Entanglement quantification and quantum benchmarking of optical communication devices

by

Nathan Killoran

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis, we develop a number of operational tests and tools for benchmarking the quantum nature of optical quantum communication devices. Using the laws of quantum physics, ideal quantum devices can fundamentally outperform their classical counterparts, or even achieve objectives which are classically impossible. Actual devices will not be ideal, but they may still be capable of facilitating quantum communication. Benchmarking tests, based on the presence of entanglement, can be used to verify whether or not imperfect quantum devices offer any advantage over their classical analogs. The general goal in this thesis is to provide strong benchmarking tools which simultaneously require minimal experimental resources but also offer a wide range of applicability. Another major component is the extension of existing qualitative benchmarks ('Is it quantum or classical?') to more quantitative forms ('How quantum is it?').

This thesis is structured as follows. Chapters 1 and 2 provide an introduction and background material on quantum theory and quantum optics. Specifically, we outline the basic notions of quantum mechanics from a quantum information perspective, define some theoretical concepts which are important throughout the thesis, and detail two different methods for encoding quantum information in states of light, namely single-photon and continuous-variable encodings.

In Chapter 3, we develop our first benchmarking results, for remote state preparation (RSP) protocols. To do this, we first distinguish quantum RSP protocols from classical RSP protocols by allowing the use of a pre-shared entangled state in the quantum case. Using the average fidelity between the desired target states and the actual remotely-prepared states to measure performance, we show how to calculate the best value achievable by a classical protocol. We apply these results to a number of different ensembles of target states, including pure states, mixed states, discrete ensembles, and continuous ensembles. From this, we propose a number of simple benchmarks based on Platonic solids. Finally, the proposed benchmarks are used to certify a quantum RSP experiment.

In Chapters 4-6, we deal with the problem of extending existing continuous-variable (CV) quantum benchmarks to provide useful quantitative information. In Chapter 4, after reviewing the known CV benchmarking results, in particular the entanglement-based approach, we outline a quantification scheme based on entanglement measures and projections of infinite-dimensional optical systems to more managable finite subspaces. From this, two complementary paths are taken for the choice of projection. In Chapter 5, we pursue a two-qubit projection, which gives good quantitative results when the tested devices are near their ideal operating point. On the other hand, Chapter 6 follows the approach of

projecting onto low-energy Fock states. This provides a better capacity to certify devices with larger degrees of imperfection.

Finally, in Chapter 7, we show how to perform quantum benchmarking using arbitrary test states. Since many existing benchmarks are still limited to special cases, this provides a much-needed way to certify devices under more realistic testing conditions. We also study how to strengthen such benchmarks, leading to the best chance of certifying quantum devices. We use this approach, along with the quantitative tools developed in Chapters 4 and 6, to certify a real CV quantum memory. Together, the results contained in this thesis comprise a comprehensive suite of tools which can be used to perform efficient benchmarking tests on quantum devices using realistic experimental resources.

Acknowledgements

First of all, I would like to thank my supervisor Norbert Lütkenhaus for his support and advice over the past four years. He was always willing to discuss my research with me, yet he also gave me space to work independently. As well, I appreciate the numerous opportunities he provided to attend international conferences and visit overseas research institutes. My thanks go as well to the members of my advisory and defense committees, Andrew Childs, Joseph Emerson, David Kribs, Kevin Resch, and to Alex Lvovsky for agreeing to serve as my external examiner.

The Institute for Quantum Computing provided a fantastic environment for my graduate studies. In particular, I would like to thank the numerous members of the OQCT group who have come and gone during my tenure: Razieh Annabestani, Juan Miguel Arrazola, Normand Beaudry, Agnes Ferenczi, Oleg Gittsovich, Hauke Häseler, Mattias Heid, Xiongfeng Ma, Will Matthews, Sergei Mikheev, Tobias Moroder, Geir-Ove Myhr, Varun Narasimhachar, Marco Piani, Dave Pitkanen, and Mohsen Razavi. As well, I would like to thank my many friends and colleagues in the ever-growing IQC community, in particular the diehards who showed up every week for ball hockey. I would also like to thank the folks at the Max Planck Institute for the Science of Light in Erlangen for providing a welcoming and congenial environment throughout my semester there.

During my graduate studies, I lived in three places - the school, the grocery store and the skating rink. I thank my teammates on *Smooth Liquid Thunder* and *Maxwell's Demons* for many memorable seasons. I also want to thank Guelph Ultimate and the Waterloo Organization of Disc Sports for facilitating my activities on many summer and fall evenings.

Finally, I'd like to thank all the other people who had an impact on me during my graduate studies. Thanks to my erstwhile roommates Devon, Chris, Mike, Osama (and Gina) for many memorable nights. Thanks to my parents for their continuing support and for always welcoming me for visits home. Most importantly, my gratitude to Emma for keeping me well during the thesis-writing process and for her enduring companionship throughout my studies.

Dedication

To my fellow scientists.

Table of Contents

List of Figures **x**

List of Tables **xii**

1 Introduction **1**

2 Background **5**

2.1 Preparation 6

2.2 Evolution 8

2.3 Measurement 9

2.4 Quantum information theory 11

2.5 Quantum optical implementations 14

2.5.1 Single-photon encoding 15

2.5.2 Continuous-variable encoding 18

3 Remote state preparation benchmarks **23**

3.1 Benchmarking framework 25

3.1.1 Quantum RSP 26

3.1.2 Classical RSP 28

3.2 Threshold calculations 31

3.2.1 Finite ensembles 31

3.2.2 Continuous ensemble . . . 35
3.2.3 Mixed states . . . 36
3.3 Experimental test . . . 38

4 Benchmarking continuous variable quantum communication devices 42
4.1 Quantum benchmarking framework . . . 44
4.1.1 Fidelity-based benchmarking . . . 45
4.1.2 Entanglement-based benchmarking . . . 47
4.2 Quantitative benchmarking . . . 56
4.2.1 Benchmarking with entanglement measures . . . 56

5 Quantitative benchmarking I: two-qubit projection 61
5.1 Quantification procedure . . . 62
5.1.1 Choosing the projection . . . 63
5.1.2 Estimating the constraints . . . 64
5.1.3 Minimizing the entanglement . . . 68
5.2 Results . . . 71

6 Quantitative benchmarking II: Fock-state projection 77
6.1 Quantification procedure . . . 78
6.1.1 Choosing the projection . . . 78
6.1.2 Estimating the constraints . . . 79
6.1.3 Minimizing the entanglement . . . 84
6.2 Results . . . 86

7 Benchmarking with realistic states 93
7.1 Benchmarking framework for arbitrary states . . . 95
7.1.1 Entanglement-based benchmarking with arbitrary states . . . 95
7.1.2 Optimizing the purifications . . . 97

7.1.3 Fidelity-based benchmarking with arbitrary states 102
7.1.4 Benchmarking with phase-symmetric ensembles 107
7.2 Certifying a quantum memory 110
7.2.1 Finding the Gram matrix 111
7.2.2 Computing the entanglement 113

8 Final remarks **119**

APPENDICES **123**

A Supplement for remote state preparation benchmarks **124**
A.1 Proof of bound for continuous case 124
A.2 Proof of optimal average fidelity for mixed states 126

B Supplement for two-qubit projection scheme **128**
B.1 Derivation of overlap bounds 128
B.2 Derivation of supplementary diagonal bounds 130
B.3 Derivation of off-diagonal bounds 131
B.4 Constraints for two-qubit optimization 132

C Supplement for Fock-state projection scheme **133**
C.1 Derivation of first order constraint 133
C.2 Derivation of second order constraint 134

D Supplement for benchmarking with arbitrary states **136**
D.1 Convexity proofs 136
D.2 Proof of standard form 137
D.3 Proof of trace norm in standard form 138

References **141**

List of Figures

2.1 Representation of a single-qubit state as a vector in the Bloch sphere . . . 17

2.2 Schematic of balanced homodyne measurement 21

3.1 Remote state preparation schematic 26

3.2 Example partitioning in a remote state preparation strategy 30

3.3 Optimal classical fidelity thresholds for Platonic solid ensembles 34

3.4 Comparison of experimentally-achieved mean fidelities with benchmark values for pure states 40

3.5 Comparison of experimentally-achieved mean fidelities with benchmark values for mixed states 41

4.1 Schematic of a measure and prepare strategy/Example CV test states . . . 46

4.2 Illustrations of entanglement-based benchmarking and effective entanglement concepts 48

4.3 Quantum domain for test ensemble containing two coherent states $|\pm\alpha\rangle$ . . 53

4.4 Quantum domain for test ensemble containing $M = 3, 4, 5, 6$ symmetrically distributed coherent states $\left|\alpha\omega_M^k\right\rangle$ 54

4.5 Quantum domain for a squeezed/antisqueezed pair $|\pm r\rangle$ 55

5.1 Relaxing a non-convex constraint for the two-qubit projection into a set of convex ones 69

5.2 Minimal negativity of a two-qubit projected state consistent with potential loss and noise values 72

5.3 Comparison of two qubit projection results with quantum domain 73

5.4 Minimal negativity of a two-qubit projected state for a 50/50 beamsplitter channel with a thermal state at the second port 75

6.1 Minimal negativity of Fock-projected state for the benchmark based on two coherent test states 87

6.2 Minimal negativity of Fock-projected state for the benchmark based on squeezed/antisqueezed test states 88

6.3 Minimal negativity of Fock-projected state for the benchmark based on three coherent test states 90

6.4 Upper and lower bounds on the negativity for the benchmark based on three coherent test states 91

7.1 Example fidelity-based benchmarking thresholds $\overline{\sqrt{F}}_{NPT}^{\max}$ for qubits 105

7.2 Comparison between fidelity benchmarks obtained by optimization and analytically. 106

7.3 Upper and lower bounds for the maximum purity $\mathcal{P}$ of experimentally-compatible Gram matrices 114

7.4 Quantum memory benchmarking results using tomographically-reconstructed density matrices 116

7.5 Quantum memory benchmarking results using quadrature data directly . . 117

List of Tables

3.1 Experimentally-achieved mean fidelities for mixed state icosahedron and dodecahedron ensembles 39

7.1 Experimentally-determined first and second moments for the conjugate quadratures $\hat{x}$ and $\hat{p}$ 111

Chapter 1

Introduction

"Have no fear of perfection — you'll never reach it." - Salvador Dalí

Quantum communication is the transmission of information via quantum states. Although the fundamentals of quantum physics have been known for almost a century, it took more time for the idea of using quantum states as information carriers to become prominent. Indeed, many modern communication technologies are based primarily on classical laws of physics, especially the theory of electromagnetism. Of course, as components are designed to function at smaller and smaller scales, quantum effects start to come into play. Often, these quantum effects are seen as undesirable since they do not fit into the classical framework. But if the fundamental small-scale workings of the universe are quantum mechanical (and to the best of our knowledge, they are), then we should embrace such quantum effects. Instead of designing our technologies based on classical laws, we should make use of the more fundamental quantum rulebook. Since classical physics is anyway a course-grained, macroscopic version of quantum physics, this shift can only improve our technological capabilities.

Indeed, this new perspective has led to the development of important quantum communication protocols that can fundamentally outperform classical technologies. For instance, quantum teleportation protocols can enable the accurate transmission of the state of a particle from one location to another using only a finite amount of resources, while any classical protocol would require infinite resources for faithful transmission. As well, quantum cryptography schemes enable users to communicate their information in true security, whereas many commonly-used classical cryptography schemes can be broken with powerful enough resources (such as a quantum computer, another device made possible through the use of quantum information carriers).

Part of the reason that quantum information theory is only now getting an appropriate level of attention is that our control over the quantum world has been imperfect in the past. For quantum communication, light is undoubtedly the best carrier for quantum information, owing to its speed and weakly-interacting nature. Advances in quantum light sources (single photons, entangled states), transmission (optical fibres, free space, light/atom interfaces), and detectors (high efficiency photodetectors, homodyne interferometers) have provided greater access to the quantum properties of light.

However, even in modern experiments, some degree of imperfection is inevitable. Such imperfections may degrade the operation of quantum communication devices to a point where a comparable classical device could achieve the same level of performance. In this case, there would no longer be any advantage to using the quantum framework. Fortunately, it is still possible to perform meaningful quantum communication tasks with imperfect components, provided the degree of imperfection is not too large. Indeed, quantum

devices with small deviations from the ideal are able to outperform their classical analogs. Although current experiments and devices remain imperfect, they are certainly at a level where the advantage of the quantum framework can be convincingly demonstrated.

The goal of *quantum benchmarking* is to certify quantum communication devices or experiments, i.e. to establish that a particular quantum device outperforms all comparable classical devices. Quantum devices include quantum teleportation systems, quantum memories, quantum repeaters, quantum channels, and quantum remote state preparation systems, among others. For all of these devices, a fundamental distinction must be made: *genuine quantum communication devices cannot be simulated by comparable classical devices*. A device that can be classically simulated is not useful for quantum communication purposes, and there is no advantage to using the quantum framework. In order to determine whether or not a device can be classically simulated, we will focus on the presence of entanglement, an undeniably quantum resource. Of primary importance will be to find and explore the *quantum domain*, the regime of operation that is only possible for genuine quantum devices. Once we have fixed a classical analog, we can map out the limits of its performance. Any device performing beyond these limits must be in the quantum domain.

Quantum benchmarking is important because it allows us to conclude that a device can facilitate quantum communication. In networks containing many quantum communication devices, the failure of one device can adversely affect the entire network, so it is important that every component functions properly. That being said, experimentalists should be free to focus on the demanding tasks of designing and building quantum devices. Therefore, it is up to the theorists to develop conceptual tools that make the actual benchmarking task as practical and pain-free as possible. Hence, we should aim for benchmarks that require a minimal amount of experimentally realistic resources at all stages. Finally, it can be useful to have benchmarks that are *quantitative* in nature, rather than strictly qualitative ('classical/quantum'). This allows us to not only determine whether a device is in the quantum domain, but also to compare the performance of different devices within the quantum domain.

This thesis contains various results related to the task of quantum benchmarking. In particular, the goal of this research was to develop strong, practical, quantitative, and general tools for the quantum benchmarking problem. Often, these results build on previous works in the same direction. For example, a large portion of this thesis is devoted to tools for benchmarking so-called continuous variable (CV) optical devices, in which quantum information is encoded using continuous degrees of freedom. The common starting point for these tools is the entanglement-based framework for CV benchmarking (which will be summarized in Ch. 4). The CV benchmarking results in this thesis can be seen as an extension or as a filling out of the existing benchmarking toolbox, enabling a better un-

derstanding of the quantum nature of communication devices. Where appropriate, we will show the advantage of the new techniques by comparing with previous results. As well, in cases where an actual experimental device is available, we will demonstrate the practical application of the benchmarking tools.

This thesis is organized as follows. In the next chapter, we review important background concepts from quantum physics that will be necessary later in the thesis. We provide some mathematical details about state preparation, evolution, and measurement, as well as introducing some tools from quantum information theory that are useful in quantum benchmarking. On the practical side, we outline how some of these concepts are realized within a quantum optical setting. Chapter 3 is devoted to obtaining benchmarks for a particular discrete quantum communication protocol called *remote state preparation* (RSP). These benchmarks are applied to certify a real-world RSP experiment. The remainder of the thesis is dedicated to benchmarking tools and results for continuous-variable quantum devices. In Chapter 4, we summarize previous CV benchmarking results and begin the first steps for extending these results to make quantitative statements about devices within the quantum domain. At this point, two complimentary approaches to quantitative benchmarking are developed: one approach is best for low degrees of imperfection, while the other works better on systems with larger imperfections. These two approaches are outlined in Chapters 5 and 6, respectively. Chapter 7 concerns the problem of benchmarking with experimentally realistic testing resources. We demonstrate how to design quantum benchmarks using arbitrary test states, which are then used to certify a physical CV quantum memory. Together, the result in this thesis contribute in new ways to the problem of benchmarking optical quantum communication devices using experimentally practical resources.

Chapter 2

Background

Quantum information theory deals with information processing and communication using quantum systems as the fundamental resources. Quantum mechanics, on the other hand, is the most well-tested theory we have developed for understanding the workings of the universe on a small scale. Therefore, an understanding of the basics of quantum mechanics is crucial before proceeding into any discussions of quantum information theory. At its heart, quantum mechanics is a mathematical framework for describing the behaviour of quantum systems. To certain primitive operational tasks, we associate a specific mathematical description. This mathematical formalism allows us to make predictions for the outcome of experiments or protocols.

On the most general level, we can identify three important operational primitives. First, a user[1] makes a *preparation* of a quantum system. This system could be prepared in a fixed state, or the preparation could be a probabilistic mixture of states (whether this mixture is intentional or not). Second, the system is subject to *evolution*. Again, the evolution might be in a deterministic form or it might have a more stochastic nature. The stochasticity could be due to interaction with the ambient environment or another outside agent. Finally, another user (or possibly the same one) makes a *measurement* on the system by interacting it with some measurement apparatus. Often, the quantum system is destroyed or converted to some unusable form by the measurement process.

As a useful guiding point, for each of the above primitives, we can identify an idealized situation and a more realistic general situation. We will now outline how these concepts fit into the mathematical framework of quantum mechanics. The interested reader is referred to any standard quantum information textbook for a more detailed exposition (e.g., [75]). We begin by fixing a Hilbert space $\mathcal{H}$ (i.e., a complete vector space endowed with a complex-valued inner product), called the *state space*. Vectors in this Hilbert space are denoted with the 'ket' symbol $|\cdot\rangle$.

2.1 Preparation

If a quantum system cannot be considered as a probabilistic mixture of other states, we say that it is 'pure.' Such preparations are mathematically described as follows.

Definition 2.1.1 (Pure states)**.** *The state of a 'pure' quantum system is represented by a normalized vector $|\psi\rangle$ in the state space $\mathcal{H}$.*

[1] We use the general term 'user' to refer to an entity who participates in a quantum physics experiment or a quantum communication protocol. This entity could be a real person or a physical device.

Pure states are not the most general preparations for quantum systems. As mentioned above, it is possible to have preparations that are probabilistic mixtures as well. Such probabilistic preparations could be caused by a user randomly preparing different pure states, from imperfections in the preparation process, from taking a subsystem of a larger system, or from combinations of these. To describe these 'mixed' preparations, we need to consider the set of bounded linear operators on the Hilbert space $\mathcal{H}$, denoted by $\mathcal{B}(\mathcal{H})$. In this framework, each pure state $|\psi\rangle \in \mathcal{H}$ is identified with the corresponding projection operator $|\psi\rangle\langle\psi| \in \mathcal{B}(\mathcal{H})$. Often, $|\psi\rangle\langle\psi|$ is also referred to as a pure state.

Definition 2.1.2 (Mixed states)**.** *The state of a 'mixed' quantum system is represented by an operator that is a probabilistic mixture*[2] *of pure states, i.e.,* $\rho = \sum_\alpha p_\alpha |\psi_\alpha\rangle\langle\psi_\alpha|$ *with* $p_\alpha \geq 0 \ \forall \ \alpha$ *and* $\sum_\alpha p_\alpha = 1$.

All preparations, whether mixed or pure, can be represented by an appropriate choice of operator $\rho \in \mathcal{B}(\mathcal{H})$, called a density operator or density matrix. Because the probability coefficients must sum to one, states are always normalized with respect to the trace operation, i.e., $\mathrm{Tr}\rho = 1$. As well, from the above definition, states are necessarily positive semidefinite operators, $\rho \geq 0$. Alternatively, we could have used these two properties to define general quantum states.

Often, we are interested in describing situations where several quantum systems are prepared in some joint state. Most basically, if we have two quantum systems, labelled A and B, with corresponding state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the state space of the joint system is given by the tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Pure states and mixed states of the joint system are defined on the state space as before. We can recover the state of each subsystem using the partial trace operation.

Definition 2.1.3 (Reduced state)**.** *If* $\rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ *is a bipartite state, we describe the state of one subsystem by tracing out the other subsystem, i.e.,* $\rho_A = \mathrm{Tr}_B \rho_{AB}$ *and* $\rho_B = \mathrm{Tr}_A \rho_{AB}$

A *factorized* state on the joint system is a state that can be split into states on both subsystems.

Definition 2.1.4 (Factorized states)**.** *A pure state* $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ *is factorized when it can be decomposed into the form* $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$*, with* $|\psi\rangle_A \in \mathcal{H}_A$ *and* $|\psi\rangle_B \in \mathcal{H}_B$*. A mixed state* $\rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ *is factorized when it can be decomposed into the form* $\rho_{AB} = \rho_A \otimes \rho_B$*, with* $\rho_A \in \mathcal{B}(\mathcal{H}_A)$ *and* $\rho_B \in \mathcal{B}(\mathcal{H}_B)$.

[2] If the index α is continuous, the summation symbol represents some appropriate integration.

As well, we can consider a probabilistic mixture of factorized states [103].

Definition 2.1.5 (Separable states)**.** *A state $\rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ is said to be* separable *when it can be decomposed as $\rho_{AB} = \sum_\alpha p_\alpha \rho_A^\alpha \otimes \rho_B^\alpha$, with $\rho_A^\alpha \in \mathcal{B}(\mathcal{H}_A)$, $\rho_B^\alpha \in \mathcal{B}(\mathcal{H}_B)$ $\forall$ α, and $\sum_\alpha p_\alpha = 1$.*

At this point we can introduce one of the distinguishing features of quantum theory, namely *entanglement*. Entanglement is an important property of quantum systems which can be employed as a resource for quantum communication tasks. Let S_{AB} denote the set of separable states on $\mathcal{B}(\mathcal{H}_{AB})$.

Definition 2.1.6 (Entangled states)**.** *A state $\rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ is said to be entangled if it is not separable, i.e., if $\rho_{AB} \notin S_{AB}$.*

Given the above definition, a pure state $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ is entangled whenever it is not a factorized state.

2.2 Evolution

The next operational primitive is allowing the quantum system to evolve. This evolution can consist of a controlled transformation, an uncontrolled interaction with an environment or other auxilliary system, some combination of these, or a transformation that leaves the system unchanged. From a quantum information perspective, we are primarily interested in situations where the evolution is generated by a time-independent Hamiltonian $\hat{H}$. These Hamiltonians are self-adjoint operators, $\hat{H} = \hat{H}^\dagger$, which represent the basic evolution of a quantum system, according to the *Schrödinger equation*:

$$i\hbar \frac{d}{dt} |\psi\rangle = \hat{H} |\psi\rangle . \tag{2.1}$$

Henceforth, we use the convention that $\hbar = 1$. The solution of the Schrödinger equation with time-independent Hamiltonian can be found by exponentiation. Since the Hamiltonian is self-adjoint, the evolution of the state must be unitary.

Proposition 2.2.1 (Unitary evolution)**.** *Evolution of a pure quantum system from an initial state $|\psi_{\text{in}}\rangle \in \mathcal{H}$ to a final state $|\psi_{\text{out}}\rangle \in \mathcal{H}$ occurs as a unitary process: $|\psi_{\text{out}}\rangle = \hat{U} |\psi_{\text{in}}\rangle$, with $\hat{U} \in \mathcal{B}(\mathcal{H})$ and $\hat{U}^\dagger \hat{U} = \hat{U}\hat{U}^\dagger = \hat{\mathbb{1}}_{\mathcal{H}}$. Similarly, mixed states evolve according to the unitary operation $\rho_{\text{out}} = \hat{U} \rho_{\text{in}} \hat{U}^\dagger$.*

In principle, Proposition 2.2.1 only describes the evolution of *closed* quantum systems. In general, evolution may also be *open*, involving interaction with other systems or transferral of the system to a different state space. Such possibilities are represented by the notion of completely positive, trace-preserving (CPTP) maps. But first, we need a few preliminary concepts relating to transformations between states with different state spaces (represented by $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$).

Definition 2.2.2 (Positive map)**.** *A transformation $\Lambda : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$ is called a* positive *map if, whenever $\hat{X} \in \mathcal{B}(\mathcal{H}_{\text{in}})$ is positive semidefinite, then $\Lambda[\hat{X}] \in \mathcal{B}(\mathcal{H}_{\text{out}})$ is positive semidefinite, i.e., $\hat{X} \geq 0 \Rightarrow \Lambda[\hat{X}] \geq 0$.*

Definition 2.2.3 (Trace-preserving map)**.** *A map $\Lambda : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$ is* trace-preserving *if $\text{Tr}(\Lambda[\hat{X}]) = \text{Tr}\hat{X}$ for all $\hat{X} \in \mathcal{B}(\mathcal{H}_{\text{in}})$.*

Clearly, positive trace-preserving maps will always take density matrices to density matrices. However, we also need to consider the situation where only one subsytem of a joint system is subject to evolution. We demand that the resulting output is a genuine state in this case as well.

Definition 2.2.4 (Completely positive map)**.** *Let $\mathcal{H}_{\text{anc}}$ be the state space of any ancillary system. A map $\Lambda : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$ is said to be* completely positive *when, for any positive semidefinite operator defined on the joint system, $\hat{X} \in \mathcal{B}(\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{in}})$, partial evolution by Λ leads to a positive semidefinite output, i.e., $(\text{id} \otimes \Lambda)[\hat{X}] \geq 0 \ \forall \ \hat{X} \geq 0$.*

Completely positive, trace-preserving maps represent the most general form of evolution for quantum systems (open or closed). In quantum information theory, such general evolution is often called a *quantum channel*. In particular, one type of channel will be of interest later, so we note it here.

Definition 2.2.5 (Entanglement-breaking channel)**.** *A channel, represented by the map $\Lambda : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$, is said to be* entanglement-breaking *if it always produces a separable output when acting partially on any state, i.e., $(\text{id} \otimes \Lambda)[\rho]$ is separable $\forall \ \rho \geq 0$.*

2.3 Measurement

The last operational primitive is the process of measurement. This task is accomplished by interacting the relevant system with some measurement device. The measurement device then provides to the user the outcome of the measurement (e.g., through a 'click/no click'

event or a dial reading), which we will label by α. As well, in the process of measurement, the system itself is transformed into some post-measurement state. We mathematically describe the process of measurement using a set of operators with certain properties.

Proposition 2.3.1. *Measurement of a quantum system is represented by a set of operators* $\{\hat{M}_\alpha\}$*, acting on the state space* $\mathcal{H}$*, that satisfy the* completeness relation $\sum_\alpha \hat{M}_\alpha^\dagger \hat{M}_\alpha = \hat{\mathbb{1}}_\mathcal{H}$*. For a state represented by the density operator* $\rho \in \mathcal{B}(\mathcal{H})$*, the probability of obtaining measurement outcome '*α*' is* $p(\alpha) = \mathrm{Tr}(\rho \hat{M}_\alpha^\dagger \hat{M}_\alpha)$*.*

The post-measurement state ρ_{PM} for outcome 'α' is given by

$$\rho_{PM} = \frac{\hat{M}_\alpha \rho \hat{M}_\alpha^\dagger}{\mathrm{Tr}(\hat{M}_\alpha \rho \hat{M}_\alpha^\dagger)}. \tag{2.2}$$

Typically, the measurement process is irreversible. If we are not interested in the post-measurement state, it is often convenient to represent measurements in a slightly different way.

Definition 2.3.2 (POVM)**.** *A positive-operator-valued measure (POVM) is a set of operators* $\hat{P}_\alpha \in \mathcal{B}(\mathcal{H})$ *satisfying the following properties: (i)* $\hat{P}_\alpha \geq 0 \ \forall \ \alpha$*, and (ii)* $\sum_\alpha \hat{P}_\alpha = \hat{\mathbb{1}}_\mathcal{H}$*.*

For a given set of measurement operators, we can identify corresponding POVM elements using

$$\hat{P}_\alpha = \hat{M}_\alpha^\dagger \hat{M}_\alpha. \tag{2.3}$$

More generally, POVMs can also be defined by summing together (or 'course-graining') a number of suitably-normalized elements in the form of Eq. (2.3). In some special cases, measurements are *projective* (or repeatable), and POVMs reduce to a simpler form:

Definition 2.3.3 (PVM)**.** *A* projection-valued measure *(PVM) is a set of operators* $\{\hat{P}_\alpha\}$ *acting on* $\mathcal{H}$ *that are orthogonal projectors,* $\hat{P}_{\alpha'} \hat{P}_\alpha = \delta_{\alpha' \alpha} \hat{P}_\alpha$*, and that satisfy the completeness relation* $\sum_\alpha \hat{P}_\alpha = \hat{\mathbb{1}}_\mathcal{H}$*.*

In many situations, we will not know the exact state of a system, and a measurement might be used to gain more information. Due to the probabilistic nature of quantum systems, a single measurement cannot provide a full description of the system. However, if we can prepare many identical copies of the same state, then repeated measurement will allow us to build up a faithful statistical description of the state. We will often be interested in certain aspects of a system that can be revealed through measurement.

Definition 2.3.4. *An* observable *is a self-adjoint operator* $\hat{O} = \hat{O}^\dagger$ *that acts on the state space,* $\hat{O} : \mathcal{H} \to \mathcal{H}$.

Observables represent some physical property of the system that can be quantified numerically (e.g., the energy). The *expectation value* of an observable with respect to a state is the numerical value of the associated physical quantity for that state. Expectation values can be computed using the following rule.

Proposition 2.3.5 (Born rule)**.** *If an observable is represented by an operator* $\hat{O}$ *and a state by the density matrix* ρ*, then the expectation value of the observable with respect to this state is given by* $\left\langle \hat{O} \right\rangle = \mathrm{Tr}(\hat{O}\rho)$.

Since observables are self-adjoint, their eigenvalues λ_O are real-valued and their eigenvectors $|\lambda_O\rangle$ are orthogonal. Hence, we can consider a PVM containing projectors onto the eigenvectors, $\hat{P}_\lambda^{\hat{O}} = |\lambda_O\rangle\langle\lambda_O|$. Weighting these outcomes by the appropriate eigenvalues, we can obtain expectation values through the measurement process. For all the situations considered in this thesis, it is possible to find a set of observables $\{\hat{O}_\alpha\}$ that are *tomographically complete* for a relevant state space $\mathcal{H}$ (i.e., the observables span $\mathcal{B}(\mathcal{H})$). Any density matrix ρ defined on that state space can be written as some linear combination of these observables:

$$\rho = \sum_\alpha c_\alpha \hat{O}_\alpha. \tag{2.4}$$

2.4 Quantum information theory

In this section, we introduce some concepts and techniques from quantum information theory that will be useful throughout the thesis. We begin with mixed states, the most general description of quantum systems. The following functional quantifies the degree of mixedness of a state.

Definition 2.4.1 (Purity)**.** *The* purity *of a density matrix* ρ *is defined by* $\mathcal{P}(\rho) = \mathrm{Tr}(\rho^2)$.

Purity is positive for any state, with a maximal value of 1. A state has unit purity if and only it is pure.

It is often more convenient or elegant to work with pure states. Even when we must consider mixed states, it is always possible to represent such states as pure states in a larger space.

Definition 2.4.2 (Purification)**.** *Let $\rho \in \mathcal{B}(\mathcal{H}_{\text{sys}})$ be a density matrix describing a particular quantum state (pure or mixed). Let $\mathcal{H}_{\text{anc}}$ be an ancillary state space. A state $|\Psi_\rho\rangle \in \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{anc}}$ is called a* purification *of ρ if $\text{Tr}_{\text{anc}}(|\Psi_\rho\rangle\langle\Psi_\rho|) = \rho$.*

Among other uses, purifications allow us to generalize the concept of state overlap or transition probability to mixed states.

Definition 2.4.3 (Fidelity)**.** *Let $\rho, \sigma \in \mathcal{B}(\mathcal{H}_{\text{sys}})$ be two density operators. Let $|\Psi_\rho\rangle, |\Psi_\sigma\rangle \in \mathcal{H}_{\text{sys}} \otimes \mathcal{H}_{\text{anc}}$ be purifications of these states (with the same purifying space). The* fidelity *$F(\rho, \sigma)$ is defined as the maximum square overlap of the purifications, i.e.,*

$$F(\rho, \sigma) = \max_{|\Psi_\rho\rangle, |\Psi_\sigma\rangle} |\langle\Psi_\rho|\Psi_\sigma\rangle|^2, \tag{2.5}$$

where $\text{Tr}_{\text{anc}} |\Psi_\rho\rangle\langle\Psi_\rho| = \rho$ and $\text{Tr}_{\text{anc}} |\Psi_\sigma\rangle\langle\Psi_\sigma| = \sigma$.

The fidelity can be interpreted as a quantitative measure of (in)distinguishability for pairs of quantum states. Alternatively, we could have omitted the square in Eq. (2.5). This alternative definition is also common in the literature, and they are both referred to as fidelity. To avoid confusion, we will refer to the unsquared quantity as the root fidelity. In this thesis, we will mainly use the first characterization. To go with the above formal definition, we also have the following closed formula [96, 52]:

Theorem 2.4.4 (Uhlmann)**.** *The fidelity is given by*

$$F(\rho, \sigma) = \left[\text{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right]^2. \tag{2.6}$$

In Ch. 7, we will show how the (root) fidelity of two arbitrary states can be computed numerically using the methods of semidefinite programming.

Finally, fix two state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, with orthonormal basis vectors $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$, respectively, and consider the composite system $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. As mentioned earlier, quantum theory allows composite systems to be entangled. Unfortunately, it can be difficult to determine in practice whether a given density matrix $\rho_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ is separable or entangled [31]. One approach to this problem is to determine whether or not a state lies in some easier to characterize set $\tilde{S}_{AB}$ that contains the set of separable states, $S_{AB} \in \tilde{S}_{AB}$. If $\rho_{AB} \notin \tilde{S}_{AB}$, then the state is entangled, but if $\rho_{AB} \in \tilde{S}_{AB}$, no conclusion can be made. A common choice for the set $\tilde{S}_{AB}$, which will be employed throughout this thesis, is the set of states that are *positive under partial transposition*, or PPT [80, 41].

Definition 2.4.5 (PPT)**.** *Let $\mathcal{T}_A : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_A)$ denote the transposition map $\mathcal{T}_A[|i\rangle\langle j|_A] = |j\rangle\langle i|_A$ for all i, j in the basis $\{|i\rangle_A\}$. A density matrix ρ_{AB} has the PPT property with respect to system A when $(\mathcal{T}_A \otimes \mathrm{id})[\rho_{AB}] \geq 0$.*

We can define an analogous partial transposition on system B. We point out that although the partial transposition of ρ_{AB} is basis-dependent, its spectrum is independent of the basis [61]. Frequently, partial transposition will be denoted by the shorter form $\rho_{AB}^{T_A}$ or $\rho_{AB}^{T_B}$. For $\dim\mathcal{H}_{AB} \leq 6$, the set of separable states and the set of PPT states are equivalent. However, for higher dimensions, there exists entangled states which are not PPT. Entangled states which are PPT are said to have 'PPT entanglement,' while those which are not PPT will be called 'NPT' entangled states.

Though it is not obvious from the earlier definition, entanglement can be thought of as a *quantitative* property of quantum systems. Therefore, it is useful to have mathematical measures which serve to enumerate the entanglement. Formally, an entanglement measure is a non-negative functional on quantum states satisfying some additional properties. Although the full set of desired properties are not universally agreed upon, entanglement measures must minimally meet two requirements [43].

Definition 2.4.6 (Entanglement measure)**.** *A functional $\mathcal{E} : \mathcal{B}(\mathcal{H}_{AB}) \to \mathbb{R}^+ \cup \{0\}$ is called an* entanglement measure *when it satisfies the following two requirements:*

1. **Monotonicity***: If a system undergoes a protocol involving only local operations and classical communication between users Alice and Bob (a so-called LOCC protocol), then the quantity of entanglement cannot increase. In other words, if the protocol is represented by the map Λ_{LOCC}, then $\mathcal{E}(\rho_{AB}) \geq \mathcal{E}(\Lambda_{\mathrm{LOCC}}[\rho_{AB}])$.*
2. **Zero on separable states***: If ρ_{AB} is separable, then $\mathcal{E}(\rho_{AB}) = 0$.*

In the above definition, an 'operation' consists of any of the aforementioned operational primitives, i.e., state preparation, evolution, or measurement. The important distinction is that they be done locally, i.e., separately on the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Classical communication allows users to share information and undergo further operations based on this information. Many entanglement measures actually obey a stronger form of monotonicity.

Definition 2.4.7 (Strong monotonicity)**.** *Let the map Λ_{LOCC} represent a LOCC protocol that, when acting on a state ρ_{AB}, outputs the state ρ_α with probability p_α ($\sum_\alpha p_\alpha = 1$), i.e., $\Lambda_{\mathrm{LOCC}}[\rho_{AB}] = \sum_\alpha p_\alpha \rho_\alpha$. An entanglement measure has the* strong monotonicity *property if*

$$\mathcal{E}(\rho_{AB}) \geq \sum_\alpha p_\alpha \mathcal{E}(\rho_\alpha). \tag{2.7}$$

An entanglement measure that is employed in many parts of this thesis is the *negativity* [111, 58, 102, 82].

Definition 2.4.8. *The* negativity *of a bipartite state ρ_{AB} is given by*

$$\mathcal{N}(\rho_{AB}) = \frac{||\rho_{AB}^{T_A}||_1 - \mathrm{Tr}(\rho_{AB})}{2}, \tag{2.8}$$

where $||\cdot||_1$ denotes the trace norm, i.e., the sum of the singular values.

By construction, the negativity of a state vanishes if and only if that state is in the PPT class, so it can't detect all entangled states. The negativity has the strong monotonicity property, and it is well-defined for non-normalized states (notice that we have included the term $\mathrm{Tr}(\rho_{AB})$ in Eq. (2.8), which is usually set to unity). The ability to evaluate non-normalized states will be useful in later chapters. Although the negativity may not have as nice an operational interpretation as some other entanglement measures, its main strength is that it is computable. At this time, we also note the following variational characterization of the negativity (cf. [102]):

$$\mathcal{N}(\rho_{AB}) = \begin{cases} \min\limits_{X} & \mathrm{Tr}X \\ \text{subject to} & X \geq 0 \\ & \rho_{AB}^{T_A} + X \geq 0 \end{cases}. \tag{2.9}$$

We remark that this variational formulation has the form of a semidefinite program [99].

2.5 Quantum optical implementations

In this final background section, we connect the above concepts to an actual physical implementation, namely quantum optics. Quantum states of light make the best carriers for quantum communication due to the fast transmission speed and weak interactions. The material in this section can be found in many standard quantum optics books; we will largely follow [6] and [59], especially for continuous-variable quantum optics.

Mathematically, the electromagnetic field can be decomposed into a collection of independent normal modes, which represent classical solutions to Maxwell's equations. This field is quantized by associating a quantum harmonic oscillator system to each mode. The

state space $\mathcal{H}$ of a harmonic oscillator has a countable basis $\{|n\rangle\}_{n=0}^{\infty}$, defined implicitly[3] via a ladder operator $\hat{a}$:

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \tag{2.10}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{2.11}$$

The states $\{|n\rangle\}$ are called *Fock states* or *photon-number states*, since they are eigenstates of the *number operator*

$$\hat{n} := \hat{a}^\dagger \hat{a}. \tag{2.12}$$

We say that a mode contains n photons when it is in the state $|n\rangle$. The state $|0\rangle$ is called the *vacuum state*. The ladder operator and its adjoint do not commute; instead, they follow the commutation relation

$$[\hat{a}, \hat{a}^\dagger] = \hat{\mathbb{1}}. \tag{2.13}$$

All further operators of interest can be built from suitable combinations of $\hat{a}$ and $\hat{a}^\dagger$. For several modes, represented with the index α, the associated ladder operators $\hat{a}_\alpha$ satisfy

$$[\hat{a}_{\alpha'}, \hat{a}_\alpha^\dagger] = \delta_{\alpha'\alpha}\hat{\mathbb{1}}. \tag{2.14}$$

There are different ways to encode quantum information in the degrees of freedom of light. In this thesis, we will encounter two distinct encodings, so it is important to differentiate between them.

2.5.1 Single-photon encoding

One popular discrete encoding of quantum information is to split a single photon among several different modes. The modes could represent paths in an interferometer, temporal time bins, polarizations of the light field, or some combination of these. For two modes, labelled H and V, the relevant state space is $\mathcal{H} = \mathrm{span}(|H\rangle\,, |V\rangle)$, where the basis vectors are given by

$$|H\rangle = |1\rangle_H \otimes |0\rangle_V\,, \tag{2.15}$$

$$|V\rangle = |0\rangle_H \otimes |1\rangle_V\,. \tag{2.16}$$

In quantum information applications, these basis vectors are often denoted as $|0\rangle$ and $|1\rangle$ (not to be confused with Fock states). Two-dimensional state spaces are referred to as

[3] In this thesis, we work in units such that the frequency ω and Planck's constant $\hbar$ are equal to one.

qubit systems. The state space for a single photon shared between more than two modes is analogous, but we will not need to consider such cases.

A convenient parameterization scheme for qubit systems is the *Bloch sphere*. Any pure qubit state $|\psi\rangle$ can be written in the form

$$|\psi(\theta,\varphi)\rangle = \cos(\tfrac{\theta}{2})\,|0\rangle + e^{i\varphi}\sin(\tfrac{\theta}{2})\,|1\rangle\,, \tag{2.17}$$

for some choice of angles $\theta \in [0,\pi]$, $\varphi \in [0,2\pi]$. On the other hand, any mixed qubit state ρ can be written

$$\rho = \frac{\hat{\mathbb{1}} + \overrightarrow{r}\cdot\overrightarrow{\sigma}}{2}, \tag{2.18}$$

where $|\overrightarrow{r}| \leq 1$ and $\overrightarrow{\sigma} = (X,Y,Z)$ are the two-dimensional Pauli matrices (in the computational basis $\{|0\rangle\,,|1\rangle\}$):

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.19}$$

This decomposition can also be expressed in the form

$$\rho(\theta,\varphi,r) = r\,|\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)| + (1-r)\frac{\hat{\mathbb{1}}}{2} \tag{2.20}$$

for some pure state $|\psi(\theta,\varphi)\rangle$ with $r = |\overrightarrow{r}|$ and θ and φ the polar and azimuthal angles of the 'Bloch vector' $\overrightarrow{r}$, respectively. This paramaterization allows us to represent any qubit state as a suitable vector within the unit ball (the 'Bloch sphere'), as depicted in Fig. 2.1.

By combining two single-photon systems in the right way, we can produce two-photon entangled states. Let A denote a single-photon system, with basis vectors $\{|0\rangle_A\,,|1\rangle_A\}$, and similarly for system B. A two-qubit *Bell state* is given by

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A \otimes |H\rangle_B + |V\rangle_A \otimes |V\rangle_B). \tag{2.21}$$

This state is also referred to as a *maximally-entangled state*. Entangled states are important resources in quantum communication protocols, such as teleportation or remote state preparation (see Ch. 3).

Evolution of single-photon states can be accomplished using simple linear-optical elements, such as beam splitters and phase shifters. As well, there might be external environmental interactions that change the state of the photons in undesirable ways. Measurements are typically performed by splitting the system (using linear optical elements) into a

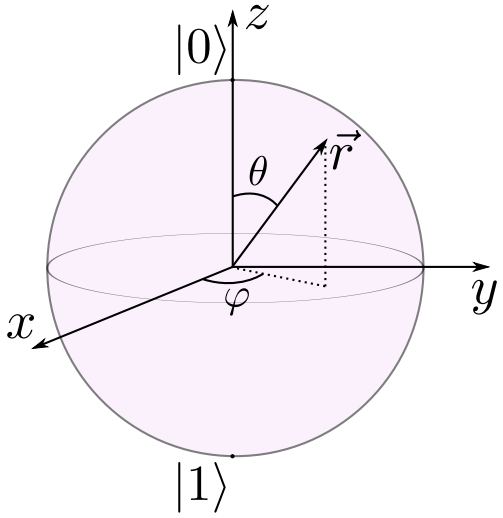


Figure 2.1: Representation of a single-qubit state as a vector in the Bloch sphere

number of different modes, each with its own photodetector. We can infer the state of the system by which detector registers a detection event[4]. Two detectors, for modes H and V, together make up a measurement device that performs the PVM $\{|H\rangle\langle H|, |V\rangle\langle V|\}$.

Importantly, since this encoding contains only one photon, it is highly susceptible to photon loss. When loss occurs, prepared states are transferred out of the encoding space and no photons are detected during measurement. Thus, the number of detection events will be less than the number of prepared states. In this situation, it is common to assume *fair sampling* [22, 79, 21], i.e., that the subset of experimental runs where a photon was successfully detected are representative of the whole. Some care must be taken with the fair sampling hypothesis when working in an adversarial situation, i.e., when an eavesdropper could have contributed to the photon loss in some biased manner. For quantum benchmarking purposes, where the experiments are under our control and no adversary is present, we will assume fair sampling in single-photon protocols.

[4]The POVM elements for a photodetector measurement can ideally be modelled as $\hat{P}_{\text{noclick}} = |\text{vac}\rangle\langle\text{vac}|$ and $\hat{P}_{\text{click}} = \hat{\mathbb{1}} - \hat{P}_{\text{noclick}}$, where $|\text{vac}\rangle$ is the state with no photons in the detector mode.

2.5.2 Continuous-variable encoding

Another approach is to encode quantum information in *phase space*, a continuous-variable characterization of quantum light. We first define the *field quadratures* as

$$\hat{x} := \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right), \tag{2.22}$$

$$\hat{p} := \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right). \tag{2.23}$$

The quadrature operators have continuous spectra,

$$\hat{x} = \int_{-\infty}^{\infty} x \left|x\right\rangle\!\left\langle x\right| \mathrm{d}x, \tag{2.24}$$

$$\hat{p} = \int_{-\infty}^{\infty} p \left|p\right\rangle\!\left\langle p\right| \mathrm{d}p, \tag{2.25}$$

and are analogous to position and momentum, having the commutation relation $[\hat{x}, \hat{p}] = i\hat{\mathbb{1}}$. Exploiting this analogy, we can represent the state of light with a distribution in some continuous phase space. For a single mode, this phase space is parameterized by two scalars $(x, p) \in \mathbf{R}^2$, which correspond to the quadratures $\hat{x}$ and $\hat{p}$. Multimode states can be represented by combining the phase spaces of each mode, though we will largely be concerned with single-mode CV systems.

The most common phase-space distribution is the *Wigner function* [104]. For a single mode, a given operator ρ has the Wigner function

$$W(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \exp(ipq)\left\langle x - \tfrac{q}{2}\right|\rho\left|x + \tfrac{q}{2}\right\rangle \mathrm{d}q. \tag{2.26}$$

If ρ is a valid state, the Wigner function is real and normalized to unity. Since the Wigner function may become negative in some regions of phase space, it is referred to as a *quasiprobability distribution*. As well as describing states, the Wigner function can be used to evaluate overlaps and expectation values. Perhaps most importantly, the marginals of the Wigner distribution are connected to the field quadratures,

$$\int_{-\infty}^{\infty} W(x,p)\mathrm{d}p = \left\langle x\right|\rho\left|x\right\rangle, \quad \int_{-\infty}^{\infty} W(x,p)\mathrm{d}x = \left\langle p\right|\rho\left|p\right\rangle. \tag{2.27}$$

A number of other phase-space representations can be defined, notably the Q function [46] and the P function [28, 93], though we will not need these.

An important subset of continuous-variable states is the *Gaussian states*, consisting of states whose Wigner functions are Gaussian distributions. The Gaussian states for a single mode are: coherent states, squeezed states, displaced squeezed states, thermal states, and displaced-squeezed thermal states. Such states are completely characterized by the first and second moments of the quadrature operators. Specifically, for a single mode, we define the vector of operators [14]

$$\hat{\xi} := (\hat{x}, \hat{p}) \tag{2.28}$$

and represent the associated phase-space scalars by

$$\xi := (x, p). \tag{2.29}$$

The first moments of a state ρ can be gathered into a displacement vector

$$D = \left\langle \hat{\xi} \right\rangle_\rho , \tag{2.30}$$

and the second moments into the *covariance matrix* (or *correlation matrix*)

$$\gamma_{ij} := \text{Re Tr}\left[\rho \left(\hat{\xi}_i - \left\langle \hat{\xi}_i \right\rangle\right)\left(\hat{\xi}_j - \left\langle \hat{\xi}_j \right\rangle\right)\right]. \tag{2.31}$$

The Wigner function of a single-mode Gaussian state is given by

$$W_G(\xi) = \frac{1}{2\pi\sqrt{\det \gamma}} \exp\left(-\frac{1}{2}(\xi - D)\left[\gamma\right]^{-1}(\xi - D)^T\right). \tag{2.32}$$

Gaussians states are typically easier to work with theoretically than more general states of light because of this compact description.

Two types of CV states will be important for later chapters, so we define them here. First, we have the *coherent states*:

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle . \tag{2.33}$$

Coherent states, defined for all $\alpha \in \mathbb{C}$, are eigenstates of the ladder operator, with eigenvalues α. The coherent states form an overcomplete basis for the state space of a single mode, so any quantity of interest can be expressed using them. The other important states are the *squeezed vacuum states*. For any $\zeta \in \mathbb{C}$, with $r = |\zeta|$ and $\vartheta = \arg\zeta$, these states are given by:

$$|\zeta\rangle = \sqrt{\text{sech}(r)}\sum_{n=0}^{\infty}\frac{\sqrt{(2n)!}}{n!}\left[-\tfrac{1}{2}e^{i\vartheta}\tanh(r)\right]^n |2n\rangle . \tag{2.34}$$

Coherent states and squeezed states are not only Gaussian states, but they also share the virtue of being *minimum uncertainty states*. To understand this property, we introduce the general quadrature operators, defined for any angle $\phi \in [0, 2\pi]$:

$$\hat{x}_\phi := \frac{1}{\sqrt{2}} \left(\hat{a}^\dagger e^{i\phi} + \hat{a} e^{-i\phi} \right). \tag{2.35}$$

The operators for angles ϕ and $\phi + \frac{\pi}{2}$ are said to be *conjugate quadratures*, since they satisfy the commutation relation

$$\left[\hat{x}_\phi, \hat{x}_{\phi+\frac{\pi}{2}} \right] = i\hat{\mathbb{1}}. \tag{2.36}$$

Alternatively, we have $\hat{x}_\phi = \hat{x}\cos\phi + \hat{p}\sin\phi$, so the regular quadrature operators $\hat{x}$ and $\hat{p}$ correspond to angles $\phi = 0$ and $\phi = \frac{\pi}{2}$, respectively. Because of the commutation relation (2.36), any physical state must satisfy the *Heisenberg uncertainty relation*

$$\mathrm{Var}\left(\hat{x}_\phi\right) \mathrm{Var}\left(\hat{x}_{\phi+\frac{\pi}{2}}\right) \geq \frac{1}{4}, \tag{2.37}$$

where $\mathrm{Var}(\hat{O}) := \left\langle \hat{O}^2 \right\rangle - \left\langle \hat{O} \right\rangle^2$ for any operator $\hat{O}$. States that achieve the lower bound $\frac{1}{4}$ for some angle ϕ are called minimum uncertainty states. States that are not minimum uncertainty states are said to have *excess noise*. In particular, all mixed states will have some excess noise.

For coherent states, the parameter α is related to the quadratures,

$$\langle \alpha | \hat{x}_\phi | \alpha \rangle = \frac{1}{\sqrt{2}} \left(\alpha e^{-i\phi} + \alpha^* e^{i\phi} \right). \tag{2.38}$$

Coherent states also have fixed variance in every direction,

$$\mathrm{Var}_{|\alpha\rangle}\left(\hat{x}_\phi\right) = \mathrm{Var}_{|\alpha\rangle}\left(\hat{x}_{\phi+\frac{\pi}{2}}\right) = \frac{1}{2}, \tag{2.39}$$

so they achieve the minimum value of the uncertainty relation (2.36) for all ϕ. Squeezed vacuum states, on the other hand, have first moments of zero,

$$\langle \zeta | \hat{x}_\phi | \zeta \rangle = 0. \tag{2.40}$$

Because of this, the variances of a squeezed state are equal to the corresponding second moments

$$\begin{aligned} \mathrm{Var}_{|\zeta\rangle}\left(\hat{x}_\phi\right) =& \langle \zeta | \hat{x}_\phi^2 | \zeta \rangle \\ =& \frac{1}{2} \left[e^{2r} \sin^2\left(\phi - \tfrac{\vartheta}{2}\right) + e^{-2r} \cos^2\left(\phi - \tfrac{\vartheta}{2}\right) \right]. \end{aligned} \tag{2.41}$$

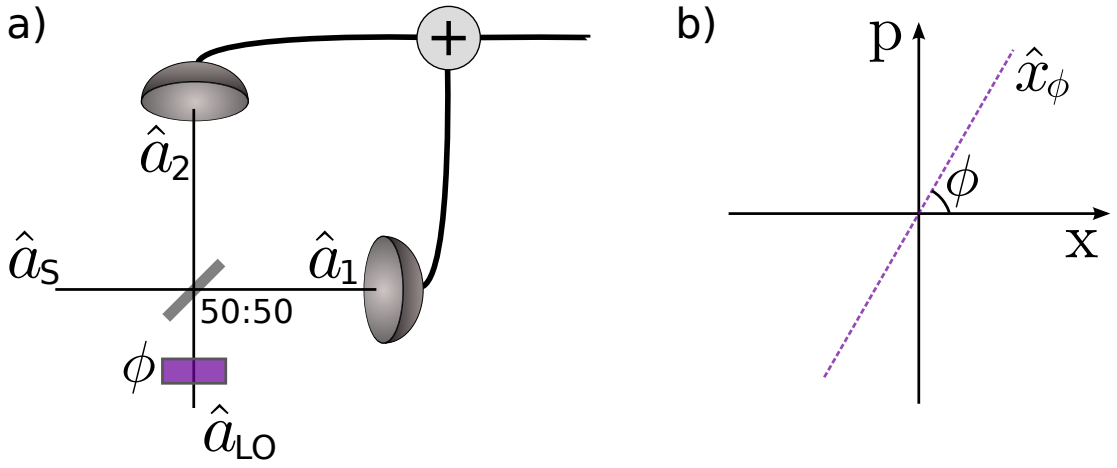


Figure 2.2: a) Measurement apparatus for balanced homodyne detection. b) When the local oscillator is phase-shifted by ϕ, the homodyne apparatus provides the expectation value of the quadrature $\hat{x}_\phi$

Squeezed states achieve the minimum value $\frac{1}{4}$ in the uncertainty relation (2.37) when either $\zeta = 0$ (i.e., there is no squeezing), or when the angles satisfy $\phi - \frac{\vartheta}{2} = k\frac{\pi}{2}$, $k \in \mathbb{Z}$. In the second case, the variances are either given by

$$\mathrm{Var}_\zeta\left(\hat{x}_\phi\right) = \tfrac{1}{2}e^{-2r},\ \mathrm{Var}_\zeta\left(\hat{x}_{\phi+\frac{\pi}{2}}\right) = \tfrac{1}{2}e^{2r} \tag{2.42}$$

or vice versa.

Homodyne measurement

A convenient setup for measuring CV states is *balanced homodyne detection* [109], depicted in Fig. 2.2. This scheme involves interfering a signal mode with a reference field (called the *local oscillator*) in a strong coherent state at a 50/50 beam splitter. The signal and local oscillator should have a fixed phase relationship, which is usually accomplished by generating both fields from the same master laser. The local oscillator phase, relative to some global reference point, is set by a phase shifter to some value ϕ. After interference, the two output modes are fed into separate linear-response photodiodes, which output electronic currents proportional to the incident intensity. These currents are then subtracted electronically to yield the quantity of interest.

Mathematically, we represent the signal and local oscillator modes by their ladder operators $\hat{a}_S$ and $\hat{a}_{LO}$. The output modes $\hat{a}_1$ and $\hat{a}_2$ are related to the signal and local

oscillator modes by the beamsplitter relation

$$\hat{a}_{1/2} = \frac{1}{\sqrt{2}} \left(\hat{a}_S \mp \hat{a}_{LO} \right). \tag{2.43}$$

The photocurrents I_1 and I_2 in each detector arm are proportional to the incident photon numbers $\hat{n}_1$ and $\hat{n}_2$, so the difference photocurrent $I_{21} = I_2 - I_1$ is proportional to the observable

$$\hat{n}_{21} = \hat{n}_2 - \hat{n}_1 = \hat{a}_{LO}\hat{a}_S^\dagger + \hat{a}_{LO}^\dagger \hat{a}_S. \tag{2.44}$$

The local oscillator is fixed in a strong coherent state $|\alpha_{LO}\rangle$, where $\alpha_{LO} = |\alpha_{LO}|e^{i\phi}$ and $|\alpha_{LO}|$ is large. This state is decoupled from the signal (i.e., the bipartite state input to the homodyne apparatus is of the form $\rho_S \otimes \rho_{LO}$), so the above observable reduces to

$$\hat{n}_{21} = \sqrt{2}|\alpha_{LO}| \left(\hat{a}_S^\dagger e^{i\phi} + \hat{a}_S e^{-i\phi} \right) = \sqrt{2}|\alpha_{LO}|\hat{x}_\phi, \tag{2.45}$$

where $\hat{x}_\phi$ denotes a general quadrature operator for the signal mode. Hence, the homodyne detector performs a measurement of the signal quadrature along angle ϕ in phase space.

As stated in Eq. (2.27), the quadrature operators $\hat{x}$ and $\hat{p}$ are related to the marginals of the Wigner function along the x and p axes. The same correspondence holds between the general quadrature operators $\hat{x}_\phi$ and $\hat{x}_{\phi+\frac{\pi}{2}}$ and the marginal distributions at angles ϕ and $\phi + \frac{\pi}{2}$. When we have many identical copies of a state ρ at our disposal, we may use homodyne measurements to tomographically reconstruct the state. This is accomplished by first fixing the phase angle ϕ and measuring enough copies of the state to get an accurate marginal distribution for that angle. By repeating this process over many angles $\phi \in [0, \pi]$, we can reconstruct the full Wigner function to arbitrary precision, giving us a complete description of the state [59, 69].

Chapter 3

Remote state preparation benchmarks

This chapter is devoted to quantum benchmarks for a particular discrete-encoded quantum communication protocol, namely remote state preparation (RSP). The material in this chapter, as well as the accompanying App. A, is based largely on [53], for which I am the primary author and theoretical researcher. The published article is copyright 2010 by the American Physical Society (APS). Portions of the article have been adapted for this thesis, under permission from APS.

The field of quantum information processing has revealed many communication and computational protocols that can theoretically outperform their classical counterparts [11, 75]. Among the most famous quantum information protocols is quantum teleportation [8], wherein a user Alice uses pre-shared entanglement and limited forward classical communication to produce an arbitrary unknown quantum state at the location of another user, Bob. Remote state preparation [63, 78] is a variant of teleportation where Alice has full knowledge of the state she intends to prepare at Bob's location. RSP protocols have several practical applications including forming part of deterministic arbitrary single-photon sources [51] or efficient, high-fidelity quantum repeaters [86].

However, due to the practical limitations of imperfect devices, no RSP experiment can yield remotely-prepared output states that *exactly* match the intended states. Indeed, we should be satisfied when the output states have a high fidelity with the intended states. This raises the question: how high must this fidelity be, on average, to demonstrate a quantum advantage? If we restrict Alice and Bob to a comparable, fixed amount of classical communication, e.g., two classical bits for RSP of qubit states—but no shared entanglement—what is the optimal average RSP fidelity they could achieve? It is only when an experiment surpasses such a classical threshold that we can be sure of having demonstrated the advantage of quantum communication.

In several early publications on teleportation, benchmarks are given to justify which results are genuinely in the non-classical regime [27, 10, 12, 13]. For example, for the teleportation of qubit states, average fidelities higher than $\frac{2}{3}$ are not possible with only classical communication [70]. However, although a number of RSP experiments have been performed to varying degrees [5, 86, 51, 25, 81, 108, 62, 107], there are almost no accompanying benchmarking tests or results. Notably, the authors of Ref. [95] introduced thresholds for RSP in the context of cluster state quantum computing. Their definition and the calculated benchmarks for the two specific situations they discuss coincide with some later results in this chapter. Although they make similar observations as we do in this chapter, they stop short of building a general benchmarking framework.

The material in this chapter is meant to address the lack of RSP benchmarks. By outlining a general framework for RSP protocols and examining the limits on RSP with

and without shared entanglement, we derive several benchmarks for separating genuinely quantum results from those that can be achieved with only classical communication. These benchmarks cover a variety of cases, including pure states, mixed states, finite ensembles, and continuous ensembles. At the end, we use these derived results to benchmark a real-world RSP experiment.

3.1 Benchmarking framework

The goal of remote state preparation is to prepare a quantum state at a distant location, without sending the actual state. Alice, the sending party, knows exactly the target state ρ^{tar} that she wants Bob, the receiving party, to have. The required communication resources (classical and/or quantum) for performing this task are limited, yet the protocol should yield output states ρ^{out} at Bob's location that closely match the target states ρ^{tar} that Alice intended to prepare. There is no universally preferred measure for evaluating protocol performance, but in benchmarking situations where we want target and output states to match, the quantum fidelity (Eq. (2.6)) is a suitable choice. Ideally, the fidelity should be $F(\rho^{\text{tar}}, \rho^{\text{out}}) = 1$ for any target state.

In order to make meaningful comparisons, we need a common framework to test the performance of RSP protocols and experiments (see Fig. 3.1). We imagine that Alice and Bob are challenged with the following task.

RSP framework. *Both parties are given full prior knowledge of some fixed ensemble of target states* $\{\rho_\alpha^{\text{tar}}, p_\alpha\}$*, and may coordinate beforehand on their strategy. Alice samples from the ensemble and, with probability* p_{α_0}*, she picks the index* α_0[1]*. She communicates a message to Bob, sending a limited number* c *of classical bits (*cbits*). Without any further communication, Bob prepares an output state* $\rho_{\alpha_0}^{\text{out}}$*. Their goal is for the output states to match the target states with the highest possible quantum fidelity, on average, i.e., to maximize the quantity*

$$\overline{F} = \sum_\alpha p_\alpha F(\rho_\alpha^{\text{tar}}, \rho_\alpha^{\text{out}}). \tag{3.1}$$

We will be considering the situation where the target ensemble consists of a finite number of states as well as that where the target ensemble forms a continuum. In the latter situation, the above sum and probabilities are generalized to an integral and probability densities, respectively.

[1]Unlike teleportation, Alice accesses the state *index*, not the state, though she has complete information about the state and may prepare herself a copy if desired.

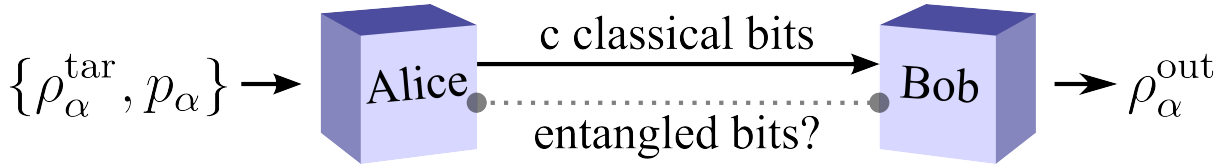


Figure 3.1: Schematic of remote state preparation protocols. Alice samples a state ρ_α^{tar} from a given distribution of target states and Bob aims to prepare a closely matching state. In classical RSP protocols, Alice may send only a limited number of classical bits to Bob. In quantum RSP protocols, the parties also share some pre-distributed entanglement. Their goal is to maximize $\sum_\alpha p_\alpha F(\rho_\alpha^{\text{tar}}, \rho_\alpha^{\text{out}})$, the RSP fidelity averaged over the entire target distribution.

We are concerned in this work with two types of remote state preparation, which we call 'quantum RSP' and 'classical RSP'. These labels refer to the communication resources allowed, not the state prepared, which is always quantum mechanical. In the quantum case, Alice and Bob share a pre-distributed entangled state to help with their task. In the classical case, no initial quantum correlations between Alice and Bob are allowed. In both cases, once a target state has been selected, only c cbits may be sent, and this classical communication is only permitted one way, from Alice to Bob. We will now investigate both of these cases separately.

3.1.1 Quantum RSP

For a quantum RSP protocol, the two users share some pre-distributed entangled state, which may be used to reduce the classical communication cost of the protocol. In this subsection, we will review a scheme for the remote preparation of arbitrary single qubit states with the aid of a Bell state (also called an *ebit*). The experimental implementation of this protocol, achieved via linear optics, will be tested against the theoretical benchmarks derived throughout the rest of this chapter.

Because of the similarity between RSP and teleportation, explicit RSP protocols can be given based on analogous teleportation protocols [63]. Because Alice has knowledge of the states to be prepared, the task of RSP should be easier than teleportation, both in terms of resource requirements and performance. This makes it harder to demonstrate a quantum advantage. It has been proven that two cbits and one ebit are necessary and sufficient communication resources for the remote preparation of an arbitrary pure qubit state [63, 60, 38]. This is the same communication cost as teleportation, but the advantage of RSP is that it does not require joint Bell-state measurements, which can be

experimentally demanding to perform, especially in linear-optical implementations [17, 56]. If we prepare states from a more restricted ensemble, then the required communication cost can be smaller. The following protocol [53], based partially on [83], uses at most two cbits and one ebit for remote preparation of arbitrary pure or mixed qubit states[2].

Consider first the Bell state $|\Phi^+\rangle$ from Eq. (2.21). This Bell state can be rewritten in terms of any arbitrary pure state $|\psi(\theta,\varphi)\rangle$ as

$$\left|\Phi^+\right\rangle = \frac{1}{2}\sum_{m=0}^{3} \sigma_m^A \otimes \sigma_m^B \left|\psi^*\right\rangle_A \otimes \left|\psi\right\rangle_B , \tag{3.2}$$

where $|\psi^*(\theta,\varphi)\rangle$ is the complex conjugate of $|\psi(\theta,\varphi)\rangle$ in the computational basis $\{|0\rangle, |1\rangle\}$, and $\sigma_m^{A(B)} \in \{\hat{\mathbb{1}}, X, XZ, Z\}$ are Pauli operators acting on Alice's (Bob's) system. When Alice wishes to remotely prepare the pure state $|\psi(\theta,\varphi)\rangle$, she first performs a measurement on her system using the following POVM:

$$\{E(\theta,\varphi)\} = \{\tfrac{1}{2}\sigma_m \left|\psi^*\right\rangle\!\left\langle\psi^*\right| \sigma_m^\dagger\}_{m=0}^3. \tag{3.3}$$

If she receives outcome $m \in \{0,1,2,3\}$, Bob's qubit will be left in the state $\sigma_m |\psi\rangle\langle\psi| \sigma_m^\dagger$. By communicating the outcome m using 2 cbits, Bob can learn the state of his qubit. Since the Pauli operators are unitary, Bob can recover $|\psi\rangle\langle\psi|$ by applying the correction $\sigma_m^\dagger$.

Finally, observe that if Alice replaces the proper message by some fixed one (e.g., '00'), and Bob acts as above, then Bob's qubit will be in the mixed state $\frac{1}{2}\hat{\mathbb{1}}$. By mixing these two strategies (with probability r, Alice sends the correct measurement result; otherwise, she sends '00'), they can prepare any mixed qubit state. Notice that this reduces the expected communication cost of the protocol (i.e., the Shannon entropy) to less than 2 cbits.

Before moving to an investigation of classical RSP protocols, we remind the reader of the fact that linear-optical experiments typically require postselection of data on successful detection of photons. The linear-optical experiment which is benchmarked later in this chapter is no different; it is possible that Alice performs her part of the protocol but Bob never receives his photon from the entangled state $|\Phi^+\rangle$. For benchmarking purposes, we will assume a fair-sampling hypothesis, namely that the postselected set of experimental outcomes is statistically representative of the full experiment. The reader is referred to [53] for more detailed discusssion.

[2]Author's declaration: I did not aid in the design of this protocol, nor its experimental implementation.

3.1.2 Classical RSP

We now examine the classical case, where Alice and Bob share no entanglement. As our goal is to find the optimal achievable fidelity $\overline{F}^{\max}$, we assume in this scenario that Alice and Bob are unencumbered by the imperfections of real-world devices. This assumption is in the spirit of security proofs for quantum key distribution, where any adversary Eve is assumed to be limited only by the laws of physics. It is only by surpassing the limits of this ideal scenario that an experiment can provably demonstrate genuine quantum advantages. Therefore, the one-way classical channel between Alice and Bob is assumed to be perfect, as is Bob's ability to prepare any desired output state.

To enable an experimental comparison, the specific benchmark values calculated in this chapter are for qubit states. However, many of the results in this section hold equally well for states in any finite dimensional Hilbert space. We begin with no assumptions about the dimension except that it is finite, and we will specialize to qubits (dimension 2) when appropriate. Furthermore, we are primarily interested in the case where the target states are pure, $\rho_\alpha^{\text{tar}} = |\psi_\alpha^{\text{tar}}\rangle\langle\psi_\alpha^{\text{tar}}|$, so that the quantum fidelity is equal to the matrix element

$$F(\rho_\alpha^{\text{tar}}, \rho_\alpha^{\text{out}}) = \left\langle \psi_\alpha^{\text{tar}} \right| \rho_\alpha^{\text{out}} \left| \psi_\alpha^{\text{tar}} \right\rangle . \tag{3.4}$$

Accordingly, we assume that the target ensemble consists of pure states $\{|\psi_\alpha^{\text{tar}}\rangle, p_\alpha\}$. In Sec. 3.2 we give benchmarks based on specific choices for this target ensemble.

We now examine the question: what is the optimal RSP strategy when the parties share no entangled state, and Alice may only send c cbits to Bob? For every target state $|\psi_\alpha^{\text{tar}}\rangle$, Alice sends a string of c classical bits. We can label all messages of this type by a natural number $m(\alpha) = k \in \{0, 1, ..., 2^c - 1\}$. In general, the message assignment may be either deterministic (e.g., $m(\alpha) = 3$) or probabilistic, i.e., $m(\alpha) = k$ with probability $q_k(\alpha)$, where for each α, $\sum_k q_k(\alpha) = 1$. Deterministic message schemes effectively split the target states into fixed partitions. The probabilistic framework contains all deterministic strategies as special cases.

Upon receiving the message k, Bob prepares some output state ρ_k^{out}. A probabilistic messaging strategy would necessarily lead Bob to prepare a *mixed* output state $\rho_\alpha^{\text{out}} = \sum_k q_k(\alpha)\rho_k^{\text{out}}$ whenever state $|\psi_\alpha^{\text{tar}}\rangle$ is chosen. Similarly, for a given message k, Bob may change the output state probabilistically. This strategy is naturally incorporated into our framework, where we allow the output states ρ_k^{out} to be mixed.

To determine which choice of output states optimize the average fidelity, we rewrite it

in terms of the 2^c unique messages:

$$\begin{aligned}\overline{F} &= \sum_{\alpha} p_\alpha \left\langle \psi_\alpha^{\text{tar}} \right| \rho_\alpha^{\text{out}} \left| \psi_\alpha^{\text{tar}} \right\rangle \\ &= \sum_{k=0}^{2^c-1} \sum_{\alpha} p_\alpha q_k(\alpha) \text{Tr}(\left| \psi_\alpha^{\text{tar}} \right\rangle\!\left\langle \psi_\alpha^{\text{tar}} \right| \rho_k^{\text{out}}) \\ &= \sum_{k=0}^{2^c-1} p_k \text{Tr}(\overline{\rho_k} \rho_k^{\text{out}}) \end{aligned} \tag{3.5}$$

where $p_k = \sum_\alpha p_\alpha q_k(\alpha)$ is the probability of Alice sending message k and

$$\overline{\rho_k} = \frac{1}{p_k} \sum_{\alpha} p_\alpha q_k(\alpha) \left| \psi_\alpha^{\text{tar}} \right\rangle\!\left\langle \psi_\alpha^{\text{tar}} \right| \tag{3.6}$$

is a weighted average of the states where message k might be sent. When the fidelity is written in this form, two notable features become apparent:

1. For each k, the quantity $\text{Tr}(\overline{\rho_k} \rho_k^{\text{out}})$ is upper bounded by the largest eigenvalue $\lambda_k^{\max}$ of the average state $\overline{\rho_k}$; this can be achieved if Bob outputs the corresponding eigenstate $\rho_k^{\text{out}} = |\lambda_k^{\max}\rangle\langle\lambda_k^{\max}|$. Thus, the optimal output states give

$$\overline{F}^{\max} = \sum_{k=0}^{2^c-1} p_k \lambda_k^{\max}. \tag{3.7}$$

2. Since the optimal fidelity depends on the purity of the average states $\overline{\rho_k}$ (by point 1), the optimal messaging strategy must be deterministic, not probabilistic. In other words, a fixed message is sent for each target state. This corresponds to only one $q_k(\alpha)$ being non-zero for each α.

Taking these two points into account greatly simplifies the structure of the fidelity optimization. Because the optimal message assignment is deterministic, the target ensemble is effectively split into 2^c disjoint partitions, depending only on the message $k \in \{0, 1, ..., 2^{c-1}\}$. For each partitioning of the target ensemble, we can also calculate the optimal output state and the resulting fidelity value using Eq. (3.7). All that remains is to determine *which partitioning* maximizes the value of Eq. (3.7). To clarify notation, we will henceforth use k to label both a message and the partition of the target ensemble

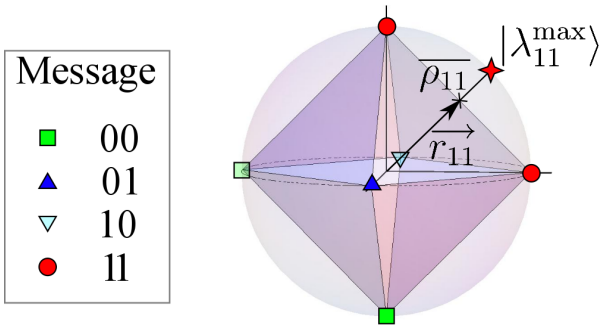


Figure 3.2: Example of a possible classical remote state preparation strategy. The target ensemble consists of the 6 pure states $\{|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)\}$ (represented here as the vertices of an octahedron inscribed within the Bloch sphere) with equal probabilities. A possible partitioning strategy is given for the case where two cbits of classical communication are allowed, and the optimal output state for partition 11 is detailed.

consisting of states for which that message is sent. The meaning will be clear from the context.

In principle, for a finite number n of target states, the remaining optimization problem only requires checking the value of Eq. (3.7) for each of the finite number of possible partitionings, which can be done by computer. However, the number of possible partitionings scales exponentially in n, rendering this calculation unreasonable for more than about $n = 10$ states. In Sec. 3.2 we outline an algorithm that efficiently provides relatively tight bounds to Eq. (3.7).

Qubits

If the states in question are qubits, we can put Eq. (3.7) into a simple geometric form. When expressed in its eigenbasis, a qubit state takes the form

$$\rho = \frac{1}{2}\begin{bmatrix} 1+r & 0 \\ 0 & 1-r \end{bmatrix} \tag{3.8}$$

where r is the radius of the state's Bloch vector. The largest eigenvector of a qubit is directly related to the radius: $\lambda^{\max} = \frac{1+r}{2}$. For any deterministic partitioning of the target ensemble, we denote the average Bloch vectors by $\vec{r}_k = \frac{1}{p_k}\sum_{\alpha\in k} p_\alpha \vec{r}_\alpha$ and their magnitudes by r_k. We find that the maximal average fidelity for qubits is given by

$$\overline{F}^{\max} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k r_k\right). \tag{3.9}$$

Hence, for a given deterministic partitioning, the best average fidelity is determined by two sets of quantities: the probabilities p_k of sending each message and the length of the average Bloch vectors $\vec{r}_k$ within each of the 2^c partitions. In the next section, we will outline how to determine which choice of messages, i.e., which partitioning of the target ensemble, maximizes Eq. (3.9).

3.2 Threshold calculations

3.2.1 Finite ensembles

Assume now that we have fixed a *finite* ensemble of target states $\{\rho_\alpha^{\text{tar}}, p_\alpha\}_{\alpha=1}^n$. It is clear that whenever $n \leq 2^c$, the optimal classical protocol can achieve perfect fidelity since there is sufficient capacity in the message to uniquely label the state. The interesting cases have $n > 2^c$. Given the results of the previous section, the optimum average fidelity can be determined by checking the value of Eq. (3.7) for all partitionings of the n target states into 2^c disjoint subsets, but this can be inefficient even for modest values of n and c.

Upper bounding the maximal classical fidelity

Instead of directly checking every possible partition to determine the maximal classical fidelity $\overline{F}^{\max}$, it can be useful to instead find some upper bound $\overline{F}^{\text{bound}}$ on this quantity which is easier to compute. If an experiment surpasses the upper bound, it has demonstrated its quantum nature, since we would have

$$\overline{F}^{\text{observed}} > \overline{F}^{\text{bound}} \geq \overline{F}^{\max}. \tag{3.10}$$

We will now outline an efficient algorithm for determining such upper bounds. For this algorithm, we make the additional assumption that each target state has equal probability to be chosen from the target ensemble. We note that each partition contains some number s of states and contributes one term to the sum in Eq. (3.7). Two different partitions with the same number of states may contribute differently to the average fidelity, depending on the arrangement of the states. However, for each number $s \in \{0, 1, ..., 2^c - 1\}$, there

is a set of s states that yields the maximal possible contribution $\overline{F}_s^{\max}$. By using these maximal values in Eq. (3.7) instead of the actual values, we obtain an upper bound on the threshold.

The first step in the algorithm involves checking all partitions of size s to find the maximal contribution $\overline{F}_s^{\max}$. Next, we list all the ways in which n elements can be divided into 2^c subsets. The order of the subsets does not matter, so for simplicity we can create our list in order of decreasing partition size. This list forms a table with 2^c columns. For each row i, we have a list of numbers $\{s_{ij}\}_{j=0}^{2^c-1}$ that sum to n. To determine the upper bound, we calculate the quantity

$$\overline{F}_i = \sum_{j=0}^{2^c-1} \frac{s_{ij}}{n} \overline{F}_{s_{ij}}^{\max}. \tag{3.11}$$

The highest $\overline{F}_i$ provides us with an upper bound on the optimal average fidelity, i.e.,

$$\overline{F}^{\text{bound}} := \max_i \overline{F}_i. \tag{3.12}$$

It may even be the case that the threshold is equal to the upper bound found via the above algorithm, especially if the target ensemble exhibits a high degree of symmetry. To verify this, one would have to find a specific partitioning that leads to the same value as the upper bound. On the other hand, if we can show through other arguments that the highest $\overline{F}_i$ is unachievable, then a new, smaller, upper bound can be obtained by re-running the above algorithm without that unachievable case. We will make use of both of these points below.

Benchmarks

Before proceeding, we pause to discuss the tradeoff between classical and quantum communication resources. The remote state preparation scheme outlined in Sec. 3.1.1 uses one entangled qubit (ebit) and two cbits sent from Alice to Bob to remotely prepare pure qubit states and less than two cbits for mixed states. A classical analog might limit Alice to sending two cbits to Bob each run, with Bob not allowed to send any messages to Alice. However, it may be argued that to distribute the entangled qubit between Alice and Bob requires at least one use of a quantum channel. A more fair comparison scenario might then allow Alice one use of this quantum channel per run, but only to send classical information. In this scenario, Alice sends three cbits in total.

Arguably, allowing an extra classical bit is unnecessary as one could consider the entanglement to be distributed by Bob or by a third party. As well, the distribution of entanglement can be restricted to take place before Alice chooses the index. Since Alice and Bob are already allowed to set their strategy in advance, an extra preliminary classical channel use, whether from Alice to Bob or Bob to Alice, would not change anything. However, the more cbits Alice is allowed to transmit, the higher the average fidelity the parties can achieve, rendering the benchmark that much harder to surpass in experiment. For completeness and comparison purposes we henceforth consider both the two and three cbit cases.

Thus far no specific target ensemble has been chosen. We now examine several specific ensembles for comparison with experiment. We restrict ourselves to ensembles of pure qubit states with a uniform distribution: $p_\alpha = \frac{1}{n}$. If our goal is to find benchmarks that are low enough to be experimentally surpassed, we should make the classical task as difficult as possible. Given the results above, this is accomplished by choosing ensembles of states that are maximally 'spread apart', so that the average Bloch vector within any partition is as small as possible.

An effective choice is to use the vertices of the *Platonic solids* inscribed in the Bloch sphere as the target states. The Platonic solids are the tetrahedron, octahedron, cube, icosahedron, and dodecahedron, with 4, 6, 8, 12, and 20 vertices, respectively. Note that the orientation of these vertices with respect to a Cartesian reference frame does not matter in the classical case, but a specific choice must be made in an experiment. Also note that the tetrahedron states do not provide a surpassable benchmark for $c \geq 2$ because they can be prepared with perfect fidelity simply by assigning a unique message to each of the four states. Similarly, for three cbits, the benchmarks yielded by the tetrahedron, octahedron and cube ensembles are all trivially unity. For the other cases, however, we expect fidelity thresholds less than unity.

Indeed, using the algorithm above (Eqs. (3.11-3.12)), we can calculate upper bounds on the remaining thresholds, all of which are less than unity. In fact, for every example studied except for one, the upper bounds were actually equal to the optimal classical thresholds, i.e., $\overline{F}^{\text{bound}} = \overline{F}^{\max}$. This was verified by finding explicit partitions such that Eq. (3.7) saturated the upper bounds. The one exception to this statement is the dodecahedron ensemble when $c = 2$. In this case, the upper bound returned by the algorithm would only be possible if we could partition the dodecahedron vertices into four disjoint pentagons. This is geometrically impossible, so we can omit this upper bound. The next highest bound, consisting of partitions of size 6, 5, 5, and 4, is indeed possible. The optimal thresholds and their corresponding partitions, along with experimental results, are given in Fig. 3.3.

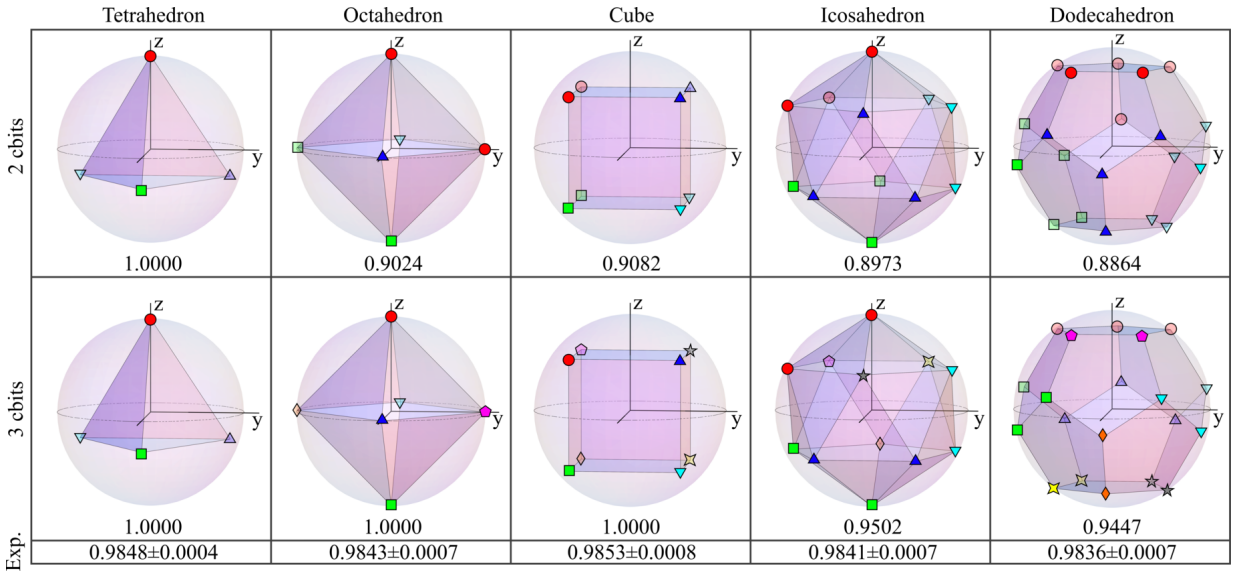


Figure 3.3: Five examples of pure state target ensembles, given by the vertices of the Platonic solids inscribed within the Bloch sphere, with uniform probability distributions. For both two and three cbits message capacity, optimal partitioning strategies are shown, along with the corresponding optimal average fidelity benchmarks. States labeled with the same symbol (e.g., red circles) are in the same partition. The tetrahedron (two or three cbits), octahedron (three cbits), and cube (three cbits) examples can in principle be remotely prepared with perfect fidelity using only classical communication, whereas the remaining ensembles cannot. Experimentally achieved mean fidelities for these ensembles are given in the bottom row; the reported uncertainty is the standard error of the mean. For all non-unity benchmarks, the experimental values surpass the benchmarks for two (three) transmitted cbits by at least 96 (46) times the standard error of the mean. The 2 cbit octahedron bound also appears in Ref. [95].

3.2.2 Continuous ensemble

Perhaps the most meaningful target ensemble is the uniform ensemble of all pure qubit states, i.e., the Bloch sphere itself. For the related problem of teleportation, the optimal classical strategy leads to an average fidelity of $\frac{2}{3}$ [70]. Remote state preparation should be easier than teleportation, since Alice has complete knowledge of the state. The fidelity threshold should therefore be higher, though the threshold will also depend on how many communicated cbits are allowed. Therefore, demonstrating genuine non-classical behaviour experimentally is more difficult for RSP than for teleportation.

We will now derive upper and lower bounds on the classical threshold for both two and three cbits. Many of the results for pure states from the previous section, suitably generalized, still hold here. Partitions will be denoted by Ω_k, with their union forming the surface of the Bloch sphere, $\cup_k \Omega_k = S^2$. The optimal average fidelity is still given by Eq. (3.9), but we make the modifications

$$\begin{aligned} p_k &\to \frac{1}{4\pi}\int_{\Omega_k} \mathrm{d}\Omega = \frac{A_k}{4\pi}, \\ \vec{r}_k &\to \frac{1}{p_k}\frac{1}{4\pi}\int_{\Omega_k} \vec{r}_\alpha \mathrm{d}\Omega = \frac{1}{A_k}\int_{\Omega_k} \vec{r}_\alpha \mathrm{d}\Omega, \end{aligned} \tag{3.13}$$

where A_k is the surface area of partition k.

To obtain lower bounds on the threshold, we simply choose a particular partitioning. For two cbits, we imagine that a tetrahedron is inscribed in the Bloch sphere and connect the four vertices by segments of great circles (note: this is not to be confused with use of Platonic solids in Sec. 3.2.1). This leads to four disjoint regions on the surface of the Bloch sphere which form our partitions. To calculate the optimal average fidelity for this arrangement, we integrate Eq. (3.13) and make use of the following equation for great circles in spherical coordinates: $\cot(\theta) = a\sin(\varphi + c)$ ([72], Lemma 28.1). Here, $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$ are the polar and azimuthal angles, respectively, and a and c are constants determined by substituting two points on the great circle. Using this relation, the bound can be worked out to be 0.8724. For three cbits, we use the eight octants as our partitions (equivalently, we connect the vertices of an inscribed octahedron). This straightforwardly gives a lower bound on the threshold of 0.9330. We conjecture that these two lower bounds are the optimal values, but we cannot provide evidence or proof of this.

To obtain upper bounds, we use an idea similar to the algorithm detailed in Sec. 3.2.1. If we can determine the maximal weighted average fidelity $\overline{F}_A^{\max}$ achievable for a given

surface area A of the sphere, then we can calculate an upper bound using these values:

$$\overline{F}^{\max} \leq \sum_{k=0}^{2^c-1} \overline{F}_{A_k}^{\max} \; s.t. \; \sum_{k=0}^{2^c-1} A_k = 4\pi. \tag{3.14}$$

Out of all possible configurations of a given partition with area A_k, a circular cap on the Bloch sphere gives the longest average Bloch vector, and hence the largest average fidelity. Also, the optimal distribution occurs when all partition areas are equal, $A_k = \frac{4\pi}{2^c} \; \forall \; k$ (see App. A.1 for proofs of these statements). Of course, it is only possible to cover the Bloch sphere with 2^c disjoint circular caps when $c = 0$ or 1, so the upper bounds for $c \geq 2$ are not achievable.

Using the equations derived in App. A.1, the upper bounds for $c = 2$ and $c = 3$ work out to be 0.8750 and 0.9375, respectively. Even these simple ideas yield reasonably tight bounds on the continuum thresholds for two and three cbits, which we summarize in the following proposition.

Proposition 3.2.1 (Continuous ensemble fidelity bounds)**.** *For RSP of arbitrary pure states on the Bloch sphere, the optimal average fidelity achievable by protocols allowed c cbits of communication from Alice to Bob is confined to the following numerical regions:*

$$0.8724 \leq \overline{F}^{\max} < 0.8750 \text{ for } c = 2,$$
$$0.9330 \leq \overline{F}^{\max} < 0.9375 \text{ for } c = 3.$$

These numbers are significantly higher than the optimal classical teleportation fidelity of $\frac{2}{3}$. This confirms that, when restricted to classical communication only, the remote preparation of a known quantum state is indeed easier than the teleportation of an unknown quantum state. It is thus more difficult to demonstrate a genuine quantum advantage in an RSP experiment than in a teleportation experiment.

3.2.3 Mixed states

Here we consider the same type of qubit ensembles as in Sec. 3.2.1, but with the modification that every state in an ensemble is a mixed state with Bloch vector length r. Unfortunately, if the target states are mixed states, finding classical thresholds is more complicated than in the pure state case. For instance, the optimal strategy is not necessarily one with deterministic messaging. Consider a target ensemble consisting of the three

qubit states $\rho_{\alpha_1}^{\text{tar}} = |0\rangle\langle 0|$, $\rho_{\alpha_2}^{\text{tar}} = |1\rangle\langle 1|$, $\rho_{\alpha_3}^{\text{tar}} = \frac{1}{2}\hat{\mathbb{1}}$ with equal probability $\frac{1}{3}$. Alice sends messages according to the distribution

$$\begin{aligned} q_0(\alpha_1) = 1,\ q_1(\alpha_1) = 0 \\ q_0(\alpha_2) = 0,\ q_1(\alpha_2) = 1 \\ q_0(\alpha_3) = \frac{1}{2},\ q_1(\alpha_3) = \frac{1}{2}, \end{aligned}$$

and Bob prepares the two output states $\rho_0^{\text{out}} = |0\rangle\langle 0|$, $\rho_1^{\text{out}} = |1\rangle\langle 1|$. It is easy to see that this probabilistic messaging strategy, which uses only one cbit, allows Alice and Bob to remotely prepare any of these three states with arbitrarily high fidelity.

In fact, for any target ensemble that is contained in the convex hull of $N \leq 2^c$ suitably chosen points, Alice and Bob can achieve an arbitrarily high fidelity by using a probabilistic messaging strategy. For instance, if Alice has access to two cbits, she could specify four pure states that form the vertices of a tetrahedron and prepare any state within this tetrahedron with perfect fidelity. Similarly, with three cbits, she could perfectly prepare any state located within a cube whose vertices were pure states. For example, consider a uniform dodecahedron ensemble with each state having Bloch radius r. For two (three) cbits, if this radius is not larger than the radius of a sphere inscribed in the tetrahedron (cube), then the ensemble can be prepared with perfect fidelity. For two (three) cbits, the insphere radius is $\frac{1}{3}$ $(\sqrt{\frac{1}{3}})$. Similar statements can be made for any ensemble with states of constant radius.

The possibility that the optimal strategy could involve probabilistic messaging renders the optimization trickier, as we can no longer use a partitioning argument to find the optimal value. Another approach is to focus on finding the optimal strategy that involves only deterministic messages. This is the special case where, for each target state ρ_α^{tar}, only one of the $q_k(\alpha)$ is non-zero. The optimal value in this case, found by optimizing over output states, provides a lower bound to the true optimum. Unfortunately, this restriction does not fairly match with the experimental protocol outlined in Sec. 3.1.1, where messages are probabilistically determined by measurement outcomes. However, surpassing this bound is at least a *necessary* condition, if not a sufficient one, for any remote state preparation experiment to demonstrate non-classical advantages. Assuming deterministic messaging, we can give the following formula for the classical threshold.

Proposition 3.2.2. *Let the target states all have the same Bloch vector radius $r \in (0, 1]$. If Alice's messages are deterministic, the optimal choices of ρ_k^{out} achieve a maximal average*

fidelity of

$$\overline{F}^{\max}_{\text{determ.}} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k \sqrt{r_k^2 + 1 - r^2}\right), \tag{3.15}$$

where p_k and r_k are the same quantities as defined for pure qubit states (Eq. (3.9)).

A proof of this proposition is provided in App. A.2. In general, this optimal value is achieved using mixed output states. The fidelity in Eq. (3.15) is modified from the pure state case, Eq. (3.9), by the additional term $1 - r^2$ under the square root. Since this term is fixed beforehand and the same for every k, it does not change which partitioning of the target ensemble is optimal. In other words, whichever partitioning maximizes Eq. (3.9) for an ensemble of pure states will also maximize Eq. (3.15), the classical fidelity threshold for the corresponding ensemble with Bloch radius r. Experimental data is compared with these theoretical bounds in Fig. 3.5.

3.3 Experimental test

The above benchmarks were used to test a specific linear-optical implementation [53] of the protocol outlined in Sec. 3.1.1. In this experiment, although postselection is used to verify that Alice and Bob share an entangled state, no other 'accidental' photon detection coindences (e.g., due to stray light, detector dark counts, or other flaws) were subtracted. These additional events contribute to the imperfections of the experiment, which will be tested with the benchmarks. The experimental entangled state was imperfect as well, having a fidelity (obtained through tomographic reconstruction) of 0.9807 and 0.9813 with the ideal state over the two days of the experiment. The density matrices of the remotely prepared output qubits were tomographically reconstructed using an overcomplete POVM based on the 6 vectors $\{|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle \pm i\,|1\rangle)\}$ and a maximum-likelihood technique [49].

Pure states $|\psi(\theta,\varphi)\rangle$ were remotely prepared using angles corresponding to the vertices of each of the five Platonic solids inscribed in the Bloch sphere. The specific orientations, along with the corresponding fidelity benchmarks, are shown in Fig. 3.3. The benchmark results are also compared graphically with the thresholds for classical RSP using two and three cbits in Fig. 3.4. For all meaningful cases, where the classical RSP benchmark is less than unity, the experimentally-determined fidelity value conclusively beats the classical threshold. This confirms that the experiment produces data that is not possible without the shared entanglement, even if we allow an additional classical bit.

r	0.00	0.25	0.50	0.75	1.00
Icosahedron	0.99944 $\pm$ 0.00008	0.99967 $\pm$ 0.00007	0.99964 $\pm$ 0.00008	0.9987 $\pm$ 0.0002	0.9841 $\pm$ 0.0007
Dodecahedron	0.9995 $\pm$ 0.00006	0.99961 $\pm$ 0.00003	0.99963 $\pm$ 0.00004	0.9987 $\pm$ 0.00015	0.9836 $\pm$ 0.0007

Table 3.1: Experimentally achieved average RSP fidelities $\overline{F}$ versus Bloch vector radius r (see also Fig 3.5). The data is for ensembles with settings $\{\theta, \varphi\}$ corresponding to the vertices of an icosahedron and dodecahedron with varying outsphere radii r. The reported uncertainty is the standard error of the mean.

To test RSP using mixed states, the icosahedron and dodecahedron ensembles were used, for radii $r \in \{0.00,\ 0.25,\ 0.50,\ 0.75,\ 1.00\}$. The calculated average fidelity values are summarized in Table 3.1. These values are compared in Fig. 3.5 to the lower bounds for classical RSP with deterministic messaging strategies derived in Sec. 3.2.3. Again, the experimental data beats the classical bounds whenever the bounds are less than unity.

Summary and outlook

In this chapter, we developed a number of benchmarking tools for discriminating genuinely quantum RSP experiments from those whose performance is no better than a classical RSP setup. We outlined how to find useful benchmarks for a number of situations, including pure states, mixed states, discrete ensembles, and continuous ensembles. For qubit states, we proposed a number of specific benchmarks based on Platonic solids, which were used to certify a quantum RSP experiment. In all cases considered, the results show a clear violation of the classical benchmark values whenever the classical protocols do not trivially allow for a perfect RSP strategy.

The results found in this chapter are easily adaptable and can be readily used in any future RSP experiment. As well, some of the general results may be useful for benchmarking other discrete quantum systems. One interesting extension to this work would be to deal carefully with post-selection. Because of device inefficiencies and losses, one photon from an entangled pair can sometimes be detected by one party, but the other photon is lost. These single counts are not used in the final analysis. Carefully counting the lost photons and allowing Alice and Bob to use them as comparable classical resources, without loss, would lead to more difficult benchmarks. Yet it would also provide even stronger support for claims that an experiment evidences genuine quantum behaviour.

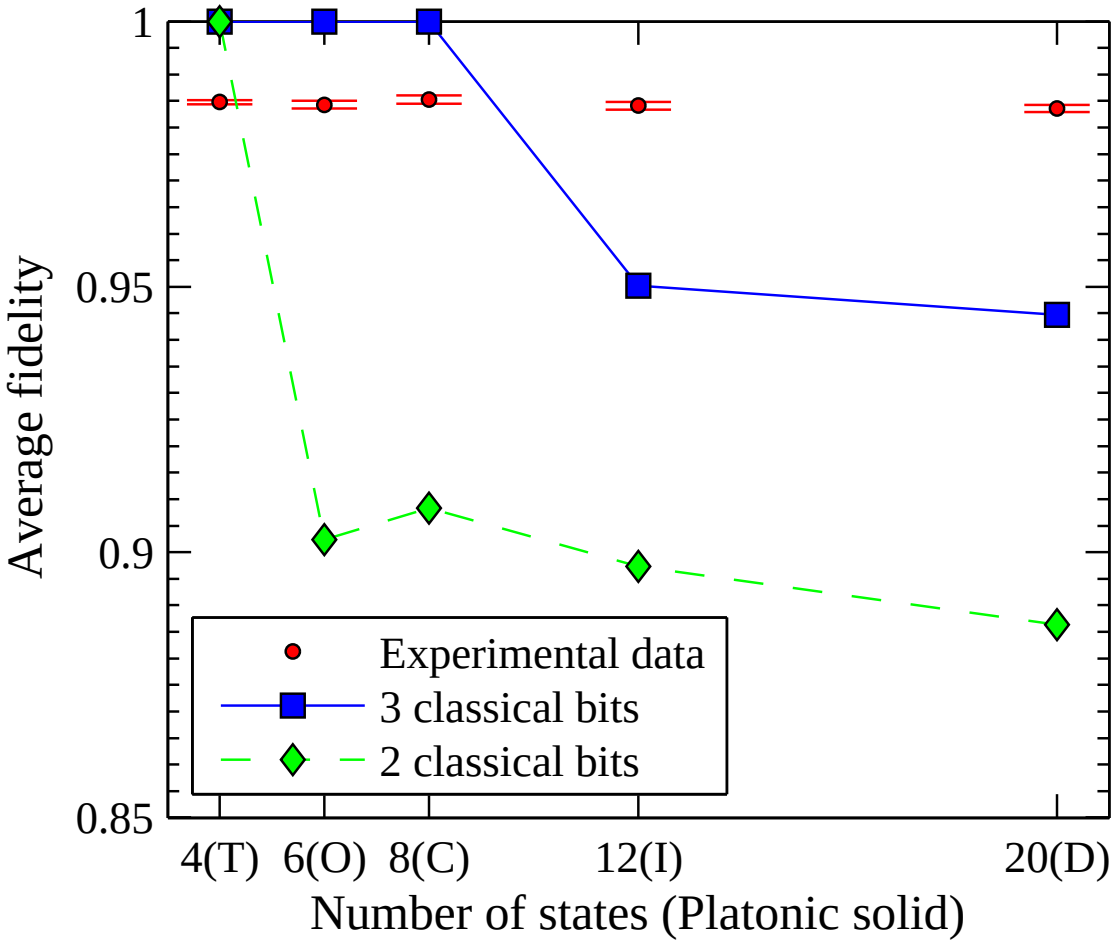


Figure 3.4: Experimentally-achieved mean fidelities $\overline{F}$ and optimal classical benchmarks for target ensembles of pure states based on the five Platonic solids shown in Fig. 3.3. The error bars shown are the standard error of the mean. Any experimental data point above the green diamonds (blue squares) represents results that are not possible with only two (three) cbits communication and no preshared entanglement. In all cases where the classical benchmark is less than unity, the experimental results surpass the benchmarks conclusively. Note: lines are included only to guide the eye and do not represent calculated thresholds.

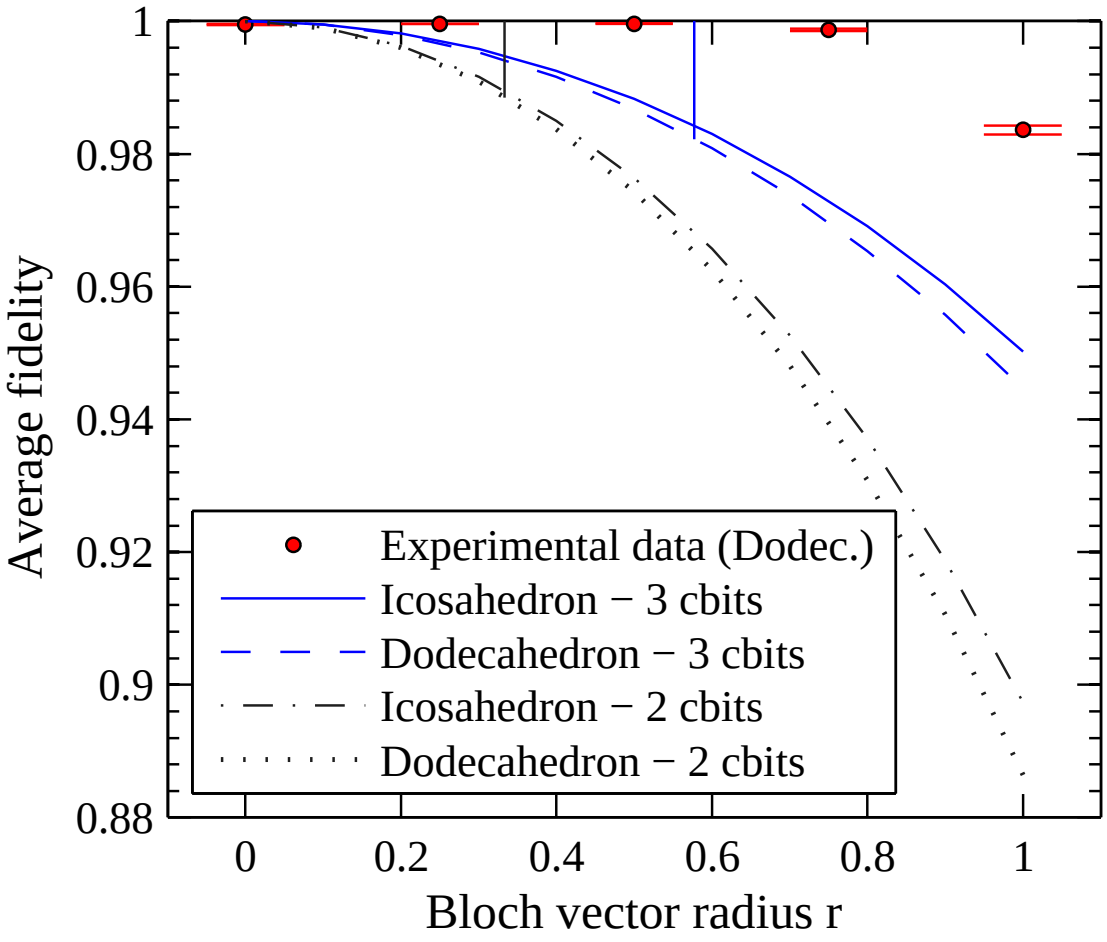


Figure 3.5: Experimentally-achieved mean fidelities and optimal classical thresholds versus Bloch vector radius. The target ensembles consist of uniform distributions of states of Bloch radius r which form the vertices of either an icosahedron or dodecahedron. The lower (upper) pair of lines are bounds on the classical average fidelity arising from specific two (three) cbit classical strategies. Within each pair, the higher bound is for the icosahedron. Experimental data must lie above and to the right of the bounds to be in the quantum regime, but even points in this region may be possible to achieve without pre-shared entanglement by some non-deterministic classical strategy. Experimental data points are for the dodecahedron ensemble. The results for the icosahedron ensembles are similar but were not plotted because at this scale they are not distinguishable from those of the dodecahedron.

Chapter 4

Benchmarking continuous variable quantum communication devices

We saw in the previous chapter that single-photon systems are capable of producing high fidelities in quantum communication protocols. However, one of the weaknesses of the single-photon encoding is its susceptibility to photon loss. In practice, this necessitates the postselection of data based on successful final detection of photons. In scenarios where the communication channel may be accessible to an adversarial eavesdropper Eve, this presents a problem: Eve could exploit this loophole to hide the evidence of her presence.

As an illustrative example, we imagine a protocol where one of two nonorthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}$ is prepared by Alice, with equal probability, using the single-photon encoding. Alice then sends the state to Bob via a quantum channel. Eve intercepts the state and performs the measurement with POVM elements $\hat{P}_0 = a(\hat{\mathbb{1}} - |\psi_1\rangle\langle\psi_1|)$, $\hat{P}_1 = b(\hat{\mathbb{1}} - |\psi_0\rangle\langle\psi_0|)$, and $\hat{P}_? = \hat{\mathbb{1}} - \hat{P}_0 - \hat{P}_1$ for some appropriate coefficients a and b. Such a POVM allows *unambiguous state discrimination* [48], in which Eve either correctly determines the state (without error), or she has an inconclusive outcome. When there is a conclusive outcome, Eve creates a new copy of the appropriate state and forwards it to Bob. When the outcome is inconclusive, Eve blocks any photons from reaching Bob. By postselecting their data, Alice and Bob allow Eve to participate in the protocol undetected. Although this hypothetical protocol is rather simplistic, it illustrates that postselection can be dangerous.

On the other hand, protocols realized with a continuous-variable encoding can avoid many of the issues associated with postselection. In CV protocols, an output state is measured *for every input state*, even if this output state is the vacuum. Photon loss affects the states by attenuating their amplitude in phase space. The drawback of CV protocols is that the fidelity between input and output states may be much lower than in single-photon encodings. But this does not preclude CV systems from being useful for quantum communication. Fidelity is a convenient measure of similarity, but it is not the only tool for benchmarking quantum communication devices. Indeed, we will see in this and the following chapters that *entanglement measures* can be of great use for quantum benchmarking. In particular, entanglement measures will allow us to make useful quantitative benchmarking statements and to compare different devices within the quantum domain.

In this chapter, we will mainly review previous results on quantum benchmarking in CV systems. In particular, we will focus on the *entanglement-based* approach to benchmarking, in which quantum devices can be certified by witnessing the presence of entanglement or entanglement-like correlations. We will review a tool widely used for entanglement-based benchmarking, the *expectation value matrix*. We will then present the first steps for applying entanglement measures to the CV benchmarking problem, relying on projection to finite-dimensional spaces. This chapter leads into Chs. 5 and 6, where we present two choices for this projection, namely a two-qubit projection and a Fock-state projection.

4.1 Quantum benchmarking framework

In this section, we review the underlying framework of quantum benchmarking, focusing mainly on the entanglement-based approach, which has been developed by other authors [85, 84, 37, 35, 36]. The new contributions in this chapter will begin in Sec. 4.2. The framework we outline here is somewhat different from that used for RSP in the previous chapter. We are still concerned about which data can be produced by a classical device, but the definition of a classical device will be appropriately altered. In many quantum communication protocols, especially quantum key distribution schemes, the goal is for two or more users to share strong quantum correlations. Indeed, there is a minimal amount of correlations that must be present for a protocol to be considered genuinely quantum.

Picture the situation, common to many quantum communication protocols, where Alice prepares a quantum state, chosen from some pre-specified ensemble, and sends the state to Bob via a channel. Imagine now that this particular channel functions as follows (see Fig. 4.1). First, the input state is measured with some POVM and the post-measurement state is discarded. Next, the outcome of this measurement is encoded and transmitted as classical data to the output node of the channel. Finally, based on this classical measurement data, a new quantum state is prepared and forwarded to Bob. Such channels are called *measure and prepare* (MP) or *intercept-resend* channels. Although this channel takes quantum states as input and gives quantum states as output, it is not a true quantum-communication channel, since the communication step is accomplished with classical means alone. In fact, by locally performing the same measurements and re-preparations themselves, Alice and Bob can achieve the same results using only a classical channel.

Measure and prepare channels will serve as the classical analog for all following quantum benchmarks. Even if a device is not designed as a MP channel, its operation may be imperfect enough that a MP channel could achieve the same performance. We will make no distinctions between MP channels and channels whose operation can be simulated by MP channels, since we have no way to discriminate between the two. It is often convenient to picture benchmarking in an adversarial way. In this scenario, we allow the possibility that a quantum device could have been replaced by a MP channel trying to pass our quantum tests. Only by conclusively ruling out MP operation can we certify a quantum device as genuine. A potential quantum device can therefore be certified by proving that its operation cannot be simulated by a MP channel. Devices that pass this test are said to be in the *quantum domain*.

With this classical yardstick set, we can proceed to the corresponding quantum bench-

marking scheme. All devices to be tested are treated as black box quantum channels[1], inputing and outputing quantum states on some relevant state spaces $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$. Mathematically, we represent the tested device by a map $\Lambda : \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$. The general benchmarking protocol is the following.

Benchmarking framework. *In each run of the benchmarking protocol, test states are prepared from some fixed ensemble* $\{\rho_\alpha^{\text{in}} \in \mathcal{B}(\mathcal{H}_{\text{in}})\}$ *according to some given probability distribution* $\{p_\alpha \geq 0 | \sum_\alpha p_\alpha = 1\}$. *These test states are input into the device under investigation, and the device outputs the corresponding states* $\{\rho_\alpha^{\text{out}} = \Lambda[\rho_\alpha^{\text{in}}] \in \mathcal{B}(\mathcal{H}_{\text{out}})\}$. *Finally, measurements of some observables* $\{\hat{O}_B^j\}$ *are performed on the output states.*

This procedure is repeated many times to generate statistically faithful measurement data for all of the test states. Using the measurement data and knowledge of the test ensemble, we must determine whether or not the device is in the quantum domain. If we use a sufficient number of test states and a sufficient set of measurements, we can determine the exact functioning of a device, a procedure known as *process tomography*. Having process tomography, we can calculate a device's performance against any theoretical benchmark [64, 65]. However, process tomography can be resource intensive, especially for CV systems. Our goal will be to certify quantum devices with minimal requirements in terms of test states and measurements. If a given benchmarking test fails, it may still be possible to certify a device by employing more test states and more measurements.

4.1.1 Fidelity-based benchmarking

At this point, one could take a similar approach as that used in Ch. 3. Namely, the average fidelity between input states and output states

$$\overline{F} = \sum_\alpha p_\alpha F(\rho_\alpha^{\text{in}}, \rho_\alpha^{\text{out}}) \tag{4.1}$$

can be used as a figure of merit. If the test states are not perfectly distinguishable, a MP channel will not be able to achieve perfect fidelity. Benchmarks can thus be based on the maximal fidelity $\overline{F}_{MP}^{\max}$ achievable by MP channels on the given set of test states, i.e., a device is in the quantum domain when

$$\overline{F}^{\text{observed}} > \overline{F}_{MP}^{\max}. \tag{4.2}$$

[1]Note the distinction between a *quantum channel*, i.e., a channel which has quantum states as input and output, and a *quantum device*, a quantum channel whose performance cannot be simulated by any MP channel.

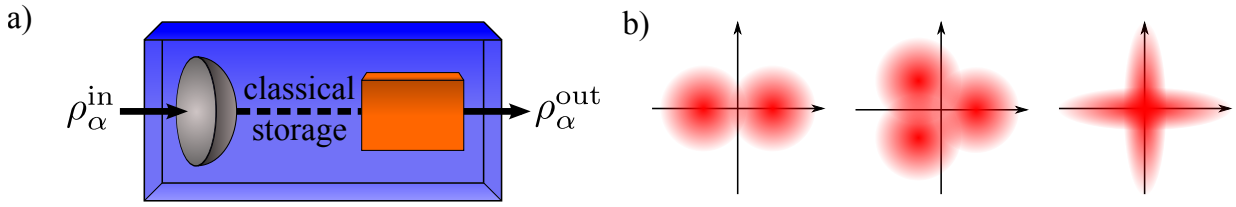


Figure 4.1: a) Device implementing a measure and prepare strategy: A measurement is made on the input state, the result is stored or transmitted classically, and a new quantum state is prepared based on this measurement result.
b) Example ensembles of CV test states: Entanglement-based benchmarks have been designed for ensembles consisting of two or more coherent states on a ring, squeezed and antisqueezed vacuum, as well as for generalizations to two mixed states.
Figure appears in [55], copyright 2011 the American Physical Society. Reprinted with permission.

This approach has a few experimental and theoretical requirements. First, we must theoretically determine (or bound) the optimal value $\overline{F}_{MP}^{\max}$ for the given test ensemble. Additionally, we must calculate (or bound) the experimentally observed fidelity $\overline{F}^{\text{observed}}$, which will typically require tomography on the output states. Finally, we should also perform tomography on the prepared test states in order to ensure a match with the theoretical ensemble. A number of fidelity-based benchmarks have been derived for various choices of continuous-variable test states. In Refs. [12, 33, 74], benchmarks are proposed and proved for a Gaussian distribution of all coherent states, centred at the origin of phase space. Ref. [29] also considers an ensemble of coherent states, but it uses a more restrictive model for classical channels than the one we are interested in here. Benchmarks for undisplaced (pure or mixed) squeezed states were studied in [1], and for displaced (pure or mixed) squeezed states in [77]. Results for test ensembles that are rotationally symmetric in phase space can be found in [16]. Most CV quantum benchmarks are derived for test ensembles with an infinite number of states, but this is not a necessary condition. In [73], fidelity-based benchmarks are calculated for test ensembles consisting of only two nonorthogonal pure states. We can also use this benchmarking scheme with figures of merit other than the fidelity, such as distance measures or inner products between states [77, 30].

The main drawback for fidelity-based benchmarks is that it is often very difficult to find the optimal classical value. Indeed, for the qubit RSP benchmarks detailed in Ch. 3, a computer algorithm was employed to search for bounds on the optimal value. For continuous-variable states, the state space is infinite dimensional, greatly increasing the complexity of this search. Some simplifications may be made if the test states are pure

and/or Gaussian; indeed, nearly all of the benchmarks mentioned above require such test states. However, the difficulty of finding $\overline{F}_{MP}^{\max}$ makes it challenging to use this approach in a general setting with arbitrary test states. Even when the fidelity threshold is known, (experimentally costly) tomographic reconstruction of the output states is typically required in order to compute the observed fidelity. When tomographic reconstruction is not an option, then unverified assumptions may have to be made, which goes against the aims of benchmarking. Finally, ensembles with an infinite number of test states present a separate concern. Since we can only test with a finite-sized ensemble, we must make extra efforts to ensure that fidelity benchmarks based on infinite ensembles are valid in practice.

4.1.2 Entanglement-based benchmarking

An alternative approach to quantum benchmarking, which avoids many of the above problems, is to show that a device preserves entanglement (see Fig. 4.2). The motivation behind this is that MP channels are equivalent [42] to *entanglement-breaking channels* (see Def. 2.2.5). Thus, devices that preserve entanglement cannot be simulated by classical MP channels. Indeed, the effective distribution of entanglement is a necessary precondition for secure quantum key distribution [23]. Importantly, we can certify that a device preserves entanglement without having to actually prepare physical entangled states. Instead, we can consider a virtual entangled state which is intimately connected with the test states $\{\rho_\alpha\}$. This *effective entanglement*[2] approach, which we will now outline, allows us to use the same device testing scenarios as the fidelity-based benchmarks above. The theoretical description of the benchmarking protocol, however, is much different.

For now, we assume that the test states are pure. The extension of entanglement-based benchmarks to arbitrary states, first studied in [35], will be discussed in Ch. 7. We modify notation so that $\mathcal{H}_{\mathrm{in}}$ becomes $\mathcal{H}_{\mathrm{A}'}$. As well, we assume that the ensemble contains a finite number M of test states, which we will now label with Latin indices:

$$\{\rho_k^{\mathrm{in}} \in \mathcal{B}(\mathcal{H}_{A'}) | \rho_k^{\mathrm{in}} = |\psi_k\rangle\langle\psi_k|\}_{k=0}^{M-1}. \tag{4.3}$$

For entanglement-based benchmarking, we imagine that the test states are coupled with an ancillary system to form the following bipartite entangled state [9, 23, 85]:

$$\left|\Psi^{\mathrm{ent}}\right\rangle_{AA'} = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle_A \otimes |\psi_k\rangle_{A'}. \tag{4.4}$$

[2]We warn that 'effective entanglement' should not be confused with the usage in [87], where the term refers to the minimal entanglement compatible with some given measurement results. This second concept is also important in this thesis, but we will typically refer to it as the 'minimal entanglement.'

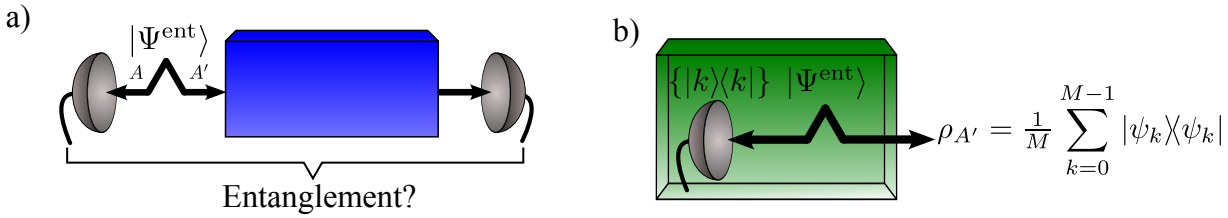


Figure 4.2: a) Entanglement-based benchmarking: Is there any entanglement remaining after part of the state $|\Psi^{\text{ent}}\rangle_{AA'}$ passes through the device? How much remains?
b) 'Effective entanglement': Any source which produces a classical mixture of the test states $|\psi_k\rangle$ can be pictured as internally preparing the entangled state in Eq. (4.4) and performing a projective measurement on subsystem A. This theoretical picture is also called a 'source replacement' scheme.
Figure appears in [55], copyright 2011 by the American Physical Society. Reprinted with permission.

Here, the ancillary system is defined on a M-dimensional state space $\mathcal{H}_A$ for which the vectors $\{|k\rangle_A\}_{k=0}^{M-1}$ form an orthonormal basis. Both the A and A' subsystems belong to Alice, who prepares the entangled state. For later chapters, it will be convenient to write this state in a block form. Using the basis $\{|0\rangle, \ldots, |M-1\rangle\}$ for system A, we have

$$\rho^{\text{in}}_{AA'} := \left|\Psi^{\text{ent}}\right\rangle\!\left\langle\Psi^{\text{ent}}\right|_{AA'} = \frac{1}{M}\begin{bmatrix} \rho^{\text{in}}_{00} & \rho^{\text{in}}_{01} & \cdots & \rho^{\text{in}}_{0,M-1} \\ \rho^{\text{in}}_{10} & \rho^{\text{in}}_{11} & \cdots & \rho^{\text{in}}_{1,M-1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho^{\text{in}}_{M-1,0} & \rho^{\text{in}}_{M-1,1} & \cdots & \rho^{\text{in}}_{M-1,M-1} \end{bmatrix}, \tag{4.5}$$

where the diagonal blocks are equal to the test states, $\rho^{\text{in}}_{kk} = \rho^{\text{in}}_k$ and the off-diagonal blocks are given by $\rho^{\text{in}}_{kl} = |\psi_k\rangle\langle\psi_l| \in \mathcal{B}(\mathcal{H}_{A'})$. Since $\rho^{\text{in}}_{AA'}$ is Hermitian, we also have $\rho^{\text{in}}_{kl} = (\rho^{\text{in}}_{lk})^\dagger$.

The device being investigated (represented by a map Λ) is allowed to act on the A' subsystem, giving outputs on some state space $\mathcal{H}_B$, while subsystem A is kept isolated. The reduced density matrix ρ_A therefore remains the same, independent of the device. Its entries are given by the relation

$$\langle k|\,\rho_A\,|l\rangle = \frac{1}{M}\text{Tr}\left(\rho^{\text{in}}_{kl}\right) = \frac{1}{M}\langle\psi_l|\psi_k\rangle\,. \tag{4.6}$$

Ignoring the prefactor and a possible transposition, the reduced density matrix ρ_A is the Gram matrix, or matrix of overlaps, for the test states. This Gram matrix connection will be especially important in Ch. 7.

By performing the local PVM $\{\hat{\Pi}_A^k := |k\rangle\langle k|_A\}_{k=0}^{M-1}$ on the entangled state, Alice can effectively prepare the test states $\{|\psi_k\rangle_{A'}\}_{k=0}^{M-1}$ at random. These states pass through the device, producing the corresponding output states

$$\left\{\rho_k^{\text{out}} \in \mathcal{B}(\mathcal{H}_B) | \rho_k^{\text{out}} = \Lambda\left[|\psi_k\rangle\langle\psi_k|\right]\right\}_{k=0}^{M-1}. \tag{4.7}$$

For the full bipartite system, the output state is given by

$$\rho_{AB}^{\text{out}} := (\text{id}_A \otimes \Lambda)\left|\Psi^{\text{ent}}\right\rangle\!\left\langle\Psi^{\text{ent}}\right|_{AA'}. \tag{4.8}$$

Again, it will often be convenient to express this state in block form. To this end, we write

$$\rho_{AB}^{\text{out}} = \frac{1}{M}\begin{bmatrix} \rho_{00}^{\text{out}} & \rho_{01}^{\text{out}} & \cdots & \rho_{0,M-1}^{\text{out}} \\ \rho_{10}^{\text{out}} & \rho_{11}^{\text{out}} & \cdots & \rho_{1,M-1}^{\text{out}} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{M-1,0}^{\text{out}} & \rho_{M-1,1}^{\text{out}} & \cdots & \rho_{M-1,M-1}^{\text{out}} \end{bmatrix}, \tag{4.9}$$

where the diagonal blocks are equal to the output states, $\rho_{kk}^{\text{out}} = \rho_k^{\text{out}}$ (we will use the notations ρ_{kk}^{out} and ρ_k^{out} interchangeably) and the off-diagonal blocks $\rho_{kl}^{\text{out}} \in \mathcal{B}(\mathcal{H}_B)$ are matrices of free parameters satisfying the constraints

$$\frac{1}{M}\text{Tr}\left(\rho_{kl}^{\text{out}}\right) = \langle k|\,\rho_A\,|l\rangle = \frac{1}{M}\langle\psi_l|\psi_k\rangle. \tag{4.10}$$

In addition, $\rho_{kl}^{\text{out}} = (\rho_{lk}^{\text{out}})^\dagger$ must hold.

Up to this point, everything has been quite general. Now, we will specialize by fixing a particular choice of measurements for Bob to perform on the output states, namely homodyne measurements. Using a balanced homodyne scheme, Bob can build up over many runs the expectation values $\langle\hat{x}\rangle$, $\langle\hat{p}\rangle$, and the variances

$$\text{Var}(\hat{x}) = \left\langle\hat{x}^2\right\rangle - \langle\hat{x}\rangle^2, \tag{4.11}$$

$$\text{Var}(\hat{p}) = \left\langle\hat{p}^2\right\rangle - \langle\hat{p}\rangle^2, \tag{4.12}$$

of the quadrature operators for each output state. These measurement results, along with the Gram matrix ρ_A, are used to determine whether or not the bipartite output state ρ_{AB}^{out} remains entangled. In the past, this has been achieved through a witnessing procedure [85, 84, 37, 36], which we will review shortly. Another way to accomplish this would be to lower bound the value of some entanglement measure based on the available information. The entanglement measure approach will be developed further in the next few chapters. As

well, any experimental implementation will have some uncertainty associated with these expectation values, which should also be considered in the benchmarking. In Ch. 7, where we benchmark a physical system, error bars will also be included in the analysis.

We restrict the available measurements on system A to the projections $\{\hat{\Pi}_A^k\}_{k=0}^{M-1}$. This might seem to limit our ability to detect entanglement. However, this restriction allows us to consider the entangled state $|\Psi^{\text{ent}}\rangle_{AA'}$ as a virtual construct. In practice, we only need to prepare and make measurements using the test states. The reduced density matrix ρ_A, serving as the Gram matrix for the test states, provides the connection between the test ensemble and the entangled state. With this *source-replacement* picture, we can determine whether entanglement can be preserved without needing to physically prepare the actual entangled state. One might imagine performing more general measurements on system A, which would prepare superpositions of the test states. However, we can straightforwardly include these superposition states within the set of test states and recast this new ensemble back to the entanglement-based form.

To ensure agreement with the theoretical test ensemble, we must have an accurate numerical description of the experimentally prepared test states. Typically, this will require tomographic reconstruction of the prepared states. In contrast, we do not require tomography on the output states to perform entanglement-based benchmarking. Indeed, the above scheme, where only two conjugate quadratures are measured, has proven sufficient for successful quantum benchmarking [67, 106]. From an experimental resource point of view, entanglement-based benchmarking can be much more practical than fidelity-based approaches.

Expectation value matrix

The entangled state $|\Psi^{\text{ent}}\rangle_{AA'}$ has an unusual form, containing both discrete and continuous subsystems. On one hand, density matrices are useful for representing small-dimensional discrete states. On the other hand, continuous states can be more compactly (though not uniquely) represented by covariance matrices and displacement vectors containing the first and second moments of the quadratures $\hat{x}$ and $\hat{p}$. In order to represent hybrid discrete-continuous states such as $|\Psi^{\text{ent}}\rangle_{AA'}$, a tool is needed that combines the strengths of both the density matrix and the covariance matrix. One such tool is the *expectation value matrix* (EVM) [85, 37, 34]. We will now briefly summarize the EVM method because it forms the qualitative comparison for later results on quantitative benchmarking. The EVM is defined as follows[3]:

[3]The definition of the EVM differs slightly between its original introduction [85] and its more general characterization [37], but the two definitions are equivalent (see e.g., App. B of [34]). We follow [37] here.

Definition 4.1.1 (Expectation value matrix)**.** *Let Alice and Bob share a joint state ρ_{AB}. Fix a set of measurement operators on each system, $\{\hat{A}_i\}$ and $\{\hat{B}_j\}$. The expectation value matrix $\chi(\rho_{AB})$ is a bipartite matrix with entries given by*

$$\chi_{ij,kl} = \langle i|_A \otimes \langle j|_B \chi |k\rangle_A \otimes |l\rangle_B := \mathrm{Tr}(\rho_{AB} \hat{A}_i^\dagger \hat{A}_k \otimes \hat{B}_j^\dagger \hat{B}_l). \tag{4.13}$$

By construction, the EVM has the following important property: *for all physical states and all choices of measurement operators, the expectation value matrix is a positive semi-definite matrix*, i.e.,

$$\forall\ \{\hat{A}_i\}, \{\hat{B}_j\},\ \rho_{AB} \geq 0 \Rightarrow \chi(\rho_{AB}) \geq 0. \tag{4.14}$$

As well, the EVM has the property that separable states $\rho_{AB}^{\mathrm{sep}} = \sum_\alpha p_\alpha \rho_A^\alpha \otimes \rho_B^\alpha$ always lead to separable EVMs, i.e.,

$$\chi(\rho_{AB}^{\mathrm{sep}}) = \sum_\alpha p_\alpha \chi_A^\alpha \otimes \chi_B^\alpha \tag{4.15}$$

where we define the local EVMs by

$$[\chi_A^\alpha]_{ij} = \mathrm{Tr}(\rho_A^\alpha \hat{A}_i^\dagger \hat{A}_j), \tag{4.16}$$

$$[\chi_B^\alpha]_{ij} = \mathrm{Tr}(\rho_B^\alpha \hat{B}_i^\dagger \hat{B}_j). \tag{4.17}$$

Thus, the entanglement of the state ρ_{AB} can be determined by testing a corresponding EVM for separability. In particular, we can use the PPT test (see Def. 2.4.5) on the level of the EVM, giving the following criterion:

$$\chi^{T_A}(\rho_{AB}) \ngeq 0 \Rightarrow \rho_{AB} \text{ is entangled.} \tag{4.18}$$

The advantage of the EVM formalism is that, by choosing small sets of measurement operators $\{\hat{A}_i\}, \{\hat{B}_j\}$, we can test for separability of infinite-dimensional states using a small finite-dimensional matrix. Indeed, for the case we are interested in, the relevant measurement operators are

$$\hat{A}_i = |?\rangle\langle i|\,,\ i = 0, \ldots, M-1 \tag{4.19}$$

where $|?\rangle$ is any fixed state vector, and

$$\hat{B}_j \in \{\hat{\mathbb{1}}, \hat{x}, \hat{p}\}. \tag{4.20}$$

As an example, consider a hybrid state ρ_{AB} which has a 2-dimensional subsystem A and an infinite-dimensional subsystem B. The above choice of measurement operators leads to the 6×6 EVM

$$\chi(\rho_{AB}) = \begin{bmatrix} \langle |0\rangle\langle 0| \otimes B\rangle_{\rho_{AB}} & \langle |0\rangle\langle 1| \otimes B\rangle_{\rho_{AB}} \\ \langle |1\rangle\langle 0| \otimes B\rangle_{\rho_{AB}} & \langle |1\rangle\langle 1| \otimes B\rangle_{\rho_{AB}} \end{bmatrix}, \tag{4.21}$$

where

$$B := \begin{bmatrix} \hat{\mathbb{1}}_B & \hat{x} & \hat{p} \\ \hat{x} & \hat{x}^2 & \hat{x}\hat{p} \\ \hat{p} & \hat{p}\hat{x} & \hat{p}^2 \end{bmatrix}. \tag{4.22}$$

Of course, the operators $\hat{x}\hat{p}$ and $\hat{p}\hat{x}$ are not strictly measurable (though their expectation values can be inferred from linear combinations of other measurements). Neither can we measure any of the off-diagonal terms $|0\rangle\langle 1| \otimes B$. However, some of these expectation values can be written in terms of known quantities. For instance, in the benchmarking scheme described above we have full knowledge of ρ_A, since it is the Gram matrix of the test states. Thus, we know the value

$$\langle |0\rangle\langle 1| \otimes \hat{\mathbb{1}}_B \rangle = \langle 1| \rho_A |0\rangle = \frac{1}{M} \langle \psi_0 | \psi_1 \rangle . \tag{4.23}$$

Other expectation values that are not experimentally measured must enter the EVM as free parameters. An EVM thus represents an equivalence class of all states which have the same values for the actual measured observables.

Having an incomplete EVM does not prevent the detection of entanglement, but may weaken it. Letting $\chi^{\vec{x}}(\rho_{AB})$ represent an EVM with free parameters $\vec{x}$, the entanglement verification criterion becomes: *an incomplete EVM $\chi^{\vec{x}}(\rho_{AB})$ corresponds to an entangled state if, for all values of the free parameters $\vec{x}$, there is no solution satisfying*

$$\chi^{\vec{x}}(\rho_{AB}) \geq 0, \tag{4.24}$$

$$[\chi^{\vec{x}}(\rho_{AB})]^{T_A} \geq 0. \tag{4.25}$$

Finally, we may encode information about the structure of the measurement operators as additional constraints in the above search. Notably, because of the commutation relation $[\hat{x}, \hat{p}] = i\hat{\mathbb{1}}$, the matrix B in Eq. (4.22) has the following structure: $B_{12} - B_{21} = iB_{00}$. Often, we must rely on numerical optimization techniques to solve the above feasibility problem. In particular, the tools of semidefinite programming are quite useful [99].

Known entanglement-based benchmarking results

The EVM formalism has been applied to a number of benchmarking scenarios, corresponding to different choices of the test states. Originally, the EVM was developed to benchmark quantum key distribution protocols based on two coherent states of opposite phase, $|\psi_{0/1}\rangle = |\pm\alpha\rangle$ [85, 67]. This approach was generalized to benchmark arbitrary

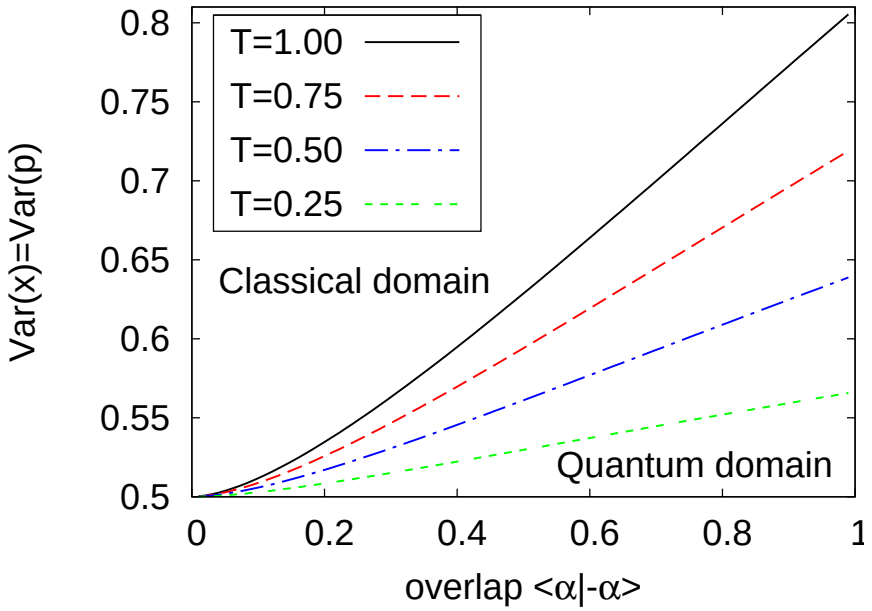


Figure 4.3: Quantum domain for test ensemble containing two coherent states $|\pm\alpha\rangle$ with different channel transmissivities T (cf. Fig. 1 in [37]). Data below the curves must come from entangled states.

quantum devices in [37]. The quantum domain for this choice of test states, found with the EVM method, can be mapped out by considering the loss and excess noise induced on the quadratures by the device. Specifically, the loss is parameterized by $1 - T$, where T is the transmissivity defined by

$$\sqrt{T} := \frac{\langle \hat{x} \rangle_{\text{out}}}{\langle \hat{x} \rangle_{\text{in}}}, \tag{4.26}$$

and the excess noise is given by

$$\text{Var}(\hat{x}_{\text{out}}) = \text{Var}(\hat{x}_{\text{in}}) + V_{\text{ex}}(\hat{x}). \tag{4.27}$$

Here, it is assumed that the loss/noise is the same for both test states and both quadratures. This assumption is not required, but aids the graphical display of the quantum domain, which is depicted in Fig. 4.3.

In Ref. [36], this scheme is extended to M coherent states having the same amplitude $\alpha \in \mathbb{R}$ and symmetrically-distributed phase angles, $|\psi_k\rangle = \left|\alpha\omega_M^k\right\rangle$, where $\omega_M = \exp(\frac{2\pi i}{M})$. Using the same loss/noise parameterization as before, the EVM method provides the quantum domain shown in Fig. 4.4.

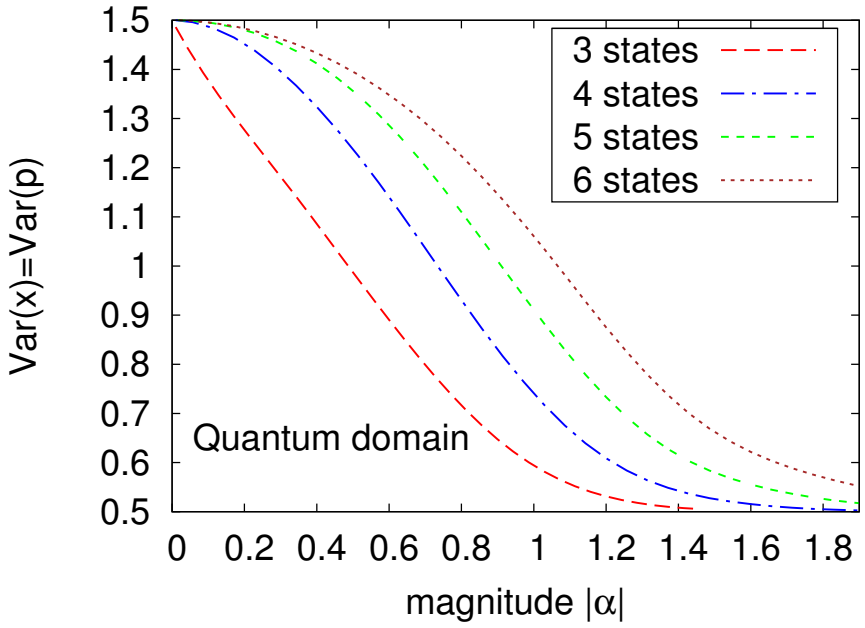


Figure 4.4: Quantum domain for test ensemble containing $M = 3, 4, 5, 6$ symmetrically distributed coherent states $\left|\alpha\omega_M^k\right\rangle$, with channel transmissivity $T = 1.0$ (cf. Fig. 3 in [36]). Data below the curves is from entangled states.

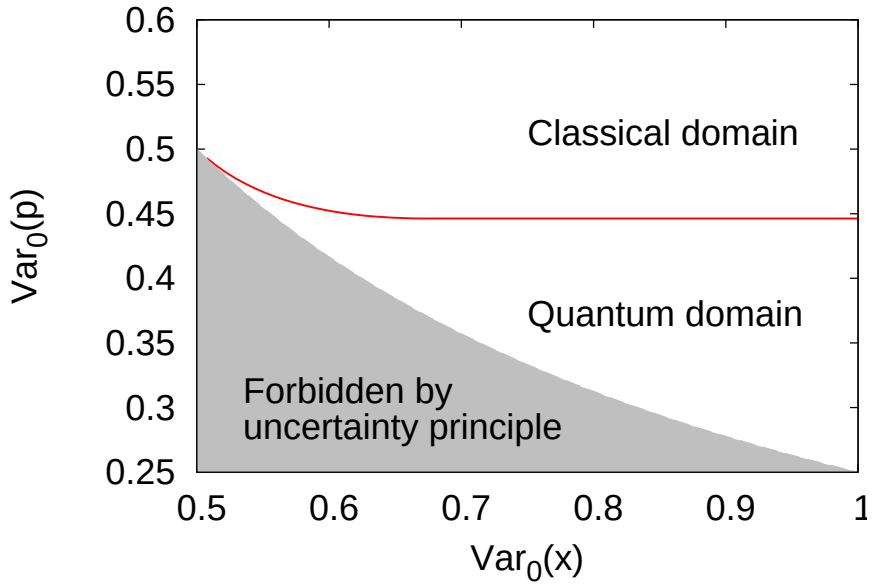


Figure 4.5: Quantum domain for a squeezed/antisqueezed pair $|\pm r\rangle$, where $r = 0.35$ and the channel transmissivity is $T = 1.0$ (cf. Fig 1 in [35]). Data between the forbidden region and the upper curve must come from entangled states.

The final situation of interest, initially considered in [35], is when the test ensemble consists of a squeezed/antisqueezed pair of states, $\left|\psi_{0/1}\right\rangle = |\pm r\rangle$. In this case, $\langle\hat{x}\rangle = \langle\hat{p}\rangle = 0$ for both input states, so the first moments are not included in the benchmark. The output state variances may take any values consistent with the uncertainty relation. To simplify the graphical depiction of the quantum domain, it is assumed that the initial symmetry relations $\mathrm{Var}_0(\hat{x}) = \mathrm{Var}_1(\hat{p})$ and $\mathrm{Var}_0(\hat{p}) = \mathrm{Var}_1(\hat{x})$ also hold for the output states. The quantum domain for this situation is displayed in Fig. 4.5.

The quantum domains depicted in Figs. 4.3-4.5 will serve as the qualitative comparison for the quantitative benchmarks to be developed in the rest of this chapter and in Chs. 5 and 6. Ideally, the quantitative benchmarking results should be faithful with these known qualitative results, giving the same quantum domains. We note that for Figs. 4.3 and 4.5, it is been shown that any quadrature data outside the depicted quantum domains can be produced by separable states [37, 35]. Therefore, for these two cases, having data in the depicted quantum domains is necessary and sufficient for certifying a device with the available information.

4.2 Quantitative benchmarking

The previous section was a review of the known entanglement-based benchmarking tools and results. The rest of this thesis is devoted to the development of newer, stronger, and more general tools which build on the existing framework. The remainder of this chapter, as well as Chs. 5-6, will study the idea of *quantitative benchmarking*.

The expectation value matrix can be thought of as a matrix-valued entanglement witness. The purpose of entanglement witnesses is simply to verify entanglement with minimal measurements, and the EVM accomplishes this. For quantum benchmarking, this allows us to discriminate between genuine quantum devices and devices that can be emulated by MP channels, i.e., to make the general distinction: *quantum or classical?* But there is a richer structure within the quantum domain. Several devices may be in the quantum domain, yet they may perform quite differently. Some devices may consume more quantum resources than others to accomplish the same task.

To capture this difference in performance, we propose a natural extension of entanglement-based benchmarking. Instead of verifying entanglement, we should study *how well* a given device preserves entanglement, a notion that we term the *quantum throughput*. Since all operations are local, entanglement cannot be created during a benchmarking test, only destroyed. By comparing the entanglement content of the initial state $|\Psi^{\text{ent}}\rangle_{AA'}$ with that of the final bipartite state ρ_{AB}^{out}, we can see how well or how poorly a particular device preserves entanglement.

Of course, any conclusions we make are only relevant for the subspace spanned by the chosen test states. Indeed, a device might have a much different quantum throughput for states in some complementary subspace. Because of this, it may be instructive to test a device using many different test state ensembles. On the other hand, we should keep in mind the desired application of a device, and use this to guide the choice of test states. Our primary interest will be the quantum throughput for states near experimentally desired working points. The examples studied in this thesis are chosen to reflect typical or ideal experimental states.

4.2.1 Benchmarking with entanglement measures

In order to study the quantum throughput of devices, it is necessary to develop quantitative tools for entanglement-based benchmarking. Fortunately, there are well-established methods for quantifying entanglement, namely entanglement measures (recall Def. 2.4.6).

However, there is no universally-preferred entanglement measure for general states; different measures capture different notions of entanglement. Showing that a device preserves entanglement with respect to one measure does not necessarily allow us to make conclusions about other measures. For the particular quantitative approach developed below, we will make certain choices that will restrict the type of allowed measures. These choices are made to allow the best connection to CV quantum benchmarking.

Ideally, the quantitative measure should fit as much as possible within the established framework for entanglement-based benchmarking. The available information remains the same: knowledge of the test states ρ_k^{in} through the Gram matrix ρ_A (Eq. 4.6) and homodyne measurements for each of the corresponding output states ρ_k^{out} (Eq. 4.7). Unfortunately, this information is not tomographically complete, so we cannot determine the entanglement exactly. However, we can search for the *minimal* entanglement, with respect to some measure $\mathcal{E}$, compatible with the available information [4]. The result of this search will give a lower bound on the true entanglement. Mathematically, this search takes the general form of an optimization problem:

$$\mathcal{E}_{\min}(\rho_{AB}^{\text{out}}) := \begin{cases} \min\limits_{\sigma_{AB}\geq 0} & \mathcal{E}(\sigma_{AB}) \\ \text{subject to} & \text{Tr}(\sigma_{AB}\,|k\rangle\langle k|_A \otimes \hat{C}_B^j) = \text{Tr}(\rho_k^{\text{out}}\hat{C}_B^j)\ \forall\ k,j\ \cdot \\ & \text{Tr}_B(\sigma_{AB}) = \rho_A \end{cases} \tag{4.28}$$

The operators $\{\hat{C}_B^j\}_{j=0}^J$ may represent observables measured in experiment (e.g., the quadratures) or something more abstract (e.g., projections onto pure states) that can be inferred from experimental data.

Projecting to finite dimensions

The main hurdle with the above optimization is that the search space is infinite-dimensional, making a numerical search problematic. To get around this issue, we make the observation that although CV states are properly defined on an infinite-dimensional Hilbert space, it is often possible to achieve a faithful description of such states on a finite-dimensional subspace. By finding suitable finite subspaces to project onto, we can render the optimization in Eq. (4.28) tractable. Provided we are careful, this simplification does not adversely affect our overall goal. Indeed, for any entangled state, entanglement can always be found by searching within some finite subspace [91]. As well, provided the entanglement measure $\mathcal{E}$ satisfies the strong monotonicity property (Def. 2.4.7), the entanglement of the projection can be used to lower bound the entanglement of the true state.

To see this property, let $\hat{\Pi}_B \in \mathcal{B}(\mathcal{H}_B)$ be a projector onto some (finite) subspace of $\mathcal{H}_B$ and let $\hat{Q}_B := \hat{\mathbb{1}}_B - \hat{\Pi}_B$. We denote the (unnormalized) projection of the benchmarking output state ρ_{AB}^{out} by

$$\rho_{AB}^{\Pi} := (\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)\rho_{AB}^{\text{out}}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B) \tag{4.29}$$

and the projection probability by $p := \text{Tr}(\rho_{AB}^{\Pi})$. By strong monotonicity, we have

$$\begin{aligned}\mathcal{E}(\rho_{AB}^{\text{out}}) \geq\ & p\mathcal{E}\left(\frac{(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)\rho_{AB}^{\text{out}}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)}{p}\right) \\ & + (1-p)\mathcal{E}\left(\frac{(\hat{\mathbb{1}}_A \otimes \hat{Q}_B)\rho_{AB}^{\text{out}}(\hat{\mathbb{1}}_A \otimes \hat{Q}_B)}{1-p}\right).\end{aligned} \tag{4.30}$$

The second term, which quantifies the (weighted) entanglement in the complementary subspace, is non-negative, so it can be discarded at the expense of another inequality, leaving

$$\mathcal{E}(\rho_{AB}^{\text{out}}) \geq\ p\mathcal{E}\left(\frac{\rho_{AB}^{\Pi}}{p}\right). \tag{4.31}$$

It will later be convenient to work directly with unnormalized states ($0 < \text{Tr}\rho_{AB}^{\Pi} \leq 1$), so we further restrict to entanglement measures that are well-defined on unnormalized states and that allow the prefactor to be absorbed, i.e., if $p \in (0, 1]$ and $\tau \geq 0$, then

$$p\mathcal{E}(\tau) \geq \mathcal{E}(p\tau). \tag{4.32}$$

For any entanglement measure $\mathcal{E}$ satisfying these demands, we have the bound

$$\mathcal{E}(\rho_{AB}^{\text{out}}) \geq \mathcal{E}(\rho_{AB}^{\Pi}). \tag{4.33}$$

For the remainder of this thesis, we will use the negativity (Eq. (2.8)) as our entanglement measure of choice. It satisfies all of the desired properties, and it also has the virtue that it is efficiently computable as a semidefinite program (Eq. (2.9)).

One drawback of the negativity is that it is not faithful, since it is not able to detect PPT entangled states. However, for benchmarking schemes based on quadrature measurements of two test states, it is not possible to detect PPT entanglement anyway. From Observation 2 in [37], for any PPT entangled state, there is always a separable state that gives the same measurement results. Hence, the unfaithfulness of the negativity is not an issue in this case. Benchmarks based on more than two test states are less well understood. In this situation, it is not known whether or not PPT entanglement can be unambiguously identified; if so,

it might be possible to quantify PPT entanglement with a different measure than the one used here.

Finally, depending on the choice of projection, we may need to relax the constraints in Eq. (4.28). Even if we know an expectation value for the state ρ_{AB}^{out}, we do not necessarily know the corresponding expectation value for the projection ρ_{AB}^{Π}. In principle, the expectation values of ρ_{AB}^{out} may contain contributions from the projected subspace as well as from the complementary subspace. But if we understand the underlying system well enough, it should be possible to find projections for which the contribution from the complement is small. In addition, we should be able to constrain the projection's expectation values using our knowledge of the observed expectation values. Ideally, we should aim to restrict each projection expectation value to some small convex set $\mathcal{C}$ that is dependent on the observed results. If we can find such constraints, the optimization (4.28) may be modified to a more tractable finite-dimensional form.

Finite-dimensional entanglement minimization. *Let ρ_{AB}^{out} be the final state of an entanglement-based benchmarking test as in Eqs. (4.8-4.9). Let σ_{AB}^{Π} be an arbitrary (unnormalized) state on the finite subspace $(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)\mathcal{H}_{AB}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)$. Our entanglement-minimization problem takes the form*

$$\mathcal{E}_{\min}(\rho_{AB}^{\Pi}) := \begin{cases} \min\limits_{\sigma_{AB}^{\Pi} \geq 0} & \mathcal{E}(\sigma_{AB}^{\Pi}) \\ \text{subject to} & Tr(\sigma_{AB}^{\Pi} |k\rangle\langle k|_A \otimes \hat{C}_B^j) \in \mathcal{C}(\rho_k^{\text{out}}, \hat{C}_B^j) \ \forall \ k, j \ , \\ & Tr_B(\sigma_{AB}^{\Pi}) \in \mathcal{C}(\rho_A) \end{cases} \tag{4.34}$$

where $\mathcal{C}(\rho_k^{\text{out}}, \hat{C}_B^j)$ and $\mathcal{C}(\rho_A)$ are some convex sets representing constraints on the measurement operators $\hat{C}_B^j$ and the reduced density matrix ρ_A. The solution of this optimization problem provides a rigorous lower bound on the entanglement of ρ_{AB}^{out}:

$$\mathcal{E}(\rho_{AB}^{\text{out}}) \geq \mathcal{E}_{\min}(\rho_{AB}^{\Pi}). \tag{4.35}$$

This final formulation of the entanglement minimization problem will serve as the basis for our quantitative approach to quantum benchmarking. We note here that all optimizations of this form will be carried out using semidefinite programs (SDPs) [99]. This aproach requires two main ingredients: an objective function which is linear in the desired variables (e.g., Eq. (2.9)), and constraints which take the form of linear inequalities (e.g., $x \geq x_0$) or positive-semidefinite matrix inequalities (e.g., $X \geq X_0$). Often, some work will have to be done to put the constraints in this form. The payoff is that SDPs can be numerically calculated in an efficient manner.

Summary

To summarize, we propose to extend the existing framework of entanglement-based benchmarking by quantifying how well entanglement is preserved through a tested device. For this, we use the same information as previous qualitative benchmarks, namely knowledge of the test states and measurement of two conjugate quadratures. We tackle the problem of infinite-dimensional states by projecting the states onto some tractable finite subspace. We search within this subspace for the least entangled state that is consistent with both the observed expectation values and the given projection operation. Choosing an entanglement measure with certain monotonicity properties and finding suitable convex constraint regions $\mathcal{C}$, we can numerically perform the optimization in Eq. (4.34). The solution to this optimization problem gives a lower bound to the entanglement of the benchmarking output state ρ_{AB}^{out}.

Of course, we have omitted many of the finer details of this approach. There are a number of open questions remaining. What projection should be used? How can we find the constraints for the projected state? How do we encode the optimization numerically? How well does this approach compare to the qualitative approach? All of these questions will be addressed in the following two chapters. In each chapter, we make a specific choice for the finite projection and follow through with the rest of the optimization. These two choices are somewhat complementary, each having its own strengths and drawbacks. The first choice, outlined in Ch. 5, is to project onto the smallest possible system that can have entanglement, namely a two-qubit system. This approach is applicable only to benchmarks using the two test states $|\pm\alpha\rangle$, but it works quite well when there is a very low level of imperfection in the device, i.e., when the output states are nearly pure. The second choice, found in Ch. 6, involves projecting onto a number of low-dimensional Fock states. This choice of projection lends itself well to situations with higher levels of imperfection, and it is easily adapted to different types of test states.

Chapter 5

Quantitative benchmarking I: two-qubit projection

In this chapter, we outline one method for achieving quantitative CV benchmarks using the framework of Ch. 4, namely by projecting onto a two-qubit subsystem. The material in this chapter, as well as the accompanying App. B, is based largely on [54], for which I am the primary author and researcher. The published article is copyright 2010 by the American Physical Society (APS). Portions of the article have been adapted for this thesis, under permission from APS.

This chapter proceeds as follows. After fixing a particular choice of test states, we identify a two-qubit subspace that is the most significant for our purposes. Following the approach of Ch. 4, we consider the projection ρ_{AB}^{Π} of the benchmarking output state ρ_{AB}^{out} down to this finite subspace. We then outline how to estimate the relevant constraints and perform the entanglement optimization in Eq. (4.34), i.e., how to calculate the minimal entanglement of the projected state compatible with the available information. Finally, the results of this optimization, which give lower bounds on the actual entanglement, are presented and discussed.

5.1 Quantification procedure

In this chapter, we will concentrate on the test ensemble consisting of two coherent states with the same amplitude but opposite phase: $|\psi_0\rangle = |\alpha\rangle$, $|\psi_1\rangle = |-\alpha\rangle$, where $\alpha \in \mathbb{R}$. These states are nonorthogonal for all $\alpha \in \mathbb{C}$. As well, they are readily generated under ideal experimental conditions and can be used as the signal states in a simple CV quantum key distribution protocol [85, 84, 67]. The initial virtual entangled state therefore takes the form (cf. Eq. (4.4))

$$\left|\Psi^{\text{ent}}\right\rangle_{AA'} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |\alpha\rangle_{A'} + |1\rangle_A \otimes |-\alpha\rangle_{A'} \Big), \tag{5.1}$$

where system A is a qubit and system A' is an optical mode. This is an entangled state for all values $\alpha \neq 0$, since it is pure but not factorized. The device being tested (represented by Λ) acts on the mode A'; we label the resulting output mode by the index B. The bipartite output state $\rho_{AB}^{\text{out}} = (\text{id}_A \otimes \Lambda)\,|\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'}$ is, in general, infinite-dimensional, but we can simplify it using the finite projection method from the previous chapter. Fortunately, the specific form of the test states allows us to choose a projection that can capture a lot of information in a very small subspace.

5.1.1 Choosing the projection

Our choice of projection is motivated by the following observation. When the pure test states $\{|\alpha\rangle, |-\alpha\rangle\}$ pass through the device, they are subject to loss and noise, and evolve in general to mixed states $\{\rho_0^{\text{out}}, \rho_1^{\text{out}}\}$; however, because these are coherent states, the change in purity comes only from the noise. Indeed, a noiseless but lossy channel (with transmissivity T) will map these coherent states to a new pair of coherent states $\left|\pm\sqrt{T}\alpha\right\rangle$. Along the same lines, if a channel is noisy, but the added noise is small, then the output states ρ_0^{out} and ρ_1^{out} will still be nearly pure. In this case, most of the information about the state ρ_{AB}^{out} is still contained in a very small subspace of the full infinite-dimensional Hilbert space. Additionally, for low levels of noise, the output states will be close to minimum uncertainty states, i.e., they will be close to the minimum value in the uncertainty relation of Eq. (2.37). For such states, we expect that quadrature measurements capture nearly all of the important information.

Therefore, we would like to identify a small mode subspace that contains as much information as possible about both output states. For simplicity, we will concentrate on the simplest non-trivial subspace, namely one of dimension 2. Writing the output states ρ_0^{out} and ρ_1^{out} in terms of their eigenvectors, in order of descending eigenvalues, we have

$$\rho_k^{\text{out}} = \sum_{j=0}^{\infty} \lambda_k^j \left|\lambda_k^j\right\rangle\!\left\langle\lambda_k^j\right|. \tag{5.2}$$

When an output state is nearly pure, one eigenvalue will be large and all others will be small. Hence, we identify the most significant subspace as the one formed using the largest eigenvalue for each state, i.e., the subspace which has $|\lambda_0^0\rangle$ and $|\lambda_1^0\rangle$ as basis vectors. To simplify notation, we will henceforth denote the largest eigenvalues by $\lambda_0^{\text{L}} := \lambda_0^0$ and $\lambda_1^{\text{L}} := \lambda_1^0$. The corresponding eigenvectors will similarly be denoted $\left|\lambda_0^{\text{L}}\right\rangle := |\lambda_0^0\rangle$ and $\left|\lambda_1^{\text{L}}\right\rangle := |\lambda_1^0\rangle$.

In general, these two basis vectors will not be orthogonal. The subspace projection operator $\hat{\Pi}_B$ will thus take the form

$$\Pi_B := \left|\lambda_0^{\text{L}}\right\rangle\!\left\langle\lambda_0^{\text{L}}\right| + \left|\lambda_0^{\text{L}\perp}\right\rangle\!\left\langle\lambda_0^{\text{L}\perp}\right| \tag{5.3}$$

where the orthogonal vector $\left|\lambda_0^{\text{L}\perp}\right\rangle$ is related to the other two by

$$\left|\lambda_0^{\text{L}\perp}\right\rangle := \frac{1}{\sqrt{s}}\Big(\left|\lambda_1^{\text{L}}\right\rangle - t\left|\lambda_0^{\text{L}}\right\rangle\Big), \tag{5.4}$$

and we have introduced the shorthand notations $t := \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$ an $s := 1 - |t|^2$. Therefore, three parameters will be important to identify this subspace: the eigenvalues λ_0^{L} and λ_1^{L}, as well as the overlap t. We will estimate these parameters using homodyne detection. Exactly how this is done will be shown in the next part. With these parameters, we can build a 4-dimensional density matrix ρ_{AB}^{Π}, which corresponds to the projection of the full qubit-mode state ρ_{AB}^{out} onto the two-qubit subspace spanned by the basis $\{|0\rangle_A, |1\rangle_A\} \otimes \{|\lambda_0^{\mathrm{L}}\rangle_B, |\lambda_1^{\mathrm{L}}\rangle_B\}$.

5.1.2 Estimating the constraints

Having fixed the projection, our next important task is to develop the constraints for the optimization in Eq. (4.34). The available homodyne measurement information does not directly lead to such constraints. However, based on the above intuition, the homodyne results can be indirectly connected to constraints on the two-qubit subspace. Since we are interested in quantum benchmarking, we will not make any approximations. Instead, we will develop rigorous bounds which will form the required constraints.

First, we will provide bounds on the three parameters λ_0^{L}, λ_1^{L} and $\langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$ that characterize the projection subspace. We will then explicitly connect these bounds to the projected state ρ_{AB}^{Π}. The derivations for many of the bounds in this part are largely technical and unilluminating, so we will mostly relegate these to App. B to avoid obscuring the main focus. Now, in Ref. [84], which considers a related entanglement-verification problem, several useful formulas for estimating the maximal eigenvalues and the overlap are given. These bounds are later refined in [110], where they are used to derive secret key rates for continuous-variable quantum key distribution. Here, we use these bounds as a starting point toward constraining the projected state ρ_{AB}^{Π}. We will roughly follow the notation of [110] in the following.

Since the output states $\{\rho_0^{\mathrm{out}}, \rho_1^{\mathrm{out}}\}$ have unit trace, their maximal eigenvalues can be parameterized by

$$\lambda_k^{\mathrm{L}} =: 1 - \tilde{\varepsilon}_k \ (k = 0, 1), \tag{5.5}$$

with $\tilde{\varepsilon}_k \in [0, 1]$. Then Eqs. (65) and (68) from [110] give directly the following bound.

Proposition 5.1.1 (Largest eigenvalue bounds)**.** *Define the quantity U_k as*

$$U_k := \frac{1}{2}\left[\left(\mathrm{Var}_k(\hat{x}) + \frac{1}{2}\right)\left(\mathrm{Var}_k(\hat{p}) + \frac{1}{2}\right) - 1\right]. \tag{5.6}$$

Then the maximal eigenvalue λ_k^{L} differs from unity by no more than U_k, i.e., $\tilde{\varepsilon}_k \leq U_k$.

Importantly, the bound can be calculated using only the measured variances of the output states.

Estimating the overlap $t = \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$ is more involved. We need to derive bounds on its magnitude based on our available information. Again, we begin with bounds provided in Refs. [84, 110]. With suitable relaxations, their bounds can be put into a specific form that will be more useful for our final entanglement minimization. The specific details of this relaxation are straightforward, and are outlined in App. B.1. To write these relaxed bounds, we will need an additional parameter, κ, which can be calculated directly using the measured first moments $\{\langle \hat{x} \rangle_k, \langle \hat{p} \rangle_k\}_{k=0,1}$. Defining two coherent states with the same means as the output states,

$$|\tilde{\alpha}_k\rangle = \left| \frac{1}{\sqrt{2}} \left(\langle \hat{x} \rangle_k + i \langle \hat{p} \rangle_k \right) \right\rangle, \tag{5.7}$$

the new parameter is given through the overlap of these coherent states,

$$\kappa := |\langle \tilde{\alpha}_0 | \tilde{\alpha}_1 \rangle|. \tag{5.8}$$

Using this quantity, the relaxed bounds are as follows (cf. Eqs. (C17)-(C18) of [110]).

Proposition 5.1.2 (Overlap bounds)**.** *The overlap $t = \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$ can be bounded to the following region:*

$$b_l(U_0, U_1, \kappa) \leq |t| \leq b_u(U_0, U_1, \kappa), \tag{5.9}$$

where

$$\begin{aligned} b_l(U_0, U_1, \kappa) = \; & \kappa \sqrt{1 - 2U_0} \sqrt{1 - 2U_1} - \sqrt{1 - \kappa^2} \sqrt{\frac{U_0}{1 - 2U_0}} \\ & - \sqrt{1 - \kappa^2} \sqrt{\frac{U_1}{1 - 2U_1}} - \sqrt{\frac{U_0}{1 - 2U_0}} \sqrt{\frac{U_1}{1 - 2U_1}} \end{aligned} \tag{5.10}$$

and

$$\begin{aligned} b_u(U_0, U_1, \kappa) = \; & \kappa + \sqrt{1 - \kappa^2} \sqrt{\frac{U_0}{1 - 2U_0}} + \sqrt{1 - \kappa^2} \sqrt{\frac{U_1}{1 - 2U_1}} \\ & + \sqrt{\frac{U_0}{1 - 2U_0}} \sqrt{\frac{U_1}{1 - 2U_1}}. \end{aligned} \tag{5.11}$$

Connecting the bounds to the projected state

With these primary bounds, computable using only homodyne measurements, we can move on to constraining the elements of the projected density matrix ρ_{AB}^{Π}. For more compact notation, we parameterize the matrix elements involving $\left|\lambda_0^{\mathrm{L}}\right\rangle$ and $\left|\lambda_0^{\mathrm{L}}\right\rangle$ the following way (recall the definition of ρ_{01}^{out} from Eq. (4.9)):

$$\chi_{AB}^{\Pi} = \left[\begin{array}{cc|cc} \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{00}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{00}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle \\ \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{00}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{00}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle \\ \hline \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{10}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{10}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{11}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_0^{\mathrm{L}}\right| \rho_{11}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle \\ \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{10}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{10}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{11}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle & \left\langle\lambda_1^{\mathrm{L}}\right| \rho_{11}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle \end{array}\right]$$
$$=: \left[\begin{array}{cc|cc} x_1 & y_1 & z_1 & z_2 \\ y_1^* & x_2 & z_3 & z_4 \\ \hline z_1^* & z_3^* & x_3 & y_2 \\ z_2^* & z_4^* & y_2^* & x_4 \end{array}\right]. \tag{5.12}$$

As the name χ_{AB}^{Π} suggests, this is an expectation value matrix based on the vectors $\{|0\rangle_A, |1\rangle_A\}$ and $\{\left|\lambda_0^{\mathrm{L}}\right\rangle_B, \left|\lambda_1^{\mathrm{L}}\right\rangle_B\}$. We remind the reader that we use the output state notations ρ_{kk}^{out} and ρ_k^{out} interchangeably.

Having set the parameters, we can explicitly write ρ_{AB}^{Π} in the basis $\{|0\rangle, |1\rangle\}\otimes\{\left|\lambda_0^{\mathrm{L}}\right\rangle, \left|\lambda_0^{\mathrm{L}\perp}\right\rangle\}$ (cf. Eq. (4.9)):

$$\rho_{AB}^{\Pi} = \frac{1}{2}\left[\begin{array}{cc|cc} x_1 & \frac{1}{\sqrt{s}}(y_1 - tx_1) & z_1 & \frac{1}{\sqrt{s}}(z_2 - tz_1) \\ \frac{1}{\sqrt{s}}(y_1^* - t^*x_1^*) & \frac{1}{s}(x_2 - ty_1^* - t^*y_1 + |t|^2x_1) & \frac{1}{\sqrt{s}}(z_3 - t^*z_1^*) & \frac{1}{s}(z_4 - tz_3 - t^*z_2 + |t|^2z_1) \\ \hline z_1^* & \frac{1}{\sqrt{s}}(z_3^* - tz_1) & x_3 & \frac{1}{\sqrt{s}}(y_2 - tx_3) \\ \frac{1}{\sqrt{s}}(z_2^* - t^*z_1^*) & \frac{1}{s}(z_4^* - t^*z_3^* - tz_2^* + |t|^2z_1^*) & \frac{1}{\sqrt{s}}(y_2^* - t^*x_3^*) & \frac{1}{s}(x_4 - ty_2^* - t^*y_2 + |t|^2x_3) \end{array}\right]. \tag{5.13}$$

We will not attempt to estimate every parameter of the EVM in Eq. (5.12). Instead, we will concentrate on constraining the diagonal elements of each block, namely the parameters x_1, x_2, x_3, x_4, z_1, and z_4. We can already estimate matrix elements of the form $\left\langle\lambda_k^{\mathrm{L}}\right| \rho_{kk}^{\mathrm{out}} \left|\lambda_k^{\mathrm{L}}\right\rangle$

(i.e., x_1 and x_4) using Prop. 5.1.1, but we need a different approach to constrain the supplementary elements $\langle\lambda_j^{\mathrm{L}}|\,\rho_{kk}^{\mathrm{out}}\,|\lambda_j^{\mathrm{L}}\rangle$ for $j \neq k$ (i.e., x_2 and x_3). To get these, we first expand ρ_{kk}^{out} into its eigenbasis, Eq. (5.2). Then, using the fact that $|\langle\phi|\xi\rangle|^2 \in [0,1]$ for any normalized vectors, we can derive the following bounds on the desired matrix elements (see App. B.2 for full details).

Proposition 5.1.3 (Supplementary diagonal bounds)**.** *The matrix elements given by* $x_2 = \langle\lambda_1^{\mathrm{L}}|\,\rho_{00}^{\mathrm{out}}\,|\lambda_1^{\mathrm{L}}\rangle$ *and* $x_3 = \langle\lambda_0^{\mathrm{L}}|\,\rho_{11}^{\mathrm{out}}\,|\lambda_0^{\mathrm{L}}\rangle$ *can be restricted to the following intervals:*

$$(1-U_0)\,|t|^2 \leq x_2 \leq (1-U_0)\,|t|^2 + U_0, \tag{5.14}$$

$$(1-U_1)\,|t|^2 \leq x_3 \leq (1-U_1)\,|t|^2 + U_1. \tag{5.15}$$

Finally, we need to estimate some elements of the off-diagonal blocks of ρ_{AB}^{Π}, or else there would be no way to differentiate an entangled state from a classical mixture of the output states. Recall that for quantum benchmarking, the test state overlaps are encoded into the reduced density matrix:

$$\mathrm{Tr}_B \rho_{AB}^{\mathrm{out}} = \rho_A = \frac{1}{2}\begin{bmatrix} 1 & c \\ c^* & 1 \end{bmatrix}, \tag{5.16}$$

where $c = \langle -\alpha|\alpha\rangle$. Each element in Eq. (5.16) is the trace of the corresponding block from Eq. (4.9), so we can enforce the condition $\mathrm{Tr}(\rho_{01}^{\mathrm{out}}) = c$. Using this as our starting point, we can determine the following (full details can be found in App. B.3).

Proposition 5.1.4 (Off-diagonal bounds)**.** *The off-diagonal elements* $z_1 = \langle\lambda_0^{\mathrm{L}}|\,\rho_{01}^{\mathrm{out}}\,|\lambda_0^{\mathrm{L}}\rangle$ *and* $z_4 = \langle\lambda_1^{\mathrm{L}}|\,\rho_{01}^{\mathrm{out}}\,|\lambda_1^{\mathrm{L}}\rangle$ *can be constrained to the following regions:*

$$|z_1| \geq |c| - \sqrt{U_0}\sqrt{1-(1-U_1)\,|t|^2}, \tag{5.17}$$

$$|z_4| \geq |c| - \sqrt{U_1}\sqrt{1-(1-U_0)\,|t|^2}. \tag{5.18}$$

We now have enough information to sufficiently constrain the projected state for the optimization of Eq. (4.34). To summarize, we have the quantities κ and U_k $(k = 0, 1)$, which can be calculated from measurements of the first moments and second moments, respectively. We want to determine ρ_{AB}^{Π}, which is the projection of ρ_{AB}^{out} onto the subspace spanned by $\{|0\rangle_A, |1\rangle_A\} \otimes \{|\lambda_0^{\mathrm{L}}\rangle_B, |\lambda_1^{\mathrm{L}}\rangle_B\}$, where $|\lambda_0^{\mathrm{L}}\rangle_B$ and $|\lambda_1^{\mathrm{L}}\rangle_B$ are the most significant eigenvectors of the output states. We have estimated some of the overlaps of ρ_{AB}^{out} with these basis vectors in Props. 5.1.1, 5.1.3, and 5.1.4. These estimates depend only on the

input parameter $c = \langle -\alpha | \alpha \rangle$ and on the output state quantities U_0, U_1, and t. The overlap t is itself bounded to a region defined by Prop. 5.1.2, which depends only on U_0, U_1 and κ. Hence, for a fixed input overlap c and a fixed set of homodyne measurement results, we have a parameter region that forms a set of constraints on ρ_{AB}^{Π}. For completeness, the full set of constraints used in the final optimization are listed in App. B.4. This constraint region must be searched to find the minimal entanglement compatible with ρ_{AB}^{Π}.

5.1.3 Minimizing the entanglement

As mentioned in Ch. 4, we will use the negativity (Eq. 2.8) as the entanglement measure for demonstrating our method. In principle, we would like to find the minimal entanglement using the methods of semidefinite programming (e.g., Eq. 2.9). However, semidefinite programs require that the constraints are convex and the objective function is linear in the employed parameters. As currently given, our constraints are non-convex (e.g., Eqs. (5.17)-(5.18)) and our parameters do not appear in a linear manner (e.g., quadratic dependancy on the parameter t). Hence, we must make some further simplifications and relaxations to bring our problem to the required form. Fortunately, the minimal entanglement under relaxed constraints will still form a lower bound to the true entanglement.

First, we exploit the fact that local unitary operations cannot change the quantity of entanglement. Therefore, without loss of generality, we can assume that the overlap $t = \left\langle \lambda_0^{\mathrm{L}} \middle| \lambda_1^{\mathrm{L}} \right\rangle$ is real and positive (since this can be accomplished by a relative change of phase on subsystem B):

$$t \geq 0. \tag{5.19}$$

As well, we can perform local phase changes on subsystem A, which allows us to also make the restriction

$$z_1 \geq 0. \tag{5.20}$$

The other off-diagonal element of interest, $z_4 = \left\langle \lambda_1^{\mathrm{L}} \middle| \rho_{01}^{\mathrm{out}} \middle| \lambda_1^{\mathrm{L}} \right\rangle$, is in general still a complex number. The accompanying bound, Eq. (5.18), is a non-convex constraint on z_4, so we have to replace it with a set of convex constraints. We accomplish this by denoting the right-hand side of Eq. (5.18) as

$$|c| - \sqrt{U_1}\sqrt{1 - (1 - U_0)\,|t|^2} =: r \tag{5.21}$$

and expanding the constraint to the region

$$|\mathrm{Re}(z_4)| + |\mathrm{Im}(z_4)| \geq r. \tag{5.22}$$

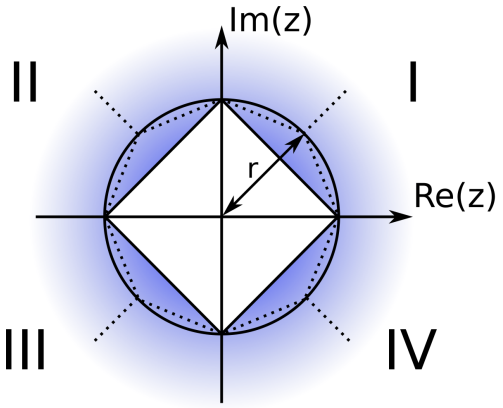


Figure 5.1: Relaxing the non-convex constraint Eq. (5.18) by inscribing a square within the circle (solid lines). Four new convex search regions (I-IV) are defined by the intersection of each quadrant with the weaker constraint Eq (5.22). These correspond to the outer regions in the diagram. Better approximations of the circular region can be made using an inscribed octagon or other polygons, but this increases the number of convex regions that must be searched for the overall minimum (dotted lines).

This relaxed constraint is still non-convex, but we can search for the minimum entanglement independently in each of the four quadrants, where the constraints are convex (see Fig. 5.1), and take the minimum over these four searches. The final result will be a lower bound to the minimum entanglement in the region constrained by Eq. (5.18). We can extend this idea further, replacing the inscribed square from Fig. 5.1 with any other inscribed polygon. With more sides, we can better approximate the non-convex constraint Eq. (5.18), but this will also increase the number of convex subregions that must be searched to find the overall minimum. Numerical evidence indicates that the minimum entanglement is often, though not always, found at a point outside the circle. The scheme was also tested with an inscribed octagon and it was not found to alter the final results significantly.

Fixing the overlap

The last hurdle comes from the overlap $t = \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$, which appears in the density matrix (Eq. (5.13)) and many constraints (e.g., Eqs. (5.14)-(5.15) and (5.17)-(5.18)) in a problematic non-linear manner. One approach would be to scan the parameter t through the domain $[b_l, b_u]$ using a discrete but fine set of points. The minimum values found in each run can be compared to find the overall minimum. However, this approach might open up

some unappealing continuity loopholes, nevermind the increased computational time.

Fortunately, when the other parameters are fixed, the two-qubit state with the minimal entanglement must always be one that has the largest possible overlap, $t = b_u$. The reason for this is that, for fixed values of λ_0^{L}, λ_1^{L}, and t, there always exists a CPTP map Ω on the B subsystem which preserves the maximal eigenvalues while making the corresponding overlap larger. Thus, a pair of qubit states with non-maximal overlap $t < b_u$ can always be mapped to a pair with the same eigenvalues but maximal overlap $t = b_u$. Such a local map cannot increase the entanglement, so indeed the minimal entanglement must come from a pair with overlap $t = b_u$. Exploiting this fact, we can eliminate the non-linear dependance in the optimization by replacing the parameter t with the fixed numerical quantity b_u.

The existence of the map Ω can be proven as a corollary to a theorem from [2] related to transformations on qubit pairs.

Theorem 5.1.5 (Alberti and Uhlmann)**.** *Let $\{\nu_k\}_{k=0,1}$ and $\{\omega_k\}_{k=0,1}$ be two pairs of qubit density matrices. There exists a CPTP map Ω such that $\omega_k = \Omega[\nu_k]$ for $k = 0, 1$ if and only if*

$$||\omega_0 - s\omega_1||_1 \leq ||\nu_0 - s\nu_1||_1 \ \forall \ s \geq 0, \tag{5.23}$$

where $||\cdot||_1$ denotes the trace norm.

Now let $\{\vec{n}_k\}_{k=0,1}$ and $\{\vec{w}_k\}_{k=0,1}$ be the Bloch vectors of these qubit states, and let θ_μ be the interior angle between the Bloch vectors of μ_0 and μ_1 ($\mu = \nu, \omega$). Then the above trace norm equates to, e.g.,

$$||\omega_0 - s\omega_1||_1 = \max\{|1 - s|, |\vec{w}_0 - s\vec{w}_1|\}. \tag{5.24}$$

By expanding the second term in Eq. (5.24) using the law of cosines, and enforcing the condition $|\vec{w}_k| = |\vec{n}_k|$ for $k = 0, 1$, we find, for all $s > 0$,

$$|\vec{w}_0 - s\vec{w}_1| \leq |\vec{n}_0 - s\vec{n}_1| \Leftrightarrow \theta_\omega \leq \theta_\nu. \tag{5.25}$$

Therefore, if the qubits $\{\omega_k\}$ have the same Bloch vector lengths as $\{\nu_k\}$ (relative to the index k), but smaller interior angle, then there is always a CPTP map taking the former to the latter[1]. Finally, we note that the parameters λ_0^{L}, λ_1^{L}, and t can be put into direct correspondence with Bloch vector lengths and an interior angle for qubit states within the projected subspace. By enacting the simplification made possible by this theorem, we can finally put the entanglement minimization into a practical linear form (see App. B.4 for a full list of the simplified constraints).

[1]Note that this is a special case. In general, there need not exist transformations between qubit pairs when the Bloch vector lengths are not fixed; see e.g., [3].

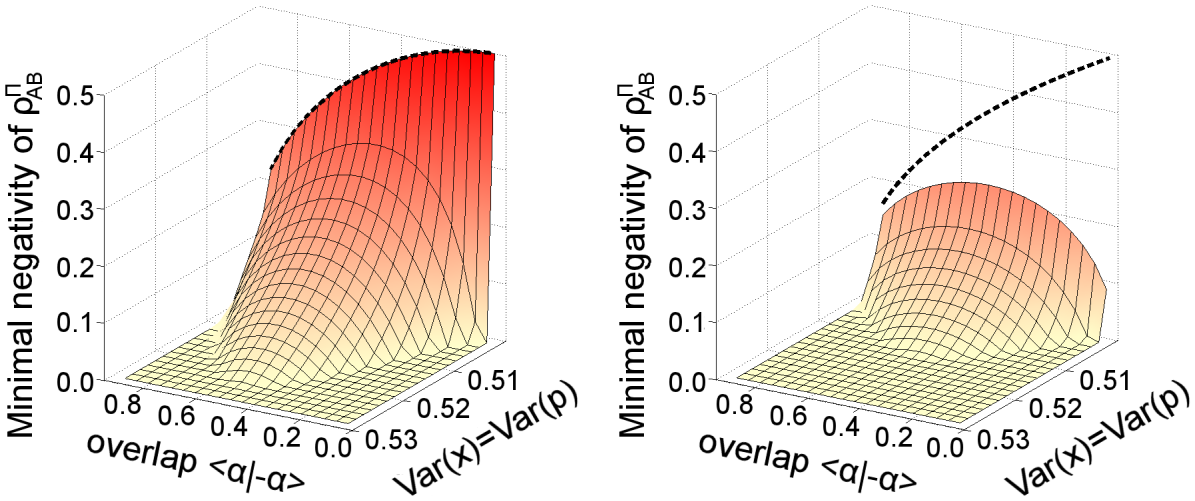
5.2 Results

In the previous section, we outlined how to estimate constraints and perform the entanglement optimization of Eq. (4.34) for a projection onto the most significant two-qubit subspace. With all the pieces now in place, we can finally apply our scheme to benchmarking quantum communication devices. For this, we do not want to make any assumptions about how a tested device works. However, in the absence of experimental data, we parameterize the device's effect on the first quadrature moments by a loss parameter and on the second moments by the excess noise, as defined in Eqs. (4.26) and (4.27). Since these parameters are defined using measurement results, we can always obtain them for the given test states.

To simplify the graphical representation of the results, and to be consistent with previous qualitative benchmarks [37], we assume that the loss and excess noise are symmetric for each state and for both quadratures $\hat{x}$ and $\hat{p}$. Note that our method does not rely on making these assumptions. The optimization was performed in Matlab as a semidefinite programming problem (see App. B.4) using the YALMIP interface [66] along with the solver SDPT3 [94]. The main results are shown in Fig. 5.2, where the minimal negativity of ρ_{AB}^{Π} compatible with the initial overlap and symmetric variances is given, for two different values of the transmissivity T. This quantity gives a lower bound on the negativity of the full state ρ_{AB}^{out}. The entanglement of the initial state, Eq. (5.1), is also shown as a function of the initial overlap in Fig. 5.2a. This initial entanglement can be compared with the calculated bounds to help elucidate the quantum throughput of the device. We note that a maximally entangled two-qubit state has negativity $\mathcal{N} = \frac{1}{2}$. For Fig. 5.2b, the modification $\alpha \to \sqrt{T}\alpha$ is made to the entangled input state in Eq. (5.1) to give similar comparisons. In the limit of zero excess noise and zero loss, our entanglement bound is tight with the initial entanglement.

Our bounds are quite high for very low noise, but they become lower as the measurement results get more noisy. At some point, a non-trivial entanglement bound can no longer be given, even though the quantum domain is known to extend to higher noise values (see e.g., Fig. 4.3 or 5.3). As well, for larger loss values, the tolerance for excess noise is lower, and the region where non-trivial bounds can be given becomes smaller. The exact noise value where our bounds become trivial depends on the initial overlap and on the measured loss, but the highest tolerable excess noise is around 0.025 for $T = 1.0$. This shrinks to about 0.015 for a transmissivity of $T = 0.5$. Though the quantification region is small, it is within the limits of current experimental technology [105].

Some entanglement degradation should be expected as the noise is increased, but entan-



(a) T=1.0 (b) T=0.5

Figure 5.2: Minimal negativity of ρ^{Π}_{AB} consistent with initial overlap $\langle\alpha|-\alpha\rangle$ and channel loss and noise parameters. For comparison, the dashed lines show the negativity for states of the form of Eq. (5.1), with α replaced by $\sqrt{T}\alpha$. For no loss and no noise, the bound exactly matches the initial entanglement. As either loss or noise increases, the bound lowers, until it becomes trivially equal to zero.

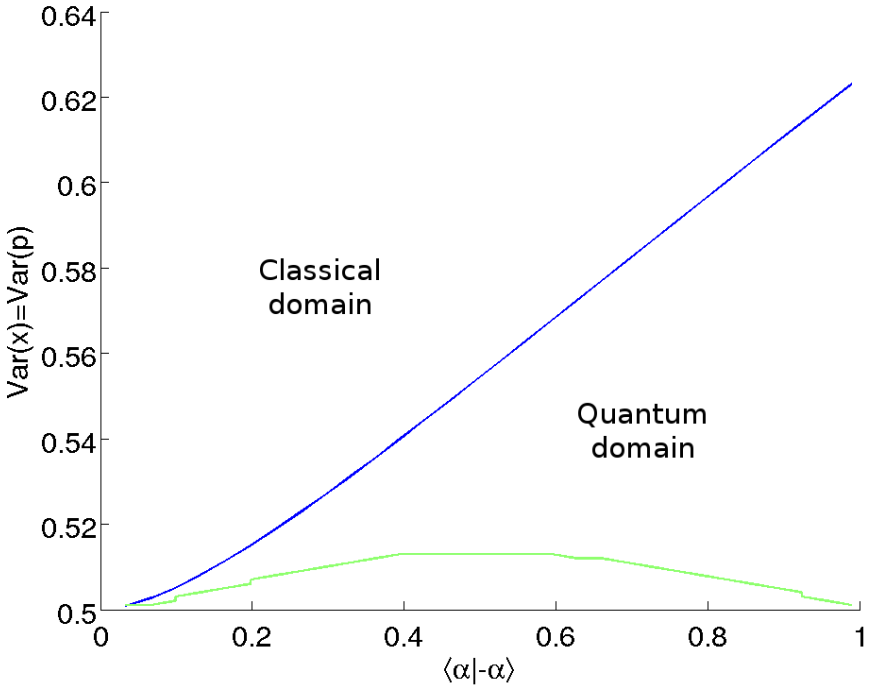


Figure 5.3: Example benchmark results using two coherent states ($T = 0.448$). The upper line was found using the EVM method; any data below this line is in the quantum domain. States for which the two-qubit projection scheme gave non-zero entanglement lie below the lower line. The 'quantitative domain' does not match the quantum domain, indicating that the two-qubit projection is not well-suited to higher noise values. Figure appears in [55], copyright 2011 by the American Physical Society. Reprinted with permission.

glement can be verified (though not previously quantified) under the same testing scenario up to much higher noise values than seen here. Thus, our bounds do not provide the full picture. The weakening of the bounds with higher noise is mainly due to the estimation procedure. Certain approximations become cruder (though still valid) as the noise increases. First, for higher noise, the output states become more mixed, spreading out into more of the infinite-dimensional mode Hilbert space. This leads to additional information being lost when we truncate down from ρ_{AB}^{out} to a two-qubit ρ_{AB}^{Π}. Another problem stems from the bounds we use to estimate ρ_{AB}^{Π}. Higher noise leads to weaker bounds on the maximal eigenvalues from Prop. 5.1.1, which weakens all other inequalities.

To examine the effects of these two approximations, we briefly consider a simple channel where the test state, Eq. (5.1), is mixed at a 50 : 50 beam-splitter with a thermalized vacuum. The first moments reduce by a factor of $\frac{1}{\sqrt{2}}$, and the increased variances of the output optical states can be determined from the mean photon number $\overline{n}$ of the thermal state. For $\overline{n} > 0$, the output states are displaced thermal states. The reason for studying this channel is that we can *exactly* determine the maximal eigenvalues λ_0^{L}, λ_1^{L}, and the overlap $\left\langle \lambda_0^{\text{L}} \middle| \lambda_1^{\text{L}} \right\rangle$. This allows us to study our approximations independently, since we decouple the effects of the two-qubit projection from the homodyne parameter estimation (in practice, of course, our quantification scheme must use both). In Fig. 5.4 we show the result of the quantification scheme when this extra information is included.

We see that the tolerable excess noise is around 0.05, more than three times what it would be if we had to estimate the eigenvalues and overlap using homodyne results (cf. Fig. 5.2b). Also included in Fig. 5.4 is the quantum domain boundary obtained using the EVM method. Any data with lower variances than this curve are in the quantum domain and must come from entangled states. The two-qubit projection is tight to the quantum domain boundary for low overlaps. For higher values, the projection becomes weaker, only working to about half the noise value that the boundary curve reaches.

Summary and outlook

We began this chapter by proposing the simplest possible finite-dimensional projection that will still allow entanglement, namely onto a two-qubit subspace. We compiled a number of bounds relating the available benchmarking information to the most relevant parameters of the two-qubit subspace. Collectively, these bounds formed the constraints for the entanglement-minimization problem of Eq. (4.34). We also gave a number of simplifications which enabled this optimization to be performed as a semidefinite program. We were successfully able to quantify a non-zero amount of entanglement for the considered benchmarking scenario, the first successful result in this direction. The tools developed

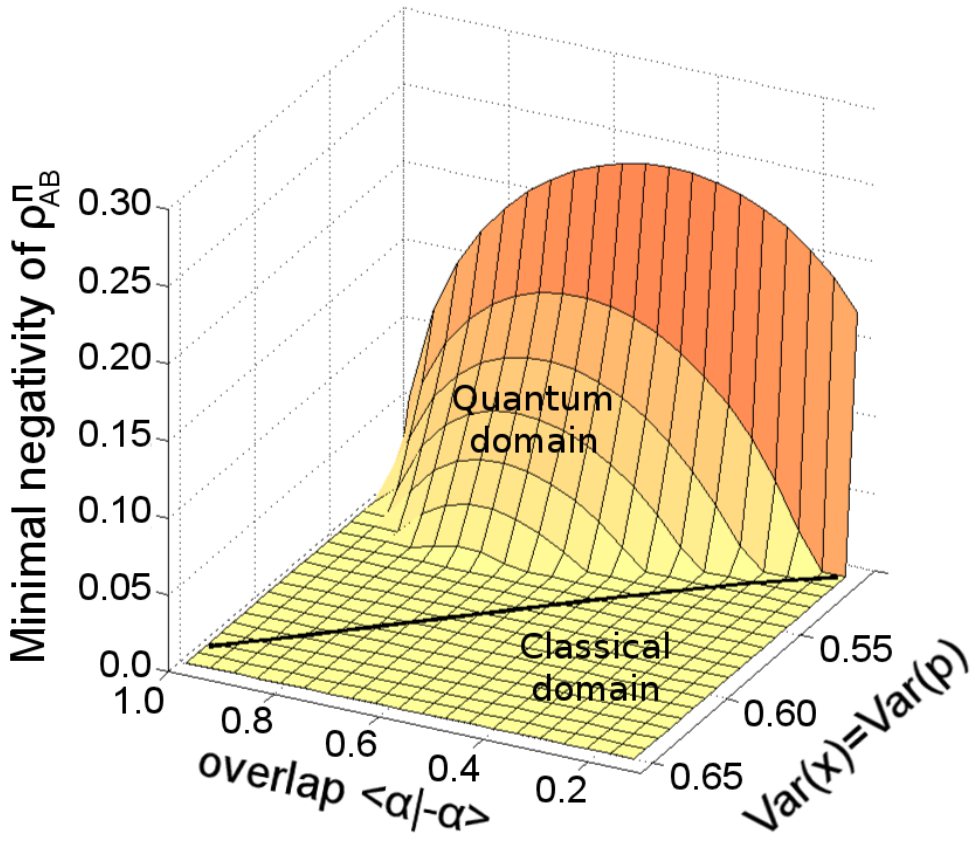


Figure 5.4: Results of the quantification scheme for a simple test channel where we can exactly determine the two-qubit projection parameters λ_0^{L}, λ_1^{L}, and $\langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$. The excess noise is due to the non-zero mean photon number of the thermal state. The overall channel transmissivity is T=0.5, as in Fig. 5.2b. We also show the region where entanglement can be verified (points with lower noise than the black line), i.e., the quantum domain. The two-qubit projection gives non-trivial entanglement bounds for roughly half the points where the entanglement can be verified.

in this section can be directly applied to quantitatively benchmark any device which fits within the given quantitative region.

Ideally, we want to be able to calculate non-trivial values for the entanglement wherever it can be verified. This would give us a true quantitative complement to existing entanglement verification methods. Comparing the quantum domain with the quantitative domain in Fig. 5.3, we see that the approach taken in this chapter is not strong enough to enable quantification for higher noise values. Thus, more work needs to be done to address this discrepancy. One obvious extension of the present scheme would be to truncate the mode subspace using the two largest eigenstates from each output state, or even more. In theory, this would strictly improve the estimates. However, in practice, this will increase the complexity of the quantification calculation, since some simplifying assumptions (e.g., certain overlaps are real) may no longer be valid. As well, the number of additional minimizations we have to do, as in our non-convex relaxation of Eq. (5.18), increases fourfold with each added dimension. Another approach might therefore be necessary to overcome this problem. One such approach is examined in the next chapter. Nevertheless, the quantification scheme outlined here is a useful method for characterizing the degree of quantumness of optical channels, especially when these channels introduce low noise.

Chapter 6

Quantitative benchmarking II: Fock-state projection

This chapter outlines an alternate method for achieving quantitative CV benchmarks using the framework of Ch. 4. This time, the finite-dimensional projection involves low-energy Fock states. The material in this chapter, as well as the accompanying App. C, is based largely on [55], for which I am the primary author and researcher. The published article is copyright 2011 by the American Physical Society (APS). Portions of the article have been adapted for this thesis, under permission from APS.

This chapter is organized as follows. We first identify a finite subspace, based on low-energy Fock states, to be used with the projection method of Ch. 4. We then derive a number of rigorous bounds which form the constraints for our finite-dimensional entanglement minimization problem, Eq. (4.34). We proceed to show how these constraints can be encoded compactly as positive semidefinite matrix inequalities, allowing us to numerically solve the given optimization. Finally, the strength of this approach is demonstrated through a number of examples involving different test ensembles.

6.1 Quantification procedure

The quantitative benchmarking results presented in the previous chapter are an important first step, but it is clear that there remains room for improvement. For one, the 'quantitative domain' should be as faithful as possible with the quantum domain. Ideally, a quantitative scheme should be just as strong for detecting entanglement as a qualitative scheme (like the EVM method), with the quantitative component providing an extra layer of information. Although the two-qubit projection in the previous chapter is quite good for low levels of imperfection, it is not very effective for higher excess noise. The resulting quantitative domain is much smaller than the corresponding quantum domain, as seen in Fig. 5.3. Additionally, the results of the previous chapter are only applicable to the case of two coherent test states. Thus, it is desirable to have a stronger and more general approach that can be applied to a number of different CV testing scenarios.

6.1.1 Choosing the projection

In order to keep our scheme as general as possible, we should use a subspace that is not based specifically on one type of test state. Indeed, we would like the subspace to contain information about many different types of relevant states. One common feature for many

of the CV test states typically used for benchmarking is that they are *low-energy*[1]. This motivates the use of a subspace which itself is made of low-energy states. For numerical simplicity, we want this subspace to be small in dimension. But it should not be too small; indeed, we saw in the previous chapter that projecting onto a qubit subspace led to important information being lost.

Given this motivation, perhaps the most natural choice of projection is a projection onto the energy eigenstates, namely the Fock states $\{|n\rangle\}_{n=0}^{\infty}$. These states form a basis for the state space of a mode, so we can define a subspace simply by truncating at some finite number N. Intuitively, the larger the cutoff N is, the closer the projected state ρ_{AB}^{Π} should be to the full state ρ_{AB}^{out}. In fact, in the limit $N \to \infty$, the projected state converges to the full state.

The projection operator for this subspace takes the form

$$\hat{\Pi}_B := \sum_{m=0}^{N} |m\rangle\langle m|_B \,. \tag{6.1}$$

The corresponding projected output state can be written as (cf. Eq. (4.9))

$$\rho_{AB}^{\Pi} = \frac{1}{M} \begin{bmatrix} \rho_{00}^N & \rho_{01}^N & \cdots & \rho_{0,M-1}^N \\ \rho_{10}^N & \rho_{11}^N & \cdots & \rho_{1,M-1}^N \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{M-1,0}^N & \rho_{M-1,1}^N & \cdots & \rho_{M-1,M-1}^N \end{bmatrix}, \tag{6.2}$$

where we define each block using the truncated Fock basis,

$$\rho_{kl}^N := \hat{\Pi}_B \rho_{kl}^{\text{out}} \hat{\Pi}_B = \sum_{m,n=0}^{N} \langle m| \rho_{kl}^{\text{out}} |n\rangle \, |m\rangle\langle n|_B \,. \tag{6.3}$$

To distinguish this type of projection, we will also denote the projected state by ρ_{AB}^N.

6.1.2 Estimating the constraints

We use the same general optimization framework of Eq. (4.34) as the two-qubit projection of the previous chapter. As was the case there, the given homodyne measurements do not

[1]Test states that are not low-energy, but which have high mutual overlaps can be converted to low-energy states through a unitary displacement of the origin of phase space.

directly tell us anything about the chosen subspace. Thus, it is necessary to determine some useful constraints indirectly from the available information. In the spirit of quantum benchmarking, we seek rigorous bounds, not approximations. We already gave some bounds for the two-qubit projection in Ch. 5. We will see that the projection onto Fock states leads to a much different set of constraints than the two-qubit case.

To begin, we make the important observation that it is not necessary for the projected subspace to be excessively large. As long as the cutoff dimension N is large compared to the mean photon number $\overline{n}$, a state and its projected form will be nearly identical. Why is this so? Because high Fock levels contribute more to the state's energy than low Fock levels. If we know $\overline{n}$, we can put strong bounds on the contributions from high Fock levels. We make this intuition concrete with the following lemma.

Lemma 6.1.1 (Trace constraint)**.** *Let τ be the state of a single optical mode, with mean photon number $\mathrm{Tr}(\tau\hat{n}) = \overline{n} < \infty$. Let τ_N be the (unnormalized) projection of τ up to the Fock level $N > 0$,*

$$\tau_N = \sum_{m,n=0}^{N} \langle m| \tau |n\rangle |m\rangle\langle n|, \tag{6.4}$$

and denote the expectation value of τ_N with respect to $\hat{n}$ by

$$\mathrm{Tr}(\tau_N \hat{n}) =: \overline{n}_N. \tag{6.5}$$

Then the following inequality holds:

$$\mathrm{Tr}(\tau) - \mathrm{Tr}(\tau_N) \leq \frac{\overline{n} - \overline{n}_N}{N+1}. \tag{6.6}$$

Proof. For $k > 0$, parametrize the diagonal entries of τ by

$$\tau_m = \langle m| \tau |m\rangle =: \frac{c_m}{m}. \tag{6.7}$$

The coefficients c_m are positive, but otherwise unknown. We have

$$\mathrm{Tr}(\tau\hat{n}) = \sum_{m=0}^{\infty} m\tau_m = \sum_{m=1}^{\infty} c_m = \overline{n}, \tag{6.8}$$

and

$$\mathrm{Tr}(\tau_N \hat{n}) = \sum_{m=1}^{N} c_m = \overline{n}_N. \tag{6.9}$$

This leads to

$$\begin{aligned}\mathrm{Tr}(\tau) - \mathrm{Tr}(\tau_N) &= \sum_{m=N+1}^{\infty} \frac{c_m}{m} \\ &\leq \sum_{m=N+1}^{\infty} \frac{c_m}{N+1} \\ &= \frac{1}{N+1}\left(\sum_{m=1}^{\infty} c_m - \sum_{m=1}^{N} c_m\right) \\ &= \frac{\overline{n} - \overline{n}_N}{N+1}. \end{aligned} \tag{6.10}$$

□

Note that this upper bound can actually be saturated, for example by the state

$$\tau = \left(1 - \frac{\overline{n}}{N+1}\right)|0\rangle\langle 0| + \frac{\overline{n}}{N+1}|N+1\rangle\langle N+1|. \tag{6.11}$$

This lemma provides an upper bound on how different the trace of a state is from the trace of its projected form. Since the mean photon number can be inferred from homodyne measurements,

$$\overline{n} := \langle \hat{n} \rangle = \frac{1}{2}\left[\langle \hat{x}^2 \rangle + \langle \hat{p}^2 \rangle - \langle \hat{\mathbb{1}} \rangle\right], \tag{6.12}$$

we can easily apply this lemma to the present benchmarking scenario. In this case, the quantity $\overline{n}_N$ will be a free parameter which is a linear combination of diagonal elements from τ_N. It is only constrained by the obvious bounds $0 \leq \overline{n}_N \leq \overline{n}$. Although it would be valid to replace the right hand side of Eq. (6.6) with the fixed numerical quantity $\overline{n}/(N+1)$, it is more useful to use the bound as is, since it links the constraints on $\mathrm{Tr}(\tau_N)$ and $\overline{n}_N$. Most importantly, since $\overline{n}$ is fixed, the bound can be made arbitrarily tight by increasing the cutoff N.

We can derive similar constraints (also depending on $\overline{n}$ and N) for all the other important expectation values. For instance, if a state τ has some known values of $\langle \hat{x} \rangle$ and $\langle \hat{p} \rangle$, then the expectation values of the same operators with respect to the truncated state τ_N cannot be entirely arbitrary. In fact, if N is large enough, the truncated state's quadratures have to be quite close to the infinite-dimensional state's quadratures. We can make this argument explicit with the following bound, involving the ladder operator $\hat{a} = \frac{1}{\sqrt{2}}(\hat{x} + i\hat{p})$.

Lemma 6.1.2 (First-order constraint)**.** *Define the quantity ϵ as follows:*

$$\epsilon := \sqrt{(\overline{n} - \overline{n}_N)(\mathrm{Tr}(\tau) - \mathrm{Tr}(\tau_{N-1}))}, \tag{6.13}$$

where τ_{N-1} is the truncation of the state τ up to Fock level $N-1$. Then the expectation value $\mathrm{Tr}(\tau\hat{a})$ is constrained to the following region:

$$|\mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a})| \leq \epsilon. \tag{6.14}$$

This constraint can be straightforwardly derived by expanding the ladder operator in the Fock basis and applying the triangle and Cauchy-Schwarz inequalities, as well as appealing to the positivity of τ. The full derivation can be found in App. C.1.

Although the quantity $\mathrm{Tr}(\tau\hat{a})$ is not directly measurable, it can be found from the expectation values of the quadratures $\hat{x}$ and $\hat{p}$ with respect to τ. As well, the bound ϵ is not fixed, since it depends on other parameters. However, by the Fock cutoff lemma, it has an upper bound

$$\epsilon \leq \frac{\overline{n}}{\sqrt{N}}. \tag{6.15}$$

Thus, it is clear that the constraint in Eq. (6.14) can also be made tighter by increasing N. In practice, we will use the adaptive constraint of Eq. (6.13), not the weaker numerical bound $\frac{\overline{n}}{\sqrt{N}}$.

The other important operators for our problem are $\hat{x}^2$ and $\hat{p}^2$. Instead of directly working with these, it is useful to consider their difference,

$$\hat{d} := \hat{x}^2 - \hat{p}^2 = \hat{a}^{\dagger 2} + \hat{a}^2. \tag{6.16}$$

Although this operator is itself an observable, the required expectation values can be readily found from the available homodyne data. The original operators can be recovered using the relations

$$\hat{x}^2 = \frac{1}{2}\left[\hat{d} + 2\hat{n} + \hat{\mathbb{1}}\right], \tag{6.17}$$

$$\hat{p}^2 = \frac{1}{2}\left[-\hat{d} + 2\hat{n} + \hat{\mathbb{1}}\right]. \tag{6.18}$$

In a similar manner as before, we can bound the difference in expectation values of $\hat{d}$ for the measured infinite-dimensional state and for its truncation.

Lemma 6.1.3 (Second-order constraint)**.** *Define the quantity δ as follows:*

$$\delta := 2\sqrt{(\overline{n} - \overline{n}_N)\left[(\overline{n} - \overline{n}_{N-2}) + (\mathrm{Tr}(\tau) - \mathrm{Tr}(\tau_{N-2}))\right]}, \tag{6.19}$$

where τ_{N-2} is the truncation of the state τ up to Fock level $N-2$ and $\overline{n}_{N-2} := \mathrm{Tr}(\tau_{N-2}\hat{n})$. Then the expectation value $\mathrm{Tr}(\tau\hat{d})$ is constrained to the following region:

$$\left|\mathrm{Tr}(\tau\hat{d}) - \mathrm{Tr}(\tau_N\hat{d})\right| \leq \delta. \tag{6.20}$$

The proof of this bound uses similar arguments as the ϵ bound (see App. C.2 for details).

The final source of information in our benchmarking scheme is the reduced density matrix ρ_A. To see how to include this type of information, let τ_{AB} be a bipartite state, with reduced density matrix $\tau_A = \mathrm{Tr}_B(\tau_{AB})$. Let $\hat{\Pi}_B$ be the projector given in Eq. (6.1) and recall the complementary projector $\hat{Q}_B = \hat{\mathbb{1}}_B - \hat{\Pi}_B$ (which implies $\hat{Q}_B\hat{\Pi}_B = \hat{\Pi}_B\hat{Q}_B = 0$). We also let

$$\tau_{AB}^N := (\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)\tau_{AB}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B), \tag{6.21}$$

and similarly define τ_{AB}^Q using Q. Using the given relations, we find

$$\begin{aligned}\tau_A =& \mathrm{Tr}_B(\tau_{AB}(\hat{\mathbb{1}}_A \otimes [\hat{\Pi}_B + \hat{Q}_B]^2)) &(6.22)\\ =& \mathrm{Tr}_B(\tau_{AB}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)^2) + \mathrm{Tr}_B(\tau_{AB}(\hat{\mathbb{1}}_A \otimes \hat{Q}_B)^2). &(6.23)\end{aligned}$$

But

$$\mathrm{Tr}_B(\tau_{AB}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)^2) = \mathrm{Tr}_B((\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)\tau_{AB}(\hat{\mathbb{1}}_A \otimes \hat{\Pi}_B)), \tag{6.24}$$

(and similarly for the Q term), so that

$$\tau_A = \mathrm{Tr}_B(\tau_{AB}^N) + \mathrm{Tr}_B(\tau_{AB}^Q). \tag{6.25}$$

Since τ_{AB}^N and τ_{AB}^Q are positive matrices, so are their reduced forms $\mathrm{Tr}_B(\tau_{AB}^N)$ and $\mathrm{Tr}_B(\tau_{AB}^Q)$. Removing $\mathrm{Tr}_B(\tau_{AB}^Q)$ at the expense of an inequality, we are left with the following.

Lemma 6.1.4 (Reduced density matrix constraint)**.** *Let τ_{AB} be an arbitrary state and τ_{AB}^N its projection up to Fock level N. Let the reduced density matrices be denoted by $\tau_A := \mathrm{Tr}_B(\tau_{AB})$ and $\tau_A^N := \mathrm{Tr}_B(\tau_{AB}^N)$. Then the following matrix inequality must hold:*

$$\tau_A \geq \tau_A^N. \tag{6.26}$$

Although it may not be obvious at this point, Lemma 6.1.4 can be used to tightly constrain expectation values for the off-diagonal blocks ρ_{kl}^N of the projected state. As with the other bounds, increasing the cutoff N will strengthen the constraints. We will elaborate further about how to use this matrix inequality below. The inequalities found in Lemmas 6.1.1-6.1.4 can be used as constraints for the general entanglement-minimization problem of Eq. (4.34). Asymptotically, as $N \to \infty$, these inequalities become equality constraints, and the finite-dimensional optimization of Eq. (4.34) converges to the infinite-dimensional optimization of Eq. (4.28). We explore how to numerically encode the finite optimization in the next subsection.

6.1.3 Minimizing the entanglement

From the homodyne measurements, we can determine the expectation values of $\hat{a}$ and $\hat{d}$ for each of the output states ρ_k^{out}. Along with $\hat{\mathbb{1}}_B$, these will be the operators $\hat{C}_B^j$ found in the entanglement minimization problem of Eq. (4.34). The bounds given in Lemmas 6.1.1-6.1.3, with τ replaced by the test states ρ_k^{out}, constitute the corresponding constraint regions $\mathcal{C}(\rho_k^{\text{out}}, \hat{C}_B^j)$. As well, we can substitute the reduced density matrix ρ_A into Lemma 6.1.4 to define the constraint region $\mathcal{C}(\rho_A)$.

To solve the optimization problem, we again turn to semidefinite programming. In principle, the matrices representing the operators $\hat{x}$ and $\hat{p}$ in the Fock basis are infinite-dimensional. This can lead to problems when working with them numerically. However, for a state that only has support up to Fock level N, there is no cause for concern. Such expectation values can be implemented by using truncated versions of the quadrature operators themselves. Indeed, if $\hat{x}_N = \hat{\Pi}_B \hat{x} \hat{\Pi}_B$ is the (bounded) projection of $\hat{x}$ up to Fock level N, then

$$\text{Tr}(\tau_N \hat{x}) = \text{Tr}(\tau_N \hat{x}_N). \tag{6.27}$$

Hence, expectation values of the quadratures are simply finite linear combinations of elements from τ_N. The same idea holds as well for higher powers of the quadratures, as in the operator $\hat{d}$.

Conveniently, the above constraints can all be written in the form of matrix inequalities. For instance, for any τ that is positive, the constraint in Lemma 6.1.2 may be recast as

$$\begin{bmatrix} \overline{n} - \overline{n}_N & \text{Tr}(\tau \hat{a}) - \text{Tr}(\tau_N \hat{a}) \\ \text{Tr}(\tau \hat{a}^\dagger) - \text{Tr}(\tau_N \hat{a}^\dagger) & \text{Tr}(\tau) - \text{Tr}(\tau_{N-1}) \end{bmatrix} \geq 0. \tag{6.28}$$

Similarly, we can rewrite the second order constraint found in Lemma 6.1.3, as the matrix

inequality

$$\begin{bmatrix} 4(\overline{n}-\overline{n}_N) & \mathrm{Tr}(\tau\hat{d})-\mathrm{Tr}(\tau_N\hat{d}) \\ \mathrm{Tr}(\tau\hat{d})-\mathrm{Tr}(\tau_N\hat{d}) & \overline{n}-\overline{n}_{N-2}+\mathrm{Tr}(\tau)-\mathrm{Tr}(\tau_{N-2}) \end{bmatrix} \geq 0. \tag{6.29}$$

We recall that two-dimensional matrices are positive semidefinite if and only if the diagonal entries and the determinant are all non-negative. This lets us compactly encode the above expectation value bounds (the determinant) as well as some auxilliary bounds (the diagonal entries). These matrix inequality constraints can be formed for each output state ρ_k^{out}.

Finally, the reduced density matrix inequality from Lemma 6.1.4 can be applied to the benchmarking states, giving directly a positive semidefinite constraint

$$\rho_A \geq \rho_A^N, \tag{6.30}$$

where $\rho_A^N := \mathrm{Tr}_B(\rho_{AB}^N)$ is the reduced form of the projected state. To understand this constraint better, we recall the block form of ρ_{AB}^{Π} from Eq. (6.2). The (k,l)-element of ρ_A^N is connected directly to the trace of the block ρ_{kl}^N, i.e.,

$$\langle k|\,\rho_A^N\,|l\rangle = \frac{1}{M}\mathrm{Tr}(\rho_{kl}^N). \tag{6.31}$$

The inequality (6.30) allows us to constrain the trace of each block ρ_{kl}^N. To see this, consider a scenario where subsystem A is two dimensional. Then matrix inequality (6.30) becomes

$$\begin{bmatrix} \mathrm{Tr}(\rho_{00})-\mathrm{Tr}(\rho_{00}^N) & \mathrm{Tr}(\rho_{01})-\mathrm{Tr}(\rho_{01}^N) \\ \mathrm{Tr}(\rho_{10})-\mathrm{Tr}(\rho_{10}^N) & \mathrm{Tr}(\rho_{11})-\mathrm{Tr}(\rho_{11}^N) \end{bmatrix} \geq 0. \tag{6.32}$$

Taking the determinant, we get

$$|\mathrm{Tr}(\rho_{01})-\mathrm{Tr}(\rho_{01}^N)| \leq \sqrt{[\mathrm{Tr}(\rho_{00})-\mathrm{Tr}(\rho_{00}^N)]\,[\mathrm{Tr}(\rho_{11})-\mathrm{Tr}(\rho_{11}^N)]}. \tag{6.33}$$

This constraint is therefore very similar to the other ones, and it should be clear that we can make it stronger by increasing the cutoff N. We should point out that if subsystem A has more than two dimensions, the inequality (6.30) becomes even stronger since it also forces higher order determinants to be positive.

As in the previous chapter, we choose the negativity (Eqs. (2.8)-(2.9)) as our entanglement measure. Hence, the constraints and the objective function of the entanglement minimization problem can all be encoded into a semidefinite program.

6.2 Results

We present results for the following ensembles of test states: (a) two coherent states [84, 37], (b) two squeezed states [35], and (c) three coherent states [36]. All optimizations were encoded as semidefinite programs in Matlab using the solver SDPT3 [94] and the frontend YALMIP [66], on a desktop computer with a 3 GHz dual-core processor and 4 GB of RAM. First, our results for the two coherent state benchmark are shown in Fig. 6.1, where we have used a cutoff at $N = 20$ and fixed the transmissivity as $T = 1.0$. To be consistent with previous qualitative benchmarks, and to simplify the display of results, we assume the transmissivity and the excess noise are symmetric for both states and both quadratures. We can see that the results are very faithful, being non-zero throughout nearly all of quantum domain. For other values of T, where the quantum domain is smaller, the results are similarly faithful.

Only in the extreme regions of low overlap/low variance and high overlap/high variance are there small differences between the quantitative domain and the quantum domain. Both of these cases correspond to high values of $\overline{n}$, where the constraints are the weakest. But we expect very little effective entanglement can be found in these regions anyway. The region where $\langle\alpha|-\alpha\rangle \to 1$ has very little initial entanglement (since the test states are nearly identical), and there will be even less after the test states pass through the device. On the other hand, in the region where $\langle\alpha|-\alpha\rangle \to 0$, ρ_A becomes diagonal and the entangled state is indistinguishable from a classical mixture of the test states with the available information. Although the benchmarking state may be highly entangled, we cannot recognize any entanglement in our source-replacement scheme with a diagonal ρ_A. In principle, the quantitative domain could be extended by raising the cutoff N. Since in the limit $N \to \infty$, the finite optimization problem (4.34) converges to the infinite-dimensional version (4.28), we conjecture that any mismatch between the quantitative domain and the quantum domain can be resolved by using sufficiently large computational resources.

Another important class of entanglement-based benchmarks uses squeezed and antisqueezed vacua as test states. For consistency with previous qualitative results [35], we restrict ourselves to devices whose operation is phase independent, so that the changes in the squeezed/antisqueezed quadratures are the same for both test states, regardless of their orientation. In this case, the relevant parameters for the quantum domain are simply the initial squeezing magnitude r and the output variances of one test state, $\mathrm{Var}_0(\hat{x})$ and $\mathrm{Var}_0(\hat{p})$. Example results for this benchmark type are shown in Fig. 6.2, for the parameters $r = 0.35$ and $N = 20$. We see that the quantitative domain is very faithful with the quantum domain in the given parameter region. For much larger values of the variance than shown in Fig. 6.2, the entanglement bounds eventually decay. Again, this is due to

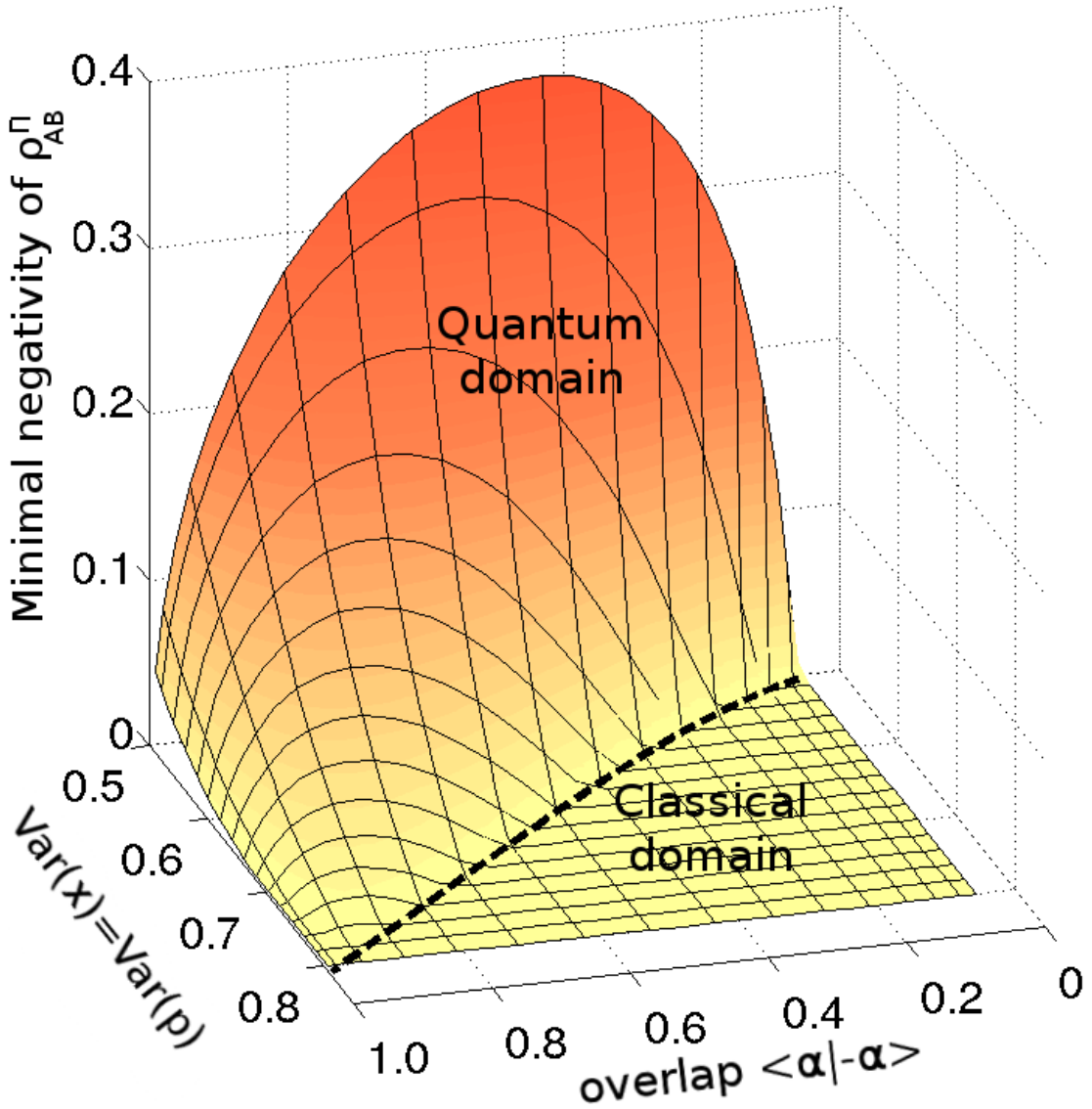


Figure 6.1: Entanglement bounds for the two coherent state benchmark, using a Fock-state projection (with $N = 20$), assuming no loss ($T = 1.0$). The dashed black line represents the boundary of the quantum domain, found using the EVM method. Variances lower than this line correspond to devices within the quantum domain, whereas variances higher than this line are known to be compatible with separable states [37] (note that the axes are inverted in order to see the results better). Direct comparison with Fig. 5.2a shows a dramatic improvement in the entanglement bounds at higher variances.

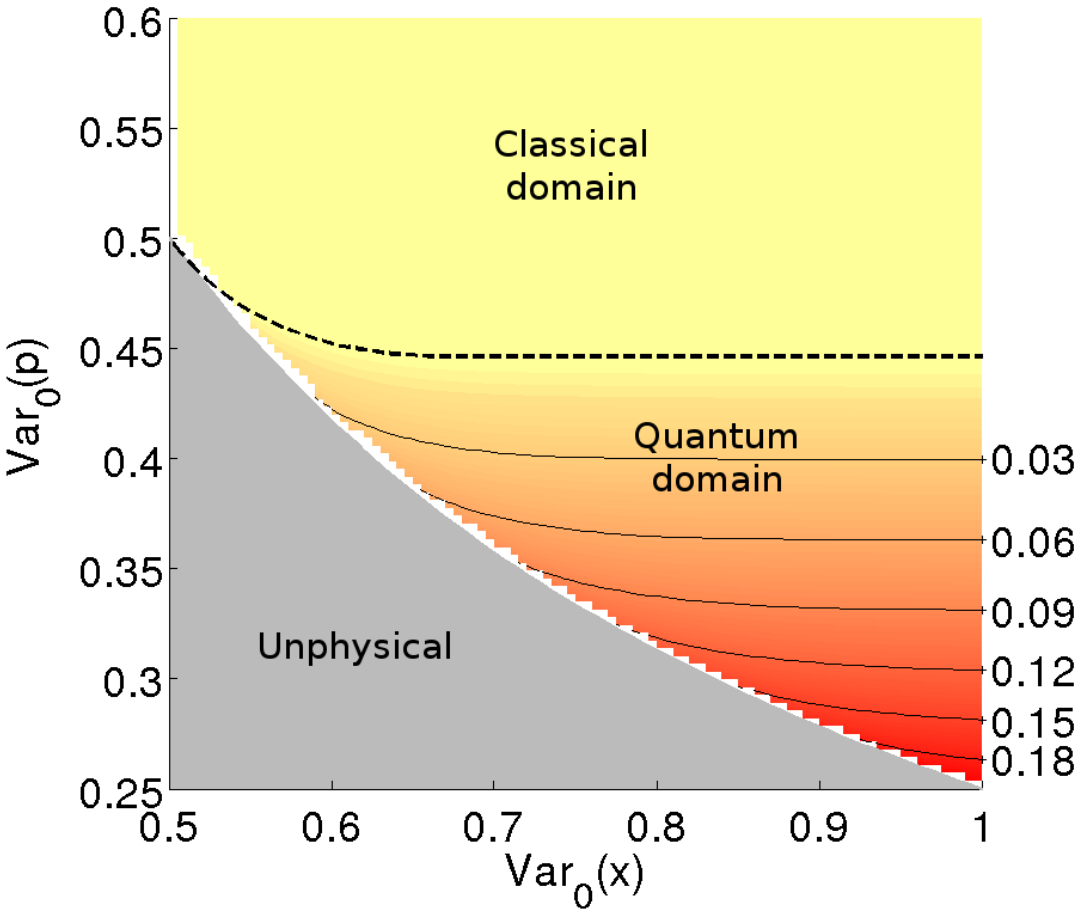


Figure 6.2: Entanglement quantification for squeezed/antisqueezed state benchmarks, using initial squeezing magnitude $r = 0.35$ and cutoff $N = 20$ (cf. Fig. 4.5). The bottom left region is forbidden by the uncertainty relation. The quantum domain lies between the forbidden region and the upper dashed line (found with EVM method – variances above this line are compatible with separable states [35]). The quantitative domain, shown using level curves of the minimal negativity, is very faithful in this parameter regime; the zero contour and the quantum domain boundary coincide within the numerical resolution. For much larger values of $\mathrm{Var}_0(\hat{x})$, the two domains begin to diverge due to reduced numerical accuracy. The small 'sawtooth' gap near the unphysical boundary is due to the finite resolution of sampled points.

the chosen cutoff $N = 20$ not being large enough to counter higher noise values.

Finally, the last example we will consider is three coherent states distributed symmetrically on a ring. Benchmarks with multiple coherent states are known to lead to larger quantum domains than those with just two coherent states (see Fig. 4.4). The magnitude $|\alpha|$ of the coherent states is used as an input parameter, while loss and excess noise paramatrize the output (again assumed symmetric). The results for this scenario are shown in Fig. 6.3, using $N = 15$ (this is lower than in the previous cases because the extra dimension on subsystem A also needs to be accommodated within our available computation resources). We find that the quantitative domain is larger than for two coherent states. However, there is a small but noticable gap between the quantitative domain and the known quantum domain.

To explore the strength of our scheme, we consider the following hybrid of the optimizations (4.28) and (4.34):

$$\mathcal{E}_{\text{hybrid}}(\rho_{AB}^{\text{out}}) = \begin{cases} \min\limits_{\sigma_{AB}^{\Pi} \geq 0} & \mathcal{E}(\sigma_{AB}^{\Pi}) \\ \text{subject to} & \text{Tr}(\sigma_{AB}^{\Pi} \left|k\right\rangle\!\left\langle k\right|_A \otimes \hat{C}_B^j) = \text{Tr}(\rho_k^{\text{out}} \hat{C}_B^j) \;\forall\; k, j \;, \\ & \text{Tr}_B(\sigma_{AB}^{\Pi}) = \rho_A \end{cases} \tag{6.34}$$

where, as above, the projection is onto $\{|m\rangle\}_{m=0}^{N}$ and the operators $\hat{C}_B^j$ are taken from the set $\{\hat{\mathbb{1}}, \hat{a}, \hat{d}\}$. In this optimization problem, we search through states in the projected subspace (for some fixed value of N), but we force the expectation values to be exactly those of the infinite-dimensional state ρ_{AB}^{out}. Whereas the results in Fig. 6.3 are a lower bound on the minimal entanglement of ρ_{AB}^{out}, the result of the hybrid optimization will necessarily be an upper bound on the minimal entanglement of ρ_{AB}^{out}. In other words, we have the relation

$$\mathcal{E}_{\min}(\rho_{AB}^{\Pi}) \leq \mathcal{E}_{\min}(\rho_{AB}^{\text{out}}) \leq \mathcal{E}_{\text{hybrid}}(\rho_{AB}^{\text{out}}). \tag{6.35}$$

In Fig. 6.4, we compare the upper bound found by this hybrid optimization (using $N = 15$) with the results shown in Fig. 6.3 by considering a section at amplitude $|\alpha| = 0.2$. We see that our result is fairly tight to the upper bound for most variance values. We also see that there is very little negativity to be found (less than 0.03) for $\text{Var}(\hat{x}) \geq 1$. The mismatch between the quantitative domain and the quantum domain again seems to be due to the combination of low entanglement and weaker constraints at high noise values. If desired, the quantitative domain could likely be extended by employing more computational resources, since this would make the constraints tighter.

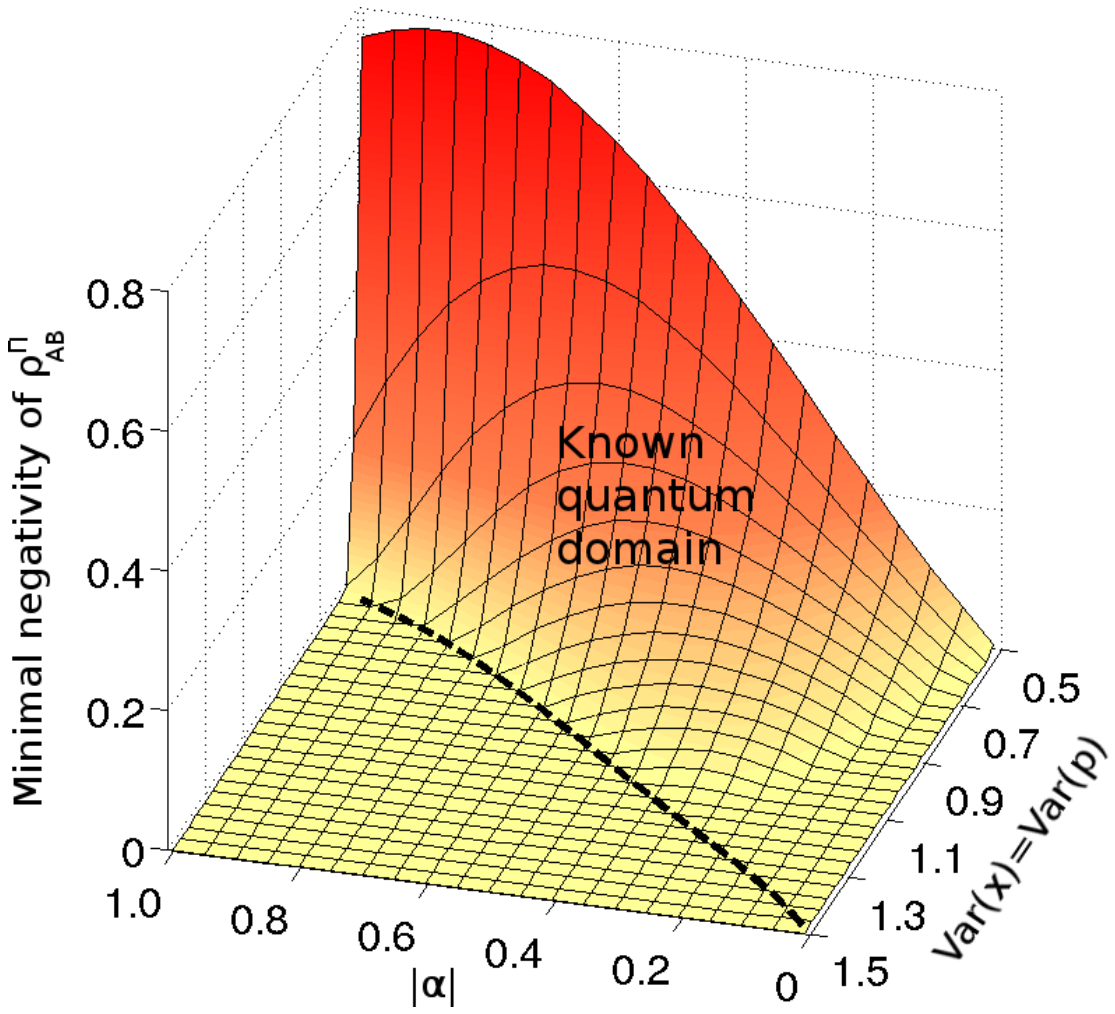


Figure 6.3: Entanglement quantification for the three coherent state benchmark, with no loss ($T = 1.0$) and cutoff $N = 15$ (cf. Fig. 4.4). Variance values below the dashed black line are known to be in the quantum domain (note again that the axes are flipped to aid visualization of the results). Unlike benchmarks using two test states, it is not known whether variances higher than the dashed line must come from separable or PPT entangled states. Although the quantitative domain is larger than the case with two coherent states, it does not cover the entire known quantum domain due to the smaller cutoff and higher energies involved.

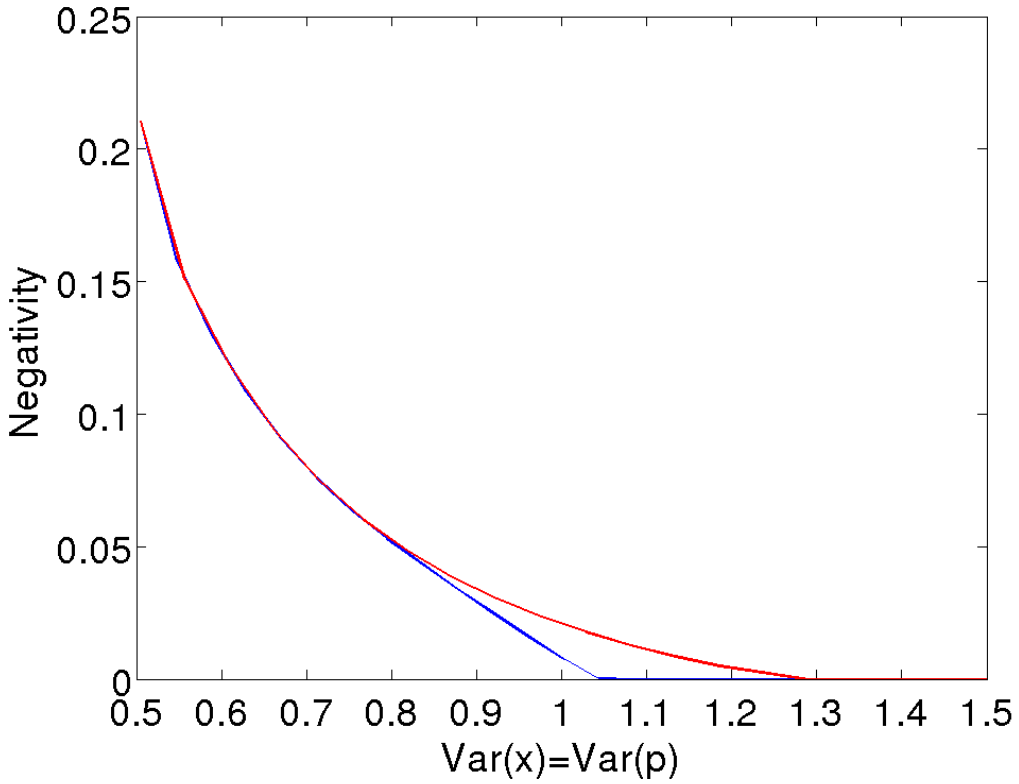


Figure 6.4: Upper and lower bounding the minimal entanglement of the infinite-dimensional benchmarking state ρ_{AB}^{out}. The lower curve is a slice through the surface in Fig. 6.3 at $|\alpha| = 0.2$ and the upper curve corresponds to results of the hybrid optimization of Eq. (6.34). We see that the minimal entanglement must be quite small after $\text{Var}(x) \approx 1$. Higher values of the cutoff N would be needed to have strong enough constraints to detect this entanglement.

Summary and outlook

In this chapter we examined a projection onto a finite subspace spanned by low-energy Fock states. Provided the chosen truncation level is large compared to the mean photon number, the projected states closely match the output states. We made this intuition rigorous by providing several bounds which relate the quadrature expectation values for the projected states and the output states. Incorporating these bounds into a semidefinite program, we calculated the minimal entanglement consistent with given data for a number of cases. For benchmarks based on two coherent states and squeezed/antisqueezed vacuum states, the quantitative domain matched very well with the qualitative domain. For three coherent states, the quantitative domain was large, but there was a noticable gap with the known quantum domain. We further studied this gap and concluded that there was very little (but non-zero) entanglement in this region, which could be captured with improved numerical capacity.

The Fock-state projection performs quite well compared to the two-qubit projection from Ch. 5, allowing us to quantify entanglement throughout much more of the quantum domain. We should note, however, that the results presented in this chapter do not supersede those from the previous chapter. Indeed, the two-qubit projection appears to be a better choice when the level of noise is small, as can be seen by comparing Figs. 5.2a and 6.1. In Fig. 5.2a the entanglement lower bounds exactly match the entanglement of the initial state when the excess noise is zero. Thus, the two-qubit approach is able to quantify all available entanglement in this case. In constrast, the corresponding entanglement lower bounds in Fig. 6.1 are numerically less than the initial entanglement. Thus, at least for the case of two coherent test states, the two approaches are complimentary.

Of course, the Fock-state projection has the additional advantage that it is more generally applicable. It can also be used to make quantitative statements in other benchmarking scenarios. As well as the presented example, this framework can be applied to essentially any finite ensemble of low-energy states. In fact, in the next chapter, we will use the Fock-state projection to help benchmark a quantum memory using multiple mixed test states, which represents the most general scenario.

Chapter 7

Benchmarking with realistic states

In this chapter, we extend the framework of entanglement-based benchmarking to allow arbitrary test states. The material in this chapter, as well as the accompanying App. D, is based largely on an unpublished manuscript, for which I am the primary author and researcher. I intend to submit this manuscript to the journal *Physical Review A*. If published, the article will be copyright 2012 by the American Physical Society. Portions of the manuscript have been adapted for this thesis.

So far, we have developed several tests and tools for verifying the quantum nature of imperfect devices. Now, if we recognize that our quantum communication devices are imperfect, we must also recognize that our state preparations may be imperfect as well. Excess noise or other flaws in the preparation procedure can cause the prepared test states to be different from the theoretical test states. This leads to discrepencies between the idealized benchmarking situation and the experimental realization. Recall from Sec. 4.1.1 that most CV benchmarks assume that the test states are pure and/or Gaussian, since such states are much more amenable to theoretical analysis than more general states of light. Using state tomography or some other process to obtain numerical descriptions of the prepared states, we may find that these states are not consistent with the ideal form (e.g., not pure or not Gaussian). In this case, is it valid to apply benchmarks which assume the ideal form? Addressing such discrepencies between theory and experiment is essential for a quantum benchmark to be meaningful.

In this chapter, we show how to extend existing quantum benchmarking methods to accommodate arbitrary states, not just states with a special form. Ref. [36] already outlines entanglement-based benchmarks for arbitrary numbers of pure states, which formed the starting point for the quantitative extensions of Chs. 4-6 in this thesis. The first attempt to generalize entanglement-based benchmarks to mixed states was taken in [35], but this was restricted to the special case of only two mixed test states. We also note that, although the chosen examples in both [36] and [35] all consist of Gaussian states, this form is not at all necessary. Hence, what remains is to generalize these previous results to the case of more than two mixed states, which would allow us to derive quantum benchmarks for arbitrary finite ensembles of test states.

The remainder of this chapter is laid out as follows. First, we outline how to generalize entanglement-based benchmarks to any number of mixed test states. We recognize that there is some inherent freedom allowed in this extension, and we study how to strengthen benchmarks to give the largest quantum domain, i.e., the best chance of certifying imperfect quantum devices. We briefly show how this idea also applies to fidelity-based benchmarks. As an application, we consider phase symmetric test ensembles, and derive a simple standard form. Finally, our general benchmarking scheme is used to certify an actual implementation of a CV quantum memory.

7.1 Benchmarking framework for arbitrary states

Experimentally, the benchmarking protocol follows the exact same lines as in previous chapters, except that the test states $\{\rho_k^{\text{in}}\}_{k=0}^{M-1}$ may now be mixed. The device acts on these mixed test states and outputs states ρ_k^{out} on subsystem B, which Bob measures. Along with a suitable Gram matrix ρ_A, this is the only information available to determine the entanglement of the output state ρ_{AB}^{out}. As we will see shortly, the theoretical treatment of the benchmarking procedure is somewhat different than before, though the goal remains the same. We still aim to rule out adversarial MP devices which attempt to mimic true quantum channels.

7.1.1 Entanglement-based benchmarking with arbitrary states

How can the virtual entangled state in Eq. (4.4) be extended to the case where the test states $\{\rho_k^{\text{in}}\}_{k=0}^{M-1}$ are mixed? Some progress was made in this direction in [35], restricting to the case of only two test states. Among several potential ways to generalize Eq. (4.4), it was found that using purifications of the test states was the most useful. In this framework, we imagine that instead of preparing the test states, we prepare purifications $\{|\Gamma_k\rangle_{A'A''}\}_{k=0}^{M-1}$, where A'' is some purifying system, i.e.,

$$\text{Tr}_{A''}(|\Gamma_k\rangle\langle\Gamma_k|_{A'A''}) = \rho_k^{\text{in}}. \tag{7.1}$$

From now on, $|\Gamma_k\rangle$ will always refer to a purification of ρ_k^{in}.

By offering the purifications instead of the actual test states, we give extra power to an adversarial MP device, since the purifications may be more easily distinguished than the test states. Although this modification may result in a slightly smaller quantum domain, any benchmarks based on the purifications are valid. Ref. [35] offers one method to reduce the impact of this relaxation, but this introduces additional numerical complexity, and we will not consider it in this thesis. However, there remains some additional freedom in the protocol, namely the choice of purifications. When choosing purifications, we should aim to make the task of an adversarial device as hard as possible. We must develop this basic intuition further in order to strengthen mixed-state benchmark schemes using purifications.

To clarify, the experimental procedure (using the test states $\{\rho_k^{\text{in}}\}$) remains the same. Theoretically, the benchmarking procedure is analyzed as if the purifications $\{|\Gamma_k\rangle_{A'A''}\}$ were used instead, i.e., the device is allowed to act on the larger system $A'A''$. Measurements are still restricted to the B subsystem, and the only information we retain about the purifications are the overlaps $\langle\Gamma_k|\Gamma_l\rangle$.

For two mixed test states ρ_0^{in} and ρ_1^{in}, the virtual entangled state takes the form

$$|\Psi\rangle_{AA'A''} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |\Gamma_0\rangle_{A'A''} + |1\rangle_A \otimes |\Gamma_1\rangle_{A'A''} \Big). \tag{7.2}$$

Purifications are not unique, but we must fix some choice to proceed further. Since we only retain information about the overlap $\langle\Gamma_0|\Gamma_1\rangle$, it is important to know the range of allowed values for this parameter. From Def. 2.4.3 and Thm. 2.4.4, we have

$$\max_{|\Gamma_0\rangle,|\Gamma_1\rangle} |\langle\Gamma_0|\Gamma_1\rangle|^2 = F(\rho_0^{\text{in}}, \rho_1^{\text{in}}) = \left[\text{Tr}\sqrt{\sqrt{\rho_0^{\text{in}}}\rho_1^{\text{in}}\sqrt{\rho_0^{\text{in}}}}\right]^2, \tag{7.3}$$

where $F(\rho_0^{\text{in}}, \rho_1^{\text{in}})$ is the fidelity between the two test states. In [35], it was argued that the best benchmarks (i.e., those which give the best opportunity to certify devices in the quantum domain) come from purifications which saturate the fidelity bound. There was some numerical support for this claim, but one can also appeal to the fact that the fidelity is a measure of (in)distinguishability. Accordingly, choosing purifications which are as indistinguishable as possible will make it harder for a MP channel to simulate a quantum channel reliably.

It is straightforward to generalize the entangled state in Eq. (7.2) to accomodate $M > 2$ mixed states. Specifically, we will use

$$|\Psi\rangle_{AA'A''} = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle_A \otimes |\Gamma_k\rangle_{A'A''}\,. \tag{7.4}$$

The reduced density matrix $\rho_A = \text{Tr}_{A'A''}\,|\Psi\rangle\langle\Psi|_{AA'A''}$ is now (aside from the prefactor) the Gram matrix of the purifications $\{|\Gamma_k\rangle\}_{k=0}^{M-1}$:

$$\langle k|\,\rho_A\,|l\rangle = \frac{1}{M}\,\langle\Gamma_l|\Gamma_k\rangle\,. \tag{7.5}$$

It is *not* straightforward how to choose purifications in this case. The fidelity is a useful measure for two states, but there is no clear extension of the concept for multiple states. Indeed, the set of allowed values for the overlaps $\langle\Gamma_k|\Gamma_l\rangle$ has a more subtle structure than just a product of the ranges allowed by Eq. (7.3). It may not be possible to choose purifications which achieve the fidelity bound for all pairs. In order to determine the best choice of purifications, we will examine the structure of entanglement-based benchmarking at a deeper level.

7.1.2 Optimizing the purifications

How can we choose purifications to optimize the strength of entanglement-based benchmarks based on multiple mixed test states? To begin answering this, we make the following observation.

Proposition 7.1.1 (Strengthening benchmarks using CPTP maps)**.** *Let* $\{|\Gamma_k\rangle\}_{k=0}^{M-1}$ *and* $\{|\Delta_k\rangle\}_{k=0}^{M-1}$ *be two different sets of purifications of the test states* $\{\rho_k^{\text{in}}\}_{k=0}^{M-1}$*. Assume that there is a completely positive, trace-preserving (CPTP) map which transforms one set of purifications to the other, i.e., there exists* Ω *such that*

$$\Omega[|\Gamma_k\rangle\langle\Gamma_k|] = |\Delta_k\rangle\langle\Delta_k| \tag{7.6}$$

for all k*. If we cannot conclude that a device is in the quantum domain with information based on the* $\{|\Delta_k\rangle\}$*, then we cannot conclude that the same device is in the quantum domain using information about the* $\{|\Gamma_k\rangle\}$*.*

Proof. Represent the device under investigation by the map Λ. This map takes in states on the joint $A'A''$ system and outputs states on the B system. We proceed in two steps. First, we assume that we can perform tomographically complete measurements on the output states. Later we will relax this to incomplete measurements. In either case, we work under the constraint that, for all k,

$$\Lambda[|\Delta_k\rangle\langle\Delta_k|] = \Lambda[|\Gamma_k\rangle\langle\Gamma_k|] = \rho_k^{\text{out}}, \tag{7.7}$$

where ρ_k^{out} is the output state corresponding to the test state ρ_k^{in}. This constraint is experimentally enforced, since the output states are independent of the purification we use to theoretically describe the protocol. Consider the case where we describe the test states using the purifications $\{|\Delta_k\rangle\}$. A benchmarking protocol is unsuccessful when we cannot discriminate between the device and a MP channel, i.e., when there is a MP channel which gives the same output states as the device. Assume then that there exists an MP channel $\tilde{\Lambda}_{MP}$ such that

$$\tilde{\Lambda}_{MP}[|\Delta_k\rangle\langle\Delta_k|] = \rho_k^{\text{out}} \tag{7.8}$$

for all k. Now consider the alternate situation where we use the purifications $\{|\Gamma_k\rangle\}$, and there exists a CPTP map Ω as in Eq. (7.6). We define another channel Σ_{MP} by

$$\Sigma_{MP} := \tilde{\Lambda}_{MP} \circ \Omega. \tag{7.9}$$

The concatenation of any channel with a MP channel is as a MP channel, so Σ_{MP} is in the MP class. From Eqs. (7.6)-(7.8), we must have

$$\Sigma_{MP}[|\Gamma_k\rangle\langle\Gamma_k|] = \rho_k^{\text{out}} \tag{7.10}$$

for all k. Therefore, there exists a MP channel which gives the observed output states when using the purifications $\{|\Gamma_k\rangle\}$.

Even when we do not have enough measurements for complete tomography, we can follow simular arguments. Instead of having one output state ρ_k^{out} for every k, we have a set of states $\mathcal{C}[\rho_k^{\text{out}}]$, all of which have the same expectation values with respect to the employed measurement operators $\{\hat{O}_B^j\}$:

$$\mathcal{C}[\rho_k^{\text{out}}] := \left\{\tau \in \mathcal{B}(\mathcal{H}_B) \;\middle|\; \text{Tr}(\tau\hat{O}_B^j) = \langle\hat{O}_B^j\rangle_{\text{meas}} \;\forall\; j\right\}. \tag{7.11}$$

In this case, a benchmarking protocol is unsuccessful when there is a MP channel $\tilde{\Lambda}_{MP}$ such that

$$\tilde{\Lambda}_{MP}[|\Delta_k\rangle\langle\Delta_k|] \in \mathcal{C}[\rho_k^{\text{out}}] \tag{7.12}$$

for all k. Using this channel, we again define a MP channel Σ_{MP} as in Eq. (7.9). By Eqs. (7.6) and (7.12), we conclude

$$\Sigma_{MP}[|\Gamma_k\rangle\langle\Gamma_k|] \in \mathcal{C}[\rho_k^{\text{out}}]. \tag{7.13}$$

In either case, if benchmarking is unsuccessful for the $\{|\Delta_k\rangle\}$, it cannot be successful for the $\{|\Gamma_k\rangle\}$.

□

This proposition has some important consequences. For one, it tells us that in the source-replacement scheme we are using, the quantity of entanglement does not have a direct bearing[1]. Instead, the focus should be to find those purifications which cannot be collectively transformed, via CPTP maps, to any other valid set. Benchmarking schemes built with such purifications provide the hardest challenge for an adversarial MP device attempting to mimic a true quantum device. Indeed, such limiting purifications necessarily lead to a larger quantum domain than any other comparable choice. Because we only use

[1]For example, when the entangled state in Eq. (7.4) has maximal entanglement, the purifications must be orthogonal, $\langle\Gamma_k|\Gamma_l\rangle = \delta_{kl}$. But orthogonal purifications can be perfectly distinguished and reproduced by a particular MP channel, giving the same output as a perfect quantum memory. Thus, no benchmarking protocol will be successful in ruling out MP channels when Eq. (7.4) is maximally entangled.

the overlaps for benchmarking, we can optimize the CPTP map condition on the level of Gram matrices. In the rest of this chapter, we will use the terms 'purifications' and 'Gram matrix (of the purifications)' somewhat interchangeably.

The following theorem will help us translate the CPTP map condition to a more amenable form.

Theorem 7.1.2 (Allowed Gram matrix transformations [97, 18, 19])**.** *Let* $\{|\gamma_k\rangle\}_{k=0}^{M-1}$ *and* $\{|\delta_k\rangle\}_{k=0}^{M-1}$ *be two sets of pure states. Let* G *and* D *be the corresponding Gram matrices, with elements* $G_{ij} := \langle\gamma_j|\gamma_i\rangle$ *and* $D_{ij} := \langle\delta_j|\delta_i\rangle$*. There exists a CPTP map* Ω *taking the former states to the latter if and only if the Gram matrices are related by*

$$G = P \circ D, \tag{7.14}$$

where $\circ$ *denotes the Hadamard (or Schur or entrywise) product. The matrix* P *satisfies* $P \geq 0$ *and its diagonal elements are given by* $\mathrm{diag}(P) = \{1, 1, 1, \dots\}$.

To avoid potential confusion, we point out that while the CPTP map Ω takes the $\{|\gamma_k\rangle\}$ to the $\{|\delta_k\rangle\}$, the Gram matrix condition, Eq. (7.14), has the opposite sense, i.e., G is obtained by doing a particular operation on D. Since some of the matrix elements of P could be zero, we cannot invert the equation to give D as a function of G, so we leave the relation in this form. We also point out a corollary to this theorem: all compatible purifications of the test states $\{\rho_k^{\text{in}}\}$ can be prepared by applying a CPTP map to a set of purifications which are orthogonal. Therefore, orthogonal purifications can be seen as generators for the rest of the set of purifications. Of course, we are interested in the other end of this generation, i.e., the limiting sets of purifications.

Finding candidate purifications

Given some ensemble of test states, it may be quite difficult to determine the best purifications analytically, especially for arbitrary test states. Alternatively, we can attempt to find limiting purifications by maximizing some objective function f, defined on ensembles of pure states (or on the corresponding Gram matrix), which preserves the order structure induced by CPTP maps. In other words, if there exists a CPTP map Ω taking the pure states $\{|\gamma_k\rangle\}_{k=0}^{M-1}$ to the pure states $\{|\delta_k\rangle\}_{k=0}^{M-1}$, the desired function must satisfy

$$f(\{|\gamma_k\rangle\}) \leq f(\{|\delta_k\rangle\}). \tag{7.15}$$

When this property holds, the purifications which are limiting in the sense of CPTP maps will maximize the objective function f. Before discussing candidates for the objective

function, we point out one caveat. Namely, the order structure imposed on the purifications by CPTP maps is not a total order. Accordingly, purifications which are not linked by a CPTP map are not comparable. Nevertheless, we can design quantum benchmarking schemes with any feasible set of purifications, and this heuristic provides a way to obtain the best choice out of all comparable purifications.

A good candidate for the objective function is the purity of the reduced density matrix ρ_A (recall from Eq. (7.5) that ρ_A is essentially the Gram matrix of the chosen purifications).

Definition 7.1.3 (Gram matrix purity)**.** *Let $\{|\Gamma_k\rangle\}_{k=0}^{M-1}$ be a set of purifications of the test states $\{\rho_k^{\text{in}}\}_{k=0}^{M-1}$, with Gram matrix $G_{ij} = \langle\Gamma_j|\Gamma_i\rangle$ and let $\rho_A = \frac{1}{M}G$. We define the* Gram matrix purity *as*

$$\begin{aligned}\mathcal{P} = \operatorname{Tr}(\rho_A^2) =& \sum_{k=0}^{M-1}\sum_{l=0}^{M-1} \left|[\rho_A]_{kl}\right|^2 \\ =& \frac{1}{M^2}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1} \left|\langle\Gamma_k|\Gamma_l\rangle\right|^2 . \end{aligned} \tag{7.16}$$

From Thm. 7.1.2, when there is a CPTP map taking $\{|\Gamma_k\rangle\} \to \{|\Delta_k\rangle\}$, we must have

$$\langle\Gamma_k|\Gamma_l\rangle = P_{kl}\,\langle\Delta_k|\Delta_l\rangle\,, \tag{7.17}$$

with $|P_{kl}| \leq 1$. Therefore the Gram matrix purity is monotonic with respect to CPTP maps, as required.

The Gram matrix purity also has links to the distinguishability of the test states. For example, when working with only two test states ρ_0^{in} and ρ_1^{in}, the maximal value of $\mathcal{P}$ is

$$\begin{aligned}\max\mathcal{P} =& \frac{1}{4}\left(2 + 2\max_{|\Gamma_0\rangle,|\Gamma_1\rangle} \left|\langle\Gamma_0|\Gamma_1\rangle\right|^2\right) \\ =& \frac{1}{2}\left(1 + F(\rho_0^{\text{in}}, \rho_1^{\text{in}})\right). \end{aligned} \tag{7.18}$$

Aside from a fixed affine transformation, the Gram matrix purity is the fidelity between the test states. For $M > 2$, the Gram matrix purity defines a kind of averaged multi-state analog of the fidelity (where the maximization has a more subtle form). Finally, consider the state

$$\rho_{A'A''} = \frac{1}{M}\sum_{k=0}^{M-1} |\Gamma_k\rangle\langle\Gamma_k|_{A'A''}\,. \tag{7.19}$$

Since a device has no information about which test state was prepared, this is the effective state input to the device in the purification picture. But since the virtual entangled state in Eq. (7.4) is pure, the spectra of the reduced states are equal, i.e., $\text{spec}(\rho_A) = \text{spec}(\rho_{A'A''})$. Therefore, when ρ_A is of high purity, then so is the effective test state $\rho_{A'A''}$. Provided the test states are non-orthogonal, a measure and prepare channel will introduce some unavoidable disturbance on $\rho_{A'A''}$. Intuitively, by making the effective test state $\rho_{A'A''}$ as pure as possible, we can magnify the observable effects of any disturbance.

One drawback of the Gram matrix purity is that it will be difficult to compute the maximum for $M > 2$, where we do not currently have an analytic formula like Eq. (7.3). Alternatively, since the objective function in Eq. (7.16) is convex and the set of compatible Gram matrices is convex (see App. D.1), we could maximize this function numerically using the methods of convex optimization. Although this presents one path towards our goal, we will not pursue it here. Instead, the Gram matrix purity helps us motivate a slightly different objective function which is easier to optimize numerically.

Definition 7.1.4 (Alternate objective function)**.** *Abbreviate the overlaps by* $Z_{kl} := \langle \Gamma_k | \Gamma_l \rangle$ *and decompose them into real and imaginary parts,* $Z_{kl} = X_{kl} + iY_{kl}$*. The alternate objective function is given by*

$$h(\{|\Gamma_j\rangle\}) := \sum_{k=l+1}^{M-1} \sum_{l=0}^{M-1} (X_{kl} + Y_{kl}) \,. \tag{7.20}$$

Aside from a prefactor and duplicated terms, the main difference between h and the Gram matrix purity $\mathcal{P}$ is that the squared modulus of the overlaps is replaced by a sum of the real and imaginary parts. The advantage of this objective function is that it is linear in the parameters X_{kl} and Y_{kl}, allowing us to numerically optimize it using a semidefinite program. In cases where the the imaginary parts Y_{kl} vanish, then $X_{kl} + Y_{kl}$ is a lower bound to the modulus $|Z_{kl}|$. As well, when the objective function h is large, the Gram matrix purity will also be large, meaning we are close to a limiting Gram matrix. The main drawback of this objective function is that it is not monotonic. Nevertheless, we remind the reader that any Gram matrix found by optimizing h is valid for benchmarking purposes. Indeed, we will see in Sec. 7.2 that, despite being non-monotonic, this function leads to a Gram matrix with near-optimal purity.

Before moving on, we pause to summarize the main results of this section. Given some arbitrary ensemble of test states $\{\rho_k^{\text{in}}\}_{k=0}^{M-1}$, we consider a virtual entangled state as in Eq. (7.4), where the states $\{|\Gamma_k\rangle_{A'A''}\}_{k=0}^{M-1}$ are purifications of the test states. Although the test states are used in practice, we benchmark a device by assuming that the device has access to the purifications. This procedure may slightly weaken the benchmarking,

but there is also some flexibility in the choice of purifications, which can be used to best restrict the effects of this relaxation. We showed that purifications which are extremal in the sense of CPTP maps are better for benchmarking than all other comparable choices, so we should aim to build benchmarks using such purifications. We suggest finding good candidate purifications by optimizing some appropriate function which is monotonic with respect to CPTP maps. We propose the Gram matrix purity $\mathcal{P}$ as a suitable candidate for this objective function, although it may be difficult to compute. We also propose a numerically simpler, though non-monotonic, objective function which may be used in place of the Gram matrix purity.

7.1.3 Fidelity-based benchmarking with arbitrary states

At this point we make a short digression to show how the above ideas can be applied to fidelity-based benchmarks. Although we are mainly interested in using entanglement to benchmark CV quantum devices, fidelity-based benchmarks still have some utility, particularly for discrete systems (e.g., the RSP protocol of Ch. 3). In fact, Ref. [36] demonstrated a link between the fidelity-based approach and the entanglement-based approach by showing that they could give the same quantum domain (although the entanglement-based approach required far less resources).

In order to study this connection, we first give a convenient formulation of the (root) fidelity as a semidefinite program.

Theorem 7.1.5 (Fidelity as SDP)**.** *Let τ_0, $\tau_1 \in \mathcal{B}(\mathcal{H}_B)$ be two arbitrary density matrices. Then the root fidelity of these two density matrices is given by the solution to the following optimization:*

$$\sqrt{F}(\tau_0, \tau_1) = \begin{cases} \max\limits_{X \in \mathcal{B}(\mathcal{H}_B)} & \operatorname{Tr}\left(\frac{X+X^\dagger}{2}\right) \\ \text{subject to} & \begin{bmatrix} \tau_0 & X \\ X^\dagger & \tau_1 \end{bmatrix} \geq 0 \end{cases}. \tag{7.21}$$

Proof. Normalizing the constraint matrix and using $\{|0\rangle_A, |1\rangle_A\}$ as orthonormal vectors on some indexing space $\mathcal{H}_A$, we define

$$\begin{aligned} \phi_{AB} := \frac{1}{2}[& |0\rangle\langle 0|_A \otimes \tau_0 + |0\rangle\langle 1|_A \otimes X \\ & + |1\rangle\langle 0|_A \otimes X^\dagger + |1\rangle\langle 1|_A \otimes \tau_1]. \end{aligned} \tag{7.22}$$

Since ϕ_{AB} is normalized and $\phi_{AB} \geq 0$ must hold, then ϕ_{AB} is a valid density matrix. Thus, we can consider its purification $|\Phi\rangle_{ABC}$ (with $\mathrm{Tr}_C |\Phi\rangle\langle\Phi|_{ABC} = \phi_{AB}$), where the Hilbert space on C is a copy of $\mathcal{H}_A \otimes \mathcal{H}_B$. Without loss of generality, we can write

$$|\Phi\rangle_{ABC} = \frac{1}{\sqrt{2}} \left[|0\rangle_A \otimes |\Omega_0\rangle_{BC} + |1\rangle_A \otimes |\Omega_1\rangle_{BC} \right]. \tag{7.23}$$

From this, we deduce that $|\Omega_0\rangle_{BC}$ and $|\Omega_1\rangle_{BC}$ must be normalized purifications of τ_0 and τ_1, respectively. But this also means that

$$X = \mathrm{Tr}_C \left(|\Omega_0\rangle\langle\Omega_1|_{BC} \right), \tag{7.24}$$

so the objective function in the SDP is

$$\mathrm{Tr} \left(\frac{X + X^\dagger}{2} \right) = \mathrm{Re}[\langle\Omega_0|\Omega_1\rangle]. \tag{7.25}$$

Without loss of generality, we can take $\mathrm{Tr}X$ to be real and positive, so the right hand side of Eq. (7.25) is equal to $|\langle\Omega_0|\Omega_1\rangle|$. Comparing to Eq. (2.5), we conclude that the solution of the above SDP is the root fidelity $\sqrt{F}(\tau_0, \tau_1)$.

□

Not only does Eq. (7.21) provide another method to calculate the fidelity, but it can also be used to compute the maximum fidelity between two states which are not fully known, since SDPs allow for free parameters.

Now, we imagine the situation where we know the test states $\{\rho_k^{\mathrm{in}}\}$. Since channels are linear, we can parameterize the corresponding output states $\{\rho_k^{\mathrm{out}} | \rho_k^{\mathrm{out}} = \Lambda[\rho_k^{\mathrm{in}}]\}$ as linear transformations of the test states. Using the Choi-Jamiolkowski isomorphism [50, 20], complete positivity of the channel can be encoded as a positive semidefinite constraint. In a similar manner, the trace preservation property can be realized as a linear constraint on the channel (see e.g., [7]). Combining these constraints with Thm. 7.1.5, we can optimize the average root fidelity $\overline{\sqrt{F}} = \sum_k p_k \sqrt{F}(\rho_k^{\mathrm{in}}, \rho_k^{\mathrm{out}})$ over arbitrary channels using a semidefinite program.

Although the root fidelity is slightly different than the fidelity, it is also valid to use it as the figure of merit for fidelity-based benchmarking, since MP channels will still have an optimal value less than unity for suitable test ensembles. If we could further enforce that Λ corresponds to a MP channel, then we could use the above formulation to calculate the maximum root fidelity achievable by such channels, forming the benchmark threshold. Unfortunately, it is not known how to efficiently encode this property, since it is

equivalent to deciding if a given state is separabile, a known hard problem [31]. However, we can instead use the weaker requirement that the channel breaks NPT entanglement [77]. Because the set of PPT states contains the set of separable states, the class of NPT-entanglement-breaking channels (i.e., channels such that $(\mathrm{id}\otimes\Lambda)[\rho]$ is PPT $\forall\ \rho$) necessarily contains all MP channels as a subset. Thus, the maximum average root fidelity over NPT-entanglement-breaking channels will be higher than the maximum over MP channels,

$$\overline{\sqrt{F}}^{\max}_{NPTB} \geq \overline{\sqrt{F}}^{\max}_{MP}. \tag{7.26}$$

This provides a sufficient (but not necessary) benchmark: any device that can achieve higher root fidelity than $\overline{\sqrt{F}}^{\max}_{NPTB}$ is in the quantum domain. The new benchmark value, although weaker, can be more efficiently determined, since PPT conditions can be checked within a semidefinite program.

Examples of fidelity-based benchmarking

To exemplify the above ideas, we consider M pure test states $\{|\psi_k\rangle\}$ on the Bloch sphere, each having the same polar angle $\theta_k = \theta \in [0, 2\pi]$ but symmetrically-distributed azimuthal angles $\varphi_k = \frac{2\pi k}{M}$ (cf. Eq. (2.17)). We assume equal probability of using each test state, $p_k = \frac{1}{M}$. These symmetry conditions are used only to simplify the results and are not necessary to calculate benchmarks.

To consider NPT-entanglement-breaking channels, we need to introduce entanglement somewhere. To do this, we follow the familiar recipe of Eq. (4.4), which provides some initial entangled state $\rho^{\mathrm{in}}_{AA'} = |\Psi^{\mathrm{ent}}\rangle\langle\Psi^{\mathrm{ent}}|_{AA'}$. A device (represented by Λ) acts on the A' subsystem, mapping to some output subsystem B. The output state $\rho^{\mathrm{out}}_{AB} = (\mathrm{id}\otimes\Lambda)\,|\Psi^{\mathrm{ent}}\rangle\langle\Psi^{\mathrm{ent}}|_{AA'}$ takes the usual form of Eq. (4.9). The diagonal blocks ρ^{out}_{kk} of the output state are connected to the test states ρ^{in}_k by some fixed linear and positive-semidefinite constraints, due to the NPT-entanglement-breaking map Λ. Finally, the standard Gram matrix condition $\mathrm{Tr}_B(\rho^{\mathrm{out}}_{AB}) = \mathrm{Tr}_{A'}(\rho^{\mathrm{in}}_{AA'}) = \rho_A$ is enforced.

Using the above constraints and the variational formula of Eq. (7.21), we can compute the benchmark value $\overline{\sqrt{F}}^{\max}_{NPTB}$ for the given test states with a SDP. Results for this investigation are shown in Fig. 7.1 for $M = 2, 3$ test states and varying polar angle θ. We can also study the effect of Gram matrix purity on fidelity benchmarks by replacing the true Gram matrix by some modified version. As an example, consider the case of $M = 2$ pure states. The true Gram matrix is

$$\rho_A = \frac{1}{2}\begin{bmatrix} 1 & \langle\psi_1|\psi_0\rangle \\ \langle\psi_0|\psi_1\rangle & 1 \end{bmatrix}. \tag{7.27}$$

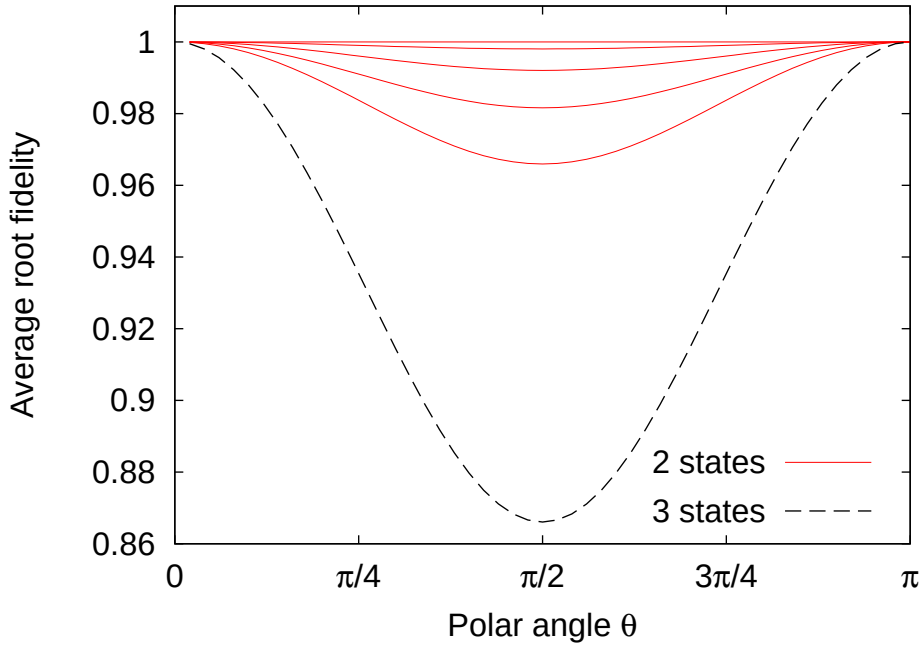


Figure 7.1: Example fidelity-based benchmark thresholds $\overline{\sqrt{F}}_{NPT}^{\max}$ for the given qubit states. Solid curves: 2 states, dashed curve: 3 states. Data above the curves cannot come from NPT-entanglement-breaking channels. The various solid curves represent the thresholds for different Gram matrix purities. From top to bottom, these correspond to the parameter values $b = 0.0,\ 0.25,\ 0.5,\ 0.75$, and 1.0 in Eq. (7.28).

We replace this by a modified version

$$\widetilde{\rho_A} := \begin{bmatrix} 1 & b\,\langle\psi_1|\psi_0\rangle \\ b^*\,\langle\psi_0|\psi_1\rangle & 1 \end{bmatrix}. \tag{7.28}$$

We take $|b| \leq 1$, so that the purity of $\widetilde{\rho_A}$ is upper bounded by the purity of ρ_A. The results of the root fidelity optimization, for different values of b, are also included in Fig. 7.1. It is clear that the purer the Gram matrix, the larger the quantum domain, as expected based on the previous section. We could also have used mixed states, and the different Gram matrices would represent different choices of purifications.

For two pure test states, we can compare these benchmarks to the known results of [26, 73], which were labourously derived analytically. Now, the analytic results are for the optimal average fidelity $\overline{F}_{MP}^{\max}$, whereas we have the quantity $\overline{\sqrt{F}}_{NPTB}^{\max}$. Fortunately, the set of PPT states and the set of separable states are the same for the case of two qubits

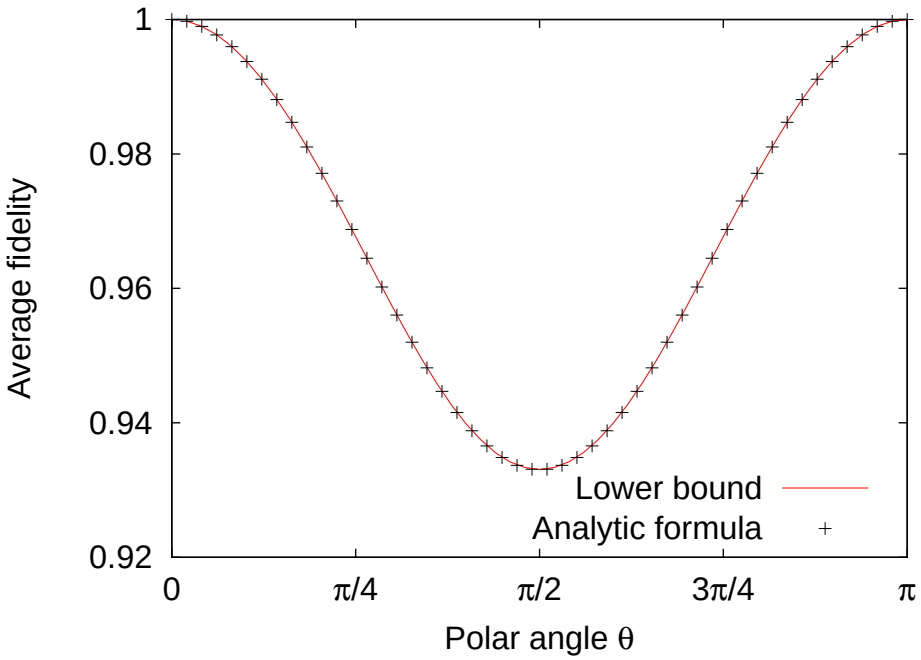


Figure 7.2: Comparison between fidelity benchmarks obtained by optimization and analytically. Points above the analytical threshold are in the quantum domain. The lower bound, obtained using the results of the root fidelity optimization, is tight with the analytically-derived optimal fidelity.

[41], which is the situation here. Thus, the set of NPT-entanglement-breaking channels is equivalent to the set of MP channels, giving

$$\overline{F}^{\max}_{NPTB} = \overline{F}^{\max}_{MP}. \tag{7.29}$$

To handle the square root, we can take the root fidelities $f_k^{\text{opt.}} := \sqrt{F}(\rho_k^{\text{in}}, \rho_k^{\text{out}})|_{\text{opt.}}$ found from our SDP optimization and substitute their squares into the average fidelity formula. The result, representing a particular achievable fidelity value over NPT-entanglement-breaking channels, forms a lower bound to $\overline{F}^{\max}_{NPTB}$. To summarize, by squaring and averaging the root fidelity terms found in our optimization, we can get a lower bound on the analytic bound, i.e.,

$$\frac{1}{2}\sum_{k=0,1}(f_k^{\text{opt.}})^2 \leq \overline{F}^{\max}_{MP}. \tag{7.30}$$

The analytic result and the lower bound calculated using the results of the optimization are shown in Fig. 7.2. We see that the two results are in agreement. Thus, the root fidelity

terms obtained via our optimization are just the square roots of the optimal fidelity terms for MP channels. A similar correspondence between separable and PPT states holds for systems of dimension 2×3, so we suspect that the root fidelity thresholds for three single-qubit test states also correspond to the optimal MP values.

Although we have not studied the topic too deeply, it is possible to find a common framework for fidelity-based and entanglement-based benchmarks. By using the variational formula of Eq. (7.21), we can compute fidelity-based benchmarks using semidefinite programming. Although the benchmarks computed this way agree with known analytic results for very low dimensions, they are likely weaker in general. Nevertheless, this technique provides a quick method to get useful benchmarks for finite-dimensional systems.

7.1.4 Benchmarking with phase-symmetric ensembles

Another useful application for the earlier ideas of this chapter is in testing devices which are phase covariant. A device (represented by Λ) is phase covariant when it commutes with unitary rotations of phase space, i.e.,

$$\Lambda[U_\phi \sigma U_\phi^\dagger] = U_\phi \Lambda[\sigma] U_\phi^\dagger \; \forall \; \sigma. \tag{7.31}$$

The rotation unitary is given by $U_\phi = \exp(-i\phi\hat{n})$, with $\hat{n}$ the standard number operator, so $U_\phi^\dagger = U_{-\phi}$. We note that any channel can be made phase covariant by phase-randomization,

$$\Lambda_C[\ \cdot\ ] = \frac{1}{2\pi} \int_0^{2\pi} U_\phi \Lambda[U_{-\phi}(\ \cdot\ ) U_{-\phi}^\dagger] U_\phi^\dagger \mathrm{d}\phi. \tag{7.32}$$

One way to accomplish this phase randomization is to use a drifting optical phase [36], a situation which is common in many continuous-variable setups. If a phase-randomized channel passes a quantum benchmark, then the channel itself must be in the quantum domain as well. On the other hand, phase-randomization may weaken a channel's ability to beat a benchmark, since it involves concatenation with other channels.

Phase-covariant channels offer a number of advantages. On the experimental side, they can be benchmarked using only one physical test state. The effects of a phase-covariant channel on many other test states can be inferred by symmetry. On the other hand, phase covariance can lead to great numerical simplifications. If the test states are unrelated, the number of free parameters in the density matrix ρ_{AB}^{out} scales quadratically with the number of states M. When phase symmetry conditions are imposed, we will show that the number of free parameters can be made to scale only linearly with M. This gives us more

computational room to push up the number of states M in the test ensemble, leading to stronger benchmarks.

To benchmark a phase-covariant channel, we consider test states from the rotationally-symmetric ensemble

$$\{\rho_k^{\text{in}} | \rho_k^{\text{in}} = U_\theta^k \rho_0^{\text{in}} U_\theta^{\dagger k}\}_{k=0}^{M-1}, \tag{7.33}$$

where $\theta = \frac{2\pi}{M}$. For phase-covariant devices, we have

$$\Lambda[\rho_k^{\text{in}}] = U_\theta^k \Lambda[\rho_0^{\text{in}}] U_\theta^{\dagger k}, \tag{7.34}$$

so we can infer the channel's effect on ρ_k^{in} by suitable rotations of its action on one real test state ρ_0^{in}. In this way we can generate multi-state benchmark data efficiently from any seed state. We will refer to the situation where both the test states are phase symmetric and the tested device is phase covariant as *phase-symmetric benchmarking*.

We will now present two standard form results relevant to phase-symmetric benchmarking. In the purification picture, the virtual entangled state takes the form $\rho_{AA'A''}^{\text{in}} = |\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'A''}$ and the corresponding output state is $\rho_{AB}^{\text{out}} = (\text{id}_A \otimes \Lambda) |\Psi^{\text{ent}}\rangle\langle\Psi^{\text{ent}}|_{AA'A''}$. The block decompositions of Eqs. (4.5) and (4.9) remain valid with the additional requirement that $\rho_{AA'}^{\text{in}} = \text{Tr}_{A''}(\rho_{AA'A''}^{\text{in}})$. For phase-symmetric states, the following relation can be imposed on the blocks of $\rho_{AA'}^{\text{in}}$:

$$U_\theta \rho_{kl}^{\text{in}} U_\theta^\dagger = \rho_{k+1,l+1}^{\text{in}} \ (\text{mod } M) \ \forall \ k, l. \tag{7.35}$$

For a phase-covariant channel, the corresponding output state blocks ρ_{kl}^{out} will have the same symmetry. Density matrices with this symmetry can be brought into a simple standard form.

Theorem 7.1.6 (Standard form)**.** *Let*

$$\tau_{AB} = \frac{1}{M} \sum_{k=0}^{M-1} \sum_{l=0}^{M-1} |k\rangle\langle l|_A \otimes \tau_{kl}, \tag{7.36}$$

be an arbitrary bipartite matrix. Let $\theta = \frac{2\pi}{M}$ and let $\omega_M = \exp(i\theta)$ denote the primitive Mth root of unity. Assume that the following symmetry relation holds:

$$U_\theta \tau_{kl} U_\theta^\dagger = \tau_{k+1,l+1} \ (\text{mod} M) \ \forall \ k, l. \tag{7.37}$$

Then τ_{AB} is unitarily equivalent to a block diagonal matrix

$$\mathcal{D}(\tau_{AB}) = \bigoplus_{k=0}^{M-1} E_k \tag{7.38}$$

where

$$E_k = \frac{1}{M} \sum_{l=0}^{M-1} \omega_M^{k \cdot l} \tau_{kl} U_\theta^l. \tag{7.39}$$

Moreover,

$$\sum_{k=0}^{M-1} E_k = \tau_{00}, \tag{7.40}$$

and τ_{AB} is positive semidefinite iff all of the E_k are positive semidefinite.

Proof. See App. D.2.

In the next section, we will quantify the entanglement of the state ρ_{AB}^{out} by computing lower bounds on the negativity (Eq. (2.8)), which involves the trace norm of the partial transpose $(\rho_{AB}^{\text{out}})^{T_A}$. For phase-symmetric benchmarking situations, we can greatly simplify this calculation.

Theorem 7.1.7 (Trace norm in standard form)**.** *Let τ_{AB} be as in Thm. 7.1.6. Then the trace norm of the partially transposed state $\tau_{AB}^{T_A}$ reduces to the form*

$$||\tau_{AB}^{T_A}||_1 = \sum_{k=0}^{M-1} ||\tilde{E}_k||_1, \tag{7.41}$$

where the $\{\tilde{E}_k\}_{k=0}^{M-1}$ are formed by rearranging the matrix elements of $\{E_k\}_{k=0}^{M-1}$ from the standard form of τ_{AB}. Specifically, the matrix elements in the Fock basis are determined via

$$[\tilde{E}_k]_{jl} = [E_{j+l-k}]_{jl} \ (\text{mod } M). \tag{7.42}$$

Proof. See App. D.3.

These two standard form results allow us to reduce the numerical complexity of phase-symmetric benchmarking. Although the available information remains unchanged (the Gram matrix ρ_A and measurements on the seed state ρ_0^{in}), the virtual benchmarking states are more compactly encoded by using the M square matrices E_k instead of the $\frac{M(M+1)}{2}$ independent blocks τ_{kl}.

7.2 Certifying a quantum memory

We now apply the above theoretical results to the task of certifying a continuous variable quantum memory[2]. This memory is based on a three-level lambda gradient echo scheme involving hyperfine spin states of warm ($\sim 80\,^{\circ}\mathrm{C}$) rubidium atoms. Its fundamental operation has been outlined in detail elsewhere [40, 44]; the data used here are based on the results reported in [44]. For the purposes of benchmarking, we will mainly omit the finer details and treat it as a black box. The one exception is to point out that the equations which model its ideal operation are *phase independent* [40]. On the level of actual test data, there is also no indication of any phase sensitivity in the memory, i.e., the observed loss and excess noise are uniform with respect to the angle in phase space. Finally, the experimental phase reference was allowed to drift freely between runs. Ideally, this drift can be used to phase randomize the device [36], i.e., to render the channel phase covariant. Unfortunately, the observed phase drift was not fast enough to ensure the uniform distribution of phase angles required in Eq. (7.32). Nevertheless, we will work under the assumption that the memory operation is phase covariant, and test the memory using a phase-symmetric ensemble generated by a single test state ρ_0^{in}.

During an experimental run, light is generated with a continuous-wave master laser. This light is split into a coupling field (for activating the memory), a strong continuous wave local oscillator, a weak signal pulse, and a memory reference pulse. The signal and memory reference pulses share the same optical phase relative to the local oscillator. Before entering the memory, the reference pulse is detuned from the active frequencies of the memory, so it passes through unaffected. The reference pulse enters the memory shortly before the signal pulse, with a temporal separation that is small compared to the timescale of experimental phase fluctuations. The reference pulse thus serves as a way to determine the phase of the signal before the memory. Both the output signal and reference pulses are interfered with the local oscillator (which has not passed through the memory) in a homodyne measurement apparatus. This process generates quadrature amplitude data for the output state ρ_0^{out}. The phase angle of the measurement is inferred through the beating pattern of the detuned reference pulse and the local oscillator. Similar data can be obtained for the input state ρ_0^{in} when the memory is inactive.

Over repeated runs, many quadrature/phase data points are collected to form a raw data set. Tomographic reconstruction was performed using an iterative maximum-likelihood algorithm [47] using data from 100,000 pulses, giving density matrices for both the input

[2] Author's declaration: I did not aid in the design of this memory, nor the gathering of experimental data, nor the tomographic reconstruction. My contributions consisted of analyzing the data (raw quadrature data and tomographically-reconstructed density matrix) for quantum benchmarking purposes

and output states in the Fock basis. A constant phase offset between the input and output signals was observed; this offset was cancelled digitally during the tomographic reconstruction. The tomographically-reconstructed density matrices were numerically truncated after the first 30 Fock states ($|0\rangle, \ldots, |29\rangle$). This cutoff is supported by the fact that both the input state and output state are essentially confined to the first 10 Fock levels, for which the cutoff error in either state is $\approx 10^{-5}$. From the tomography, the input state was found to have mean photon number $\langle \hat{n}_{\text{in}} \rangle = 0.67$ [44]. We do not categorize this state, but it qualitatively resembles a coherent state with added noise. The tomographically-reconstructed output state had a similar form, with mean photon number $\langle \hat{n}_{\text{out}} \rangle = 0.57$.

As demonstrated in earlier chapters, output state tomography is not required for successful benchmarking; measurement of two conjugate quadrature variables may be sufficient. However, having the tomographically reconstructed density matrices will allow us to study the difference in strength between the two approaches. To get the required quadrature expectation values, we collected the original data into bins containing 500 data points and restricted our attention to two bins corresponding to the quadratures $\hat{x}$ and $\hat{p}$. Taking the mean and standard deviation of the data within these bins, we get estimates of $\langle \hat{x} \rangle$, $\langle \hat{p} \rangle$, $\text{Var}(\hat{x})$, and $\text{Var}(\hat{p})$. Error bars, based on the finite sample size of the bins, are calculated using standard error propagation techniques. The final quadrature moment values are listed in Table 7.1.

Operator	First moment $\langle \cdot \rangle$	Second moment $\langle \cdot \rangle^2$
$\hat{x}$	0.01 ± 0.03	0.57 ± 0.04
$\hat{p}$	-0.95 ± 0.03	1.41 ± 0.09

Table 7.1: Experimentally-determined first and second moments for the conjugate quadratures $\hat{x}$ and $\hat{p}$.

7.2.1 Finding the Gram matrix

The test ensemble is generated by rotations of the seed state ρ_0^{in}, as in Eq. (7.33), forming a ring in phase space. Our theoretical description of the seed state comes from the tomographic reconstruction with the finite cutoff in Fock space. We make no further assumptions about the seed state other than that the tomographic description is accurate. Purifications, and the associated Gram matrix, are based on this numerical description. Due to the mixed nature of this state, previous entanglement-based benchmarks would be limited to only two test states. We will see later that two test states are not sufficient in

this case to reliably (i.e., within experimental error) certify the memory, but adding more test states enables a successful benchmarking.

In order to find candidate Gram matrices for the purifications, we convert the optimization to a semidefinite program. To this end, we consider the bipartite matrix (cf. Eq. (4.5))

$$\begin{aligned}\rho^{\text{in}}_{AA'} =& \text{Tr}_{A''}(\rho^{\text{in}}_{AA'A''}) \\ =& \frac{1}{M}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1} |k\rangle\langle l|_A \otimes \rho^{\text{in}}_{kl}. \end{aligned} \tag{7.43}$$

The diagonal blocks of $\rho^{\text{in}}_{AA'}$ are the test states, i.e., $\rho^{\text{in}}_{kk} = \rho^{\text{in}}_k$, and the off-diagonal blocks $\rho^{\text{in}}_{kl} \in \mathcal{B}(\mathcal{H}_{A'})$ consist of free parameters. The off-diagonal blocks are linked to the purifications through the relation

$$\text{Tr}(\rho^{\text{in}}_{kl}) = \langle k|\, \rho_A\, |l\rangle = \frac{1}{M}\langle \Gamma_l|\Gamma_k\rangle\,. \tag{7.44}$$

We have traced out the purifying system A'' since no measurements are performed on that system, but we have kept subsystem A' in order to later ascribe some quantity of entanglement to the input state.

As stated in Sec. 7.1.2, instead of using the Gram matrix purity $\mathcal{P}$, we optimized the slightly different and numerically more simple objective function h from Def. 7.1.4. Although it might be more elegant to use the Gram matrix purity $\mathcal{P}$, nothing in the benchmarking procedure depends on that function. In fact, the Gram matrix found by optimizing h over the given experimental data works quite well for our purposes. To see this, we can consider simple lower and upper bounds on the maximum value of $\mathcal{P}$ compatible with the given constraints.

For one, the purity of the Gram matrix that maximizes h (denoted $\arg\max h$) is less than the maximum possible Gram matrix purity over all purifications, i.e.,

$$\mathcal{P}|_{\arg\max h} \leq \max \mathcal{P}. \tag{7.45}$$

On the other hand, we can easily find an upper bound on $\mathcal{P}$ by considering the pairwise fidelities:

$$\max \mathcal{P} \leq \frac{1}{M^2}\sum_{k=0}^{M-1}\sum_{l=0}^{M-1} F(\rho^{\text{in}}_k, \rho^{\text{in}}_l). \tag{7.46}$$

In Fig. 7.3, we plot the values of these lower and upper bounds for different numbers of rotationally symmetric test states (omitting the constant factors $\frac{1}{M^2}$). The computed

bounds are very close to each other, differing only in the third decimal place. This is the same order as the estimated numerical precision of the optimization. We conclude that using the modified objective function from Def. 7.1.4 is suitable for the situation we are considering, and that the obtained Gram matrix purity is close to what would be obtained by maximizing $\mathcal{P}$ itself.

7.2.2 Computing the entanglement

Having used the heuristic function h to find a feasible $\rho^{\text{in}}_{AA'}$ which corresponds to a near-optimal Gram matrix, we now consider the entanglement of the corresponding output state ρ^{out}_{AB}. We use the negativity (Eqs. (2.8)-(2.9)) as our entanglement measure. For states written in standard form, the negativity can be computed on the level of the individual matrices E_k. Using the entanglement quantification tools developed in Chs. 4 and 6, we compute the lowest value of the negativity that could be compatible with the given data. For this test, we impose the optimization cutoff at Fock level $N = 15$, making the truncated matrices 16-dimensional.

The quantification procedure was applied to four measurement scenarios:

(i) **Tomography**: the output density matrix is fully known numerically (up to the truncation level N);

(ii) **Quadratures from tomography**: only measurements on conjugate quadratures $\hat{x}$ and $\hat{p}$ for the output state are used, and these values are obtained from the tomographically-reconstructed density matrix;

(iii) **Quadratures from data**: same as (ii), but the quadrature values are obtained directly from the homodyne data;

(iv) **Quadratures with error bars**: the same quadrature data is used as in (iii), but estimates of data error bars are included in the computation ($\sigma - 3\sigma$ levels).

Recall from Ch. 6 that the choice of Fock cutoff N affects the strength of the optimization procedure itself, not just the density matrix. Truncating at a higher level would lead to better bounds on the entanglement. In all cases, we used the standard form results of Thms. 7.1.6 and 7.1.7. Finally, we straightforwardly included error bars by relaxing the constraint regions $\mathcal{C}(\rho^{\text{out}}_k, \hat{C}^j_B)$ in the entanglement minimization of Eq. (4.34). We performed the optimization as a semidefinite program in Matlab, using the frontend YALMIP [66] and the solvers SDPT3 [94] and SeDuMi [92]. The numerical uncertainty of this optimization

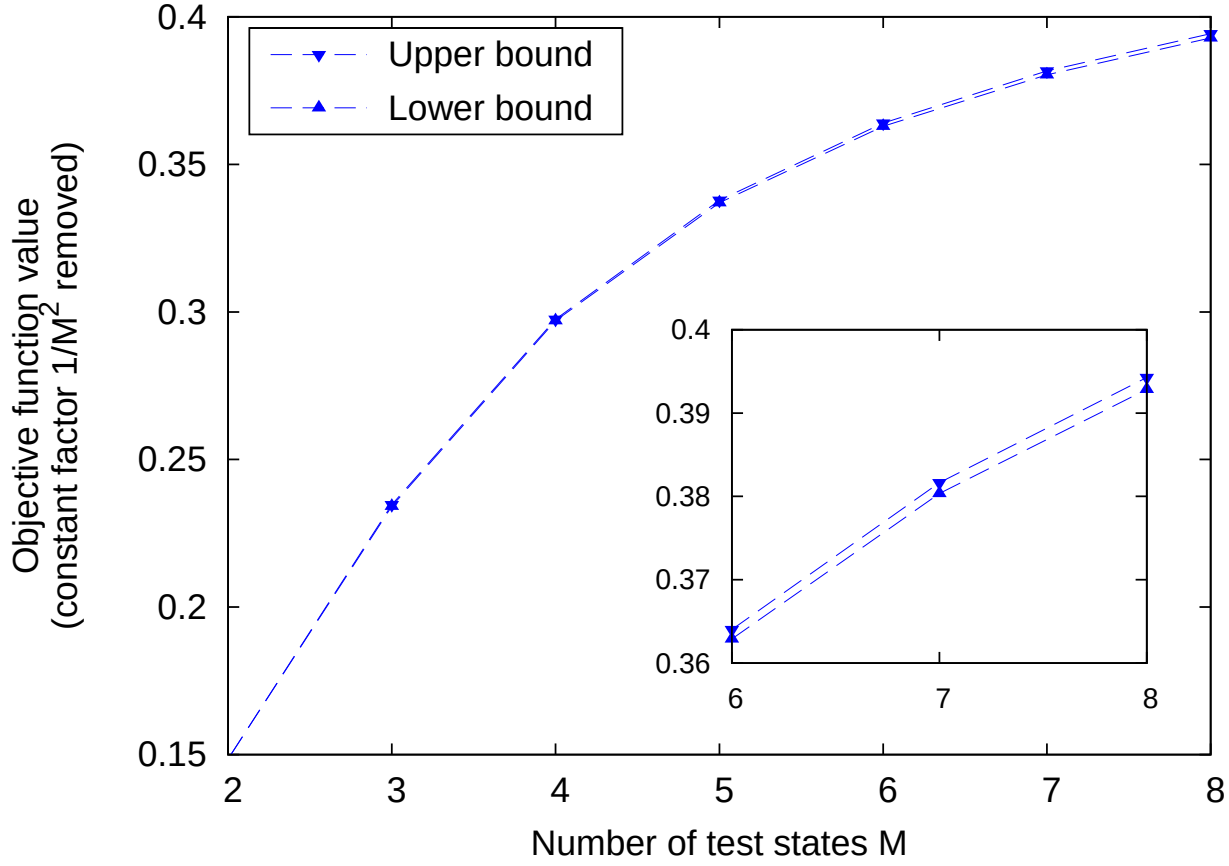


Figure 7.3: Upper and lower bounds for the maximum purity $\mathcal{P}$ of experimentally-compatible Gram matrices, corresponding to rotationally symmetric test ensembles of different cardinality. We have removed the factor $\frac{1}{M^2}$, which is common to both the upper and lower bounds, and independent of the purifications. The difference between the two bounds is on the order of 10^{-3} or less (inset), meaning that the obtained Gram matrix has purity which is near-optimal (represented by the lower curve). The estimated numerical precision of the optimization is $\approx 10^{-3}$.

is estimated to be $\approx 10^{-3}$ by comparing results from the two solvers under a number of situations. The results of these computations for different sized rotationally-symmetric ensembles are shown in Figs. 7.4 and 7.5.

There are a number of things to point out about the results in Figs. 7.4 and 7.5. Primarily, we can certify that the memory is in the quantum domain. Not only is the output state ρ_{AB}^{out} entangled for all M when we use the tomographically reconstructed density matrix ρ_0^{out}, but we can also see non-zero entanglement using the restricted set of measurements, including error bars. Furthermore, there is an evident advantage in using more than two test states, since it leads to higher entanglement in all cases. Indeed, it is not until $M > 2$ that the 3σ level conclusively leads to non-zero entanglement in the output state.

Another interesting result is that scenarios (i) and (ii) give very similar results[3] for the entanglement when $M \geq 3$. This is likely due to the fact that the output state has low levels of excess noise. The quadratures would already reveal that such a state is close to a minimum uncertainty state. Additional measurement information therefore does not contribute significantly to our knowledge of the state. For other types of states, quadrature measurements and tomography should not be expected to yield similar results (though there may be other choices of measurement operators which work well).

We also point out the advantage offered by phase-symmetric benchmarking and the standard form. In Ch. 6, we were limited, for numerical reasons, to considering only two or three test states. Although the Fock-projection approach applies to any number of (pure) test states, the computational resources required for more than three test states were prohibitive. Here, using the standard form, we have no problem pushing up to much higher numbers of states; Figs. 7.3-7.5 contain results for up to 8 test states. In fact, with a desktop PC, we were able to calculate benchmarks for up to 10 states, but these results are not included in the figures because they do not significantly change after $M = 8$.

Summary and outlook

In this chapter, we generalized entanglement-based benchmarks to handle arbitrary test states, not just those of a special form. We showed how this generalization leads to some freedom, namely in the choice of purifications used to describe the test states. By optimizing the purifications, we make the associated benchmarks stronger, leading to a larger quantum domain and a better chance of certifying quantum devices. We also studied

[3]Note that we do not compare situations (i) and (iii) because of the extra phase shift included in the tomographic reconstruction.

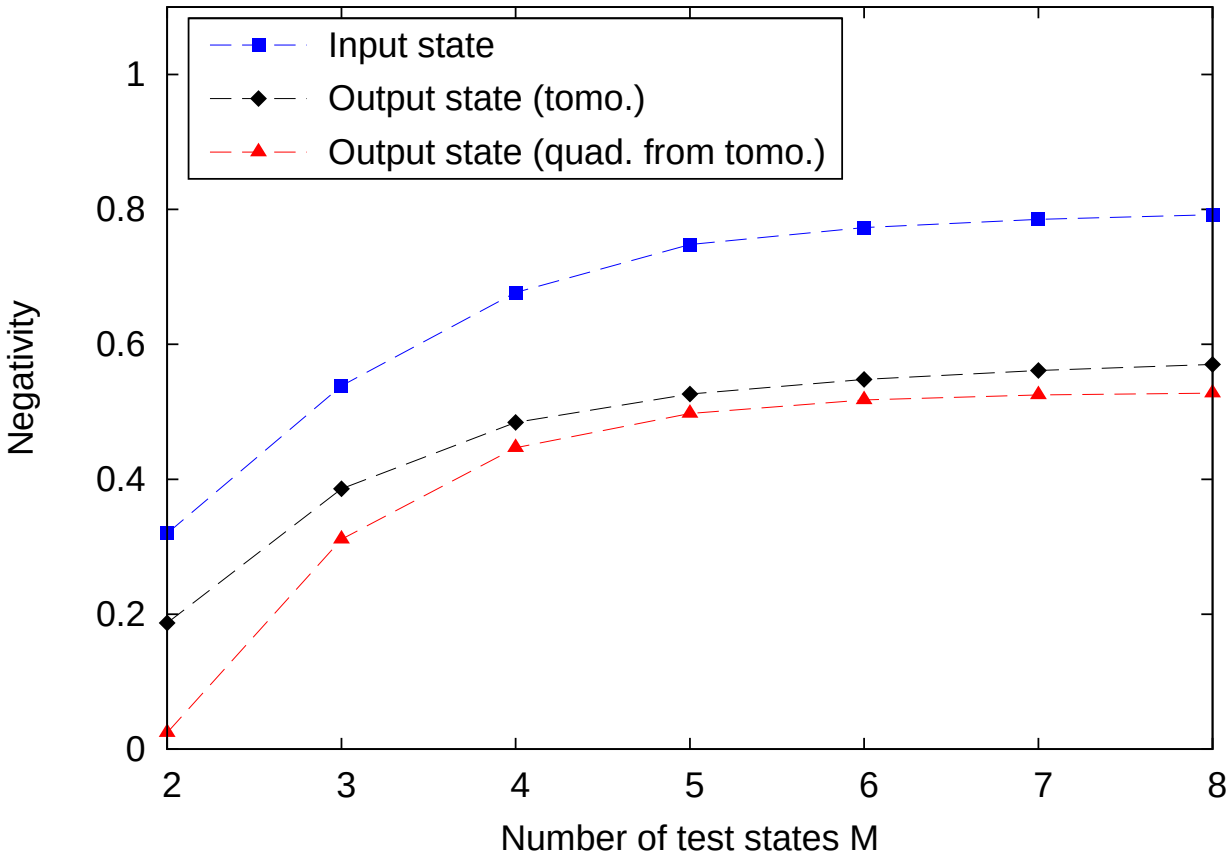


Figure 7.4: Quantum memory benchmarking results based on rotationally symmetric test ensembles using tomographically-reconstructed density matrices. The top curve is the negativity of the input state $\rho^{\text{in}}_{AA'}$ found by optimizing the heuristic function h. The other curves are lower bounds to the negativity of ρ^{out}_{AB} based on (in descending order): (i) tomographic reconstruction and (ii) quadrature values obtained from the tomographic reconstruction. Having output state negativity larger than zero is sufficient to certify the quantum memory.

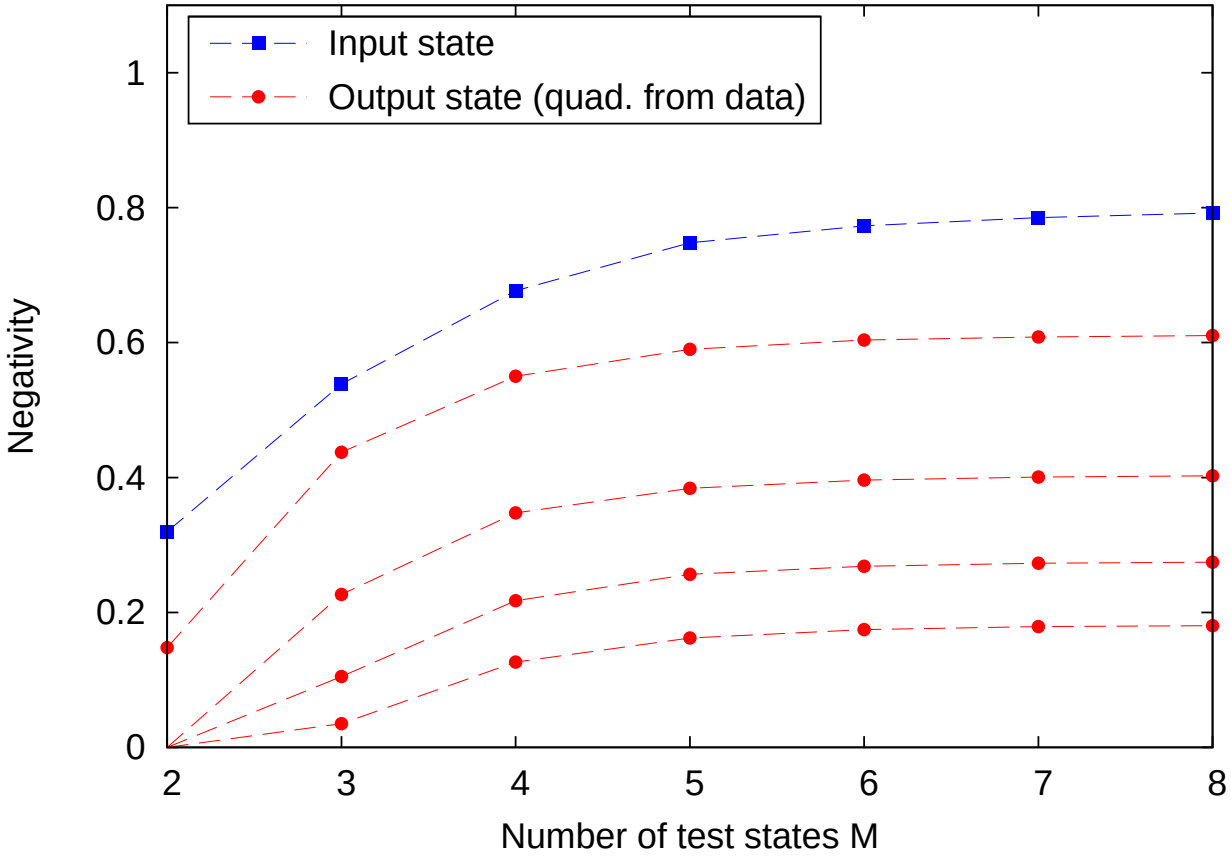


Figure 7.5: Quantum memory benchmarking results based on rotationally symmetric test ensembles using direct quadrature measurement data. The top curve is the same as Fig. 7.4. The other curves are lower bounds to the negativity of ρ_{AB}^{out} based on (in descending order): (iii) quadrature values obtained directly from measurement data and (iv) quadrature data with error bars included in the optimization (1σ, 2σ, and 3σ levels). For more than 3 test states, there is non-zero entanglement remaining even when including error estimates.

the effect of using different Gram matrix purities by considering some simple fidelity-based benchmarks. We gave a variational formula for the fidelity, which allowed these benchmarks to be computed using a semidefinite program. We also proved theorems for reducing the test states to a standard form under phase-symmetry conditions, allowing us to generate benchmarks efficiently from any single seed state. Although we mainly considered test states which were of a continuous-variable nature, all of our results, except the standard form, apply to discrete states as well. Together, these theoretical results were used to certify a CV quantum memory and to quantitatively explore how well the memory preserves entanglement in different scenarios.

Together, Chs. 4-7 provide a number of tools and techniques for benchmarking CV quantum communication devices with minimal and realistic experimental demands. Not only did we extend existing protocols to allow for entanglement quantification, but we also generalized entanglement-based schemes to accommodate arbitrary finite ensembles of test states. We applied a number of these tools to the task of certifying a CV quantum memory. Now that the theory of entanglement-based benchmarking has been developed in sufficient breadth and depth, we hope that this approach will be used to benchmark many more CV-encoded quantum optical devices. Indeed, this approach can be employed not only for optical systems, but for any situation where quantum information is encoded continuously in a harmonic oscillator system.

Chapter 8

Final remarks

The overarching goal of this thesis was to develop a suite of tools and tests for characterizing genuine quantum communication devices. Although we considered two different types of quantum technologies (single-photon devices and continuous-variable devices), the underlying principle was the same, namely that entanglement can be used to distinguish quantum devices from their classical analogs. From this general starting point, we built up a variety of quantum benchmarking results.

To make the benchmarking task as efficient and pain-free as possible, many of the benchmarks were designed to provide useful information with limited experimental resources. Our fidelity-based benchmarks for remote state preparation, based on Platonic solid ensembles, allow the certification of RSP systems using a small number of test states. On the other hand, the minimal requirements for benchmarking continuous variable devices are measurements of conjugate quadratures and the Gram matrix ρ_A. With only these basic ingredients, we can study the power of CV quantum communication devices to preserve entanglement. i.e.,

Another major focus in this thesis was to provide quantitative extensions to existing qualitative CV benchmarking tools. Using these quantitative tools, we can compare the strength of different communication devices within the quantum domain. We proposed to tackle the infinite dimensionality of optical-mode systems by projecting down to a finite subspace. With an appropriately chosen entanglement measure, e.g. the negativity, we can find lower bounds on how much entanglement was preserved in a particular device by searching within the projected space. We proposed two quite different choices for the projection and outlined how to solve the resulting entanglement optimization problems efficiently. These two choices are complementary; the two-qubit projection performs better for low levels of noise while the Fock projection is better suited for higher noise values.

Finally, the developed benchmarking results were used to certify two real-world quantum-optical devices. Using our calculated classical fidelity thresholds, a single-photon RSP experiment was shown to be strongly in the quantum domain. This experiment outperformed not only the optimal 2-cbit classical RSP device, but also the best 3-cbit classical device. The RSP experiment also met necessary conditions to be in the quantum domain for mixed state preparations. On the other hand, a number of our CV benchmarking results were used to demonstrate the entanglement-preserving ability of a quantum memory. In addition to the Fock-state projection used to quantify the entanglement, we also made use of standard form results for phase-symmetric benchmarking and studied how to strengthen the benchmarking scheme when using multiple realistic mixed states.

Although we considered specific scenarios, the ideas developed in this thesis are also applicable to a number of other situations. The most obvious extension is to move from

a prepare and measure scenario to one where actual discrete/continuous entangled states are present. Such 'hybrid' entangled states play a role in proposed quantum repeater systems [98, 57] and nanomechanical demonstrations of quantum phenomena [88]. The tools developed in Chs. 4-6 would be directly applicable for quantifying the entanglement in such systems. Another potential application for the ideas in this thesis would be to continuous-variable quantum key distribution. The two-qubit projected state from Ch. 5 has connections to related QKD protocols [110], but the corresponding key rates are not particularly good. Potentially, the bounds from the Fock projection in Ch. 6 could be adapted to this problem.

As well, the variational formula for the fidelity appearing in Ch. 7 could also prove useful for problems outside of quantum benchmarking. As already noted, it may be used to find the maximum possible fidelity between two states which are not completely known. Another potential use is to calculate the success probability of Grover's algorithm with mixed states [90]. Perhaps most importantly, since the fidelity is linked to the Bures distance [15, 45], the variational formulation can be used to efficiently compute the distance of any given state to the set of PPT states, which is a measure of PPT entanglement [101, 100].

We have developed a number of tools which expand the feature set of entanglement-based benchmarking, but there is still room for further improvement. For one, we have considered imperfect devices and imperfect state preparations, but we have not addressed the question of imperfect measurement devices. Most importantly, the local oscillator in homodyne measurements is typically assumed to be in a strong decoupled classical state during measurement. If unverified, this assumption opens up a potential loophole which can be exploited by an adversarial device. On the other hand, this loophole can be closed by considering so-called Stokes measurements, which incorporate the local oscillator, and successful quantum benchmarking is still possible in such a situation [37]. It would be fruitful to extend the quantitative picture to this scenario. Another direction for future research is to consider phase-symmetric benchmarks for the case where the test ensemble has an infinite number of states. Indeed, there are some very suggestive links between our standard form results and continuous Fourier transforms [32]. Finally, we have resisted fixing a formal definition for the quantum throughput in this thesis. However, it could be useful and illuminating to mathematically define and study the properties of this concept.

Entanglement is clearly of fundamental importance to quantum communication and quantum benchmarking, but we should be wary of subscribing too strictly to Schrödinger's much-quoted dictum [89]: "I would not call (entanglement) *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." Not to begrudge Schrödinger's seminal contributions to the development

of quantum theory, but entanglement is not the only quantum correlation of importance. In recent years, there has been a trend in quantum information research toward identifying and quantifying other types of correlations that are not present in classical systems, such as the quantum discord [76, 39] or the measurement-induced disturbance [68]. Indeed, in Ch. 7, we noticed that the best test ensembles within our quantum benchmarking framework are those that have high Gram matrix purity, not necessarily those that provide the highest initial entanglement. It would thus be illuminating to further study the Gram matrix purity and its possible connections to other measures of quantum correlations.

APPENDICES

Appendix A

Supplement for remote state preparation benchmarks

A.1 Proof of bound for continuous case

In this appendix, we prove two claims from Sec. 3.2.2 used to find upper bounds on the classical threshold for states on the Bloch sphere.

Claim 1. Define a circular cap as the set of points on the surface of the Bloch sphere lying north of some fixed latitude or any rigid spherical rotation of this. Amongst all partitions of surface area $A > 0$, a circular cap has the longest average Bloch vector.

Proof. Consider an arbitrary partition of total surface area $A > 0$ (we do not assume that this partition is connected). This partition, which we call Γ, defines some average Bloch vector $\vec{r}_\Gamma$. We will compare partition Γ with a circular cap of area A centred along the direction of $\vec{r}_\Gamma$, which we shall denote by C. Partition C has an average Bloch vector $\vec{r}_C$. If $\vec{r}_\Gamma$ is the zero vector, then $r_C \geq r_\Gamma = 0$. If not, then without loss of generality we can assume $\vec{r}_\Gamma$ points along the z-axis. By construction, $\vec{r}_C$ must also point along the z-axis. Using Γ and C, the Bloch sphere can be divided into four disjoint regions: $R_1 = \Gamma \cap C$, $R_2 = \Gamma - C$, $R_3 = \Gamma^c \cap C$, and $R_4 = \Gamma^c - C$. Each of these regions has average Bloch vector $\vec{r}_i$ and area A_i, $i = 1, ..., 4$. Also note that we must have $A_2 = A_3$.

Since $\Gamma = R_1 \cup R_2$, and $C = R_1 \cup R_3$, we must have

$$\vec{r}_\Gamma = \frac{A_1}{A_1 + A_2}\vec{r}_1 + \frac{A_2}{A_1 + A_2}\vec{r}_2, \text{ and} \tag{A.1}$$

$$\vec{r}_C = \frac{A_1}{A_1 + A_2}\vec{r}_1 + \frac{A_3}{A_1 + A_3}\vec{r}_3. \tag{A.2}$$

From this we conclude that

$$\vec{r}_C = \vec{r}_\Gamma + \frac{A_2}{A_1 + A_2}(\vec{r}_3 - \vec{r}_2), \tag{A.3}$$

i.e., that the vector $\vec{r}_3 - \vec{r}_2$ also lies along the z-axis. However, it might point in the negative z-direction.

But the boundary of C lies at some fixed height H_C on the z-axis. By construction, every state in R_3 has a z-component higher than H_C and every state in R_2 has a z-component lower than H_C. Then the z-component of $\vec{r}_3$ must be larger than that of $\vec{r}_2$. Therefore, their difference $\vec{r}_3 - \vec{r}_2$ has a positive z-component. From Eq. (A.3), we can conclude that $\vec{r}_C$ is longer than $\vec{r}_\Gamma$. Thus, for fixed area A, a circular cap gives the longest average Bloch vector. □

Claim 2. Knowing that a circular cap gives the optimum Bloch vector length for fixed area A, we want to optimize the objective function

$$\sum_{k=0}^{2^c-1} \overline{F}_{A_k}^{\max} = \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} p_k r_k^{\max}\right) \tag{A.4}$$

subject to the constraint

$$\sum_{k=0}^{2^c-1} A_k = 4\pi. \tag{A.5}$$

We claim that this is optimized when all areas are equal.

Proof. To obtain the optimal Bloch vector as a function of area, we temporarily centre a spherical cap on the z-axis and integrate up to some final angle θ_k^f,

$$\begin{aligned} r^{\max}(\theta_k^f) =& \frac{1}{A_k}\left|\int_{\varphi=0}^{2\pi}\int_{\theta=0}^{\theta_k^f} \sin(\theta)\cos(\theta)\mathrm{d}\varphi\mathrm{d}\theta\right| \\ =& \frac{1}{A_k}\pi\sin^2(\theta_k^f). \end{aligned} \tag{A.6}$$

Reparameterizing using $A_k = 4\pi \sin^2\left(\frac{\theta_k^f}{2}\right)$, we end up with

$$r^{\max}(A_k) = 1 - \frac{A_k}{4\pi}. \tag{A.7}$$

The corresponding probabilities are given by $p_k = \frac{A_k}{4\pi}$. We can group the objective function (A.4) together with the constraint (A.5) into the following Lagrange function:

$$\begin{aligned}\Lambda(A_k, \lambda) =& \frac{1}{2}\left(1 + \sum_{k=0}^{2^c-1} \frac{A_k}{4\pi}\left(1 - \frac{A_k}{4\pi}\right)\right) \\ &+ \lambda\left(\sum_{k=0}^{2^c-1} \frac{A_k}{4\pi} - 1\right).\end{aligned} \tag{A.8}$$

Solving this Lagrange problem for the maximum yields $A_k = \frac{4\pi}{2^c}$ for every k. Hence, the optimal distribution of areas occurs when all they are all equal. □

A.2 Proof of optimal average fidelity for mixed states

In this appendix, we prove the optimality of Eq. (3.15). Since we are dealing with qubits, we can make use of an alternative formula for fidelity found in [71], namely

$$F(\sigma, \tau) = \mathrm{Tr}(\sigma\tau) + \sqrt{1 - \mathrm{Tr}(\sigma^2)}\sqrt{1 - \mathrm{Tr}(\tau^2)}. \tag{A.9}$$

Under the assumptions that the target states all have the same Bloch vector length r and that the message strategy is deterministic, the average fidelity is

$$\begin{aligned}\overline{F} &= \sum_{\alpha} p_\alpha F(\rho_\alpha^{\mathrm{tar}}, \rho_\alpha^{\mathrm{out}}) \\ &= \sum_{k=0}^{2^c-1} \sum_{\alpha \in k} p_\alpha F(\rho_\alpha^{\mathrm{tar}}, \rho_k^{\mathrm{out}}) \\ &= \sum_{k=0}^{2^c-1} p_k \left[\mathrm{Tr}(\overline{\rho_k}\rho_k^{\mathrm{out}}) + \sqrt{\frac{1-r^2}{2}}\sqrt{1 - \mathrm{Tr}((\rho_k^{\mathrm{out}})^2)}\right].\end{aligned} \tag{A.10}$$

As before, $p_k = \sum_{\alpha \in k} p_\alpha$ is the probability of sending message k and $\overline{\rho_k} = \frac{1}{p_k}\sum_{\alpha \in k} p_\alpha \rho_\alpha$ is the weighted average of states where message k is sent. The quantity in square brackets

will be denoted by

$$B_k[\rho_k^{\text{out}}] := \text{Tr}(\overline{\rho_k}\rho_k^{\text{out}}) + \sqrt{\frac{1-r^2}{2}}\sqrt{1-\text{Tr}((\rho_k^{\text{out}})^2)}. \tag{A.11}$$

For each k, we need to find the choice of ρ_k^{out} that optimizes B_k. Working in the eigenbasis of $\overline{\rho_k}$, we have

$$\rho_k^{\text{out}} = \begin{bmatrix} a & b \\ b^* & d \end{bmatrix}, \tag{A.12}$$

with $a, d \in \mathbb{R}, b \in \mathbb{C}$. From the above expression for the fidelity, the optimal choice of ρ_k^{out} should be simultaneously diagonal with $\overline{\rho_k}$, i.e., $b = 0$. Equivalently, the Bloch vectors of $\overline{\rho_k}$ and the optimal ρ_k^{out} should be parallel. Denoting the magnitudes of these Bloch vectors by r_k and s_k, respectively, we are left with

$$\begin{aligned} B_k =& \frac{1}{4}\left[(1+r_k)(1+s_k) + (1-r_k)(1-s_k)\right] \\ &+ \sqrt{\frac{1-r^2}{2}}\sqrt{\frac{1-s_k^2}{2}} \\ =& \frac{1}{2}\left(1 + r_k s_k\right) + \sqrt{\frac{1-r^2}{2}}\sqrt{\frac{1-s_k^2}{2}}. \end{aligned} \tag{A.13}$$

Since r_k is fixed by the choice of target state partitioning, we differentiate B_k with respect to s_k and find where this derivative equals zero. The result is

$$s_k = \pm\frac{r_k}{\sqrt{r_k^2 + 1 - r^2}}. \tag{A.14}$$

The positive root will give the maximum of B_k, which works out to be

$$B_k^{\max} = \frac{1}{2}\left(1 + \sqrt{r_k^2 + 1 - r^2}\right). \tag{A.15}$$

Collecting all the terms together yields Eq. (3.15).

Appendix B

Supplement for two-qubit projection scheme

B.1 Derivation of overlap bounds

In this appendix, we derive the bounds from Eqs. (5.10)-(5.11) for the magnitude of the overlap of the maximal eigenstates $t = \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$. As the starting point, Refs. [84, 110] provide the following statement (cf. Eqs. (C17)-(C18) of [110]):

Overlap Bounds. Let the largest eigenvalue of ρ_k^{out} be parameterized by

$$\lambda_k^{\mathrm{L}} =: 1 - \tilde{\varepsilon}_k, \tag{B.1}$$

and let the fidelity between the output states and the coherent states $|\tilde{\alpha}_k\rangle$ from Eq. (5.7) be given by

$$\langle \tilde{\alpha}_k | \rho_k^{\mathrm{out}} | \tilde{\alpha}_k \rangle =: 1 - \varepsilon_k \tag{B.2}$$

and let

$$\kappa := |\langle \tilde{\alpha}_0 | \tilde{\alpha}_1 \rangle| . \tag{B.3}$$

Then the following holds:

$$c_l(\kappa, \varepsilon_k, \tilde{\varepsilon}_k) \leq |t| \leq c_u(\kappa, \varepsilon_k, \tilde{\varepsilon}_k), \tag{B.4}$$

with

$$\begin{aligned} c_l = \kappa &\sqrt{\frac{1-\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}}\sqrt{\frac{1-\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &- \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &- \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}} \\ &- \sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}} \end{aligned} \tag{B.5}$$

and

$$\begin{aligned} c_u = \kappa &\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}} \\ &+ \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_0}{1-\tilde{\varepsilon}_0}}\sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}} \\ &+ \sqrt{1-\kappa^2}\sqrt{\frac{1-\varepsilon_1}{1-\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}} \\ &+ \sqrt{\frac{\varepsilon_1-\tilde{\varepsilon}_1}{1-2\tilde{\varepsilon}_1}}\sqrt{\frac{\varepsilon_0-\tilde{\varepsilon}_0}{1-2\tilde{\varepsilon}_0}}. \end{aligned} \tag{B.6}$$

In our scenario, we cannot calculate the quantities ε or $\tilde{\varepsilon}$ in practice. We now modify these bounds from the above form to one involving only the parameters κ (calculated from first moments) and the U_k (calculated from second moments). To do this, we make use only of the following inequalities (cf. Eqs. (65) and (68) from [110]):

$$0 \leq \tilde{\varepsilon}_k \leq \varepsilon_k \leq U_k. \tag{B.7}$$

From this, we can easily derive the following auxiliary inequalities:

$$\sqrt{\frac{1-\varepsilon_k}{1-\tilde{\varepsilon}_k}} \leq 1, \tag{B.8}$$

$$\sqrt{\frac{\varepsilon_k-\tilde{\varepsilon}_k}{1-2\tilde{\varepsilon}_k}} \leq \sqrt{\frac{\varepsilon_k}{1-2\tilde{\varepsilon}_k}} \leq \sqrt{\frac{U_k}{1-2U_k}}\ ;\ \left(U_k < \frac{1}{2}\right), \tag{B.9}$$

$$\sqrt{\frac{1-\varepsilon_k-\tilde{\varepsilon}_k}{1-2\tilde{\varepsilon}_k}} \geq \sqrt{1-2U_k}\ ;\ \left(U_k < \frac{1}{2}\right). \tag{B.10}$$

It is important to note that the second and third inequalities only hold so long as $U_k < \frac{1}{2}$. For symmetric noise, the value $U_k = \frac{1}{2}$ corresponds to $\mathrm{Var}_k(\hat{x}) = \mathrm{Var}_k(\hat{p}) = \sqrt{2} - \frac{1}{2} \approx 0.914$, almost twice the vacuum variance. This value is far outside the region where our method gives non-trivial bounds, so it is not an issue. Substituting the inequalities (B.8) and (B.10) into Eqs. (B.5) and (B.6), we arrive at the bounds given in Eqs. (5.10)-(5.11).

B.2 Derivation of supplementary diagonal bounds

Here we aim to bound the quantities $\langle \lambda_j^{\mathrm{L}} | \rho_{kk}^{\mathrm{out}} | \lambda_j^{\mathrm{L}} \rangle$ for $j \neq k$, as found in Eqs. (5.14)-(5.15). An eigenbasis expansion of ρ_{00}^{out} leads to

$$\begin{aligned}
\langle \lambda_1^{\mathrm{L}} | \rho_{00}^{\mathrm{out}} | \lambda_1^{\mathrm{L}} \rangle &= (1 - \tilde{\varepsilon}_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 + \sum_{k=1}^{\infty} \lambda_0^k \left| \langle \lambda_0^k | \lambda_1^{\mathrm{L}} \rangle \right|^2 \\
&\leq (1 - \tilde{\varepsilon}_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 + \sum_{k=1}^{\infty} \lambda_0^k \\
&= (1 - \tilde{\varepsilon}_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 + \tilde{\varepsilon}_0 \\
&= \tilde{\varepsilon}_0 \left(1 - \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 \right) + \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 \\
&\leq U_0 \left(1 - \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 \right) + \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 \\
&= (1 - U_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 + U_0. \qquad \text{(B.11)}
\end{aligned}$$

A lower bound can be derived in a similar way:

$$\begin{aligned}
\langle \lambda_1^{\mathrm{L}} | \rho_{00}^{\mathrm{out}} | \lambda_1^{\mathrm{L}} \rangle =& (1 - \tilde{\varepsilon}_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 + \sum_{k=1}^{\infty} \lambda_0^k \left| \langle \lambda_0^k | \lambda_1^{\mathrm{L}} \rangle \right|^2 \\
\geq& (1 - \tilde{\varepsilon}_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 \\
\geq& (1 - U_0) \left| \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle \right|^2 . \qquad \text{(B.12)}
\end{aligned}$$

Substituting the parameters $x_2 = \langle \lambda_1^{\mathrm{L}} | \rho_{00}^{\mathrm{out}} | \lambda_1^{\mathrm{L}} \rangle$ and $t = \langle \lambda_0^{\mathrm{L}} | \lambda_1^{\mathrm{L}} \rangle$, we arrive at the desired bounds. The bounds for $x_3 = \langle \lambda_0^{\mathrm{L}} | \rho_{11}^{\mathrm{out}} | \lambda_0^{\mathrm{L}} \rangle$ follow by interchanging indices.

B.3 Derivation of off-diagonal bounds

This appendix outlines the derivation of the off-diagonal bounds from Eqs. (5.17)-(5.18). We completely know ρ_A, which constrains that we must have $\mathrm{Tr}(\rho_{01}^{\mathrm{out}}) = \langle -\alpha|\alpha\rangle = c$. First, we consider the full density matrix ρ_{AB}^{out} in the basis defined by $\{|0\rangle, |1\rangle\}$ for system A and the eigenbasis of ρ_{00}^{out}, $\{|\lambda_0^k\rangle\}_{k=0}^{\infty}$, for system B. Using the block form of Eq. (4.9), we denote the diagonal elements of the block ρ_{11}^{out} by $\{b_k\}_{k=0}^{\infty}$ and the diagonal elements of the block ρ_{01}^{out} by $\{d_k\}_{k=0}^{\infty}$ (the diagonal elements of ρ_{00}^{out} are its eigenvalues). Using the triangle inequality, we have

$$|c| = \left|\mathrm{Tr}(\rho_{01}^{\mathrm{out}})\right| = \left|d_0 + \sum_{k=1}^{\infty} d_k\right| \leq |d_0| + \sum_{k=1}^{\infty} |d_k|. \tag{B.13}$$

From positivity of ρ_{AB}, we find

$$|c| \leq |d_0| + \sum_{k=1}^{\infty} \sqrt{\lambda_0^k}\sqrt{b_k}, \tag{B.14}$$

and from the Cauchy-Schwarz inequality,

$$|c| \leq |d_0| + \sqrt{\left(\sum_{k=1}^{\infty} \lambda_0^k\right)\left(\sum_{k=1}^{\infty} b_k\right)}. \tag{B.15}$$

The first sum is just $\tilde{\varepsilon}_0$ and the second is $1 - b_0$. Now, using the bounds from App. B.2, we get

$$\begin{aligned} b_0 =& \left\langle \lambda_0^{\mathrm{L}}\right| \rho_{11}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle \\ \geq& (1 - U_1)\left|\left\langle \lambda_0^{\mathrm{L}}\right| \lambda_1^{\mathrm{L}}\right\rangle\right|^2, \end{aligned} \tag{B.16}$$

which we can substitute above to obtain

$$|c| \leq |d_0| + \sqrt{\tilde{\varepsilon}_0}\sqrt{1 - (1 - U_1)\left|\langle \lambda_0^{\mathrm{L}}| \lambda_1^{\mathrm{L}}\rangle\right|^2}. \tag{B.17}$$

Replacing d_0 with $\left\langle \lambda_0^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle$, we are led to the off-diagonal bound

$$\left|\left\langle \lambda_0^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle\right| \geq |c| - \sqrt{U_0}\sqrt{1 - (1 - U_1)\left|\langle \lambda_0^{\mathrm{L}}| \lambda_1^{\mathrm{L}}\rangle\right|^2}. \tag{B.18}$$

Finally, we substitute in the parameters $z_1 = \left\langle \lambda_0^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_0^{\mathrm{L}}\right\rangle$ and $t = \left\langle \lambda_0^{\mathrm{L}}\right| \lambda_1^{\mathrm{L}}\rangle$ to give the desired bounds. By applying the same arguments using the eigenbasis of ρ_{11}^{out}, we can arrive at an analogous bound for $z_4 = \left\langle \lambda_1^{\mathrm{L}}\right| \rho_{01}^{\mathrm{out}} \left|\lambda_1^{\mathrm{L}}\right\rangle$.

B.4 Constraints for two-qubit optimization

In this appendix, we explicitly list the full set of constraints used in the two-qubit projection optimization of Ch. 5. The reader is referred to the chapter itself for definitions of the parameters (in particular, Eqs. (5.6), (5.12), (5.13), and (5.21)). In these constraints, the optimal substitution $t \to b_u$ has already been incorporated.

The constraints are the following:

1. Physicality of density matrix constraints
   - $\rho_{AB}^{\Pi} \geq 0$
   - $\mathrm{Tr}(\rho_{AB}^{\Pi} |0\rangle\langle 0|_A \otimes \hat{\mathbb{1}}_B) \leq \frac{1}{2}$
   - $\mathrm{Tr}(\rho_{AB}^{\Pi} |1\rangle\langle 1|_A \otimes \hat{\mathbb{1}}_B) \leq \frac{1}{2}$
2. Test state constraints
   - $x_1 \geq 1 - U_0$
   - $x_1 \leq 1$
   - $x_4 \geq 1 - U_1$
   - $x_4 \leq 1$
   - $x_1 \geq x_2$
   - $x_4 \geq x_3$
   - $x_2 \geq (1 - U_0)|b_u|^2$
   - $x_2 \leq (1 - U_0)|b_u|^2 + U_0$
   - $x_3 \geq (1 - U_1)|b_u|^2$
   - $x_3 \leq (1 - U_1)|b_u|^2 + U_1$
3. Off-diagonal constraints
   - $\mathrm{Re}(z_1) \geq 0$
   - $\mathrm{Im}(z_1) = 0$
   - $\mathrm{Re}(z_1) \geq |c| - \sqrt{U_0}\sqrt{1 - (1 - U_1)|b_u|^2}$
   - $|\mathrm{Re}(z_4)| + |\mathrm{Im}(z_4)| \geq r$, with $r := |c| - \sqrt{U_1}\sqrt{1 - (1 - U_0)|b_u|^2}$

Appendix C

Supplement for Fock-state projection scheme

C.1 Derivation of first order constraint

Here, we detail how to arrive at the bound given in Lemma (6.1.2), which forms part of the constraints for the Fock state projection. Let τ be a bounded positive-semidefinite operator and let τ_N be the projection of τ onto the subspace spanned by the Fock states $\{|0\rangle, \ldots |N\rangle\}$: $\tau_N = \sum_{l,m=0}^{N} \langle l| \tau |m\rangle |l\rangle\langle m|$. We seek to bound the magnitude of the difference

$$\begin{aligned} \mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a}) &= \sum_{m=0}^{\infty} \langle m| (\tau - \tau_N)\hat{a} |m\rangle \\ &= \sum_{m=0}^{\infty} \sqrt{m} \langle m| (\tau - \tau_N) |m-1\rangle . \end{aligned} \tag{C.1}$$

For simplicity, denote general matrix elements by $\langle m| \tau |n\rangle =: \tau_{m,n}$, and diagonal entries by $\tau_{m,m} =: \tau_m$. Then, from the triangle inequality,

$$|\mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a})| \leq \sum_{m=N+1}^{\infty} \sqrt{m} |\tau_{m,m-1}| \tag{C.2}$$

From the positivity of τ, we must have

$$|\tau_{m,l}|^2 \leq \tau_m \tau_l. \tag{C.3}$$

Therefore,

$$|\mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a})| \leq \sum_{m=N+1}^{\infty} \sqrt{m}\sqrt{\tau_m}\sqrt{\tau_{m-1}} \tag{C.4}$$

Using the Cauchy-Schwarz inequality on this sum, we find

$$|\mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a})| \leq \sqrt{\left(\sum_{m=N+1}^{\infty} m\tau_m\right)\left(\sum_{m=N+1}^{\infty} \tau_{m-1}\right)}. \tag{C.5}$$

The first bracketed term is the difference in mean photon number between τ and τ_N, while the second is the difference in trace between τ and its truncation after the level $N-1$. Finally, we arrive at the desired bound:

$$|\mathrm{Tr}(\tau\hat{a}) - \mathrm{Tr}(\tau_N\hat{a})| \leq \sqrt{(\overline{n} - \overline{n}_N)(\mathrm{Tr}(\tau) - \mathrm{Tr}(\tau_{N-1}))}. \tag{C.6}$$

C.2 Derivation of second order constraint

In this appendix, we outline how to arrive at the bound on the difference operator found in Lemma 6.1.3, which forms another constraint for the Fock state projection. We begin with

$$\begin{aligned}\mathrm{Tr}(\tau\hat{a}^{\dagger 2}) - \mathrm{Tr}(\tau_N\hat{a}^{\dagger 2}) &= \sum_{m=0}^{\infty} \langle m| (\tau - \tau_N)\hat{a}^{\dagger 2} |m\rangle \\ &= \sum_{m=N-1}^{\infty} \sqrt{m+1}\sqrt{m+2}\tau_{m,m+2}.\end{aligned} \tag{C.7}$$

Similarly,

$$\mathrm{Tr}(\tau\hat{a}^2) - \mathrm{Tr}(\tau_N\hat{a}^2) = \sum_{m=N-1}^{\infty} \sqrt{m+1}\sqrt{m+2}\tau^*_{m,m+2}. \tag{C.8}$$

Therefore, with $\hat{d} := \hat{a}^{\dagger 2} + \hat{a}^2$,

$$\begin{aligned}\left|\mathrm{Tr}(\tau\hat{d}) - \mathrm{Tr}(\tau_N\hat{d})\right| &= \left|2\sum_{m=N-1}^{\infty} \sqrt{m+1}\sqrt{m+2}\mathrm{Re}[\tau_{m,m+2}]\right| \\ &\leq 2\sum_{m=N-1}^{\infty} \sqrt{m+1}\sqrt{m+2}\,|\tau_{m,m+2}|\,.\end{aligned} \tag{C.9}$$

As in App. C.1, we can use the positivity of τ and the Cauchy-Schwarz inequality to get

$$\begin{aligned}&\left|\mathrm{Tr}(\tau\hat{d}) - \mathrm{Tr}(\tau_N\hat{d})\right| \\ &\leq 2\sqrt{\left(\sum_{m=N-1}^{\infty}(m+2)\tau_{m+2}\right)\left(\sum_{m=N-1}^{\infty}(m+1)\tau_m\right)}.\end{aligned} \tag{C.10}$$

Finally, by rewriting the right hand side as

$$2\sqrt{(\overline{n}-\overline{n}_N)\left[(\overline{n}-\overline{n}_{N-2})+(\mathrm{Tr}(\tau)-\mathrm{Tr}(\tau_{N-2}))\right]} = \delta, \tag{C.11}$$

we arrive at the desired bound.

Appendix D

Supplement for benchmarking with arbitrary states

D.1 Convexity proofs

In this appendix, we prove the following two statements about convexity relevant to Ch. 7: (i) the objective function in Eq. (7.16) is a convex function, and (ii) the set of Gram matrices which are consistent with purifications of the test states is a convex set. First, for positive semidefinite operators, the purity is equivalent to the squared Hilbert-Schmidt norm. By definition, all norms are convex, and taking the square preserves this convexity. Hence, our objective function is convex.

To prove the second statement, let $\{|\Gamma^0_k\rangle_{A'A''}\}_{k=0}^{M-1}$ and $\{|\Gamma^1_k\rangle_{A'A''}\}_{k=0}^{M-1}$ be two sets of purifications of the test states $\{\rho^{\text{in}}_k\}_{k=0}^{M-1}$ (without loss of generality, we can consider the purifying system to be the same), with Gram matrices G_0 and G_1, respectively. Fix some $p \in [0,1]$ and take the convex combination of Gram matrices $G = pG_0 + (1-p)G_1$. We need to show that there is some compatible set of purifications leading to the Gram matrix G.

To do this, we define the following states:

$$|\chi_k\rangle_{A'A''A'''} := \sqrt{p}\,|\Gamma^0_k\rangle_{A'A''} \otimes |0\rangle_{A'''} + \sqrt{1-p}\,|\Gamma^1_k\rangle_{A'A''} \otimes |1\rangle_{A'''}\,, \tag{D.1}$$

where $|0\rangle_{A'''}$ and $|1\rangle_{A'''}$ are orthonormal states on some additional purifying system A'''.

Tracing out all systems except A', we find

$$\begin{aligned}\mathrm{Tr}_{A''A'''}\left|\chi_k\right\rangle\!\left\langle\chi_k\right|_{A'A''A'''} &= p\mathrm{Tr}_{A''}\left|\Gamma_k^0\right\rangle\!\left\langle\Gamma_k^0\right|_{A'A''} \\ &\quad + (1-p)\mathrm{Tr}_{A''}\left|\Gamma_k^1\right\rangle\!\left\langle\Gamma_k^1\right|_{A'A''} \\ &= \rho_k^{\mathrm{in}}. \end{aligned} \tag{D.2}$$

Thus, the $\left|\chi_k\right\rangle_{A'A''A'''}$ are purifications of the ρ_k^{in}. The elements of the corresponding Gram matrix are

$$\begin{aligned}\left\langle\chi_k|\chi_l\right\rangle &= p\left\langle\Gamma_k^0|\Gamma_l^0\right\rangle + (1-p)\left\langle\Gamma_k^1|\Gamma_l^1\right\rangle \\ &= p[G_0]_{lk} + (1-p)[G_1]_{lk}, \end{aligned} \tag{D.3}$$

which are exactly the elements of the convex combination G. Therefore, the set of Gram matrices which come from purifications of the test states is a convex set.

D.2 Proof of standard form

In this appendix, we prove the standard form results for phase-symmetric benchmarking found in Thm. 7.1.6. To begin, when the symmetry condition of Eq. (7.37) holds, then τ_{AB} can be transformed by the unitary matrix

$$R = \bigoplus_{k=0}^{M-1} U_\theta^k \tag{D.4}$$

to the form

$$\begin{aligned}\mathcal{C}(\tau_{AB}) &= R^\dagger \tau_{AB} R \\ &= \frac{1}{M}\begin{bmatrix} \tau_{00} & W_{01} & W_{02} & \cdots & W_{0,M-1} \\ W_{0,M-1} & \tau_{00} & W_{01} & \cdots & W_{0,M-2} \\ W_{0,M-2} & W_{0,M-1} & \tau_{00} & \cdots & W_{0,M-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ W_{01} & W_{02} & W_{03} & \cdots & \tau_{00} \end{bmatrix} \end{aligned} \tag{D.5}$$

with $W_{ij} := \tau_{ij} U_\theta^j$. The matrix $\mathcal{C}(\tau_{AB})$ has a *block circulant* structure, meaning that each row of blocks is the same as the previous row, but shifted by one to the right. Now, let $\omega_M = \exp(i\theta)$ be the primitive Mth root of unity and let

$$[F_M]_{ij} = \tfrac{1}{\sqrt{M}}\omega_M^{i\cdot j} \tag{D.6}$$

be the (unitary) discrete Fourier transform matrix. Using a standard theorem on block circulant matrices [24], $\mathcal{C}(\tau_{AB})$ can be block diagonalized by the matrix $F_M \otimes \hat{\mathbb{1}}_B$. Explicitly,

$$\begin{aligned}\mathcal{D}(\tau_{AB}) =&(F_M^\dagger \otimes \hat{\mathbb{1}}_B)\mathcal{C}(\tau_{AB})(F_M \otimes \hat{\mathbb{1}}_B)\\ =&\bigoplus_{k=0}^{M-1} E_k,\end{aligned} \tag{D.7}$$

with

$$E_k = \frac{1}{M}\sum_{l=0}^{M-1} \omega_M^{k\cdot l} W_{kl} \tag{D.8}$$

Since the partial trace is unaffected by local unitaries on the same subsystem, we have

$$\begin{aligned}\sum_{k=0}^{M-1} E_k =&\mathrm{Tr}_A\left(\sum_{k=0}^{M-1} |k\rangle\langle k|_A \otimes E_k\right)\\ =&\mathrm{Tr}_A \mathcal{D}(\tau_{AB})\\ =&\mathrm{Tr}_A \mathcal{C}(\tau_{AB}).\end{aligned} \tag{D.9}$$

Comparing this with Eq. (D.5), we conclude

$$\sum_{k=0}^{M-1} E_k = \tau_{00}, \tag{D.10}$$

which proves Eq. (7.40). Finally, the positive semidefinite condition follows directly from the unitary equivalence of τ_{AB} and $\mathcal{D}(\tau_{AB})$.

□

D.3 Proof of trace norm in standard form

In this appendix, we prove Thm. 7.1.7, which gives a formula for the negativity involving the standard form. Now, if τ_{AB} satisfies the symmetry condition in Eq. (7.37), then so will the partial transpose $\tau_{AB}^{T_A}$. Therefore, $\tau_{AB}^{T_A}$ is unitarily equivalent to some block diagonal matrix $\mathcal{B}(\tau_{AB}^{T_A}) = \bigoplus_{k=0}^{M-1} \tilde{E}_k$. The trace norm is a unitarily invariant norm, so we must have

$$||\tau_{AB}^{T_A}||_1 = \left|\left|\bigoplus_{k=0}^{M-1} \tilde{E}_k\right|\right|_1 = \sum_{k=0}^{M-1} ||\tilde{E}_k||_1, \tag{D.11}$$

which proves Eq. (7.41).

In order to determine the matrices $\tilde{E}_k$ in Eq. (7.42), we first find an explicit expression relating the standard form matrices E_k and the matrix τ_{AB}. Define the matrix elements of a bipartite matrix H by

$$[H]_{ij,kl} := \langle i|_A \otimes \langle j|_B H |k\rangle_A \otimes |l\rangle_B . \tag{D.12}$$

For subsystem B, we work in the Fock basis, where the rotation operator U_θ is diagonal, with elements

$$[U_\theta]_{jl} = \omega_M^{-j} \delta_{jl}. \tag{D.13}$$

The unitary matrix R in Eq. (D.4), formed by taking powers of U_θ, is also diagonal in this basis, with the following elements:

$$[R]_{ij,kl} = \omega_M^{-i\cdot j} \delta_{ik} \delta_{jl}. \tag{D.14}$$

Therefore, the Fock basis elements of the block circulant matrix $\mathcal{C}(\tau_{AB})$, defined in Eq. (D.5), are given by

$$[\mathcal{C}(\tau_{AB})]_{ij,kl} = \omega_M^{i\cdot j - k\cdot l} [\tau_{AB}]_{ij,kl} \tag{D.15}$$

To get the standard form, we need to perform a Fourier transform on the block circulant matrix $\mathcal{C}(\tau_{AB})$ as in Eq. (D.7). The elements of the discrete Fourier transform F_M are given in Eq. (D.6). After substitution, we arrive at the matrix elements of the standard form:

$$\begin{aligned}
[\mathcal{D}(\tau_{AB})]_{ij,kl} =& \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{n\cdot k - i\cdot m} [\mathcal{C}(\tau_{AB})]_{mj,nl} \\
=& \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-i)+n(k-l)} [\tau_{AB}]_{mj,nl}.
\end{aligned} \tag{D.16}$$

Since $\mathcal{D}(\tau_{AB})$ is block diagonal, $\mathcal{D}(\tau_{AB}) = \bigoplus_{k=0}^{M-1} E_k$, we have

$$\begin{aligned}
[E_k]_{jl} :=& [\mathcal{D}(\tau_{AB})]_{kj,kl} \\
=& \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-k)+n(k-l)} [\tau_{AB}]_{mj,nl}.
\end{aligned} \tag{D.17}$$

This is the final formula linking the elements of τ_{AB} and the matrices $\{E_k\}_{k=0}^{M-1}$. For completeness, the inverse formula is given by

$$[\tau_{AB}]_{ij,kl} = \frac{1}{M} \sum_{m=0}^{M-1} \omega_M^{m(i-k)+k\cdot l - i\cdot j} [E_m]_{jl}. \tag{D.18}$$

When $\tau_{AB}^{T_A}$ is used in this formula instead of τ_{AB}, we find the relation

$$[\tilde{E}_k]_{jl} := \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(j-k)+n(k-l)} [\tau_{AB}]_{nj,ml}. \tag{D.19}$$

Hence, the matrix $\tilde{E}$ indexed by $(j+l-k)$ has elements

$$[\tilde{E}_{j+l-k}]_{jl} = \frac{1}{M} \sum_{m=0}^{M-1} \sum_{n=0}^{M-1} \omega_M^{m(k-l)+n(j-k)} [\tau_{AB}]_{nj,ml}, \tag{D.20}$$

which is the same as Eq. (D.17), after interchanging the summation indices m and n. Therefore, $[\tilde{E}_{j+l-k}]_{jl} = [E_k]_{jl}$ (in the Fock basis).

References

[1] G. Adesso and G. Chiribella. Quantum benchmark for teleportation and storage of squeezed states. *Phys. Rev. Lett.*, 100:170503, 2008.

[2] P. Alberti and A. Uhlmann. A problem relating to positive linear maps on matrix algebras. *Rep. Math. Phys.*, 18:163 – 176, 1980.

[3] P. M. Alberti. Playing with fidelities. *Rep. Math. Phys.*, 51:87 – 125, 2003.

[4] K. M. R. Audenaert and M. B. Plenio. When are correlations quantum?: verification and quantification of entanglement by simple measurements. *New J. Phys.*, 8:266, 2006.

[5] S. A. Babichev, B. Brezger, and A. I. Lvovsky. Remote preparation of a single-mode photonic qubit by measuring field quadrature noise. *Phys. Rev. Lett.*, 92:047903, 2004.

[6] S. M. Barnett and P. M. Radmore. *Methods in theoretical quantum optics.* Oxford University Press, 1997.

[7] Bengtsson and Życzkowski. *Geometry of Quantum States.* Cambridge University Press, 2006.

[8] C. H. Bennett, G. Brassard, C. Jozsa, R. Crépeau, A. Peres, and W. K. Wooters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[9] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[10] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 80:1121–1125, 1998.

[11] D. Bouwmeester, A. Ekert, and A. Zeilinger. *The Physics of Quantum Information*. Springer, Berlin, 2000.

[12] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble. Criteria for continuous-variable quantum teleportation. *J. Mod. Opt.*, 47:267–278, 2000.

[13] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock. Quantum versus classical domains for teleportation with continuous variables. *Phys. Rev. A*, 64:022321, 2001.

[14] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, 2005.

[15] D. Bures. An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite w^*-algebras. *Trans. Am. Math. Soc.*, 135:199, 1969.

[16] J. Calsamiglia, M. Aspachs, R. Muñoz Tapia, and E. Bagan. Phase-covariant quantum benchmarks. *Phys. Rev. A*, 79:050301, 2009.

[17] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Appl. Phys. B*, 72:67–71, 2001.

[18] A. Chefles. Deterministic quantum state transformations. *Phys. Lett. A*, 270:14–19, 2000.

[19] A. Chefles, R. Jozsa, and A. Winter. On the existence of physical transformations between sets of quantum states. *Int. J. Quant. Info.*, 2:11–21, 2004.

[20] M.-D. Choi. Completely positive linear maps on complex matrices. *Lin. Alg. Appl.*, 10:285 – 290, 1975.

[21] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10:526–535, 1974.

[22] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969. Erratum: *ibid* **24**.

[23] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004.

[24] P. J. Davis. *Circulant matrices, 2nd. ed.* AMS Chelsea Publishing, 1994.

[25] M. Ericsson, D. Achilles, J. T. Barreiro, D. Branning, N. A. Peters, and P. G. Kwiat. Measurement of geometric phase for mixed states using single photon interferometry. *Phys. Rev. Lett.*, 94:050401, 2005.

[26] C. A. Fuchs and M. Sasaki. Squeezing quantum information through a classical channel: measuring the "quantumness" of a set of quantum states. *Quant. Inf. Comp.*, 3:377–404, 2003.

[27] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282:706–709, 1998.

[28] R. J. Glauber. Photon correlations. *Phys. Rev. Lett.*, 10:84–86, 1963.

[29] F. Grosshans and P. Grangier. Quantum cloning and teleportation criteria for continuous quantum variables. *Phys. Rev. A*, 64:010301, 2001.

[30] M. Guţă, P. Bowles, and G. Adesso. Quantum-teleportation benchmarks for independent and identically distributed spin states and displaced thermal states. *Phys. Rev. A*, 82:042310, 2010.

[31] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the thirty-fifth annual ACM symposium on theory of computing*, pages 10–19, New York, NY, USA, 2003.

[32] J. Gutierrez-Gutierrez and P. Crespo. Asymptotically equivalent sequences of matrices and Hermitian block Toeplitz matrices with continuous symbols: applications to MIMO systems. *IEEE Transactions on Information Theory*, 54:5671–5680, 2008.

[33] K. Hammerer, M. M. Wolf, E. S. Polzik, and J. I. Cirac. Quantum benchmark for storage and transmission of coherent states. *Phys. Rev. Lett.*, 94(1):150503, 2005.

[34] H. Häseler. *Verschränkungsnachweise mit Anwendungen in der Quantenkommunikation.* PhD thesis, Universität Erlangen-Nürnberg, Erlangen, Germany, 2010.

[35] H. Häseler and N. Lütkenhaus. Probing the quantumness of channels with mixed states. *Phys. Rev. A*, 80:042304, 2009.

[36] H. Häseler and N. Lütkenhaus. Quantum benchmarks for the storage or transmission of quantum light from minimal resources. *Phys. Rev. A*, 81:060306, 2010.

[37] H. Häseler, T. Moroder, and N. Lütkenhaus. Testing quantum devices: Practical entanglement verification in bipartite optical systems. *Phys. Rev. A*, 77:032303, 2008.

[38] A. Hayashi, T. Hashimoto, and M. Horibe. Remote state preparation without oblivious conditions. *Phys. Rev. A*, 67:052302, 2003.

[39] L. Henderson and V. Vedral. Classical, quantum and total correlations. *J. Phys. A*, 34:6899, 2001.

[40] G. Hétet. *Quantum memories for continuous variable states of light in atomic ensembles*. PhD thesis, Australian National University, Canberra, 2008.

[41] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1 – 8, 1996.

[42] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement breaking channels. *Rev. Mod. Phys.*, 15:629, 2003.

[43] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, 2009.

[44] M. Hosseini, G. Campbell, B. M. Sparkes, P. K. Lam, and B. C. Buchler. Unconditional room-temperature quantum memory. *Nat. Phys.*, 7:794–798, 2011.

[45] M. Hübner. Explicit computation of the Bures distance for density matrices. *Phys. Lett. A*, 163:239–242, 1992.

[46] K. Husimi. Some Formal Properties of the Density Matrix. *Proc. Phys. Math. Soc. Jpn.*, 22:264–314, 1940.

[47] J. Řeháček, Z. Hradil, and M. Ježek. Iterative algorithm for reconstruction of entangled states. *Phys. Rev. A*, 63:040303, 2001.

[48] I. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123:257 – 259, 1987.

[49] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Phys. Rev. A*, 64:052312, 2001.

[50] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275 – 278, 1972.

[51] E. Jeffrey, N. A. Peters, , and P. G. Kwiat. Towards a periodic deterministic source of arbitrary single-photon states. *New J. Phys.*, 6:100, 2004.

[52] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41:2315–2323, 1994.

[53] N. Killoran, D. N. Biggerstaff, R. Kaltenbaek, K. J. Resch, and N. Lütkenhaus. Derivation and experimental test of fidelity benchmarks for remote preparation of arbitrary qubit states. *Phys. Rev. A*, 81:012334, 2010.

[54] N. Killoran, H. Häseler, and N. Lütkenhaus. Quantum throughput: Quantifying quantum-communication devices with homodyne measurements. *Phys. Rev. A*, 82:052331, 2010.

[55] N. Killoran and N. Lütkenhaus. Strong quantitative benchmarking of quantum optical devices. *Phys. Rev. A*, 83:052320, 2011.

[56] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[57] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto. Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light. *New J. Phys.*, 8:184, 2006.

[58] J. Lee, M. S. Kim, Y. J. Park, and S. Lee. Partial teleportation of entanglement in the noisy environment. *J. Mod. Opt.*, 47:2151, 2000.

[59] U. Leonhardt. *Measuring the Quantum State of Light*. Cambridge University Press, 1997.

[60] D. W. Leung and P. W. Shor. Oblivious remote state preparation. *Phys. Rev. Lett.*, 90:127905, 2003.

[61] M. Lewenstein, D. Bru, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems-a primer. *J. Mod. Opt.*, 47:2481–2499, 2000.

[62] W.-T. Liu, W. Wu, B.-Q. Ou, P.-X. Chen, C.-Z. Li, and J.-M. Yuan. Experimental remote preparation of arbitrary photon polarization states. *Phys. Rev. A*, 76:022308, 2007.

[63] H. K. Lo. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Phys. Rev. A*, 62:012313, 2000.

[64] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. I. Lvovsky. Complete characterization of quantum-optical processes. *Science*, 322(5901):563–566, 2008.

[65] M. Lobino, C. Kupchak, E. Figueroa, and A. I. Lvovsky. Memory for light as a quantum process. *Phys. Rev. Lett.*, 102:203601, May 2009.

[66] J. Löfberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004. IEEE. Available from http://users.isy.liu.se/johanl/yalmip/.

[67] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection. *Phys. Rev. A*, 74:042326, 2006.

[68] S. Luo. Using measurement-induced disturbance to characterize correlations as classical or quantum. *Phys. Rev. A*, 77:022301, 2008.

[69] A. I. Lvovsky and M. G. Raymer. Continuous-variable optical quantum-state tomography. *Rev. Mod. Phys.*, 81:299–332, 2009.

[70] S. Massar and S. Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74:1259–1263, 1995.

[71] J. A. Miszczak, Z. Puchala, P. Horodecki, A. Uhlmann, and K. Zyczkowski. Sub- and super-fidelity as bounds for quantum fidelity. *Quant. Inf. Comp.*, 9:0103–0130, 2009.

[72] F. Morgan. *Real analysis and applications: including Fourier series and the calculus of variations*. AMS Bookstore, 2005.

[73] R. Namiki. Verification of the quantum-domain process using two nonorthogonal states. *Phys. Rev. A*, 78:032333, 2008.

[74] R. Namiki, M. Koashi, and N. Imoto. Fidelity criterion for quantum-domain transmission and storage of coherent states beyond the unit-gain constraint. *Phys. Rev. Lett.*, 101:100502, 2008.

[75] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge Univ. Press, Cambridge, 2000.

[76] H. Ollivier and W. H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88:017901, 2001.

[77] M. Owari, M. B. Plenio, E. S. Polzik, A. Serafini, and M. M. Wolf. Squeezing the limit: quantum benchmarks for the teleportation and storage of squeezed states. *New J. Phys.*, 10:113014, 2008.

[78] A. K. Pati. Minimum classical bit for remote preparation and measurement of a qubit. *Phys. Rev. A*, 63:014302, 2000.

[79] P. M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, 1970.

[80] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[81] N. A. Peters, J. T. Barreiro, M. E. Goggin, T.-C. Wei, and P. G. Kwiat. Remote state preparation: Arbitrary remote control of photon polarization. *Phys. Rev. Lett.*, 94:150502, 2005.

[82] M. B. Plenio. Logarithmic negativity: A full entanglement monotone that is not convex. *Phys. Rev. Lett.*, 95:090503, 2005.

[83] R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445:65, 2007.

[84] J. Rigas. Detection of prepare & measure entanglement in continuous variable quantum key distribution. Diploma thesis, Universität Erlangen-Nürnberg, Erlangen, Germany, 2006.

[85] J. Rigas, O. Gühne, and N. Lütkenhaus. Entanglement verification for quantum-key-distribution systems with an underlying bipartite qubit-mode structure. *Phys. Rev. A*, 73:012341, 2006.

[86] W. Rosenfeld, S. Berner, J. Volz, M. Weber, and H. Weinfurter. Remote preparation of an atomic quantum memory. *Phys. Rev. Lett.*, 98:050504, 2007.

[87] K. Roszak, P. Horodecki, and R. Horodecki. Sudden death of effective entanglement. *Phys. Rev. A*, 81:042308, 2010.

[88] T. L. Schmidt, K. Børkje, C. Bruder, and B. Trauzettel. Detection of qubit-oscillator entanglement in nanoelectromechanical systems. *Phys. Rev. Lett.*, 104:177205, 2010.

[89] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 1935.

[90] D. Shapira, Y. Shimoni, and O. Biham. Groverian measure of entanglement for mixed states. *Phys. Rev. A*, 73:044301, 2006.

[91] J. Sperling and W. Vogel. Verifying continuous-variable entanglement in finite spaces. *Phys. Rev. A*, 79:052313, 2009.

[92] J. F. Sturm. Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones. *Optim. Meth. Soft.*, 11:625–653, 1999.

[93] E. C. G. Sudarshan. Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Phys. Rev. Lett.*, 10:277–279, 1963.

[94] K. C. Toh, R. H. Tutuncu, and M. J. Todd. SDPT3–a Matlab software package for semidefinite programming. *Optim. Meth. Soft.*, 11:545–581, 1999.

[95] Y. Tokunaga, S. Kuwashiro, T. Yamamoto, M. Koashi, and N. Imoto. Generation of high-fidelity four-photon cluster state and quantum-domain demonstration of one-way quantum computing. *Phys. Rev. Lett.*, 100:210501, 2008.

[96] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[97] A. Uhlmann. Eine bemerkung uber vollstandig positive abbildungen von dichteoperatoren. *Wiss. Z. KMU Leipzig, Math.-Naturwiss. R.*, 34:580–582, 1985.

[98] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto. Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.*, 96:240501, 2006.

[99] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38:49–95, 1996.

[100] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619–1633, 1998.

[101] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275–2279, 1997.

[102] G. Vidal and R. F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002.

[103] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, 1989.

[104] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, 1932.

[105] C. Wittmann. private communication, 2010.

[106] C. Wittmann, J. Fürst, C. Wiechers, D. Elser, H. Häseler, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement over a 2km fiber channel. *Opt. Expr.*, 18:4499–4509, 2010.

[107] W. Wu, W.-T. Liu, P.-X. Chen, and C.-Z. Li. Deterministic remote preparation of pure and mixed polarization states. *Phys. Rev. A*, 81:042301, 2010.

[108] G.-Y. Xiang, J. Li, B. Yu, and G.-C. Guo. Remote preparation of mixed states via noisy entanglement. *Phys. Rev. A*, 72:012315, 2005.

[109] H. P. Yuen and V. W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8:177–179, 1983.

[110] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys. Rev. A*, 79:012307, 2009.

[111] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A*, 58:883–892, 1998.