\omega = \hbar\omega N_\omega$, the von-Neumann entropy is maximised by Gaussian thermal states with average occupation number N_ω [36]. For M_s spatial modes, we prove in Appendix D the following result:

Theorem 5.1. *For a quantum system of M_s spatial modes, the uniform state at frequency ω, i.e. the state that maximises the entropy, is the Gaussian thermal state (see Eq. (29)) with equal single-mode occupation numbers, i.e.*

$$\tau_{M_s}(\boldsymbol{\delta}_\omega) := \tau(\delta_\omega) \otimes \tau(\delta_\omega) \otimes \cdots \otimes \tau(\delta_\omega), \tag{39}$$

where $\boldsymbol{\delta}_\omega = (\delta_\omega, \delta_\omega, \ldots, \delta_\omega)$, $\delta_\omega := N_\omega/M_s$, and N_ω is the total occupation number for all spatial modes with frequency ω. Considering both spatial and frequency modes, the uniform state

becomes

$$\tau_M(\boldsymbol{\delta}) = \bigotimes_{\omega=\omega_1}^{\omega_{M_f}} \tau_{M_s}(\boldsymbol{\delta}_\omega), \tag{40}$$

where M_f is the total number of frequencies. The covariance matrix of $\tau_M(\boldsymbol{\delta})$ reads

$$\boldsymbol{V}\left[\tau_M(\boldsymbol{\delta})\right] = \bigoplus_{\omega=\omega_1}^{\omega_{M_f}} (2\delta_\omega + 1)\ \boldsymbol{I}_{2M_s}. \tag{41}$$

This result has an intuitive explanation. The von-Neumann entropy of a Gaussian state (see Eq. (15)) depends solely on the symplectic eigenvalues, and the m-th eigenvalue is a function of the m-th mode's temperature (see Eq. (14)). To maximise the entropy, we need to consider thermal states. Among thermal states, the uniform state is defined as the state with the most homogeneous distribution of single-mode energies.

Both the general and the Gaussian version of this resource theory have the same set of free states. We could, in principle, distinguish them via the set of free operations.

Definition 5.2. The *uniformity-preserving operations* (UP) are all maps that preserve the uniform state $\tau_M(\boldsymbol{\delta})$ (see Theorem 5.1), i.e.

$$\Lambda_{UP}(\tau_M(\boldsymbol{\delta})) = \tau_M(\boldsymbol{\delta}). \tag{42}$$

We call the Gaussian channels in UP the *uniformity-preserving Gaussian operations* (UPG).

Clearly $UPG \subseteq UP$, but we do not know whether this inclusion is strict. Concerning Gaussian operations, a more practical set of free operations is that of *Gaussian noisy operations* (GN), i.e. Gaussian channels Λ_{GN} that admit the following decomposition:

$$\Lambda_{GN}[\rho] = \mathrm{Tr}_{M_E}\left[\hat{U}_{\boldsymbol{O}}^{(M+M_E)}\ (\rho \otimes \tau_{M_E}(\boldsymbol{\delta}))\ \hat{U}_{\boldsymbol{O}}^{(M+M_E)\dagger}\right], \tag{43}$$

where $\tau_{M_E}(\boldsymbol{\delta})$ is the uniform state (see Theorem 5.1) for M_E environmental modes and with the same $\boldsymbol{\delta}$ of the system (see Eq.(40)), and $\hat{U}_{\boldsymbol{O}}^{(M+M_E)}$ is an $(M+M_E)$-mode passive Gaussian unitary.

Gaussian noisy operations preserve the equilibrium state. This can be seen in phase space representation, since, for every frequency sector, the covariance matrix of $\tau_M(\boldsymbol{\delta}) \otimes \tau_{M_E}(\boldsymbol{\delta})$ is proportional to the identity (see Eq. (41)), and the symplectic matrix of $\hat{U}_{\boldsymbol{O}}^{(M+M_E)}$ is orthogonal. Clearly, $GN \subseteq UPG$, but also here we do not know whether this inclusion is strict.

We introduce a quantifier for the resource of non-uniformity as follows:

Definition 5.3. A function $\mathcal{P}$, mapping density operators to real numbers, is a *non-uniformity monotone* if

(P1) $\mathcal{P}$ is non-negative and vanishes for the uniform state (see Theorem 5.1).

(P2) $\mathcal{P}$ does not increase under the chosen set of free operations, for instance UP (see Def. 5.2), i.e.

$$\mathcal{P}(\Lambda_{UP}(\rho)) \leq \mathcal{P}(\rho) \qquad \forall\, \Lambda_{UP}. \tag{44}$$

We define *Gaussian non-uniformity monotones* as those functions $\mathcal{P}^G$ satisfying (P1) and (P2) for uniformity-preserving Gaussian operations (see Def. 5.2).

In analogy with coherence, we introduce the *relative entropy of non-uniformity*:

$$\mathcal{P}_{rel}(\rho) := S\left(\rho \| \tau_M(\boldsymbol{\delta})\right). \tag{45}$$

This function clearly satisfies (P1). The property (P2) follows from the contractivity of the relative entropy,

$$\mathcal{P}_{rel}(\rho) = S\left(\rho \,\|\, \tau_M(\boldsymbol{\delta})\right) \geq S(\Lambda_{UP}[\rho] \,\|\, \Lambda_{UP}[\tau_M(\boldsymbol{\delta})]) = S(\Lambda_{UP}[\rho] \,\|\, \tau_M(\boldsymbol{\delta})) = \mathcal{P}_{rel}(\Lambda_{UP}[\rho]). \tag{46}$$

Restricting ourselves to Gaussian states and operations, we find results for the relative entropy of Gaussian non-uniformity $\mathcal{P}^G_{rel}(\rho)$ (that is the relative entropy of non-uniformity for Gaussian states).

Theorem 5.4. *The relative entropy of Gaussian non-uniformity (see Eq.* (45)*) of a Gaussian state ρ is equal to its maximal coherence (see Eq.* (36)*):*

$$\mathcal{P}^G_{rel}(\rho) = \mathcal{C}^G_{rel;\, max}(\rho). \tag{47}$$

This result follows from Theorem 4.3:

$$\mathcal{C}^G_{rel;\, max}(\rho) = \sum_{\omega=\omega_1}^{\omega_{M_f}} S\left(\rho_\omega \,\middle\|\, \tau_{M_s}\left(\frac{N_\omega}{M_s}, \ldots, \frac{N_\omega}{M_s}\right)\right) = S\left(\rho \| \tau_M(\boldsymbol{\delta})\right) = \mathcal{P}_{rel}(\rho), \tag{48}$$

and establishes a strong connection between coherence and non-uniformity for Gaussian systems, in analogy to DV systems [10].

We conclude this section by noticing two additional properties of the relative entropy of Gaussian non-uniformity, which can be found by employing Theorem 5.4:

- Pure Gaussian states $|\psi_G\rangle\langle\psi_G|$ maximise the relative entropy of Gaussian non-uniformity among the states with given average occupation number N_ω and total number of spatial modes M_s:

$$\begin{aligned} \mathcal{P}^G_{rel}(|\psi_G\rangle\langle\psi_G|) &= S(|\psi_G\rangle\langle\psi_G| \,\|\, \tau_M(\boldsymbol{\delta})) \\ &= \sum_{\omega=\omega_1}^{\omega_{M_f}} \left[(N_\omega + M_s)\, \log\left(\frac{N_\omega}{M_s} + 1\right) - N_\omega \log \frac{N_\omega}{M_s}\right], \end{aligned} \tag{49}$$

  which follows from Eq. (33).

- The relative entropy of Gaussian non-uniformity is invariant under passive Gaussian unitaries, i.e.

$$\mathcal{P}^G_{rel}(\rho) = \mathcal{P}^G_{rel}(\hat{U}_{\boldsymbol{O}}\, \rho\, \hat{U}^\dagger_{\boldsymbol{O}}) \tag{50}$$

  This property follows by noticing that the maximal Gaussian coherence cannot be increased via passive Gaussian unitaries (see Eq. (34)).

6 Hierarchy of quantum resources in CV systems

The relative entropy also quantifies, for CV systems, multipartite entanglement [18] and symmetric quantum discord [37, 38]:

$$\mathcal{D}_{rel}(\rho) = \inf_{\sigma\in\mathcal{Z}} S(\rho\|\sigma), \tag{51}$$

$$\mathcal{E}_{rel}(\rho) = \inf_{\sigma\in\mathcal{S}} S(\rho\|\sigma), \tag{52}$$

where $\mathcal{Z}$ and $\mathcal{S}$ denote the sets of zero-discord and separable states, respectively. The former contains all mixtures of pure, locally orthonormal projectors [37, 39], while the latter contains all convex combinations of arbitrary product states [36], i.e.

$$\mathcal{Z} \ni \rho = \sum_{\boldsymbol{m}} p_{\boldsymbol{m}} \left|\psi_{m_1}\right\rangle\left\langle\psi_{m_1}\right| \otimes \left|\psi_{m_2}\right\rangle\left\langle\psi_{m_2}\right| \otimes \cdots \otimes \left|\psi_{m_M}\right\rangle\left\langle\psi_{m_M}\right|, \tag{53}$$

$$\mathcal{S} \ni \rho = \sum_{\boldsymbol{m}} p_{\boldsymbol{m}}\, \rho_{m_1} \otimes \rho_{m_2} \otimes \cdots \otimes \rho_{m_M}, \tag{54}$$

where $\langle\psi_{m_k}|\psi_{l_k}\rangle = \delta_{ml}$ for all $k = 1, \ldots, M$, $\boldsymbol{m} := m_1 m_2 \ldots m_M$, $p_{\boldsymbol{m}} \geq 0$ and $\sum_{\boldsymbol{m}} p_{m_1 m_2 \ldots m_M} = 1$. Note that $\mathcal{Z}$ is non-convex, since the convex combination of two sets of orthonormal projectors is not, in general, orthonormal.

Using the relative entropy, we can extend the ordering of resources for discrete-variable to continuous-variable systems:

$$\mathcal{P}_{rel}(\rho) \geq \mathcal{C}_{rel}(\rho) \geq \mathcal{D}_{rel}(\rho) \geq \mathcal{E}_{rel}(\rho). \tag{55}$$

This relation directly follows by noting that $\tau_M(\boldsymbol{\delta}) \in \mathcal{I} \subset \mathcal{Z} \subset \mathcal{S}$, and holds for all quantum states ρ (see Fig. 2).

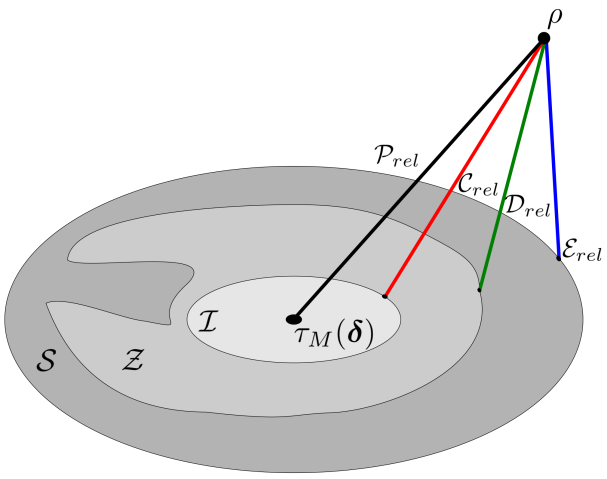

Figure 2: Graphical depiction of the relative entropy of non-uniformity $\mathcal{P}_{rel}$ (black line), coherence $\mathcal{C}_{rel}$ (red line), symmetric quantum discord $\mathcal{D}_{rel}$ (green line) and entanglement $\mathcal{E}_{rel}$ (blue line) for a quantum state ρ. The uniform state $\tau_M(\boldsymbol{\delta})$ is an element of the incoherent set $\mathcal{I}$, which is a convex subset of the zero-discord set $\mathcal{Z}$, which in turn is a non-convex subset of the separable set $\mathcal{S}$.

Let us now consider the Gaussian case. Let $\mathcal{D}^G_{rel}$ and $\mathcal{E}^G_{rel}$ be the relative entropies of Gaussian discord and entanglement, respectively. They are obtained with Eq. (51) and (52) by performing the minimization over the Gaussian subsets $\mathcal{Z}_G$ and $\mathcal{S}_G$ of $\mathcal{Z}$ and $\mathcal{S}$, respectively. While $\mathcal{S}_G$ is defined analogously to Eq. (54), by taking Gaussian states, $\mathcal{Z}_G$ is formed by product Gaussian states [38, 40], i.e.

$$\mathcal{Z}_G \ni \rho = \rho_{m_1} \otimes \rho_{m_2} \otimes \cdots \otimes \rho_{m_M}, \tag{56}$$

$$\mathcal{S}_G \ni \rho = \sum_{\boldsymbol{m}} p_{\boldsymbol{m}}\, \rho_{m_1} \otimes \rho_{m_2} \otimes \cdots \otimes \rho_{m_M}, \tag{57}$$

where $\rho_{m_1}, \rho_{m_2} \ldots, \rho_{m_M}$ and ρ are Gaussian states, and with $\boldsymbol{m} := m_1 m_2 \ldots m_M$, $p_{\boldsymbol{m}} \geq 0$ and $\sum_{\boldsymbol{m}} p_{\boldsymbol{m}} = 1$ in Eq. (57). Since $\tau_M(\boldsymbol{\delta}) \in \mathcal{I}_G \subset \mathcal{Z}_G \subset \mathcal{S}_G$, Eq. (55) holds also in this case.

We have discussed in Sec. 4 how passive unitaries can generate coherence. It is well established that they can also generate entanglement [41] and discord [42].

Let us introduce

$$\mathcal{D}^G_{rel;\, max}(\rho) := \sup_{\hat{U}_{\boldsymbol{O}}} \mathcal{D}^G_{rel}(\hat{U}_{\boldsymbol{O}}\, \rho\, \hat{U}^\dagger_{\boldsymbol{O}}), \tag{58}$$

$$\mathcal{E}^G_{rel;\, max}(\rho) := \sup_{\hat{U}_{\boldsymbol{O}}} \mathcal{E}^G_{rel}(\hat{U}_{\boldsymbol{O}}\, \rho\, \hat{U}^\dagger_{\boldsymbol{O}}). \tag{59}$$

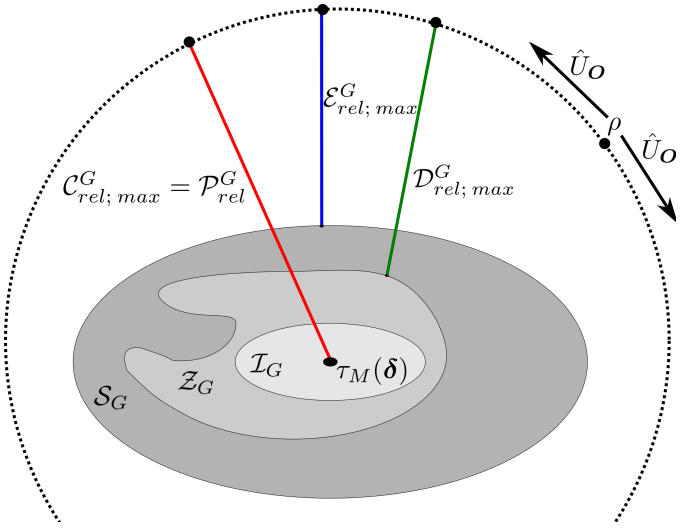

Figure 3: Graphical depiction of Eq. (60). The dotted circle represents all the states that can be obtained from ρ via passive unitaries $\hat{U}_{\boldsymbol{O}}$. The red line, connecting the uniform state $\tau_M(\boldsymbol{\delta})$ to the MCMGS, is the maximal Gaussian coherence $\mathcal{C}^G_{rel;\, max}(\rho) = \mathcal{P}^G_{rel}(\rho)$. The green and blue lines are the maximal Gaussian discord $\mathcal{D}^G_{rel;\, max}$ and entanglement $\mathcal{E}^G_{rel;\, max}$, respectively. The uniform state $\tau_M(\boldsymbol{\delta})$ is an element of the Gaussian incoherent set $\mathcal{I}_G$, which is a convex subset of the Gaussian zero-discord set $\mathcal{Z}_G$, which in turn is a non-convex subset of the Gaussian separable set $\mathcal{S}_G$.

We prove in Appendix E the following hierarchy between the mentioned CV resources (see Fig. 3):

Theorem 6.1. *The relative entropy of Gaussian non-uniformity $\mathcal{P}^G_{rel}$ (Eq. (45)) of any Gaussian state ρ is equal to the maximal relative entropy of Gaussian coherence $\mathcal{C}^G_{rel;\,max}$ (Eq. (36)), and this quantity upperbounds the maximal relative entropies of Gaussian symmetric discord $\mathcal{D}^G_{rel;\,max}$ (Eq. (58)) and Gaussian entanglement $\mathcal{E}^G_{rel;\,max}$ (Eq. (59)):*

$$\mathcal{P}^G_{rel}(\rho) = \mathcal{C}^G_{rel;\,max}(\rho) \geq \mathcal{D}^G_{rel;\,max}(\rho) \geq \mathcal{E}^G_{rel;\,max}(\rho). \tag{60}$$

Here we discussed the action of energy-preserving unitaries, in particular passive Gaussian unitaries. An energy non-preserving unitary can, in principle, increase the energy indefinetely and create infinite resources. However, for a fixed finite energy, the ordering of Eq. (55) is preserved, because the ordering of the sets remains. In the Gaussian scenario, we conjecture that active unitaries exist that keep the hierarchic ordering in Eq. (60). The verification of this claim is an interesting open question.

7 Conclusions

In this manuscript, we extended a hierarchy of dicrete-variable quantum resources to continuous-variable systems, under the condition of fixed energy. Considering Gaussian states and operations and using quantifiers based on the relative entropy, we found that the Gaussian non-uniformity is equal to the maximal Gaussian coherence, and we provided an analytical expression for this quantity. This means that, if we quantify the resources with the relative entropy, any amount of Gaussian non-uniformity can be converted into Gaussian coherence by means of a suitable energy-preserving Gaussian unitary. To quantify the non-uniformity, we designed a resource theory by identifying purity at fixed energy as resource. We also considered generic (non-Gaussian) states and found that the non-uniformity always upper-bounds the coherence. Finally, we showed that, for Gaussian states the non-uniformity and the maximal coherence provide upper bounds on the maximal symmetric quantum discord and the maximal entanglement. Our results advance the field of continuous-variable resource theories and establish a further connection between quantum thermodynamics and quantum information theory.

Our work leaves some interesting questions open. A possible next step could be to study the hierarchy of resources in the presence of energy-nonpreserving Gaussian unitaries, up to a finite maximum energy. In addition, one should investigate whether the equality of maximal coherence and non-uniformity also holds in the general non-Gaussian case. In order to achieve this a deeper understanding of non-Gaussian resource theories is required.

Acknowledgements

DB acknowledges inspiring discussions with participants of the Central-European Workshop on Quantum Optics (CEWQO 2019) in Paderborn, in particular with Christine Silberhorn. This research was partially supported by the German Federal Ministry of Education and Research (BMBF), within the project HQS, and by the EU H2020 QuantERA ERA-NET Cofund in Quantum Technologies, within the project QuICHE.

A Proof of Theorem 4.2

For simplicity of notation, we shall drop in the proof the subscript ω in $\bar{n}_{\omega;j}$, ρ_ω and N_ω.

The theorem can be proven with a constrained optimization. Let $\boldsymbol{n} = \{\bar{n}_1, \ldots, \bar{n}_{M_s}\}$ and $\mathcal{L}(\boldsymbol{n}, \lambda)$ be the Lagrangian function

$$\begin{aligned}\mathcal{L}(\boldsymbol{n}, \lambda) :=& \mathcal{C}^G_{rel}(\rho; \boldsymbol{n}) - \lambda \left(N - \sum_{j=1}^{M_s} \bar{n}_j \right) \\ =& S(\rho) + \sum_{j=1}^{\tilde{M}_s} \left[(\bar{n}_j + 1) \log(\bar{n}_j + 1) - \bar{n}_j \log \bar{n}_j \right] + \lambda \sum_{j=1}^{\tilde{M}_s} \bar{n}_j - \lambda N,\end{aligned} \tag{61}$$

where $\tilde{M}_s$ is the number of modes for which $\bar{n}_j \neq 0$. Since $S(\rho)$ depends only on the symplectic spectrum (see Eq. 15), it holds

$$\frac{\partial \mathcal{L}(\boldsymbol{n}, \lambda)}{\partial \bar{n}_j} = \begin{cases} \log\left(\frac{\bar{n}_j + 1}{\bar{n}_j}\right) + \lambda & \text{for } \bar{n}_j \neq 0 \\ 0 & \text{for } \bar{n}_j = 0 \end{cases} \tag{62}$$

The condition $\partial \mathcal{L} / \partial \bar{n}_j = 0$ for $\bar{n}_j \neq 0$ is equivalent to

$$\lambda = -\log\left(\frac{\bar{n}_j + 1}{\bar{n}_j}\right), \qquad \forall j \tag{63}$$

The above relations are satisfied by any state ρ^* with $\tilde{M}_s$ reduced occupation numbers $\bar{n}_j = N/\tilde{M}_s \quad \forall\, j = 1, \ldots \tilde{M}_s$ and the others equal to zero. Clearly $1 \leq \tilde{M}_s \leq M_s$.

The Gaussian coherence of any ρ^* reads:

$$\mathcal{C}^G_{rel}(\rho^*) = -S(\rho^*) + (N + \tilde{M}_s) \log\left(\frac{N + \tilde{M}_s}{\tilde{M}_s}\right) - N \log\left(\frac{N}{\tilde{M}_s}\right). \tag{64}$$

Taking the derivative of this expression with respect to $\tilde{M}_s$, i.e.

$$\frac{d\mathcal{C}^G_{rel}(\rho^*)}{d\tilde{M}_s} = \log\left(\frac{N + \tilde{M}_s}{\tilde{M}_s}\right) > 0, \tag{65}$$

one can verify that this function is monotonically increasing with $\tilde{M}_s$.

The minimum is therefore obtained for $\tilde{M}_s = 1$, i.e. when N is contained in a single reduced spatial mode, and the maximum is obtained for $\tilde{M}_s = M_s$, i.e. when N is equally distributed.

B Proof of Theorem 4.3

Let $\hat{U}_{\mathcal{C}} = \bigotimes_{\omega=\omega_1}^{\omega_{M_f}} \hat{U}_{\mathcal{C}\omega}$ be the passive unitary that maximises the relative entropy of Gaussian coherence for ρ, i.e.

$$\rho_{max} = \hat{U}_{\mathcal{C}}\, \rho\, \hat{U}^\dagger_{\mathcal{C}} = \bigotimes_{\omega=\omega_1}^{\omega_{M_f}} \hat{U}_{\mathcal{C}\omega}\, \rho_\omega\, \hat{U}^\dagger_{\mathcal{C}\omega}. \tag{66}$$

Let $\tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})$ be the thermal state with the same $\bar{n}_{\omega;j}$ as ρ_{max}. Using Theorem 4.2, $\tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})$ reads

$$\tau_M(\bar{\boldsymbol{n}}_{\rho_{max}}) := \bigotimes_{\omega=\omega_1}^{\omega_{M_f}} \tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}}), \qquad \bar{\boldsymbol{n}}^\omega_{\rho_{max}} := \left(\frac{N_\omega}{M_s}, \frac{N_\omega}{M_s}, \ldots, \frac{N_\omega}{M_s}\right). \tag{67}$$

Using Eq. (33) we get

$$\begin{aligned}\mathcal{C}^G_{rel}(\rho_{max}) =& S\left(\rho_{max} \,\|\, \tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})\right) = -S(\rho_{max}) + \mathrm{Tr}\left[\rho_{max} \log\, \tau_M(\bar{\boldsymbol{n}}_{\rho_{max}})\right] = \\ =& -S(\rho) + \sum_{\omega=\omega_1}^{\omega_{M_f}} \mathrm{Tr}\left[\hat{U}_{\mathcal{C}\omega}\, \rho_\omega\, \hat{U}^\dagger_{\mathcal{C}\omega}\, \log\, \tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})\right] \\ =& -S(\rho) + \sum_{\omega=\omega_1}^{\omega_{M_f}} \mathrm{Tr}\left[\rho_\omega\, \log\, \left(\hat{U}^\dagger_{\mathcal{C}\omega}\, \tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})\, \hat{U}_{\mathcal{C}\omega}\right)\right].\end{aligned} \tag{68}$$

Here, we have used the invariance of entropy under unitary operation and the diagonality of $\tau(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})$ in the Fock basis. We then notice that

$$\hat{U}^\dagger_{\mathcal{C}\omega}\, \tau_{M_s}\left(\bar{\boldsymbol{n}}^\omega_{\rho_{max}}\right)\, \hat{U}_{\mathcal{C}\omega} = \tau_{M_s}\left(\bar{\boldsymbol{n}}^\omega_{\rho_{max}}\right). \tag{69}$$

This can be proven by using the phase space representation, since the covariance matrix of $\tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})$ is proportional to the identity (consider equal $\bar{n}_m$ in Eq. (30)), and passive Gaussian unitaries are associated to symplectic orthogonal matrices, by Def. 2.2. It follows that

$$\begin{aligned}\mathcal{C}^G_{rel}(\rho_{max}) =& -S(\rho) + \sum_{\omega=\omega_1}^{\omega_{M_f}} \mathrm{Tr}\left(\rho_\omega\, \log\, \tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})\right) \\ =& -\sum_{\omega=\omega_1}^{\omega_{M_f}} S(\rho_\omega) + \sum_{\omega=\omega_1}^{\omega_{M_f}} \mathrm{Tr}\left(\rho_\omega\, \log\, \tau_{M_s}(\bar{\boldsymbol{n}}^\omega_{\rho_{max}})\right) \\ =& \sum_{\omega=\omega_1}^{\omega_{M_f}} S\left(\rho_\omega \,\middle\|\, \tau_{M_s}\left(\frac{N_\omega}{M_s}, \ldots, \frac{N_\omega}{M_s}\right)\right).\end{aligned} \tag{70}$$

C Maximal Gaussian coherence for specific states

In this section, we will consider modes with the same frequency and drop the subscript ω. By Theorem 4.2, we can search for a passive unitary that equally distributes the average occupation number N of a Gaussian state ρ among its modes: this unitary maximises the relative entropy of coherence of ρ.

As a first case, let us consider a generic two-mode Gaussian state ρ, with mode operators $\hat{a}_1$ and $\hat{a}_2$. We now apply a $50:50$ beam splitter of phase ϕ (to be specified later):

$$\begin{aligned}\hat{a}_1 \mapsto \hat{b}_1 &= \frac{1}{\sqrt{2}}\, \hat{a}_1 + \frac{e^{\mathrm{i}\phi}}{\sqrt{2}}\, \hat{a}_2 \\ \hat{a}_2 \mapsto \hat{b}_2 &= \frac{1}{\sqrt{2}}\, \hat{a}_2 - \frac{e^{-\mathrm{i}\phi}}{\sqrt{2}}\, \hat{a}_1\end{aligned} \tag{71}$$

Then we have

$$
\begin{aligned}
\langle \hat{b}_1^\dagger \hat{b}_1 \rangle &= \frac{1}{2} \langle \hat{a}_1^\dagger \hat{a}_1 \rangle + \frac{1}{2} \langle \hat{a}_2^\dagger \hat{a}_2 \rangle + \frac{e^{\mathrm{i}\phi}}{2} \langle \hat{a}_1^\dagger \hat{a}_2 \rangle + \frac{e^{-\mathrm{i}\phi}}{2} \langle \hat{a}_1 \hat{a}_2^\dagger \rangle \\
&= \frac{N}{2} + \mathrm{Re}\left(e^{-\mathrm{i}\phi} \langle \hat{a}_1 \hat{a}_2^\dagger \rangle \right) \\
\langle \hat{b}_2^\dagger \hat{b}_2 \rangle &= \frac{1}{2} \langle \hat{a}_2^\dagger \hat{a}_2 \rangle + \frac{1}{2} \langle \hat{a}_1^\dagger \hat{a}_1 \rangle - \frac{e^{-\mathrm{i}\phi}}{2} \langle \hat{a}_2^\dagger \hat{a}_1 \rangle - \frac{e^{\mathrm{i}\phi}}{2} \langle \hat{a}_2 \hat{a}_1^\dagger \rangle \\
&= \frac{N}{2} - \mathrm{Re}\left(e^{-\mathrm{i}\phi} \langle \hat{a}_1 \hat{a}_2^\dagger \rangle \right).
\end{aligned}
\tag{72}
$$

With $\langle \hat{a}_1 \hat{a}_2^\dagger \rangle = |\langle \hat{a}_1 \hat{a}_2^\dagger \rangle| e^{\mathrm{i}\theta_{12}}$, we can choose $\phi = \frac{\pi}{2} - \theta_{12}$, leading to $\langle \hat{b}_1^\dagger \hat{b}_1 \rangle = \langle \hat{b}_2^\dagger \hat{b}_2 \rangle = N/M_s$ (in this case $M_s = 2$), thus maximising the coherence.

Let us now consider a generic M_s-mode product state $\rho = \varrho_1 \otimes \cdots \otimes \varrho_{M_s}$ with $\boldsymbol{d} = 0$. We prove that the *quantum Fourier transform* (QFT)

$$
\hat{a}_j \mapsto \hat{b}_j := \sum_{k=1}^{M_s} U_{jk} \, \hat{a}_{jk} = \frac{1}{\sqrt{M_s}} \sum_{k=1}^{M_s} e^{\frac{2\pi\,\mathrm{i}}{M_s}(j-1)(k-1)} \, \hat{a}_j \tag{73}
$$

is the passive Gaussian unitary that maximises the coherence. After the action of the QFT, the occupation number for the mode j reads

$$
\langle \hat{b}_j^\dagger \, \hat{b}_j \rangle = \frac{1}{M_s} \sum_{k,k'=1}^{M_s} e^{\frac{2\pi\,\mathrm{i}}{M_s}(j-1)(k'-k)} \, \langle \hat{a}_k^\dagger \, \hat{a}_{k'} \rangle \, . \tag{74}
$$

We separate the sum into two parts, with $k = k'$ and $k \neq k'$:

$$
\begin{aligned}
\langle \hat{b}_j^\dagger \, \hat{b}_j \rangle =& \frac{1}{M_s} \sum_{k=1}^{M_s} \langle \hat{a}_k^\dagger \, \hat{a}_k \rangle + \frac{1}{M_s} \sum_{k \neq k'} e^{\frac{2\pi\,\mathrm{i}}{M_s}(j-1)(k'-k)} \, \langle \hat{a}_k^\dagger \, \hat{a}_{k'} \rangle \\
=& \frac{N}{M_s} + \frac{1}{M_s} \sum_{k \neq k'} e^{\frac{2\pi\,\mathrm{i}}{M_s}(j-1)(k'-k)} \, \langle \hat{a}_k^\dagger \, \hat{a}_{k'} \rangle \, .
\end{aligned}
\tag{75}
$$

Since ρ is a product state and $\boldsymbol{d} = 0$, we conclude the proof by noticing

$$
\langle \hat{a}_k^\dagger \, \hat{a}_{k'} \rangle = \langle \hat{a}_k^\dagger \rangle \, \langle \hat{a}_{k'} \rangle = 0. \tag{76}
$$

Remarkably, this transformation is an extension of the DV unitary to CV. The unitary that maximises the coherence of an arbitrary DV state ρ for any MIO monotone reads [10]

$$
\hat{U}_{max}^{DV} = \frac{1}{\sqrt{d}} \sum_{n=1}^{d} \sum_{k=1}^{d} e^{\frac{2\pi\,\mathrm{i}}{M_s}(n-1)(k-1)} \, |k\rangle \, \langle \rho_n| \, , \tag{77}
$$

where d is the dimension of ρ, $|\rho_n\rangle$ are the eigenstates of ρ, and $|k\rangle$ are the elements of the incoherent basis. Notice, however, that the CV result only holds for product states with $\boldsymbol{d} = 0$.

D Proof of Theorem 5.1

This proof is similar to that of Theorem 4.2, and also here we drop the subscript ω in $\bar{n}_{\omega;j}$ and N_ω.

The covariance matrix of a Gaussian thermal state (see Eq. (30)) is diagonal and coincides with the diagonal matrix $\boldsymbol{D}$ in Williamson's theorem (see Eq. (11)). From Eq. (15), it follows that the von-Neumann entropy of $\tau_{M_s}(\bar{\boldsymbol{n}})$ reads

$$S\left(\tau_{M_s}(\bar{\boldsymbol{n}})\right) = \sum_{j=1}^{\tilde{M}_s} \left[(\bar{n}_j + 1)\,\log(\bar{n}_j + 1) - \bar{n}_j\,\log \bar{n}_j\right], \tag{78}$$

where $\boldsymbol{n} = (\bar{n}_1, \ldots, \bar{n}_{M_s})$ and $\tilde{M}_s$ is the number of modes for which $\bar{n}_j \neq 0$. Let $\mathcal{L}(\boldsymbol{n}, \lambda)$ be the Lagrangian function

$$\begin{aligned}\mathcal{L}(\boldsymbol{n}, \lambda) :=& S\left(\tau_{M_s}(\bar{\boldsymbol{n}})\right) - \lambda \left(N - \sum_{j=1}^{\tilde{M}_s} \bar{n}_j\right) \\ =& \sum_{j=1}^{\tilde{M}_s} \left[(\bar{n}_j + 1)\log(\bar{n}_j + 1) - \bar{n}_j \log \bar{n}_j\right] + \lambda \sum_{j=1}^{\tilde{M}_s} \bar{n}_j - \lambda N,\end{aligned} \tag{79}$$

It holds

$$\frac{\partial \mathcal{L}(\boldsymbol{n}, \lambda)}{\partial \bar{n}_j} = \begin{cases} \log\left(\frac{\bar{n}_j + 1}{\bar{n}_j}\right) + \lambda & \text{for } \bar{n}_j \neq 0 \\ 0 \qquad \text{for } \bar{n}_j = 0 \end{cases} \tag{80}$$

The condition $\partial \mathcal{L}/\partial \bar{n}_j = 0$ for $\bar{n}_j \neq 0$ is equivalent to

$$\lambda = -\log\left(\frac{\bar{n}_j + 1}{\bar{n}_j}\right), \qquad \forall\, j. \tag{81}$$

The above relations are satisfied by any state $\tau_{M_s}(\bar{\boldsymbol{n}}^*)$ with $\tilde{M}_s$ reduced occupation numbers $\bar{n}_j = N/\tilde{M}_s \quad \forall\, j = 1, \ldots \tilde{M}_s$ and the others equal to zero. Clearly $1 \leq \tilde{M}_s \leq M_s$.

The entropy of any $\tau_{M_s}(\bar{\boldsymbol{n}}^*)$ reads:

$$S\left(\tau_{M_s}(\bar{\boldsymbol{n}}^*)\right) = (N + \tilde{M}_s)\log\left(\frac{N + \tilde{M}_s}{\tilde{M}_s}\right) - N\log\left(\frac{N}{\tilde{M}_s}\right). \tag{82}$$

Taking the derivative of this expression with respect to $\tilde{M}_s$

$$\frac{dS\left(\tau_{M_s}(\bar{\boldsymbol{n}}^*)\right)}{d\tilde{M}_s} = \log\left(\frac{N + \tilde{M}_s}{\tilde{M}_s}\right) > 0, \tag{83}$$

one can verify that this function is monotonically increasing with $\tilde{M}_s$.

The minimum is therefore obtained for $\tilde{M}_s = 1$, i.e. when N is contained in a single reduced spatial mode, and the maximum is obtained for $\tilde{M}_s = M_s$, i.e. when N is equally distributed.

E Proof of Eq. (60)

Let $\hat{U}_{\mathcal{E}}$ be the passive Gaussian unitary that achieves $\mathcal{E}^G_{rel;\,max}(\rho)$ in Eq. (59). Then we have

$$\begin{aligned}\mathcal{E}^G_{rel;\,max}(\rho) &= \mathcal{E}^G_{rel}\left(\hat{U}_{\mathcal{E}}\,\rho\,\hat{U}^\dagger_{\mathcal{E}}\right) \leq \mathcal{D}^G_{rel}\left(\hat{U}_{\mathcal{E}}\,\rho\,\hat{U}^\dagger_{\mathcal{E}}\right) \\ &\leq \sup_{\hat{U}_{\boldsymbol{O}}} \mathcal{D}^G_{rel}\left(\hat{U}_{\boldsymbol{O}}\,\rho\,\hat{U}^\dagger_{\boldsymbol{O}}\right) = \mathcal{D}^G_{rel;\,max}(\rho).\end{aligned} \tag{84}$$

Similarly, let $\hat{U}_{\mathcal{D}}$ be the Gaussian unitary that achieves $\mathcal{D}^G_{rel;\,max}(\rho)$ in Eq. (58). Then

$$\begin{aligned}\mathcal{D}^G_{rel;\,max}(\rho) &= \mathcal{D}^G_{rel}\left(\hat{U}_{\mathcal{D}}\,\rho\,\hat{U}^\dagger_{\mathcal{D}}\right) \leq \mathcal{C}^G_{rel}\left(\hat{U}_{\mathcal{D}}\,\rho\,\hat{U}^\dagger_{\mathcal{D}}\right) \\ &\leq \sup_{\hat{U}_{\boldsymbol{O}}} \mathcal{C}^G_{rel}\left(\hat{U}_{\boldsymbol{O}}\,\rho\,\hat{U}^\dagger_{\boldsymbol{O}}\right) = \mathcal{C}^G_{rel;\,max}(\rho).\end{aligned} \tag{85}$$

Finally, using $\mathcal{C}^G_{rel}(\rho_{max}) = \mathcal{P}^G_{rel}(\rho)$ from Theorem 5.4, we obtain the desired result.

References

[1] Eric Chitambar and Gilad Gour. "Quantum resource theories". In: *Rev. Mod. Phys.* 91.025001 (2019).

[2] Johan Åberg. "Quantifying superposition". In: *arXiv preprint quant-ph/0612146* (2006).

[3] Tillmann Baumgratz, Marcus Cramer, and Martin B Plenio. "Quantifying coherence". In: *Phys. Rev. Lett.* 113.140401 (2014).

[4] Iman Marvian and Robert W. Spekkens. "How to quantify coherence: Distinguishing speakable and unspeakable notions". In: *Phys. Rev. A* 94.052324 (2016).

[5] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. "Colloquium: Quantum coherence as a resource". In: *Rev. Mod. Phys.* 89.041003 (2017).

[6] Yu-Ran Zhang et al. "Quantifying coherence in infinite-dimensional systems". In: *Phys. Rev. A* 93.012334 (2016).

[7] Jianwei Xu. "Quantifying coherence of Gaussian states". In: *Phys. Rev. A* 93.032111 (2016).

[8] Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. "Reversible transformations from pure to mixed states and the unique measure of information". In: *Phys. Rev. A* 67.062104 (2003).

[9] Gilad Gour et al. "The resource theory of informational nonequilibrium in thermodynamics". In: *Phys. Rep.* 583.1 (2015).

[10] Alexander Streltsov et al. "Maximal coherence and the resource theory of purity". In: *New J. Phys.* 20.053058 (2018).

[11] Marco G. Genoni, Matteo G. A. Paris, and Konrad Banaszek. "Quantifying the non-Gaussian character of a quantum state by quantum relative entropy". In: *Phys. Rev. A* 78.060303 (2008).

[12] V. Vedral and M. B. Plenio. "Entanglement measures and purification procedures". In: *Phys. Rev. A* 57.1619 (1998).

[13] Stefano Olivares. "Quantum optics in the phase space". In: *Eur. Phys. J. ST* 203.3 (2012).

[14] Christian Weedbrook et al. "Gaussian quantum information". In: *Rev. Mod. Phys.* 84.621 (2012).

[15] Gerardo Adesso, Sammy Ragy, and Antony R Lee. "Continuous variable quantum information: Gaussian states and beyond". In: *Open Syst. Inf. Dyn.* 21.1440001 (2014).

[16] Alessio Serafini. *Quantum continuous variables: a primer of theoretical methods*. CRC press, 2017.

[17] Ludovico Lami et al. "Gaussian quantum resource theories". In: *Phys. Rev. A* 98.022335 (2018).

[18] Jens Eisert, Christoph Simon, and Martin B Plenio. "On the quantification of entanglement in infinite-dimensional quantum systems". In: *J. Phys. A Math. Gen.* 35.3911 (2002).

[19] Michael Keyl, Dirk Schlingemann, and Reinhard F Werner. "Infinitely entangled states". In: *arXiv preprint quant-ph/0212014* (2002).

[20] Koenraad MR Audenaert and Jens Eisert. "Continuity bounds on the quantum relative entropy". In: *J. Math. Phys.* 46.102104 (2005).

[21] Koenraad MR Audenaert and Jens Eisert. "Continuity bounds on the quantum relative entropy—II". In: *J. Math. Phys.* 52.112201 (2011).

[22] A Serafini et al. "Gaussian thermal operations and the limits of algorithmic cooling". In: *Phys. Rev. Lett.* 124.010602 (2020).

[23] Varun Narasimhachar et al. "Thermodynamic resources in continuous-variable quantum systems". In: *npj Quantum Inf.* 7.1 (2021).

[24] John Williamson. "On the algebraic problem concerning the normal forms of linear dynamical systems". In: *Am. J. Math.* 58.1 (1936).

[25] Alexander S Holevo, Masaki Sohma, and Osamu Hirota. "Capacity of quantum Gaussian channels". In: *Phys. Rev. A* 59.1820 (1999).

[26] Biswadeb Dutta, N Mukunda, R Simon, et al. "The real symplectic groups in quantum mechanics and optics". In: *Pramana* 45.6 (1995).

[27] Claude Fabre and Nicolas Treps. "Modes and states in quantum optics". In: *Rev. Mod. Phys.* 92.035005 (2020).

[28] Alexander S Holevo and Reinhard F Werner. "Evaluating capacities of bosonic Gaussian channels". In: *Phys. Rev. A* 63.032312 (2001).

[29] Uttam Singh et al. "Maximally coherent mixed states: Complementarity between maximal coherence and mixedness". In: *Phys. Rev. A* 91.052115 (2015).

[30] Yao Yao et al. "Maximal coherence in a generic basis". In: *Phys. Rev. A* 94.062339 (2016).

[31] Dominik Janzing et al. "Thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the second law". In: *Int. J. Theor. Phys.* 39.12 (2000).

[32] Fernando G. S. L. Brandão et al. "Resource Theory of Quantum States Out of Thermal Equilibrium". In: *Phys. Rev. Lett.* 111.250404 (2013).

[33] Matteo Lostaglio. "An introductory review of the resource theory approach to thermodynamics". In: *Rep. Prog. Phys.* 82.114001 (2019).

[34] Nelly Huei Ying Ng and Mischa Prebin Woods. "Resource Theory of Quantum Thermodynamics: Thermal Operations and Second Laws". In: *Thermodynamics in the Quantum Regime: Fundamental Aspects and New Directions*. Ed. by Felix Binder et al. Cham: Springer International Publishing, 2018, pp. 625–650.

[35] Uttam Singh et al. "Quantum thermodynamics in a multipartite setting: A resource theory of local Gaussian work extraction for multimode bosonic systems". In: *Phys. Rev. A* 100.042104 (2019).

[36] Samuel L Braunstein and Peter Van Loock. "Quantum information with continuous variables". In: *Rev. Mod. Phys.* 77.513 (2005).

[37] Kavan Modi et al. "Unified View of Quantum and Classical Correlations". In: *Phys. Rev. Lett.* 104.080501 (2010).

[38] Mark Bradshaw, Ping Koy Lam, and Syed M Assad. "Gaussian multipartite quantum discord from classical mutual information". In: *J. Phys. B* 52.245501 (2019).

[39] Kavan Modi et al. "The classical-quantum boundary for correlations: Discord and related measures". In: *Rev. Mod. Phys.* 84.1655 (2012).

[40] Gerardo Adesso and Animesh Datta. "Quantum versus classical correlations in Gaussian states". In: *Phys. Rev. Lett.* 105.030501 (2010).

[41] Michael M. Wolf, Jens Eisert, and Martin B. Plenio. "Entangling Power of Passive Optical Elements". In: *Phys. Rev. Lett.* 90.047904 (2003).

[42] Paolo Giorda and Matteo GA Paris. "Gaussian quantum discord". In: *Phys. Rev. Lett.* 105.020503 (2010).