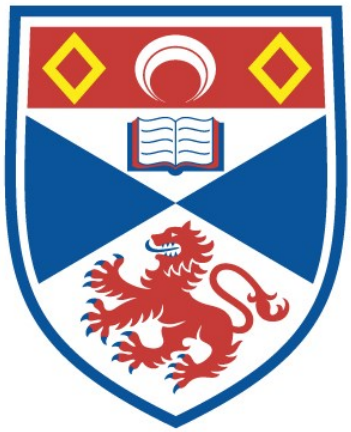
HYBRID ANCILLA-BASED QUANTUM COMPUTATION AND EMERGENT GAUSSIAN MULTIPARTITE ENTANGLEMENT

Victor Manuel Nordgren

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2022

Hybrid Ancilla-Based Quantum Computation
and
Emergent Gaussian Multipartite Entanglement

Viktor Manuel Nordgren

University of
St Andrews

This thesis is submitted in partial fulfilment for the degree of

Doctor of Philosophy (PhD)

at the University of St Andrews

July 2022

Candidate's declaration

I, Viktor Manuel Nordgren, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 40,000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.
I was admitted as a research student at the University of St Andrews in September 2017.
I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 25 / 07 / 2022 Signature of candidate

Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date 26/07/2022 Signature of supervisor

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Viktor Manuel Nordgren, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed copy

No embargo on print copy.

Electronic copy

No embargo on electronic copy.

Date 25 / 07 / 2022 Signature of candidate

Date 26/07/2022 Signature of supervisor

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Viktor Manuel Nordgren, understand that by declaring that I have original research data or digital outputs, I should make every effort in meeting the rsity's and research funders' requirements on the deposit and sharing of research or research digital outputs.

Date 25 / 07 / 2022 Signature of candidate

Permission for publication of underpinning research data or digital outputs

We understand that for any original research data or digital outputs which are deposited, we are giving permission for them to be made available for use in accordance with the requirements of the University and research funders, for the time being in force.

We also understand that the title and the description will be published, and that the underpinning research data or digital outputs will be electronically accessible for use in accordance with the license specified at the point of deposit, unless exempt by award of an embargo as requested below.

The following is an agreed request by candidate and supervisor regarding the publication of underpinning research data or digital outputs:

No embargo on underpinning research data or digital outputs.

Date 25 / 07 / 2022 Signature of candidate

Date 26/07/2022 Signature of supervisor

Abstract

In the first half of this thesis, we present two models of ancilla-based quantum computation (ABQC). Computation in the ABQC models is based on effecting changes on a register through the interaction with and manipulation of an ancillary system. The two models presented enable quantum computation through only unitary control of the ancilla – the ancilla-controlled model (ACQC) – or supplemented by measurements on the ancilla which drive the register transformations – the ancilla-driven model (ADQC). For each of the models, we work on systems which couple two continuous variables (CV) or which are hybrid: the register is formed by two-level systems while the ancilla is a CV degree of freedom.

The initial models are presented using eigenstates of momentum as the ancillas. We move to a more realistic scenario by modelling the ancillas as finitely squeezed states. We find that the completely unitary ACQC contains persistent entanglement between register and ancilla in the finite-squeezing scenario. In the ancilla-driven model, the effect of finite squeezing is to scale the register state by a real exponential which is inversely proportional to the squeezing in the ancilla.

In the second part, we cover work on Genuine Gaussian Multipartite Entanglement (Gaussian GME). We present an algorithm for finding Gaussian states that have GME despite having all two-state reductions separable. This touches on the idea of entanglement as an emergent phenomenon. We determine GME via witnesses which probe only a subset of the state. We therefore referred to them as partially blind witnesses. The algorithm is based on semi-definite programs (SDPs). Such optimisation schemes can be used to efficiently find an optimal, partially blind, GME witness for a given CM and vice versa. We then present results of multipartite states of up to six parties. For the tripartite example, we present two experimental schemes to produce the state using a circuit of beam-splitters and squeezers.

Acknowledgements

First and foremost, I would like to thank my supervisor, Professor Natalia Korolkova. I truly appreciate the support and mentoring you have given me in the past years. Thank you also for the opportunities and encouragement to do science with others including giving me the chance to be part of a collaboration. You also let me value the breadth of qualities which makes a good researcher. I could not have done this without your guidance.
I appreciate everyone who allowed me to improve. Drs. Bernd Braunecker and Brendon Lovett for the yearly guidance and suggestions during the reviews. Also thanks to my examiners Dr. Tommaso Tufarelli and Bernd whose comments have been very useful in improving this thesis. I also extend my thanks to Dr. Sarah Croke, my master's project supervisor who opened the doors to research in quantum physics to me. The company of Margarida and Neil allowed me to appreciate the social part of research. I appreciate the opportunity to have worked with you in your projects, Iason, Adam and Kenny. I hope you saw the joy in research as much as I did during them. I am also thankful to all the undergraduates who I had the privilege to tutor and who reminded me of the joy of thinking about topics I so enjoyed. I would also like to deeply thank the Olomouc group – Dr. Ladislav Mišta, Olga Leskovjanová and Jan Provazník – for the privilege to have been your colleague. Thank you very much, Lada, for hosting me (including during the start of a pandemic) and giving me the opportunity to learn from you. I am also grateful for the environment – physical, social and scientific – created by the people in the Physics and Astronomy department in St Andrews. I extend my thanks to the Head office and the Equality, Diversity and Inclusivity committee for showing me how the well-being of others can be a driving force for decisions. I would also like to acknowledge the researchers in QUISCO who have created a great space to share ideas between the quantum information researchers in Scotland, helping me colour in parts of the map of this amazing field. In the wider scientific community, I extend my gratitude to all participants in conferences and summer schools who I have had the privilege to meet and learn from. I have repeatedly rejoiced in being part of such a wonderful human business that is science.
I say thanks to every single one of you who made my time in St Andrews a truly wonderful one. I say with ease that your love has made my life better. Among others, I start by offering my thanks to my dear flatmate, Ian Shand, for the morning coffees which made it easier to go up in the morning when it was hardest and for being the best office mate in the department and at home. I thank you Vyome for all the love you share and your wonderful company. I am very grateful to Margarida for your company in this journey; even if it was far and irregular (and a pandemic getting in the way), I appreciated your company. I have had the opportunity to enjoy the company of wonderful people. Thanks Steph for sharing all the sandy walks and wilderness trips – long and short, sometimes with *One Man*. Thank you also Veronica and Radim for filling the past year with great company and tasty meals. I look happily back to all the coffees, hugs and games, Rose and Elliot and look forward to the next with wee Ollie! James, thank you for the discussions and conceptualising the practical and abstract and reminding me of the joy of philosophy. I appreciated your joyful company, Kristin, Mari, and Andreas – in Fife and Dundee; next time in Scandinavia! Thank you Philip, Soraya, and Paloma for a ball of a time and allowing me to visit you in the old office. Thank you all for that and much more!
I am also grateful to all in the Buddhist meditation group who have given my the chance to explore interesting ideas with inquisitive people. Particular thanks go to Sam for your clear explanations and guided meditations.
Lastly, I am extremely grateful to my family for all the support. I feel very privileged to be a part of it. Thanks to my parents for supporting me during the pandemic and outwith it. Thank you Claudia and Marc for giving me a roof every time I have needed it. I know that all my siblings would have done the same. Thank you Carla, Rober, Marcos, y Clau for always giving me your unconditional love. I also thank the latest generation: Martina, Matilda, Sebastian and Gabriella for the joy you bring me. Los Amo.

Funding

This work was supported by the EPSRC (grant number 1947916)

Contents

List of Symbols and Abbreviations

Abbreviations

ABQC Model of computation: Ancilla-based, see section 2.2.4

ADQC Model of computation: Ancilla-controlled (unitary ancilla operations control computation), see section 2.2.4.2

ADQC Model of computation: Ancilla-driven (measurements drive computation), see section 2.2.4.1

BCHD Baker-Campbell-Haussdorf-Dynkin relation for combining exponential with non-commuting arguments. See Thm. A.1.

CM Covariance matrix

d.p. decimal places

GBQC Model of computation: Gate-based, see section 2.2.1

GME Genuine multipartite entanglement

MBQC Model of computation: Measurement-based, see section 2.2.2

SDP Semi-definite program

Mathematical groups/sets

$\mathcal{H}_A$ Hilbert space A. Subscript omitted for general statements

$\mathcal{H}_\infty$ Hilbert space of states with continuous observables. Subscript omitted for general statements

$\mathcal{L}(\mathcal{H}_A)$ Space of *linear maps* on Hilbert space $\mathcal{H}_A$, see text after Def. 1.1

C Clifford group of operations that are efficiently simulated with classical resources

$\mathbb{N}$ Set of natural numbers, $0, 1, 2, 3, ...$

$\mathbb{R}$ Set of real numbers

SO($2N$) Group of orthogonal matrices of size $2N \times 2N$ with unit determinant (Special orthogonal group)

Sp($2N, F$) Symplectic group of $2N$ dimensions over the field F. Group of symplectic transformations on N modes with entries in the real field ($F = \mathbb{R}$) (5.37)

Symbols

$[\hat{A}, \hat{B}]$ *Commutator* between operators $\hat{A}$ and $\hat{B}$, see Postulate 6

$\langle\psi|$ Pure state *bra*. Dual to pure state with label ψ

$\hat{a}^\dagger(\hat{a})$ *Creation (annihilation)* operators. Also known as ladder operators, see eq. (1.31)

$\delta(a-b)$ *Dirac delta function*, see Def. A.1

δ_{ab} *Kronecker delta function*, see Def. A.1

$\|\psi\rangle\langle\psi\|$	*projector* onto state $\|\psi\rangle$
$\gamma^{(N)}$	Covariance matrix of state with N modes (5.14)
$\gamma^{(N)}_{ABC}$	Submatrix, corresponding to correlations between modes A, B and C, of covariance matrix of state with N modes
$\hat{U}(\hat{H})$	*Unitary operator* describing time evolution generated by Hamiltonian $\mathcal{H}$, see Postulate 4
$\hat{x}_i, \hat{p}_i$	*Quadratures* (position and momentum) in the i-th mode
$\|\psi\rangle$	Pure state *ket* labelled ψ, see Postulate 1
$\hat{n}$	*Number* operator of excitations in a harmonic oscillator.
Ω	Symplectic form in $XPXP$ ordering (5.8)
$\hat{A}, \hat{B}$	*Operators* representing observable quantities, see Postulate 3
$\hat{x}$, $\hat{p}$	*Quadrature operators* (momentum and position), see eq. (1.36)
$\hat{q}$	*Quadrature operator* (momentum or position), see text after eq. (1.36)
ρ_{ABC}	*Density matrix* acting on spaces A, B and C, see Def. 1.1
Σ	Symplectic form in $XXPP$ ordering ($\Sigma = T\Omega T^T$).
$A \geq B$	Denotes that $A - B$ is positive semidefinite for matrices A and B. The definition is analogous for $\leq, <, >, =$.
N	Number of modes of a multi-mode state

List of Figures

Introduction

Thesis overview

This thesis is written in two parts. Part I concerns models of quantum computation on composite systems where we couple continuous and discrete variables. This allows us to combine the advantages of two different quantum information platforms. Specifically, we consider Quantum Computation with Ancillas on Hybrid Systems. Ancilla-based models of quantum computation (ABQC) have the common feature of delegating some computational load to a secondary system - an ancilla. This native dual-system description makes the ancilla-based models suitable for implementation on hybrid platforms. In this thesis, we use *hybrid* to mean systems composed of a sub-system described by continuous variables (quantum modes) and one described by discrete variables (qubits). Computational models can suffer from being merely abstract mathematical descriptions. The aim here is to include a physics perspective since any computation needs a physical system to be performed. We do this by formulating computation models from interaction Hamiltonians. We take a further step towards a more realistic description of the computational models by extending the computational elements to physically attainable systems.

The second part covers work on Genuine Gaussian Multipartite Entanglement (GGME). We investigate the connection between *local* and *global* entanglement in quantum mechanical systems with continuously varying properties. We find that entanglement can be an emergent property in that it may be missing from the parts but still appears when considering the system as a whole. We do this in the context of Gaussian quantum states. In other words, we find states which are multipartite entangled even though the correlations between any two sub-elements show no sign of entanglement. What is more, it suffices to probe only two-element correlations to infer the existence of entanglement in the whole state. Furthermore, probing of *all* two-element correlations is not required. To infer entanglement we use entanglement witnesses, which are both useful mathematical tools and physical observables connected to efficient measurement schemes to detect entanglement. The goal is thus to find states with the desired properties: Gaussian states with non-entangled two-particle subsystems and whose multipartite entanglement is inferred from witnesses which probe a subset of all correlations. We do the search with a numerical procedure using optimisation programs on semi-definite matrices. The found examples in the realm of Gaussian states are more tolerant to noise compared to their discrete variable counterparts. This carries the promise of the experimental demonstration of the effect and has stimulated us to devise optical circuits which produce the state.

If I would be required to find a common thread between the two parts, it is entanglement as a resource in quantum information technologies. Specifically, we investigate entangling interactions used to perform quantum computation (ABQC) and states with global properties which can be detected from local measurement (GGME). Entanglement has been found to be a resource that sets apart classical and quantum information. It is therefore not surprising that a key component of the computation models presented herein are operations which couple – entangle – different computational elements. Ironically, it is also entanglement which becomes a hindrance when extending the models away from theoretic abstraction. It is a poignant reminder that entanglement comes easily in quantum systems, the crux of quantum information lies in generating the *correct* type of entanglement. In the second part, entanglement takes the role of an end itself rather than a means-to-an-end.

Detailed overview

Part I: Quantum Computation with Ancillas on Hybrid Systems
The goal is to phrase models of quantum computation using ancillas. We introduce the background in chapter 2, starting with a definition of universal computation in section 2.1. In there, we define what a quantum circuit is (section 2.1.2) and how to implement a universal set of transformations. We then present the models of quantum computation, in section 2.2, which lead to the ancilla-based models (ABQC) in section 2.2.4.

The ancilla-based models that form the work in this thesis are presented in chapters 3 and 4. The ancilla-based models are based on either solely unitary control of the ancilla (ACQC, chapter 3) or driven by ancilla measurement (ADQC, chapter 4). The two chapters have the same structure, so the topics and methods are described in more detail in chapter 3. A continuous-variable model of ABQC is derived in section 3.1 (4.1), followed by hybrid ABQC in section 3.2 (4.2). The hybrid models are described by an interaction between a qubit register and continuous-variable ancillas. In this scenario, the ancillas are described by eigenstates of position or momentum. These states are unphysical as they require an infinite amount of energy to be created. We therefore analyse the effect of using physical ancilla states in section 3.3 (4.3).
Part II: Genuine Gaussian Multipartite Entanglement
In chapter 5 we give the background for the research presented in chapter 6. The formalism used in this part is based on symplectic matrices. We go through this mathematical framework in section 5.2. At the same time, we repeat the theory of Gaussian quantum information in this framework. Next, in section 5.3, we briefly return to density matrices and present the classification of multipartite entanglement which is at the core of the part. We then return to the symplectic description in section 5.4. The numerical work is based on a class of optimisation schemes, called Semi-definite programs (SDPs). We therefore give the background required to understand these programs in section 5.5 which are used to formulate procedures to find GME witnesses in section 5.6. Moving closer to the main topics in this part, we introduce the way in which we use graphs to describe witnesses which do not use information of the whole state. This is done in section 5.7.

Moving on to chapter 6, we present the main work done on Gaussian genuine multipartite entanglement (GME). The main research question is if we can find Gaussian states with separable two-party reductions that carry GME which is detected by witnesses that probe only part of the state. To describe these witnesses, we introduce the notion of partially blind entanglement witnesses, using the terminology of trees. This we do in section 6.2. Then, in section 6.3, we derive the search algorithm which finds examples of states with the desired properties. The search algorithm is used to find results of up to six modes, presented in section 6.4. We end the chapter by deriving two optical circuits which may be used to prepare the three-mode examples in section 6.5.

Part III: Appendices
In appendix A we present some useful functions and mathematical results. For the work on the ancilla-based models of quantum computing, we present derivations to main results in the following appendices: appendix B, where we derive the gates for a hybrid ancilla-controlled model; appendix C, where we derive the ancilla-driven gates; appendix D, where the finite-squeezing effects on the CV ADQC are presented; appendix E, where the case of hybrid ADQC is covered. For the work on genuine Gaussian multipartite entanglement, in appendix G we present the example of a Gaussian state proving that two classes (fully inseparable and not biseparable) of GME states are not equivalent. In appendix H we show the equivalence between the two experimental circuits presented in chapter 6.

CHAPTER 1

Elements of Quantum Theory

In this chapter we cover the basics and plunge later into the details required for each of the two main research parts of this thesis. Since we deal with both discrete-variable (DV) and continuous-variable (CV) systems, we note where the two theories differ. Some references used in the preparation of this chapter and throughout the thesis work are the undergraduate quantum theory textbooks by Rae (2007) and Bransden & Joachain (2000), both titled *Quantum Mechanics* [1, 2] along with the more advanced graduate textbook, *Modern Quantum Mechanics* (1993) by Sakurai [3] and, a seminal textbook on quantum computation, *Quantum Computation and Quantum Information* (2000) by Nielsen and Chuang [4].

We start from first principles and define the formalism used in this thesis.

Postulate 1 (Quantum states)**.** A *pure quantum state* is given by a unit vector in a Hilbert space, $|\cdot\rangle \in \mathcal{H}$, called a *ket*. To differentiate between states, we label them with Latin or Greek letters: $|a\rangle, |\phi\rangle$.

Pure states carry no classical correlations. To include such correlations, we need the larger set of *mixed states*. This is done in Def. 1.1 below.

Postulate 2 (Superposition principle)**.** A *superposition* is a linear combination of states and is itself in a possible quantum state. That is, for scalars $\alpha, \beta \in \mathbb{C}$,

$$\alpha |\phi\rangle + \beta |\psi\rangle \in \mathcal{H}, \tag{1.1}$$

with $|\alpha|^2 + |\beta|^2 = 1$ so α and β may be interpreted as *probabilty amplitudes*. We use the common notation $|\alpha|^2 = \alpha^* \alpha$, with α^* the complex conjugate of α. More generally, for $|\psi_j\rangle \in \mathcal{H}$ and $\alpha_j \in \mathbb{C}$, $\sum_j \alpha_j |\psi_j\rangle \in \mathcal{H}$ and $\sum_j |\alpha_j|^2 = 1$. For continuous variables, the sum is to be understood as an integral over j and the parameters α_j become complex functions, $\alpha(j)$.

To each ket $|\phi\rangle$ there is a, unique, corresponding *bra* $\langle\phi|$. In fact, a bra is formally given by the linear map $\langle\cdot| : \mathcal{H} \to \mathbb{C}$ from which one may define the inner product between two kets

$$\langle |\phi\rangle, |\psi\rangle \rangle = \langle\phi|\psi\rangle \in \mathbb{C}, \tag{1.2}$$

using the convention for an inner product $\langle\cdot,\cdot\rangle$. The usual properties of inner products on complex Hilbert spaces hold. In particular

- $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$ where the asterisk denotes the complex conjugate,
- $\mathbb{R} \ni \langle\phi|\phi\rangle > 0$ for all $|\phi\rangle \in \mathcal{H}$,
- $\langle\phi|\phi\rangle = 1$ for normalised $|\phi\rangle \in \mathcal{H}$
- $\langle\phi|\psi\rangle = 0$ if and only if $|\phi\rangle$ is orthogonal to $|\psi\rangle$.

The inner product defines a norm in $\mathcal{H}$ and can be used to normalise a state vector:

$$\frac{|\phi\rangle}{\sqrt{\langle\phi|\phi\rangle}}. \tag{1.3}$$

The term *inner* product suggests that there is an *outer* product. While the inner product maps vectors to scalars, the outer product increases the *dimension* of the object, mapping vectors

to maps on vectors. In terms of bras and kets we write the outer product, denoted by $\times$ between $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ as

$$|\phi\rangle \times |\psi\rangle = |\phi\rangle\langle\psi| . \tag{1.4}$$

The maps $|\phi\rangle\langle\phi|$ are called projectors as they map any $|\psi\rangle \in \mathcal{H}$ to a scalar multiple of $|\phi\rangle$. Projectors will be very important when dealing with measurements in Postulate 5.

Using projectors we can introduce classical mixtures of quantum systems, described by a density matrix.

Definition 1.1 (Density operator)**.** For pure states $|\psi_k\rangle$, a mixed state is an operator given by

$$\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k| , \tag{1.5}$$

with $\sum_k \lambda_k = 1$ and $\lambda_k \in [0, 1]$. We refer to ρ as the *density operator* or *density matrix*.

States described by density operators are said to be *statistical mixtures* of vector states. The weights λ_k are classical probabilities – one may create mixed states with an apparatus outputting randomly one of the states $|\psi_k\rangle$. Density matrices with only one non-zero weight λ_k, in the expansion as per Def. 1.1, are pure and they correspond to a projector.

Note that mixed states are operators acting on $\mathcal{H}$ rather than vectors. Letting $\mathcal{L}(\mathcal{H})$ be the space of linear operators mapping $\mathcal{H}$ to itself, we identify $\rho \in \mathcal{L}(\mathcal{H})$.

Postulate 3 (Observables)**.** Measurable properties are described by operators $\hat{A} \in \mathcal{L}(\mathcal{H})$ which are self-adjoint: $\hat{A}^\dagger = \hat{A}$. The adjoint map or Hermitian adjoint, $(\cdot)^\dagger$, is defined through the inner product: $\langle\phi| (A |\psi\rangle) = (\langle\phi| \hat{A}^\dagger) |\psi\rangle$. We use the terms self-adjoint and *Hermitian* interchangeably[1] .

In finite dimensions, observables allow for a matrix representation. The particular form depends on the vector representation of the basis of $\mathcal{H}$. An example of this is given in section 1.6.1 for two-level quantum systems.

The *eigenvalues* and corresponding *eigenkets*, or *eigenstates* of some operator $\hat{A}$ are all vectors $|a\rangle \in \mathcal{H}$ such that

$$\hat{A} |a\rangle = a |a\rangle , \tag{1.6}$$

with $a \in \mathbb{R}$ (since $\hat{A}$ is self-adjoint).

A useful result is the spectral decomposition of observables. Let $\hat{A} : \mathcal{H} \to \mathcal{H}$ be some observable with non-degenerate eigenvalues. The eigenvectors of $\hat{A}$, $\{|a\rangle\}$, form an orthonormal basis of $\mathcal{H}$, called the *eigenbasis* of $\hat{A}$. Using the projectors of the eigenbasis, we may write the operator in diagonal form, as stated in the spectral decomposition theorem.

Theorem 1.1 (Spectral decomposition)**.** *Let $\hat{A}$ be an operator corresponding to an observable with the eigenvalue equations $\hat{A} |a\rangle = a |a\rangle$ for $a \in \mathcal{F}$. Then we may write $\hat{A}$ in this basis as*

$$\hat{A} = \sum_{\mathcal{F}} a |a\rangle\langle a| , \tag{1.7}$$

with the sum to be understood as an integral whenever $\mathcal{F}$ is a continuous field (for example, $\mathbb{R}$).

[1] In finite dimensions, self-adjoint and Hermitian coincide. In infinite-dimensional spaces, one needs to be more careful (see the chapter on unbounded operators of ref. [5]).

The spectral decomposition may obtained by conjugating with the resolution of the identity in the eigenbasis, $\mathbb{1} = \sum |a\rangle\langle a|$. Luckily, the theorem holds even when the spectrum of $\hat{A}$ is continuous (i.e. $\dim(\mathcal{H}) = \infty$) [6, chap. 7]. That means that for many calculations on infinite-dimensional operators, we can replace sums by integrals over $\mathbb{R}$.

Using the spectral decomposition we can see define functions of operators. Taking the series expansion and using the orthogonality of eigenkets $|a\rangle$, we can define a function of operators from the functions over some field $\mathcal{F}$, $f : \mathcal{F} \to \mathcal{F}$. That is,

$$f(\hat{A}) := \sum_{\mathcal{F}} f(a)\, |a\rangle\langle a| \,. \tag{1.8}$$

This result is very useful when dealing with dynamical equations, which are described by unitary matrices – exponentials of Hamiltonians.

Postulate 4 (Unitary Dynamics)**.** Time evolution of states under Hermitian Hamiltonians is described by the Schrödinger equation:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle \,. \tag{1.9}$$

The resulting action on states is given by unitary transformations $\hat{U} \in \mathcal{L}(\mathcal{H})$ with $\hat{U}^\dagger = \hat{U}^{-1}$.

$$U(\hat{H}) = e^{-it\hat{H}/\hbar}. \tag{1.10}$$

In this thesis, we work with time-independent Hamiltonians. For an interaction time t, the generated evolution due to $\hat{H}$ is [2]

In fact, for any unitary $\hat{U}$, there is a Hermitian $\hat{G}$ such that $\hat{U} = e^{\hat{G}}$ [7].

There is an alternative description of time evolution, called the *Heisenberg picture*, where the time dependence is passed onto the operators. The dynamical equations of a process, described by time-independent Hamiltonian $\hat{H}$, are of the form

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{A} = i[\hat{H}, \hat{A}], \tag{1.12}$$

with solutions $\hat{A}(t) = e^{i\hat{H}t/\hbar}\hat{A}(0)e^{-i\hat{H}t/\hbar} = U\hat{A}(0)U^\dagger$.

Processes described by unitary operators are reversible – one may, in principle, apply the transformation $\hat{U}(-\hat{H})$ to return the system to its initial state.

Measurement in quantum mechanics is destructive and inherently stochastic contrasting classical theory. The trade-off between the amount of information gained and destroyed in a quantum measurement has a formal statement [8] and had a central role since early research into the theory[3].

Postulate 5 (Measurement outcomes)**.** Measurements of some observable $\hat{A}$ in state $|\psi\rangle$ have an expected value given by

$$\langle\hat{A}\rangle = \frac{\langle\psi|\hat{A}|\psi\rangle}{\langle\psi|\psi\rangle}. \tag{1.13}$$

[2] The unitary evolution due to some time-dependent Hamiltonian $\hat{H}(t)$ takes the general form

$$U(\hat{H}) = e^{-i\hat{T}[\int \mathrm{d}t\hat{H}(t)/\hbar]}, \tag{1.11}$$

with $\hat{T}$ the time-ordering operator.

[3] It is interesting to note that this is very much in line with Heisenberg's thought experiment giving rise to the famous error-disturbance relation [9, chap. 2].

The state after a measurement with outcome m is put – collapses – into eigenstate $|m\rangle$, of $\hat{A}$. When the state $|\psi\rangle$ is normalised, the expectation value is simply $\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle$.

Measurements are modelled more generally by so-called positive operator-valued measures (POVM) [7]. POVMs for finite-dimensional Hilbert spaces, are sets of orthogonal projectors, Π_j, which sum to the identity: $\sum_j \Pi_j = \mathbb{1}$.

In presenting the work for this thesis, projective measurements suffice. Measurements may therefore be described by projectors $|m\rangle\langle m|$ with outcome $m \in \mathbb{R}$. The Hermiticity of observables assures that $\langle\hat{A}\rangle \in \mathbb{R}$.

A useful function is used for calculating expectation values is the trace map.

Definition 1.2 (Trace map)**.** The *trace* map, $\mathrm{Tr} : \mathcal{H} \to \mathbb{R}$, is defined as

$$\mathrm{Tr}\left[\hat{A}\right] = \sum_j \langle\alpha_j|\hat{A}|\alpha_j\rangle\,, \tag{1.14}$$

where the states $|\alpha_j\rangle$ form an orthonormal basis of $\mathcal{H}$.

Each term in the sum is the expectation value of $\hat{A}$ in the state $|\alpha_j\rangle$. Note that in the eigenbasis of $\hat{A}$, $\{|a_j\rangle\}$, we have $\mathrm{Tr}\left[\hat{A}\right] = \sum_j \langle a_j|\hat{A}|a_j\rangle = \sum_j a_j$. The trace is basis independent, which can be checked by introducing the identity, resolved in an arbitrary basis, on either side of $\hat{A}$ in eq. (1.26).

1.1 State compositions and reductions

In the most simple case of states formed by multiple uncorrelated degrees of freedom, the *composite* is described by a tensor products of pure states. For states $|a\rangle \in \mathcal{H}_A$ and $|\phi\rangle \in \mathcal{H}_\Phi$ the composite is $|a\rangle \otimes |\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_\Phi$, with a natural extension to larger compositions. At times, when there is no ambiguity, we omit the tensor product symbol, $\otimes$. In terms of density matrices, a *composition* or *extension* of states is given by

$$\rho = \bigotimes_{j=1}^{N} \rho_j := \rho_1 \otimes \ldots \otimes \rho_N \in \mathcal{L}(\mathcal{H}_1) \otimes \ldots \otimes \mathcal{L}(\mathcal{H}_N). \tag{1.15}$$

The Hilbert space on which the composite deinstiy matrix acts is given by $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$.

Just as states may be joined, a *reduction* is given by the removal of sub-states. For this we define the partial trace map

Definition 1.3 (Partial Trace)**.** For some composite system ρ acting on $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_N$, the partial trace over spaces $\mathcal{G} \subset \mathcal{H}$ is the map $\mathrm{Tr}_\mathcal{G} : \mathcal{H} \to \mathcal{H}/\mathcal{G}$ defined by

$$\mathrm{Tr}_\mathcal{G}[\rho] = \sum_\mathcal{G} \langle a_1| \ldots \langle a_G|\,\rho\,|a_G\rangle \ldots |a_1\rangle\,, \tag{1.16}$$

with $\sum_\mathcal{G}$ denoting the sum over the basis of $\mathcal{G}$, $\{|a_1\rangle, \ldots, |a_G\rangle\}$ and $G = \dim(\mathcal{G})$.

For some state $\rho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the partial trace over space B is

$$\mathrm{Tr}_B[\rho_{AB}] = \sum_j \langle b_j|\rho|b_j\rangle\,, \tag{1.17}$$

with $\{|b_j\rangle\}$ a basis of $\mathcal{H}_B$. Tying in to terminology in statistics, we sometimes refer to reductions as *marginals*.

Note that composite states may have a more complicated structure than the examples given here, arising from classical mixing and quantum correlations. In part II, we consider states with the interesting statistical property of possessing multipartite entanglement while only having classical correlations between two-body marginals.

1.2 Entangled states

Quantum states possess types of correlations that cannot be explained by classical probability theory. The most famous quantum correlation is probably entanglement. It also has the reputation of being a quirky feature of quantum systems [10]. It does not therefore help that the current textbook definition of entangled states is done through those which are not entangled[4]. It is useful to start by defining states which are *not* entangled.

Definition 1.4 (Separable pure states)**.** A *separable* state of two parties is one which allows the description

$$|\Psi\rangle = |\psi\rangle_A \otimes |\phi\rangle_B \,, \tag{1.18}$$

where the labels denote the Hilbert space of each sub-system.

Entangled states are defined from these as those which do not allow such a description.

Definition 1.5 (Entangled pure states)**.** A state $|\Psi\rangle$ is entangled if it is not a separable state (Def. 1.4).

For states of more than two parties, there are different classifications of entanglement. Since multipartite entanglement is at the core of part II, we leave out their introduction here.

Some textbook examples of entangled states are the Bell states. Define the ground and excited states of some two-level system as $|0\rangle$ and $|1\rangle$ respectively. With this notation, the qubit Bell states are written as [7]

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right), \tag{1.19}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle\right), \tag{1.20}$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle\right), \tag{1.21}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle\right). \tag{1.22}$$

Even though they are written in the basis $\{|0\rangle, |1\rangle\}$, there is not a basis where $|\Psi^\pm\rangle$ or $|\Phi^\pm\rangle$ may be written as a product state, $|\alpha\rangle \otimes |\beta\rangle$ say. However, proving this is not an easy task in general[5]. The Bell states can be used to form an argument against *hidden variable theories*,

[4] It would be useful to have a positive definition of entanglement highlighting its role as a building block for many quantum informational tasks. I believe that it becomes natural to think of it in positive terms when working with it. Examples of formal phrasings of this are entanglement resource theories. An interesting proposal where entanglement appears as a basic unit is "categorical quantum mechanics" [11, 12]

[5] In the language of complexity theory, determining whether a high-dimensional state is entangled is NP-HARD [13].

where quantum correlations would be stored in a classical, though experimentally inaccessible, hidden variable [14]. For the argument against hidden variable theories, see ref. [7, chap. 5].

To further appreciate the difference between classical correlations and entanglement, we need to consider density matrices. Pure separable states carry no classical correlations.

Definition 1.6 (Bipartite state entanglement)**.** A quantum state ρ on the composite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be *separable* if it can be written as a convex decomposition

$$\rho = \sum_j \lambda_j \rho_j^{(1)} \otimes \rho_j^{(2)} \tag{1.23}$$

with $\sum_j \lambda_j = 1$ ($\lambda_j \geq 0$ for all j) and where the subsystems are given by the density matrices $\rho^{(1)}$ and $\rho^{(2)}$ which act on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively as defined in Def. 1.1. Otherwise ρ is said to be *entangled*.

A state described by a separable density matrix could be prepared by a random choice between states $\rho_j^{(1)} \otimes \rho_j^{(2)}$, with weights given by the classical probabilities λ_j. The description of states produced by such a set-up contain classical correlations (through λ_j) yet no entanglement since all possible states are separable.

We cover entanglement in density matrices in more detail in section 5.3 (Entanglement in terms of density matrices), where the work on Gaussian multipartite entanglement is introduced. For a deeper look into entanglement and its use in quantum information protocols see refs. [4, 7, 15].

1.3 Quantum statistics

Quantum theoretical statements about systems are most often probabilistic and this thesis is no exception. We introduce below some statistical statements that are possible in quantum physics.

The most basic term is the *expectation value*, already introduced in Postulate 5 when describing projective measurements,

$$\langle \hat{A} \rangle = \frac{\langle \psi | \hat{A} | \psi \rangle}{\langle \psi | \psi \rangle}. \tag{1.24}$$

This is also referred to as the *mean* and is the first statistical moment of observable $\hat{A}$ in state $|\psi\rangle$. Expanding $\hat{A}$ via the spectral decomposition theorem, Thm. 1.1, gives

$$\langle \hat{A} \rangle = \sum_j a_j |\langle a | \psi \rangle|^2, \tag{1.25}$$

where we set $\langle \psi | \psi \rangle = 1$ for simplicity (and we assume states to be normalized).

For dealing with mixed states, we calculate the expectation value of some mixed state, ρ, via the trace map from Def. 1.2,

$$\langle \hat{A} \rangle_\rho = \mathrm{Tr}\left[\rho \hat{A}\right]. \tag{1.26}$$

Writing $\rho = \sum_j \lambda_j \left|\psi_j\right\rangle\!\left\langle\psi_j\right|$ and expanding the trace in the eigenbasis of $\hat{A}$, we find

$$\begin{aligned} \mathrm{Tr}\left[\rho \hat{A}\right] &= \sum_k \sum_j \lambda_j \left\langle a_k | \psi_j \right\rangle \left\langle \psi_j \right| \hat{A} \left| a_k \right\rangle \\ &= \sum_j \lambda_j \left\langle \psi_j \right| \hat{A} \Big(\sum_k \left| a_k \right\rangle\!\left\langle a_k \right| \Big) \left| \psi_j \right\rangle \\ &= \sum_j \lambda_j \left\langle \psi_j | \hat{A} | \psi_j \right\rangle, \end{aligned} \tag{1.27}$$

a weighted sum of expectation values. In that, we used the resolution of the identity in the eigenbasis of $\hat{A}$.

Using the expectation value, one may define the second moments – standard deviations and, for multi-particle states, covariances. The *standard deviation* of $\hat{A}$ in normalised state $|\psi\rangle$ is defined as

$$\Delta\hat{A} := \langle\psi| \left(\hat{A} - \langle\psi|\hat{A}|\psi\rangle\right)^2 |\psi\rangle . \tag{1.28}$$

Quantum theory puts a bound to products of variances for non-commuting observables.

Theorem 1.2 (Robertson uncertainty relation)**.** *For two observables, $\hat{A}$ and $\hat{B}$, the following inequality holds*[6] *[17]*

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}\left|\langle[\hat{A},\hat{B}]\rangle\right|. \tag{1.29}$$

This inequality has been called many names but in the uncertainty relations literature it is referred to as the *Robertson uncertainty relation* [17]. As a bound on second moments, Thm. 1.2 is a useful tool for testing entanglement properties of quantum states, most famously by the Peres-Horodecki criterion based on the partial trace.

Theorem 1.3 (Positive partial transpose (PPT) criterion on states)**.** *If a state ρ on Hilbert space $H = H_A \otimes H_B$ is separable, then [18, 19]*

$$\rho^{T_B} \geq 0, \tag{1.30}$$

with $(.)^{T_B}$ the partial transposition map $(\mathbb{1} \otimes \mathcal{T})$ equivalent to transposition T on subsystem $\rho_B = \mathrm{Tr}_A[\rho]$ only (see the discussion preceding Def. 5.16). Whenever $\dim(H) = \dim(H_A)\times\dim(H_B) \leq 6$, this condition is necessary and sufficient [20].

We may see the validity of this theorem by noting that if $\rho = \sum_j \rho_A^{(j)} \otimes \rho_B^{(j)}$, that is, it is separable, then $\rho^{T_B} = \sum_j \rho_A^{(j)} \otimes \rho_B^{(j),T}$. Since the spectra of ρ_B and ρ_A are the same and ρ_B is non-negative, we find that $\rho^{T_B} \geq 0$. A proof for the sufficient condition for 2×2 and 2×3 is not as straightforward and require the results of refs. [21, 22], which show that the partial transposition map[7] in systems of dimension 6 or less may be decomposed in a useful way. The interested reader may refer to refs. [18–22] for more details. Examples of inseparable density matrices with a positive PPT were given in [20].

1.4 Gaussian quantum optics

Quantum optics provides a framework for some of the best described quantum mechanical systems with a privileged position in terms of the proximity between theoretical and experimental work. This close conversation between the two approaches has created a fruitful environment to ask questions about quantum systems.

Although some elements are covered in introductory quantum physics textbooks, there are useful resources focussing on quantum optics. Some used in the work for this thesis are two introductory texts: Leonhardt's *Essential Quantum optics* (2010) [23], and Gerry and Knight's

[6] The initial derivation for the special case of position and momentum was done two years prior, in 1927 by Kennard [16].

[7] In fact, the results were proven in the more general case for completely positive maps.

Introductory Quantum Optics (2004) [24]; the exposition below follows the graduate level textbook, *Methods in Theoretical Quantum Optics* (1997) by Barnett and Radmore [25]. For Gaussian quantum information in particular, I highlight the Serafini's *Quantum Continuous Variables* (2017) [26] and the review articles in refs. [27, 28].

For our purposes, quantum optics plays a central role in both parts. In part I, we use continuous-variable (CV) states (including Gaussian states) to describe CV quantum computational models as well as qubit computation using CV ancillas. In part II, we deal exclusively with Gaussian states. The language used – the symplectic formalism – is introduced in that part, in chapter 5. It is, nonetheless, useful to introduce quantum optical results with more common terminology.

1.4.1 The harmonic oscillator and ladder operators

A fundamental model of quantum optics is the Harmonic oscillator

$$\hat{H}_{H.O.} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) = \hbar\omega\left(\hat{n} + \frac{1}{2}\right), \tag{1.31}$$

with $\hat{a}^\dagger(\hat{a})$ the creation (annihilation) operator increasing (lowering) the number of excitations in the oscillator and $\hat{n} = \hat{a}^\dagger\hat{a}$ the excitation number operator.

The eigenstates of $\hat{n}$, $\{|n\rangle\,|\hat{n}\,|n\rangle = n\,|n\rangle, n \in \mathbb{N}_0\}$, are an orthonormal set which form the Fock-basis[8]. The action of the creation and annihilation operators on the Fock-basis states is

$$\begin{aligned}\hat{a}\,|n\rangle &= \sqrt{n}\,|n-1\rangle, \text{ and}\\ \hat{a}^\dagger\,|n\rangle &= \sqrt{n+1}\,|n+1\rangle,\end{aligned} \tag{1.32}$$

with the additional definition $\hat{a}\,|0\rangle = 0$. Because of their effect of increasing or lowering the excitation number, they are also known as ladder operators. Their commutator is

$$[\hat{a}^\dagger, \hat{a}] = 1, \tag{1.33}$$

where we indicate the identity operator simply as "1" for ease of notation. This commutator may be derived by writing the ladder operators in the Fock basis.

1.4.2 Quadratures[9]

Alongside $\hat{n}$, the most important observables defined from ladder operators are the *quadrature* operators[10]. They are linear combinations of $\hat{a}^\dagger$ and $\hat{a}$ weighted by exponentials of phases $\lambda \in \mathbb{R}$

$$\hat{q}_\lambda := \frac{1}{\sqrt{2}}\left(\hat{a}e^{-i\lambda} + \hat{a}^\dagger e^{i\lambda}\right), \tag{1.34}$$

resulting in Hermitian operators. Quadrature operators that have a phase difference of $\pi/2$ are canonically conjugated (like position and momentum). In particular, their commutator is

$$[\hat{q}_\lambda, \hat{q}_{\lambda+\pi/2}] = i, \tag{1.35}$$

[8] Also known as the number basis.

[9] The route taken in this section follows ref. [25, chap. 3 and app. 4].

[10] The term seems to be an adoption from electrical engineering referring to sinusoids in angle modulation that are 90° off-phase, much like position and momentum are in phase-space. In the Cartesian coordinate system a *quadrature* spans 90°.

so they obey the same uncertainty principle as in Thm. 1.2.

In this thesis, we let $\lambda = 0$ and define the position and momentum quadratures by

$$\begin{aligned} \hat{x} := \hat{q}_0 &= \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}\right), \text{ and} \\ \hat{p} := \hat{q}_{\pi/2} &= \frac{i}{2}\left(\hat{a}^\dagger - \hat{a}\right). \end{aligned} \tag{1.36}$$

We use the symbol $\hat{q}$ for describing either quadrature.

The operators $\hat{x}$ and $\hat{p}$ are different from discrete observables in that it is not possible to construct eigenvectors in the same space in which the operators act: the usual example of infinite dimensional Hilbert space, $\mathcal{H}_\infty$, of states with continuous observable quantities is the space of square-integrable states[11]. To define the eigenstates of the quadratures, we need to go beyond the square-integrable functions and consider generalised functions[12]. Let the states $|x\rangle$ be such that they satisfy the eigenvalue equation

$$\hat{x}\,|x\rangle = x\,|x\rangle\,, \tag{1.37}$$

with $x \in \mathbb{R}$. Then orthogonality does not follow the same rules as for countable spaces – they do not satisfy orthogonality via the Kronecker-delta from eq. (A.2)[13]. Instead, the eigenstates satisfying eq. (1.37) have their overlap given by

$$\langle x|x'\rangle = \delta(x - x'), \tag{1.38}$$

where $\delta(x - x')$ is the Dirac-delta function, given in Def. A.1.

Under this definition, the eigenstates may be used to resolve the identity,

$$\int_{\mathbb{R}} \mathrm{d}x\, |x\rangle\langle x| = \mathbb{1}, \tag{1.39}$$

and may be used to expand any state in $\mathcal{H}_\infty$.

The eigenstates of the momentum quadrature, $|p\rangle$, are similarly defined, with $\langle p|p'\rangle = \delta(p - p')$ and are related to the position eigenstates as Fourier conjugate pairs

$$\langle x|p\rangle = \frac{e^{ixp}}{\sqrt{2\pi}}. \tag{1.40}$$

In many cases, it is clearer to denote whether the basis state is that of position or momentum rather than using the labels. In those cases, we use subscripts to denote this. For example, for two quadrature eigenstates we have

$${}_x\langle a|b\rangle_p = \frac{e^{iab}}{\sqrt{2\pi}}, \tag{1.41}$$

where $\hat{x}\,|a\rangle_x = a\,|a\rangle_x$ and $\hat{p}\,|b\rangle_p = b\,|b\rangle_p$.

Using this labelling, we define the Fourier transformation, $\hat{F}$, by its action on the position and momentum eigenbasis[14]

$$\hat{F}\,|x\rangle_{\hat{x}} = |x\rangle_{\hat{p}} \text{ and } \hat{F}\,|y\rangle_{\hat{p}} = |-y\rangle_{\hat{x}}\,. \tag{1.42}$$

[11] Square-integrability is necessary to calculate probabilities from the probability amplitudes of continuous quantum states.

[12] For a detailed discussion, see [25, App. 4].

[13] One reaches a contradiction if the Kronecker-delta orthogonality is assumed, see [25, App. 4].

[14] For a comparison to the Fourier transform on real functions, see appendix A.2

We end this subsection with a brief discussion on the commutator between the quadratures that might be of interest to the reader. The commutator between two observables can tell us about a number of their important properties. Their role in dynamics is particularly clear in the Heisenberg picture, eq. (1.12). Commutation relations are also central to sequential measurements (Postulate 5) and error-disturbance relations (see footnote 3). Sometimes, the commutator between position and momentum is stated as a postulate.

Postulate 6 (Commutation between conjugate variables)**.** The commutation between the position and momentum operators is

$$[\hat{x}, \hat{p}] = i\hbar. \tag{1.43}$$

Conventionally, one may include the square root of $\hbar$ into the definitions of position and momentum allowing us to set $\hbar = 1$.

However, one may also reach this statement from an analysis of the connection between conjugate variables as generators of transformation in the other[15]. Define a unitary operator which shifts the position of a particle by some amount δx. Call *momentum* the generator of this displacement. The unitary operator describing this action is $U = e^{\frac{i}{\hbar}\delta_x \hat{p}}$ through Postulate 4[16]. We may expand some state $|\delta_x\rangle$ in the momentum eigenbasis, $\{|p\rangle\}$ as $|\delta_x\rangle = \int \frac{\mathrm{d}p}{\sqrt{2\pi}} U_{\delta_x} |p\rangle = \int \frac{\mathrm{d}p}{\sqrt{2\pi}} e^{i\delta_x p} |p\rangle$. Conjecturing that the position operator has the spectral decomposition $\hat{x} = \int x |x\rangle\langle x| \,\mathrm{d}x$, we see that $|\delta_x\rangle$ are the eigenstates of position:

$$\begin{aligned} \hat{x} |\delta_x\rangle &= \int\int \mathrm{d}x\mathrm{d}p \frac{1}{\sqrt{2\pi}} e^{i\delta_x p} x \langle x|p\rangle |x\rangle \\ &= \int \mathrm{d}x \delta(x - \delta_x) x |x\rangle \\ &= \delta_x |\delta_x\rangle , \end{aligned} \tag{1.44}$$

with $\delta(a-b) = \int \mathrm{d}c \exp[i(a-b)c]/2\pi$ the delta function and $\langle x|p\rangle = \frac{e^{ixp}}{\sqrt{2\pi}}$ from the definitions of $\hat{x}$ and $|\delta_x\rangle$ above.

1.4.3 Gaussian superposition of quadrature states

We move on to describe Gaussian states and operations which preserve their Gaussian nature.

A Gaussian state may be written in the quadrature eigenbasis as

$$|\mu, \sigma, c\rangle = \int_{\mathbb{R}} \mathrm{d}x g_{\mu,\sigma,c}(x) |x\rangle_x , \tag{1.45}$$

a superposition of position eigenstates weighted by the normalised Gaussian distribution $g_{\mu,\sigma,c}(x)$ centred at $(\langle x\rangle, \langle p\rangle) = (\mu, c)$ with variance σ. In full detail,

$$g_{\mu,\sigma,c}(x) := \sqrt{N} \exp\left(-\frac{(x-\mu)^2}{4\sigma^2}\right) \exp(ixc), \tag{1.46}$$

with $N = \frac{1}{\sqrt{2\pi\sigma^2}}$ the normalisation function of the square of $g_{\mu,\sigma,c}(x)$[17].

[15] The following arguments follows the forum answer in ref. [29]. See also ref. [30].

[16] Note that this is highly reminiscent of the W. Heisenberg's thought experiment of a measurement apparatus for probing the position of a particle which lead to his phrasing of the famous uncertainty relation between conjugate variables [9, chap. 2].

[17] The square root makes sure that the states are correctly normalised $\langle \mu, \sigma, c|\mu, \sigma, c\rangle = 1$.

The form of the state in the momentum quadrature eigenbasis may be obtained via a Fourier transform or, alternatively, by pre-multiplying the identity resolved in the position eigenbasis to obtain

$$|\mu, \sigma, c\rangle = \frac{e^{ic\mu}}{\sqrt{N}} \int_{\mathbb{R}} \mathrm{d}p \exp\left(-\sigma^2 (p-c)^2\right) \exp(ip\mu) \, |p\rangle_p \,, \tag{1.47}$$

a Gaussian with width $\frac{1}{\sigma}$ centred at c. This relationship between distribution widths exemplifies the uncertainty between Fourier pairs. The global phase $e^{ic\mu}$ does not involve any quadrature and so does not affect the statistics. For a proof of eq. (1.47), see appendix A.3.2.

We use this description of Gaussian states in part I with the simplification of centering the states around null momentum: $c = 0$. In those cases, we write simply $|\mu, \sigma\rangle$.

Note that the state in eqs. (1.45) and (1.47) is situated around null momentum ($\langle \hat{p} \rangle_{\mu,\sigma} = 0$). To take momentum shifts into account, we may introduce a phase term, , in eq. (1.45); a phase term e^{ixc} corresponds to a shift in momentum by c.

Gaussian states formed by multiple harmonic oscillators are described by Gaussian states on composite Hilbert spaces, $\bigotimes_j |\mu_j, \sigma_j\rangle$. Each part is referred to as a *mode* of the state.

Phase-space

Gaussian states have a description in the space spanned by the quadrature eigenvalues (phase-space). While we do not use that formalism, it provides useful interpretational imagery for the effect of operations on Gaussian states. Gaussian states appear like multivariate Gaussian distributions in phase-space. The description is done through quasi-probability functions [25, sec. 4.4], most famously the *Wigner function*, which we do not define here.

In the space spanned by eigenvalues of the quadratures, referred to as phase-space, Gaussian states are described by normal distributions. This is illustrated in fig. 1.1.

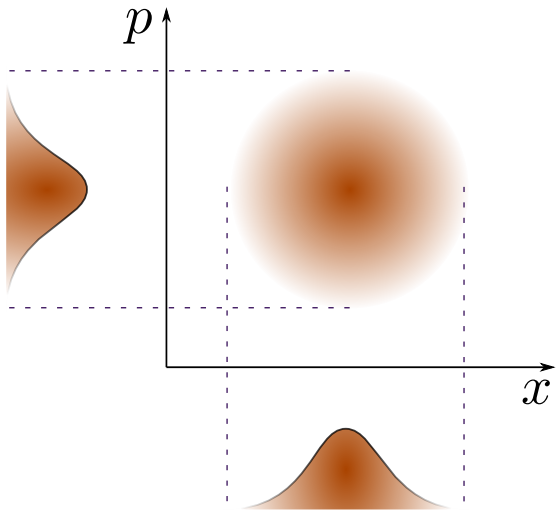


Figure 1.1: Gaussian state in phase-space. The *marginals* onto each quadrature are obtained as univariate Gaussian distributions through projection (dashed lines). Gaussian states of N-modes correspond to multivariate distributions with the variables x_j, p_j for $j = 1, ..., N$.

1.4.4 Gaussian operations

Gaussian operations are those which preserve the Gaussian nature of states. That is, the power in the exponential in eq. (1.46) is, at most, quadratic after the operation. One way of categorising these is by considering the time evolution of the quadratures under various Hamiltonians formed by polynomials in the quadrature operators as in ref. [31].

Recall the time evolution in the Heisenberg picture (eq. (1.12)), $\frac{\mathrm{d}}{\mathrm{d}t}\hat{A} = i[\hat{H}, \hat{A}]$, and the commutator between position and momentum (Postulate 6), $[\hat{x}, \hat{p}] = i$.

We get directly the relation between position and momentum as generators of displacements in each other. For $\hat{H} = \hat{x}$ applied for a duration of time, t, we have the mappings $\hat{x} \mapsto \hat{x}$ and $\hat{p} \mapsto \hat{p} - t$. Similarily, for $\hat{H} = \hat{p}$, we have $\hat{x} \mapsto \hat{x} + t$ and $\hat{p} \mapsto \hat{p}$.

For the effect on Gaussian states however, we are interested in the effect of applying the Hamiltonians $\hat{q}, \hat{q}^2, \hat{q}^3, ...$ on $\hat{q}^m$ for some $m \in \mathbb{N}$. The insight comes from the commutators

$$i[\hat{x}, \hat{p}^m] = -m\hat{p}^{m-1}, \quad i[\hat{p}, \hat{x}^m] = m\hat{x}^{m-1}, \tag{1.48}$$

where the effect of commuting with a linear Hamiltonian is to decrease the polynomial order by one. One may also swap the commutator arguments and see that quadratic Hamiltonians preserve the order while cubic terms increase it by one. Note, though, that momentum is mapped onto position and vice versa[18]. This prescribes a classification of Gaussian operations: those which preserve the order of polynomials of quadratures. Importantly, Gaussian operations preserve Gaussian states. As noted above, it is the operations generated by quadratic (or lower) Hamiltonians.

We now describe some important Gaussian transformations. We have seen that Hamiltonians linear in the quadratures generate linear transformations in the conjugate quadrature. Putting both together, the displacement operator is given by

$$\hat{D}(d_x, d_p) = e^{id_p\hat{x} - id_x\hat{p}}, \tag{1.49}$$

where $d_p, d_x \in \mathbb{R}$ are the momentum and position translations respectively. The effect of a displacement operation on a Gaussian state is to shift the mean by the parameter d_x or d_p in the position and momentum bases respectively. The group formed by displacement operators on N oscillators is called the Heisenberg-Weyl group [32].

Two single-mode transformations generated from quadratic Hamiltonians are the rotating and squeezing operations. These are obtained from the Hamiltonians $\hat{H}_{\mathrm{Rot}} = \frac{1}{2}(\hat{x}^2 + \hat{p}^2)$ and $\hat{H}_{\mathrm{Sq}} = \frac{1}{2}(\hat{x}\hat{p} + \hat{p}\hat{x})$ respectively. The terms come from their effect on the shape of the distribution in phase-space, as seen in fig. 1.3. To see this, consider the unitaries generated from $\hat{H}_{\mathrm{Rot}}$ and $\hat{H}_{\mathrm{Sq}}$. First the unitary describing the application of $\hat{H}_{\mathrm{Rot}}$ for a time $t = \theta$ is

$$\hat{U}_{\mathrm{Rot}}(\theta) = \exp\left(i\frac{\theta}{2}(\hat{x}^2 + \hat{p}^2)\right). \tag{1.50}$$

It is a basis transformation with the following mapping on the quadrature states $\hat{x} \mapsto \cos(\theta)\hat{x} + \sin(\theta)\hat{p}$ and $\hat{p} \mapsto \cos(\theta)\hat{p} - \sin(\theta)\hat{x}$. This can be interpreted as a rotation by θ in phase-space (with axes defined by the quadrature eigenvalues). One may also see that for the choice $\theta = \pi/2$, we obtain the Fourier transform, swapping position and momentum spaces:

$$F := \hat{U}_{\mathrm{Rot}}(\pi/2) = \exp\left(i\frac{\pi}{4}(\hat{x}^2 + \hat{p}^2)\right). \tag{1.51}$$

[18] We have that $i[\hat{p}^2, \hat{x}] = 2\hat{p}$, $i[\hat{x}^2, \hat{p}] = -2\hat{x}$, $i[\hat{p}^3, \hat{x}] = 3\hat{p}^2$, $i[\hat{x}^3, \hat{p}] = -3\hat{x}^2$,

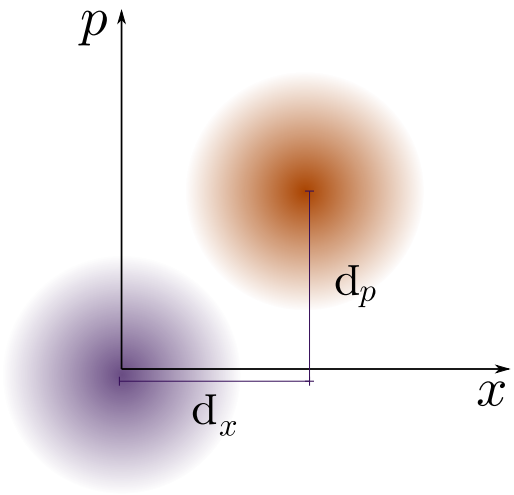


Figure 1.2: Vacuum (purple) displaced by $\hat{D}(d_x, d_p)$ a coherent state (orange) – both Gaussian states.

Next, the Hamiltonian $\hat{H}_{\mathrm{Sq}}$ generates the unitary

$$\hat{U}_{\mathrm{Sq}}(\eta) = \exp\left(i\frac{\eta}{2}(\hat{x}\hat{p} + \hat{p}\hat{x})\right), \tag{1.52}$$

obtained after an interaction time $t = \eta$ with η the *squeezing parameter*. Its effect on the quadratures as a rescaling of the position and momentum quadratures by a factor of $e^{\mp\eta}$ respectively. When $\eta > 0$, we say that the position quadrature is *squeezed* while the momentum is *anti-squeezed*. Note that since the position and momentum quadratures are squeezed and anti-squeezed by the same amount so that the product of variances is not altered by a squeezing operation and therefore the uncertainty principle is not violated by such an operation (given that the pre-squeezed state did not already do so).

An example of a two-mode transformation based on a quadratic Hamiltonian is the unitary describing the action of mixing on a beam-splitter,

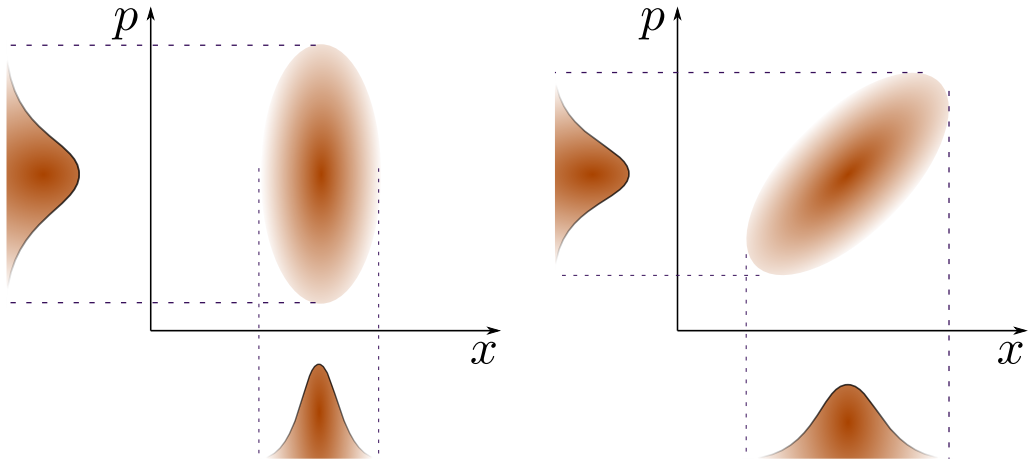
$$\hat{U}_{\mathrm{BS}}(\Theta) = \exp\left(i\frac{\Theta}{2}(\hat{x}_1\hat{p}_2 - \hat{x}_2\hat{p}_1)\right), \tag{1.53}$$

where the subscripts label the mode and $\Theta = t$. A beam-splitter rotates the state in the space spanned by the quadratures $\hat{q}_1$ and $\hat{q}_2$. For an example of the effect of applying such a transformation on state with a pair of oppositely squeezed modes see fig. 1.4.

1.4.5 Non-Gaussian operations

The transformations so far have been at most quadratic polynomials in terms of the quadratures. They are therefore all Gaussian operations, leaving the Gaussian nature of a state intact. Tracking the effect of these can be done in an efficient manner using only classical computers [32][19].

[19] In ref. [32], the authors provide a continuous-variable analogue to the Gottesman-Knill [33] theorem which states the transformations that are simulated classically in an efficient manner.



(a) Single-mode position squeezed Gaussian state.

(b) Rotated single-mode squeezed Gaussian state.

Figure 1.3: One mode of a Gaussian squeezed and rotated, respectively. We depict the rotated state as a previously squeezed one to highlight the effect of rotation.

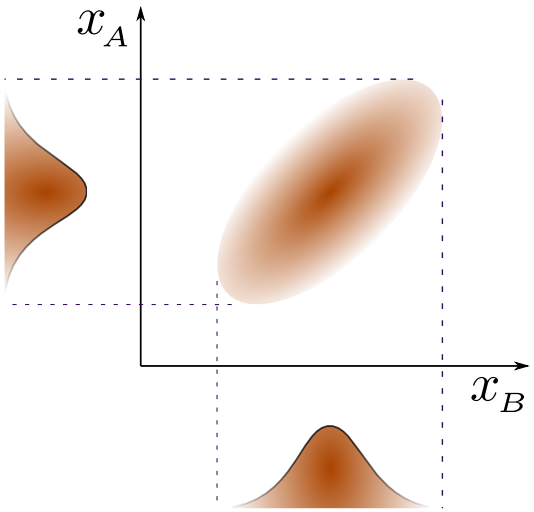


Figure 1.4: Entangled state (Einstein-Podolsky-Rosen) prepared by intereference of two quantum states of opposite squeezing [23, sec 5.1]. Displaced from the origin. The marginals in modes A and B appear as Gaussian distributions.

Thus, we mention two transformations which introduce non-Gaussian elements into a state. The one mentioned in ref. [31] is due to a Kerr non-linearity with Hamiltonian $\hat{H}_{\text{Kerr}} = (\hat{x}^2 + \hat{p}^2)^2$. This Hamiltonian, together with $\hat{x}, \hat{p}, \hat{H}_{\text{Rot}}, \hat{H}_{\text{Sq}}$, generates an algebra which includes all Hamiltonians which are polynomials of the quadratures[20]. The transformation we use in this

[20] This can be seen by noting the following commutators [31], $[\hat{H}_{\text{Kerr}}, \hat{x}] = \frac{i}{2}(\hat{x}^2\hat{p} + \hat{p}\hat{x}^2 + 2\hat{p}^3)$, $[\hat{H}_{\text{Kerr}}, \hat{x}] = \frac{i}{2}(\hat{x}^2\hat{p} + \hat{p}\hat{x}^2 + 2\hat{p}^3)$, $[\hat{H}_{\text{Kerr}}, \hat{p}] = \frac{-i}{2}(\hat{p}^2\hat{x} + \hat{x}\hat{p}^2 + 2\hat{x}^3)$, $[\hat{x}, [\hat{H}_{\text{Kerr}}, \hat{H}_{\text{Sq}}]] = \hat{p}^3$,

thesis is the cubic phase gate – named after the analogous qubit phase gate. The unitary evolution, due to Hamiltonian $\hat{H}_{3,\hat{q}} = \hat{q}^3$ is

$$\hat{U}_{3,\hat{q}}(\gamma) = \exp\left(-i\frac{\gamma}{3}\hat{q}^3\right), \tag{1.54}$$

with $\gamma \in \mathbb{R}$, for $\hat{q} = \hat{x}, \hat{p}$. Its action on the quadratures can be seen by the commutators

$$i[\hat{H}_{3,\hat{p}}, \hat{x}] = \hat{p}^2, \text{ and } i[\hat{H}_{3,\hat{x}}, \hat{p}] = -\hat{x}^2. \tag{1.55}$$

Further, for a general polynomial term $\hat{p}^m\hat{x}^n$,

$$i[\hat{H}_{3,\hat{p}}, \hat{p}^m\hat{x}^n] = -\hat{p}^{m+2}\hat{x}^{n-1}, \text{ and } i[\hat{H}_{3,\hat{x}}, \hat{p}^m\hat{x}^n] = -\hat{p}^{m-1}\hat{x}^{n+2}. \tag{1.56}$$

This means that the unitaries generated by $\hat{x}^3$ and $\hat{p}^3$, together with $\hat{x}$, $\hat{p}$, $\hat{H}_{\text{Rot}}$, $\hat{H}_{\text{Sq}}$, allow the generation of any transformation which can be written as a polynomial in the quadrature operators. This forms the basis for a definition of universal computation in part I, following ref. [31].

1.5 Coupling light to atoms

Apart from describing the quantum properties of light, quantum optics also provides a framework for describing the interaction between light and matter. Since light is the archetype of continuous variable quantum systems and atoms can be used to instantiate discrete variables, understanding their interaction is of utter importance for hybrid quantum technologies. We present here a way of modelling such an interaction using the formalism of quantum optics, following ref. [25, sec. 1.3]. The Hamiltonian derived here, the Jaynes-Cummings Hamiltonian, will form part of the interaction used to derive the models of quantum computation in part I.

A useful approximation of an atom interacting with a field begins by modelling the atom as a dipole[21]. The dipole operator may be written as

$$\hat{\mu} = \mu^*\hat{\sigma}_+ + \mu\hat{\sigma}_-, \tag{1.57}$$

with the action of the two-level operators, $\hat{\sigma}_+$ and $\hat{\sigma}_-$, being to transform between the states $\{|0\rangle, |1\rangle\}$ to the right and to the left respectively. In that basis,

$$\hat{\sigma}_+ := |1\rangle\langle 0| = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \text{ and } \hat{\sigma}_- := |0\rangle\langle 1| = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right). \tag{1.58}$$

The excitations are eigenstates of the Pauli-z matrix,

$$\hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.59}$$

The matrix representation of the other Pauli matrices are given in eq. (1.74).

The interaction of a two-level atom and a classical electric field, $\boldsymbol{E}$, can be described by [25]:

$$\hat{H} = \frac{1}{2}(\omega_1 + \omega_0)\mathbb{1} + \frac{1}{2}(\omega_1 - \omega_0)\hat{\sigma}_z - \mu \cdot \boldsymbol{E}(t)(\hat{\sigma}_+ + \hat{\sigma}_-), \tag{1.60}$$

$[\hat{p}, [\hat{H}_{\text{Kerr}}, \hat{H}_{\text{Sq}}]] = \hat{x}^3$.

[21] This approximation is reasonable whenever the wavelength of the field is much greater than the average separation of the electron and nucleus in the atom [25].

with ω_j, $j = 0, 1$, the energies of the ground and excited state respectively. We have taken $\mu \in \mathbb{R}$ for simplicity. The two first terms in eq. (1.60) are the free Hamiltonian of the dipole.

Moving to the full-quantum picture, we quantize the electric field. This is done by decomposing the field into normal modes and associating a harmonic oscillator to each mode. The observables related to a quantized oscillator are described by the ladder operators, $\hat{a}^\dagger$ and $\hat{a}$, which increase or decrease the excitation number of a continuous-variable quantum state. Using the Harmonic oscillator Hamiltonian, $\hat{H}_{H.O.} = \omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)$, we have the equations of motion[22]

$$\dot{\hat{a}}^\dagger(t) = i\omega\hat{a}^\dagger(t) \tag{1.61}$$

$$\dot{\hat{a}}(t) = -i\omega\hat{a}(t). \tag{1.62}$$

A time-varying electric field operator in one dimension at position r can be quantised as

$$\hat{\boldsymbol{E}}(r,t) = i\left(\frac{\omega}{2\varepsilon_0\mathcal{V}}\right)^{1/2}\varepsilon\left[\hat{a}\exp(-i\omega t + ikr) - \hat{a}^\dagger\exp(i\omega t - ikr)\right], \tag{1.63}$$

with ε_0 the permittivity of free space, $\mathcal{V}$ the quantization volume, ε the linear polarization and k the wave vector in the axis (so $\omega = |k|c$). Placing the atom at the origin, $r = 0$, allows us to obtain the fully quantum version of the **A**tom-**F**ield Hamiltonian in eq. (1.60) as

$$\begin{aligned}\hat{H}_{\text{A-F,Int}}(t) = \\ \frac{1}{2}(\omega_1+\omega_0)\mathbb{1} + \frac{1}{2}(\omega_1-\omega_0)\hat{\sigma}_z - i\lambda\left[\hat{a}\exp(-i\omega t) - \hat{a}^\dagger\exp(i\omega t)\right](\hat{\sigma}_+ + \hat{\sigma}_-),\end{aligned} \tag{1.64}$$

where $\lambda = \mu\varepsilon(\frac{\omega}{3\varepsilon_0\mathcal{V}})$.

We may remove the time-dependence of the field by moving to the Schrödinger picture via the transformation $\hat{U}_{\text{H.O.}} = \exp\left(i\hat{H}_{\text{H.O.}}t\right)$[23]. We have

$$\hat{H}_{\text{A-F}} = \frac{1}{2}(\omega_1+\omega_0)\mathbb{1} + \frac{1}{2}(\omega_1-\omega_0)\hat{\sigma}_z + \hat{H}_{\text{H.O.}} - i\lambda(\hat{a}-\hat{a}^\dagger)(\hat{\sigma}_+ + \hat{\sigma}_-), \tag{1.66}$$

Starting from $\hat{H}_{\text{A-F}}$, we return to the interaction picture through the unitaries $\hat{U}_{\text{H.O}}$ and

$$\hat{U}_0 = \exp\left(\frac{i}{2}\left[(\omega_1+\omega_0+\Delta-2\delta)\,\mathbb{1} + \omega\hat{\sigma}_z\right]t\right), \tag{1.67}$$

where $\Delta := \omega_1 + \omega_0 - \omega$ is the detuning between the atomic transition frequency and the field frequency and $\delta = \Delta/2$. The resulting Hamiltonian in the interaction picture is

$$\hat{H}_{\text{I}} = \frac{\Delta}{2}\hat{\sigma}_z - i\lambda\left[\hat{\sigma}_+\exp(i\omega t) + \hat{\sigma}_-\exp(-i\omega t)\right]\left[\hat{a}\exp(-i\omega t) + \hat{a}^\dagger\exp(i\omega t)\right] \tag{1.68}$$

To obtain the Jaynes-Cummings Hamiltonian [34] we perform the rotating wave approximation which nullifies the explicit time-dependence:

$$\hat{H}_{\text{JC}} = \frac{\Delta}{2}\hat{\sigma}_z - i\lambda\left(\hat{\sigma}_+\hat{a} - \hat{\sigma}_-\hat{a}^\dagger\right). \tag{1.69}$$

We may see that the terms involving $\hat{a}^\dagger\hat{\sigma}_+$ and $\hat{a}\hat{\sigma}_-$ – which do not conserve the excitation number – are strongly suppressed [25, p. 24].

[22] Note that one may be obtained from the other by complex conjugation.

[23] The Hamiltonian in the interaction picture, $\hat{H}_{\text{I}}$, is obtained from the Schrödinger picture's $\hat{H}_{\text{S}}$ through [25, chap. 2]

$$\hat{H}_{\text{I}} = i\dot{\hat{U}}\hat{U}^\dagger + \hat{U}\hat{H}_{\text{S}}\hat{U}^\dagger. \tag{1.65}$$

1.6 Quantum Information

Classical information theory provides a powerful language for science and technology. It paved the way for entirely new fields of study and industries changing the societal landscape tremendously: it is difficult to underestimate the impact of computation and telecommunications on the everyday life of most humans. It has also spawned new interdisciplinary research fields such as bioinformatics [35] as well as providing new tools for established fields such as thermodynamics[24], linguistics[25], cryptography and others.

Any informational task requires a physical system to be performed. There is a link between the physical system and which informational tasks it is suitable for, giving rise to a plethora of evolved biological systems [37, 38] as well as human-created devices [39–42] which perform computations in different ways.

1.6.1 Quantum information with discrete variables

A large part of research in quantum information is using the famous qubits. Qubits are the basic quantum information analogy to the classical bit. They are described by a two-dimensional basis, most often $\{|0\rangle, |1\rangle\}$, and an arbitrary qubit pure state is written as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{1.70}$$

for some $\alpha, \beta \in \mathbb{C}$.

Qubits have been implemented for quantum informational tasks spanning all areas but are most prominent in computing. They have been instantiated in a large variety of physical systems such as trapped ions [43], superconducting circuits [44] and even bosonic systems [45] (to name a few).

Not all qubits are made equal, however. Instantiations vary in ease of manipulation, coherence times (parametrised by information loss due to energy relaxation, t_1, and dephasing, t_2). For example ion traps have been engineered that preserved its quantum informational state for over one hour[26] [46] while two-qubit operation on superconducting qubits has been implemented with a 99% fidelity in 30ns [47].

Bases which are Fourier-like related are very useful when working with quantum information protocols. In the quantum computation setting, the basis $\{|0\rangle, |1\rangle\}$ is usually referred to as the computational basis. Its conjugate is formed by the symmetric and anti-symmetric superpositions of the computational basis. The transformation mapping between the two bases (the qubit analogy of the Fourier transform) is the Hadamard, H.

Definition 1.7 (Hadamard matrix)**.** Using the following vector representation of the computational basis: $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$, $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$; the Hadamard matrix is given by

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.71}$$

The conjugate basis is defined thence

$$|+\rangle := H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle := H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{1.72}$$

The Hadamard is involutory ($H = H^{-1}$) and it therefore also maps the conjugate basis to the computational one. To avoid confusion with a Hamiltonian, we omit the circumflex.

[24] For a use of information science to tackle Maxwell's demon see ref. [36].
[25] For an informational theoretic discussion of redundancy in natural language, please see ref. [7, sec. 1.4].
[26] $t_1 = 12000 \pm 2200s$ and $t_2 = 4200 \pm 580s$.

Single-qubit transformations

Unitary transformations on single qubits in the basis above are, in their most general form, given by [4, sec. 4.2]

$$U = \exp(i\alpha)\exp\left(-i\theta\frac{\mathbf{n}\cdot\boldsymbol{\sigma}}{2}\right), \tag{1.73}$$

with $\alpha, \theta \in \mathbb{R}$, $\boldsymbol{n} \in \mathbb{R}^3$ a unit vector and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, the vector of the Pauli matrices, in turn defined as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.74}$$

The form of eq. (1.73) can be understood as the Pauli matrices, together with the identity, form a basis for Hermitian matrices over $\mathbb{R}$[27]. One may picture this by noting the relationship between $SU(2)$ and rotations on a (Bloch) sphere. The vector $\boldsymbol{n}$ sets the direction of rotation while a non-zero α results in a global phase.

However, we work with another general form of unitary matrices, in particular for the work presented in part I. It comes from rotation about two axes, which we choose to be the axes in the direction of σ_z and σ_x. Thus, any unitary on one qubit may be decomposed as

$$U = e^{i\alpha}e^{i\beta\sigma_z}e^{i\gamma\sigma_x}e^{i\delta\sigma_z}. \tag{1.75}$$

This result is important for the work presented here and goes back to the following theorem.

Theorem 1.4 (Unitary transformations (qubits))**.** *Defining* $J(\frac{\theta}{2}) = He^{i\theta\sigma_z/2}$*, eq.* (1.75) *may be written as [48]*

$$U = e^{i\alpha}J(0)J(\beta)J(\gamma)J(\delta). \tag{1.76}$$

We used that H *is involutory and* $H\sigma_z H = \sigma_x$*.*

Two-qubit transformations

In this thesis we are interested in two-qubit unitaries which couple the two systems. We consider therefore elements of 4×4 unitaries with unit determinant, $SU(4)$. Since we are interested in the non-local unitaries, we do not need elements of $SU(2)\otimes SU(2)$. This smaller space does not require a full basis of 4×4 Hermitian matrices. Instead, we need only a subset of these [49, 50]: $\{\sigma_x\otimes\sigma_x,\ \sigma_y\otimes\sigma_y,\ \sigma_z\otimes\sigma_z\}$

[27] The Pauli matrices span the vector space of 2×2 Hermitian matrices with complex entries over $\mathbb{R}$, $Herm_{\mathbb{C}}(2,\mathbb{R})$: Let N be some arbitrary matrix in $Herm_{\mathbb{C}}(2,\mathbb{R})$. That is $N = \left(\begin{smallmatrix} a & b \\ b^* & a \end{smallmatrix}\right)$. The space spanned by the Pauli matrices (along with the identity) is all the matrices

$$M = \alpha_0\mathbb{1} + \alpha_x\sigma_x + \alpha_y\sigma_y + \alpha_z\sigma_z = \begin{pmatrix} \alpha_0+\alpha_x & \alpha_x - i\alpha_y \\ \alpha_x + i\alpha_y & \alpha_0 - \alpha_x \end{pmatrix},$$

with $\alpha_j \in \mathbb{C}$, for $j = 0, x, y, z$. We may obtain the arbitrary N by setting

$$\alpha_0 = \frac{1}{2}(a+c), \quad \alpha_z = \frac{1}{2}(a-c), \quad \alpha_x = \frac{1}{2}(b+b^*), \quad \alpha_y = \frac{-i}{2}(b-b^*).$$

They are also linearly independent,

$$\alpha_0\mathbb{1} + \alpha_x\sigma_x + \alpha_y\sigma_y + \alpha_z\sigma_z = 0 \iff \alpha_j = 0 \text{ for } j = 0, x, y, z,$$

and are therefore a field. Note that Hermitian matrices are not closed under multiplication by i and do, therefore, not form a vector space over $\mathbb{C}$.

Adding local components, $k_1^{(j)} \otimes k_2^{(j)} \in SU(2) \otimes SU(2)$, $j = 1, 2$, allows us to write any arbitrary $U \in SU(4)$ as [49]

$$U = k_1^{(2)} \otimes k_2^{(2)} \exp\left[i \left(\alpha_x \sigma_x \otimes \sigma_x + \alpha_y \sigma_y \otimes \sigma_y + \alpha_z \sigma_z \otimes \sigma_z\right)\right] k_1^{(1)} \otimes k_2^{(1)}, \tag{1.77}$$

with $\alpha_j \in \mathbb{R}$, $j = x, y, z$.

As mentioned earlier, entanglement is a property of quantum states which is harnessed in informational tasks. In part I, we consider computing models so the question of which transformations allow for the maximum generation of entanglement is important. The answer comes in terms of the parameters $[\alpha_x, \alpha_y, \alpha_z]$. Certain combinations allow for the production of maximally entangled states [49]. In particular $[\pi/4, 0, 0]$, the $CNOT$ gate. We refer to $[0, 0, \pi/4]$ as the controlled-Z, CZ, gate. That is,

$$CZ = \exp\left(i \frac{\pi}{4} \hat{\sigma}_z \otimes \hat{\sigma}_z\right). \tag{1.78}$$

Note that $CZ = H \otimes H \cdot CNOT \cdot H \otimes H$.

1.6.2 Elements of Quantum information with continuous variables

Moving on to continuous variable quantum information, we have introduced most elements in section 1.4 (Gaussian quantum optics). We repeat them here for completeness.

The quantum states of continuous variables which we deal with in this thesis are those which can be expanded in the quadrature eigenbases. A normalised state is thus given, most generally, by

$$|\Psi\rangle = \int_{\mathbb{R}} \mathrm{d}x \psi(x) |x\rangle_x , \tag{1.79}$$

with $\langle\Psi|\Psi\rangle = 1$. The continuous-variable analog of the qubit is called a *qumode*. For Gaussian quantum information we limit the functional form of the superposition coefficients to a Gaussian distribution $\psi(x) = g_{\mu,\sigma}(x)$ (see eq. (1.46)).

CV operations

Just as with states, we differentiate between Gaussian operations and the rest. Gaussian operations are those which preserve the Gaussian character of states. In terms of the generating Hamiltonians, Gaussian operations are those which maintain or lower the polynomial order of products of quadratures (see section 1.4.4).

We repeat the operations most relevant for this thesis below.

The quadrature displacement is given by

$$\hat{D}(d_x, d_p) = e^{i d_p \hat{x} - i d_x \hat{p}}, \tag{1.49 revisited}$$

where $d_p, d_x \in \mathbb{R}$ are the momentum and position translations respectively. Its effect is to shift the position and momentum quadratures by d_x and d_p respectively.

The one-mode rotation and squeezing are

$$\hat{U}_{\mathrm{Rot}}(\theta) = e^{i \frac{\theta}{2} (\hat{x}^2 + \hat{p}^2)} \text{ and } \hat{U}_{\mathrm{Sq}}(\eta) = e^{i \frac{\eta}{2} (\hat{x}\hat{p} + \hat{p}\hat{x})}, \tag{1.50 and 1.52 revisited}$$

respectively. The effect of the rotation is to mix the position and momentum quadrature. In phase-space this amounts to a rotation in the $x - p$ plane. The statistical properties are left invariant by a rotation operation. The squeezing operation alters the variances of the position

and momentum quadrature in inverse proportions. This means that the product of variances, $\Delta\hat{x}\Delta\hat{p}$, is left unaltered. In phase-space, the effect of the squeezing operation is to scale down one quadrature axis by some factor, η_{Sq} say, and scale up the conjugate quadrature by a factor of $1/\eta_{Sq}$.

Two single-mode rotations with interesting interpretations are the *NOT* gate and the Fourier transform, $\hat{F}$. They are given by rotations through π and $\pi/2$ respectively:

$$\hat{F} = \hat{U}_{\text{Rot}}(\pi/2), \text{ and } NOT = \hat{F}^2 = \hat{U}_{\text{Rot}}(\pi). \tag{1.80}$$

We use two Gaussian gates which act on two modes. First we have the beam-splitter interaction:

$$\hat{U}_{\text{BS}}(\Theta) = \exp\left(i\frac{\Theta}{2}(\hat{x}_1\hat{p}_2 - \hat{x}_2\hat{p}_1)\right), \tag{1.53 revisited}$$

where the subscripts label the mode. Its effect is to mix the quadratures in two modes. The phase-space interpretation is a rotation in the spaces spanned by $\hat{x}_1$ and $\hat{x}_2$ as well as $\hat{p}_1$ and $\hat{p}_2$ simultaneously.

We will also use another quadratic gate, which we call the continuous-variable controlled-Z defined as

$$CZ_\infty = \exp(i\hat{x}_1 \otimes \hat{x}_2). \tag{1.81}$$

We omit the subscript or use the symbol CZ_{AR} when there is no risk of confusion with the qubit controlled-Z (eq. (2.8)). The CV controlled-Z gate can be interpreted as a conditional displacement of one qumode, up to an amount depending on the state of the other qumode. That is,

$$CZ_{AB}\,|a\rangle_A = \hat{D}_B(a), \tag{1.82}$$

for some eigenstate of position in the first space, $\mathcal{H}_A$, with eigenvalue $a \in \mathbb{R}$.

A non-Gaussian gate is the cubic phase gate.

$$\hat{U}_{3,\hat{q}}(\gamma) = \exp\left(-i\frac{\gamma}{3}\hat{q}^3\right), \tag{1.54 revisited}$$

with $\gamma \in \mathbb{R}$, for $\hat{q} = \hat{x}, \hat{p}$. Its action on the quadratures is to increase the polynomial order by one. The qubic phase gates also excites statistical moments above the second one meaning that it does not preserve the Gaussian nature of states.

Putting the gates above together, allows one to construct, via commutators, polynomials of arbitrary order in the quadratures.

Part I

Quantum Computation with Ancillas on Hybrid Systems

CHAPTER 2

Background to quantum computation models

Can we perform universal quantum computation on a discrete variable register by driving it using a continuous variable system? We will work within the framework of ancilla-based models of quantum computation (ABQC), which we introduce in section 2.2.4. Before that, we introduce the notion of universal computation on discrete and continuous variables, based on sections 1.6.1 and 1.6.2. We continue, in section 2.2, with a zoo of models of computation which lead to ABQC.

In the next chapters, we phrase ancilla-based models that can be implemented in *hybrid* systems of continuous (CV) and discrete variables (DV). First we derive ancilla-controlled models (ACQC), where only unitary evolution of the ancilla induces gates on the register. We do that in chapter 3. Then, in chapter 4, we present the ancilla-driven model (ADQC). In ADQC, we allow measurements of the ancilla to enact the gates on the register. We present continuous-variable and hybrid models of ADQC. In both chapters we also analyse the effects of treating the continuous-variable ancillas as finitely squeezed states.

The structure is almost identical in both chapters so chapter 3 includes more detailed introduction and discussion of the different themes covered. However, most statements apply to both ancilla-based models. For this reason, chapter 4 is more descriptive in style.

2.1 Universal quantum computation

Universality in quantum computation is the notion that a collection of transformations can be used to generate a much larger set. In fact, a universal set is one which can be used to generate *all* transformations of a given space. We have already encountered this idea in section 1.6 (Quantum Information) when considering qubit and continuous variable operations.

2.1.1 Alphabets, states, and registers

A way to define computation more formally starts by defining the allowed computation values [51]. We define an *alphabet*, Σ, to be a set with elements called *symbols* $\{a \in \Sigma\}$. In classical binary computation, the alphabet is simply $\{0, 1\}$. In quantum computation, the symbols are often taken to be quantum states: any superposition of $|0\rangle$ and $|1\rangle$ for qubits and quadrature basis states, $\{|q\rangle \mid \hat{q}\,|q\rangle = q\,|q\rangle\,, q \in \mathbb{R}\}$ for continuous variables[1]. In general, we define quantum alphabets as sets $\Sigma_d = \{|\psi\rangle \in \mathcal{H}_d\}$, for some Hilbert space $\mathcal{H}_d$ of dimension d. The basis in which alphabets are written is referred to as the *computational basis*. We use the following in this thesis

$$\mathcal{B}_2 = \{|0\rangle\,, |1\rangle\} \text{ and } \mathcal{B}_\infty = \{|x\rangle \mid \hat{x}\,|x\rangle = x\,|x\rangle\,, x \in \mathbb{R}\}, \tag{2.1}$$

where $\mathcal{B}_d$ denotes the basis of Hilbert space with dimension d. The conjugate basis is given by $\{|+\rangle\,, |-\rangle\}$ for qubits (see eq. (1.72)) and the momentum eigenstates for qumodes. The map

[1] For defining universality in continuous-variable quantum computation one limits this space to a certain type of superpositions. See sections 1.6.2 and 2.1.3.2 for more details.

between the computational and conjugate bases are the Hadamard and Fourier transforms for $\mathcal{B}_2$ and $\mathcal{B}_\infty$ respectively.

A *register* is a computer element in which data, in the form of symbols, may be stored or manipulated. Although this definition of a register appears rather abstract, it is worth remembering that it is always instantiated in a physical system. Any number of registers concatenated may be rightly considered as a register. It is therefore useful to have the recursive definition [51]

Definition 2.1 (Register)**.** A *register* is either

- An alphabet Σ_d; or
- A tuple $(\mathcal{R}_1, ..., \mathcal{R}_N)$ of registers $\mathcal{R}_j$, $j = 1, .., N$.

A major difference between classical and quantum computation is that classical registers have determinate values whilst this is famously not the case for quantum registers.

Quantum registers may increase size through composition

$$\mathcal{R} = \mathcal{H}_1 \otimes ... \otimes \mathcal{H}_N, \tag{2.2}$$

for Hilbert spaces $\mathcal{H}_1, ..., \mathcal{H}_N$. Although a register may become entangled during computation so that eq. (2.2) does not exhaustively define registers. A decrease in register size corresponds to a reduction by the partial trace map (Def. 1.3).

Elements which aid computation, but do not store data are referred to as *ancillary* elements – *ancillas* for short. In quantum computation, these are quantum states themselves. The role of an ancilla can span a plethora of tasks. They can be used for communication between computation elements. Ancillas can enact transformations on the register (for example by being one input to a two-element gate). In design decisions, the temporary nature of ancillas may be taken into account. In fact, this is a core point of the ancilla-based models presented in section 2.2.4.

We move on to describe how computation is depicted in quantum circuits.

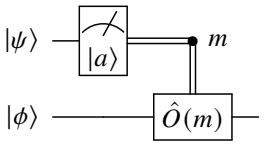
2.1.2 Quantum circuits

We perform computations on registers by manipulating the data they hold. We describe the basic elements of quantum circuits, which we do in the circuit model of computation. We cover a type of computation, unique to quantum computers, based on measurements in section 2.2.2.

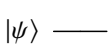
Circuits are two-dimensional depictions of a computation or procedure. The register is positioned in the vertical axis and the horizontal axis is time, although neither is scaled. Information flows in *wires* (fig. 2.1(a)) from left to right. Data is transformed by *gates* (figs. 2.1(b)–(d)), corresponding to quantum operations on the registers. We use the terms *operation* and *gate* interchangeably in this part of the thesis. Gates on a single register element are denoted by boxes while gates on two elements are given by vertical lines connecting two wires.

We separate the space of ancillary states from the register by a dashed line. Gates acting across the spaces are presented in the same way as between two register states as in fig. 2.1(d).

Computation results, even in quantum computers, are real numbers. Read-out of quantum states is done via measurements (Postulate 5). In a circuit, measurement outcomes are transferred as classical information, through a classical wire. A measurement used to control an operation is described by the circuit which follows. It describes the measurement of $|\psi\rangle$ in the basis $\{|a\rangle\}$ with its outcome, m, used to control operation $\hat{O}$ on $|\phi\rangle$.



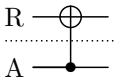
(2.3)



(a) State and wire

(b) Gate on a single register state

(c) Gate between two register states



(d) Gate between register (R) and ancilla (A)

Figure 2.1: Wires and gates for quantum computation.

One point to note is that, while circuits are read left-to-right, the order of operations acting on some register is read right-to-left. As an example, we have the equality

$$|\psi\rangle \;\boxed{\hat{A}}\;\boxed{\hat{B}}\;\boxed{\hat{C}} = \hat{C}\hat{B}\hat{A}\,|\psi\rangle \tag{2.4}$$

Circuits will not always produce exactly the desired operations. However, in many cases the error terms may commute through operations and can be accounted for (for example by a redefinition of the computational basis). A computation is said to be *deterministic* whenever any errors may be corrected in a deterministic manner. Further, it is *stepwise deterministic* if it is deterministic after each computational step.

2.1.3 A universal set of operations

Definition 2.2 (Universal set)**.** For a given Hilbert space $\mathcal{H}$, a *universal set* is a set of quantum operations which can generate all unitaries acting on $\mathcal{H}$, or a given dense subset of it[2].

We say that a set of operations, Ψ, *generates* some other set, Φ, whenever elements in Ψ may be multiplied, possibly with an infinite limit, to give all maps $\phi \in \Phi$. In such case, we refer to Ψ as a generating set or generator of Φ. Recall that, in section 1.4 (Gaussian quantum optics), we saw that a small set of Hamiltonians generated all operators which are polynomial in the quadrature operators through commutation. The relationship between the "generating operation" for Hamiltonians (commutation) and for gates (multiplication) is due to the Baker-Campbell-Haussdorf-Dynkin relation (BCHD) (Thm. A.1).

Definition 2.3 (Universal set)**.** For a given alphabet Σ_d, a *universal set* is a set of quantum operations which can generate $\mathcal{G}(\mathcal{H}_d)$.

In terms of circuits, a set of gates is universal when a circuit composed of only that set can enact any unitary in the relevant Hilbert space [4].

An elementary example from classical binary computation is the $NAND$ (not and) gate which can be shown to be universal by simulating the set $\{NOT, AND, OR\}$. See ref. [4, sec. 3.1.2] for a proof of this.

[2] Especially for CV quantum computation. See for example section 2.1.3.2.

2.1.3.1 Universal Quantum computation on qubits

We need a set of operations which generate unitaries on N qubits. By definition, any universal set may be used to generate any other. In this thesis, we use set of arbitrary single qubit unitaries together with an entangling gate. It turns out that any entangling gate will do for universal computation [52, 53].

We repeat some important results from section 1.6.1 (Quantum information with discrete variables). The transformation between the computational and conjugate basis is given by the Hadamard (Def. 1.7), $H|0\rangle = |+\rangle\,; H|1\rangle = |-\rangle$, with the vector representation of the computational basis

$$H = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right). \qquad \text{(1.7 revisited)}$$

The Hadamard is its own inverse, $H^2 = \mathbb{1}$.

The Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.5}$$

together with the identity generate $SU(2)$.

As noted in Thm. 1.4, the Pauli matrices and the Hadamard allow us to write any single-qubit unitary, up to a global phase, as [48]

$$\hat{U}_1 = \hat{J}(\alpha)\hat{J}(\beta)\hat{J}(\gamma), \tag{2.6}$$

where

$$\hat{J}(\alpha) := He^{i\frac{\alpha}{2}\hat{\sigma}_z}, \tag{2.7}$$

with $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, the Pauli-Z matrix, and $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, the Hadamard transformation.

As for the two-qubit entangling gate, we use eq. (1.77) and set $\alpha_x = \alpha_y = 0$ and $\alpha_z = \pi/4$ to get

$$\hat{U}_2 = \exp\left(i\frac{\pi}{4}\hat{\sigma}_z \otimes \hat{\sigma}_z\right). \tag{2.8}$$

In chapter 3 we show how the set $\{\hat{J}, \hat{U}_2\}$ is enacted in hybrid ancilla-based models.

2.1.3.2 Universal Quantum computation on qumodes

In continuous-variables, one limits the space on which to prove universality. In section 1.6.2, following ref. [31][3], we limited ourselves to the space of operators which can be written as a polynomial in the quadratures, $\hat{x}$ and $\hat{p}$. Note that this is still quite general: being able to simulate such polynomials, allows us, in the infinite limit, to enact any analytic function of operators – those which have a Taylor series expansion.

The register and ancilla states of a continuous-variable quantum computer, expanded in the computational basis - the position eigenstates - are given most generally by $|\psi\rangle = \int_{\mathbb{R}} \mathrm{d}x \psi(x)\,|x\rangle_{\hat{x}}$, with $\hat{x}\,|x\rangle = x\,|x\rangle$, $x \in \mathbb{R}$. The continuous-variable analog of the Hadamard is the Fourier transform, $\hat{F}$ (eq. (1.51)). It maps the computational to the conjugate basis and back by

$$\hat{F}\,|x\rangle_{\hat{x}} = |x\rangle_{\hat{p}} \;\text{ and }\; \hat{F}\,|y\rangle_{\hat{p}} = |-y\rangle_{\hat{x}}\,. \tag{2.9}$$

The Fourier transform is a rotation by $\pi/2$, so from eq. (1.51), we have

$$\hat{F} = \exp\left(i\frac{\pi}{4}(\hat{x}^2 + \hat{p}^2)\right). \qquad \text{(1.51 revisited)}$$

[3] See also [54].

Note that, unlike the Hadamard, the Fourier operator is not involutory, but rather $\hat{F}^4 = \mathbb{1}$. This means that $\hat{F}^2 = (\hat{F}^\dagger)^2$.

The universal set is given by the Gaussian gates and a non-Gaussian one. The Gaussian operations are (eqs. (1.49), (1.50), (1.52) and (1.53)):

$$\begin{aligned}
\hat{D}(d_x, d_p) &= \exp\big(id_p\hat{x} - id_x\hat{p}\big) && d_p, d_x \in \mathbb{R} \\
\hat{U}_{\text{Rot}}(\theta) &= \exp\left(i\frac{\theta}{2}(\hat{x}^2 + \hat{p}^2)\right) && \theta \in [0, 2\pi] \\
\hat{U}_{\text{Sq}}(\eta) &= \exp\left(i\frac{\eta}{2}(\hat{x}\hat{p} + \hat{p}\hat{x})\right) && \eta \in \mathbb{R}^+ \cup \{0\} \\
\hat{U}_{\text{BS}}(\Theta) &= \exp\left(i\frac{\Theta}{2}(\hat{x}_1\hat{p}_2 - \hat{x}_2\hat{p}_1)\right), && \Theta \in [0, 2\pi],
\end{aligned} \tag{2.10}$$

with phase-space interpretations given in figs. 1.2 to 1.4. The non-Gaussian gate used in this thesis is the cubic phase gate:

$$\hat{U}_{3,\hat{q}}(\gamma) = \exp\left(-i\frac{\gamma}{3}\hat{q}^3\right), \tag{1.54 revisited}$$

with $\gamma \in \mathbb{R}$, for $\hat{q} = \hat{x}, \hat{p}$. This gate is required to go beyond quadratic Hamiltonians and beyond classical simulability of CV operations [32].

The Gaussian operations in eq. (2.10) contain both position and momentum terms. We can simplify this further by using the Fourier transform and noting that for some function, f, on operators (see Thm. 1.1 and eq. (1.8))

$$\hat{F}^\dagger f(\hat{p})\hat{F} = f(\hat{x}). \tag{2.11}$$

Particularly important for us is

$$\hat{F}^\dagger e^{i\theta\hat{p}^k}\hat{F} = e^{i\theta\hat{x}^k}, \tag{2.12}$$

for any $k \in \mathbb{N}$ and $\theta \in \mathbb{R}$.

When building a universal set using the commutators between quadrature monomials in section 1.4.4, it suffices to show how to enact the following[4]

$$\begin{aligned}
\hat{F} &= \hat{U}_{\text{Rot}}(\frac{\pi}{2}); \\
\hat{D}(d_p) &= \exp\big(id_p\hat{x}\big), \quad d_p \in \mathbb{R}; \\
\hat{U}_{2,\hat{x}}(\theta) &= \exp\left(i\frac{\theta}{2}\hat{x}^2\right), \quad \theta \in [0, 2\pi]; \\
\hat{U}_{3,\hat{x}}(\gamma) &= \exp\left(i\frac{\gamma}{3}\hat{x}^3\right), \quad \gamma \in \mathbb{R},,
\end{aligned} \tag{2.13}$$

where we defined the quadratic phase gate $\hat{U}_{2,\hat{x}}$. Writing $\hat{U}_{1,\hat{x}}(d_p) = \hat{D}(d_p, 0)$ and using the same parameter θ for all the gates, we may write the short-hand

$$\hat{U}_{\text{k}}(\theta) = \exp\left(i\frac{\theta}{k}\hat{x}^k\right) \text{ for } k = 1, 2, 3. \tag{2.14}$$

The two-mode operation will be fulfilled by the CV controlled-Z operation, which we define as

$$CZ_\infty := \exp(i\hat{x}_1\hat{x}_2), \tag{2.15}$$

[4] For the quadratic unitary, one needs to go to the fourth term in the BCHD formula and retains both rotation and squeezing forms.

which, via the BCHD formula (Thm. A.1), allows to build polynomials of quadrature on N modes as done with the beam-splitter in ref. [31].

The universal set for continuous variable quantum computation we use in this thesis is then

$$\{\hat{F},\ \hat{U}_{\mathrm{k}}(\theta),\ CZ_{\infty} \mid k = 1, 2, 3; \theta \in \mathbb{R} \ \text{ or } [0, 2\pi] \text{ for } k = 2\}. \tag{2.16}$$

2.2 Models of Quantum computation

A computing model is, in its most basic form, a collection of units together with rules for operating on those units. In modern day computers, a computing model is phrased in terms of bits (instantiated by voltage differences in a wire) operated on by boolean gates (implemented by electronic components).

Models of computation can lead to phrasing computation languages which are used to program a universal computer. For example, the classical computation models, λ-calculus and the object model have given rise to functional programming languages such as Haskell and LISP, and object-oriented programming languages respectively [39]. In quantum information, several languages have already been formulated [55], for both continuous [56] and discrete quantum computers [57]. However, a model of computation can also give hints for constructing the physical architecture itself. The models of quantum computation considered in this thesis are examples of this approach. In fact, architectural benefits are arguments passed for the models proposed in refs. [58, 59] which form a basis for the work presented in chapters 3 and 4. We go briefly through a taxonomy of computation models related to the ancilla-based models which are the basis for this part[5].

2.2.1 Circuit- or Gate-based model (GBQC)

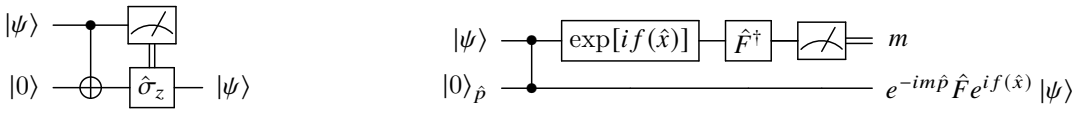
The circuit model [62] is the most familiar one starting from classical computation. Computations are performed by circuits as presented in section 2.1.2. Unitary transformations are thus at the core of GBQC. We will use the language of circuits to describe the protocols for enacting the universal gates in the ancilla-based models.

2.2.2 Measurement based model (MBQC)

Models of quantum computation have fanned out palm-like to include models without a classical analogue. The prime example of this is the measurement-based model [63–65]. Unlike the circuit-based model, the primitives driving computation in MBQC are measurements on entangled states. The back-action due to a measurement of a section of the state leads to an effective transformation of the rest. Measurement outcomes are used to perform corrections - oftentimes a simple redefinition of the computational basis. This may be illustrated by the teleportation circuit [54, 66], given in fig. 2.2. Focusing on fig. 2.2(b), we see that any diagonal unitary, $e^{if(\hat{x})}$, may be performed through manipulation and measurement of an ancilla.

Computation starts by preparation of a resource state called cluster state [63, 67]. Cluster states can be depicted by lattices where each qubit, initiated in the conjugate state $|+\rangle = H|0\rangle$, is situated at a node and an edge between nodes corresponds to an operation $\exp\left(i\frac{\pi}{4}\hat{\sigma}_z\hat{\sigma}_z\right)$ [63]. A circuit is prepared by removing certain qubits through measurement of $\hat{\sigma}_z$. The unmeasured state forms the circuit and computation takes place through successive measurements of the

[5] Since we focus on the ancilla-based models, we do not cover other interesting models such as the adiabatic [60] or topological [61] models of quantum computing.



(a) Qubit teleportation

(b) CV teleportation

Figure 2.2: Qubit [66] and continuous-variable [54] teleportation gates performed by a controlled operation conditioned on the measurement outcome. Qubit circuit starting by a controlled-*NOT* ($\mathbb{1} \oplus \hat{\sigma}_x$, fig. 2.1(c)) while CV initiates with control-Z as defined in eq. (3.5).

remaining qubits. In the case of a two-dimensional lattice, the circuit and measurement-based models share similar diagrams.

The qubit model has been extended to for continuous-variables [54]. Conjugate states of continuous variables, $|p\rangle_{\hat{p}}$, form the lattice with homodyne measurements replacing the Pauli measurements of the DV model. The CV model was show to be fault tolerant for states with squeezing below $20dB$ [68] – a higher degree of squeezing than current state-of-the art squeezing of $15dB$ [69]. However, by encoding logical qubits on a CV system [70], the squeezing threshold for fault-tolerant measurement-based quantum computation was lowered to $12.7dB$ [71].

2.2.3 Qubus model

The measurement-based model uses measurements to create and operate circuits. However, the cluster state architecture limits the interaction to nearest neighbours. The Qubus model [59, 72] was proposed to facilitate gates between separate nodes by adding an ancillary system called a *quantum bus*. Single element gates are thus supplemented by multi-element gates implemented via the bus. Most suitable systems for the bus are so-called flying ancillas, which physically travel between locations in the register, giving a possible advantage over nearest-neighbour interactions. Two methods are presented for the way in which the ancilla produces the gates: via measurement or through entirely unitary means [72].

The Qubus model is phrased for implementation in hybrid systems from the start. The register states can be chosen engineered for information storage with the bus being formed by systems adapted for communication. In fact, Qubus model was presented where the ancilla-register interaction couples a CV system to a qubit via [59]

$$\hat{H}_{\text{Qubus,eff}} = \hbar\chi \left[\hat{a}^\dagger \hat{a}\hat{\sigma}_z + \hat{\sigma}_+\hat{\sigma}_-\right], \tag{2.17}$$

with $\hat{\sigma}_+ := \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $\hat{\sigma}_- := \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, and $\chi \in \mathbb{R}$. The hybrid models presented in chapters 3 and 4 use the Hamiltonian of eq. (2.17) as a primitive. The derivation may be found in in ref. [73].

2.2.4 Ancilla-based models

The ancilla-based models of quantum computation (ABQC) take the idea of delegating computational tasks to the ancilla even further [58, 74–79]. Like the Qubus model, gates between two register elements are effected by an ancilla. In ABQC, even single register gates are applied via manipulation of ancilla states. The interaction between the ancilla and register is required to be unique in the ancilla-based models [58, 78]. This allows for optimising systems when building an ABQC computer. Apart from the interaction with the ancilla, the register can be engineered to be well-isolated from the environment, improving the informational integrity. This is particularly

important, since one of the road-blocks in building a quantum computer is the sensitivity to noise that quantum systems exhibit.

The ancilla models describe systems which have a natural bi-partitioning. A computer built using such a divided system has two main elements: the register space R and the ancilla space A. Computations in the register are performed through interaction with the ancilla followed by ancilla manipulation. The ancillas are either measured (ADQC) or allowed to further interact with the register leading to their disentanglement. Schematics of the ancilla-based models are presented in fig. 2.3.

Definition 2.4 (Ancilla-based model of quantum computation)**.** An ancilla-based model is defined by

- Register states $|\psi\rangle \in \mathcal{H}_R$;
- Ancilla states $|a\rangle \in \mathcal{H}_A$;
- A *unique* register-ancilla interaction, E_{AR}; and
- A universal set of operations on the register using only E_{AR} and ancilla manipulation (including measurements for ADQC).

Whenever $dim(\mathcal{H}_R) \neq dim(\mathcal{H}_A)$, we call the model *hybrid*, otherwise we refer to it by the dimension of $\mathcal{H}_R$, or as *homogeneous*.

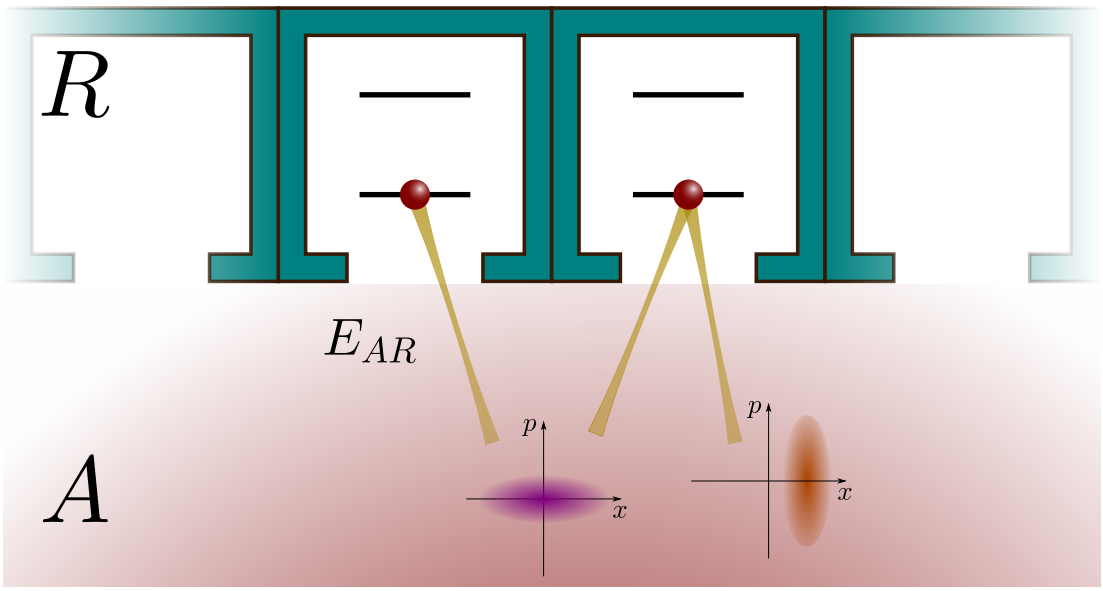


Figure 2.3: Schematic of ancilla-based models on hybrid quantum systems. The register states are depicted as two-level systems which are well-isolated from the environment (teal boxes). The unique interaction, E_{AR}, allows the register to interact with the ancillas (red shaded region). The ancillas are given as continuous-variable states, described as Gaussian states in phase space (see section 1.4.3). Operations on the register are implemented by measuring the ancilla in the ancilla-driven model [75, 78], while only unitary control of the ancillas are required in the ancilla-controlled model [78].

The ancilla-register operation is of the form

$$E_{AR} = \hat{k}_A^{(2)} \hat{k}_R^{(2)} \hat{U}_{\mathrm{AR}}(\hat{H}_{\mathrm{AR}}) \hat{k}_A^{(1)} \hat{k}_R^{(1)} \tag{2.18}$$

where $\hat{k}_A^{(j)} \in \mathcal{L}(\mathcal{H}_A)$, and $\hat{k}_R^{(j)} \in \mathcal{L}(\mathcal{H}_R)$, $j = 1, 2$, local gates on the ancilla and register spaces respectively. The non-local term, $\hat{U}_{\mathrm{AR}}(\hat{H}_{\mathrm{AR}})$, is the unitary generated by the interaction Hamiltonian $\hat{H}_{\mathrm{AR}}$. The symbol, E_{AR}, of the ancilla-register operation is chosen to allude to the fact that the register and ancilla states are entangled in the hybrid scenarios presented in chapters 3 and 4.

We begin with the ancilla-based model which uses ancilla measurements to perform computations.

2.2.4.1 Ancilla-driven quantum computation (ADQC)

The ancilla-driven model of quantum computation carries traces of all the models presented above [58, 75–77]. Measurements drive computation and manipulation of the register is limited to the unique interaction with ancillas.

The relationship to MBQC is more than only through measurement. Each computation step in the ADQC model can be thought of as a minimal computation in a measurement-model – whenever the ancilla only interacts once with up to two register states, the two models are equivalent [80]. Their equivalence can be highlighted by phrasing computations in ADQC as procedurally generated cluster states[6]. Despite their equivalence in ideal conditions, the two models do not share noise resilience properties with the ADQC outperforming in a number of noise scenarios [81].

A particular model of Qubit ADQC is defined by [58]

- Register states and ancilla states $|\psi\rangle, |a\rangle \in \mathcal{H}_R$, with $dim(\mathcal{H}_R) = 2$;
- Ancilla states prepared in the conjugate basis element $|+\rangle$;
- The ancilla-register interaction
$$E_{AR} = H_A H_R C_{AR},$$
with $C_{AR} := \mathbb{1}_4 - 2\,|11\rangle\langle 11|$;
- A universal set of operations given by eqs. (2.19) and (2.20) below.

Comparing to the general form in eq. (2.18), we may identify $\hat{k}_A^{(2)} = \hat{k}_R^{(2)} = H$, $\hat{U}_{\mathrm{AR}}(\hat{H}_{\mathrm{AR}}) = C_{AR}$, and $\hat{k}_A^{(1)} = \hat{k}_R^{(1)} = \mathbb{1}$.

The universal set $\{\hat{J}, \hat{U}_2\}$ from eqs. (2.7) and (2.8) can be produced in the qubit ancilla-driven model [58]. The single-qubit gate may be obtained through the following operations on the ancilla:

$$_A\langle m|\, \hat{J}_A(\beta) E_{AR}\, |+\rangle_A = \hat{\sigma}_{x,R}^m \hat{J}(\beta), \tag{2.19}$$

where the measurement is performed in the computational basis, $m = 0, 1$ and the subscripts denote the spaces of the ancilla or register. The $\hat{\sigma}_{x,R}^m$ is an error term that depends on the ancilla measurement outcome. Due to the random nature of measurement, this term is intrinsic to the model. However, the errors may be removed by a redefinition of the computational basis at the next step of computation [58]. Hence, despite the probabilistic nature of quantum measurements, ADQC can be seen as a stepwise deterministic model.

The two-qubit gate onto register states, labelled by R_1 and R_2, is implemented through

$$_A\langle y_m|\, E_{AR_1} E_{AR_2}\, |+\rangle_A = \hat{\sigma}_{x,R_1}^m \otimes \hat{\sigma}_{x,R_2}^m C_{R_1 R_2}. \tag{2.20}$$

Once again, the error terms may be removed by a redefinition of the computational basis, for example, by changing the measurement basis of the next operation.

[6] For this reason, ADQC has been referred to as *sequential MBQC* [80, 81]

More generally, universal qubit ADQC models with deterministic correction of errors are built from ancilla-register interactions which are locally equivalent to the following ancilla-register interaction unitaries [58, 74]:

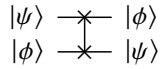
$$C = \mathbb{1}_4 - 2\,|11\rangle\langle 11| \;\text{ or }\; C + SWAP = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| - |11\rangle\langle 11|\,. \tag{2.21}$$

It was shown that hybrid ancilla models, where the register and ancilla spaces are such that $dim(\mathcal{H}_A) > dim(\mathcal{H}_R)$, are not stepwise deterministic. Rather, error terms may be corrected only probabilistically [76]. In chapter 4 we will see how this comes up in a specific hybrid model.

2.2.4.2 Ancilla-controlled quantum computation (ACQC)

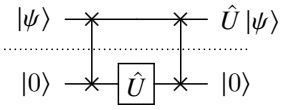
Ancilla-controlled quantum computation models take a step away from MBQC by allowing only unitary control of the ancillas: they are no longer destroyed by measurements [76, 78–80].

Ancilla-controlled quantum computation in platforms where the register and ancilla are of the same type offer a simple model based on the $SWAP$ gate. The $SWAP$ gate is defined by its action on any two states, $|\phi\rangle, |\psi\rangle \in \mathcal{H}$, and is denoted by two crosses as given in the following circuit:

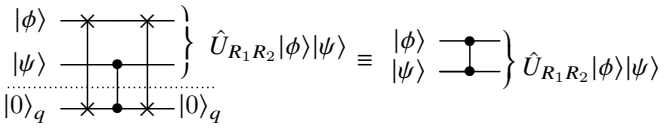


(2.22)

ACQC with $E_{AR} = SWAP$ proceeds by moving the state of the register onto the ancilla where it may be manipulated. For this, see the one and two-element gates



(2.23)



(2.24)

In this thesis, we present the two flavours of ABQC by deriving models starting from interaction Hamiltonians. For the measurement-driven model, CV and hybrid models have been investigated in a general form [76]. On the other hand, only the homogeneous CV or DV cases have been considered for the unitary controlled model. In chapter 3 we present ACQC models on continuous and hybrid variables, deriving them from Hamiltonians. The preparation of quadrature eigenstates require infinite squeezing (and therefore energy) and are therefore unphysical. For this reason, we also present an analysis of the impact of finite squeezing for all models derived.

CHAPTER 3

Ancilla-based computation controlled by unitary manipulation of the ancilla

The content of this chapter is unpublished work.
The ACQC models presented in sections 3.1 and 3.2.0.1 were introduced in the master's thesis from ref. [82]. My addition to those sections was to provide more details and a cleaner derivation of the gateset presented; expanded qualitative statements – for example on suitable experimental platforms and the set-up in fig. 3.2. I further expanded the analytic work by deriving the hybrid model in section 3.2.0.2; performing the finite-squeezing analysis in section 3.3 as well as adding an argument for the requirement of having two ancillas in the hybrid scenarios. I also included one statement stemming from a master's thesis which I co-supervised - this is highlighted with a footnote.

In this chapter we present models of the ancilla-controlled quantum computation [78, 80] as introduced in section 2.2.4.2. First we present a homogeneous continuous-variable model based on the CV *SWAP*. Then, in section 3.2, we move on to the hybrid variable scenario and derive two models based on interaction Hamiltonians that couple qubits with continuous variables. Moving away from the unphysical quadrature eigenstates, in section 3.3 we perform a finite-squeezing analysis of the derived models.

3.1 Continuous variable ACQC

In the homogeneous model presented here, the ancilla and register are both parametrised by continuous variables. In what follows, the register states are left generic,

$$|\psi\rangle = \int_{\mathbb{R}} \mathrm{d}x \psi(x) \, |x\rangle \, , \tag{3.1}$$

the ancillas are all initialized as the eigenstate of position with zero eigenvalue. That is,

$$|A\rangle = |0\rangle_{\hat{x}} \, . \tag{3.2}$$

We now show that one may write a universal model based on the CV *SWAP* gate [83]. It may be constructed by the one and two-mode rotation gates from section 1.4.4 (Gaussian operations) as

$$SWAP := NOT_A B_{AR}(\pi/2), \tag{3.3}$$

where NOT_A and B_{AR} are single and two qumode rotations respectively, given by

$$\begin{aligned} NOT_A := \hat{U}_{\mathrm{Rot}}(\pi) \; &= e^{i\frac{\pi}{2}(\hat{x}_A^2+\hat{p}_A^2)}, \text{ and} \\ B_{AR}(\pi/2) := \hat{U}_{\mathrm{BS}}(\pi/2) &= e^{i\frac{\pi}{2}(\hat{x}_R\hat{p}_A-\hat{p}_R\hat{x}_A)}, \end{aligned} \tag{3.4}$$

using the definitions in eqs. (1.53) and (1.80). Recall that the subscripts, A and R, denote that the operation acts on the ancilla and register spaces respectively. The action of NOT_A is given by the following map: $|a\rangle_{\hat{q}} \mapsto |-a\rangle_{\hat{q}}$, for $\hat{q} = \hat{x}, \hat{p}$.

The $SWAP$ is not sufficient to enact entangling gates between two register modes. For the required two-mode interaction we use the CV CZ:

$$CZ_{AR} := \exp(i\hat{x}_A\hat{x}_R). \tag{3.5}$$

We can, therefore, use that the ancillas are prepared as position eigenstates with null eigenvalue to function as a switch for the entangling interaction: $CZ_{AR}\,|0\rangle_{\hat{x}} = \mathbb{1}$.

We define the ancilla-register entangling interaction using eqs. (3.3) and (3.5) as

$$E_{AR}^{CV-CV} = SWAP_{AR}CZ_{AR} \tag{3.6}$$

Note that the only local gate is the NOT_A on the ancilla (comparing with the general form of the ancilla-register interaction in eq. (2.18), we have the other local gates $\hat{k}_A^{(1)} = \hat{k}_R^{(2)} = \hat{k}_R^{(1)} = \mathbb{1}$). The circuit corresponding to the ancilla-register interaction is given in fig. 3.1.

The elements of the $SWAP$ gate may be understood by their action on the quadratures. The local NOT_A is a rotation in phase-space by π, equivalent to two Fourier transforms, mapping $q_A \to -q_A$. Meanwhile, $B_{AR}(\pi/2)$ is a rotation (and twist) of the quadratures between two modes: the ancilla and register quadratures are swapped with a factor of -1 appearing in the register. Writing the position quadratures of the ancilla and register as a vector with entries in that order, we have

$$\begin{pmatrix}\hat{x}_A\\ \hat{x}_R\end{pmatrix} \xrightarrow{B(\pi/2)} \begin{pmatrix}-\hat{x}_R\\ \hat{x}_A\end{pmatrix}. \tag{3.7}$$

Putting the two together gives the expected $SWAP$ operation.

Using that the CZ_{AR} is effectively an identity when it involves the ancilla in its initial state, we find that the ancilla-register interaction gives

$$\begin{aligned} E_{AR}\,|A\rangle\,|R\rangle &= SWAP_{AR}CZ_{AR}\,|0\rangle_{q,A}\,|\phi\rangle_R \\ &= SWAP_{AR}\,|0\rangle_{q,A}\,|\phi\rangle_R \\ &= |\phi\rangle_A\,|0\rangle_{q,R}\,. \end{aligned} \tag{3.8}$$

The need for the CZ_{AR} gate becomes clear when enacting the two-register gate (see eq. (3.10) below).

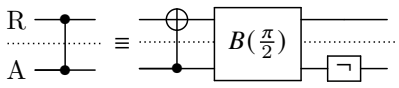


Figure 3.1: CV-CV ACQC basic interaction definition, E_{AR}. The gates label $B(\frac{\pi}{2})$ and ¬ correspond to the beam-splitter with phase $\pi/2$ and the NOT gate respectively.

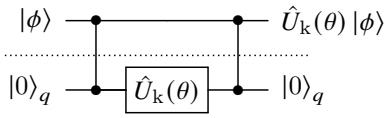
Next we show how to use the ACQC model to produce the following universal gates for continuous variable quantum computation

$$\left\{\hat{F},\ \hat{U}_{\mathrm{k}}(\theta) = \exp\left(i\frac{\theta}{k}\hat{x}^k\right),\ CZ_\infty = \exp(i\hat{x}_1\hat{x}_2)\right\}, \tag{3.9}$$

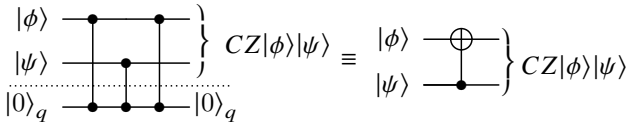
for $k = 1, 2, 3$, as given in eq. (2.16) in section 2.1.3.2.

Gates for CV-CV ACQC

The gates used for the ACQC model presented here are based on the fact that the ancilla-register interaction is equivalent to a $SWAP$ whenever one of the states is the zero position eigenvalue. Thus, the single mode gates are enacted without local operation of the register by moving the information onto the ancilla where the desired gate is implemented:



The two-mode gate follows a similar procedure by first swapping the ancilla and one register state before interacting with a second register state. The information still contained in the ancilla is returned to its original mode effecting a control-Z between the two register states. The circuit and its effective action on the register is



(3.10)

Note that for gates on both one and two modes, the ancilla is preserved in its initial state after computation. This opens up the possibility of reusing the ancilla during computation. This would be more economical in preparation resources and allow for an architecture as presented in fig. 3.2.

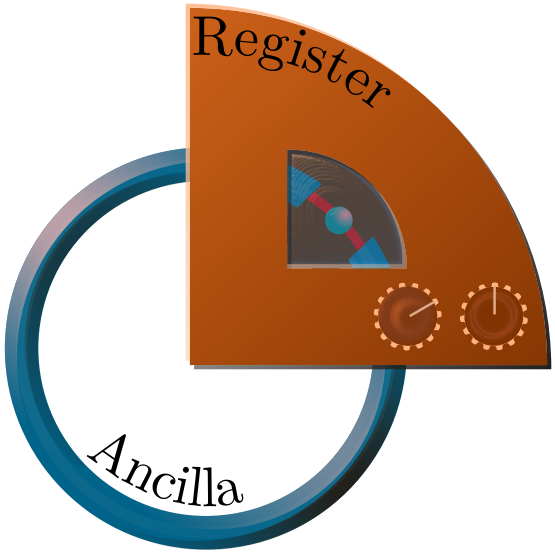


Figure 3.2: Diagram of a possible quantum computer architecture with a reusable flying ancilla. Gates on the register elements – here depicted as a sphere – are implemented by each pass of the ancilla. The flying ancilla could be reused to perform computation through the CV and hybrid ancilla-controlled models presented in this chapter.

Summary of CV ACQC

We have presented a model of quantum computing which allows for deterministic computation on a register which is accessed only via an ancillary state. Furthermore, the ancilla is left unchanged after the computation, leaving the option for architectures that are more economical in terms of ancilla preparation. An important factor is the relationship between the informational lifetime in the ancilla and gate times. As noted earlier, the ancilla and register need not be the same physical platform. For example, one may couple an optical system to a mechanical resonator [84], a superconducting circuit to mechanical resonator inside a cavity [85, 86] or a cantilever with the position and momentum of a trapped ion [87]. Due to long coherence times and fast gate operations, these platforms lend themselves readily for register implementation. Meanwhile, beneficial characteristics of ancillas include ease of manipulation to mobility. For this, optical systems are particularly well suited [88, 89]. Other CV systems, such as microwaves, have seen use for interfacing processing elements internally and with communication platforms [90].

3.2 Hybrid variable ACQC

A main theme of this report is that of taking a step toward practical implementation of the ACQC model. Future quantum computers are likely to be hybrid systems made up of different physical platforms [84]. Qubit systems are maturing for use in computational tasks and it is therefore natural to discuss computation on qubits. Platforms implementing qubits span many areas of research such as superconducting circuits [91–95], ion traps [43, 96–100] and photonic systems [101–103], to name a few, possibly by combining a number of them. For example, using superconducting circuits for calculations and ion traps for memories, as suggested in [84, 104, 105].

For useful computation, information needs to be transferred between separate components. Continuous variable systems are well-suited for this task and have seen application in quantum communication protocols – see citing articles of ref. [106]. They can therefore serve the role of ancillas in ACQC. Earlier in this thesis, quadratures of light have been discussed as an example of continuous degrees of freedom. Other examples include the motion of mechanical oscillators [86, 107–109] and the position and momentum of trapped ions [104, 105].

Here we present models of computation, within the ACQC umbrella, suitable for hybrid systems where the register is made up of qubits and the ancillas are continuous. We give two particular examples where the register is coupled quadratically or linearly to the ancilla's quadrature operators.

A model that gives rise to both Hamiltonians considered below is the Jaynes-Cummings model [110]. The linear case follows directly while the quadratic Hamiltonian is a special case of the model, taken to the dispersive regime.

3.2.0.1 Quadratic Hamiltonian

We present an ACQC model based on the following Hamiltonian[1]

$$\hat{H}_2 = \chi \left[\hat{a}^\dagger \hat{a} \hat{\sigma}_z + \hat{\sigma}_+ \hat{\sigma}_-\right] = \frac{\chi}{2}\left[\left(\hat{x}^2 + \hat{p}^2\right)\hat{\sigma}_z + \hat{\sigma}_+ \hat{\sigma}_-\right], \tag{3.11}$$

with χ giving the strength of interaction. We left out the subscripts (A,R) since there is no ambiguity as to which space the operators act on. The Hamiltonian $\hat{H}_2$ couples the qubit quadratically (in terms of ladder or quadrature operators) to the continuous variable mode.

[1] For a derivation, see ref. [73].

In the analysis below, we disregard in the Hamiltonians the local terms on the register and ancilla as these can be taken into account by the local gates in the definition of E_{AR}. Since $\hat{\sigma}_+\hat{\sigma}_- = \frac{1}{2}(\mathbb{1} + \hat{\sigma}_z)$ commutes with $\hat{\sigma}_z$, we can extract $\exp(\hat{\sigma}_+\hat{\sigma}_-)$ and let the local gate on the register include[2] $\hat{k}_R^{(2)} = e^{\hat{\sigma}_+\hat{\sigma}_-}$. We therefore redefine

$$\hat{H}_2 = \frac{\chi}{2}\left[\left(\hat{x}^2 + \hat{p}^2\right)\hat{\sigma}_z\right] \tag{3.12}$$

Suitable platforms are ones which couple the qubit quadratically to the qumode, for example a Jaynes-Cummings like interaction. In the dispersive regime, one finds that the effective interaction involves a $\hat{a}\hat{a}^\dagger\hat{\sigma}_z$ term [73]. The dispersive Jaynes-Cummings interaction has been enacted in the cavity QED setting of a transmon coupled to cavity modes [111–114]. Physical systems include a superconducting qubit coupled to either a cavity mode or a mechanical resonator [115, 116]. Other examples are that of a spin ensemble coupled to a cavity mode via the Tavis-Cummings interaction [84, 117] or a single-spin qubit in an NV-center coupled to a mechanical resonator [107, 108].

We define the ancilla-register interaction from Hamiltonian in eq. (3.12). We let the evolution time be $t = \frac{\pi}{\chi^2}$ and set the local gates to $\hat{k}_A^{(2)} = \hat{F}^\dagger$, $\hat{k}_R^{(2)} = H$, and $\hat{k}_A^{(1)} = \hat{k}_R^{(1)} = \mathbb{1}$. Then we have

$$\begin{aligned} E_{AR} &= \hat{F}^\dagger H e^{i\frac{\pi}{4}(\hat{x}^2+\hat{p}^2)\hat{\sigma}_z} \\ &= \hat{F}^\dagger H\left[\hat{F}\,|0\rangle\langle 0| + \hat{F}^\dagger\,|1\rangle\langle 1|\right] \\ &= H\left[\mathbb{1}_A\,|0\rangle\langle 0| + \hat{F}^2\,|1\rangle\langle 1|\right], \end{aligned} \tag{3.13}$$

where we used that $\hat{F}^{\dagger 2} = \hat{F}^{\dagger^2}\hat{F}^{\dagger 4} = \hat{F}^{\dagger 2}$. We used eq. (1.8) to expand the exponential function of operators. An interpretation of E_{AR} is that the qubit conditions a rotation of the ancilla in phase-space.

The last line in eq. (3.13) uncovers the interpretation of E_{AR} as a mirroring of the ancilla about $q = 0$, conditioned on the state of the qubit. That is, we have the transformation $|a\rangle \xrightarrow{E_{AR}} |a\rangle$ if the qubit is $|0\rangle$; and $|a\rangle \xrightarrow{E_{AR}} |-a\rangle$ if the qubit is $|1\rangle$. Meanwhile, the register qubit is mapped to the conjugate basis by the Hadamard operator.

Compared to the homogeneous CV-CV case, a simple swap is not possible due to the different dimensions of the spaces of the ancilla and register. Instead, computation is effected by entangling the register and ancilla such that manipulation of the ancilla lead to a back-action effect on the register.

When it comes to applying the gates on the register, this hybrid ACQC model shows three differences to the CV-CV model presented in section 3.1. First, both gates require a displacement of the ancilla. Second, the particular state of the ancilla is important as its eigenvalue, a, appears in the resulting effect on the register. Third, a second ancilla is required to perform computation. This becomes apparent by attempting to produce the qubit rotation, $J(\gamma) = He^{i\frac{\gamma}{2}\hat{\sigma}_z}$, by using only one ancilla.

We will compare the qubit rotation with the case when we use only one ancilla. For example, removing the second ancilla from eq. (3.16). Let $\hat{O}$ be some operator on the ancilla space.

[2] Recall the general form of the ancilla-register interaction in eq. (2.18): $E_{AR} = \hat{k}_A^{(2)}\hat{k}_R^{(2)}\hat{U}_{\mathrm{AR}}(\hat{H}_{\mathrm{AR}})\hat{k}_A^{(1)}\hat{k}_R^{(1)}$.

Consider then the effective operator on the register due to the following:

$$\begin{aligned} E_{AR}\hat{O}E_{AR} &= H[\mathbb{1}_A |0\rangle\langle 0| + \hat{F}^2 |1\rangle\langle 1|] \cdot \hat{O} \cdot H[\mathbb{1}_A |0\rangle\langle 0| + \hat{F}^2 |1\rangle\langle 1|] \\ &= H\left[\hat{O} \langle -|0\rangle |0\rangle\langle 0| + \hat{O}\hat{F}^2 \langle +|0\rangle |1\rangle\langle 0| + \hat{F}^2\hat{O} \langle -|1\rangle |0\rangle\langle 1| + \hat{F}^2\hat{O}\hat{F}^2 \langle +|1\rangle |1\rangle\langle 1|\right] \\ &= H\left[-|0\rangle\langle 0|\,\hat{O} + |1\rangle\langle 0|\,\hat{O}\hat{F}^2 + |0\rangle\langle 1|\,\hat{F}^2\hat{O} + |1\rangle\langle 1|\,\hat{F}^2\hat{O}\hat{F}^2\right] \\ &= H\begin{pmatrix} -\hat{O} & \hat{F}^2\hat{O} \\ \hat{O}\hat{F}^2 & \hat{F}^2\hat{O}\hat{F}^2 \end{pmatrix}. \end{aligned} \tag{3.14}$$

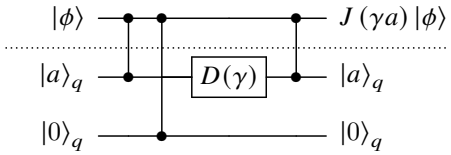
The last line is a short-hand using the vector representation of the computational basis.

Let us compare now eq. (3.14) with the qubit rotation:

$$\begin{aligned} J(\gamma) &= He^{i\frac{\gamma}{2}\hat{\sigma}_z} \\ &= H\left[e^{-i\frac{\gamma}{2}} |0\rangle\langle 0| + e^{i\frac{\gamma}{2}} |1\rangle\langle 1|\right] \\ &= H\begin{pmatrix} e^{-i\frac{\gamma}{2}} & \mathbb{O} \\ \mathbb{O} & e^{i\frac{\gamma}{2}} \end{pmatrix}. \end{aligned} \tag{3.15}$$

To avoid the off-diagonal terms, we would require $\hat{O} = \mathbb{O}$. However, this would set also the diagonal entries to vanish. Thus it is not possible to produce the qubit rotation using only one ancilla in the model presented here.

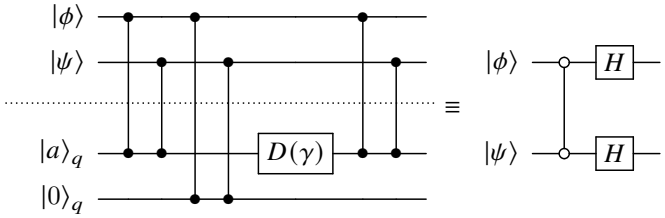
A solution to this is the inclusion of a second ancilla. If the ancilla is the zero eigenstate of position or momentum, then E_{AR} is equivalent to a Hadamard on the register. One may see this using the interpretation of E_{AR} as a conditional rotation by π. Such a rotation leaves the zero eigenstates in their initial state. Since $\hat{F}^2 |0\rangle = |-0\rangle = \mathbb{1} |0\rangle$, we have that $E_{AR} |0\rangle_A = H[|0\rangle\langle 0| + |1\rangle\langle 1|] |0\rangle_A = H |0\rangle_A$, by the resolution of the identity in the basis $\{|0\rangle, |1\rangle\}$. Thus, including a second ancilla in eq. (3.14) gives the desired result. This operation is given by the following circuit:



(3.16)

The dashed line marks the register (above) and ancilla (below) spaces. Note that interaction of the register successively with two ancillas are used to enact the qubit rotation, $J(\gamma a)$. The particular rotation parameter can be controlled by the ancilla displacement $D(\gamma)$.

The two-qubit gate follows a similar reasoning for the requirements of two ancillas. Nonetheless, a universal qubit entangling gate may be enacted through the circuit:



(3.17)

Let the register spaces be R_1 and R_2 and let γ parametrise the displacement on the ancilla. The

resulting operation on the register states, $|\phi\rangle$ and $|\psi\rangle$, is

$$H_{R_1} H_{R_2} \exp\left(i\gamma\hat{x}\hat{\sigma}_z^{R_1}\hat{\sigma}_z^{R_1}\right)|a\rangle_A = |a\rangle_A \hat{U}_{2,R_1R_2}(\gamma a), \tag{3.18}$$

with $\hat{U}_{2,R_1R_2}(\gamma a)$ given in eq. (2.8).

Whenever $|\gamma a| \leq \pi/2$, $\hat{U}_{2,R_1R_2}(\gamma a)$ is entangling and is sufficient for universal quantum computation together with arbitrary single qubit rotations [118].

We have shown how to perform deterministic computation in a register made up of qubits which is accessed only through the interaction with a continuous-variable ancilla. Usefully, only linear displacements of the ancilla are required.

3.2.0.2 Linear Hamiltonian

We next build a model based on the following Hamiltonian, linear in the position quadrature:

$$\hat{H}_1 = \lambda\left(\hat{a}^\dagger + \hat{a}\right)\hat{\sigma}_z, = 2\lambda\hat{x}\hat{\sigma}_z, \tag{3.19}$$

with λ setting the interaction strength. This Hamiltonian couples the qubit *linearly* to the qumode, in terms of the quadrature operators. Similarly to Hamiltonian $\hat{H}_2$ in eq. (3.12), it may be interpreted as a conditional operation on the ancilla, based on the state of the qubit. In this case we have a displacement due to the linear coupling. This interaction may be seen in Jaynes-Cummings type interactions (without going to the dispersive regime unlike for $\hat{H}_2$ in eq. (3.12)) [44, 111, 112, 119].

Physical platforms which could be used to implement the ACQC model based on the $\hat{H}_1$ in eq. (3.19) include the coupling of the two lowest eigenstates of an optical cavity, forming a qubit, with a mechanical resonator or propagating photons [84]. Cavity QED would also be a suitable platform [111].

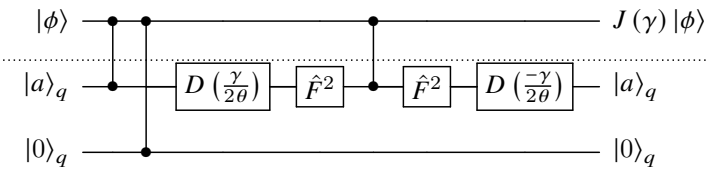
To define the ancilla-register interaction, we parametrise the time evolution by $\theta = 2\lambda t$. Let further the local gates be $\hat{k}_A^{(2)} = \mathbb{1}_A$, $\hat{k}_R^{(2)} = H$ and $\hat{k}_A^{(1)} = \hat{k}_R^{(1)} = \mathbb{1}$ so that the ancilla-register operation is

$$E_{AR} = He^{i\theta\hat{x}\hat{\sigma}_z}. \tag{3.20}$$

We now provide a universal set of gates. The single qubit gate may be enacted through

$$J(\beta) = e^{-i\hat{p}\frac{\beta}{2\theta}} \cdot \hat{F}^2 E_{AR} \hat{F}^2 \cdot e^{i\hat{p}\frac{\beta}{2\theta}} \cdot E_{A_0R} E_{AR}, \tag{3.21}$$

where E_{A_0R} is the interaction between the register and an ancilla prepared in the zero eigenstate of position. The interaction with the zero ancilla is a Hadamard on the register: $E_{AR}|0\rangle \equiv H$. A derivation of eq. (3.20), in the flavour of ref. [31], may be found in appendix B.



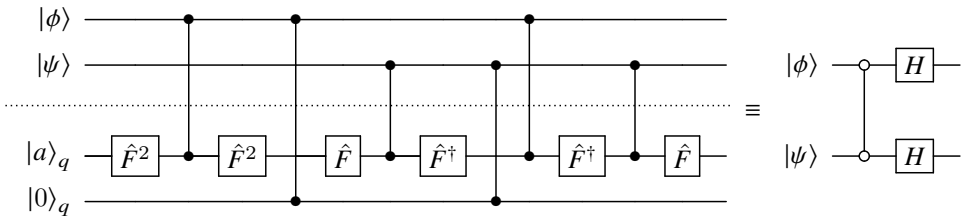
(3.22)

Note that there are operators at the end of the circuit which do not act on the register ($e^{-i\hat{p}\frac{\gamma}{2\theta}} \cdot \hat{F}^2$). While these are not required to perform the desired operation on the register, they return the ancilla to its initial position. In cases when the ancillas would be discarded, these can be left out, leaving the ancilla in the position eigenstate state $\left|-a - \frac{\gamma}{2\theta}\right\rangle_{\hat{x}}$.

The two qubit gate may be implemented by the following procedure:

$$\hat{U}_{2,R_1R_2}(\theta) = \hat{F}E_{AR_2}\hat{F}^\dagger \cdot E_{AR_1} \cdot \hat{F}^\dagger E_{A_0R_2}E_{AR_2}\hat{F} \cdot \hat{F}^2 E_{A_0R_1}E_{AR_1}\hat{F}^2, \tag{3.23}$$

and is described by the following circuit:



(3.24)

Once again, the last Fourier transform returns the ancilla to its initial state.

Note that there is no displacement of the ancilla which controls the two-qubit interaction in eq. (3.23). This parameter is set by the register-ancilla interaction through θ. Hence, in this scenario, we set $\theta = \pi/4$ so that the two-qubit gate is maximally entangling. In turn, the single-qubit rotation in eq. (3.21) is obtained by choosing suitable ancilla displacements.

An interesting point is that the state of the non-zero ancilla is not important as the state eigenvalue does not appear in the effective qubit gates. However, the zero ancilla state is important to enact the Hadamard gate.

Together, the gates in eqs. (3.21) and (3.23) suffice for universal computation using the ACQC model based on Hamiltonian H_1 from eq. (3.19).

Summary of hybrid ACQC

We presented the ACQC model built from Hamiltonians which couple the qubits linearly or quadratically to the quadratures of the ancilla. While we derived specific models, others may be similarly formulated. For example, one may couple linearly to the momentum quadrature which corresponds to a mere redefinition of the ancilla state. In the quadratic model, one may alter the interaction time and preserve the same ancilla-register interaction by modifying the local gate on the ancilla such that $t = \frac{3\pi}{\chi 4}$ and $k_A = \hat{F}^{\dagger 3}$.

The examples given all produce deterministic computation with no correction terms. Since, apart from E_{AR}, the register is left untouched it can be engineered to decrease information leakage. Further, since the register-ancilla interaction is unique, the physical platform may be optimised for allowing that interaction. The register can be made of superconducting circuits, ion traps, nuclear spin while the ancillas may be mechanical resonators, photons, vibrational modes of trapped ions [84, 120].

Another commonality amongst the ACQC schemes presented here is that the ancillas are returned to their initial state. This opens up the possibility for multiple uses, allowing a more economical use of resources and for more efficient operation. A diagram of this architecture was given in fig. 3.2.

In contrast to the homogeneous models of continuous and discrete variables, the hybrid models seem to require a secondary ancilla. However, these ancillas could be taken from the same pool by displacing them prior to computation.

This concludes our presentation of the ACQC models on hybrid systems where the register is made up of qubits and are controlled by continuous variable ancillas. Taking a further step

[3] This result was obtained by Iason Apostolatos who carried out their master's project under my co-supervision.

towards experimental systems, we provide an analysis of realistic ancilla states on both the CV-CV and CV-DV models.

3.3 Finite squeezing effects in the ancilla-based models

Moving towards a physical implementation of the hybrid ACQC, we analyse the effect of using realistic ancillas. Quadrature eigenstates are unphysical as they don't form part of the ancilla Hilbert space (e.g. they are not square-integrable). Instead, they may be described by delta-functions in phase-space corresponding to the limiting cases of infinitely squeezed coherent states. Infinite squeezing requires unbounded energy. We now consider the effect of finite squeezing on the ACQC model.

Squeezing is defined by the squeezing operator [26, p. 90] (see eq. (1.52))

$$S(\xi) = \exp\left(\frac{\xi}{2}\hat{x}\hat{p}\right) = \exp\left(i\frac{\xi}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})\right), \tag{3.25}$$

with $\xi \in \mathbb{R}$ for the purposes of this section ($\xi \in \mathbb{C}$ in general). Its effect on the quadratures is

$$S^\dagger(\xi)\hat{x}S(\xi) = e^{-\xi}\hat{x}. \tag{3.26}$$

The variance in position is given by $\mathrm{Var}[\hat{x}] = \langle\hat{x}\rangle^2 - \langle\hat{x}^2\rangle$, with $\langle\hat{x}\rangle$ giving the mean position. For a coherent state – eigenstate of the annihilation operator $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$ – the variance is reduced by the amount determined by the squeezing parameter:

$$\mathrm{Var}[\hat{x}] = \frac{e^{-\xi}}{2}. \tag{3.27}$$

Squeezing in one variable produces anti-squeezing in the conjugate so that the Heisenberg uncertainty relation is preserved: $\mathrm{Var}[\hat{x}]\mathrm{Var}[\hat{p}] = \frac{e^{-\xi}}{2}\frac{e^{\xi}}{2} = \frac{1}{4}$. That is, squeezing retains the product of variances along orthogonal axes but changes each individual variance. Taking the limit $\xi \to \infty$ elucidates the interpretation of quadrature eigenstates having zero variance around an eigenvalue of position. The same argument applies for eigenstates of momentum.

Here we will describe finitely squeezed ancilla states as Gaussian superpositions of quadrature eigenvectors [54]:

$$\left|A_{s,d}\right\rangle = \int_{\mathbb{R}} g_{s,d}(a)\,|a\rangle_{\hat{x}}\,\mathrm{d}a, \tag{3.28}$$

with $\hat{x}\,|a\rangle_q = a\,|a\rangle_q$ and normalised Gaussian weights $g_{s,d}(x) = \sqrt{N}\exp\left[\frac{(x-d)^2}{4s^2}\right]$ with N such that $\int_{\mathbb{R}} g^2_{s,d}(x)\mathrm{d}x = 1$. The ancillas are thus Gaussian superpositions of position eigenvalues centred at d and with variance s. Taking the limit of squeezing to infinity ($s \to 0$) collapses the Gaussian to a Dirac delta-function and returns, as expected, the position eigenstate with eigenvalue d

$$\lim_{s\to 0}\left|A_{s,d}\right\rangle = |d\rangle_q\,. \tag{3.29}$$

From this definition, one retrieves the zero-ancilla by a position displacement of $-d$: $\left|A_{s,0}\right\rangle = \hat{D}(-d)\left|A_{s,d}\right\rangle$ where $\hat{D}(d) = e^{-id\hat{p}}$ (see eq. (1.49)).

We now analyse the effects on the computing models.

3.3.1 Hybrid ACQC with finite squeezing

For the model from the quadratic Hamiltonian, $H_2 = \frac{\chi}{2}\left(\hat{x}^2 + \hat{p}^2\right)\sigma_z$, the single and two-qubit gates are enacted through the following interaction with the infinitely squeezed ancillas

$$\begin{aligned} E_{AR}e^{-i\frac{\alpha}{2d}}E_{A_0R}E_{AR}\left|d\right\rangle_q &\equiv \hat{J}(\alpha); \\ E_{AP}E_{AR}e^{i\frac{\beta}{d}}E_{A_0P}E_{A_0R}E_{AP}E_{AR}\left|d\right\rangle_q &\equiv \hat{U}_{2,R_1R_2}(\beta), \end{aligned} \tag{3.30}$$

with $\hat{J}$ and $\hat{U}_{2,R_1R_2}$ given in eqs. (2.7) and (2.8).

Replacing the ancillas with the finitely squeezed ones from eq. (3.28), gives the following

$$E_{AR}e^{-i\frac{\alpha}{2d}}E_{A_0R}E_{AR}\left|A_{s,0}\right\rangle_q\left|A_{s,d}\right\rangle_q = \left|A_{s,0}\right\rangle_q\int g_{s,d}(a)\left|a\right\rangle_q\hat{J}\left(\frac{\alpha a}{d}\right)\mathrm{d}a, \tag{3.31}$$

and

$$E_{AP}E_{AR}e^{i\frac{\beta}{d}}E_{A_0P}E_{A_0R}E_{AP}E_{AR}\left|A_{s,0}\right\rangle_q\left|A_{s,d}\right\rangle_q = \left|A_{s,0}\right\rangle_q\int g_{s,d}(a)\left|a\right\rangle_q\hat{U}_{2,RP}\left(\frac{\beta a}{d}\right)\mathrm{d}a. \tag{3.32}$$

We can note three things: first, the result agrees with the infinite squeezing result when we take the limit $s \to 0$; finite squeezing in the zero-ancilla produces no effect as it returns to its initial state (because it is symmetric about $x = 0$) and; third, for any finite s, the register and ancilla remain entangled after the gate application. We discuss the third point below.

Next we move on to hybrid ACQC from a linear Hamiltonian, $H_1 = 2\lambda\hat{x}\hat{\sigma}_z$, giving the non-local part of $E_{AR} = He^{i\theta\hat{x}\hat{\sigma}_z}$.

In this case, interaction with the zero-ancilla is required to implement the bare Hadamard, allowing the equality in eqs. (3.21) and (3.23). Extending the ancillas to $\left|A_{s,0}\right\rangle$, as per eq. (3.28), leads to the same conclusion as above: the register and ancilla remain entangled after the circuit.

There are a number of consequences of the remaining entanglement. First, there may be information leaking into the ancilla as time passes, corrupting the register state. Likewise, noise may be introduced through the coupling to the ancilla. This could be understood as the ancilla bridging the register qubits and the environment. A next step in analysing the model could be by performing a fault-tolerance analysis. Such an analysis showed that the continuous-variable measurement-based model was fault-tolerant for squeezing up to $20.5dB$ [68]. A point to consider, however, is that the finite squeezing effects enter differently in measurement-based scenarios compared to fully unitary schemes.

Next, at the end of computation, a read-out measurement has to be performed. This leads to removal of the entanglement between register and ancilla. However, it also removes determinism from computation, as is the case with ADQC [58, 77] (see section 4.3). Looking at eq. (3.31), we may see that the rotation on the qubit depends on the measurement outcome. Since any correction would also be probabilistic, determinism is lost.

3.4 Chapter summary and discussion

We have presented models of quantum computation on a register which is not directly controlled. In fact, apart from an interaction between register and a secondary state – the ancilla – all operations are performed on the ancilla. The models presented are thus examples of Ancilla-controlled quantum computation [77–79]. For a summary of the properties of the ancilla-based models presented here and in chapter 4, please see table 3.1.

We investigated three settings: a model where register and ancilla states are both described by continuous variables; two hybrid models where the register is made up of qubits and the ancillas

are continuous variables – one where the interaction is quadratic in the ancilla quadrature and one linear.

The models share some common properties, despite the different interpretations of the effect of the register-ancilla interaction. The models describe deterministic quantum computation without the need for correction. Further, the initial state of the ancillas is retained after computation, opening the possibility for multiple uses. We presented a diagram of such a set-up in fig. 3.2. In a realistic scenario, it seems sensible that the ancillas are reused only a number of times, as errors could increase with the number of actions on the ancilla. To give a specific number of ancilla operations, an analysis of the physical platform would be required.

There are several suitable platforms for the hybrid ACQC mode. For the quadratic case, based on $\hat{H}_2$ from eq. (3.11), the model presented is based on an interaction which couples the qubit quadratically to the qumode. The ancilla-register coupling used is generated by the dispersive Jaynes-Cummings interaction. That interaction has been investigated in the cavity QED setting of a transmon coupled to cavity modes [111–114]. Physical systems include a superconducting qubit coupled to either a cavity mode or a mechanical resonator [115, 116]. Examples with similar interactions are that of a spin ensemble coupled to a cavity mode via the Tavis-Cummings interaction [84, 117] or a single-spin qubit in an NV-center coupled to a mechanical resonator [107, 108].

Meanwhile the linear model, built from $\hat{H}_1$, can be prepared by systems with a non-dispersive Jaynes-Cummings interaction [44, 111, 112, 119]. Physical platforms include those where the two lowest eigenstates of an optical cavity, forming a qubit, are coupled with a mechanical resonator or propagating photons [84]. Cavity QED would also be a suitable platform [111].

A suitable continuation of the work presented here is to build models from other interactions. A starting point can be with a particular physical system in mind. Also phrasing adjacent models to the ones presented here by making some alteration to the requirements. For example adding the possibility of a different interaction time in the ancilla-register interaction opens up to a broader class of computation models. However, this also leads to the loss of certain properties of the ancilla-based models presented here – having a unique register-ancilla interaction allows to build strongly optimised systems.

The hybrid variable models have some added requirements. Primarily, the register is required to interact with a second ancilla for implementing the elementary gates although they may be prepared from the other ancillas through a displacement. We showed an argument as to why the second ancilla is required in the models presented.

This line of thought leads to the question about generalising ancilla-based models. The second ancilla allows the register to disentangle from the first ancilla. It would be interesting to know if there are other useful properties of ancilla-based models with more than one ancilla. In the long term, it would be useful to have a general theory of hybrid ancilla-controlled models, in the vein of ref. [76] where ADQC and homogeneous ACQC were phrased in general terms.

In section 3.3, we presented a finite-squeezing analysis of the hybrid models. This is a step towards a realistic scenario. The set-up was to generalise the ancillas from position eigenstates to Gaussian superpositions of those. The Gaussian variance corresponds to the level of squeezing. The analysis shows that the ancilla and register remain entangled after computation, leading to a lessened isolation of the register. This opens a channel for information leaking to the environment. A way to understand the effect on the register could be through methods used in open quantum systems. To understand the viability of the hybrid ACQC models, ways of dealing with the persistent entanglement need to be investigated. One way forward is to consider the measurement during read-out. In this case the ACQC models collapses to ADQC and the remaining entanglement means that computation becomes stochastic (see chapter 4).

The analysis could be complemented with a fidelity calculation of the gates in the finite-

squeezing scenario[4]. The resulting gate on the register can be obtained by tracing out the ancilla space and calculating the fidelity to the perfect gate implementation. Define the gate due to interaction with a finitely-squeezed ancilla as G_{fs} and the ideal gate as G_{ideal} and the let the density matrices of the reduced register states under those transformation be given by ρ_{fs} and ρ_{ideal} respectively. As a starting point, one may consider the overlap[5], $\text{Tr}[\rho_{\text{fs}}\,\rho_{\text{ideal}}]$, as a figure of merit. For a pure register state $|\phi\rangle$, this overlap is simply

$$|\,\langle\phi|G_{\text{fs}}G_{\text{ideal}}|\phi\rangle|^2. \tag{3.33}$$

Since the overlap depends on the state $|\psi\rangle$, this needs to be carefully considered. One approach is to take the average over possible register states. We leave this calculation for future work.

Despite the similarities between the measurement-based model and the ancilla-driven model, the latter has been shown to be more resilient to certain types of noise than the measurement-based model [81] in the qubit scenario. It would be interesting to investigate how ACQC fares compared to both. While the ACQC models requires more interactions between register and ancilla, it avoids the imperfections in measurement so there is promise of improvement.

Table 3.1: Comparison of different ancilla-based models of quantum computation

Model	$\dim(\mathcal{H}_{\text{R}})$	$\dim(\mathcal{H}_{\text{A}})$	Finite squeezing	Ancillas	Determinism	Errors	Ref.
ADQC	DV	DV	N/A	1	Yes	Commutable; Fixed by basis redefinition	[75]
	CV	CV	No	1	Yes	Commutable; Fixed by basis redefinition	[77]
			Yes	1	Yes	Commutable; only Gaussian gates checked; interpretation?	chapter 4
	DV	CV	No	1	No	Probabilistically removed	[77]
			Yes	1	No	Probabilistically removed *	chapter 4
ACQC	DV	DV	N/A	1 (reusable)	Yes	Commutable (in general case)	[78, 79]
	CV	CV	No	1 (reusable)	Yes	None **	[77]
			Yes	1 (reusable)	***	Residual entanglement	chapter 3
	DV	CV	No	2 (reusable)	Yes	None	chapter 3
			Yes	2 (reusable)	***	Residual entanglement	chapter 3

* Probabilities altered by squeezing.

** Commutable in general case. No error term appears in the model considered in this paper.

*** Effect of residual entanglement on determinism unclear.

[4] This complementary analysis was suggested by the external examiner to this thesis, Tommaso Tufarelli.

[5] In the case of pure states, this coincides with the Uhlmann fidelity [26, p.228], $\text{Tr}\big[\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}\big]$, for density matrices ρ_0 and ρ_1.

CHAPTER 4

Ancilla-based quantum computation driven by measurements on the ancilla

The content of this chapter is unpublished work.
The ACQC models presented herein were introduced in the master's thesis from ref. [82]. My addition to those sections was to provide more details and a cleaner derivation of the gateset presented; expanded qualitative statements – for example on suitable experimental platforms. I also corrected the error-analysis in section 4.2 arriving to a alternative conclusion. I further expanded the analytic work by performing the finite-squeezing analysis in section 4.3.

We present models of ancilla-based quantum computation where measurements on the ancilla effect gates on registerWe do that in two setting: homogeneous continuous variable and hybrid, where the register is made up of qubits and the ancillas are CV systems.

4.1 Continuous variable ADQC

We show how to use the ADQC model to implement the universal set of gates for CV quantum computation:

$$\left\{\hat{F},\ \hat{U}_{\mathrm{k}}(\theta) = \exp\left(i\frac{\theta}{k}\hat{x}^k\right),\ CZ_{AR} := \exp(i\hat{x}_A\hat{x}_R)\right\}, \tag{4.1}$$

where $k = 1, 2, 3$.

The register states are arbitrary CV states,

$$|\psi\rangle = \int_{\mathbb{R}} \mathrm{d}x\psi(x)\,|x\rangle \in \mathcal{H}_R, \tag{4.2}$$

for a complex function ψ. The ancillas are initialised in the continuous variable conjugate (momentum) basis,

$$|A\rangle := |0\rangle_{\hat{p}} \in \mathcal{H}_A, \tag{4.3}$$

as momentum eigenstates with zero eigenvalue. Although $\mathcal{H}_A$ and $\mathcal{H}_R$ are of the same type, we label operations on the different spaces by a subscript.

The operation between register and ancilla used to derive the homogeneous CV model is

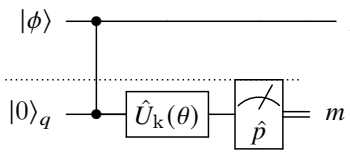
$$E_{AR} := \hat{F}_A^\dagger \hat{F}_R CZ_{AR}, \tag{4.4}$$

where CZ is a continuous variable controlled-Z gate, CZ_∞, that couples register and ancilla as given in eq. (4.1).

The gates on a single register qumode, as parametrised in eq. (4.1), are implemented as follows:

$${}_p\langle m|\,\hat{U}_{\mathrm{k,A}}(\theta)\hat{E}_{AR}\,|0\rangle_{p,A} = \hat{X}(m)\hat{F}_R\hat{U}_{\mathrm{k,R}}(\theta). \tag{4.5}$$

Here $\hat{X}(m) := \exp(-im\hat{p}_R)$ is a displacement in the position quadrature generated by the ancilla measurement. Similar to the qubit case in section 2.2.4.1, the error term, $\exp(-im\hat{p}_R)$, may be accounted for by a redefinition of the computational basis or corrected after computation through classical feed-forward from the measurement outcome. For the derivation of eq. (4.5) see appendix C. The circuit which produces the single-mode gate is

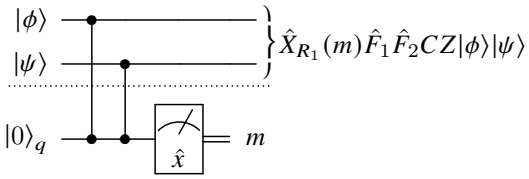


(4.6)

The CZ_∞ gate is implemented through a measurement of the ancilla in the *position* basis

$$ {}_q\langle m|\, E_{AR_2}E_{AR_1}\,|0\rangle_p = e^{-im\hat{x}_1}\hat{F}_1\hat{F}_2\exp(-i\hat{x}_1\hat{x}_2). \tag{4.7} $$

One obtains the correct form of CZ by recalling that $\hat{F}^2\hat{x}\hat{F}^2 = -\hat{x}$. Likewise, the term $\exp(-im\hat{x}_1)$ may be corrected by a Fourier transformation and a basis redefinition. The implementation of the CZ gate is therefore stepwise-deterministic, as was the case with the measurement-free ACQC in chapter 3. The ADQC procedure giving the two-mode gate is represented by the following circuit:



(4.8)

We derived a model of continuous-variable ADQC from on the Hamiltonian $\hat{x}_A\hat{x}_R$. Computation is deterministic. Computational errors may be corrected by a redefinition of the computational basis, determined by the ancilla measurement outcomes.

4.2 Hybrid variable ADQC

We move on to the hybrid scenario where the register is made up of qubits and the ancilla is a position quadrature eigenstate. That is, $|\phi\rangle \in \mathcal{H}_2$, and $|A\rangle = |a\rangle_{\hat{x}}$.

The Hamiltonian from which we derive the ancilla-register interaction, E_{AR}, is

$$ \hat{H}_{2,\text{Full}} = \chi\left[\hat{a}^\dagger\hat{a}\hat{\sigma}_z + \hat{\sigma}_+\hat{\sigma}_-\right] = \frac{\chi}{2}\left[\left(\hat{x}^2+\hat{p}^2\right)\hat{\sigma}_z + \hat{\sigma}_+\hat{\sigma}_-\right]. \qquad \text{(eq. (3.11) revisited)} $$

Here, the quadratures are defined as $\hat{x} = (\hat{a}^\dagger + \hat{a})/\sqrt{2}$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})/\sqrt{2}$. The Hamiltonian in eq. (3.11) describes the Jaynes-Cummings interaction where the frequency difference between the qubit and quantum mode, $\Delta = \omega_0 - \omega$, is large enough for dispersive interactions [24, sec. 4.8]. For a derivation starting from the Jaynes-Cummings Hamiltonian given in eq. (1.69), see ref. [73].

We are interested in the term coupling register and ancilla, so we define

$$ \hat{H}_2 := \frac{\chi}{2}\left(\hat{x}^2+\hat{p}^2\right)\hat{\sigma}_z. \tag{4.9} $$

Note that we may absorb the qubit-local component, $\hat{\sigma}_+\hat{\sigma}_-$, into the local gates of E_{AR}. This is possible since $\hat{\sigma}_+\hat{\sigma}_- = \frac{1}{2}(\mathbb{1} + \hat{\sigma}_z)$ commutes with $\hat{\sigma}_z$. We may therefore define the ancilla-register interaction as

$$ E_{AR} = \hat{F}^\dagger H\hat{U}(\hat{H}_2), \tag{4.10} $$

where $\hat{U}(\hat{H}_2)$ is the unitary generated by the interaction of the register and ancilla for a time, t, such that $\pi = t\chi$. That is,

$$E_{AR} = \hat{F}^\dagger H e^{-i\frac{\pi}{2}\hat{\sigma}_z(\hat{x}^2+\hat{p}^2)}. \tag{4.11}$$

Expanding the non-local component in the qubit basis gives

$$\exp\left(-i\frac{\pi}{2}\hat{\sigma}_z(\hat{x}^2+\hat{p}^2)\right) = \left[\hat{F}\otimes|0\rangle\langle 0| + \hat{F}^\dagger\otimes|1\rangle\langle 1|\right]. \tag{4.12}$$

Hence we can re-write the ancilla-register interaction as

$$E_{AR} = H\left[\mathbb{1}\otimes|0\rangle\langle 0| + \hat{F}^2\otimes|1\rangle\langle 1|\right], \tag{4.13}$$

where we used that $(\hat{F}^\dagger) = \hat{F}^2$. We uncover thus the interpretation of E_{AR} as the applications of $\hat{F}^2$ on the ancilla conditioned on the state of the register qubit, followed by a Hadamard on the qubit. To use the effect of the conditional Fourier transform, we displace the ancilla from the zero eigenstate. We choose

$$|A\rangle = |a\rangle_{\hat{x}} = \exp(-ia\hat{p})\,|0\rangle_{\hat{x}}\,. \tag{4.14}$$

We now show how to effect the following universal set:

$$\left\{\hat{J}(\alpha) := He^{i\frac{\alpha}{2}\hat{\sigma}_z}, \hat{U}_2 = \exp\left(i\frac{\pi}{4}\hat{\sigma}_z\otimes\hat{\sigma}_z\right)\right\}. \qquad \text{(eqs. (2.7) and (2.8) revisited)}$$

We start with the one-qubit gate by defining $\mathcal{J}(\gamma) := \hat{F}e^{i\gamma\hat{x}/2}$. Then

$${}_{\hat{x}}\langle m|\,\mathcal{J}(\gamma)E_{AR}\,|a\rangle_{\hat{x}} = e^{ima\hat{\sigma}_x/2}\hat{J}(\gamma a), \tag{4.15}$$

where we used $He^{i\alpha\hat{\sigma}_z}H = e^{i\alpha\hat{\sigma}_x}$, the resolution of the identity, $\mathbb{1}_2 = |0\rangle\langle 0| + |1\rangle\langle 1|$, and eq. (1.8) to write $e^{i\alpha\hat{\sigma}_z} = e^{i\alpha}\,|0\rangle\langle 0| + e^{-i\alpha}\,|1\rangle\langle 1|$.

The error term, $\exp(ima\hat{\sigma}_x/2)$, is problematic: it does not commute with future gates ($[\hat{\sigma}_z,\hat{\sigma}_x] = 2i\hat{\sigma}_y$). Consider a sequence of two qubit rotations with ancilla measurement outcomes m and n respectively. The resulting operation is

$$e^{ina\hat{\sigma}_x}\hat{J}(\theta a)e^{ima\hat{\sigma}_x}\hat{J}(\phi a). \tag{4.16}$$

To investigate the error term, $\mathcal{E}$, consider the following:

$$\hat{J}(\theta a)\exp(ima\hat{\sigma}_x) = \mathcal{E}\hat{J}(\theta a) = \mathcal{E}H\exp(i\theta a\hat{\sigma}_z), \tag{4.17}$$

giving

$$\begin{aligned}\mathcal{E} &= H\exp(i\theta a\hat{\sigma}_z)\exp(ima\hat{\sigma}_x)\exp(-i\theta a\hat{\sigma}_z)H\\ &= \begin{pmatrix}\cos(ma)+i\cos(\theta a)\sin(ma) & \sin(\theta a)\sin(ma)\\ -\sin(\theta a)\sin(ma) & \cos(ma)-i\cos(\theta a)\sin(ma)\end{pmatrix}.\end{aligned} \tag{4.18}$$

Unlike the continuous variable case where the measurement outcome could be used to correct for the error, $\mathcal{E}$ may only be removed stochastically, when $m = 0$. One may see that $\mathcal{E} = \cos(ma)\mathbb{1} + i\cos(\theta a)\sin(ma)\hat{\sigma}_z + i\sin(\theta a)\sin(ma)\hat{\sigma}_y$, so it does not satisfy the conditions of a Pauli correction [58].

The gate on two register qubits labelled by R_1 and R_2 is obtained as follows. Interacting the ancilla with the register states has the following effect:

$$\begin{aligned}E_{AR_2}E_{AR_1}\,|a\rangle_{\hat{x}} = H_2H_1\big[\,&|a\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|0\rangle\langle 0|_{R_1} + |1\rangle\langle 1|_{R_2}\,|1\rangle\langle 1|_{R_1}\right)\\ &+ |-a\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|1\rangle\langle 1|_{R_1} + |1\rangle\langle 1|_{R_2}\,|0\rangle\langle 0|_{R_1}\right)\big],\end{aligned} \tag{4.19}$$

where we omitted the tensor product sign for clarity.

The ancilla is now measured in the momentum basis, due to the further Fourier transform induced by the second interaction with the register. We obtain thus

$$ {}_{\hat{p}}\langle m| E_{AR_2} E_{AR_1} |a\rangle_{\hat{x}} = H_2 H_1 \exp\left(ima\hat{\sigma}_{z,R_1} \otimes \hat{\sigma}_{z,R_2}\right). \tag{4.20} $$

For more details of the derivation see appendix C. The circuits for hybrid ADQC look the same as the homogeneous case in section 4.1, with suitable changes to the gates implemented.

The two-qubit gate in eq. (4.20) does not contain an error term unlike the one-qubit gate. However, the amount of entanglement produced is probabilistic – conditioned on the measurement outcome of the ancilla. Note that for most measurement outcomes, eq. (4.20) will produce an entangling gate. However, any entangling gate can be used to perform universal computation, when paired together with arbitrary single qubit unitaries [52]. Although the method introduced in ref. [52] is based on the ability to enact the same entangling gate multiple times, a theory could possibly be devised for stochastically produced entangling gates. Nonetheless, that presupposes that single qubit unitaries may be enacted precisely. Note that the loss of determinism is in accordance with previous results [76].

The loss of determinism, means that the fully unitary (ACQC) models in chapter 3 present a stronger case for implementation.

4.3 Finite squeezing analysis

The phrasing of the models above was done with eigenstates of the quadratures. They are unphysical states requiring infinite energy to produce. Quadrature eigenstates can be approximated by infinitely squeezed states. We move to a physical picture and model the ancilla as a finitely squeezed vacuum state [54]:

$$ |A\rangle = \int \mathrm{g}_{0,s}(a) \, |a\rangle_{\hat{p}} \, \mathrm{d}a, \tag{4.21} $$

where $g_{\mu,\sigma}(x) = \frac{1}{\sigma(2\pi)^{1/4}} \exp\left(-\frac{(x-\mu)^2}{4\sigma^2}\right)$ is a normalised Gaussian centred at μ with standard deviation σ. We set $\mu = 0$ so the ancilla state is a momentum vacuum state with the amount of squeezing defined by s. Infinitely squeezed states are approached by taking the limit $s \to 0$

4.3.1 Finite squeezing in CV ADQC

We present the finite-squeezing effects on the Gaussian gates. For the derivations see appendix D.1.

One-mode Gaussian gates

First, we have that the general effect of a one-mode gate using a finitely squeezed ancilla is

$$ {}^{A}_{\hat{p}}\langle m| \hat{U}_{\hat{x},k}(c) \, E_{AR} \, |A\rangle = \iint \hat{U}_{a+r,k}(c) \, e^{-ima} \mathrm{g}_{0,s}(a) \hat{X}(m) f(r) \, |r\rangle_{\hat{p}} \, \mathrm{d}r\mathrm{d}a. \tag{4.22} $$

We integrate over a to find the effect due to the Gaussian single-mode gates ($k = 1, 2$). The cubic phase gate requires other methods to calculate, for example using Airy functions [121, 122].

The implementation of the displacement, $\hat{U}_{\hat{x},1}(c)$, using the finitely-squeezed ancilla give following effective operation on the register:

$$ {}^{A}_{p}\langle m| \hat{U}_{\hat{x},1}(c) \, E_{AR} \, |A\rangle \, |\psi\rangle = e^{-(c-m)^2 s^2} \hat{X}(m) \hat{F} \hat{U}_{r,1}(c) \tag{4.23} $$

where $\hat{X} := \exp(im\hat{p})$ is a displacement. The ideal gate is scaled by a real exponential dependent on the amount of squeezing. This means that the state must be normalised after computation with the ancilla. One may compare this to the result for CV measurement-based quantum computation [54]. The finite squeezing effect in CV MBQC was a convolution of the original state coefficient function with a Gaussian. The scaling in ADQC differs in that it is a global scaling in the affected mode leading to a decreased amplitude compared to the other register modes.

The quadratic gate, $\hat{U}_{\hat{x},2}(c)$, has the following result:

$$\begin{aligned}{}_{\hat{p}}^{A}\langle m|\hat{U}_{\hat{x},2}(c)E_{AR}|A\rangle|\psi\rangle \\ = \frac{1}{\sqrt{1-2ics^2}}\exp\left(-\frac{s^2\left(c^2r^2-cmr+m^2\right)}{4c^2s^4+1}\right)\hat{X}\left(-\frac{2mc^2s^4}{4c^2s^4+1}\right)\hat{X}(m)\hat{F}\hat{U}_{\hat{x},2}\left(\frac{c}{4c^2s^4+1}\right),\end{aligned}$$

Even though the form of the alteration due to finite squeezing looks more complicated, it is not dissimilar to the displacement gate. The error term, $\hat{X}$, is supplemented by a further correction, $\hat{X}(-\frac{2mc^2s^4}{4c^2s^4+1})$, is still a displacement which can be accounted for at the end of computation since all parameters in the argument are known. The error term, $\hat{X}$, is still a displacement which can be accounted for at the end of computation since all parameters in the argument are known.

Note that both gates are restored to the ideal ones when taking the limit of infinite squeezing. Taking $s \to 0$, we get

$$\lim_{s\to 0} e^{-(c-m)^2s^2}\hat{X}(m)\hat{F}\hat{U}_{r,1}(c) = \hat{X}(m)\hat{F}\hat{U}_{r,1}(c) \tag{4.24}$$

and

$$\lim_{s\to 0}\frac{1}{\sqrt{1-2ics^2}}\exp\left(-\frac{s^2\left(c^2r^2-cmr+m^2\right)}{4c^2s^4+1}\right)\hat{X}\left(-\frac{2mc^2s^4}{4c^2s^4+1}\right)\hat{X}(m)\hat{F}\hat{U}_{\hat{x},2}\left(\frac{c}{4c^2s^4+1}\right) = \hat{X}(m)\hat{F}\hat{U}_{\hat{x},2}(c)\,. \tag{4.25}$$

CZ gate

We end by considering the implementation of the two-mode gate with a finitely-squeezed ancilla.

Define the input register modes by

$$|\psi\rangle = \int f(r)|r\rangle_{\hat{x}}\,\mathrm{d}r, \text{ and } |\phi\rangle = \int h(\rho)|\rho\rangle_{\hat{x}}\,\mathrm{d}\rho, \tag{4.26}$$

for some complex functions f, h. We begin by noting that

$$E_{AP}E_{AR}|A\rangle|\phi\rangle|\psi\rangle = \iiint e^{ia\rho}e^{ir\rho}|-(a+r)\rangle_{\hat{p}}|r\rangle_{\hat{p}}|\rho\rangle_{\hat{p}}\,h(\rho)f(r)\mathrm{g}_{0,s}(a)\mathrm{d}r\mathrm{d}\rho\mathrm{d}a. \tag{4.27}$$

For the two-mode gate, interaction with a finitely squeezed ancilla state produces the following on a pair of register states:

$${}_{\hat{x}}^{A}\langle m|E_{AP}E_{AR}|A\rangle|\phi\rangle|\psi\rangle = \hat{X}_{R_1}(m)\hat{F}_{R_1}\hat{F}_{R_2}CZ_{\infty}|\psi\rangle|\rho\rangle\,, \tag{4.28}$$

with $|\phi'\rangle = \int e^{-(\rho-m)^2s^2}h(\rho)|\rho\rangle_{\hat{p}}|\rho\rangle_{\hat{x}}\,\mathrm{d}\rho$. Note that it matches the infinite squeezing result (see eq. (4.7)) when taking the limit of infinite squeezing.

Finite squeezing in the two-mode gate results in a convolution of the original state with a Gaussian centred at m with standard deviation $1/s$. The resulting distortion is thus inversely dependent on the squeezing parameter. This matches the result in ref. [54].

4.3.2 Finite squeezing in hybrid ADQC

We continue the analysis onto the hybrid model. In this model, the displacement of the ancilla was used to induce the transformation on the register. We keep the definition of the ancilla as centred at zero displacement. We define

$$D(d) = \exp(-id\hat{p}), \tag{4.29}$$

so that the finitely squeezed ancilla centred at position d can be written as $D(d)\,|A\rangle$.

One-qubit gate

The single-qubit gate in the case of finite squeezing in the ancillas is given by:

$${}_q\langle m|\,\mathcal{J}_A(\gamma)E_{AR}D(d)\,|A\rangle = \nu \exp\left[-s^2(m+\gamma)^2\right]\exp[imd\hat{\sigma}_x]J(2d\gamma), \tag{4.30}$$

where $\nu = N\sqrt{2\pi s}$, with s the squeezing parameter and N the Gaussian normalizing factor.

We see that the effect of the finitely squeezed ancillas is to introduce a scaling factor. However, as was the case with CV ADQC, the scaling factor can be absorbed when normalising the state. However, the probabilities of the measurement outcomes are altered. For an illustration of the procedure for enacting the single-qubit rotation in eq. (4.30), see fig. 4.1. The measurement probabilities are modified by the squeezing parameter and ancilla displacement. In a similar process to the one-qubit gate as sketched in fig. 4.1.

Two-qubit gate

The effect of finite squeezing on the entangling gate on two register qubits is also a scaling factor. The amount of entanglement produced remains probabilistic. Specifically, we obtain:

$${}_p\langle m|\,E_{AR_2}E_{AR_1}D(d)\,|A\rangle = \nu \exp\left[-s^2m^2\right]\exp[imd\hat{\sigma}_z \otimes \hat{\sigma}_z], \tag{4.31}$$

with $\nu = N\sqrt{2\pi s}$. The measurement probabilities are modified by the ancilla squeezing, however.

4.4 Summary and discussion

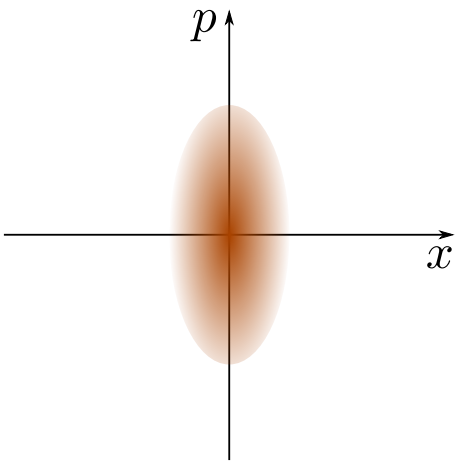
We have presented two models of ancilla-driven quantum computation. The first model is based on the interaction between continuous variable systems. The Hamiltonian descibing the interaction between register and ancilla states is $\hat{x}_A\hat{x}_R$. The resulting interaction is a conditional displacement on the momentum quadrature. A displacement error term appears in both single and multi-qumode gates. However, the error can be removed using the measurement outcome of the ancilla by redefining the computational basis of following gates, or at the end of computation by feeding forward the measurement outcomes. We investigated the effect, on computation, of treating the ancillas as finitely squeezed states. This results in a real scaling factor in the single-mode gates. The scaling decreases the amplitude inversely related to the amount of squeezing. The states acted on need to be renormalised. This can be compared to CV MBQC [54]. In that model, the finite squeezing effect is a convolution of the original state coefficient function with a Gaussian. The scaling due to the single-mode gates in ADQC differs in that it is a global scaling in the affected mode leading to a uniformly decreased amplitude compared to the other register modes. The multimode gate matches the result in ref. [54] in that one of the register states is convolved with a Gaussian centred at m, the ancilla measurement outcome. The standard deviation of the convolution Gaussian is $1/s$, the reciprocal of the ancilla squeezing. Following the

suggestion for dealing with the distortion in CV MBQC, one may concatenate several gates and perform a smaller number of measurements. Perhaps by inspiration of the fully-unitary ACQC from chapter 3, one may phrase a model where measurements are performed only at the end. However, if the same ancillas are used for computation care needs to be taken to understand the unwanted correlations that will appear between register states – recall that ACQC with finitely squeezed ancillas produced gates where ancilla and register remained entangled.

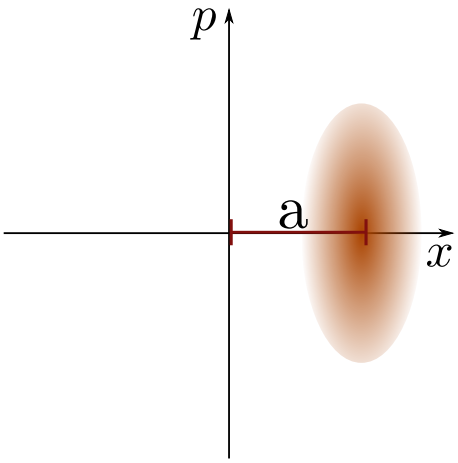
We also presented an ADQC model on hybrid systems where $\dim(\mathcal{H}_R) = 2$ and $\dim(\mathcal{H}_A) = \infty$. Computation is possible only in a stochastic manner: single qubit gates have errors which are only removed depending on measurement outcomes. Furthermore, the two-qubit gate is implemented probabilistically. Extending the model to finitely squeezed ancillas results only in a scaling of the implemented gates. The scaling is absorbed by the normalisation of the state so the gates are unaltered. On the other hand, the measurement probabilities are adjusted by the finite squeezing in the ancilla.

Compared to the ACQC models described in the previous chapter, measurement-based ancilla models are suitable for systems where ancillas are cheap to create and, more importantly, where measurements can be performed with high precision. Measurements should also be fast as they will influence the gate times in ADQC.

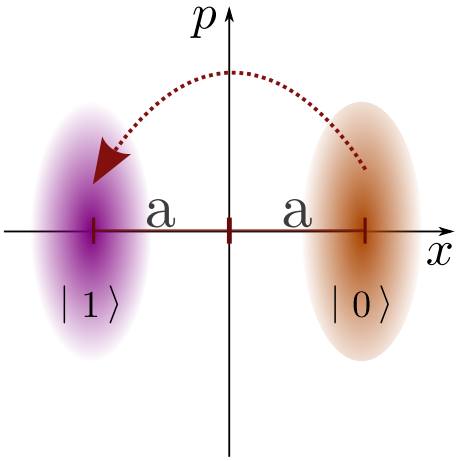
We summarise the results obtained here in table 3.1. For a more detailed discussion of possible platforms for ancilla-based models, see section 3.4.



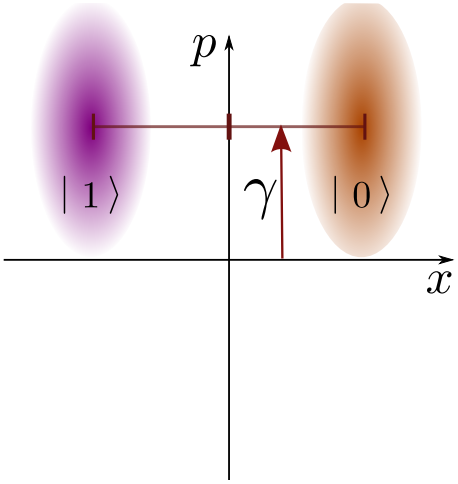
(a) Finitely squeezed ancilla centred at $x = 0$.



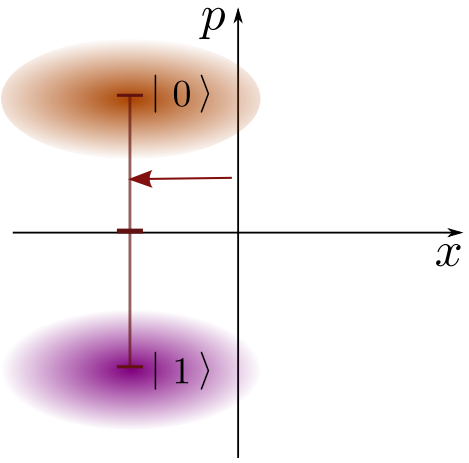
(b) Displacement in the position quadrature by a.



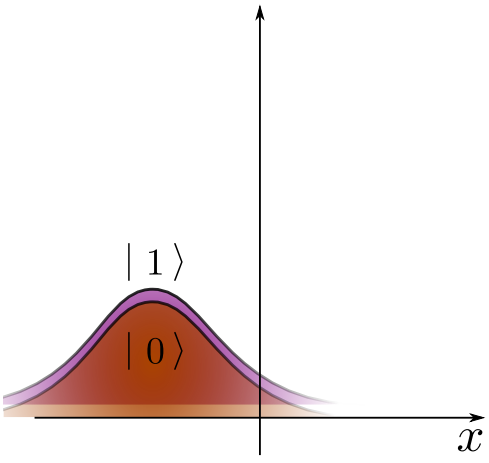
(c) Interaction with register, E_{AR}. Rotation by $\pi/4$ conditioned on qubit. Purple is the state $\hat{F}^2 |a\rangle_q$.



(d) Displacement by γ in the momentum quadrature.



(e) Fourier transform



(f) Measurement of position. Note that no information is gained about the state of the qubit. The overlapping distributions are shifted for illustrative purposes.

Figure 4.1: Illustration of single qubit rotation in the hybrid ADQC model, as per eq. (4.15).

Part II

Genuine Gaussian Multipartite Entanglement

CHAPTER 5

Background to Gaussian multipartite correlations

In this chapter, we provide the formalism used for describing Genuine Gaussian Multipartite Entanglement (GGME) at the level of second statistical moments: covariance matrices (CM). We use this formalism to rephrase the theory of Gaussian quantum optics in section 5.2. We then take a detour to density matrices do present a classification of multipartite entanglement, followed by its translation onto covariance matrices in sections 5.3 and 5.4. In there, we introduce entanglement witnesses at the level of covariance matrices. The presentation of the work requires an introduction to optimisation schemes over semidefinite matrices – called semidefinite programs (SDP). We introduce SDPs in section 5.5. Using SDPs we present a numerical scheme for finding witnesses from ref. [123]. We end this background chapter by laying out the description of simply connected graphs and the quantum marginal problem which are used to introduce the main topic of this part.

5.1 Mathematical preliminaries and notation

Vectors, matrices and scalars

Vectors and *matrices* are given by bold letters from the Latin or Greek alphabets: $\boldsymbol{y}, \boldsymbol{v}, \boldsymbol{\xi}, \boldsymbol{\xi}$. The latter are reserved for important objects while the former are used as dummy variables for short derivations or footnotes, though some exceptions occur.

Scalars and vector elements are given by letters (Latin or Greek) in the lower case in normal font. This includes when the elements are operators. For example, the entries of $\boldsymbol{\xi}$ are operators but follow the same convention: $(\boldsymbol{\xi})_j = \xi_j$ for one-dimensional vectors and $(\boldsymbol{A})_{jk} = A_{jk}$ for matrices.

The *dimension* of the vectors are given by capital Latin letters N or M. Since we deal with square matrices only, their dimensions are $N \times N$ or $M \times M$. While we deal with Gaussian states which are defined on a Hilbert space of infinite dimension, we will see that N mode states can be represented by an N-dimensional vector – corresponding to the mean – and a $(2N)^2$-dimensional symplectic matrix – corresponding to correlations between positions and momenta of each mode.

Some vectors and matrices are sufficiently special that they get their own symbol. $\mathbb{1}_N$ and $\mathbb{O}_N$ are the $N \times N$ identity and zero matrices respectively - whenever there is no ambiguity about the size the subscript is left out. For vectors, $\mathbf{0}$ is the zero vector. Covariance matrices (CMs) will be denoted by γ.

We use E and F to denote some fields (usually $\mathbb{R}$ or $\mathbb{C}$) and define the vector space of $N \times N$ matrices with entries in E over the field F as $\mathcal{M}_E(N, F)$. Similarly $\mathcal{V}_E(N, F)$ denotes a set of N-dimensional vectors with entries in E that form a vector space over F. Whenever $E = \mathbb{R}$, we omit the subscript. Note that E may not be a proper subfield of F since, for $M \in \mathcal{M}_E(N, F)$ and $\alpha \in F/E$, $\alpha M \notin \mathcal{M}_E(N, F)$ so $\mathcal{M}$ is not closed under scalar multiplication standing in contradiction to the axioms of vector spaces. If only F is given, we therefore assume that $F = E$. $E \subseteq F$ is allowed. For example matrices with complex entries form a vector space over the real numbers. Let, for the rest of the section, $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{V}_E(N, F)$, $\boldsymbol{A}, \boldsymbol{B} \in \mathcal{M}_E(N, F)$ and $\alpha, \beta \in F$ unless

Table 5.1: Symbols used to represent vectors and matrices

Symbol	Object represented
$\boldsymbol{v}, \boldsymbol{\xi}$	Vector
$\boldsymbol{v}_i$	i^{th} vector of a list
v_j, ξ_j	Vector element
$\boldsymbol{A}$	Matrix
$\boldsymbol{A}_i$	i^{th} matrix of a list
A_{jk}	Matrix element
Notable exceptions	
γ	Covariance matrix
$\mathbb{1}_N$	N identity matrix
$\mathbb{O}_N$	N zero matrix

specified otherwise. For simplicity also read $\mathcal{M} = \mathcal{M}_E(N, F)$ and $\mathcal{V} = \mathcal{V}_E(N, F)$. Use $K \subset \mathcal{M}$ and $L \subset \mathcal{M}$.

Transposition and hermitian conjugate

The *transposition* is the usual map $(\cdot)^T : \mathcal{M} \to \mathcal{M}$ defined by its action on the elements of a matrix

$$(\boldsymbol{A}^T)_{jk} = (A_{jk})^T = A_{kj}. \tag{5.1}$$

The transposition maps a column vector to a row vector and *vice versa*. So for some vector $\boldsymbol{u} = (u_1, ..., u_N)^T$,

$$\boldsymbol{u}^T = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}^T = (u_1, ..., u_N). \tag{5.2}$$

Along with the normal vector multiplication this allows us to define the inner and outer products below. For the case when $E = \mathbb{C}$ we interpret the transposition as the Hermitian conjugate instead: $\boldsymbol{A}^\dagger = (\boldsymbol{A}^T)^*$, which is defined using the map $A_{jk} \mapsto A^*_{kj}$ where z^* is the complex conjugate of $z \in \mathbb{C}$. In the work presented in this thesis, we consider only matrices with real entries. To preserve continuity with the work presented, we abstain from using the $(\cdot)^\dagger$ notation. Likewise, the complex conjugation of elements is left implicit.

Inner and outer product of vectors, direct sum and commutators

Write the vectors as $\boldsymbol{u} = (u_1, u_2, ..., u_N)^T$ and $\boldsymbol{v} = (v_1, v_2, ..., v_N)^T$. Then the *inner product*[1] $\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \to F$ is defined by

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle = \boldsymbol{u}^T \boldsymbol{v} = \sum_{j=1}^{N} u_j v_j = u_j v_j \tag{5.3}$$

with the last equality follows form using the Einstein summation convention.

The *outer product* $\otimes : \mathcal{U} \times \mathcal{V} \to \mathcal{M}$ returns a matrix with elements given by

$$(\boldsymbol{u} \otimes \boldsymbol{v})_{jk} = (\boldsymbol{u}\boldsymbol{v}^T)_{jk} = u_j v_k. \tag{5.4}$$

The product of the spaces, $\mathcal{U} \otimes \mathcal{V}$, is called the *tensor product* and is made up of all possible matrices $\boldsymbol{u} \otimes \boldsymbol{v}$ for $\boldsymbol{u} \in \mathcal{U}$ and $\boldsymbol{v} \in \mathcal{V}$ so $\dim(\mathcal{U} \otimes \mathcal{V}) = \dim(\mathcal{U}) \dim(\mathcal{V})$.

Matrices may also be extended via the tensor product which may be defined via the action on vectors. Let $A \in \mathcal{M}(N), \boldsymbol{u} \in \mathcal{U}(N)$ and $B \in \mathcal{M}(N), \boldsymbol{v} \in \mathcal{V}(M)$ then

$$(\boldsymbol{A} \otimes \boldsymbol{B})(\boldsymbol{u} \otimes \boldsymbol{v}) = \boldsymbol{A}\boldsymbol{v} \otimes \boldsymbol{B}\boldsymbol{u}. \tag{5.5}$$

Choosing $\boldsymbol{u}$ and $\boldsymbol{v}$ to be basis states allows $\boldsymbol{A} \otimes \boldsymbol{B}$ to be extended to the full space by linearity.

Using the outer product we can define the commutator and anti-commutator for vectors of non-commuting elements. The *commutator* is given by

$$[\boldsymbol{u}, \boldsymbol{v}^T] = \boldsymbol{u}\boldsymbol{v}^T - (\boldsymbol{u}\boldsymbol{v}^T)^T. \tag{5.6}$$

Note that the second term is not necessarily the same as $\boldsymbol{u}\boldsymbol{v}^T$ as the components of $\boldsymbol{u}$ and $\boldsymbol{v}$ do not necessarily commute. We use this and the symmetric product below for dealing with vectors of operators. In that case, not even the entries of $\boldsymbol{v}$ necessarily commute.

The *anti-commutator* is

$$\{\boldsymbol{u}, \boldsymbol{v}^T\} = \boldsymbol{u}\boldsymbol{v}^T + (\boldsymbol{u}\boldsymbol{v}^T)^T. \tag{5.7}$$

Element-wise we have

$$[\boldsymbol{u}, \boldsymbol{v}^T]_{jk} = u_j v_k - u_k v_j, \text{ and} \tag{5.8}$$

$$\{\boldsymbol{u}, \boldsymbol{v}^T\}_{jk} = u_j v_k + u_k v_j. \tag{5.9}$$

Note that

$$\left\{\boldsymbol{v}, \boldsymbol{v}^T\right\} + \left[\boldsymbol{v}, \boldsymbol{v}^T\right] = 2\boldsymbol{v}\boldsymbol{v}^T. \tag{5.10}$$

Another way of joining vectors $\boldsymbol{u} = (u_1, ..., u_N)^T, \boldsymbol{v} = (v_1, ..., v_M)$ is through the *direct sum* $\oplus$:

$$\boldsymbol{v} \oplus \boldsymbol{v} = (\boldsymbol{u}, \boldsymbol{v})^T = (u_1, ..., u_N, v_1, ..., v_M)^T, \tag{5.11}$$

with $\boldsymbol{u}$ and $\boldsymbol{v}$ not necessarily in the same space. The extension to direct sums involving more terms is analogous.

---

[1] Recall that the inner product must satisfy three criterion: For $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathcal{M}(N, F)$ and $\alpha, \beta \in F$,

1. **Linearity:** $\langle (\alpha \boldsymbol{A} + \beta \boldsymbol{B}), \boldsymbol{C} \rangle = \alpha \langle \boldsymbol{A}, \boldsymbol{C} \rangle + \beta \langle \boldsymbol{B}, \boldsymbol{C} \rangle$
2. **Symmetry:** $\langle \boldsymbol{A}, \boldsymbol{B} \rangle = \langle \boldsymbol{B}, \boldsymbol{A} \rangle^*$
3. **Positive-definiteness:** $\langle \boldsymbol{A}, \boldsymbol{A} \rangle > 0$ for non-zero $\boldsymbol{A}$, and $\langle \boldsymbol{A}, \boldsymbol{A} \rangle = 0$ only if $\boldsymbol{A} = 0$.

For matrices $A \in \mathcal{M}(N_A)$ and $B \in \mathcal{M}(N_B)$ we have

$$A \oplus B = \begin{pmatrix} A & \mathbb{O}_{N_A \times N_B} \\ \mathbb{O}_{N_B \times N_A} & B \end{pmatrix}, \tag{5.12}$$

with $\mathbb{O}_{j\times k}$ the zero matrix of j rows and k columns. We have $\dim(A\oplus B) = (N_A+N_B)\times(N_A+N_B)$. We extend the definition to larger sums of matrices $A_1, ..., A_N$ via

$$\bigoplus_{k=1}^{N} A_k = A_1 \oplus A_2 \oplus ... \oplus A_N. \tag{5.13}$$

The space of the resulting matrix is the direct sum of the spaces of each A_k, $k \in [1, N]$.

To define the inner product of matrices we need to introduce the trace map. For $\boldsymbol{A} \in \mathcal{M}(N, F)$ and some orthonormal basis $\{\boldsymbol{v}_j \mid j \in [1, N]\}$ of $\mathcal{V}(N, F)$, the *trace*, $\mathrm{Tr} : \mathcal{M} \to F$ is defined by the mapping

$$\mathrm{Tr}[\boldsymbol{A}] = \sum_{j=1}^{N} \boldsymbol{v}_j \boldsymbol{A} \boldsymbol{v}_j^T = \sum_{j=1}^{N} A_{jj}, \tag{5.14}$$

where A_{jk} is the entry of A in the j^{th} row and k^{th} column. The elements A_{jj} are therefore to the diagonal entries of A. The trace of a matrix is an invariant so the basis may be chosen liberally - although the eigenbasis is commonly used so that, for $\mathrm{eig}(\boldsymbol{A}) = \{a_1, ..., a_N\}$, we have that $\mathrm{Tr}[\boldsymbol{A}] = \sum_{j=1}^{N} a_j$.

The trace is a linear map so

$$\mathrm{Tr}[\alpha \boldsymbol{A} + \beta \boldsymbol{B}] = \alpha \,\mathrm{Tr}[\boldsymbol{A}] + \beta \,\mathrm{Tr}[\boldsymbol{B}], \tag{5.15}$$

for $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathcal{M}(N, F)$ and $\alpha, \beta \in F$. It is also cyclic - it is invariant under permutation of its arguments

$$\mathrm{Tr}[\boldsymbol{ABC}] = \mathrm{Tr}[\boldsymbol{BCA}] = \mathrm{Tr}[\boldsymbol{CAB}]. \tag{5.16}$$

For outer products of matrices, we have that

$$\mathrm{Tr}[\boldsymbol{A} \otimes \boldsymbol{B}] = \mathrm{Tr}[\boldsymbol{A}] \,\mathrm{Tr}[\boldsymbol{B}]. \tag{5.17}$$

Let us now define the operation between matrices (which we suggestively denote like the inner product above):

$$\langle \boldsymbol{A}, \boldsymbol{B} \rangle = \mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{B}\big], \tag{5.18}$$

with $(\cdot)^T = (\cdot)^\dagger$ whenever $F = \mathbb{C}$. Using linearity and symmetry properties, one may show that the operation $\langle \cdot, \cdot \rangle$ satisfies the properties of an inner product[2]. At one point we use the definition of $\bullet : \mathcal{M} \times \mathcal{M} \to F$ as

$$\boldsymbol{A} \bullet \boldsymbol{B} = \langle \boldsymbol{A}, \boldsymbol{B} \rangle = \mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{B}\big], \tag{5.19}$$

to differentiate this from the inner product between vectors.

[2] In this case, the inner product requirements from footnote 1 translate to

1) **Linearity:** $\mathrm{Tr}\big[(\alpha \boldsymbol{A}^T + \beta \boldsymbol{B}^T)\boldsymbol{C}\big] = \alpha \,\mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{C}\big] + \beta \,\mathrm{Tr}\big[\boldsymbol{B}^T \boldsymbol{C}\big]$

2) **Symmetry:** $\mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{B}\big] = \mathrm{Tr}\big[\boldsymbol{B}^T \boldsymbol{A}\big]$

3) **Positive-definiteness:** $\mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{A}\big] = \sum_j A_{jj}^2 \geq 0$ and $\mathrm{Tr}\big[\boldsymbol{A}^T \boldsymbol{A}\big] = 0$ only if $\boldsymbol{A} = 0$.

Congruence

Occasionally, we refer to two matrices being related by *congruence*. This means that, for matrices $\boldsymbol{A}, \boldsymbol{B} \in \mathcal{M}$, $\boldsymbol{A}$ is said to be congruent to $\boldsymbol{B}$ if there exists invertible $\boldsymbol{U} \in \mathcal{M}'$ such that

$$\boldsymbol{A} = \boldsymbol{U}\boldsymbol{B}\boldsymbol{U}^T. \tag{5.20}$$

The spaces $\mathcal{M}$ and $\mathcal{M}'$ along with the operation $(\cdot)^T$ are replaced with the relevant objects for the situation under consideration which should be clear from context. Vector fields $\mathcal{M}$ and $\mathcal{M}'$ are over the same field.

Spaces and some results

In this part we use the common definition of the relational operators and their negations on matrices. For any such operator,

Definition 5.1 (Relational operation on matrices)**.** For any relational operation $\doteq \in \{>, \geq, =, \leq, <\}$, $\boldsymbol{A} \doteq 0$ is to be interpreted as $a \doteq 0$, for $a \in \mathrm{eig}(\boldsymbol{A})$ – an eigenvalue of $\boldsymbol{A}$. Furthermore, $\boldsymbol{A} \doteq \boldsymbol{B}$ is equivalent to $\boldsymbol{A} - \boldsymbol{B} \doteq 0$ and we say "$\boldsymbol{A}$ is $\doteq \boldsymbol{B}$".

Now we define the vector spaces used in this part.

Definition 5.2 (Symmetric matrices)**.**

$$Sym(N) = \{S \in \mathcal{M}_{\mathbb{R}}(N, \mathbb{R}) \mid S^T = S\}. \tag{5.21}$$

Although one may generalise from the $E = F = \mathbb{R}$ here, it is not required for the purposes of this thesis. If $F = \mathbb{C}$, we have instead the Hermitian matrices which are invariant under the operator $(\cdot)^\dagger$.

Definition 5.3 (Hermitian matrices)**.**

$$Herm(N, F) = \{H \in \mathcal{M}_{\mathbb{C}}(N, F) \mid H^\dagger = H\}. \tag{5.22}$$

We leave F general here as $F = \mathbb{R}$ is a choice we use in later sections. This is possible since $\mathbb{R}$ is contained in $\mathbb{C}$ allowing all vector space operations to be closed so that $\mathcal{M}_{\mathbb{C}}(N, \mathbb{R})$ is a subspace of $\mathcal{M}_{\mathbb{C}}(N, \mathbb{C})$. Whenever $F = \mathbb{C}$, we write $Herm(N)$.

Definition 5.4 (Positive (semi)definite matrices)**.** The positive semi-definite (PSD) matrices are those with non-negative elements in the diagonal irrespective of the basis chosen for their representation.

$$PSD(N) = \{P \in \mathcal{M}_{\mathbb{R}}(N, \mathbb{R}) \mid P \geq 0\}, \tag{5.23}$$

where the inequality relation of matrices is defined in Def. 5.1. The positive definite matrices are the subset of PSD which have strictly positive elements in their diagonal.

$$PD(N) = \{P \in \mathcal{M}_{\mathbb{R}}(N, \mathbb{R}) \mid P > 0\}. \tag{5.24}$$

An equivalent statement that to $\boldsymbol{A} \in PSD$ is that for all $\boldsymbol{v} \in \mathbb{R}^N$, $\quad \boldsymbol{v}^T\boldsymbol{A}\boldsymbol{v} \geq 0$ and similarly for $\boldsymbol{A} \in PD$.

Note that elements in PSD have their traces positive semi-definite. Members of PSD are said to be PSD: "$\boldsymbol{A}$ is PSD" $\iff$ $\boldsymbol{A} \in PSD$. The same argument applies for PD matrices. Note also that $PSD(N) \subset Sym(N)$[3].

An important set is that of the symplectic matrices which is constructed in more detail in section 5.2.

Definition 5.5 (Symplectic matrices)**.**

$$Sp(2N, \mathbb{R}) = \{S \in \mathcal{M}(N, \mathbb{R}) \,|\, S\Omega S^T = \Omega\}, \tag{5.25}$$

where $\Omega_N = \bigoplus_{i=1}^{N} \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Finally, orthogonal matrices are defined as follows

Definition 5.6 (Orthogonal matrices)**.** Matrices with unit determinant whose transpose is equal to the inverse form the set of orthogonal matrices defined by

$$SO_E(N, F) = \{O \in \mathcal{M}_E(N, F) \,|\, O^T = O^{-1}, \det(O) = 1\}. \tag{5.26}$$

We write $SO_{\mathbb{R}}(N, \mathbb{R}) = SO(N)$.

5.2 Gaussian quantum optics and the symplectic formalism

We make heavy use of the symplectic formalism for describing correlations in quantum states. An introductory treatment of the topic can be found in A. Serafini's "*Quantum continuous variables*" [26], which we follow in the sections below.

We start by defining the physical observables known as the x (position) and p (momentum) quadratures of quantum states as in eq. (1.36). Recall the well-known bosonic creation and annihilation operators $\hat{a}, \hat{a}^\dagger$, from section 1.4.1, which raise and decrease the energy of a harmonic oscillator respectively. We then define the quadratures by

$$\hat{x} := \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}} \tag{5.27}$$

$$\hat{p} := \frac{\hat{a} - \hat{a}^\dagger}{i\sqrt{2}}. \tag{5.28}$$

Using the commutation relation between these (see eq. (1.33)), $[\hat{a}, \hat{a}^\dagger] = 1$, we may find that the commutation between the quadratures is

$$[\hat{x}, \hat{p}] = i. \tag{5.29}$$

Thus, they satisfy the same commutation relations as position and momentum and gives rise to the same time-evolution[4].

For multi-mode states $\hat{x}_i$ ($\hat{p}_i$) denotes $\hat{x}$ ($\hat{p}$) in the i-th mode. Capital N denotes the number of modes. One can then write the canonical commutation relations (CCR) as

$$[\hat{x}_j, \hat{p}_k] = i\delta_{jk}. \tag{5.30}$$

[3] Note that $\boldsymbol{M} \in PSD(N, \mathbb{R})$ means that $\boldsymbol{M}$ is symmetric: for all $\boldsymbol{v} =\in \mathbb{R}^{2N}$ such that $\boldsymbol{v}^T\boldsymbol{M}\boldsymbol{v} = m \geq 0$ we find $\boldsymbol{v}^T\boldsymbol{M}^T\boldsymbol{v} = (\boldsymbol{v}^T\boldsymbol{M}\boldsymbol{v})^T = m \Rightarrow \boldsymbol{v}^T(\boldsymbol{M} - \boldsymbol{M}^T)\boldsymbol{v} = 0 \Rightarrow \boldsymbol{v}^T\boldsymbol{M}\boldsymbol{v} - \boldsymbol{v}^T\boldsymbol{M}^T\boldsymbol{v} = 0 \Rightarrow \boldsymbol{M} = \boldsymbol{M}^T$, with the last line follows since $\boldsymbol{v}$ is an arbitrary vector.

[4] One way to see this is by recalling the time evolution of an operator $\hat{O}$ under some Hamiltonian $\boldsymbol{H}$ is given by $\frac{\mathrm{d}}{\mathrm{d}t}\hat{O} = i[\hat{H}, \hat{O}]$, in the Heisenberg picture.

To build the symplectic formalism one defines a vector of the quadrature operators. First one needs to choose a way in which to order the quadratures. The two most usual ways are referred to as the $XPXP$ and $XXPP$ ordering. In the first ordering, the vector of quadrature operators is defined below.

Definition 5.7 (Canonical operators (XPXP))**.** The canonical operators (quadratures) in the $XPXP$ ordering are given by the $2N$ vector

$$\boldsymbol{\xi} = (\hat{x}_1, \hat{p}_1, ..., \hat{x}_n, \hat{p}_n)^T. \tag{5.31}$$

With an analogous definition, $\boldsymbol{\chi} = (\hat{x}_1, \hat{x}_2, ..., \hat{x}_N, \hat{p}_1, \hat{p}_2, ..., \hat{p}_N)^T$ gives the vector in the $XXPP$ ordering.

Next, to write the CCR in terms of this vector, we define the symplectic form $\boldsymbol{\Omega}$. We define the representations of $\boldsymbol{\Omega}$ with respect to the operator vector orderings. From the name, it becomes clear that this object takes a central role in the formalism used.

Definition 5.8 (Symplectic form)**.** For a quadratures in the $XPXP$ ordering, $\boldsymbol{\xi} = (x_1, p_2, ..., x_N, p_N)$, let the symplectic form be the $2N \times 2N$ matrix

$$\Omega_N = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{5.32}$$

Note that $\boldsymbol{\Omega}$ has real entries and is anti-symmetric ($\boldsymbol{\Omega}^T = -\boldsymbol{\Omega}$). This means that $i\boldsymbol{\Omega}$ is Hermitian since $(i\boldsymbol{\Omega})^\dagger = -i\boldsymbol{\Omega}^T = i\boldsymbol{\Omega}$. Further, all the eigenvalues of $\boldsymbol{\Omega}$ are purely imaginary so that $i\boldsymbol{\Omega}$ has real eigenvalues.

The canonical commutation relation in the $XPXP$ ordering can therefore be summarised as

$$[\boldsymbol{\xi}, \boldsymbol{\xi}^T] = i\boldsymbol{\Omega}, \tag{5.33}$$

where the commutator of a vector with its transpose should be read as the outer product.

It is possible to translate that statement to the alternate ordering. First we define the map that allows a change of ordering:

Definition 5.9 (Ordering transformation)**.** The ordering transformation λ between $XPXP$ to $XXPP$ is a $2N \times 2N$ matrix defined piecewise by

$$\lambda_{ij} = \begin{cases} 1 & (i,j) = (k, 2k-1), \quad k \in [1, N], \\ 1 & (i,j) = (N+k, 2k), \quad k \in [1, N], \\ 0 & \text{otherwise.} \end{cases} \tag{5.34}$$

The transformation λ acts by congruence to transform matrices between the quadrature orderings. Note that $\lambda^T = \lambda^{-1}$. The definitions of symbols in each ordering can be found in table 5.2.

The vector of quadratures in the $XXPP$ ordering may then be written as

$$\boldsymbol{\chi} = \lambda\boldsymbol{\xi}, \tag{5.35}$$

and gives the alternative CCR

$$[\boldsymbol{\chi}, \boldsymbol{\chi}^T] = i\Sigma_N, \quad \text{with } \Sigma_N = \begin{pmatrix} \mathbb{O}_N & \mathbb{1}_N \\ -\mathbb{1}_N & \mathbb{O}_N \end{pmatrix}, \tag{5.36}$$

Table 5.2: Ordering conversion between $XPXP$ and $XXPP$ orderings of objects used in this part. The transformation matrix, λ, as given in Def. 5.9, is an orthogonal matrix with $\lambda_{j,2j-1} = \lambda_{N+j,2j} = 1, j = 1, ..., N$, the only non-zero elements.

Object name (Symbol)	Conversion
Quadrature vector (ξ)	$\chi = \lambda\xi$
Covariance matrix (γ)	$\sigma = \lambda\gamma\lambda^T$
Symplectic form (Ω_N)	$\Sigma_N = \lambda\Omega_N\lambda^T$
Symplectic matrix (S)	$Q = \lambda S\lambda^T$

where $\mathbb{O}_N$ and $\mathbb{1}_N$ are the $N \times N$ zero and identity matrices respectively. The conversion between symplectic forms in the different orderings is once again done via congruence with λ ($\Sigma_N = \lambda\Omega_N\lambda^T$). For a more complete list of symbols used in the different transformations please refer to table 5.2.

Using the symplectic form in Def. 5.8, we can define the symplectic group, $Sp(2N, \mathbb{R})$, which is made up of real matrices that leave the symplectic form invariant under congruence

$$Sp(2N, \mathrm{R}) = \{S \mid S\Omega S^T = \Omega\}. \tag{5.37}$$

The group operation is matrix multiplication.

Before moving on to defining the Gaussian operations, we introduce a set of important invariants: the symplectic eigenvalues.

Definition 5.10 (Symplectic eigenvalues)**.** The symplectic eigenvalues, ν_i, of an $N \times N$ matrix A are the eigenvalues

$$\mathrm{eig}(i\Omega_N A) = \{\nu_1, \nu_2, ..., \nu_N\}, \tag{5.38}$$

with Ω_N the symplectic form. We use the symbol W to represent the diagonal matrix whose entries are the symplectic eigenvalues of A. That is, $W = \mathrm{diag}(\nu_1, ..., \nu_N)$.

For a positive definite matrix A, we will see in Thm. 5.1 that one may find a decomposition $A = SWS^T$ for some symplectic matrix $S \in Sp(2N, \mathbb{R})$. It is interesting to note that under the transformation $S^T AS$, the symplectic eigenvalues correspond to the normal mode frequencies.

5.2.1 Gaussian quantum states

In characterising the Gaussian states, one may ask which Hamiltonians produce them. In this section, we characterise those Hamiltonians.

One may get a Hamiltonian operator (Hamiltonian) from a symmetric matrix[5] H and vector $\boldsymbol{\Xi}$ through

$$\hat{H} = \frac{1}{2}\boldsymbol{\xi}^T H\boldsymbol{\xi} + \boldsymbol{\xi}^T\boldsymbol{\Xi}, \tag{5.39}$$

where $\boldsymbol{\Xi} \in \mathbb{R}^{2N}$ and $\boldsymbol{\xi}$ is the vector of quadrature operators from Def. 5.7. We call $H \in Sym(2N, \mathbb{R})$ the Hamiltonian matrix and it describes energy relations that are quadratic in the quadrature operators. Meanwhile, linear relations are encoded in $\boldsymbol{\Xi}$. For example, the array of N harmonic oscillators would be given by $H = \mathbb{1}$ and $\boldsymbol{\Xi} = \mathbf{0}$, the zero vector: $\hat{H} = \frac{1}{2}\boldsymbol{\xi}^T\boldsymbol{\xi} = \frac{1}{2}\sum_i(\hat{x}_i^2 + \hat{p}_i^2)$. We refer to Hamiltonian operators as "linear" or of "first-order" if they are generated by functions

[5] Not to be confused with the Hadamard transformation from part I.

linear in the quadratures ($H = \mathbb{O}$); and "quadratic" or of "second-order" if $H \neq \mathbb{O}$. Hamiltonians with no linear components ($\boldsymbol{\Xi} = \mathbf{0}$) are referred to as "purely quadratic".

An alternative way of writing the Hamiltonian in eq. (5.39) is through the definition $\bar{\boldsymbol{\xi}} = -H^{-1}\boldsymbol{\Xi}$, which is possible for any positive-definite H. Up to a constant, which does not alter any dynamics, we can write

$$\hat{H}' = \frac{1}{2}(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T H (\boldsymbol{\xi} - \bar{\boldsymbol{\xi}}). \tag{5.40}$$

One may see $\bar{\boldsymbol{\xi}}$ as a shift in phase-space of the quadratures which produces a change of mean of a Gaussian state.

We now define the quantum states, starting from quadratic Hamiltonians as per eq. (5.39).

Definition 5.11. All Gaussian states may be generated from some quadratic Hamiltonian operator $\hat{H} = \frac{1}{2}(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T H (\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})$, (see eq. (5.40)):

$$\rho(H, \bar{\boldsymbol{\xi}}) = \frac{e^{-\beta \hat{H}}}{\mathrm{Tr}\left[e^{-\beta \hat{H}}\right]}, \tag{5.41}$$

with $\beta \in \mathbb{R}^+$ positive and non-zero. The limiting cases, $\beta \to \infty$, correspond to the pure Gaussian states.

Here is where the requirement of $H > 0$ in eq. (5.39) is needed as the state would not be well defined for the eigenstates corresponding to the negative eigenvalue.

5.2.2 Gaussian operations

Which operations map the set of Gaussian states to itself? We presented in the previous section the Hamiltonians that generate these states[6]. Gaussian operations are those which preserve the character of Gaussian states. That is, those operations which do not increase the polynomial of quadratures above order two in Def. 5.11.

In this section we present the Gaussian transformations in the symplectic formalism. See table 5.3 for a comparison between the unitary description of Gaussian operations and their analogs presented using the symplectic formalism in this section.

Table 5.3: Gaussian transformations in the unitary and symplectic formalisms. The symplectic form is given by $\boldsymbol{\Omega} = \bigoplus^N \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ (see Def. 5.8).

Operation	Unitary description		Symplectic description	
Displacement (Weyl)	$\hat{D}(d_x, d_p) = e^{i d_p \hat{x} - i d_x \hat{p}}$	(1.49)	$\hat{D}_{\boldsymbol{d}} = e^{i \boldsymbol{d}^T \boldsymbol{\Omega} \boldsymbol{\xi}}$	(5.12)
Single-mode rotation	$\hat{U}_{\mathrm{Rot}}(\theta) = e^{i \frac{\theta}{2}(\hat{x}^2 + \hat{p}^2)}$	(1.50)	$\Phi(\phi) = \left(\begin{smallmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{smallmatrix}\right)$	(5.54)
Single-mode squeezing	$\hat{U}_{\mathrm{Sq}}(\eta) = e^{i \frac{\eta}{2}(\hat{x}\hat{p} + \hat{p}\hat{x})}$	(1.52)	$R = \bigoplus_{j=1}^{N=1} \left(\begin{smallmatrix} r_j & 0 \\ 0 & r_j^{-1} \end{smallmatrix}\right)$	(5.52)
Two-mode beam-splitter	$\hat{U}_{\mathrm{BS}}(\Theta) = e^{i \frac{\Theta}{2}(\hat{x}_1 \hat{p}_2 - \hat{x}_2 \hat{x}_1)}$	(1.53)	$BS_2(\theta)$	(5.53)

[6] See also section 1.4.4 in chapter 1 for another route to the result that Gaussian operations are generated by Hamiltonians that are quadratic in the quadratures. There we follow ref. [31].

In the phase space of continuous variable quantum states, the displacement operators are known as Weyl operators[7].

Definition 5.12 (Weyl operators)**.** For a vector of quadratures $\boldsymbol{\xi}$ and a real-valued vector $\boldsymbol{d}$, let the Weyl operator be given by

$$\hat{D}_{\boldsymbol{d}} = e^{i\boldsymbol{d}^T\Omega\boldsymbol{\xi}}. \tag{5.42}$$

Note that the inverse is $\hat{D}^\dagger = \hat{D}_{-\boldsymbol{d}}$. Two Weyl operators may be joined through

$$\hat{D}_{\boldsymbol{d}_1+\boldsymbol{d}_2} = \hat{D}_{\boldsymbol{d}_1}\hat{D}_{\boldsymbol{d}_2}e^{\frac{i}{2}\boldsymbol{d}_1^T\Omega\boldsymbol{d}_2}, \tag{5.43}$$

with $\boldsymbol{d}_1$ and $\boldsymbol{d}_2$ N-dimensional vectors with real entries. [26]

From Def. 5.12, one may find that

$$\hat{D}_{-\boldsymbol{d}}\boldsymbol{\xi}\hat{D}_{\boldsymbol{d}} = \boldsymbol{\xi} - \boldsymbol{d}, \tag{5.44}$$

so the conjugation of the quadratures with the Weyl operators may indeed be interpreted as displacements in phase-space. The Weyl operators are to be understood as acting on each element of $\boldsymbol{\xi}$ individually.

Using these definitions, one may then write the Hamiltonian in eq. (5.40) as

$$\hat{H}' = \frac{1}{2}\hat{D}_{-\bar{\boldsymbol{\xi}}}\boldsymbol{\xi}^T H\boldsymbol{\xi}\hat{D}_{\bar{\boldsymbol{\xi}}}. \tag{5.45}$$

While the Weyl transforms may be understood as transformations generated by linear Hamiltonians, we now consider the transformations generated by purely quadratic ones: $\frac{1}{2}\boldsymbol{\xi}^T H\boldsymbol{\xi}; \bar{\boldsymbol{\xi}} = 0$. Such Hamiltonians may be produced from the more general one in eq. (5.45) by a displacement (through a linear Hamiltonian). Let therefore $\hat{H} = \frac{1}{2}\boldsymbol{\xi}^T H\boldsymbol{\xi}$ for now. The time evolution of the quadratures may be given as

$$\dot{\boldsymbol{\xi}} = \Omega H\boldsymbol{\xi}. \tag{5.46}$$

This may be verified element-wise[8] and has the solution $\boldsymbol{\xi}(t) = e^{\Omega Ht}\boldsymbol{\xi}(0)$.

The transformation $e^{\Omega Ht}$ represents an evolution in time due to a time-independent Hamiltonian and is given by a unitary operator acting on the underlying Hilbert space. It must therefore preserve the CCR and one finds that it preserves the symplectic form after a congruence operation. Working from the CCR $[\boldsymbol{\xi}, \boldsymbol{\xi}^T] = i\Omega$ (eq. (5.33)) we have that

$$[\boldsymbol{\xi}, \boldsymbol{\xi}^T] = [e^{\Omega Ht}\boldsymbol{\xi}, \boldsymbol{\xi}^T(e^{\Omega Ht})^T] = e^{\Omega Ht}[\boldsymbol{\xi}, \boldsymbol{\xi}^T](e^{\Omega Ht})^T = e^{\Omega Ht}i\Omega(e^{\Omega Ht})^T. \tag{5.47}$$

That is

$$e^{\Omega Ht}\Omega(e^{\Omega Ht})^T = \Omega, \tag{5.48}$$

which, by definition, means that $e^{\Omega Ht}$ is a symplectic matrix (see eq. (5.37)). We use the symbol S to define the symplectic matrices generated from purely quadratic Hamiltonians $S = e^{\Omega Ht}$.

[7] The name is related to the Weyl transform or correspondence: a map between operators in the Schrodinger picture and functions in quantum phase space [124]. Here, the Weyl operators are the operators obtained through the Weyl correspondence which are linear in the quadrature operators.

[8] From [26], p.41:

$$\begin{aligned}\dot{\xi}_j &= \frac{i}{2}[\hat{H}, \xi_j] = \frac{i}{2}\sum_{mn}[\xi_m H_{mn}\xi_n, \xi_j] = \frac{i}{2}\sum_{mn}H_{mn}(\xi_m[\xi_n, \xi_j] + [\xi_m, \xi_j]\xi_n)\\ &= \sum_{mn}\Omega_{jm}H_{mn}\xi_n,\end{aligned}$$

where we used that $[\xi_m, \xi_n] = i\Omega_{mn}$, the antisymmetry of Ω and that H is symmetric.

We note here that the matrices S describe the action of purely quadratic Hamiltonians:

$$e^{\frac{i}{2}\boldsymbol{\xi}^T H \boldsymbol{\xi}} \boldsymbol{\xi} e^{\frac{-i}{2}\boldsymbol{\xi}^T H \boldsymbol{\xi}} = S\boldsymbol{\xi}, \tag{5.49}$$

where we absorbed the time variable into H.

The Weyl operators from Def. 5.12 and the symplectic transformations Def. 5.5 describe all Gaussian transforms. This may be seen by noting that the former are generated by linear Hamiltonians while purely quadratic Hamiltonians generate the latter. Thus a general Gaussian Hamiltonian, as in eq. (5.39), may be generated by combinations $\hat{D}_{\boldsymbol{d}}$ and S.

Symplectic matrices are also useful in their role for decomposing symmetric matrices via Williamson's theorem.

Theorem 5.1 (Williamson's Theorem)**.** *A real symmetric positive definite $2N \times 2N$ matrix, A, can be taken to diagonal form, W, through congruence with some symplectic matrix.[125, 126] That is, for any $A \in PD(2N)$, there is a matrix $S \in Sp(2N)$ and diagonal $W \in \mathcal{M}(2N)$ such that*

$$A = SWS^T. \tag{5.50}$$

The entries of W are the symplectic eigenvalues of A. This statement holds in either ordering of the quadrature operators, which can be verified by transforming the matrices S, A and W by the ordering transformation λ (Def. 5.9).

Symplectic matrices may in turn be written as a product of two orthogonal and a diagonal matrix, which are linked to optical elements.

Theorem 5.2 (Bloch-Messiah decomposition)**.** *Any symplectic matrix S may be written in terms of two orthogonal and symplectic matrices with unit determinant, $U, V \in Sp(2N, \mathbb{R}) \cap SO(2N)$, and diagonal $R \in \mathcal{M}(2N, \mathbb{R})$ as follows [26, 127]:*

$$S = VRU, \tag{5.51}$$

where

$$R = \bigoplus_{j=1}^{N} \begin{pmatrix} r_j & 0 \\ 0 & r_j^{-1} \end{pmatrix}. \tag{5.52}$$

The matrix R is usually referred to as the *active*[9] elements: squeezers. Squeezing gets its name from the effect on the second statistical moment of Gaussian states - the width of the Gaussian in phase space gets scaled in orthogonal axes by stretching and squeezing. In quantum optics the terminology used is that a quadrature is squeezed while the other is anti-squeezed. Squeezing along an arbitrary axis is also possible with anti-squeezing in the orthogonal axis. The uncertainty principle is preserved after a squeezing operation.

Next, the *passive* elements are given by the matrices U and V which preserve the energy eigenvalues of a Hamiltonian under congruence[10]. In the context of quantum optics, these describe beam-splitters and phase-shifters.

[9] The term active stems from the fact that single mode squeezing does not preserve the energy of the system which can be seen as they are generated by the Hamiltonians proportional to $s_k = x_k p_k$ which does not commute with the free Hamiltonian $[s_k, H_{\text{free}}]\ [x_k p_k, \sum_i x_i^2 + p_i^2] = [x_k p_k, x_k^2 + p_k^2] = i(p_k - x_k) \neq 0$. This stands in comparison to the *passive* elements - phase-shifters and beam-splitters - which are generated by Hamiltonians proportional to $x_i^2 + p_i^2$ and $p_i x_j - x_i p_j$ respectively and can be seen to commute with the free Hamiltonian. For more information see reference [26, sec. 5.1.2].

[10] For some Hamiltonian H with eigenvalues v and orthogonal O, $H\boldsymbol{v} = v\boldsymbol{v} \implies HO^T O\boldsymbol{v} = v\boldsymbol{v} \implies OHO^T(O\boldsymbol{v}) = v(O\boldsymbol{v}) \implies OHO^T\boldsymbol{u} = v\boldsymbol{u}$, so the eigenvalues, v, are left unchanged.

In the phase-space picture, one may parametrise the passive and active elements as follows. Beam-splitters between two modes perform a rotation in phase-space about the origin which can be parametrised by an angle θ and, in the $XPXP$ ordering, it looks like

$$BS_2(\theta) = \begin{pmatrix} \cos\theta & 0 & \sin\theta & 0 \\ 0 & \cos\theta & 0 & \sin\theta \\ -\sin\theta & 0 & \cos\theta & 0 \\ 0 & -\sin\theta & 0 & \cos\theta \end{pmatrix}, \tag{5.53}$$

where $\cos^2(\theta)$ gives the beam-splitter transmissivity. The phase-shifters are rotations in phase-space within a single mode and can be represented by 2×2 rotation matrices:

$$\Phi(\phi) = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}. \tag{5.54}$$

The squeezing transformation is given in eq. (5.52) with $r_j > 1$ modelling squeezing in the x and anti-squeezing in the p quadratures of mode j and $r_j < 1$ giving the opposite effect. Squeezing corresponds to a decrease in noise - linked to narrowing of a Gaussian distribution - while anti-squeezing has the opposite effect. Squeezing is at times given in dB (decibels), in particular in the experimental literature. The conversion is done through

$$[dB] = \left[10\log_{10}(r^2)\right]. \tag{5.55}$$

One can break down passive transformation on N modes into only two-mode beam-splitters and single mode phase-shifts [26]. Some practical methods are presented in references [128, 129]. For the particular case of three modes, a beam-splitter array can be decomposed into three beam splitters. This is the well-known Euler decomposition of a rotation in three dimensions.

Theorem 5.3 (Euler decomposition of beam-splitters on three modes)**.** *One may write any beam-splitter operation on three modes, $\mathcal{BS}$, as a product of three two-mode beam-splitter transformations, as given in eq. (5.53), extended by identities in the relevant modes. That is,*

$$\mathcal{BS}(\theta_{AB},\theta_{AC},\theta_{BC}) = BS(\theta_{BC})BS(\theta_{AC})BS(\theta_{AB}), \tag{5.56}$$

where $\theta_{AB},\theta_{AC},\theta_{BC} \in [0,2\pi]$.

The three beam-splitters between modes $A-B$, $A-C$ and $B-C$ are described by the following matrices:

$$BS(\theta_{AB}) = \left(\begin{array}{c|c} BS_2(\theta_{AB}) & \mathbb{O}_{4\times 2} \\ \hline \mathbb{O}_{2\times 4} & \mathbb{1}_2 \end{array}\right); \tag{5.57}$$

$$BS(\theta_{AC}) = \left(\begin{array}{cc|c|cc} \cos\theta_{AC} & 0 & & \sin\theta_{AC} & 0 \\ 0 & \cos\theta_{AC} & \mathbb{O}_2 & 0 & \sin\theta_{AC} \\ \hline \multicolumn{2}{c|}{\mathbb{O}_2} & \mathbb{1}_2 & \multicolumn{2}{c}{\mathbb{O}_2} \\ \hline -\sin\theta_{AC} & 0 & & \cos\theta_{AC} & 0 \\ 0 & -\sin\theta_{AC} & \mathbb{O}_2 & 0 & \cos\theta_{AC} \end{array}\right); \tag{5.58}$$

and

$$BS(\theta_{BC}) = \left(\begin{array}{c|c} \mathbb{1}_2 & \mathbb{O}_{2\times 4} \\ \hline \mathbb{O}_{4\times 2} & BS_2(\theta_{BC}) \end{array}\right). \tag{5.59}$$

5.2.3 The statistical moments of Gaussian quantum states

It is well known that Gaussian distributions can be parametrised by their two first statistical moments: the mean and variance. For multivariate distributions these become a vector and a (covariance) matrix respectively. In a similar way, Gaussian states may be parametrised by two mathematical objects carrying the same name. We define $\bar{\boldsymbol{\xi}}$ to be the first and γ the second statistical moments of quadrature operators on the state under consideration. While the statements we present apply to the first two statistical moments of any quantum state, they determine Gaussian states entirely. One may see this by recalling that Gaussian states are generated by quadratic Hamiltonians so no higher order correlations are needed for a full description[11].

We begin by defining the first moment or mean of a state.

Definition 5.13 (Gaussian state mean)**.** The vector of quadrature means on the state ρ, generated by the Hamiltonian $\hat{H} = \frac{1}{2}(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T H(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})$ is given by

$$\bar{\boldsymbol{\xi}} = \mathrm{Tr}[\rho \boldsymbol{\xi}]. \tag{5.60}$$

The non-trivial proof for identifying the vector of quadrature means with $\bar{\boldsymbol{\xi}}$ in the definition of the generating Hamiltonian, $\hat{H}$, of the state may be found in reference [26][12].

Next, we recall the definition of the covariance for classical variables. Let x_j and x_k be two classical variables with expectation value $\mu(x_j)$ and $\mu(x_k)$ respectively. Then the covariance between them is given by

$$cov(x_j, x_k) = \mu[(x_j - \mu(x_j)) \cdot (x_k - \mu(x_k))]. \tag{5.61}$$

The variance is obtained when $j = k$: $\sigma_j = cov(x_j, x_j) = \mu[(x_k - \mu(x_k))^2]$. For multivariate covariances we define the vector of variables $\boldsymbol{x} = (x_1, ..., x_N)$ so that the covariance matrix can be written as

$$cov(\boldsymbol{x}, \boldsymbol{x}) = \mu[(\boldsymbol{x} - \bar{\boldsymbol{x}}) \cdot (\boldsymbol{x} - \bar{\boldsymbol{x}})^T], \tag{5.62}$$

where $\bar{\boldsymbol{x}} = (\mu(x_1), ..., \mu(x_N))$ is the vector of means of variables $x_j, j \in [1, N]$.

Definition 5.14 (Covariance matrix)**.** The covariance matrix, γ, of a state ρ is defined as

$$\gamma = \mathrm{Tr}\big[\{(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}}), (\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T\}\rho\big], \tag{5.63}$$

where $\{\boldsymbol{\xi}, \boldsymbol{\xi}^T\} = \boldsymbol{\xi}\boldsymbol{\xi}^T + (\boldsymbol{\xi}\boldsymbol{\xi}^T)^T$ and $\boldsymbol{\xi}\boldsymbol{\xi}^T$ is to be understood as the outer product of $\boldsymbol{\xi}$ with itself as defined in eq. (5.4). Considering γ element-wise one may see that[13]

$$(\gamma)_{jk} = \langle\{\xi_j, \xi_k\}\rangle - 2\langle\xi_j\rangle\langle\xi_k\rangle \tag{5.64}$$

[11] In fact, any Gaussian state with statistical moments $\bar{\xi}$ and γ may be written as $\rho = \frac{1}{(2\pi)^N}\int_{\mathbb{R}^{2N}} d\boldsymbol{r}\, e^{-\frac{1}{4}\boldsymbol{r}^T\gamma\boldsymbol{r} + i\boldsymbol{r}^T\bar{\xi}}\hat{D}_{\Omega^T\bar{\xi}}$, where $\boldsymbol{r} = \Omega^T\boldsymbol{\xi}$. [26, eq.(4.49), p.79]

[12] It goes through expanding ρ in the Fock basis and using the state space analog of symplectic decomposition of $\boldsymbol{H}$.

[13] Starting from the definition of the anti-commutator (eq. (5.7)): $\{\boldsymbol{\xi}, \boldsymbol{\xi}^T\}_{jk} = \xi_j\xi_k + \xi_k\xi_j$ we have that.

$$\begin{aligned}
(\gamma)_{jk} &= \mathrm{Tr}\big[\{(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}}), (\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T\}_{jk}\rho\big] \\
&= \mathrm{Tr}\Big[\Big(\{\boldsymbol{\xi}, \boldsymbol{\xi}^T\}_{jk} - \{\boldsymbol{\xi}, (\bar{\boldsymbol{\xi}})^T\}_{jk} - \{\bar{\boldsymbol{\xi}}, \boldsymbol{\xi}^T\}_{jk} + \{\bar{\boldsymbol{\xi}}, (\bar{\boldsymbol{\xi}})^T\}_{jk}\Big)\rho\Big] \\
&= \mathrm{Tr}\big[(\xi_j\xi_k + \xi_k\xi_j)\rho\big] + \mathrm{Tr}\big[(\xi_j\bar{\xi}_k + \bar{\xi}_k\xi_j)\rho\big] + \mathrm{Tr}\big[(\bar{\xi}_j\xi_k + \xi_k\bar{\xi}_j)\rho\big] + \mathrm{Tr}\big[(\bar{\xi}_j\bar{\xi}_k + \bar{\xi}_k\bar{\xi}_j)\rho\big] \\
&= \mathrm{Tr}\big[\{\xi_j, \xi_k\}\rho\big] - 2\bar{\xi}_k\,\mathrm{Tr}\big[\xi_j\rho\big] - 2\bar{\xi}_j\,\mathrm{Tr}[\xi_k\rho] + 2\bar{\xi}_j\bar{\xi}_k \\
&= \mathrm{Tr}\big[\{\xi_j, \xi_k\}\rho\big] - 2\bar{\xi}_k\bar{\xi}_j - 2\bar{\xi}_j\bar{\xi}_k + 2\bar{\xi}_j\bar{\xi}_k \\
&= \mathrm{Tr}\big[\{\xi_j, \xi_k\}\rho\big] - 2\bar{\xi}_k\bar{\xi}_j. \quad \square
\end{aligned}$$

with ξ_j the j^{th} element of the vector of canonical operators and where the mean is taken over the quantum state in question and the means are equated as $\bar{\xi}_j = \langle \xi_j \rangle$.

Notice that, differing from the classical definition in eq. (5.62), we included the anti-commutator, $\{\cdot,\cdot\}$, in the definition. This is because the elements of $\boldsymbol{\xi}$ do not all commute and we want the covariance matrix to be symmetric. Notice also that the variance terms, $(\gamma)_{jj}$, have a factor of 2 in the first term which does not appear in the usual definition of variance. This is because we want the vacuum covariance matrix to be the identity with no scalar factors[14].

The symplectic eigenvalues ν_j of the covariance matrix of a Gaussian state generated by the Hamiltonian $H = S_H \text{diag}(\omega_1, \omega_2, ...) S_H^T$ are obtained by $\nu_j = \frac{1+e^{-\beta\omega_j}}{1-e^{-\beta\omega_j}}$ [26]. One may also see here that all Gaussian states on N modes must have $\nu_j \geq 1$ for all $j = 1, ..., N$ and that the pure states ($\beta \to \infty$) have $\nu_j = 1$ for all $j = 1, ..., N$.

The covariance matrix holds all correlation properties of Gaussian states, so it plays a central role in codifying the uncertainty principle in the symplectic formalism.

Theorem 5.4 (Robertson uncertainty relation)**.** *For some quantum state ρ, its covariance matrix, γ, satisfies*

$$\gamma + i\Omega \geq 0. \tag{5.65}$$

This rephrases the well known uncertainty relation between conjugate variables in terms of the CM[15]. It may be equivalently recast in terms of the symplectic eigenvalues of γ through symplectic diagonalisation: Let $S \in Sp$ be such that $S^T \gamma S = W$ via Williamson's Theorem (Thm. 5.1) and using the defining property of symplectic matrices, $S^T \Omega S = \Omega$, we find that

$$W + i\Omega = \bigoplus_{j=1}^{N} \begin{pmatrix} \nu_j & i \\ -i & \nu_j \end{pmatrix} \geq 0, \tag{5.66}$$

where ν_j are the symplectic eigenvalues of γ. This is equivalent to requiring

$$\nu_j \geq 1 \text{ for } j \in [1, N]. \tag{5.67}$$

This statement will be used when phrasing the so-called positive-partial transposition (PPT) criterion at the level of the covariance matrix and is used extensively in the next chapter.

Covariance matrices are symmetric positive definite matrices: Def. 5.14 (Covariance matrix) is invariant under the index swap $j \leftrightarrow k$. Positive definiteness may be seen from Thm. 5.4 [26] as γ fulfils a stricter inequality to positivity. Non-negativity, $\gamma \geq 0$, follows directly from Thm. 5.4 since Ω has no real non-zero eigenvalues[16]. Strict positivity is more involved and can be shown by contradiction [26][17].

Since Gaussian states are completely characterised by the mean ($\bar{\boldsymbol{\xi}}$) and covariance matrix (γ) we can understand the dynamics by tracking the changes to only these objects.

---

[14] See for example the remark after eq. (5.129) or the second paragraph in section 6.5 of ref. [26].

[15] The proof for this relationship [26] follows from noticing that $2\,\text{Tr}\left[\rho(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T\right] = \gamma + \text{Tr}\left[\rho[\boldsymbol{\xi}, \boldsymbol{\xi}^T]\right] = \gamma + i\Omega$, where we used eq. (5.10) and that $\boldsymbol{v}\boldsymbol{v}^T$ is the outer product between vectors as defined in eq. (5.4). Upon defining $\hat{O} = \sqrt{2}\boldsymbol{y}^\dagger(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})$ for arbitrary $\boldsymbol{y} \in \mathbb{C}^{2N}$, one finds that $\boldsymbol{y}^\dagger(\gamma + i\Omega)\boldsymbol{y} = \text{Tr}\left[\rho\hat{O}\hat{O}^\dagger\right] \geq 0$. Since $\boldsymbol{y}$ was arbitrary, this proves Thm. 5.4.

[16] This follows from the fact that Ω is skew-symmetric so any real eigenvalue is zero: for some vector $\mathbf{v} \in \mathbb{R}^{2N}$ let $\mathbf{v}^T\Omega\mathbf{v} = a \in \mathbb{R}$; we have then simultaneously that $-a = \mathbf{v}^T\Omega^T\mathbf{v} = (\mathbf{v}^T\Omega\mathbf{v})^T = a$ so that $a \in \mathbb{R}$ is nullity. □

[17] Assume $\mathbf{u} \in \mathbb{R}^{2N}$ to be such that $\mathbf{u}^T\gamma\mathbf{u} = 0$. Then let $\mathbf{w} = ia\mathbf{u} + v$ for some $\mathbf{v} \in \mathbb{R}^{2N}$ with $\mathbf{v}^T\Omega\mathbf{u} = b \neq 0$ where $b \in \mathbb{R}$. Note then that $\mathbf{w}^\dagger(\gamma + i\Omega)\mathbf{w} = \mathbf{v}^T\gamma\mathbf{v} - 2ab$ so one may choose b so that Thm. 5.4 is not satisfied, reaching a contradiction. □ In this proof we used that $\mathbf{x}^T\Omega\mathbf{x} = 0$ for all $\mathbf{x} \in \mathbb{R}^{2N}$ and $\mathbf{u}^T\gamma\mathbf{v} = \mathbf{v}^T\gamma\mathbf{u}$ since γ is symmetric .

We start with the Weyl operators from Def. 5.12 - displacements generated by linear Hamiltonians. Applying the state transformations $\rho \mapsto D_{-\boldsymbol{d}}\rho D_{\boldsymbol{d}}$, into Defs. 5.13 and 5.14 (Gaussian state mean and Covariance matrix), we find the rules

$$\begin{aligned}\bar{\boldsymbol{\xi}} &\mapsto \bar{\boldsymbol{\xi}} = \bar{\boldsymbol{\xi}} - \boldsymbol{d} \\ \gamma &\mapsto \gamma,\end{aligned} \tag{5.68}$$

where $\boldsymbol{d}$ is a vector of displacements in the correct quadrature ordering. For getting this result, remember that the mean $\bar{\boldsymbol{\xi}}$ is also shifted by the displacement.

The latter is found by recalling that the Weyl operators act on $\boldsymbol{\xi}$ element-wise and that the trace is invariant under permutations of its argument: $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$. Let γ' be the covariance matrix of the displaced state, $\rho' = \hat{D}_{-\boldsymbol{d}}\rho\hat{D}_{\boldsymbol{d}}$. The mean is now $\bar{\boldsymbol{\xi}}' = \bar{\boldsymbol{\xi}} - \boldsymbol{d}$. We have therefore

$$\begin{aligned}\gamma'_{jk} &= \mathrm{Tr}\big[\{(\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d})), (\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d}))^T\}_{jk}\hat{D}_{-\boldsymbol{d}}\rho\hat{D}_{\boldsymbol{d}}\big] \\ &= \mathrm{Tr}\Big[\hat{D}_{\boldsymbol{d}}\left((\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d}))_j(\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d}))_k + (\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d}))_k(\boldsymbol{\xi} - (\bar{\boldsymbol{\xi}} - \boldsymbol{d}))_j\right)\hat{D}_{-\boldsymbol{d}}\rho\Big] \\ &= \mathrm{Tr}\big[\hat{D}_{\boldsymbol{d}}(\xi_j - (\bar{\xi}_j - d_j))(\xi_k - (\bar{\xi}_k - d_k))\hat{D}_{-\boldsymbol{d}} + \hat{D}_{\boldsymbol{d}}(\xi_k - (\bar{\xi}_k - d_k))(\xi_j - (\bar{\xi}_j - d_j))\hat{D}_{-\boldsymbol{d}}\rho\big],\end{aligned} \tag{5.69}$$

where we used that the commutator of quadrature vectors is, in term of components, given by $[\boldsymbol{v}, \boldsymbol{v}^T]_{jk} = v_j v_k - v_k v_j$ as per eq. (5.8).

Let us look at one of the terms inside the trace. From eq. (5.44) we get that $\hat{D}_{\boldsymbol{d}}\boldsymbol{\xi}\hat{D}_{-\boldsymbol{d}} = \boldsymbol{\xi} + \boldsymbol{d}$ by swapping signs in the subscript of the Weyl operators. Recall also that $\bar{\boldsymbol{\xi}}, \boldsymbol{d} \in \mathbb{R}^{2N}$ so the Weyl operators give the identity on each element. We find therefore that

$$\begin{aligned}\hat{D}_{\boldsymbol{d}}(\xi_j - (\bar{\xi}_j - d_j))(\xi_k - (\bar{\xi}_k - d_k))\hat{D}_{-\boldsymbol{d}} &= \hat{D}_{\boldsymbol{d}}(\xi_j - (\bar{\xi}_j - d_j))\hat{D}_{-\boldsymbol{d}}\hat{D}_{\boldsymbol{d}}(\xi_k - (\bar{\xi}_k - d_k))\hat{D}_{-\boldsymbol{d}} \\ &= (\hat{D}_{\boldsymbol{d}}\xi_j\hat{D}_{-\boldsymbol{d}} - (\bar{\xi}_j - d_j))(\hat{D}_{\boldsymbol{d}}\xi_k\hat{D}_{-\boldsymbol{d}} - (\bar{\xi}_k - d_k)) \\ &= ((\xi_j + d_j) - (\bar{\xi}_j - d_j))((\xi_k + d_k) - (\bar{\xi}_k - d_k)) \\ &= (\xi_j - \bar{\xi}_j)(\xi_k - \bar{\xi}_k).\end{aligned} \tag{5.70}$$

This means that

$$\begin{aligned}\gamma'_{jk} &= \mathrm{Tr}\big[\big((\xi_j - \bar{\xi}_j)(\xi_k - \bar{\xi}_k) + (\xi_k - \bar{\xi}_k)(\xi_j - \bar{\xi}_j)\big)\,\rho\big] \\ &= \mathrm{Tr}\big[\{(\boldsymbol{\xi} - \bar{\boldsymbol{\xi}}), (\boldsymbol{\xi} - \bar{\boldsymbol{\xi}})^T\}_{jk}\rho\big] \\ &= \gamma_{jk}.\end{aligned} \tag{5.71}$$

That is

$$\gamma' = \gamma, \tag{5.72}$$

as noted in eq. (5.68).

In this part, we deal with entanglement properties so eq. (5.68) is of particular interest. It implies that displacement operations are irrelevant for properties dependent only on second moments. It also means that for any states we consider when investigating entanglement properties, we may freely nullify the mean: $\bar{\boldsymbol{\xi}} = 0$.

Next, the mean and covariance matrix are mapped by transformations described by symplectic matrices, S, as

$$\bar{\boldsymbol{\xi}} \mapsto S\bar{\boldsymbol{\xi}} \tag{5.73}$$

$$\gamma \mapsto S\gamma S^T, \tag{5.74}$$

where the state has been transformed as $\rho \to \hat{S}^\dagger \rho \hat{S}$ with $\hat{S} = e^{\frac{i}{2}\xi^T H \xi}$ and $S = e^{\Omega H}$. This follows from the map of quadratures $\boldsymbol{\xi}$ under such an operation since $\hat{S}^\dagger \boldsymbol{\xi} \hat{S} = S\boldsymbol{\xi}$ (see eq. (5.49)).

One point to note before we proceed, the statements about the mean and CM derived in this section are general in that they apply for *any* quantum state. However, non-Gaussian states may require higher statistical moments for a full description. In particular, the CM is not sufficient to describe all entanglement properties: the absence of entanglement in the CM does not exclude all entanglement in non-Gaussian states.

5.2.3.1 Statistical moments of state reductions and extensions

One may combine or separate composite states. These we call extensions and reductions respectively. We begin with the former.

Let ρ_A and ρ_B be two Gaussian density matrices with means $\bar{\boldsymbol{\xi}}_A$ and $\bar{\boldsymbol{\xi}}_A$ and covariance matrices γ_A and γ_B. The *extended* state $\rho = \rho_A \otimes \rho_B$ has the statistical moments composed as

$$\bar{\boldsymbol{\xi}} = \bar{\boldsymbol{\xi}}_A \oplus \bar{\boldsymbol{\xi}}_B = \begin{pmatrix} \boldsymbol{\xi}_A \\ \boldsymbol{\xi}_B \end{pmatrix} \tag{5.75}$$

$$\gamma = \gamma_A \oplus \gamma_B = \begin{pmatrix} \gamma_A & \mathbb{O}_2 \\ \mathbb{O}_2 & \gamma_B \end{pmatrix}, \tag{5.76}$$

with a natural extension to a larger composition of states.

If, instead, we start with a state ρ with $\bar{\boldsymbol{\xi}} = \bar{\boldsymbol{\xi}}_A \oplus \bar{\boldsymbol{\xi}}_B$ and $\gamma_{AB} = \begin{pmatrix} \gamma_A & \gamma^{AB} \\ \gamma^{AB} & \gamma_B \end{pmatrix}$, then the *partial trace*[18] with respect to mode A is obtained by removing[19] rows and columns involving the mode index A thus decreasing the dimension of a $2N \times 2N$ CM to $2(N-1) \times 2(N-1)$. For γ_{AB} above, this would correspond to removing all submatrices except γ_B. For an N-mode state made up from modes $\mathcal{A} = \{A_i | i \in [1, N]\}$, we write the reduction onto modes $\mathcal{B} \subset \mathcal{A}$ as $\gamma_{\mathcal{B}}$. Since the number of modes dealt with here is often not large, we sometimes use the convention of labelling the modes with capital Latin letters. We might therefore write γ_{AC} for the reduction of some, say, three-modes covariance matrix γ_{ABC} when removing mode B. To avoid confusion, we use the superscript to denote the 2×2 covariance matrix between two modes. The remnant modes after a partial trace is referred to as a *marginal*. Since we use it in the coming chapter, we put it in a definition.

Definition 5.15 (Marginals of states (covariance matrix))**.** Let $\gamma_{\mathcal{A}}$ be the covariance matrix of a multi-mode Gaussian state. The *marginal*, labelled by subscript $\mathcal{B} \subset \mathcal{A}$, is the resulting covariance matrix after a partial trace with respect to a subset, $\mathcal{B}$ of modes. That is

$$\gamma_{\mathcal{A}} = PT_{\mathcal{A}\backslash\mathcal{B}}[\gamma], \tag{5.77}$$

with $PT_{\mathcal{A}\backslash\mathcal{B}}[\cdot]$ denoting the partial trace operation, on the level of covariance matrices, over modes not in $\mathcal{B}$ ($\mathcal{A}\backslash\mathcal{B}$ is the complement of $\mathcal{B}$ in $\mathcal{A}$).

In the three-mode example, γ_{ABC} has three possible marginals: γ_{AB}, γ_{AC}, and γ_{BC}, obtained by removing modes C, B, and A respectively.

Next, we consider the partial transposition of a multi-mode state and its effect on the statistical moments.

[18] The term partial trace comes from the operation on density matrices.

[19] At the level of density matrices, reductions are obtained through the partial trace map. The global term that appears does not move onto the covariance matrix. Reductions are therefore obtained by straight removal of the relevant rows and columns.

Partial transposition, across collection of modes A and B, of a state at the phase space level can be described by the map $(\mathbb{1} \otimes \mathcal{T})$ mapping $\rho_A \otimes \rho_B \mapsto \rho_A \otimes \mathcal{T}\rho_B$, where $\mathcal{T}\rho_B := \rho_B^T$ and is extended to states with more partitions by applying the transformation $\mathcal{T}$ to the relevant modes in some local basis. Using the definitions for the quadratures from the creation and annihilation operators from eq. (5.28): $\hat{x} = (\hat{a} + \hat{a}^\dagger)\backslash\sqrt{2}$ and $\hat{p} = (\hat{a} + \hat{a}^\dagger)\backslash i\sqrt{2}$ for position and momentum respectively and noting that the action of the bosonic operators, $\hat{a}$ and $\hat{a}^\dagger$, on Fock states is entirely described by real coefficients, one may equate the hermitian conjugate of $\hat{a}$ with it transposition: $\hat{a}^\dagger = \hat{a}^T$. Thus, we find the effect of transposition on the quadratures:

$$\hat{x}^T = \frac{(\hat{a} + \hat{a}^\dagger)^T}{\sqrt{2}} = \hat{x}, \quad \hat{p}^T = \frac{(\hat{a} - \hat{a}^\dagger)^T}{i\sqrt{2}} = -\hat{p}. \tag{5.78}$$

Transposition thus produces a negative sign in each momentum term (resultingly, $\langle \hat{p}^2 \rangle$ does not change sign). On statistical moments, this means that transposition can be represented by the operation of $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ on the mode undergoing transposition. For multi-mode states, only the relevant momenta get a sign change so we define the partial transposition (PT) operator as follows.

Definition 5.16 (Partial transposition (PT) on statistical moments)**.** Let $\boldsymbol{\xi}$ and γ be the statistical moments of some quantum state of N modes. Partial transposition in modes $\mathcal{K}$ is described by the operator

$$T_{\mathcal{K}} = \bigoplus_{j=1}^{N} \tau \quad \text{with} \quad \tau = \begin{cases} \sigma_z & j \in \mathcal{K}, \\ \mathbb{1}_2 & \text{otherwise.} \end{cases} \tag{5.79}$$

The partial transposition transformation T acts by congruence on the covariance matrix so, for $\mathcal{K} = \{B\}$ and $\gamma = \left(\begin{smallmatrix} \gamma_A & \gamma^{AB} \\ \gamma^{AB} & \gamma_B \end{smallmatrix}\right)$, we write

$$\gamma^{T_B} := T_B \gamma T_B^T = T \begin{pmatrix} \gamma_A & \gamma^{AB} \\ \gamma^{AB} & \gamma_B \end{pmatrix} T^T = \begin{pmatrix} \gamma_A & -\gamma^{AB} \\ -\gamma^{AB} & \gamma_B \end{pmatrix}. \tag{5.80}$$

Note that the diagonal element γ_B is the variance in mode B so involves the square of $\hat{p}_B$ and has therefore no sign change. Note also that $\gamma^{T_A} = \gamma^{T_B}$ since the negative sign appears in the off-diagonal terms which involve terms of both marginals.

Before moving on to defining multipartite entanglement on covariance matrices, we define the notion of *partitions*.

Definition 5.17 (Partitions of multimode states)**.** For a multimode CM, $\gamma_{\mathcal{A}}$, a partition into k parts, labelled by $\mathcal{B}_j$, with $\bigcup_{j=1}^{k} \mathcal{B}_j = \mathcal{A}$, is written as

$$\gamma_{\mathcal{B}_1|\mathcal{B}_2|\ldots|\mathcal{B}_k}, \tag{5.81}$$

Each part $\mathcal{B}_j$ may be formed by more than one mode.

A three mode CM, γ_{ABC} has three possible bipartitions, labelled by $AB|C$,$AC|B$, and $A|BC$. Practically, operations on one part of the state correspond to acting on the CM elements with the relevant mode indices.

We now have all the required tools to treat entanglement properties at the level of covariance matrices.

5.3 Entanglement in terms of density matrices

Entanglement is a quintessentially quantum property. It provides a concrete example of the phrase "the sum is larger than the parts": the textbook definition characterises entanglement negatively[20] by presenting a decomposition whenever a state is *not* entangled, as we will see in section 5.3. Quantum entanglement has served to explore various phenomena - examples include open quantum systems [130, 131], quasi-particle behaviour [132] as well as in a variety of effects in quantum optics [133, 134] and a plethora of quantum information tasks - protocols ranging from ghost imaging [135], secure communication [136–138], computing [58, 63] (see also part I), to improved imaging [139], to name but a few.

In this section, we will end up with a test for so-called genuine multipartite entanglement on covariance matrices and how to find it numerically [123]. In getting there, we cover the definition of entanglement at the level of states, including the classification of multi-partite entanglement in section 5.3. In the next section, section 5.4, we rephrase the definitions to apply on the covariance matrices of quantum states.

5.3.1 Bipartite entanglement

As noted in section 1.2, entanglement is defined via its complement in the space of quantum states. We therefore start by defining the states which are *not* entangled.

Definition 5.18 (Bipartite state entanglement)**.** A quantum state ρ on the composite Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be *separable* if has the decomposition

$$\rho = \sum_j \lambda_j \rho_j^{(1)} \otimes \rho_j^{(2)} \tag{5.82}$$

with $\sum_j \lambda_j = 1$ ($\lambda_j \geq 0$ for all j) and where the subsystems are given by the density matrices $\rho^{(1)}$ and $\rho^{(2)}$ which act on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively as defined in Def. 1.1. Otherwise ρ is said to be *entangled*.

It should be noted that $\mathcal{H}_1$ and $\mathcal{H}_2$ need not be of the same dimension. In particular, they need not be made up of one state - bipartite entanglement is a statement of correlations between two components which may be composite themselves. This means that this definition already covers some type of multipartite entanglement.

States accepting Def. 5.18 are not entangled. However, the sum coefficients, λ_j, define classical correlations. In the CM of the state, these appear as entries in the off-diagonals.

Tests for bipartite entanglement abound, but we make use of one based on the partial transposition in particular[21].

Theorem 5.5 (Positive partial transpose (PPT) criterion on states)**.** *If a state ρ on Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is separable, then*

$$\rho^{T_B} \geq 0, \tag{5.83}$$

with $(.)^{T_B}$ the partial transposition map $(\mathbb{1} \otimes \mathcal{T})$ equivalent to transposition T on subsystem $\rho_B = \mathrm{Tr}_A[\rho]$ only [18, 19] (see the discussion preceding Def. 5.16). Whenever $\dim(\mathcal{H}) = \dim(\mathcal{H}_1) \times \dim(\mathcal{H}_2) \leq 6$, this condition is necessary and sufficient [20].

[20] Two terms that get to this idea of a negative definition, taken from philosophy and theology, are antithesis and apophasis. A definition by antithesis is one where one gives the negation of the original thesis. In apophatic theology, religious concepts are defined by properties they do not carry.

[21] We repeat Thm. 1.3 here.

The last statement means that it serves to characterise fully the entanglement 2×2 states. An interpretation of Thm. 5.5 is that whenever ρ is separable, its partial transposition is a valid quantum state. This interpretation remains when we move on the equivalent theorem at the level of covariance matrices (Thm. 5.7, PPT criterion on two-mode covariance matrices).

5.3.2 Genuine multipartite entanglement

There are multiple ways of classifying entanglement among more than two parties. The last sentence in Def. 5.18 (Bipartite state entanglement) evidences a certain classification of multipartite entanglement corresponding to answering the question of how many partitions are separable in a given state [140].

We start at the end of entanglement-free states. These are the states that are called *fully separable* - they are separable no matter which partitions[22] we measure entanglement across.

Definition 5.19 (Fully separable states)**.** States that are fully separable on N modes, ρ_{Fullysep}, are those for which there exists a basis such that

$$\rho_{\text{Fully sep}} = \sum_j \lambda_j \bigotimes_{k=1}^{N} \rho_j^{(k)}, \tag{5.84}$$

with $\rho_m^{(k)}$ a separable state on H_m for $m \in [1, N]$. These states are those separable across all partitions.

We may join any two states and allow them to be entangled to obtain a slightly less restrictive condition of $N-1$ separability. We may do this operation successively $(N-k)$ times to get the increasingly more inclusive sets of k-separable states

Definition 5.20 (k-separable states)**.** States of N modes that are separable across $K < N$ partitions, referred to as k-separable, are those which may be written as

$$\rho_{k-\text{sep}} = \sum_j \lambda_j \bigotimes_{k=1}^{K} \rho_j^{(k)}, \tag{5.85}$$

with $\sum_j \lambda_j = 1$ and where the sum occurs over all possible partitions into k parts[23]. The states $\rho_j^{(k)}$ may be composed of multiple entangled subsystems.

We should note here that a k-separable state could be formed by a mixture of states which are not separable across the same partitions so that the state as a whole might not be separable across some particular partition. For this reason, sometimes the convex sum is left out of the definition. Nonetheless, since our aim is to define the states with genuine N-partite entanglement, we keep the definition involving the convex sum. This is because it is unintuitive to attribute l-partite $(l > k)$ entanglement to refer to a state composed of states that are separable across k partitions[24].

[22] For a definition of partitions see Def. 5.17.

[23] The number of ways this can be done in is given by the Stirling numbers of the second kind. They are the number of ways of partitioning N labelled objects into k non-empty sets denoted $S(n,k)$. Whereas the general case is the non-trivial $S(N,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^j \binom{k}{j}(k-j)^N$, the bipartite case ($k=2$) collapses to the simple $2^{N-1}-1$.

[24] For example consider the 3-mode state

$$\rho = \lambda_1 \rho_1 \otimes \rho_{23} + \lambda_2 \rho_2 \otimes \rho_{13} + \lambda_3 \rho_3 \otimes \rho_{12}$$

Through the joining procedure of states in a partition we can see a hierarchy in the classification presented. This gives the 2-separable states forming the set including all $N > k > 2$ separable states. We call these the biseparable states.

Definition 5.21 (Biseparable states)**.** States of N modes called *biseparable* are those which can be expanded as the convex sum

$$\rho_{\text{Bisep}} = \sum_{k}^{K} \lambda_k \rho_k^{(1)} \otimes \rho_k^{(2)}, \tag{5.86}$$

with $K = 2^{N-1} - 1$[25]. We recall that the superscript in the subsystems $\rho_k^{(1)}$ and $\rho_k^{(2)}$ does not imply that the bipartition is over the same subsystems for all k (see appendix G and footnote 24).

One may write the bipartitions $\rho_k^{(1)} \otimes \rho_k^{(2)} = \rho_{\pi(k)}$ by defining the set of all possible bipartitions of N elements

$$\Pi(N) = \{\pi(k) | k \in [1, 2^{N-1} - 1]\}. \tag{5.87}$$

For three and four modes we have $\Pi(3) = \{AB|C, AC|B, A|BC\}$ and
$\Pi(4) = \{ABC|D, ABD|C, ACD|B, A|BCD, AB|CD, AC|BD, AD|BC\}$.

Once more we define genuinely multipartite entangled states through a negative condition.

Definition 5.22 (Genuine multipartite entanglement (GME))**.** A state ρ on N modes is said to be *genuine multipartite entangled* if it cannot be written as a biseparable state as per eq. (5.86).

The three-mode case is presented schematically in fig. 5.1.

Now that we have the definitions (and one criterion) of different classes of entanglement, we present one further general test of entanglement through so-called entanglement witnesses.

5.3.3 Entanglement witnesses

An entanglement witness W is an observable with non-negative expectation value in all separable states [19] - for a chosen type of separability - and has a negative expectation value for at least one entangled state. Let us define them.

Definition 5.23 (Entanglement witness on states)**.** Let W be an observable on some Hilbert space H on which the states ρ and ρ_{Sep} are also defined. If

$$\begin{aligned} \text{Tr}\left[\rho_{\text{Sep}} W\right] &\geq 0 \quad \text{for all separable } \rho_{\text{Sep}} \\ \text{Tr}[\rho W] &< 0 \quad \text{for at least one entangled } \rho, \end{aligned}$$

then W is said to be an entanglement witness.

Entanglement witnesses have formally been connected to entanglement inequalities such as, for example, the Bell inequalities [142] and p-measures [123].

---

with $\lambda_1 + \lambda_2 + \lambda_3 = 1$ [140, sec. 3.2.2]. We see that ρ is produced by, at most, bipartite entanglement and classical mixing. No term in the sum involves entanglement between all three modes so it does not seem correct to attribute genuine 3-partite entanglement. We give a CM example in appendix G.

[25] See footnote 23. The number of bipartitions of N elements may also be reached by a calculation argument. The number of ways of dividing N elements into two groups is 2^N. However, two of these are such that either part is empty. Since we want partitions with non-empty subsets we have $2^N - 2$ possibilities. Since the ordering of the partitions does not matter we half the above to get the required $2^{N-1} - 1$.

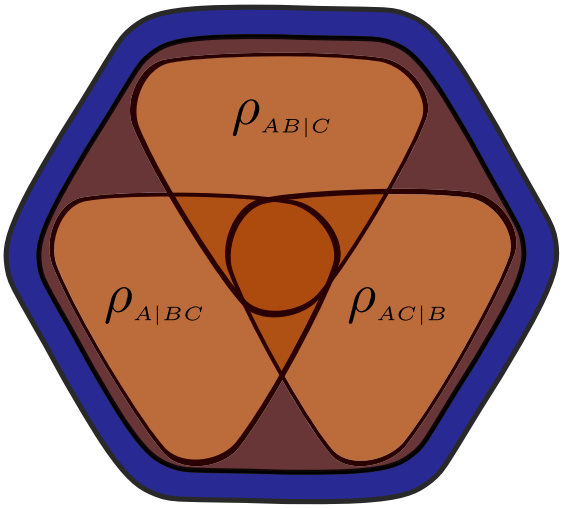


Figure 5.1: Schematic diagram of a full classification of three-partite entanglement. States separable across one bipartition are members of the orange regions. The overlapping regions correspond to states that are separable across two bipartitions or fully separable. Biseparable states (Def. 5.21) are contained in the convex sum of these, marked by the red region. States satisfying separability criteria such as the PPT criterion (Thm. 5.5) generally cover a larger set (blue region). States outside the red region carry genuine multipartite entanglement. Figure redrawn from ref. [141].

In this thesis we use so-called *optimal* witnesses of entanglement [123, 143] which are those that minimise the value $\mathrm{Tr}[\rho W]$ for a given state ρ. One may describe these pictorially through hyperplanes on the space of states that touch the set of separable states as in fig. 5.2. The insight to defining entanglement witnesses is that the set of separable states is convex: for bipartite states, $(\alpha\rho^{(1)} + (1-\alpha)\rho^{(2)})^{T_B} \geq 0$ if each $\rho^{(1)}$ and $\rho^{(2)}$ are PPT. Brushing formal details under the rug, this allows the partitioning of the space of states so that all the separable states are on one part and the other contains only entangled states (see fig. 5.2). A proof of this may be found in reference [19] and is based on a corollary of the Hahn-Banach theorem [144] which states that a functional may be defined that bisects the (real Banach) space such that two convex closed sets, where one of them is compact, are on separate parts of the bisection. In a Hilbert space, $\mathcal{H}$, the functional is defined by Hermitian $W \in \mathcal{L}(\mathcal{H})$ and the trace map: $\mathrm{Tr}[\cdot\, W]$. As we show in the next section, the notion of witnesses can be translated onto covariance matrices.

We now move on to translate these definitions in terms of covariance matrices.

5.4 Gaussian Entanglement

Since entanglement is a type of correlation, the covariance matrix is naturally the object that holds the relevant information for Gaussian states. It is worth restating two points at this stage - first, Gaussian quantum states may be fully characterised by the first and second statistical moments and; second, the mean may be set to zero since displacement operations do not affect the covariance matrix (see eq. (5.68)). Hence, for questions pertaining entanglement, we need only consider the covariance matrix of states. While there may be entanglement beyond that

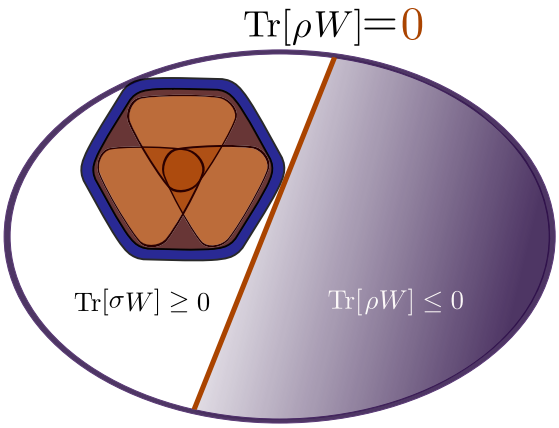


Figure 5.2: Representation of entanglement witnesses as hyperplanes on the space of quantum states (purple oval). Hyperlines are formed by the states, ρ, which give $\mathrm{Tr}[\rho W] = k$ for some $k \in \mathbb{R}$ and define the witness W. The orange line marks $k = 0$. The hyperline bisects the space with all separable states (convex set, taken from fig. 5.1) contained on one side. The witness detects GME in states in the purple region. Optimal entanglement witnesses are those that touch the convex set of separable states, which W exemplifies. Optimality is defined with respect to a particular state ρ and the optimal entanglement witness minimise $\mathrm{Tr}[\rho W]$. Although witnesses may be curved towards the separable set we only consider linear witnesses in this thesis.

present at the covariance matrix level, the statements we say are conclusive for Gaussian states. Any argument presented are implicitly constrained to entanglement at the level of CMs and be referred to as "Gaussian entanglement". For states generated by higher-than-second-order Hamiltonians the arguments apply only at the level of the second moment but not beyond.

After translating the definitions of entanglement onto statements on CMs we present some entanglement criterion in section 5.4.1 and formulate the entanglement witnesses in section 5.4.2, taking particular attention to witnesses of GME on CMs. We present a derivation of the main results of reference [123] for a numerical scheme to find such GME witnesses. We end the chapter by briefly covering trees which we use to describe the structure of witnesses that use only a subset of the CM elements to detect entanglement in section 5.7. which offers a way to phrase the main research question in this part.

5.4.1 Entanglement criteria on covariance matrices

We begin with the bipartite separability criterion and finish with the PPT test. Let us first define a two-mode CM, γ block-element wise as

$$\gamma = \begin{pmatrix} \gamma_A & \gamma^{AB} \\ \gamma^{AB} & \gamma_B \end{pmatrix}. \tag{5.88}$$

We write the partition CMs γ_A and γ_B with the subscript since these correspond to the reductions of the initial state. To avoid confusion with the reduction of a higher mode state, for example $\gamma_{ABC} \to \gamma_{AB}$, we label the covariance between modes A and B with the superscript γ^{AB}.

Theorem 5.6 (Necessary and sufficient criterion for bipartite separability)**.** *An N-mode state with CM γ is separable at the covariance matrix level across some bipartition into mode collections*

A and B if, and only if, there exist local covariance matrices γ_A and γ_B such that [145][26]

$$\gamma - \gamma_A \oplus \gamma_B \geq 0. \tag{5.89}$$

If γ does not allow for such a decomposition, then the states with CM γ are entangled. Whenever we say that γ is entangled, it is a shorthand for this statement.

For two mode states, we can use the PPT criterion from Thm. 5.5 to determine separability.

Theorem 5.7 (PPT criterion on two-mode covariance matrices)**.** *A two-mode Gaussian state with covariance matrix γ_{AB} is separable if and only if it satisfies the uncertainty principle in Thm. 5.4 under partial transposition (PPT). [147] More formally,*

$$\gamma_{AB} \text{ is of a separable state} \iff \gamma_{AB}^{T_B} + i\Omega \geq 0, \tag{5.90}$$

where the partial transposition operation, $(\cdot)^{T_B}$, is given in Def. 5.16.

Recall that the partial transposition of modes B corresponds to the map $\hat{p}_B \mapsto -\hat{p}_B$ at the level of covariance matrices. The PPT criterion in terms of density and covariance matrices allow this similar interpretation: a state is separable across a given bipartition, $A|B$, if the partial transposition $(\cdot)^{T_B}$ returns a valid quantum state ($\rho^{T_B} \geq 0$ or $\gamma^{T_B} + i\Omega \geq 0$).

The extension of Thm. 5.7 to entanglement across $1 \times N$ (but nothing larger[27]) modes was done in reference [145]. For our purposes, however, separability of two-mode Gaussian states is sufficient.

For multi-mode entanglement, one may rephrase Def. 5.21 along with the relevant definition in section 5.3.2. We only do so for GME here although the other classes may be rephrased based on the statements presented herein.

Definition 5.24 (Biseparability on covariance matrices)**.** A covariance matrix γ_{Bisep} of N modes belongs to a biseparable state, as defined in Def. 5.21, if there exist positive $\lambda_k \leq 1$ and covariance matrices $\gamma_{\pi(k)}$ which are block-diagonal across the bipartition $\pi(k)$ such that [123]

$$\gamma_{\text{Bisep}} - \sum_{k=1}^{K} \lambda_k \gamma_{\pi(k)} \geq 0, \tag{5.91}$$

with the $K = 2^{N-1} - 1$ bipartitions $\pi(k)$ defined as in eq. (5.87). States with covariance matrices that do not satisfy this inequality are **genuinely multipartite entangled**.

[26] ($\Rightarrow$): If γ satisfies eq. (5.89), then we may write $\gamma = (\gamma_A \oplus \gamma_B) + Y$ for some $Y \geq 0$. Such a CM corresponds to a product state (with CM $\gamma_A \oplus \gamma_B$) prepared by local unitary displacements with Gaussian weights (distributed according to CM Y) [26, Sec. 5.3.2].

($\Leftarrow$): If γ is the CM of a separable state, then the density matrix of the state can be decomposed into a convex mixture of separable states with uncorrelated CMs. For a state $\rho = \sum_k \lambda_k \rho_A^{(k)} \otimes \rho_B^{(k)}$, we have the following inequality [26, 146]

$$\gamma(\rho) = \sum_k \lambda_k \gamma\left(\rho_A^{(k)} \otimes \rho_B^{(k)}\right) + \sum_k \lambda_k \{\bar{\xi}_k, \bar{\xi}_k^T\} - \left\{\sum_j \lambda_j \bar{\xi}_j, \sum_k \lambda_k \bar{\xi}_k^T\right\} \geq \sum_k \lambda_k \gamma(\rho_A^{(k)} \otimes \rho_B^{(k)}),$$

where $\gamma(\rho_k)$ is the CM of state ρ_k. Identifying $\sum_k \lambda_k \gamma\left(\rho_A^{(k)} \otimes \rho_B^{(k)}\right)$ with $\gamma_A \oplus \gamma_B$ completes the proof.

[27] The authors of ref. [145] produce and example of a 2×2 mode entangled state is shown to be positive under partial transposition.

We refer to the CMs being entangled although this is a short-hand for "the CM corresponds to an entangled state".

As was the case for biseparable density matrices, biseparable covariance matrices form a convex set[28]. This means that fig. 5.1 may be repurposed by swapping $\rho \to \gamma$.

5.4.2 Optimal witnesses on covariance matrices

The concept of optimal witnesses introduced in section 5.3.3 can be translated onto the space of covariance matrices: fig. 5.2 could be inserted here by swapping $\rho \to \gamma$. This is possible because the separable covariance matrices also form a convex closed set so hyperplanes may be defined that partition the set of covariance matrices with the separable states contained entirely on one of the partitions. The witness on CMs may be defined as follows.

Theorem 5.8 (Witnesses on covariance matrices)**.** *The two inequalities [123]*

$$\begin{aligned} \mathrm{Tr}[\gamma W] &< 1 \quad \textit{for at least one entangled } \gamma, \\ \mathrm{Tr}\left[\gamma_{Sep} W\right] &\geq 1 \quad \textit{for all separable } \gamma_{Sep} \end{aligned}$$

define an entanglement witness on covariance matrices. Such witnesses on N mode states are $2N \times 2N$ symmetric positive definite matrices acting on covariance matrices [123].

We provide proofs of Thm. 5.8 for bipartite and genuine multipartite entanglement in sections 5.6.1 and 5.6.2 respectively[29].

There are some minor differences when comparing to the definition at the level of states. The equations that characterise the witnesses on covariance matrices are bounded by 1 and the trace does not lend itself to the same interpretation as the mean. The bound of unity becomes clear in section 5.6 where we present the task of finding the optimal entanglement witness on CMs as an optimization problem.

Another difference is the meaning of $\mathrm{Tr}[\rho W]$ and $\mathrm{Tr}[\gamma W]$. For density states, the trace is the expected value of the operator W. Meanwhile, the trace of the product γW corresponds to a linear combination of covariance measurements, $\langle \hat{q}_j \hat{q}_k \rangle_\rho$ for $\hat{q} = \hat{x}, \hat{p}$, contained in γ with weights set by the entries of W.

The differences with witnesses at the level of density matrices notwithstanding, the diagram in fig. 5.2 can be translated to the space of covariance matrices by swapping $\rho \to \gamma$ and defining witnesses by the hyperplanes for $\mathrm{Tr}[\gamma W] = 1$. A key point in understanding the similarity between the statements and theorems is that the set of separable density and covariance matrices are both convex: a convex sum of separable states (CMs) is also separable.

5.5 Semidefinite programming

The definitions and results presented here were taken mostly from references [148, 149]. See also [123] for a discussion of SDPs pertaining to entanglement witnesses on covariance matrices which we cover in the next section.

[28] For biseparable CMs $\gamma^{(j)}_{\mathrm{Bisep}}$, let the CM given by the convex sum $\Gamma_{\mathrm{Bisep}} = \sum_j \Lambda_j \gamma^{(j)}_{\mathrm{Bisep}}$. We find that Γ_{Bisep} is biseparable as is satisfies the following equation.

$$0 \leq \Gamma_{\mathrm{Bisep}} - \sum_j \Lambda_j \sum_k^K \lambda_k^{(j)} \gamma_{\pi(k)} = \Gamma_{\mathrm{Bisep}} - \sum_k^K \lambda'_k \gamma_{\pi(k)},$$

with $\lambda'_k = \sum_j \Lambda_j \lambda_k^{(j)}$.

[29] The detailed derivations given in sections 5.6.1 and 5.6.2 are obtained with a different method than presented in the original paper [123].

We take a detour to introduce the main numerical method used for the work in this part: semidefinite programming. A semidefinite program is an optimization scheme in which a target function is maximised subject to constraints on semidefinite matrices.

In this section we consider variable matrices $X \in Sym(N, \mathbb{R})$, target matrices $C \in Sym(N, \mathbb{R})$ and constraint matrices $A_i \in Sym(N, \mathbb{R}), i \in [1, M]$ for some positive integer $M \in \mathbb{Z}^+$, along with constraint vector $\boldsymbol{b} \in \mathbb{R}^M$. However, the results may be translated to fields other than $\mathbb{R}$. For example, in the next section we use complex matrices over the real numbers, $\mathcal{M}_{\mathbb{C}}(N, \mathbb{R})$ and composite vector spaces such as $Sym(2N) \otimes Herm(2N)$.

To keep the same language as reference [148], we follow the convention where $(\cdot)^T$ returns the adjoint of its argument. Hence $(\cdot)^T = (\cdot)^\dagger$ when the underlying field is $\mathbb{C}$.

The inner product between matrices $X, Y \in Sym(N)$ is important here so we repeat eq. (5.19): $Y \bullet X := \langle Y, X \rangle = \mathrm{Tr}\left[Y^T X\right] \in \mathbb{R}$. Element-wise it gives

$$Y \bullet X = \sum_{i=1,j=1}^{n} X_{ij} Y_{ij}. \tag{5.92}$$

We also note that the operation $(\cdot)^T$ is to be read as the adjoint, and is to be read as the hermitian conjugation $(\cdot)^\dagger$ if the matrices have are over the field $F = \mathbb{C}$. The scalar product for vectors is the usual $(\langle \boldsymbol{y}, \boldsymbol{x} \rangle) = (\boldsymbol{y}^T \boldsymbol{x}) = \sum_j y_j x_j \in F$.

Definition 5.25 (Semidefinite program (primal))**.** A semidefinite program is an optimization problem of the form

$$\begin{aligned} \underset{X}{\text{maximise}} \quad & C \bullet X \\ \text{subject to} \quad & A_i \bullet X = b_i, \quad i = 1, 2, ..., m \\ & X \geq 0 \end{aligned}$$

where $X \in Sym(N)$ defines the space over which the search for a solution occurs. Requiring $X \geq 0$ constrains the search to positive semidefinite matrices. The specific problem is defined through $C \in Sym(N)$, which gives the *objective function* $C \bullet X = \langle C, X \rangle = \mathrm{Tr}\left[C^T X\right]$. The m constraints are defined by $\mathbf{b} \in \mathbb{R}^M$ and $A_i \in Sym(N)$.

One may abbreviate the constraints by defining the map $A : Sym(N) \to \mathbb{R}^M$ by $A(X) = (A_1 \bullet X, A_2 \bullet X, ..., A_m \bullet X)$, so that

$$A(X) = \mathbf{b}. \tag{5.93}$$

An SDP is said to be *feasible* if there is a matrix $\bar{X} \in PSD(N)$ with $A(\bar{X}) = \mathbf{b}$. Then $\bar{X}$ is called a solution or solution matrix. The result of the objective function is called the *value*

$$p := C \bullet \bar{X} \text{ for feasible } \bar{X} (\text{i.e } A(\bar{X}) = \boldsymbol{b}). \tag{5.94}$$

To the best solution we associate the adjective optimal

Definition 5.26 (Optimal solution)**.** For an SDP in standard form (Def. 5.25), the *optimal value* is obtained when there is a solution matrix $\tilde{X}$ such that

$$p^\star := C \bullet \tilde{X} \geq C \bullet X \text{ for all feasible } X \in Sym(N). \tag{5.95}$$

The matrix $\tilde{X}$ is then called the *optimal solution.*

Semidefinite programs have associated problems called their dual.

Definition 5.27 (Semidefinite dual program)**.** For an SDP in standard form

$$\begin{aligned} \underset{X}{\text{maximise}} \quad & C \bullet X \\ \text{subject to} \quad & A(X) = \boldsymbol{b} \\ & X \geq 0, \end{aligned}$$

the *dual program* is the SDP on the variable $\boldsymbol{y} \in \mathbb{R}^N$

$$\begin{aligned} \underset{\boldsymbol{y}}{\text{minimise}} \quad & \boldsymbol{b}^T \boldsymbol{y} \\ \text{subject to} \quad & \sum_{j=1}^{M} y_j A_j \geq C. \end{aligned}$$

We may write $\sum_{j=1}^{M} y_j A_j = A^T(\boldsymbol{y})$ where A^T is the adjoint of map A[30].

Duals to SDPs are themselves SDPs where the objective function and constraints swap roles. This relationship will become clearer when we present a method for going between the two problems.

One may notice two things. First, whereas the primal SDP has constraints in equality form whereas the dual has inequality constraints. In fact, had we started with inequality constraints on the primal then we would end up with equality constraints in the dual. Further the dual program is a minimisation scheme when the primal maximises the target function. In fact, the optimal values bound each other.

Theorem 5.9 (Weak duality)**.** *If a primal semidefinite program has optimal value $p^\star$ and its dual program is feasible with optimal value $d^\star$, then the optimal values bound each other through*

$$d^\star \geq p^\star. \tag{5.96}$$

This is known as weak duality[31]*.*

Whenever $d^\star = p^\star$ we speak of strong duality. These programs are those with solution matrices that are positive definite[32]. These matrices are known as the interior points of the positive semidefinite set[33]. Strong duality may therefore also be stated thus

Theorem 5.10 (Strong duality)**.** *If a semidefinite program is feasible with finite optimal value $p^\star$ and there is positive definite matrix $\bar{X}$ satisfying $A(\bar{X}) = \mathbf{b}$ then the dual program is feasible and has optimal value $d^\star = p^\star$.*

[30] From the definition of the adjoint of a map, we have that $\langle X, A^T(\boldsymbol{y})\rangle := \langle A(X), \boldsymbol{y}\rangle = [A(X)]^T\boldsymbol{y} = (A_1 \bullet X, ..., A_M \bullet X)^T\boldsymbol{y} = \sum_{j=1}^{M} A_j \bullet X \cdot y_j = \sum_{j=1}^{M} y_j A_j \bullet X = (\sum_{j=1}^{M} y_j A_j) \bullet X = \langle X, \sum_{j=1}^{M} y_j A_j\rangle$, Where we used the linearity in the inner product. Hence $A^T(\boldsymbol{y}) = \sum_{j=1}^{M} y_j A_j$ as required. [148, p.54]

[31] Technically, this statement uses the so-called limit-feasible values (values which are approached by forming sequences of semidefinite matrices). For more detail please refer textbooks in refs. [148, 149].

[32] This is known as Slater's theorem. [149, p.226]

[33] This is because the positive semidefinite cone is generated by matrices $\boldsymbol{x}\boldsymbol{x}^T$ and so for some non-zero $\boldsymbol{y}$ with $\boldsymbol{y}^T\boldsymbol{x}\boldsymbol{x}^T\boldsymbol{y}$ and positive definite matrix M, $\boldsymbol{y}^T(\boldsymbol{x}\boldsymbol{x}^T + M)\boldsymbol{y} = \boldsymbol{y}^T M\boldsymbol{y} > 0$. Similarly $\boldsymbol{y}(\boldsymbol{x}\boldsymbol{x}^T - M)\boldsymbol{y} < 0$ so that $\boldsymbol{x}\boldsymbol{x} - M \notin PSD(n)$ so that $\boldsymbol{x}\boldsymbol{x}^T$ is on the boundary. Following the same steps for a matrix with one zero eigenvalue and choosing $\boldsymbol{y}$ to be the zero eigenvector, we find that the boundary is given by the matrices with one or more zero eigenvalues. Hence the interior is made up from the positive definite matrices. I thank Jeff Snider in `math.stackexchange.com` for a post that included the argument included in this footnote.

Another useful theorem which provides a useful test to see if an SDP fulfills strong duality:

Theorem 5.11 (Slater's theorem)**.** *For an SDP with inequality constraints* $A(X) - \boldsymbol{b} \geq 0$*, if there exists a solution* $\bar{X}$ *such that*

$$A(\bar{X}) - \boldsymbol{b} > 0, \tag{5.97}$$

then strong duality holds. [149, p.226] Then $\bar{X}$ *is called strictly feasible.*

5.5.1 The method of Lagrange multipliers

Now we cover the method of Lagrange multipliers to obtain the primal from the dual problem. For this we follow reference [149] using the conventions set out above[34]. We derive the form of the primal problem starting from its dual.

Recall that the dual program may be written, in standard form, as in Def. 5.27

$$\begin{aligned} \underset{\boldsymbol{y}}{\text{minimise}} \quad & \boldsymbol{b}^T\boldsymbol{y} \\ \text{subject to} \quad & A^T(\boldsymbol{y}) \geq C, \end{aligned}$$

with $\boldsymbol{b}, \boldsymbol{y} \in \mathbb{R}^M$, $C \in Sym(N)$ and $A : \mathbb{R}^M \to Sym(N)$.

Lagrange's method starts with the central object which encodes the SDP, the bilinear *Lagrange function*

$$\mathcal{L}(\boldsymbol{y}, \lambda) = \langle \boldsymbol{b}, \boldsymbol{y} \rangle - \langle (A^T(\boldsymbol{y}) - C), \lambda \rangle = \boldsymbol{b}^T\boldsymbol{y} - \mathrm{Tr}\big[(A^T(\boldsymbol{y}) - C)^T\lambda\big], \tag{5.98}$$

with $\lambda \in PSD(N)$. We will see that λ becomes the primal variable, X. To describe the dual SDP, we minimise over the variable $\boldsymbol{y}$ and define the *dual function*

$$g(\lambda) = \inf_{\boldsymbol{y} \in \mathbb{R}^M} \mathcal{L}(\boldsymbol{y}, \lambda) = \inf_{\boldsymbol{y} \in \mathbb{R}^M} \left(\boldsymbol{b}^T\boldsymbol{y} - \mathrm{Tr}\big[(A^T(\boldsymbol{y}) - C)^T\lambda\big] \right). \tag{5.99}$$

Let us now gather the terms that depend on $\boldsymbol{y}$. We have

$$\begin{aligned} g(\lambda) &= \inf_{\boldsymbol{y}} \left(\boldsymbol{b}^T\boldsymbol{y} - \langle A^T(\boldsymbol{y}) - C, \lambda \rangle \right) \\ &= \inf_{\boldsymbol{y}} \left(\boldsymbol{b}^T\boldsymbol{y} - \langle A^T(\boldsymbol{y}), \lambda \rangle + \langle C, \lambda \rangle \right) \\ &= \langle C, \lambda \rangle + \inf_{\boldsymbol{y}} \left(\boldsymbol{b}^T\boldsymbol{y} - \langle A^T(\boldsymbol{y}), \lambda \rangle \right). \end{aligned} \tag{5.100}$$

Recall that $A^T(\boldsymbol{y}) = \sum_{j=1}^M y_j A_j$ where $A_j, j \in [1, M]$ encode the M constraints of the primal problem (see Def. 5.27). Hence,

$$\langle A^T(\boldsymbol{y}), \lambda \rangle = \langle \sum_{j=1}^M y_j A_j, \lambda \rangle = \sum_{j=1}^M y_j \langle A_j, \lambda \rangle = \sum_{j=1}^M y_j A_j \bullet \lambda = (A_1 \bullet \lambda, ..., A_M \bullet \lambda)^T\boldsymbol{y} = \langle A(\lambda), \boldsymbol{y} \rangle, \tag{5.101}$$

[34] Most of the treatment in reference [149] is on optimisation of objective functions $f : \mathbb{R}^N \to \mathbb{R}$. The results presented in this thesis were translated to the formalism used in reference [148] which deals with more abstract elements of convex sets.

using the definition of the map A as done after Def. 5.25[35]. Inserting this into eq. (5.100) allows the dual function to be written as

$$g(\lambda) = \langle C, \lambda\rangle + \inf_{\boldsymbol{y}} \left(\boldsymbol{b}^T\boldsymbol{y} - [A(\lambda)]^T\boldsymbol{y}\right) \tag{5.102}$$

$$= \langle C, \lambda\rangle + \inf_{\boldsymbol{y}} \left((\boldsymbol{b} - [A(\lambda)])^T\boldsymbol{y}\right) \tag{5.103}$$

$$= \langle C, \lambda\rangle + \inf_{\boldsymbol{y}} \langle(\boldsymbol{b} - [A(\lambda)]), \boldsymbol{y}\rangle. \tag{5.104}$$

Now, the infimum of linear functions is $-\infty$ unless the coefficients are all null. Since the inner product is linear in both arguments we must have $A(\lambda) - \boldsymbol{b} = 0$ for $g(\lambda)$ to be bounded. Note how the roles of C and $\boldsymbol{b}$ are swapped - $\boldsymbol{b}$ now becomes part of a constraint and C has become part of the target function with respect to the Lagrange variable λ.

We can now identify the elements of the primal SDP: $\langle C, \lambda\rangle$ is the objective function and $A(\lambda) - \boldsymbol{b}, \lambda \geq 0$ gives the constraints. This means that we can make the replacement $\lambda = X$. To extract the bound on the values of the primal SDP we can simply find the supremum of the dual function

$$\sup_{\lambda} g(\lambda) = \sup_{\lambda}\inf_{\boldsymbol{y}} \mathcal{L}(\boldsymbol{y}, \lambda) = d^\star, \tag{5.105}$$

where the last equality uses the definition of the optimal value of the dual problem.

Interestingly, this already gives Weak duality (Thm. 5.9). Start from the Lagrangian with the $\boldsymbol{y}$ terms gathered, $\mathcal{L}(\boldsymbol{y}, \lambda) = \langle C, \lambda\rangle + \inf_{\boldsymbol{y}}\langle(\boldsymbol{b} - [A(\lambda)]), \boldsymbol{y}\rangle$. The primal problem finds the maximum with respect to feasible λ, $\sup_\lambda \mathcal{L}(\boldsymbol{y}, \lambda)$. The bound of the dual is the optimal primal value so

$$p^\star = \inf_{\boldsymbol{y}}\sup_{\lambda} \mathcal{L}(\boldsymbol{y}, \lambda), \tag{5.106}$$

wherefrom weak Lagrangian duality, $d^\star \geq p^\star$, follows[36].

Let us summarise.

Theorem 5.12 (Method of Lagrange multipliers)**.** *For a given SDP in dual standard form, Def. 5.27, one may find its corresponding primal program by the following recipe:*

i. Identify the dual objective function $\boldsymbol{b}^T\boldsymbol{y}$ and constraints in the form $A^T(y) - C$;

ii. Set the space and other structure of the primal variable, X, by comparing to the spaces of C and $A^T(\boldsymbol{y})$;

iii. Find the Lagrangian $\mathcal{L}(\boldsymbol{y}, X) = \boldsymbol{b}^T\boldsymbol{y} - \mathrm{Tr}\left[(A^T(\boldsymbol{y}) - C)^T X\right]$ (eq. (5.98));

iv. Rearrange the Lagrangian by gathering the terms including $\boldsymbol{y}$;

v. Obtain the constraints by setting the coefficient $A^T(\boldsymbol{y}) - \boldsymbol{b}$ to zero;

vi. The other term, $\langle C, X\rangle$, is the primal objective;

vii. Combine the elements above to write the primal SDP in standard form.

We now return to entanglement using the machinery set out in this section.

[35] Note that the second equality, $\langle\sum_{j=1}^{M} y_j A_j, \lambda\rangle = \sum_{j=1}^{M} y_j\langle A_j, \lambda\rangle$ must be done carefully whenever $y_j \notin \mathbb{R}$. For example, in section 5.6.1 we have $\boldsymbol{y} = (\gamma_A \oplus \gamma_B, x_e)$ so $y_1 \in Sym \oplus Sym$. Hence to pull the element out of the inner product, we decompose y_1 in a suitable basis and extract the coefficients.

[36] For this one uses the general result that

$$\inf_y \sup_x \mathcal{L}(y, x) \geq \sup_x \inf_y \mathcal{L}(y, x). \tag{5.107}$$

The proof is left for the reader.

5.6 Finding the witness for a CM as a semidefinite program

When interested in a state's entanglement, one may ask which measurements provide the strongest evidence. Here we cover results from ref. [123] on so-called optimal entanglement witnesses which act on the level of covariance matrices. They are optimal in the sense that they satisfy Thm. 5.8 (Witnesses on covariance matrices) and, for a given CM γ, the witness W gives the lowest value of $\mathrm{Tr}[\gamma W]$. The detailed derivations presented in the coming sections are done using a different method than in reported in the original reference.

This section provides the background for chapter 6, where we present new work by relaxing the requirement on full knowledge of the CM but still establish the presence of multipartite Gaussian entanglement via optimal witnesses.

5.6.1 Bipartite entanglement witnesses

Although we are interested in the multipartite scenario, it is didactic to start with the bipartite case. Our primary goal is to get a scheme that, for a given CM, finds the witness that gives the strongest evidence of bipartite entanglement with respect to Thm. 5.8. This is our primal SDP. However, phrasing the dual is easier so this will be our starting point[37].

Let the CM γ be composed of N modes and separate it into N_A and N_B modes which we call A and B respectively. For simplicity, we may reorganise the CM so that modes A appear in the top-left and modes B in the bottom-right. Covariances between modes in A and B are contained in the off-diagonal blocks. We consider separability across the bipartition $A|B$.

Recall the sufficient criterion for separability, given in Thm. 5.6. It states that if there are local CMs γ_A and γ_B on modes A and B, such that $\gamma - \gamma_A \oplus \gamma_B \geq 0$, then γ is separable across the bipartition $A|B$. Furthermore, since γ_A and γ_B are CMs, they must satisfy the uncertainty relation, so $\gamma_A \oplus \gamma_B + i\Omega_N \geq 0$.

The requirements on the CMs and bipartite separability allows us to devise a test to check whether a given CM is entangled or not.

SDP 5.1 (Dual program for optimal bipartite entanglement witness)**.** For a given CM γ on $N = N_A + N_B$ modes, if the SDP

$$\begin{aligned} \underset{\gamma_A,\gamma_B,x_e}{\text{minimise}} \quad & -x_e \\ \text{subject to} \quad & \gamma - \gamma_A \oplus \gamma_B \geq 0 \\ & \gamma_A \oplus \gamma_B + (1+x_e)i\Omega \geq 0. \end{aligned}$$

has an optimal solution where $x_e \geq 0$ then γ is separable as $\gamma_A \oplus \gamma_B$ would satisfy a stricter inequality than the Robertson uncertainty relation (Thm. 5.4). Otherwise, if $x_e < 0$, then γ is entangled across the bipartition $A|B$.

We'll follow the recipe in Thm. 5.12 using each step as a heading.

I. Identify the dual objective function $\boldsymbol{b}^T\boldsymbol{y}$ and constraints in the form $A^T(y) - C$;

[37] Note that in ref. [123], SDP 5.1 is referred to as the primal problem. However, to keep the notation presented in section 5.5, we deviate from this. Recall that the dual of an SDP is an SDP itself and you regain the primal problem by taking the dual of the dual problem so this redefinition poses no issue.

Let us write SDP 5.1 in standard form (Def. 5.27) so that we may more easily phrase the primal program. To this end, let us define the optimization variable

$$\boldsymbol{y} = (\gamma_A \oplus \gamma_B, x_e). \tag{5.108}$$

Note that we may have included the local CMs, γ_A, γ_B, as separate entries in $\boldsymbol{y}$ but it makes the derivation clearer to keep them joined. Furthermore, only terms involving $\gamma_A \oplus \gamma_B$ appear in the SDP so this definition is without loss of generality. The objective function is returned by identifying

$$\boldsymbol{b} = (\mathbb{O}_{2N_A} \oplus \mathbb{O}_{2N_B}, -1), \tag{5.109}$$

with $\mathbb{O}_{2N_j}$ the $2N_j \times 2N_j$ zero matrix for $j = A, B$. We could have written $\mathbb{O}_{2N}$ but left the block-diagonal notation for clarity in what is to come.

Next, we may write the constraints as $A^T(\boldsymbol{y}) - C = \begin{pmatrix} -\gamma_A \oplus \gamma_B \\ \gamma_A \oplus \gamma_B + x_e i\Omega \end{pmatrix}^T + \begin{pmatrix} \gamma \\ i\Omega \end{pmatrix}^T \geq 0$, allowing us to identify[38]

$$\begin{aligned} A^T(\boldsymbol{y}) &= \left(-(\mathbb{1}_{2N_A} \oplus \mathbb{1}_{2N_B}, 0)^T \boldsymbol{y}, (\mathbb{1}_{2N_A} \oplus \mathbb{1}_{2N_B}, i\Omega)^T \boldsymbol{y}\right); \quad \text{and} \\ C &= (-\gamma, -i\Omega)\,. \end{aligned} \tag{5.110}$$

II. Set the space for the primal variable, X, by comparing to the spaces of C and $A^T(\boldsymbol{y})$;

We can now add more structure on the primal variable X. Consider $C = (\gamma, i\Omega) \in Sym(2(N_A + N_B)) \otimes Herm(2(N_A + N_B))$. We can then let[39]

$$X = (X_1, X_2) \in Sym(2(N_A + N_B)) \otimes Herm(2(N_A + N_B)). \tag{5.111}$$

In reference [123], the identification goes as $X \in \mathbb{C}^{4(N_A+N_B)\times 4(N_A+N_B)}$ corresponding to partitioning the system into the first N_A modes followed by N_B and repeated once. It is further noted that the constraints involve block-diagonal terms of each component of X. We can see this here by looking at $A^T(\boldsymbol{y})$. The real and symmetric part of X must have block-diagonal terms equal to the real part of the Hermitian block due to both $\mathbb{1} \oplus \mathbb{1}$ terms. This becomes apparent when by collecting terms involving $\gamma_A \oplus \gamma_B$.

III. Find the Lagrangian $\mathcal{L}(\boldsymbol{y}, X) = \boldsymbol{b}^T \boldsymbol{y} - \mathrm{Tr}\left[(A^T(\boldsymbol{y}) - C)X\right]$;

The Lagrangian from eq. (5.98) is here

$$\begin{aligned} \mathcal{L}(\boldsymbol{y}, X) &= -x_e - \mathrm{Tr}[(((-\gamma_A \oplus \gamma_B), (\gamma_A \oplus \gamma_B + x_e i\Omega)) - (-\gamma, -i\Omega))\, X] \\ &= \mathrm{Tr}\left[(-\gamma, -i\Omega)^T X)\right] - x_e - \mathrm{Tr}\left[(-\gamma_A \oplus \gamma_B, \gamma_A \oplus \gamma_B + x_e i\Omega)^T X\right]. \end{aligned} \tag{5.112}$$

IV. Rearrange the Lagrangian by gathering the terms including $\boldsymbol{y}$;

We gather the terms element-wise: $\gamma_A \oplus \gamma_B$ and x_e separately. Note that

$$(-\gamma_A \oplus \gamma_B, \gamma_A \oplus \gamma_B + x_e i\Omega) = (-\gamma_A \oplus \gamma_B, \gamma_A \oplus \gamma_B) + (\mathbb{O}_{2N_A} \oplus \mathbb{O}_{2N_N}, x_e i\Omega), \tag{5.113}$$

[38] Note that $A^T(\alpha y + \beta z) = A^T(\alpha y) + A^T(\beta z)$ for $\alpha, \beta \in \mathbb{C}$ so A^T is linear as required.

[39] Since $i\Omega = \left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right)$, is not symmetric, we must extend the space to Hermitian matrices. This carries on to definition of the target variable in the dual program SDP 5.2.

so the Lagrangian may be written as

$$\mathcal{L}(\boldsymbol{y}, X) = \mathrm{Tr}\big[(-\gamma, -i\Omega)^T X\big] - x_e - \mathrm{Tr}[-\gamma_A \oplus \gamma_B X_1 + \gamma_A \oplus \gamma_B X_2] - \mathrm{Tr}\big[x_e i\Omega^T X_2\big], \tag{5.114}$$

where we used that $X = (X_1, X_2)$ and that CMs are symmetric.

Thus, the Lagrangian becomes

$$\begin{aligned}\mathcal{L}(\boldsymbol{y}, X) &= -\mathrm{Tr}\big[(\gamma, i\Omega)^T X\big] - x_e - \mathrm{Tr}[-\gamma_A \oplus \gamma_B X_1 + \gamma_A \oplus \gamma_B X_2] - \mathrm{Tr}\big[x_e i\Omega^T X_2\big], \\ &= -\mathrm{Tr}\big[(\gamma, i\Omega)^T X\big] - x_e(1 + \mathrm{Tr}\big[i\Omega^T X_2\big]), - \mathrm{Tr}[\gamma_A \oplus \gamma_B(-X_1 + X_2)]\end{aligned} \tag{5.115}$$

V. Obtain the constraints by setting the coefficient of $\boldsymbol{y}$, $A^T(\boldsymbol{y}) - \boldsymbol{b}$, *to zero;*

From setting the coefficient of x_e to zero, we have that

$$\mathrm{Tr}\big[i\Omega^T X_2\big] = -1. \tag{5.116}$$

Meanwhile, for the $\gamma_A \oplus \gamma_B$ term we have to be more careful. In particular, we need to be able to extract the dual variable elements from inside the trace. To this end we define the vectors whose entries are real symmetric matrices with repeated blocks, $\mathcal{B}(2N)$, as

$$\mathcal{B}(N) = \mathrm{span}(\{(F_{jk}, F_{jk}) | j, k \in [1, N]\}), \tag{5.117}$$

where the basis elements F_{jk} have all entries null except for

$$(F_{jk})_{jk} = (F_{jk})_{kj} = 1 \tag{5.118}$$

Then we can decompose the real part of the terms involving $\gamma_A \oplus \gamma_B$ as

$$(\gamma_A \oplus \gamma_B, \gamma_A \oplus \gamma_B)_{jk} = \sum_{j,k=1}^{N_A} a_{jk}(F_{jk}, F_{jk}) + \sum_{j,k=N_A+1}^{N_A+N_B} b_{jk}(F_{jk}, F_{jk}), \tag{5.119}$$

with a and b the coefficients of γ_A and γ_B in the basis of $\mathcal{B}(2N)$ respectively. Define

$$g_{jk} = \begin{cases} a_{jk} \text{ if } j, k \in [1, N_A] \\ b_{jk} \text{ if } j, k \in [1 + N_A, N] \end{cases} \tag{5.120}$$

with $N = N_A + N_B$.

This basis allows us to write the middle term in eq. (5.115) as

$$-\mathrm{Tr}\big[(\gamma_A \oplus \gamma_B)_{jk}(X_1 - X_2)\big] = g_{jk}\,\mathrm{Tr}\big[F_{jk}(X_1 - X_2)\big]. \tag{5.121}$$

Since F_{jk} are real and $\mathrm{Tr}\big[X^T Y\big] = \langle X, Y\rangle$, we have that

$$-\mathrm{Tr}\big[(\gamma_A \oplus \gamma_B)_{jk}(X_1 - X_2)\big] = g_{jk}\langle F_{jk}, X_1\rangle - g_{jk}\langle F_{jk}, X_2\rangle. \tag{5.122}$$

Now each inner product picks the coefficient of X_1 and X_2 corresponding to each basis element so we end up with

$$\begin{aligned}-\mathrm{Tr}\big[(\gamma_A \oplus \gamma_B)_{jk}(X_1 - X_2)\big] &= ([X_1^{\mathrm{re}}]_{jk} - [X_2^{\mathrm{re}}]_{jk})a_{jk} + b_{jk}([X_1^{\mathrm{re}}]_{jk} - [X_2^{\mathrm{re}}]_{jk}) \\ &= g_{jk}([X_1^{\mathrm{re,bd}}]_{jk} - [X_2^{\mathrm{re,bd}}]_{jk}),\end{aligned} \tag{5.123}$$

where $[X_1^{\text{re,bd}}]_{kj}$ denotes that this is the coefficient in a real (re), symmetric and block-diagonal (bd) space. Since the component of X which appears in the objective function is real and symmetric, this does not pose a problem.

Now we set to zero the coefficient to each g_{jk}, this means that

$$X_1^{\text{re,bd}} = X_2^{\text{re,bd}}. \tag{5.124}$$

The two constraints are thus given in eqs. (5.116) and (5.124) as well as requiring each element $X_1, X_2 \geq 0$.

VI. The other term,$\langle C, X\rangle$, is the primal objective;

From eq. (5.116) ($\text{Tr}\left[i\Omega^T X_2\right] = -1$), we find that the objective function becomes

$$\langle C, X\rangle = -\text{Tr}\left[\gamma X_1 + i\Omega^T X_2\right] = -(\text{Tr}[\gamma X_1] - 1), \tag{5.125}$$

where we used that $X = (X_1, X_2)$.

We have thus all elements for writing the primal problem.

VII. Combine the elements above to write the primal SDP in standard form (Def. 5.25).

Before we write the primal SDP in standard form, recall that the objective function is maximised with respect to X. Since our target function is $-(\text{Tr}[\gamma X_1] - 1)$ it is equivalent to instead minimise its negative.

We end up therefore with the semidefinite program that finds the optimal witness for a given CM.

SDP 5.2 (Primal program for optimal bipartite entanglement witness)**.** For a given CM γ, the SDP

$$\begin{aligned} \underset{X}{\text{minimise}} \quad & \text{Tr}[\gamma X_1] - 1 \\ \text{subject to} \quad & X_1^{\text{bd,re}} = X_2^{\text{bd,re}} \\ & X_1, X_2 \geq 0 \\ & \text{Tr}[i\Omega X_2] = -1, \end{aligned}$$

has a feasible solution with $\text{Tr}\left[\gamma X_1^{\text{re}}\right] - 1 \geq 0$ whenever γ is separable. If γ is entangled, the program returns a negative value.

The superscripts $(\cdot)^{\text{bd,re}}$ and $(\cdot)^{\text{re}}$ denote the real part of the block-diagonal entries and the whole matrix respectively.

To prove that X_1^{re} is indeed a witness, we need to show that it statisfies Thm. 5.8:

$$\text{Tr}[\gamma W] < 1 \quad \text{for at least one entangled } \gamma, \tag{5.126}$$

$$\text{Tr}\left[\gamma_{\text{Sep}} W\right] \geq 1 \quad \text{for all separable } \gamma_{\text{Sep}}. \tag{5.127}$$

By weak duality (Thm. 5.9), the optimal values of the primal and duals SDPs are related by

$$p^\star := -(\text{Tr}\left[\gamma W^\star\right] - 1) \leq -x_e^\star =: d^\star, \tag{5.128}$$

for $W^\star = X_1$ and $x_e^\star$ the optimal solutions for the primal and dual respectively. Hence,

$$\text{Tr}\left[\gamma W^\star\right] \geq 1 + x_e. \tag{5.129}$$

One may show that equality in eq. (5.129) holds due to strong duality. One may do so by giving a solution to the either SDP 5.1 or SDP 5.2 that fulfills the constraints strictly and use Slater's theorem (Thm. 5.11). In reference [123] the authors give an example for the primal so we present here one for the dual. One solution to SDP 5.1 that fulfills Slater's criterion is $\boldsymbol{y} = (\gamma^A \oplus \gamma^B - \mathbb{1}, \nu_{\max} + 1)\}$, where γ^A and γ^B are the reductions of γ into modes A and B respectively and $\nu_{\max}$ is the largest symplectic eigenvalue of $\gamma^A \oplus \gamma^B$[40].

This means that we may translate the analysis for x_e in the dual. There, we noted that $x_e \geq 0$ implied separability of γ, so the first witness inequality (eq. (5.126)) is fulfilled. Meanwhile, if γ is entangled, then $x_e < 0$ and the second requirement is fulfilled. Hence, the solution to SDP 5.2 is a witness of bipartite entanglement.

5.6.2 GME witnesses

We move on to witnesses of genuine multipartite entanglement on CMs. We will end up with the SDP

SDP 5.3 (Primal program for optimal GME witness)**.** For a given CM γ of an N-mode state, the SDP

$$\begin{aligned} \underset{X}{\text{minimise}} \quad & \mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \\ \text{subject to} \quad & X_1^{\mathrm{re,bd},\pi(k)} = X_{k+1}^{\mathrm{re,bd},\pi(k)} \quad \text{for all} \quad k = 1, \ldots, K, \\ & \mathrm{Tr}[i\Omega_N X_{k+1}] + X_{K+2} - X_{K+3} + X_{K+3+k} = 0, \quad \text{for all} \quad k = 1, \ldots, K \\ & X_{K+2} - X_{K+3} = 1. \end{aligned}$$

has a feasible solution with $\mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \geq 0$ whenever γ is biseparable. If γ is genuinely multipartite entangled, the program produces a negative value. We used $\pi(k)$ to denote the k^{th} bi-partition (out of $K = 2^{N-1} - 1$ possible). $X^{\mathrm{re,bd},\pi(k)}$ is the real part of X that is block-diagonal with respect to partition $\pi(k)$ - elements across the partition are set to zero.

Let us start with the dual problem once more. We want a test that detects whenever an N-mode CM γ may be written as a sum of separable CMs across all possible bipartitions, $\pi(k)$: $\sum_k \gamma_{\pi(k)}$. The CMs $\gamma_{\pi(k)}$ should fulfill the HUP when taken as a sum. This gives us the following SDP

[40] Let $\boldsymbol{y} = (\gamma^A \oplus \gamma^B - \mathbb{1}, \epsilon)$. Then the first constraint reads

$$\gamma - y_1 = \begin{pmatrix} \mathbb{1} & \gamma^{AB} \\ \gamma^{AB} & \mathbb{1} \end{pmatrix} > 0,$$

with γ^{AB} the covariance between modes across the partition $A|B$. We also have that

$$y_2 + i\Omega = \gamma^A \oplus \gamma^B - \mathbb{1} + (1+\epsilon) i\Omega > \gamma^A \oplus \gamma^B + (1+\epsilon) i\Omega > 0.$$

To obtain the last inequality, write $-\nu_{\max} = \min\{eig(i\Omega\gamma^A \oplus \gamma^B)\}$ remembering that the symplectic eigenvalues come in pairs of opposite sign as the eigenvalues of the product of the matrix with $i\Omega$. One has $i\Omega\gamma^A \oplus \gamma^B + (1+\epsilon) \geq 0$. Choosing $\epsilon = \nu_{\max}$ gives $\epsilon > \nu_{\max} - 1$. This completes the proof that $A^T(\boldsymbol{y}) - \boldsymbol{C} > 0$ and hence that $\boldsymbol{y} = (\gamma^A \oplus \gamma^B, \nu_{\max})$ satisfies Slater's condition Thm. 5.11.

SDP 5.4 (Dual program for optimal GME witness)**.** For a given CM γ, if the SDP

$$\begin{aligned}
\underset{\{\gamma_{\pi(k)},\lambda_k\},x_e}{\text{minimise}} \quad & -x_e \\
\text{subject to} \quad & \gamma - \sum_k \gamma_{\pi(k)} \geq 0 && \text{(C1)} \\
& \gamma_{\pi(k)} + \lambda_k i\Omega \geq 0 \text{ for all } k \in [1,K] && \text{(C2)} \\
& \sum_{k=1}^{K} \lambda_k = 1 + x_e && \text{(C3)} \\
& \lambda_k \geq 0 \text{ for all } k && \text{(C4)}
\end{aligned}$$

has a solution where $x_e \geq 0$ then γ is biseparable as it would satisfy Robertson uncertainty relation (Thm. 5.4). Otherwise, if $x_e < 0$, then γ is genuinely multipartite entangled. We have labelled the constraints eqs. (C1) to (C4) for convenience.

We may see that this does indeed test for biseparability by considering the constraints. From the second and third constraints we get that $\sum_{k=1}^{K} \gamma_{\pi(k)} \geq (1+x_e) i\Omega$ so that the first constraint becomes

$$\gamma - (1+x_e) i\Omega \geq \gamma - \sum_{k=1}^{K} \gamma_{\pi(k)} \geq 0. \tag{5.130}$$

Multiplying by $i\Omega$ gives

$$|i\Omega\gamma| \geq (1+x_e)\mathbb{1}, \tag{5.131}$$

where we used that $\Omega^2 = -\mathbb{1}$. Whenever $x_e \geq 0$, γ has all symplectic eigenvalues greater than one and is therefore a valid CM which satisfies the biseparability criterion (the first constraint). If $x_e < 0$, no quantum CMs $\gamma_{\pi(k)}$ could be found such that the first constraint of SDP 5.4 is fulfilled.

To find the primal SDP, we use the method of Lagrange multipliers from section 5.5.1 once again.

I. Identify the dual objective function $\boldsymbol{b}^T\boldsymbol{y}$ and constraints in the form $A^T(y) - C$;

We begin by identifying the elements of the dual in standard from Def. 5.25. For this, we write the constraint $\sum_k \lambda_k = (1+x_e)$ in inequality form to get

$$\begin{aligned}
\sum_k \lambda_k - (1+x_e) \geq 0; \\
-(\sum_k \lambda_k) + 1 + x_e \geq 0.
\end{aligned} \tag{5.132}$$

The dual SDP has the parameters:

$$\begin{aligned}
\boldsymbol{y} &= (\gamma_{\pi(1)}, ..., \gamma_{\pi(K)}, \lambda_1, ..., \lambda_K, x_e) \\
\boldsymbol{b} &= (\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 0, ..., 0, -1) \\
C &= -(\underbrace{\gamma}_{(C1)}, \underbrace{\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}}_{(C2)}, \underbrace{-1, 1}_{(C3)}, \underbrace{0, ..., 0}_{(C4)}),
\end{aligned} \tag{5.133}$$

where we marked the constraints to which elements of C correspond. The negative sign in front of C is due to our convention of writing the constraints as $A^T(\boldsymbol{y}) - C$. The $M = 1 + K + 1 + 1 + K$ constraints may be written as

$$
\begin{aligned}
A^T(\boldsymbol{y}) = (&\underbrace{-\sum_{k=1}^{K}\gamma_{\pi(k)}}_{(C1)}, \underbrace{\gamma_{\pi(1)} + i\Omega_{2N}\lambda_1, ..., \gamma_{\pi(K)} + i\Omega_{2N}\lambda_K}_{(C2)}, \underbrace{-x_e + \sum_{k=1}^{K}\lambda_k, x_e - \sum_{k=1}^{K}\lambda_k}_{(C3)}, \underbrace{\lambda_1, ..., \lambda_K}_{(C4)}) \\
= (&\{(-\mathbb{1}_{2N}, ..., -\mathbb{1}_{2N}, 0, ...0, 0)\cdot\boldsymbol{y},\}\ (C1) \\
&\left.\begin{array}{l}(\mathbb{1}_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, i\Omega_{2N}, 0, ..., 0, 0)\cdot\boldsymbol{y}, \\ \qquad\qquad\vdots \\ (\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, \mathbb{1}_{2N}, 0, ..., 0, i\Omega_{2N}, 0)\cdot\boldsymbol{y},\end{array}\right\}(C2) \\
&\left.\begin{array}{l}(\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 1, ..., 1, -1)\cdot\boldsymbol{y}, \\ (\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, -1, ..., -1, 1)\cdot\boldsymbol{y},\end{array}\right\}(C3) \\
&\left.\begin{array}{l}(\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 1, 0, ..., 0, 0)\cdot\boldsymbol{y}, \\ \qquad\qquad\vdots \\ (\mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 0, ..., 0, 1, 0)\cdot\boldsymbol{y}\end{array}\right\}(C4) \\
&).
\end{aligned}
\tag{5.134}
$$

II. Set the space for the primal variable, X, by comparing to the spaces of C and $A^T(\boldsymbol{y})$;

$\dim X = \dim A^T(\boldsymbol{y}) = 2N \times 2N.K \times 1 \times 1 \times 1.K$.
To find the space of the primal variable, consider the entries of $A(\boldsymbol{y})$ to find

$$
X \in \underbrace{Sym(2N, \mathbb{R})}_{(C1)} \otimes \underbrace{\bigotimes_{k=1}^{K}(Herm(2N, \mathbb{R}) \cap \mathcal{B}(2N, \pi(k)))}_{(C2)} \otimes \underbrace{\mathbb{R}\otimes\mathbb{R}}_{(C3)} \otimes \underbrace{\bigotimes_{k=1}^{K}\mathbb{R}}_{(C4)}, \tag{5.135}
$$

with $\mathcal{B}(2N, \pi(k))$ the $2N \times 2N$ matrices which are block-diagonal with respect to bi-partition $\pi(k)$. We use the first entry, $X_1 \in Sym(2N, \mathbb{R})$ as the witnesses, so we must choose a basis that constrains the relevant values. As for the bipartite case, write the basis of symmetric matrices as $\{F_{ij}\} \in Sym(2N, \mathbb{R})$ (see eq. (5.118)). Further, let the basis of real block-diagonal matrices across bipartition $\pi(k)$ be given by $\{x_{\pi(k),ij}\} \in \mathcal{B}(2N, \pi(k))$ so $\text{span}(\{F_{ij}x_{\pi(k),ij}\}) = Sym(2N) \cap \mathcal{B}(2N, \pi(k))$, where the entries in F_{ij} and $x_{\pi(k)}$ are zero except for

$$
\begin{aligned}
(F_{ij})_{ij} = (F_{ij})_{kj} = 1; \text{ and} \\
(x_{\pi(k),ij})_{ij} = (x_{\pi(k),ij})_{kj} = 1,
\end{aligned}
\tag{5.136}
$$

and $(x_{\pi(k),ij})_{ij} = 0$ whenever i, j correspond to element mixing across the partition $\pi(k)$. We use $\text{span}(\{F_{ij}\}) = Sym(2N, \mathbb{R})$ (rather than $Herm$) to form a vector space of the real symmetric matrices over the real numbers since the element we extract as the witness, $X_1^{\text{re},\pi(k)}$, is real and symmetric, much like in the bipartite case.

III. Find the Lagrangian $\mathcal{L}(\boldsymbol{y}, X) = \boldsymbol{b}^T\boldsymbol{y} - \text{Tr}\big[(A^T(\boldsymbol{y}) - C)X\big]$;

Let us return to the Lagrangian, which we can write as

$$\begin{aligned}\mathcal{L}(\boldsymbol{y}, X) &= -x_e - \mathrm{Tr}\big[A^T(\boldsymbol{y})X\big] + \mathrm{Tr}\big[C^T X\big] \\ &= \mathrm{Tr}\big[C^T X\big] - x_e - \mathrm{Tr}\big[A^T(\boldsymbol{y})X\big] \\ &= \mathrm{Tr}[\gamma X_1 - X_{K+2} + X_{K+3}] - x_e - \mathrm{Tr}\big[A^T(\boldsymbol{y})X\big],\end{aligned} \tag{5.137}$$

obtained using the parameters in eq. (5.133) and by writing
$X = (\underbrace{X_1}_{(C1)}, \underbrace{X_2, ..., X_{K+1}}_{(C2)}, \underbrace{X_{K+2}, X_{K+3}}_{(C3)}, \underbrace{X_{K+4}, ..., X_{2K+3}}_{(C4)})$.

IV. Rearrange the Lagrangian by gathering the terms including $\boldsymbol{y}$;

Now, we want to write $A(\boldsymbol{y})$ in terms of the dual variables, $\{\gamma_{\pi(k)}\}, \{\lambda_k\}, x_e$.

$$\begin{aligned}\mathrm{Tr}\big[A^T(\boldsymbol{y})X\big] &= \mathrm{Tr}\left[\left(-\sum_{k=1}^{K}\gamma_{\pi(k)}, \gamma_{\pi(1)} + i\Omega_{2N}\lambda_1, ..., \gamma_{\pi(K)} + i\Omega_{2N}\lambda_K, -x_e + \sum_{k=1}^{K}\lambda_k, x_e - \sum_{k=1}^{K}\lambda_k, \lambda_1, ..., \lambda_K\right)^T X\right] \\ &= \mathrm{Tr}\Big[\gamma_{\pi(1)}^T(-\mathbb{1}_{2N}, \mathbb{1}_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 0, 0, 0, ..., 0)X\Big] + \\ &\qquad\vdots \\ &+ \mathrm{Tr}\Big[\gamma_{\pi(K)}^T(-\mathbb{1}_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, \mathbb{1}_{2N}, 0, 0, 0, ..., 0)X\Big] \\ &+ \lambda_1 \mathrm{Tr}[(\mathbb{O}_{2N}, i\Omega_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 1, -1, 1, 0, ..., 0)X] + \\ &\qquad\vdots \\ &+ \lambda_K \mathrm{Tr}[(\mathbb{O}_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, i\Omega_{2N}, 1, -1, 0, ...0, 1)X] \\ &+ x_e \mathrm{Tr}[(\mathbb{O}_{2N}, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, 1, -1, 0, ...0, 0)X],\end{aligned} \tag{5.138}$$

where we treat the multiplication of $\gamma_{\pi(k)}, k \in [1, K]$ with the vector in a scalar fashion with the relevant elements only for convenience.

V. Obtain the constraints by setting the coefficient of $\boldsymbol{y}$, $A^T(\boldsymbol{y}) - \boldsymbol{b}$, to zero;

Setting the coefficients of the dual variables to zero to avoid the dual function blowing up is straight forward for the scalar variables $x_e, \lambda_k, k \in [1, K]$. They produce to the following constraints

$$X_{K+2} - X_{K+3} = 1 \tag{Cx_e}$$

$$\mathrm{Tr}[i\Omega X_k] + X_{K+2} - X_{K+3} + X_{K+3+k} = 0 \text{ for } k \in [1, K]. \tag{Cλ_k}$$

For getting (Cx_e) we used the term $-x_e$ in the Lagrangian.

The terms involving CMs $\gamma_{\pi(k)}$ need to be treated in the same way as previously. We decompose them in the basis ($\{F_{ij}x_{\pi(k),ij}\}$) of $Sym(2N) \cap \mathcal{B}(2N, \pi(k))$. Performing a similar analysis to the bipartite case leaves us with terms

$$g_{ij}\,\mathrm{Tr}\big[F_{ij}x_{\pi(k),ij}(-X_1 + X_{1+k})\big] \tag{5.139}$$

for $k \in [1, K]$. Using the fact that the basis is symmetric so that the trace corresponds to the inner product of X with the basis, we can equate

$$X_1^{\mathrm{re,bd},\pi(k)} = X_{k+1}^{\mathrm{re,bd},\pi(k)}, \text{ for } k \in [1, K], \tag{C$\gamma_{\pi(k)}$}$$

where the superscript re,bd, $\pi(k)$ denotes the real and block-diagonal components with respect to bipartition $\pi(k)$.

VI. The other term, $\langle C, X\rangle$ *, is the primal objective;*

The only thing that remains before phrasing the constraints of the primal program is to note that the objective function may be written as

$$\begin{aligned}\mathrm{Tr}[-(\gamma, \mathbb{O}_{2N}, ..., \mathbb{O}_{2N}, -1, 1, 0, ...0)X] &= -(\mathrm{Tr}[\gamma X_1] - X_{K+2} + X_{K+3}) \\ &= -(\mathrm{Tr}[\gamma X_1] - 1), \end{aligned} \tag{5.140}$$

where we used the constraint (Cx_e) and the definition of C from eq. (5.133).

VII. Combine the elements above to write the primal SDP in standard form (Def. 5.25).

This allows us to write the SDP that finds the optimal genuine multipartite entanglement witness for a given CM. We put together constraints (Cx_e),(Cλ_k) and (C$\gamma_{\pi(k)}$) together with the objective function from eq. (5.140)[41] to get

SDP 5.5 (Primal program for optimal GME witness (repetition of SDP 5.3))**.** For a given CM γ of an N-mode state, the SDP

$$\begin{aligned} \underset{X}{\text{minimise}} \quad & \mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \\ \text{subject to} \quad & X_1^{\mathrm{re,bd},\pi(k)} = X_{k+1}^{\mathrm{re,bd},\pi(k)} \quad \text{for all} \quad k = 1, \ldots, K, \\ & \mathrm{Tr}[i\Omega_N X_{k+1}] + X_{K+2} - X_{K+3} + X_{K+3+k} = 0, \quad \text{for all} \quad k = 1, \ldots, K \\ & X_{K+2} - X_{K+3} = 1. \end{aligned}$$

has a feasible solution with $\mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \geq 0$ whenever γ is biseparable. If γ is genuinely multipartite entangled, the program produces a negative value. We used $\pi(k)$ to denote the k^{th} bi-partition (out of $K = 2^{N-1} - 1$ possible). $X^{\mathrm{re,bd},\pi(k)}$ is the real part of X that is block-diagonal with respect to partition $\pi(k)$ - elements across the partition are set to zero.

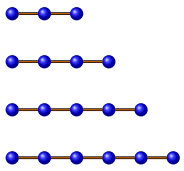
5.7 Briefly on graphs which represent witnesses

In the next chapter we work with, what we call minimal knowledge graphs. These correspond to the fewest quadrature correlation measurements needed to determine GME in a state, as linear sums of covariance matrix elements. We show that only a subset of all measurements suffice. The way we describe the situation is through graphs where each vertex corresponds to a mode and each edge to covariance measurements between the modes. It turns out that the simplest graphs - trees - are sufficient. Let us define graphs more formally.

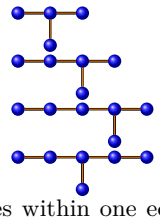
A graph is a collection of N vertices, V, and edges E between $v \in V$, denoted (V, E). The simplest graphs are called *trees* which are graphs with the least number of undirected edges that connect all vertices (no loops and no disjoint vertices). Other equivalent definitions are that any two vertices are connected by a unique path or the removal of any edge would partition (V, E) into two unconnected graphs. Some examples of graphs are depicted in fig. 5.3 for a low number of vertices. A *complete graph* is one which has all vertices a distance one from any other

[41] Recall that the primal SDP is a maximisation scheme in our convention so that we may alternatively minimise the negative of the objective function.

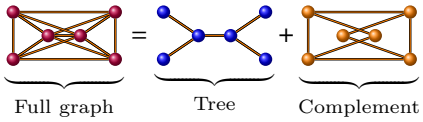
- all vertices are connected directly. The *complement* of a tree is formed by the vertices V and edges E' of the complete graph with the edges E removed**.** You can see this relationship in figs. 5.3(c)–(f).



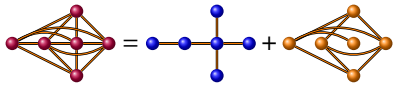
(a) Linear trees for $N = 3, 4, 5, 6$ vertices.



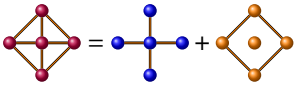
(b) Tree with vertices within one edge of the main path, also known as a caterpillar tree.



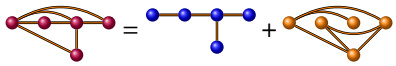
(c) A tree (blue nodes) and its complement (orange nodes). The fully connected graph is the union of the two.



(d) A caterpillar tree for $N = 6$ with complement and full graph. Two other are found in (b). There are 4 in total, excluding the linear and star graphs.



(e) Star tree for $N = 5$ with complement and full graph.



(f) Caterpillar tree for $N = 5$ with complement and full graph.

Figure 5.3: Some example knowledge graphs describing the two-body correlations inquired by partially witnesses. They represent the minimum number of measurements required to establish the presence of GME in the state measured.

We use graphs to depict the information extracted by a witness on covariance matrices. We let each vertex represent a mode in the state and each edge represent the covariance between the modes. Thus, witnesses represented by incomplete graphs are those that use a subset of the information encoded in a CM - these we call *partially blind* witnesses. Further, trees correspond to witnesses that use the least amount of information required for establishing GME. This is because if we had a graph that had at least one vertex with no connection, then the witness could not rule out entanglement across that partition of the state. We use the term *knowledge graphs* to refer to those which represent witnesses.

We introduce witnesses represented by trees in more detail in section 6.2.

CHAPTER 6

Inferring genuine Gaussian multipartite entanglement from separable marginals

This chapter will cover new work. A manuscript has been produced and is currently under review for publication (arXiv:2103.07327).

6.1 Phrasing the problem

Sensing an object requires at least two components – the viewer and the viewed – which can be in different informational states. There are, likewise, various ways to extract questions from this chapter's title. One example, from the angle of the viewer, is in terms of drawing conclusions from incomplete information: frequently we are positioned to determine the presence of something from extraneous clues in the environment. For example we might become aware of a car speeding towards us by the sound of the engine or the hesitancy of fellow pedestrians to cross the street. We have concluded that there is an approaching vehicle in the vicinity without seeing the vehicle itself or absorbing *all* the cues caused by the car. This is an example of using *incomplete* and *indirect* information as evidence. This question has been formalised in mathematics and statistics as the marginal problem. The translation to the quantum scenario has been done in refs. [150, 151]. The question we will consider in this chapter is an aspect of the quantum marginal problem. Specifically pertaining to entanglement properties [141, 152–154]. Consider a multi-particle state with unknown entanglement properties. One may inquire about the presence of genuine multipartite entanglement (GME) through looking at only the correlations of two-body reductions - the marginals. Then the question can be phrased as "Which entanglement properties can we determine from probing reductions of a multipartite state"? More specifically we can ask "Are there Gaussian states whose GME can be inferred from an incomplete set of two-body correlations?".

Another approach is related to the topic of emergence [155]. A property is said to be emergent if, in a composite system, it does not exist in the components yet appears once there is a sufficient number of elements (or complexity, or connections, etc.) Examples span many fields of study, including correlated condensed matter systems, biological systems [156] and social structures [157]. Closer to the topic at hand, one may ask: could multipartite entanglement be present in a multipartite state even when there is no entanglement among pairs of subsystems? That is, could entanglement appear at a high level – in terms of number of particles involved – even when no trace of it exists at the lowest order. In a different way: can separable parts be arranged such that they are entangled only at the level of the whole state? We phrase our question then goes as "Can we infer the presence of GME in Gaussian states which have separable two-body marginals?".

We can put these two lines of thought together. They offer two points of view, one concerns internal properties of the state: GME; separable marginals. The other regards the way of determining these properties by an outside viewer: incomplete information. We formulate the full research question as: "Are there Gaussian quantum states with GME which can be inferred from a subset of separable two-body marginals?". As we will see, we answer this question affirmatively and provide examples for three and four-mode states.

The work presented here follows research done on qubit systems. Analytical examples exhibiting some of the properties were derived in ref. [152]. Numerical schemes were used to find states with a stronger effect [153], even in the partial-information scenario [141]. This includes an experimental realisation of a state with the desired properties [154].

In section 6.2 we introduce the concept of partially-blind witnesses. Then we move on to formulate the semidefinite conditions that define our problem in section 6.3 where we also present the search algorithm. The results of the algorithm are found in section 6.4. To bridge the gap to experiment, we present a scheme for producing the three-mode example in an optical laboratory.

6.2 Partly-blind GME witnesses

It is often desirable to minimise the number of measurements required to determine certain properties, including entanglement in quantum states. Decreasing tomography costs can be useful for quantum information tasks, for example for verifying state properties or reading computation results. This can lead to an increased speed of protocols or even enable some by reducing overhead costs and allowing verification to be done online - whilst running the protocol.

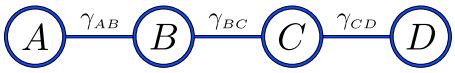
When determining whether a Gaussian quantum state carries GME, it is interesting to know whether a minimal set of measurements exists. That is the topic of this chapter. The minimal sets we consider here in the entanglement scenario correspond to measurements of two-mode correlations.

To depict the witnesses we use graphs (trees) as presented in section 5.7 (Briefly on graphs which represent witnesses), which we refer to as *knowledge graphs*. The vertices represent each subsystem of a multipartite state. For a witness, the edges E correspond to the correlation measurements used to determine some states' GME. Since trees are not fully connected graphs, the connections that are not present in the graph (the complement to E, E') correspond to zeros in the witness matrix. This means that witnesses with a tree as a knowledge graph do not probe the whole CM. For this reason, we will refer to them as *partially blind*. Note that a tree-like knowledge graph is the smallest possible for detecting GME since, if we would have two disjoint sub-graphs, we would not be able to determine entanglement across the corresponding bipartition. We give the four-mode examples of partially-blind witnesses in fig. 6.1.

Witnesses of entanglement on covariance matrices correspond to linear combinations of measurements of the quadrature operators [123]. These were introduced in section 5.6 (Finding the witness for a CM as a semidefinite program). Imposing the requirements of incomplete information on these witnesses amounts to setting some of their entries to zero. For example, if the correlations between modes A_i and A_j are not measured then the 2×2 submatrix in the witness representation, corresponding to variances between $x_i, x_j, p_i, p_j, (i \neq j)$, would be set to zero. These are the elements in E'. The requirements on the partially blind GME witnesses are given in table 6.1.

Table 6.1: SDP constraints and their physical interpretation for finding the optimal GME witness for a given CM.

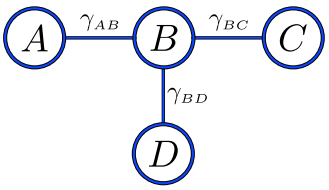
Witness (W) requirement	**Physical meaning**
Positive semidefinite	as required in [123];
$\mathrm{Tr}[W\gamma] < 1$	W detects entanglement in γ;
W has zero entries in some submatrices	Partial-blindess criterion (see section 6.2).



(a) Linear knowledge graph.

$$\begin{pmatrix} A & ab & \mathbb{O} & \mathbb{O} \\ ab & B & bc & \mathbb{O} \\ \mathbb{O} & bc & C & cd \\ \mathbb{O} & \mathbb{O} & cd & D \end{pmatrix}$$

(b) Matrix form of linear witness.



(c) T-shaped knowledge graph.

$$\begin{pmatrix} A & ab & \mathbb{O} & \mathbb{O} \\ ab & B & bc & bd \\ \mathbb{O} & bc & C & \mathbb{O} \\ \mathbb{O} & bd & \mathbb{O} & D \end{pmatrix}$$

(d) Matrix form of linear witness.

Figure 6.1: The two possible knowledge graphs for a four-mode state along with the witness structure. The witness entries are 2×2 matrices. The labels denote the corresponding mode in the $XPXP$ ordering.

Witnesses of Gaussian genuine multipartite entanglement acting on covariance matrices can be found via optimisation schemes with constraints written as inequalities on semidefinite matrices [123]. In section 5.5, we introduced semidefinite programs (SDPs) and in section 5.6 we presented an SDP for finding the optimal GME witness for a given covariance matrix. We can write the blindness conditions, defined in terms of the graph E, as an SDP constraint

$$(W)_{jk} = \mathbb{O}_2, \quad \text{if} \quad \{j,k\} \notin E, \tag{6.1}$$

for some witness W. Experimentally the blindness criterion corresponds to measuring fewer CM matrix elements: quadrature elements $\langle \hat{q}_j \hat{q}_k \rangle$ can be ignored for $j,k \notin E$.

Including the blindness criterion into the program which finds the optimal entanglement witness, SDP 5.3, gives the following optimization rules

SDP 6.1 (Optimal GME witness (partially blind))**.** For an N-mode state with covariance matrix γ and knowledge graph E, one may test whether the state is genuinely multipartite entangled at the Gaussian level through the following SDP.

$$\begin{aligned} \underset{X}{\text{minimize}} \quad & \mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \\ \text{subject to} \quad & X_1^{\mathrm{re,bd},\pi(k)} = X_{k+1}^{\mathrm{re,bd},\pi(k)} \quad \text{for all} \quad k = 1,\dots,K, \\ & \mathrm{Tr}[i\Omega_N X_{k+1}] + X_{K+2} - X_{K+3} + X_{K+3+k} = 0, \quad \text{for all} \quad k = 1,\dots,K \\ & X_{K+2} - X_{K+3} = 1 \\ & (X)_{ij}^{\mathrm{re}} = \mathbb{O}_2, \quad \text{if} \quad \{i,j\} \in E'. \end{aligned}$$

If the value $\mathrm{Tr}\left[\gamma X_1^{\mathrm{re}}\right] - 1 \geq 0$ then γ is biseparable and otherwise it has GME so that the output, X_1^{re}, satisfies the criterion for being a GME witness.

How the constraints in SDP 6.1 are arrived at is explained in detail in section 5.6. In short, the top-left block of the SDP variable, X (a matrix), satisfies the properties of a witness while the other blocks X_j, $j \neq 1$, are derived from the requirements of separability from the dual problem, SDP 5.4 which is in a more physically informative form.

6.3 Search algorithm

We are nearly in a position to phrase an algorithm that finds examples of covariance matrices of states with separable marginals and whose GME can be inferred from witnesses using incomplete information. For that we need to complete two main tasks: 1) find the optimal witness for a given covariance matrix (SDP 6.1), and 2) find the optimal covariance matrix for a given witness (as will be given in SDP 6.2 in section 6.3.1). Once we have those protocols, we can feed the output of one into the other to iteratively find stronger examples. The algorithm is presented in algorithm 1.

In the previous section, we saw that optimal GME witnesses on covariance matrices can be found which probe only a subset of state correlations via SDP 6.1. We now turn the task around and ask, for a given witness, which CM carries the most detectable genuine multipartite entanglement?

6.3.1 Semidefinite program for finding the optimal state

An SDP may also be formulated for finding the optimal[1] covariance matrix (CM) for a given witness since the requirements we impose on the CMs can be written as linear constraints on semi-definite matrices. These conditions are summarised in table 6.2. For a brief introduction to semidefinite programs see section 5.5.

Firstly, covariance matrices of quantum (or otherwise) states must be positive semi-definite since variances are either zero or positive (see footnote 17 on page 70 and associated text for a proof). One may see that they are also symmetric since the quadrature covariances, $\mathrm{Tr}\big[\{\xi_j, \xi_k\}\rho\big]$, are unaltered by a swap of indices $j \leftrightarrow k$. [2]

Next, quantum CMs must fulfill the Heisenberg uncertainty principle, given in Thm. 5.4. That is, for a covariance matrix γ we must have $\gamma + i\Omega \geq 0$, where Ω is the symplectic form (see Def. 5.8). Further, we impose the requirement of having separable two-body marginals (tying to the idea of GME as an emergent property). We do this by using the positive-partial transpose criterion from Thm. 5.7: $\gamma_{AB}^{T_A} + i\Omega_2 \geq 0$.

Lastly, we want to find CMs of states that are easier to produce experimentally. One step in that direction is to limit the search to states with no x-p correlations. To this end we set to zero the elements corresponding to *all* correlations between position and momentum. This also offers the computational advantage of further limiting the search space.

Using the constraints in table 6.2, the SDP that finds the optimal CM (γ_W) for a given witness (W) can be cast as in SDP 6.2.

SDP 6.2 (Optimal covariance matrix)**.** For a GME witness W, one finds the covariance matrix that optimizes the amount of entanglement detected by W through

$$\begin{aligned} \underset{\gamma_W}{\text{minimize}} \quad & \mathrm{Tr}[\gamma_W W] - 1 \\ \text{subject to} \quad & \gamma_W + i\Omega_N \geq 0, \\ & \gamma_{W,jk}^{(T_j)} + i\Omega_2 \geq 0, \quad \text{for all} \quad j \neq k = 1, \ldots, N, \\ & (\gamma_W)_{2j-1,2k} = (\gamma_W)_{2j,2k-1} = 0, \quad j, k = 1, \ldots, N. \end{aligned}$$

Whenever the witness, W, input already detects GME in some state, the program produces a CM γ_W with $\mathrm{Tr}[\gamma_W W] - 1 < 0$.

[1] Optimality is defined in the same manner as for witnesses: "for a given witness W, the CM γ which minimises $\mathrm{Tr}[\gamma W]$". See sections 5.5 and 5.6 for more details.

[2] Note that $\gamma \in PSD$ implies that $\gamma \in Sym$. See footnote 3 in chapter 5.

Table 6.2: SDP constraints and their physical interpretation for finding the optimal CM for a given GME witness.

Covariance matrix (γ) requirement	Physical reason
Positive semi-definite, $y^T\gamma y \geq 0, \forall y \in \mathbb{R}^{2N}$	Variances are necessarily positive;
Symmetric, $\gamma - \gamma^T = 0$	Variances unaltered by variable swap;
$\gamma + i\Omega \geq 0$	Satisfy the uncertainty principle;
Two-party marginals fail PPT	Separable marginals;
$(\gamma)_{2i-1,2j} = 0$	No $x-p$ correlations.

We subtract one from $\mathrm{Tr}[\gamma_W W]$ in the minimization target function as the optimal entanglement witness on covariance matrices detects entanglement if $\mathrm{Tr}\left[\gamma_{Entangled} W\right] > 1$. This allows us to only check the sign of the output of the SDP 6.2. We also note that the two first constraints in table 6.2 (Positive semi-definite and symmetric) are fulfilled automatically by the nature of SDPs and the initial input into the algorithm respectively (see footnotes 3 and 16 along with the associated text).

6.3.2 Generating a random Gaussian CM

We need one last element before formulating the algorithm - we need an initial input into SDP 6.1. To that end we prepare a random Gaussian CM.

Since we want to avoid finding states with $x-p$ correlations, it is easier to start in the $XXPP$ ordering. This is because CMs with no correlations between position and momentum are block-diagonal of the form $\sigma = X \oplus P = \left(\begin{smallmatrix} X & \mathbb{0} \\ \mathbb{0} & P \end{smallmatrix}\right)$, where X and P are $N \times N$ matrices corresponding to the position and momentum correlations respectively.

One may return to the original $XPXP$ ordering through a congruence transformation with the matrix λ (Def. 5.9). We remind the reader that λ is an orthogonal matrix with zero entries except for $\lambda_{j,2j-1} = \lambda_{N+j,2j} = 1, j = 1, ..., N,$. The transformations and symbol definitions in each ordering are then given in table 6.3.

Table 6.3: Ordering conversion between $XPXP$ and $XXPP$ orderings. The transformation matrix, λ, as given in Def. 5.9, is an orthogonal matrix with $\lambda_{j,2j-1} = \lambda_{N+j,2j} = 1, j = 1, ..., N$, the only non-zero elements.

Object name (Symbol)	Conversion
Quadrature vector (ξ)	$\chi = \lambda\xi$
Covariance matrix (γ)	$\sigma = \lambda\gamma\lambda^T$
Symplectic form (Ω_N)	$\Sigma_N = \lambda\Omega_N\lambda^T$
Symplectic matrix (S)	$Q = \lambda S\lambda^T$

In the section on Gaussian operations (section 5.2.2), we saw that a general Gaussian covariance matrix may be decomposed as per Williamson's Theorem (Thm. 5.1) which we apply to the covariance matrix σ in the $XXPP$ ordering to get

$$\sigma = Q\Delta Q^T, \tag{6.2}$$

where Q is a symplectic transformation and Δ is a diagonal matrix of the symplectic eigenvalues of the CM σ. Since Q is symplectic, it satisfies $Q\Sigma Q^T = \Sigma$ with $\Sigma = \left(\begin{smallmatrix} \mathbb{O} & \mathbb{1} \\ -\mathbb{1} & \mathbb{O} \end{smallmatrix}\right)$. Recall that if $\Delta = \mathbb{1}_N$ then $\sigma = QQ^T$ describes a pure state.

Since we limit ourselves to states with no $x-p$ correlations, Q must be block-diagonal. Thus $Q = Q_X \oplus Q_P$ with $Q_{X(P)}$ an $N \times N$ matrix corresponding to the position (momentum) correlations.

Since Q needs to be symplectic, we can constrain its elements further. That is, since $Q\Sigma Q^T = \Sigma$, we have [3] $(Q_X \oplus Q_P)\left(\begin{smallmatrix} \mathbb{O} & \mathbb{1} \\ -\mathbb{1} & \mathbb{O} \end{smallmatrix}\right)(Q_X \oplus Q_P)^T = \left(\begin{smallmatrix} \mathbb{O} & Q_X Q_P^T \\ -Q_P Q_X^T & \mathbb{O} \end{smallmatrix}\right) \stackrel{!}{=} \left(\begin{smallmatrix} \mathbb{O} & \mathbb{1} \\ -\mathbb{1} & \mathbb{O} \end{smallmatrix}\right)$, so that $Q_P = \left(Q_X^T\right)^{-1}$. Since the two blocks are related we write $Q_X = \tilde{Q}$. Note that $\tilde{Q}$ is a generic matrix and so may be filled by random real entries.

Putting things together, we can create a random Gaussian CM using $N^2 + N$ random real numbers encoded in the diagonal matrix of symplectic eigenvalues, $\mathcal{V} = \mathrm{diag}(\nu_1, \nu_2, ..., \nu_N)$ (with $\nu_i \geq 1$), and an $N \times N$ matrix with random entries $\tilde{Q}$. We can then write

$$\sigma = (\tilde{Q}\mathcal{V}\tilde{Q}^T) \oplus ((\tilde{Q}^T)^{-1}\mathcal{V}\tilde{Q}^{-1}). \tag{6.3}$$

Finally, to get a random Gaussian covariance in the $XPXP$ ordering, we transform eq. (6.3) as

$$\gamma = \lambda^T \sigma \lambda. \tag{6.4}$$

This procedure produces a CM that will serve as an input to the main part of the algorithm. It corresponds to line (1) in algorithm 1.

6.3.3 Joining the two SDPs

We are now in a position to set up an algorithm that finds examples of covariance matrices of states with the desired properties along with witnesses that detects the GME. The two main parts we need are the SDPs 6.1 and 6.2 for finding the optimal GME witness given a CM and vice versa, respectively. As an initial input we produce a random Gaussian covariance matrix as described in section 6.3.2.

The algorithm then follows the steps given in algorithm 1. Starting from an input random Gaussian CM (eq. (6.3)) we run SDPs 6.1 and 6.2 iteratively n times, outputting in most cases a pair (γ, W) of CM γ with separable marginals and GME detected by witness W. Next, we present some example obtained using the program written for three and four-mode Gaussian CMs in section 6.4.

[3] The symbol "$\stackrel{!}{=}$" is to be read as "must be equal to".

Algorithm 1: Gaussian GME factory
Pseudo-code for program to find examples of covariance matrices with the required properites (see text). The two optimization problems on lines `(2)/(5)` and `(3)/(6)` are given by the SDPs 6.1 and 6.2 respectively. The random Gaussian input is prepared as prescribed in section 6.3.2 (eq. (6.3) specifically).

(1) **Data:** Prepare random covariance matrix γ_{in}
(2) $W_0 \leftarrow$ `findOptimalWitness`(γ_{in});
(3) $\gamma_0 \leftarrow$ `findOptimalCovarianceMatrix`(W_0);
(4) **for** $i \in [0, n-1]$ **do**
(5) $\quad W_{i+1} \leftarrow$ `findOptimalWitness`(γ_i);
(6) $\quad \gamma_{i+1} \leftarrow$ `findOptimalCovarianceMatrix`(W_i);
(7) $W_n \leftarrow$ `findOptimalWitness`(γ_n);
(8) **Output:** $(\gamma_n\ ,\ W_n)$

For the results presented in the coming section, we [4] wrote a MATLAB program using the optimization toolbox YALMIP [159] with the SDP solver `SeDuMi`[160] (toolbox `MOSEK`[161] was also used during research).

6.4 Results

Using a program based on algorithm 1, we produced examples of states of three and four modes. In order to find states that allow for easier experimental realisation we selected the best examples using two further requisites. First, we want the examples to maintain the desired properties even when the entries are rounded to 2 decimal places (d.p.)[5]. This is so that we can find states that are more resilient to deviations in an experimental realisation. Further, we remove any examples where the solver (`SeDuMi`) passed an error or warning.

In this work, we looked at examples of up to six modes, with the three and four-mode examples presented in more detail. The witness knowledge graphs we use are shown in fig. 6.2. For results up to six modes, see table 6.7.

6.4.1 Three modes

We run algorithm 1 for a total of $n = 10$ iterations[6] and for $N = 3$ modes. The witness which detects GME probes only the parts of the CM, $\gamma^{(3)}$, which correspond to $\gamma^{(3)}_{AB}$ and $\gamma^{(3)}_{BC}$ as well as all mode-local variances, γ_A, γ_B and γ_C. The knowledge graph thus corresponds to a linear tree and is depicted in fig. 6.2 a). As required, $\gamma^{(3)}$ has all marginals separable. Since this example ends up showing the most promise for experimental realisation we also add a number of further requirements. First we bound the diagonal elements to the range $[1, 10]$ in order to limit the

[4] Co-author J. Provazník in the associated article [158] updated the routine `MultiWit` [123] to be compatible with the current MATLAB version and added the constraints for the three-mode and linear four-mode scenarios. I then used that routine to write an instance of algorithm 1 (including writing the computer code for SDP 6.2).

[5] In some examples, we found that some CMs lost some of the properties – marginal separability or GME – after rounding. A detailed analysis could be performed to characterise these effects. For our purposes, we simply filtered out examples that did not meet our rounding requirements.

[6] See appendix F where we present supporting evidence for this choice.

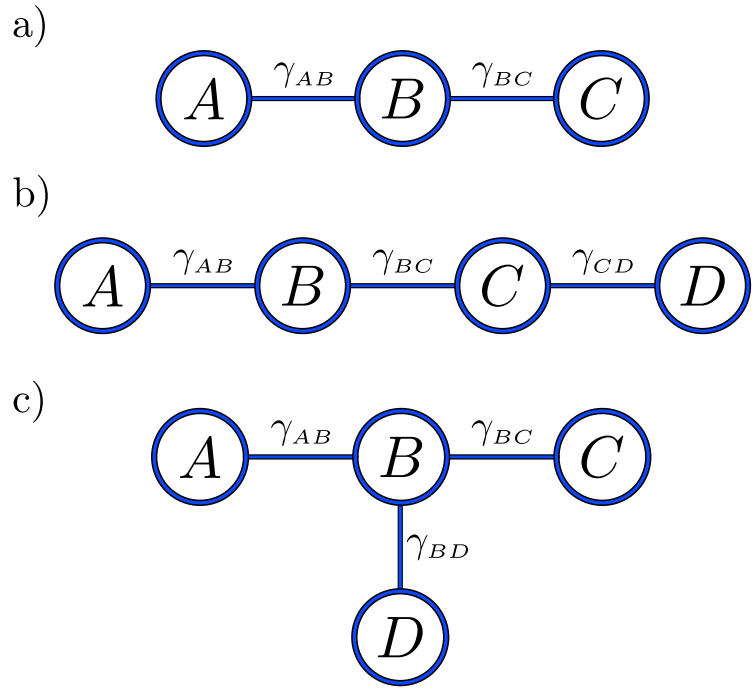


Figure 6.2: Knowledge graphs witnesses detecting GME from marginal CMs of three and four modes.

amount of squeezing required to produce the state with CM $\gamma^{(3)}$[7]. For the same reason, we also required the smallest eigenvalue of $\gamma^{(3)}$ to be above 0.2[8].

The CM with the strongest value for $\mathrm{Tr}[\gamma^{(3)}W^{(3)}] - 1$ obtained through this procedure is:

$$\gamma^{(3)} = \begin{pmatrix} 1.34 & 0 & -0.35 & 0 & -0.82 & 0 \\ 0 & 10.00 & 0 & 8.45 & 0 & 1.87 \\ -0.35 & 0 & 7.80 & 0 & -8.05 & 0 \\ 0 & 8.45 & 0 & 7.92 & 0 & 2.09 \\ -0.82 & 0 & -8.05 & 0 & 10.00 & 0 \\ 0 & 1.87 & 0 & 2.09 & 0 & 1.62 \end{pmatrix}. \tag{6.5}$$

[7] The submatrix for each mode needs to also satisfy the uncertainty principle (Thm. 5.4 or eq. (5.67)) so if the variances $\langle x_i^2 \rangle$ and $\langle p_i^2 \rangle$ are very different, then the state requires a high amount of local squeezing in the i^{th} mode.

[8] We have $\gamma = URV^T WVRU^T$ via Williamson's Theorem. Eigenvalues are preserved under similarity transformations so the eigenvalues of γ are given by $eig(\gamma) = eig(RV^T WVR)$, with $eig(\cdot)$ the vector of eigenvalues. The entries of W are the symplectic eigenvalues so we may set $W = \mathbb{1}$ since any $eig(W) \ni w \geq 1$. We get, in that case, $eig(\gamma) = eig(R^2)$ since V is orthogonal. Using the conversion to dB through eq. (5.55), equating the smallest value of R with $\sqrt{0.2}$ would give a squeezing of about $7dB$ - well below the record of $15dB$ [69].

Its optimal witness, $W^{(3)}$, is such that $\mathrm{Tr}[\gamma^{(3)}W^{(3)}] - 1 = -0.143$. It is given by

$$W^{(3)} = 10^{-2}\begin{pmatrix} 6.8 & 0 & -0.4 & 0 & 0 & 0 \\ 0 & 34.3 & 0 & -39.5 & 0 & 0 \\ -0.4 & 0 & 25.1 & 0 & 20.9 & 0 \\ 0 & -39.5 & 0 & 46.1 & 0 & -2.0 \\ 0 & 0 & 20.9 & 0 & 17.5 & 0 \\ 0 & 0 & 0 & -2.0 & 0 & 6.6 \end{pmatrix}. \tag{6.6}$$

One may see that the witness corresponds to the linear knowledge graph by noticing the zero entries in the 2×2 blocks corresponding to $\gamma^{(3)}_{AC}$ (top-right and lower-left corners).

We required the two-body marginals to be separable. This can be verified via the PPT criterion (Thm. 5.7). The smallest eigenvalues of $(\gamma^{(3)}_{XY})^{T_X} + i\Omega_2$ for $XY = AB, AC, BC$ are presented in table 6.4. As can be seen all are positive numbers as required for separability.

Table 6.4: Minimal eigenvalue $\varepsilon^{(3)}_{jk} \equiv \min\{\mathrm{eig}[(\gamma^{(3)}_{jk})^{(T_j)} + i\Omega_2]\}$.

jk	AB	AC	BC
$\varepsilon^{(3)}_{jk}$	0.002	0.849	0.004

Since the result presented for the three-mode case turns out to be the strongest one with respect to $\mathrm{Tr}[\gamma W]$, we do a comparison with the best qubit results obtained in Ref. [141]. Note that the values $\mathrm{Tr}[\rho W]$ and $\mathrm{Tr}\left[\gamma W^{(3)}\right]$ are not directly comparable. For that reason, let us compare the difference between the best theoretical result with the best example found numerically. For qubits, the best theoretical witness mean of $-1.98\cdot 10^{-2}$ when all marginals are know is three times larger than the best qubit mean of $\mathrm{Tr}[\rho W] = -6.58\cdot 10^{-3}$ for three modes [153] created experimentally in [154]. Meanwhile the result presented here of $\mathrm{Tr}\left[\gamma^{(3)}W^{(3)}\right] - 1 = -0.143$ can be compared to the theoretical value of -0.103 of Gaussian bound entanglement [123, 145] which was experimentally prepared in [162]. This provides evidence for the experimental accessibility of our result. Further, the noise tolerance is also more promising in the Gaussian scenario. The noise tolerance of CM $\gamma^{(3)}$ is of 10% [9] while the qubit exhibited a tolerance to the addition of 5% [153] noise. This value coincides with the demonstrated Gaussian bound entanglement result [123].

We have thus a promising example for experimental realisation. We therefore present a circuit of optical elements for producing CM $\gamma^{(3)}$ in section 6.5. Before that we present the results for four modes.

6.4.2 Four modes

We extended the search to find examples of CMs corresponding to four-mode Gaussian quantum states. In this case, there are two possible knowledge graphs: the linear tree of four nodes and the 't'-shaped or star tree. These are presented in fig. 6.2 b) and c). We also kept the constraints that the effects should be present when the entries to the witness and CM are rounded to 2 decimal places.

[9] Addition of white noise, parametrised by p, at the CM level corresponds to adding the identity wieghted by p: $\gamma_p = \gamma + p\mathbb{1}$. For $\gamma = \gamma^{(3)}$, we may find a witness that detects GME up to $p = 0.1092$. Writing the threshold at which noise destroys the effect as $p_{\max} = 0.1092$, one finds through the addition of $5\%(p_{\max}/2)$ of white noise the new CM $\gamma^{(3)} \to \gamma^{(3)}_{p=p_{\max}/2} = \gamma^{(3)} + \frac{0.1092}{2}\mathbb{1}_6$ which has an optimal entanglement witness W with $\mathrm{Tr}\left[\gamma^{(3)}_{p=p_{\max}/2}W\right] - 1 = -0.073$. The smallest symplectic eigenvalues of the marginals AB,AC and BC are $\eta_{AB} = 0.056$,$\eta_{AC} = 0.8773$ and $\eta_{BC} = 0.058$ respectively.

6.4.2.1 Linear graph

First we present the results for the case when the witness is oblivious to the correlations between modes AC, AD and BD. This corresponds to setting the 2×2 submatrices $\gamma_{AC}, \gamma_{AD}, \gamma_{BD}$ to zero. In terms of the constrains of SDP 6.1, this corresponds to the knowledge graph given in fig. 5.3 b).

The best example produced running SDP 6.1 for $n = 10$ iterations is

$$\gamma^{(4,L)} = \begin{pmatrix} 2.83 & 0 & -0.02 & 0 & -1.38 & 0 & 2.83 & 0 \\ 0 & 7.18 & 0 & 8.06 & 0 & 7.09 & 0 & -4.12 \\ -0.02 & 0 & 3.91 & 0 & -2.46 & 0 & 4.73 & 0 \\ 0 & 8.06 & 0 & 9.79 & 0 & 8.47 & 0 & -4.81 \\ -1.38 & 0 & -2.46 & 0 & 2.58 & 0 & -4.68 & 0 \\ 0 & 7.09 & 0 & 8.47 & 0 & 10.00 & 0 & -3.08 \\ 2.83 & 0 & 4.73 & 0 & -4.68 & 0 & 10.00 & 0 \\ 0 & -4.12 & 0 & -4.81 & 0 & -3.08 & 0 & 3.22 \end{pmatrix}. \tag{6.7}$$

It has an optimal witness, $W^{(4,L)}$, such that $\mathrm{Tr}\left[\gamma^{(4,L)} W^{(4,L)}\right] - 1 = -0.069$ which takes the following numeric form

$$W^{(4,L)} = 10^{-2} \cdot \begin{pmatrix} 2.70 & 0 & -1.12 & 0 & 0 & 0 & 0 & 0 \\ 0 & 33.29 & 0 & -28.67 & 0 & 0 & 0 & 0 \\ -1.12 & 0 & 6.86 & 0 & 6.30 & 0 & 0 & 0 \\ 0 & -28.67 & 0 & 29.50 & 0 & -5.46 & 0 & 0 \\ 0 & 0 & 6.30 & 0 & 74.73 & 0 & 33.42 & 0 \\ 0 & 0 & 0 & -5.46 & 0 & 7.37 & 0 & 2.18 \\ 0 & 0 & 0 & 0 & 33.42 & 0 & 16.30 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2.18 & 0 & 4.11 \end{pmatrix}. \tag{6.8}$$

The separability of all marginals may be confirmed once again by the PPT criterion (see table 6.5).

Table 6.5: Minimal eigenvalue $\varepsilon_{jk}^{(4,L)} \equiv \min\{\mathrm{eig}[(\gamma_{jk}^{(4,L)})^{(T_j)} + i\Omega_2]$.

jk	AB	AC	AD	BC	BD	CD
$\varepsilon_{jk}^{(4,L)}$	0.005	0.347	0.213	0.004	0.087	0.224

The smallest value in table 6.5 is comparable to the three-mode case (table 6.4) so those marginals seem equally close to being entangled. The effect strength, however, is about half that of the three-mode case. This, together with the fact that there are more modes involved (and hence would require a more complicated set-up at face value), means that producing the four-mode state would be experimentally more demanding.

6.4.2.2 T-shaped graph

We now present the other four-mode example: the one whose knowledge graph is the 't'-shaped (or four-vertex star) graph as in fig. 6.2. This corresponds to a witness blind to correlations contained in γ_{AC}, γ_{AD}, and γ_{CD} (see eq. (6.10)).

The best CM produced with the same procedure as previously ($n = 10$) is

$$\gamma^{(4,T)} = \begin{pmatrix} 5.23 & 0 & 0.45 & 0 & -0.02 & 0 & -2.43 & 0 \\ 0 & 1.16 & 0 & 3.00 & 0 & 1.15 & 0 & 0.51 \\ 0.45 & 0 & 3.35 & 0 & 0.91 & 0 & -5.20 & 0 \\ 0 & 3.00 & 0 & 10.00 & 0 & 3.52 & 0 & 2.06 \\ -0.02 & 0 & 0.91 & 0 & 4.09 & 0 & -2.97 & 0 \\ 0 & 1.15 & 0 & 3.52 & 0 & 1.62 & 0 & 0.62 \\ -2.43 & 0 & -5.20 & 0 & -2.97 & 0 & 10.00 & 0 \\ 0 & 0.51 & 0 & 2.06 & 0 & 0.62 & 0 & 1.49 \end{pmatrix}. \tag{6.9}$$

The witness, giving $\mathrm{Tr}[\gamma^{(4,T)} W^{(4,T)}] - 1 = -0.068$, is

$$W^{(4,T)} = 10^{-2} \cdot \begin{pmatrix} 1.984 & 0 & -0.815 & 0 & 0 & 0 & 0 & 0 \\ 0 & 76.150 & 0 & -26.031 & 0 & 0 & 0 & 0 \\ -0.815 & 0 & 37.883 & 0 & -1.525 & 0 & 19.701 & 0 \\ 0 & -26.031 & 0 & 18.014 & 0 & -22.092 & 0 & -0.760 \\ 0 & 0 & -1.525 & 0 & 2.895 & 0 & 0 & 0 \\ 0 & 0 & 0 & -22.092 & 0 & 54.640 & 0 & 0 \\ 0 & 0 & 19.701 & 0 & 0 & 0 & 10.563 & 0 \\ 0 & 0 & 0 & -0.760 & 0 & 0 & 0 & 3.149 \end{pmatrix}. \tag{6.10}$$

Note that the witness in eq. (6.10) is rounded to more decimal places. This is because positivity is not preserved when rounding as in the previous cases.

The marginals are separable, as seen in table 6.6 (and using the PPT criterion).

Table 6.6: Minimal eigenvalue $\varepsilon_{jk}^{(4,T)} \equiv \min\{\mathrm{eig}[(\gamma_{jk}^{(4,T)})^{(T_j)} + i\Omega_2]\}$.

jk	AB	AC	AD	BC	BD	CD
$\varepsilon_{jk}^{(4,T)}$	0.0481	0.0032	0.5256	0.1103	0.0001	0.5489

The effect strength and separability are comparable to the linear four-mode example. A noteworthy point is that the examples given here are CMs of mixed states (this can be checked by verifying that the symplectic eigenvalues are not all unity) while the best four-mode qubit example corresponded to a 't'-shaped tree and was a pure state [141][10].

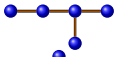
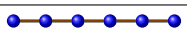
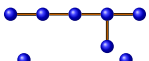
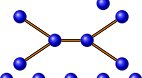
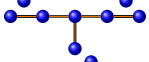
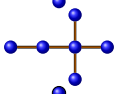
6.4.3 Five and six modes

We now cover some work looking at a larger number of modes[11]. Using the same constraints as earlier we perform the search for examples of five and six modes. Since the number of possible knowledge graphs is larger, we present the results in table 6.7. The $N = 5, 6$ examples were chosen from 100 produced for each knowledge graph type. For $N = 3, 4$, the number of examples produced during research exceeds that.

[10] Note that requiring purity in SDP 6.2 is a quadratic constraint on the minimization variable γ. One way to see this is through the determinant of the CM: $\mu(\rho) = \mathrm{Tr}[\rho^2] = (\mathrm{Det}(\gamma))^{-1/2} = 1$ [26, p.61]. It is linear in each column separately but not the whole matrix. Constraints in SDPs have to be affine - convex (linear) combinations - in the optimization variable [149, 163].

[11] This follows from work by an undergraduate student, Adam Johnston, who I co-supervised. His project over a summer involved extending the existing code into the general case (more than four modes). The results presented here are my own working using the generalised code.

Table 6.7: Best examples found for $N \leq 6$ modes. Algorithm 1 was run for 10 iterations using the extra constraints on the CM element size and minimal eigenvalue. The witness knowledge graphs are given as described in sections 5.7 and 6.2. Qubit results taken from ref. [141]. The witness mean for the 3-mode qubit example from ref. [153] is given in ref. [154].

N	Index	Configuration	$\mathrm{Tr}[\gamma W] - 1$	$\mathrm{Tr}[\rho \mathcal{W}]$
3	3*a*		$-1.47 \cdot 10^{-1}$	$-1.98 \cdot 10^{-2}$
4	4*a*		$-7.53 \cdot 10^{-2}$	$-3.15 \cdot 10^{-3}$
	4*b*		$-7.35 \cdot 10^{-2}$	$-3.56 \cdot 10^{-3}$
5	5*a*		$-4.38 \cdot 10^{-2}$	$-1.13 \cdot 10^{-3}$
	5*b*		$-4.14 \cdot 10^{-2}$	$-1.31 \cdot 10^{-3}$
	5*c*		$-5.17 \cdot 10^{-2}$	$-1.38 \cdot 10^{-3}$
6	6*a*		$-2.58 \cdot 10^{-2}$	$-2.01 \cdot 10^{-4}$
	6*b*		$-2.82 \cdot 10^{-2}$	$-2.56 \cdot 10^{-4}$
	6*c*		$-2.58 \cdot 10^{-2}$	$-2.84 \cdot 10^{-4}$
	6*d*		$-2.36 \cdot 10^{-2}$	$-2.92 \cdot 10^{-4}$
	6*e*		$-3.25 \cdot 10^{-2}$	$-3.80 \cdot 10^{-4}$
	6*f*		$-3.56 \cdot 10^{-2}$	$-4.54 \cdot 10^{-4}$

We should note that, in obtaining the examples of five and six modes, we did not check that the CMs and witnesses preserve the effects when the entries are rounded off. This means that the difference between the three- and four-mode cases compared to the five and six could be lessened as the latter were found with fewer constraints. Nonetheless, we see a decrease in the best examples found as the number of modes increases. At the same time, there does not seem to be a clear difference between witness knowledge graphs. A statistical investigation might shed some more light on this last point.

We may compare the results obtained here to the qubit scenario [141], restated the last column of table 6.7. It is worth repeating that directly comparing the numbers is not necessarily fruitful given the different interpretations of $\mathrm{Tr}\left[\rho W_\rho\right]$ and $\mathrm{Tr}[\gamma W] - 1$. However, we may see differences in how the values change within each scenario as we increase the number of parties. While the qubit scenario decreases almost by an order of magnitude, the decrease in the Gaussian scenario is closer to a factor of 2 as we increase the number of modes. This means that the effect could be preserved for larger states and therefore more suitable for use in realistic quantum informational protocols. Next is a statement about computational resources. In the qubit scenario it was noted that obtaining the examples took < 1 minute, 45 minutes and about 6hrs for the four, five and six modes respectively[12]. Meanwhile, even for the six mode Gaussian examples run with 10 iterations and all the additional requirements mentioned in section 6.4.1, suitable examples were found in just over a minute on average[13]. One possible explanation for the difference in runtime

[12] Obtained through private communication by collaborator L. Mišta.

[13] From results obtained by a member of the collaboration, finding 10 mode-examples with the desired criteria took around 20 minutes ($n = 10$). However, the runtime showed high variability: even at eight modes, the program

between the qubit and Gaussian scenarios is that the solution space of qubits increases with the number of qubits, N, as 2^N while CMs scale as $(2N)^2$ – allowing a more efficient search.

6.5 Experimental scheme

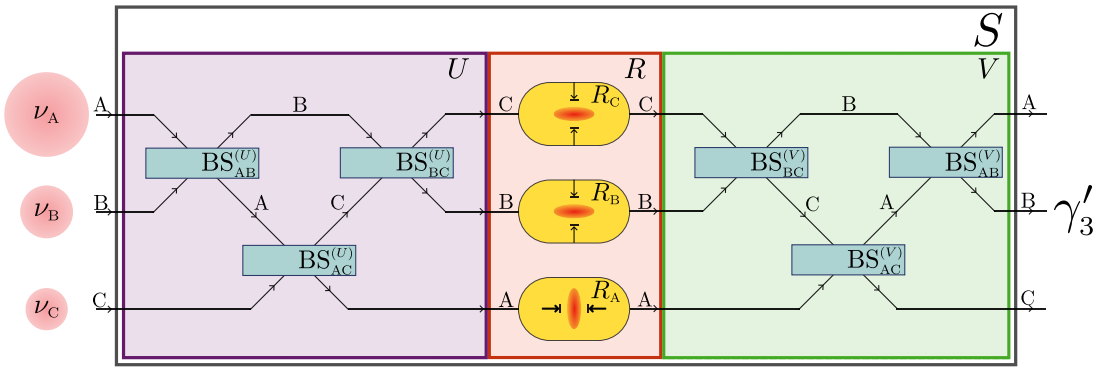


Figure 6.3: Decomposition of symplectic transformation S generating a Gaussian state with CM $\gamma = \gamma^{(3)}$ of three modes A, B and C: ν_j – thermal states with mean number of thermal photons $(\nu_j - 1)/2$, $j = A, B, C$ with ν_j the symplectic value of mode j (red circles); U – passive transformation consisting of beam splitters $\mathrm{B}^{(U)}_{jk}$, $jk = AB, AC, BC$ (magenta block); V – passive transformation consisting of beam splitters $\mathrm{B}^{(V)}_{jk}$ (green block); R – squeezing transformation consisting of one squeezer in position quadrature, R_A, and two squeezers in momentum quadrature, R_B and R_C (pink block). For rounded parameters as in tables 6.8 and 6.9 the circuit produces the CM $\gamma'^{(3)}$, which closely approximates the CM γ, and retains its entanglement properties. See text for details.

Since the three mode example, $\gamma^{(3)}$, shows most promise for experimental realisation, we will now show a scheme of linear-optical elements to produce a state with that CM. The first iteration of the scheme is presented in fig. 6.3. For notational simplicity, we redefine $\gamma = \gamma^{(3)}$ for the rest of the chapter. We will use the machinery of the Symplectic formalism introduced in section 5.2. The basic idea is that, due to the structure of CMs, one may find matrices describing beam-splitters and squeezers that output the CM, given some thermal states as inputs.

The process utilises Thm. 5.1 (Williamson's Theorem) to obtain the symplectic transformation on a set of thermal inputs; then follows the Bloch-Messiah decomposition of symplectic matrix into beam-splitters and phase-shifters, Thms. 5.2 and 5.3. The latter is used to separate a beam-splitter array into individual components.

We begin by invoking Williamson's Theorem on the covariance matrix $\gamma^{(3)}$: there is a symplectic transformation $\mathcal{S}$ such that

$$\mathcal{S}\gamma\mathcal{S}^T = \bigoplus_{i=1}^{N} \nu_i \mathbb{1}_2 = W, \tag{6.11}$$

could run for three hours without finding a suitable example.

where the entries in W are the symplectic eigenvalues, $\nu_1, \nu_2, ..., \nu_N$, of γ. These can be found from the covariance matrix by equating them to the positive eigenvalues of $i\Omega\gamma$ and can be found in table 6.8. The symplectic transformation may be found numerically using the methods presented in references [164, 165].

Defining $S := \mathcal{S}^{-1}$, we can rewrite the above equation as $\gamma = SWS^T$. We can then invoke the Bloch-Messiah decomposition (Thm. 5.2) and find passive transformations $U, V \in \mathrm{SO}(2N) \cap \mathrm{Sp}(2N, \mathbb{R})$ and active [14] transformation R to write

$$S = VRU. \tag{6.12}$$

The active transformation (squeezing) is represented by a diagonal matrix, R, defined by

$$R = R_A(s_A) \oplus R_B(s_B^{-1}) \oplus R_C(s_C^{-1}), \tag{6.13}$$

where $R_i(s_j) = \mathrm{diag}(s_j, s_j^{-1}), j = A, B, C$. The squeezing parameters, s_j, are given in table 6.8.

Table 6.8: Symplectic eigenvalues ν_j and the squeezing parameters s_j.

j	A	B	C
ν_j	6.835	1.012	1.004
s_j	0.396	0.851	0.478

The next step is to separate the passive transformations U and V into an array of beam-splitters and phase-shifters. Here is where looking for examples with no $x-p$ correlations comes in handy - it means that phase shifters are not required for producing states with covariance matrix $\gamma^{(3)}$. One may see this by noting that the beam-splitter matrices define correlations that do not mix position and momentum (see eq. (5.53)). The decomposition of U and V is possible due to Thm. 5.3 (Euler decomposition of beam-splitters on three modes) and can be performed numerically using the methods used in Refs. [128, 129]. We write the decomposition of the beam-splitter arrays into two-mode mixing as

$$\begin{aligned} U &= B^{(U)}_{BC}(T_{BC})B^{(U)}_{AC}(T_{AC})B^{(U)}_{AB}(T_{AB}), \\ V &= B^{(V)}_{AB}(\tau_{AB})B^{(V)}_{AC}(\tau_{AC})B^{(V)}_{BC}(\tau_{BC}), \end{aligned} \tag{6.14}$$

where the elements $B^{(M)}(T_{jk}), M = U, V, jk = AB, AC, BC$ of the decomposition are extended in the correct mode for the product to be defined. For more details see Thm. 5.3. The transmissivities T_{jk} can be found in table 6.9.

Table 6.9: Amplitude transmissivities T_{jk} and τ_{jk}.

jk	AB	AC	BC
T_{jk}	0.555	0.947	0.492
τ_{jk}	0.716	0.904	0.657

The decomposition presented is numerical and thus the parameters in tables 6.8 and 6.9, which have been rounded to three decimal places, differ from the true values. The resulting CM, $\gamma'^{(3)}$, is therefore not the same as the original γ. Nonetheless, we find that $\gamma'^{(3)}$ retains all relevant entanglement properties by checking that the marginals are separable and that there is a witness that detects GME by finding an Optimal GME witness (partially blind) (through SDP 6.1). Letting $W'^{(3)}$ denote the optimal witness of $\gamma'^{(3)}$, genuine multipartite entanglement

Table 6.10: Minimal eigenvalue $\varepsilon'_{jk} \equiv \min\{\mathrm{eig}[\gamma'^{(T_j)}_{jk} + i\Omega_2]\}$.

jk	AB	AC	BC
ε_{jk}	0.005	0.852	0.010

is still present as $\mathrm{Tr}[\gamma'^{(3)}W'^{(3)}] - 1 = -0.138$. The marginals are also still separable, as can be seen in table 6.10.

The CM $\gamma'^{(3)}$ and its optimal witness are given by

$$\gamma'^{(3)} = \begin{pmatrix} 1.34 & 0 & -0.35 & 0 & -0.82 & 0 \\ 0 & 10.01 & 0 & 8.45 & 0 & 1.86 \\ -0.35 & 0 & 7.78 & 0 & -8.03 & 0 \\ 0 & 8.45 & 0 & 7.92 & 0 & 2.08 \\ -0.82 & 0 & -8.03 & 0 & 9.99 & 0 \\ 0 & 1.86 & 0 & 2.08 & 0 & 1.62 \end{pmatrix}, \tag{6.15}$$

and

$$W'^{(3)} = 10^{-2}\begin{pmatrix} 6.856 & 0 & -0.453 & 0 & 0 & 0 \\ 0 & 34.115 & 0 & -39.307 & 0 & 0 \\ -0.453 & 0 & 25.035 & 0 & 20.874 & 0 \\ 0 & -39.307 & 0 & 45.925 & 0 & -2.051 \\ 0 & 0 & 20.874 & 0 & 17.426 & 0 \\ 0 & 0 & 0 & -2.051 & 0 & 6.622 \end{pmatrix}, \tag{6.16}$$

respectively.

Equivalent circuits are not always equal in the context of experiment. For example, in the scheme presented in this section, squeezing is required after the first beam-splitter array. However, it is oftentimes desirable to perform squeezing prior to their use in experiments. Then, only successfully squeezed states need to be mixed. Further, eliminating some components might produce similar - enough - states but may simplify the experiment considerably. We therefore present a "simpler" circuit in the coming section - or at least one that is more suitable for certain experimental set-ups.

6.5.1 Lab-friendly circuit

The scheme presented in the section 6.5 allows for two simplifications to the design. First, one may see that the input states of modes B and C can be approximated by vaccua by replacing ν_B and ν_C with unity in table 6.8. Second, the squeezing operation may be shifted to the beginning of the circuit by noticing that the output of the first beam-splitter array in fig. 6.3 is a classically correlated state and entanglement is not produced until after mixing of squeezed states. In fact, one may produce the same output as after the squeezing operation by swapping the squeezing and beam-splitters U. Rather than mixing after the squeezing operation, the squeezed states may be displaced in a correlated manner such that the input into beam-splitter array V is the same for either method.

Setting the first simplification ($\nu_B = \nu_C = 1$), the two circuits can be shown to be equivalent, which we prove in appendix H. A less formal argument is that the thermal input into mode

[14] See footnote 9 for discussion on the terms "active" and "passive".

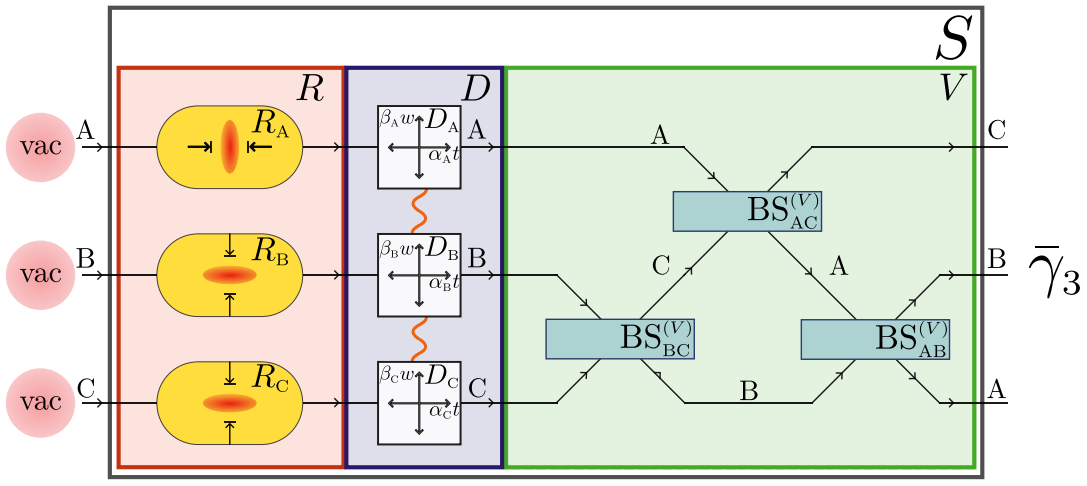


Figure 6.4: Scheme for preparation of a Gaussian state with CM $\bar{\gamma}^{(3)}$ carrying genuine multipartite entanglement verifiable from nearest-neighbour separable marginals. The input comprises three vacuum states (red circles). The squeezing transformation R (red box) and the transformation V (green box) are the same as in fig. 6.3. The block D (blue box) contains correlated displacements D_A, D_B and D_C (white squares) given in eq. (6.17), where the parameters α_j and β_j are in table 6.11 and the uncorrelated Gaussian variables t and w are such that $\langle t^2\rangle = \langle w^2\rangle = (\nu_A - 1)/2$. See text for more details.

A can be replaced by a vacuum state acted upon with the displacements [15] $x_A^{(0)} \to x_A^0 + t$ and $p_A^0 \to p_A^0 + w$, where $x_A^{(0)}(p_A^{(0)})$ is the position (momentum) quadrature and t and w are uncorrelated classical Gaussian random variable with zero mean and second moments given by $\langle t^2\rangle = \langle w^2\rangle = (\nu_A - 1)/2$. Due to the linearity of U and R at the level of quadrature operators, we can move the displacements after the squeezing R. The quadratures are displaced as

$$x_i \to x_i + \alpha_i t, \quad p_i \to p_i + \beta_i w, \tag{6.17}$$

with $i = A, B, C$. Let now $D = (\alpha_1 t, \beta_1 w, \alpha_2 t, \beta_2 w, \alpha_3 t, \beta_3 w)$ describe the correlated displacement. The parameters α_i and β_i are given (rounded to 1 d.p.) in table 6.11. Weighted by α_i and β_i, the variables t and w allow for the correlations due to mixing U and initial noise in mode A to be accounted for in the alternative scheme.

We analyse the states produced using the beam-splitter transmissivities and squeezing parameters from the second rows of table 6.12 along with the displacement parameters in table 6.11 running through the circuit in fig. 6.4. The CM of a state which has GME that can be detected

[15] Whereas we are not interested in a shift of the state in phase-space (we are not interested in first moments), an increase in noise due to the correlated variables t and w is induced in the state. While the displacement we talk about here of one mode would not by itself produce a change in the second moment, a correlated displacement across a number of modes would appear in the covariance matrix. It is this fact which we use to claim the equivalence of the circuits.

Table 6.11: Parameters α_j and β_j of displacements from eq. (6.17).

j	A	B	C
α_j	0.2	- 0.7	1.3
β_j	1.3	- 0.5	0.3

Table 6.12: Repetition of tables 6.8 and 6.9

Amplitude transmissivities.

jk	AB	AC	BC
T_{jk}	0.555	0.947	0.492
τ_{jk}	0.716	0.904	0.657

Symplectic eigenvalues and squeezing parameters.

j	A	B	C
ν_j	6.835	1.012	1.004
s_j	0.396	0.851	0.478

from a set of separable two-body marginals, produced by the circuit in fig. 6.4, is

$$\bar{\gamma}^{(3)} = \begin{pmatrix} 1.39 & 0 & -0.21 & 0 & -1.05 & 0 \\ 0 & 9.95 & 0 & 8.26 & 0 & 1.7 \\ -0.21 & 0 & 7.36 & 0 & -7.83 & 0 \\ 0 & 8.26 & 0 & 7.63 & 0 & 1.94 \\ -1.05 & 0 & -7.83 & 0 & 10.12 & 0 \\ 0 & 1.7 & 0 & 1.94 & 0 & 1.59 \end{pmatrix}. \tag{6.18}$$

Note that $\bar{\gamma}^{(3)} \neq \gamma^{(3)}$ since the experimental parameters have been rounded for a simpler production. The optimal witness, giving $\mathrm{Tr}[\bar{\gamma}^{(3)}\bar{W}^{(3)}] - 1 = -0.139$, has the following numerical form:

$$\bar{W}^{(3)} = 10^{-2} \begin{pmatrix} 5.867 & 0 & -0.543 & 0 & 0 & 0 \\ 0 & 33.707 & 0 & -39.602 & 0 & 0 \\ -0.543 & 0 & 26.222 & 0 & 21.009 & 0 \\ 0 & -39.602 & 0 & 47.097 & 0 & -1.872 \\ 0 & 0 & 21.009 & 0 & 16.865 & 0 \\ 0 & 0 & 0 & -1.872 & 0 & 6.167 \end{pmatrix}. \tag{6.19}$$

The CM has its marginals separable as evidenced in table 6.13.

Table 6.13: Minimal eigenvalue $\bar{\varepsilon}_{jk} \equiv \min\{\mathrm{eig}[(\bar{\gamma}^{(3)})^{(T_j)} + i\Omega_2]\}$.

jk	AB	AC	BC
$\bar{\varepsilon}_{jk}$	0.027	0.862	0.037

6.6 Chapter summary and discussion

We saw in this chapter a method to find covariance matrices of genuinely multipartite entangled states with separable two-body marginals along with GME witnesses that act on the smallest set of correlations required. This was done using an algorithm that finds the optimal covariance matrix and witness iteratively and was seeded with random Gaussian covariance matrices. We presented the best numerical results found for all three- and four-mode examples that preserve the effects when applying rounding. The three-mode example showed an effect strength of

$\mathrm{Tr}\left[\gamma^{(3)}W^{(3)}\right] - 1 = -0.143$ with the four-mode examples giving about half of that. The results presented herein complement the work on multi-qubit systems that have the same properties [141, 152, 153] where the best result presented in qubit systems is $\mathrm{Tr}[\rho W] = -6.58 \cdot 10^{-3}$ [141]. We note, however, that a comparison with the Gaussian result should be done carefully since the values have different meanings in the space of density matrices and covariance matrices. For example, a covariance matrix may be fully described by its marginals while this does not hold for density matrices (for example an entangled state looks like two thermal states locally) so that the partial blindness criterion on witnesses at the two levels cannot necessarily be mapped to each other in a simple manner. One way of understanding this difference is that composition of states – through tensor products – at the CM level corresponds to direct sums. Marginals of correlated (including entangled) CMs include the off-diagonal blocks so the addition of all marginals, barring double-counting, returns the whole CM.

One point of difference between the results is the tolerance to white noise. The results presented here for the Gaussian scenario tolerated the addition of 10% white noise – compared to the qubit result which tolerated half of that. A question that leads from this is: what is the effect of other types of noise? For example correlated noise, or the effect of noise and errors in the circuit elements which produce the CM. The former is an open question. Meanwhile, the latter was recently investigated by in a master's thesis[16]. The results pointed to an asymmetric susceptibility to noise of the components. For example, the squeezer on mode A showed less resilience to the other squeezers. It would be interesting to see if this is a feature of other states produced using algorithm 1.

We note here that the covariance matrices presented in section 6.4 all have values that saturate the upper bound on the condition of entries being contained in $[1, 10]$. In fact, before the addition of this requirement, we found that CMs with low[17] optimal witness means had large entries which were several orders of magnitude difference between the largest and smallest entries. It would be interesting to find out whether this is a feature of states carrying the investigated properties or whether the effect is due to the construction of the SDPs in algorithm 1. If it the conclusion is that it is a structural feature of the states, that would be a useful step in characterising CMs which posses GME detected by witnesses on separable marginals.

Further, two optical circuits that prepare a quantum state with the required properties were derived for the three-mode example presented ($\gamma^{(3)}, W^{(3)}$). The first scheme made use of Thm. 5.1 (Williamson's Theorem), Thm. 5.2 (Bloch-Messiah decomposition), and Thm. 5.3 (Euler decomposition of beam-splitters on three modes) to produce a circuit involving a squeezing transformation sandwiched between two beam-splitter arrays with thermal inputs in three modes, given in fig. 6.3. It can be preferable to perform squeezing on pure states at the beginning so we offered two simplifications: two of the thermal state inputs could be vacua whence the squeezing transformation could be moved to the beginning and the classical correlations replaced by a correlated displacement. We presented therefore the alternative circuit along with the CM produced by it and its optimal witness. Although not used here, some CM-witness pairs found during research allowed further simplifications. Examples of these include removing some beam splitters and decreasing squeezing required.

The work presented here adds a further piece in the puzzle of the quantum marginal problem. In the scenario of Gaussian GME at the level of second moments, we showcased a method that will find such states using a limited set of measurements.

Looking forward, one may perform a similar analysis to the one presented here with a particular experimental set-up in mind. As was noted in the work on optimal entanglement witnesses on covariance matrices [123], one may include further constraints on the scheme for finding the opti-

[16] Kenny Campbell performed the analysis under my co-supervision.
[17] Values were in the order of the $\gamma^{(3)}$ example, $\mathrm{Tr}[\gamma W] = O(-1)$.

mal witness (SDP 6.1). In conversation with an experimental group, one may find requirements on apparatus or measurements that correspond to linear constraints on the witness. Another approach may be to start with a decomposition of a covariance matrix and see how the state behaves under some alterations to the circuit as done in section 6.5.1 (Lab-friendly circuit). At the time of writing, this is being investigated by co-authors to the work presented here [166]. Another step towards the experimental preparation of such states is to perform a loss and error analysis of the optical schemes[18]. In a more theoretical path, the test could be investigated in the hybrid scenario, where continuous and discrete variable quantum systems are entangled. This would involve devising a scheme for finding optimal witnesses of hybrid entanglement. For work on hybrid entanglement and their analytical witness see refs. [167, 168].

Another question that appears naturally every time an exotic state is presented is: what is it useful for? One possible avenue for investigation is on their use for validation of resource states in quantum information protocols. Performing full tomography of states is costly so finding subsets of measurements would be advantageous - even using evidence from parts of a large state could be useful. States that posses GME which can be determined from a smaller set of measurements could find use in informational tasks. An example from quantum computing may be obtained in measurement-based quantum computing in which the main resource are states called cluster states. One could perhaps use some part of a cluster state [63] to provide evidence of the particular multipartite entanglement required. [19]

Concentrating more narrowly on the project at hand, there are some open questions that can be addressed. For example, will any seed Gaussian input into algorithm 1 produce an example of a state with the desired properties, given sufficiently large number of iterations, n? As far as running the numerical program, there seems to be a diminishing improvement as n increases – see appendix F. In many cases when the optimizer presented no valid solution, error messages noting the infeasibility of the problem were displayed. One possible reason for this breaking is that the scheme finds CMs that lie in a shrinking vicinity of the solution to each subsequent iteration. The number of relevant decimal digits increases until the machine precision is exceeded. A typical question that arises in numerical projects is how the research question may me tackled using analytical methods. For this, methods for finding CM witnesses analytically would need to be devised. Further, there is a drop in the best examples found for increasing number of modes as seen in table 6.7. The requirements of having GME and separable marginals put opposing constrains on the CM so that, intuitively, one might expect the GME detected to decrease as the number of states that we require to be separable increases. Furthermore, the proportion marginals ignored increases with number of modes, which limit further the states which partially blind GME witnesses detect. A related question is about the difference between knowledge graphs which becomes more varied as the number of modes increases. For example, it seems that graphs with well-connected nodes give a stronger effect in both the continuous and discrete variable scenarios (see table 6.7). Perhaps more highly-connected graphs allow for detecting of states with stronger GME. The code produced for this work has now been extended in an undergraduate student project (see footnote 11) to an arbitrary number of modes which paves the way to tackle these questions.

All examples presented here are produced by numerical means. This makes a classification of states that exhibit the properties into small parameter families difficult. To gain more insight into how the properties investigated appear in states it would be useful to have such a classification. Work done by collaborators, following the project presented herein, is taking steps towards this

[18] For figs. 6.3 and 6.4, this is the topic of a master's project I am co-supervising at the time of writing.

[19] Perhaps the results of measurements used to define the circuit could be compiled to extract information about the success of producing the CV cluster state used. The complementary vertices of the computational circuit would be used to form witnesses to test the entanglement properties.

by finding simple schemes with a low number of parameters related to optical circuit elements [166]. A route via SDPs could be by using the dual programs to classify the parameter space for circuits producing CMs. Perhaps ref. [169] can serve as an inspiration.

Another question related to GME witnesses on covariance matrices - and possibly optimal GME witnesses more generally - is whether they can be used to define a measure of entanglement. Throughout the chapter I use the declaration that a larger (more negative) value for $\mathrm{Tr}[\gamma W] - 1$ implied a stronger ("better") effect. The intuition lies in that the "optimal" nature of the witness found gives a value related to the state itself and not only to a particular combination of measurements. It would, however, be interesting to make a formal proof of this statement. Perhaps some methods from semi-definite programming would be needed to show that optimal witnesses satisfy the criterion for being a measure - possibly using the limiting sequences of SDP 5.3 (Primal program for optimal GME witness). For the role of limiting sequences see ref. [148]. As a start, the bipartite dual SDP is shown to be connected to the p-measure [123]. A similar result would be useful for GME.

Part III

Appendices

APPENDIX A

Distributions, integrals and other results

A.1 The delta functions

Dirac delta function:

Definition A.1 (Dirac Delta Function)**.** The Dirac delta function[1] had the defining property that, for some function $f(x)$, $\int \mathrm{d}x f(x)\delta(x-a) = f(a)$. It has the form

$$\delta(x-y) = \frac{1}{2\pi}\int \mathrm{d}\alpha \exp(i(x-y)\alpha). \tag{A.1}$$

Kronecker delta function:

$$\delta_{ab} = \begin{cases} 1, & \text{if } a = b, \\ 0, & \text{if } a \neq b. \end{cases} \tag{A.2}$$

A.2 Fourier transform

For a function $f(x)$ where x is the position eigenvalues, the Fourier transform onto momentum space is given by

$$\mathcal{F}[f(x)](p) = \frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}} \mathrm{d}x f(x) e^{-ixp} \tag{A.3}$$

We define the function in momentum space as

$$\bar{f}(p) := \mathcal{F}[f(x)](p). \tag{A.4}$$

One may return to the position space by the *inverse Fourier transform*

$$f(x) = \mathcal{F}[f(x)](p) = \frac{1}{\sqrt{2\pi}}\int_{\mathbb{R}} \mathrm{d}p \bar{f}(p) e^{ixp}. \tag{A.5}$$

A.3 Useful mathematical formulae

A.3.1 Baker-Haussdorf formula

Theorem A.1 (Baker-Cambpell-Haussdorf-Dynkin (BCHD) formula)**.** *For, possibly non-commuting, operators $\hat{A}, \hat{B}$, we have the equation [170, 171]*

$$e^{\hat{A}} e^{\hat{B}} = e^{\hat{C}}, \tag{A.6}$$

with

$$\hat{C} = \hat{A} + \hat{B} + \frac{1}{2}[\hat{A}, \hat{B}] + \frac{1}{12}[\hat{A}, [\hat{A}, \hat{B}]] - \frac{1}{12}[\hat{B}, [\hat{A}, \hat{B}]] + \dots . \tag{A.7}$$

[1] Despite its name, the Dirac delta function is not technically a function. Rather, it is a distribution (or generalised function).

Two common scenarios we deal with in this thesis is when $\hat{A}$ and $\hat{B}$ commute and when they commute with their commutator (for example, position and momentum have $[\hat{x}, \hat{p}] = i$). In these cases, the BCH formula collapses to

$$\begin{aligned} e^{\hat{A}}e^{\hat{B}} &= e^{\hat{A}+\hat{B}}, && \text{when } [\hat{A}, \hat{B}] = 0, \\ e^{\hat{A}}e^{\hat{B}} &= e^{\hat{A}+\hat{B}+\frac{1}{2}[\hat{A},\hat{B}]}, && \text{when } [\hat{A}, [\hat{A}, \hat{B}]] = [\hat{B}, [\hat{A}, \hat{B}]] = 0. \end{aligned} \tag{A.8}$$

A.3.2 Gaussian integrals

Gaussian integral with an imaginary linear term [172, 173]:

$$\int_{\mathbb{R}} \exp\left(-\frac{x^2}{2a} - ixy\right)\mathrm{d}x = \sqrt{2\pi a}\exp\left(-\frac{a}{2}y^2\right), \quad a, y \in \mathbb{R},\ a > 0 \tag{A.9}$$

$$\int_{\mathbb{R}} \exp\left(-\frac{x^2}{a}\right)\mathrm{d}x = \sqrt{\pi a}, \quad a \in \mathbb{R},\ a > 0 \tag{A.10}$$

A.3.2.1 Gaussian states in the position and momentum bases

A Gaussian state may be written in the position quadrature eigenbasis as

$$|\mu, \sigma, c\rangle = \int_{\mathbb{R}} \mathrm{d}x g_{\mu,\sigma,c}(x)\,|x\rangle_x\,, \tag{A.11}$$

a superposition of position eigenstates weighted by the normalised Gaussian distribution $g_{\mu,\sigma}(x)$ centred at μ with variance σ. The global phase, c, corresponds to the mean in momentum space, as we will see below. The form of the coefficients is

$$g_{\mu,\sigma,c}(x) := \sqrt{N}\exp\left(-\frac{(x-\mu)^2}{4\sigma^2}\right)\exp(ixc), \tag{A.12}$$

with $N = \frac{1}{\sqrt{2\pi\sigma^2}}$.

The form of the state in the momentum quadrature eigenbasis may be obtained via a Fourier transform or, alternatively, by pre-multiplying the identity resolved in the momentum eigenbasis

$$\begin{aligned} |\mu, \sigma, c\rangle &= \int_{\mathbb{R}} \mathrm{d}p\,|p\rangle\langle p|\,|\mu, \sigma, c\rangle \\ &= \int_{\mathbb{R}} \mathrm{d}p\,|p\rangle\langle p| \int_{\mathbb{R}} \mathrm{d}x g_{\mu,\sigma,c}(x)\,|x\rangle_x \\ &= \int_{\mathbb{R}}\int_{\mathbb{R}} \mathrm{d}p\mathrm{d}x g_{\mu,\sigma,c}(x)\,\langle p|x\rangle\,|p\rangle_p \\ &= \int_{\mathbb{R}}\int_{\mathbb{R}} \mathrm{d}p\mathrm{d}x g_{\mu,\sigma,c}(x)\frac{1}{\sqrt{2\pi}}e^{-ixp}\,|p\rangle_p \\ &= \sqrt{\frac{N}{2\pi}}\int_{\mathbb{R}}\int_{\mathbb{R}} \mathrm{d}p\mathrm{d}x \exp\left(-\frac{(x-\mu)^2}{4\sigma^2}\right)e^{-ix(p-c)}\,|p\rangle_p \\ &= \sqrt{\frac{N}{2\pi}}\int_{\mathbb{R}}\int_{\mathbb{R}} \mathrm{d}p\mathrm{d}x \exp\left(-\frac{(x-\mu)^2}{4\sigma^2} - ix(p-c)\right)|p\rangle_p \\ &= \sqrt{\frac{N}{2\pi}}\int_{\mathbb{R}} \mathrm{d}p\,|p\rangle_p \int_{\mathbb{R}} \mathrm{d}x \exp\left(-\frac{(x-\mu)^2}{4\sigma^2} - ix(p-c)\right) \end{aligned}$$

We can evaluate the integral over x by using the Gaussian integral result from eq. (A.9), $\int_{\mathbb{R}} \exp\left(-\frac{x^2}{2a} - ixy\right)\mathrm{d}x = \sqrt{2\pi a}\exp\left(-\frac{a}{2}y^2\right)$, identifying $a = 2\sigma^2$, $y = (p - c)$ and making the change of variable $x' \mapsto x - \mu$ ($\mathrm{d}x' = \mathrm{d}x$), we obtain

$$|\mu, \sigma, c\rangle = \sqrt{\frac{N}{2\pi}} \int_{\mathbb{R}} \mathrm{d}p\, |p\rangle_p \int_{\mathbb{R}} \mathrm{d}x \exp\left(-\frac{x^2}{4\sigma^2} - i(x+\mu)(p-c)\right) \tag{A.13}$$

$$= \left(2\pi\sigma^2\right)^{\frac{1}{4}} \int_{\mathbb{R}} \mathrm{d}p \exp\left(-\sigma^2 y^2\right) \exp(iy\mu)\, |y + c\rangle_p\,, \tag{A.14}$$

$$= \frac{e^{ic\mu}}{\sqrt{N}} \int_{\mathbb{R}} \mathrm{d}p \exp\left(-\sigma^2 (p-c)^2\right) \exp(ip\mu)\, |p\rangle_p\,, \tag{A.15}$$

a Gaussian with width $\frac{1}{\sigma}$ centred at c. The global phase, $e^{ic\mu}$, does not involve any variable so will not affect the statistics of the state.

APPENDIX B

Derivation of the gates for hybrid ACQC with the linear Hamiltonian

We derive the gates presented in section 3.2.0.2.

B.1 One qubit gate

$$\begin{aligned} J(2\theta t) &= He^{i\theta t\hat{\sigma}_z} \\ &= He^{-i\hat{p}t}e^{-i\hat{\sigma}_z\hat{x}\theta}e^{i\hat{p}t}e^{i\hat{\sigma}_z\hat{x}\theta} \\ &= e^{-i\hat{p}t}\cdot F^2He^{i\theta\hat{\sigma}_z\hat{x}}F^2\cdot e^{i\hat{p}t}\cdot H^2e^{i\theta\hat{\sigma}_z\hat{x}} \\ &= e^{-i\hat{p}t}\cdot F^2E^{AR}F^2\cdot e^{i\hat{p}t}\cdot HE_{AR} \\ &= e^{-i\hat{p}t}\cdot F^2E^{AR}F^2\cdot e^{i\hat{p}t}\cdot E_{A_0R}E_{AR}. \end{aligned}$$

So that single qubit gates may be enacted entirely through ancilla-register interactions and manipulation of the ancilla - in an entirely unitary fashion:

$$J(\beta) = e^{-i\hat{p}\frac{\beta}{2\theta}}\cdot F^2E^{AR}F^2\cdot e^{i\hat{p}\frac{\beta}{2\theta}}\cdot E_{A_0R}E_{AR}. \tag{B.1}$$

B.2 Two-qubit gate

Similarily, the two qubit gate may be implemented by the procedure

$$\begin{aligned} H^{(1)}\otimes H^{(2)}C_z(\theta) &= H^{(1)}\otimes H^{(2)}e^{i\frac{\theta^2}{2}\sigma_z^{(1)}\sigma_z^{(2)}} \\ &= H^{(1)}\otimes H^{(2)}e^{i\theta\hat{\sigma}_z^{(2)}\hat{p}}\cdot e^{i\theta\hat{\sigma}_z^{(1)}\hat{x}}\cdot e^{-i\theta\hat{\sigma}_z^{(2)}\hat{p}}\cdot e^{-i\theta\hat{\sigma}_z^{(1)}\hat{x}} \\ &= FH^{(2)}e^{i\theta\hat{\sigma}_z^{(2)}\hat{x}}F^\dagger\cdot H^{(1)}e^{i\theta\hat{\sigma}_z^{(1)}\hat{x}}\cdot F^\dagger(H^{(2)})^2e^{i\theta\hat{\sigma}_z^{(2)}\hat{x}}F\cdot F^2(H^{(1)})^2e^{i\theta\hat{\sigma}_z^{(1)}\hat{x}}F^2 \\ &= FE_{AR^{(2)}}F^\dagger\cdot E_{AR^{(1)}}\cdot F^\dagger(H^{(2)})E_{AR^{(2)}}F\cdot F^2(H^{(1)})E_{AR^{(1)}}F^2 \\ &= FE_{AR^{(2)}}F^\dagger\cdot E_{AR^{(1)}}\cdot F^\dagger E_{A_0R^{(2)}}E_{AR^{(2)}}F\cdot F^2E_{A_0R^{(1)}}E_{AR^{(1)}}F^2. \end{aligned}$$

Once again, using only unitary ancilla-register interactions and ancilla manipulations, we find that an entangling gate on two register qubits may be enacted:

$$H^{(1)}\otimes H^{(2)}C_z(\theta) = FE_{AR^{(2)}}F^\dagger\cdot E_{AR^{(1)}}\cdot F^\dagger E_{A_0R^{(2)}}E_{AR^{(2)}}F\cdot F^2E_{A_0R^{(1)}}E_{AR^{(1)}}F^2. \tag{B.2}$$

APPENDIX C

Derivations of gates for the ADQC models presented in chapter 4

C.1 Continuous variable ADQC

The register states are arbitrary CV states,

$$|\psi\rangle = \int_{\mathbb{R}} \mathrm{d}x \psi(x) |x\rangle \in \mathcal{H}_R, \tag{C.1}$$

for a complex function ψ. The ancillas are initialised in the conjugate basis,

$$|A\rangle := |0\rangle_{\hat{p}} \in \mathcal{H}_A. \tag{C.2}$$

The ancilla-register interaction is

$$E_{AR} := \hat{F}_A^\dagger \hat{F}_R \exp\{i\hat{x}_A \hat{x}_R\} = \hat{F}_A^\dagger \hat{F}_R CZ_{AR}. \tag{C.3}$$

C.1.1 Single qumode gate

We have the single-mode operations:

$$\hat{U}_{\mathrm{k},\hat{q}_j}(\theta) = \exp\left(i\frac{\theta}{k}\hat{q}_R^k\right), \tag{C.4}$$

for $k = 1, 2, 3$, and $\hat{q} = \hat{x}, \hat{p}$ in spaces $j = A, R$.

$$\begin{aligned}
{}_p\langle m|\hat{U}_{\mathrm{k},\hat{x}_A}(\theta)\hat{E}_{AR}|0\rangle_p &= {}_p\langle m|\hat{U}_{\mathrm{k},\hat{x}_A}(\theta)\hat{F}_A^\dagger \hat{F}_R e^{i\hat{x}_A\hat{x}_R}|0\rangle_p \\
&= \hat{F}_R\, {}_p\langle m|\hat{U}_{\mathrm{k},\hat{x}_A}(\theta)\hat{F}_A^\dagger e^{i\hat{x}_A\hat{x}_R}|0\rangle_p \\
&= \hat{F}_R \int \mathrm{d}x\, {}_p\langle m|\hat{U}_{\mathrm{k,x}}(\theta)|x\rangle\langle x|_x \hat{F}_A^\dagger \int \mathrm{d}y e^{iy\hat{x}_R}|y\rangle\langle y|_x|0\rangle_p \\
&= \hat{F}_R \iint \mathrm{d}x\,\mathrm{d}y\, \hat{U}_{\mathrm{k,x}}(\theta)e^{iy\hat{x}_R}\, {}_p\langle m|x\rangle_x\, {}_x\langle x|\hat{F}_A^\dagger|y\rangle_x\, {}_x\langle y|0\rangle_p \\
&= \hat{F}_R \int \mathrm{d}x\, \hat{U}_{\mathrm{k,x}}(\theta)\, {}_p\langle m|x\rangle_x \left(\int \mathrm{d}y\, e^{iy\hat{x}_R}\, {}_x\langle x|\hat{F}_A^\dagger|y\rangle_x\right) \\
&= \hat{F}_R \int \mathrm{d}x\, \hat{U}_{\mathrm{k,x}}(\theta)e^{-imx}\,(\delta(x-\hat{x}_R)) \\
&= \hat{F}_R\hat{U}_{\mathrm{k},\hat{x}_R}(\theta)e^{-im\hat{x}_R} \\
&= \hat{X}_R(m)\hat{F}_R\hat{U}_{\mathrm{k},\hat{x}_R}(\theta),
\end{aligned}$$

where we used ${}_x\langle x|0\rangle_p = 1$ and

$$\int \mathrm{d}y\, e^{iy\hat{x}_R}\, {}_x\langle x|\hat{F}_A^\dagger|y\rangle_x = \int \mathrm{d}y\, e^{iy(x-\hat{x}_R)} = \delta(x-\hat{x}_R). \tag{C.5}$$

C.1.2 Two-mode gate

$$
\begin{aligned}
{}_{\hat{x}}\langle m|\, E_{AR_2}E_{AR_1}\,|0\rangle_{\hat{p}} &= {}_{\hat{x}}\langle m|\, E_{AR_2}\hat{F}_1\,|-\hat{x}_1\rangle_{\hat{x}} \\
&= {}_{\hat{x}}\langle m|\, \hat{F}_1\hat{F}_2\exp(-i\hat{x}_1\hat{x}_2)\,|-\hat{x}_1\rangle_{\hat{p}} \\
&= \hat{F}_1\hat{F}_2\exp(-i\hat{x}_1\hat{x}_2)\,{}_{\hat{x}}\langle m|-\hat{x}_1\rangle_{\hat{p}} \\
&= \hat{F}_1\hat{F}_2\exp(-i\hat{x}_1\hat{x}_2)e^{-im\hat{x}_1} \\
&= e^{-im\hat{x}_1}\hat{F}_1\hat{F}_2\exp(-i\hat{x}_1\hat{x}_2),
\end{aligned}
$$

where the ancilla states $|\hat{x}_1\rangle$ are to be understood as $\int_{\mathbb{R}} \mathrm{d}x\,|x\rangle\langle x|_{\hat{x}_{R_1}}\, e^{-ix\hat{x}_A}\,|0\rangle_{\hat{p}_A}$.

C.2 Hybrid ADQC

C.2.1 Single qubit gate

For $\mathcal{J}(\gamma) := \hat{F}e^{i\gamma\hat{x}/2}$, we have

$$
\begin{aligned}
{}_{\hat{x}}\langle m|\, \mathcal{J}(\gamma)E_{AR}\,|a\rangle_{\hat{x}} &= {}_{\hat{x}}\langle m|\, \hat{F}e^{i\gamma\hat{x}/2}H\left[\mathbb{1}\otimes|0\rangle\langle 0| + \hat{F}^2\otimes|1\rangle\langle 1|\right]|a\rangle_{\hat{x}} \\
&= {}_{\hat{x}}\langle m|\, \hat{F}e^{i\gamma\hat{x}/2}H\left[|a\rangle_{\hat{x}}\otimes|0\rangle\langle 0| + |-a\rangle_{\hat{x}}\otimes|1\rangle\langle 1|\right] \\
&= {}_{\hat{x}}\langle m|\, H\left[\hat{F}e^{i\gamma a/2}\,|a\rangle_{\hat{x}}\otimes|0\rangle\langle 0| + \hat{F}e^{-i\gamma a/2}\,|-a\rangle_{\hat{x}}\otimes|1\rangle\langle 1|\right] \\
&= {}_{\hat{x}}\langle m|\, H\left[e^{i\gamma a/2}\,|a\rangle_{\hat{p}}\otimes|0\rangle\langle 0| + e^{-i\gamma a/2}\,|-a\rangle_{\hat{p}}\otimes|1\rangle\langle 1|\right] \\
&= {}_{\hat{x}}\langle m|\, He^{i\gamma a\hat{\sigma}_z/2}\left[|a\rangle_{\hat{p}}\otimes|0\rangle\langle 0| + |-a\rangle_{\hat{p}}\otimes|1\rangle\langle 1|\right] \\
&= He^{i\gamma a\hat{\sigma}_z/2}\left[{}_{\hat{x}}\langle m|a\rangle_{\hat{p}}\otimes|0\rangle\langle 0| + {}_{\hat{x}}\langle m|-a\rangle_{\hat{p}}\otimes|1\rangle\langle 1|\right] \\
&= He^{i\gamma a\hat{\sigma}_z/2}\left[e^{ima}\,|0\rangle\langle 0| + e^{-ima}\,|1\rangle\langle 1|\right] \\
&= He^{i\gamma a\hat{\sigma}_z/2}e^{ima\hat{\sigma}_z/2}\left[|0\rangle\langle 0| + |1\rangle\langle 1|\right] \\
&= He^{i\gamma a\hat{\sigma}_z/2}e^{ima\hat{\sigma}_z/2} \\
&= e^{ima\hat{\sigma}_x/2}\hat{J}(\gamma a),
\end{aligned}
\tag{C.6}
$$

where we used

$$
He^{i\alpha\hat{\sigma}_z}H = e^{i\alpha\hat{\sigma}_x}, \tag{C.7}
$$

and the spectral decomposition and eq. (1.8) to write

$$
e^{i\alpha\hat{\sigma}_z} = e^{i\alpha}\,|0\rangle\langle 0| + e^{-i\alpha}\,|1\rangle\langle 1|\,. \tag{C.8}
$$

C.3 Two-qubit gate

The gate on two register qubits labelled by R_1 and R_2 is obtained thus

$$
\begin{aligned}
E_{AR_2}E_{AR_1}\,|a\rangle_{\hat{x}} &= E_{AR_2}H_1\left[|a\rangle_{\hat{x}}\,|0\rangle\langle 0|_{R_1} + |-a\rangle_{\hat{x}}\,|1\rangle\langle 1|_{R_1} +\right] \\
&= H_2\left[|a\rangle_{\hat{x}}\,|0\rangle\langle 0|_{R_2} + |-a\rangle_{\hat{x}}\,|1\rangle\langle 1|_{R_2} +\right]H_1\left[|a\rangle_{\hat{x}}\,|0\rangle\langle 0|_{R_1} + |-a\rangle_{\hat{x}}\,|1\rangle\langle 1|_{R_1} +\right] \\
&= H_2H_1\big[\,|a\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|0\rangle\langle 0|_{R_1} + |1\rangle\langle 1|_{R_2}\,|1\rangle\langle 1|_{R_1}\right) \\
&\qquad + |-a\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|1\rangle\langle 1|_{R_1} + |1\rangle\langle 1|_{R_2}\,|0\rangle\langle 0|_{R_1}\right)\big]
\end{aligned}
$$

Thus,

$$\begin{aligned}{}_{\hat{x}}\langle m|\, E_{AR_2}E_{AR_1}\,|a\rangle_{\hat{x}} &= H_2H_1\Big[{}_{\hat{x}}\langle m|a\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|0\rangle\langle 0|_{R_1}+|1\rangle\langle 1|_{R_2}\,|1\rangle\langle 1|_{R_1}\right)\\ &\qquad +{}_{\hat{x}}\langle m|{-a}\rangle_{\hat{x}}\left(|0\rangle\langle 0|_{R_2}\,|1\rangle\langle 1|_{R_1}+|1\rangle\langle 1|_{R_2}\,|0\rangle\langle 0|_{R_1}\right)\Big].\\ &= H_2H_1\exp\left(ima\hat{\sigma}_{z,R_1}\otimes\hat{\sigma}_{z,R_2}\right)\end{aligned}$$

APPENDIX D

Derivations of the finite squeezing results for the continuous-variable ADQC model

We derive the results of the finite squeezing analysis of the continuous-variable ADQC model from section 4.3.

We model a finitely squeezed ancilla state by

$$|A\rangle = \int \mathrm{g}_{0,s}(a)\,|a\rangle_{\hat{p}}\,\mathrm{d}a, \tag{D.1}$$

where $g_{\mu,\sigma}(x) = \frac{1}{\sigma(2\pi)^{1/4}} \exp\left(-\frac{(x-\mu)^2}{4\sigma^2}\right)$ is a normalised Gaussian centred at μ with standard deviation σ. We set $\mu = 0$ so the ancilla state is a momentum vacuum state with the amount of squeezing defined by s. Infinitely squeezed states are approached by taking the limit $s \to 0$.

D.1 Finite squeezing in CV ADQC

D.1.1 Elements of the CV-CV ADQC model

In the continuous-variable ancilla-driven model presented in chapter 4, we can expand the register states in the position and momentum basis:

$$|\psi\rangle = \int f(r)\,|r\rangle_{\hat{x}}\,\mathrm{d}r; \tag{D.2}$$

and

$$|\phi\rangle = \int h(\rho)\,|\rho\rangle_{\hat{x}}\,\mathrm{d}\rho. \tag{D.3}$$

In what follows, we differentiate between register modes by the alphabet from which the variable originates (Latin or Greek).

The ancilla-register entangling interaction (eq. (4.4)) is

$$E_{AR} = F_A^\dagger F_R \exp(i\hat{x}_A \otimes \hat{x}_R). \tag{D.4}$$

D.1.2 Basic interaction

Entangling the register and ancilla:

$$E_{AR}\,|\psi\rangle\,|A\rangle = \iint f(r)\mathrm{g}_{0,s}(a)\,|a+r\rangle_{\hat{x}}\,|r\rangle_{\hat{p}}\,\mathrm{d}r. \tag{D.5}$$

Measuring the ancilla in the momentum basis gives:

$$\begin{aligned}
{}_{\hat{p}}^{A}\langle m|\, E_{AR}\, |A\rangle &= \iint f(r) \mathrm{g}_{0,s}(a) e^{-im(a+r)} \,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a \\
&= \int \mathrm{g}_{0,s}(a) e^{-ima} \hat{X}(m) \hat{F}\,|\psi\rangle\, \mathrm{d}a \\
&= e^{-m^2 s^2} \hat{X}(m) \hat{F}\,|\psi\rangle\,,
\end{aligned}$$

with $\hat{X}(m) := \exp(im\hat{x})$ an error which may be corrected by classical feed-forward. Taking the limit of infinite squeezing, $s \to 0$, we retain the ideal scenario result. The exponential term due to finite squeezing scales the resulting state. Note that it is not a unitary operation, so the state requires normalisation afterwards. The finite squeezing effect in CV MBQC was a convolution of the original state coefficient function with a Gaussian [54][1] The scaling in ADQC differs in that it is a global scaling in the affected mode.

D.1.3 One-mode gates

For single-mode gates, the goal is to implement the operator

$$\hat{U}_{\hat{x},k}\,(a) = \exp\left(ia\frac{\hat{x}^k}{k}\right), \tag{D.6}$$

for $k = 1, 2, 3$. Together with the Fourier transform, they produce the quadrature displacement, rotation and cubic phase gate respectively. The gates with $k = 1, 2$ are Gaussian gates while the last one is required for applying unitaries generated by Hamiltonians that are arbitrary polynomials of the quadratures (see section 1.6.2).

Noting that

$$\begin{aligned}
\hat{U}_{\hat{x},k}\,(c)\, E_{AR}\,|A\rangle &= \hat{U}_{\hat{x},k}\,(c) \iint f(r) \mathrm{g}_{0,s}(a)\,|a+r\rangle_{\hat{x}}\,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a \\
&= \iint \hat{U}_{a+r,k}\,(c)\, \mathrm{g}_{0,s}(a) f(r)\,|a+r\rangle_{\hat{x}}\,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a,
\end{aligned}$$

we can see that measuring ancilla in the momentum basis gives:

$$\begin{aligned}
{}_{\hat{p}}^{A}\langle m|\, \hat{U}_{\hat{x},k}\,(c)\, E_{AR}\,|A\rangle &= \iint \hat{U}_{a+r,k}\,(c)\, \mathrm{g}_{0,s}(a) f(r)\, {}_{\hat{p}}^{A}\langle m|a+r\rangle_{\hat{x}}\,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a \\
&= \iint \hat{U}_{a+r,k}\,(c)\, e^{-im(a+r)} \mathrm{g}_{0,s}(a) f(r)\,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a \\
&= \iint \hat{U}_{a+r,k}\,(c)\, e^{-ima} \mathrm{g}_{0,s}(a) \hat{X}(m) f(r)\,|r\rangle_{\hat{p}}\, \mathrm{d}r\mathrm{d}a.
\end{aligned} \tag{D.7}$$

We integrate over a for the different values of k, constraining ourselves to the Gaussian gates ($k = 1, 2$)The cubic phase gate requires other methods to calculate, for example using Airy functions [121, 122].

[1] The analysis presented in the reference is limited to the Gaussian gates as done here.

$k = 1$

The relevant integral is, recalling that $\hat{U}_{x,k}(c) = e^{icx^k/k}$:

$$\int \mathrm{g}_{0,s}(a) e^{-ima} \hat{U}_{a+r,1}(c)\,\mathrm{d}a = e^{-(c-m)^2 s^2} e^{irc},$$

which results in the effective register gate:

$$e^{-(c-m)^2 s^2} \hat{X}(m) \hat{F} \hat{U}_{r,1}(c)\,.$$

This, upon taking the limit $s \to 0$, collapses to the expected result:

$$\hat{X}(m) \hat{F} \hat{U}_{r,1}(c)\,.$$

As with the Fourier transform above, the effect of finite squeezing is to scale the affected state.

$k = 2$

Evaluating the relevant integral[2], we have that

$$\begin{aligned}
\int \mathrm{g}_{0,s}(a) e^{-ima} \hat{U}_{a+r,2}(c) &= \frac{1}{\sqrt{1-2ics^2}} \exp\left(-\frac{cr^2 + 2im(m-2cr)s^2}{4cs^2+2i}\right) \\
&= \frac{1}{\sqrt{1-2ics^2}} \exp\left(-\frac{m^2 s^2}{4c^2 s^4+1}\right) \exp\left(\frac{cms^2}{4c^2 s^4+1} r\right) \exp\left(-\frac{c^2 s^2}{4c^2 s^4+1} r^2\right) \\
&\qquad \times \exp\left(-i\frac{2cm^2 s^4}{4c^2 s^4+1}\right) \exp\left(i\frac{2mc^2 s^4}{4c^2 s^4+1} r\right) \exp\left(i\frac{c}{4c^2 s^4+1}\frac{r^2}{2}\right) \\
&= \frac{1}{\sqrt{1-2ics^2}} \exp\left(-\frac{s^2\left(c^2 r^2 - cmr + m^2\right)}{4c^2 s^4+1}\right) \exp\left(-i\frac{2cm^2 s^4}{4c^2 s^4+1}\right) \exp\left(i\frac{2mc^2 s^4}{4c^2 s^4+1} r\right) \exp\left(i\frac{c}{4c^2 s^4+1}\frac{r^2}{2}\right),
\end{aligned}$$

which will result in the following action on the register:

$$\frac{1}{\sqrt{1-2ics^2}} \exp\left(-\frac{s^2\left(c^2 r^2 - cmr + m^2\right)}{4c^2 s^4+1}\right) \hat{X}(m) \hat{X}\left(-\frac{2mc^2 s^4}{4c^2 s^4+1}\right) \hat{F} \hat{U}_{\hat{x},2}\left(\frac{c}{4c^2 s^4+1}\right),$$

where the displacement by m was included from eq. (D.7). Once again, taking the limit $s \to 0$ coincides with the CV ADQC with infinite squeezing:

$$\hat{X}(m) \hat{F} \hat{U}_{\hat{x},2}(c)\,,$$

Even though the form of the alteration due to finite squeezing looks more complicated, it is not dissimilar to the displacement gate. The error term, $\hat{X}$, is supplemented by a further correction, $\hat{X}(-\frac{2mc^2 s^4}{4c^2 s^4+1})$, is still a displacement which can be accounted for at the end of computation since all parameters in the argument are known.

In any measurements we obtain the square of the coefficients. In that case, the scaling is

$$\frac{1}{\sqrt{4c^2 s^4+1}} \exp\left(-\frac{2s^2\left(c^2 r^2 - cmr + m^2\right)}{4c^2 s^4+1}\right). \tag{D.8}$$

This implies a decrease in amplitude compared to the other register states.

[2] For example, symbolically in MATHEMATICA.

D.1.4 Two-mode gate

We end by considering the implementation of the two-mode gate with a finitely-squeezed ancilla.

Consider first that

$$E_{AP}E_{AR}\left|A\right\rangle\left|\phi\right\rangle\left|\psi\right\rangle = \iiint e^{ia\rho}e^{ir\rho}\left|-(a+r)\right\rangle_{\hat{p}}\left|r\right\rangle_{\hat{p}}\left|\rho\right\rangle_{\hat{p}}h(\rho)f(r)\mathrm{g}_{0,s}(a)\mathrm{d}r\mathrm{d}\rho\mathrm{d}a.$$

Measuring the ancilla in the position basis gives the following:

$$\begin{aligned}
{}_{\hat{x}}\left\langle m\right|E_{AP}E_{AR}\left|A\right\rangle\left|\psi\right\rangle\left|\phi\right\rangle &= \iiint e^{ia\rho}e^{ir\rho}\,{}_{\hat{x}}\left\langle m\right|\left|-(a+r)\right\rangle_{\hat{p}}\left|r\right\rangle_{\hat{p}}\left|\rho\right\rangle_{\hat{p}}h(\rho)f(r)\mathrm{g}_{0,s}(a)\mathrm{d}r\mathrm{d}\rho\mathrm{d}a \\
&= \iiint e^{ia\rho}e^{ir\rho}e^{-im(a+r)}\mathrm{g}_{0,s}(a)\ \left|r\right\rangle_{\hat{p}}\left|\rho\right\rangle_{\hat{p}}h(\rho)f(r)\mathrm{d}r\mathrm{d}\rho\mathrm{d}a \\
&= \iint e^{ir\rho}e^{-imr}\left|r\right\rangle_{\hat{p}}\left|\rho\right\rangle_{\hat{p}}h(\rho)f(r)\mathrm{d}r\mathrm{d}\rho\int e^{ia(\rho-m)}\mathrm{g}_{0,s}(a)\mathrm{d}a \\
&= \iint e^{ir\rho}e^{-imr}\left|r\right\rangle_{\hat{p}}\left|\rho\right\rangle_{\hat{p}}h(\rho)f(r)\exp\left(-(\rho-m)^2s^2\right)\mathrm{d}r\mathrm{d}\rho \\
&= e^{-im\hat{p}_{R_1}}e^{i\hat{p}_{R_1}\hat{p}_{R_2}}\int f(r)\left|r\right\rangle_{\hat{p}}\mathrm{d}r\int e^{-(\rho-m)^2s^2}h(\rho)\left|\rho\right\rangle_{\hat{p}}\mathrm{d}\rho \\
&= e^{-im\hat{p}_{R_1}}e^{i\hat{p}_{R_1}\hat{p}_{R_2}}\hat{F}_{R_1}\hat{F}_{R_2}\int f(r)\left|r\right\rangle_{\hat{x}}\mathrm{d}r\int h'(\rho)\left|\rho\right\rangle_{\hat{x}}\mathrm{d}\rho \\
&= e^{-im\hat{p}_{R_1}}\hat{F}_{R_1}\hat{F}_{R_2}e^{i\hat{x}_{R_1}\hat{x}_{R_2}}\int f(r)\left|r\right\rangle_{\hat{x}}\mathrm{d}r\int h'(\rho)\left|\rho\right\rangle_{\hat{x}}\mathrm{d}\rho \\
&= \hat{X}_{R_1}(m)\hat{F}_{R_1}\hat{F}_{R_2}CZ_{\infty}\left|\psi\right\rangle\left|\rho'\right\rangle.
\end{aligned} \tag{D.9}$$

Finite squeezing in the two-mode gate results in a convolution of the original state with a Gaussian – inversely dependent on the squeezing parameter and ancilla measurement outcome. This matches the result in ref. [54].

D.1.5 Summary

$\hat{F}$

$${}^{A}_{p}\left\langle m\right|E_{AR}\left|A\right\rangle\left|\psi\right\rangle = e^{-m^2s^2}\hat{X}(m)\hat{F}\left|\psi\right\rangle; \tag{D.10}$$

$\hat{U}_{\hat{x},1}(c)$

$${}^{A}_{p}\left\langle m\right|\hat{U}_{\hat{x},1}(c)\,E_{AR}\left|A\right\rangle\left|\psi\right\rangle = e^{-(c-m)^2s^2}\hat{X}(m)\hat{F}\hat{U}_{r,1}(c); \tag{D.11}$$

$\hat{U}_{\hat{x},2}(c)$

$${}^{A}_{p}\left\langle m\right|\hat{U}_{\hat{x},2}(c)E_{AR}\left|A\right\rangle\left|\psi\right\rangle$$
$$= \frac{1}{\sqrt{1-2ics^2}}\exp\left(-\frac{s^2\left(c^2r^2-cmr+m^2\right)}{4c^2s^4+1}\right)\hat{X}(m)\hat{X}(-\frac{2mc^2s^4}{4c^2s^4+1})\hat{F}\hat{U}_{\hat{x},2}\left(\frac{c}{4c^2s^4+1}\right);$$

CZ

$$\overset{A}{\hat{x}}\langle m|\, E_{AP}E_{AR}\,|A\rangle\,|\phi\rangle\,|\psi\rangle = \hat{X}_{R_1}(m)\hat{F}_{R_1}\hat{F}_{R_2}CZ_\infty\,|\psi\rangle\,|\rho\rangle\,, \tag{D.12}$$

with $|\phi'\rangle = \int e^{-(\rho-m)^2 s^2} h(\rho)\,|\rho\rangle_{\hat{p}}\,|\rho\rangle_{\hat{x}}\,\mathrm{d}\rho$.

APPENDIX E

Derivations of the finite squeezing results for the hybrid ADQC model

E.1 Finite squeezing in Hybrid ADQC

We derive the results of the finite squeezing analysis of the hybrid-variable ADQC model from section 4.3.

E.1.1 Generic one qubit gate

Any operation on the qubit by means of evolving and measuring the ancilla is:

$$ {}_q\langle m| O_A E_{AR} D(d) |A\rangle , \tag{E.1} $$

with $D(d) = \exp(id\hat{p})$ and $|A\rangle$ the vacuum Gaussian state as in eq. (D.1).

We look at it in parts. First of all, note that the effect of the entangling interaction on the ancilla is:

$$ \begin{aligned} E_{AR} D(d) |A\rangle &= \mathbb{I} \otimes H \left[\mathbb{I} \otimes |0\rangle\langle 0| + \hat{F}^2 \otimes |1\rangle\langle 1| \right] \int g_{s,d}(a) |a\rangle_q \\ &= \int \mathrm{d}a \, g_{s,d}(a) H \left[|0\rangle\langle 0| \otimes |a\rangle_q + |1\rangle\langle 1| \otimes |-a\rangle_q \right] . \end{aligned} \tag{E.2} $$

Therefore, the whole effect is:

$$ \begin{aligned} {}_q\langle m| O_A E_{AR} D(d) |A\rangle = \quad & H \int \mathrm{d}a \, g_{s,d}(a) {}_q\langle m| O_A E_{AR} |a\rangle |0\rangle\langle 0| \\ & + H \int \mathrm{d}a \, g_{s,d}(a) {}_q\langle m| O_A E_{AR} |-a\rangle |1\rangle\langle 1| . \end{aligned} \tag{E.3} $$

That is, the action on the computational basis vectors is

$$ |0\rangle \xrightarrow{O_A} \int \mathrm{d}a \, g_{s,d}(a) {}_q\langle m| O_A E_{AR} |a\rangle |+\rangle \tag{E.4} $$

$$ |1\rangle \xrightarrow{O_A} \int \mathrm{d}a \, g_{s,d}(a) {}_q\langle m| O_A E_{AR} |-a\rangle |-\rangle , \tag{E.5} $$

Where the operator over the arrow denotes the tranformation (discounting the entangling and initial displacement) of the ancilla. The transformations above do not preserve norm (normalized states are not mapped to normalized states).

To get the correct transformation rule begin by writing the *effective operation* on the qubit as:

$$ \mathcal{E}_d(O_A) :=_q \langle m| O_A E_{AR} D(d) |A\rangle . \tag{E.6} $$

The transformation rule then becomes

$$ |\phi\rangle \xrightarrow{O_A} \frac{{}_q\langle m| O_A E_{AR} D(d) |A\rangle |\phi\rangle}{\sqrt{\langle\phi|\mathcal{E}_d(O_A)^\dagger \mathcal{E}_d(O_A)|\phi\rangle}} . \tag{E.7} $$

With computational basis transformations:

$$|0\rangle \xrightarrow{O_A} \frac{\int \mathrm{d}a\, g_{s,d}(a)_q \langle m|\, O_A E_{AR}\, |a\rangle\, |+\rangle}{\sqrt{\langle 0|\mathcal{E}_d(O_A)^\dagger \mathcal{E}_d(O_A)|0\rangle}}; \text{ and} \tag{E.8}$$

$$|1\rangle \xrightarrow{O_A} \frac{\int \mathrm{d}a\, g_{s,d}(a)_q \langle m|\, O_A E_{AR}\, |-a\rangle\, |-\rangle}{\sqrt{\langle 1|\mathcal{E}_d(O_A)^\dagger \mathcal{E}_d(O_A)|1\rangle}}. \tag{E.9}$$

E.1.2 'Minimal' one-qubit gate

We calculate ${}_q\langle m|\, E_{AR}\, |A\rangle$, or $O_A = \mathbb{I}$, $d = 0$. Note that $\langle j|\mathcal{E}_0(\mathbb{I})^\dagger \mathcal{E}_0(\mathbb{I})|j\rangle = g_{s,0}(a)$ for $j = 0, 1$.

Using the general form obtained above, we find the basis tranformations:

$$\begin{aligned} |0\rangle \xrightarrow{\mathbb{I}_A} & \int \mathrm{d}a\, g_{s,0}(a)_q \langle m|a\rangle_q\, |+\rangle \\ &= \frac{g_{s,0}(m)}{\sqrt{\langle 0|\mathcal{E}_0(\mathbb{I})^\dagger \mathcal{E}_0(\mathbb{I})|0\rangle}} H\,|0\rangle \\ &= H\,|0\rangle \end{aligned} \qquad \begin{aligned} |1\rangle \xrightarrow{\mathbb{I}_A} & \int \mathrm{d}a\, g_{s,0}(a)_q \langle m|-a\rangle_q\, |-\rangle \\ &= \frac{g_{s,0}(-m)}{\sqrt{\langle 1|\mathcal{E}_0(\mathbb{I})^\dagger \mathcal{E}_0(\mathbb{I})|1\rangle}} H\,|1\rangle \\ &= H\,|1\rangle\,. \end{aligned} \tag{E.10}$$

A generic state is therefore transformed as follows

$$|\psi\rangle \xrightarrow{\mathbb{I}_A} H\,|\psi\rangle\,. \tag{E.11}$$

E.1.3 One-qubit rotation

We want to enact $J(\gamma) = H \exp\left[-i\frac{\gamma}{2}\hat{\sigma}_z\right]$ on the register.

Translating naively from the infinite squeezing case, we let $O_A = \mathcal{J}_A(\gamma) := F \exp[i\gamma\hat{q}]$.

Now, if we proceed with the same procedure, we inevitable run into problems as

$${}_q\langle m|\, \mathcal{J}_A(\gamma)\, |\pm a\rangle = \exp[\pm i\gamma a]_q \langle m|\pm a\rangle_p = \exp[\pm(\gamma + m)a] \tag{E.12}$$

and

$$\int g_{s,0}(a) \exp[\pm(\gamma + m)a] = \exp\left[-s^2(\gamma + m)^2\right], \tag{E.13}$$

so that the qubit is not rotated (there is no 'i'). This is because the "average" effect of the operation on the qubit is parametrised by the mean of the Gaussian of the ancilla state. Furthermore, in the infinite squeezing case, the eigenvalue of the ancilla (translation from vacuum) gave the rotation of the register qubit. Following that vein of thought, we consider displacing the ancilla prior to performing the usual operation.

That is, consider the following:

$${}_q\langle m|\, \mathcal{J}_A(\gamma) E_{AR} D(d)\, |A\rangle\,. \tag{E.14}$$

We start from eq. (4.15), which gives the operation resulting in the qubit rotation.

$$
\begin{aligned}
{}_q\langle m|\,\mathcal{J}_A(\gamma)E_{AR}D(d)\,|A\rangle &= {}_q\langle m|\,\mathcal{J}_A(\gamma)E_{AR}\int g_{s,d}(a)\,|a\rangle_q\,\mathrm{d}a \\
&= H\int g_{s,d}(a)\,[\exp[i(\gamma+m)a]\,|0\rangle\langle 0| + \exp[-i(\gamma+m)a]\,|1\rangle\langle 1|]\,\mathrm{d}a \\
&= \nu\exp\left[-s^2(m+\gamma)^2\right]H\,[\exp[i(\gamma+m)d]\,|0\rangle\langle 0| + \exp[-i(\gamma+m)d]\,|1\rangle\langle 1|] \\
&= \nu\exp\left[-s^2(m+\gamma)^2\right]H\exp[i(\gamma+m)d\hat{\sigma}_z] \\
&= \nu\exp\left[-s^2(m+\gamma)^2\right]\exp[imd\hat{\sigma}_x]H\exp[i\gamma d\hat{\sigma}_z] \\
&= \nu\exp\left[-s^2(m+\gamma)^2\right]\exp[imd\hat{\sigma}_x]J(2d\gamma),
\end{aligned}
\tag{E.15}
$$

where we set $\nu = N\sqrt{2\pi s}$, with N the Gaussian normalizing factor and s the squeezing parameter. We used eq. (A.9) to evaluate the integral.

The coefficient $\nu\exp\left[-s^2(m+\gamma)^2\right]$ is removed when the state is normalized. That is, the effective gate on the qubit is

$$
|\psi\rangle \xrightarrow{\mathcal{J}_A(\gamma)} \exp[imd\hat{\sigma}_x]J(2d\gamma)\,|\psi\rangle\,. \tag{E.16}
$$

We see then that eq. (E.16) coincides with the infinite squeezing one-qubit rotation, eq. (4.15). In particular, it suffers from the same error which can only be removed probabilistically.

E.1.4 Two-qubit gate

We proceed as in the previous section and by analogy to the original proposal using infinite squeezing and calculate the following (note that we are now measuring the momentum of the ancilla):

$$
\begin{aligned}
{}_p\langle m|\,E_{AR_2}E_{AR_1}D(d)\,|A\rangle &= \\
&= \int g_{s,d}(a)\,{}_p\langle m|\,E_{AR_2}E_{AR_1}D(d)\,|a\rangle\,\mathrm{d}a \\
&= \int g_{s,d}(a)\Big[\exp[ima]\,(|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|) \\
&\qquad + \exp[-ima]\,(|0\rangle\langle 0|\otimes|1\rangle\langle 1| + |1\rangle\langle 1|\otimes|0\rangle\langle 0|)\Big]\mathrm{d}a \\
&= \nu\exp\left[-s^2m^2\right]\Big[\exp[imd]\,(|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |1\rangle\langle 1|\otimes|1\rangle\langle 1|) \\
&\qquad + \exp[-imd]\,(|0\rangle\langle 0|\otimes|1\rangle\langle 1| + |1\rangle\langle 1|\otimes|0\rangle\langle 0|)\Big] \\
&= \nu\exp\left[-s^2m^2\right]\exp[imd\hat{\sigma}_z\otimes\hat{\sigma}_z],
\end{aligned}
\tag{E.17}
$$

with $\nu = N\sqrt{2\pi s}$. The effect of finite squeezing is to add a scaling which dose not remain after normalisation. That is, two qubits are transformed as follows

$$
|\psi\rangle\,|\phi\rangle \longrightarrow \exp[imd\hat{\sigma}_z\otimes\hat{\sigma}_z]\,|\psi\rangle\,|\phi\rangle\,, \tag{E.18}
$$

once again coinciding with the infinite squeezing case ($s\to 0$).

APPENDIX F

Effect of number of iterations of algorithm 1 on the witness mean

We provide some evidence supporting our choice of running algorithm 1 for $n = 10$ iterations.

We find that the largest decrease in the witness mean, $\mathrm{Tr}[\gamma W]$, occurs after the first step. We present a plot, in fig. F.1, of running algorithm 1 for a number of iterations, $n \in [1, 20[$. The dependent axis shows the percentage increase in the witness mean, $c_n := \mathrm{Tr}[\gamma_n W_n]$, for γ_n and W_n the CM and witness at the n^{th} respectively.

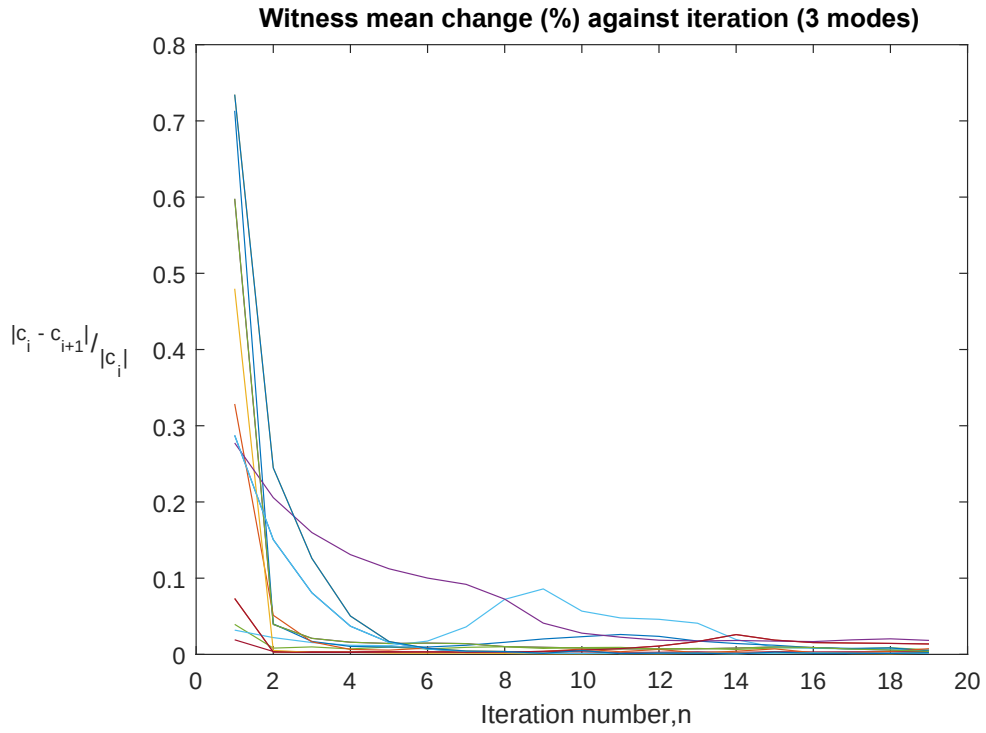


Figure F.1: Percentage change of witness mean with increased number of iterations of algorithm 1. Discrete points interpolated by lines for clarity.

We see that after $n = 10$, the further improvement is less than 0.1% for most cases. We argue therefore, that the choice of number of iterations is sufficient for finding suitable examples of CMs with the desired properties.

Full inseparability does not imply genuine multipartite entanglement

In the classification of multipartite entanglement one finds two classes that might at first sight be the same: the fully inseparable states and ones that are biseparable. Fully inseparable state are those that are not separable across any partition biseparable state are those that can be written as a convex sum of separable states (see section 5.3.2).

A qubit example of a state that is biseparable but fully inseparable was presented in ref. [140, sec. 3.2.2]. The three party state is an equal mixture of Bell states of two parties with the third party being the ground state:

$$\sum_{\substack{i,j,k=A,B,C \\ i\neq j\neq k}} \frac{1}{3}\left(\left|\phi^+\right\rangle\!\left\langle\phi^+\right|^{ij} \otimes |0\rangle\!\langle 0|^k\right),$$

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

An analogous example for CMs was not found in the literature. In analogy to the qubit density matrix case we present a covariance matrix of a biseparable state that is nonetheless not separable across any bipartition:

$$\frac{1}{3}\left(\gamma_{AB} \oplus \mathbb{I}_C + \gamma_{AC} \oplus \mathbb{I}_B + \gamma_{BC} \oplus \mathbb{I}_A\right), \tag{G.1}$$

where the ordering of modes is preserved in the representation of the covariance matrix. That is,

$$\gamma_{AB} \oplus \mathbb{I}_C := \begin{pmatrix} \gamma_A & \gamma_{AB} & \mathbb{O} \\ \gamma_{AB} & \gamma_B & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & \mathbb{I}_C \end{pmatrix};$$

$$\gamma_{AC} \oplus \mathbb{I}_B := \begin{pmatrix} \gamma_A & \mathbb{O} & \gamma_{AC} \\ \mathbb{O} & \mathbb{I}_B & \mathbb{O} \\ \gamma_{AC} & \mathbb{O} & \gamma_C \end{pmatrix};$$

$$\gamma_{BC} \oplus \mathbb{I}_B := \begin{pmatrix} \mathbb{I}_A & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & \gamma_B & \gamma_{BC} \\ \mathbb{O} & \gamma_{BC} & \gamma_C \end{pmatrix},$$

with γ_j the covariance matrix of mode j and γ_{jk} the covariance matrix of the modes j and k; $\mathbb{I}$ and $\mathbb{O}$ are the 2×2 identity and zero matrices respectively.

We show that full inseparability at the covariance matrix level does not imply that the state corresponding to that covariance matrix is genuine multipartite entangled. We do that by giving an example of CMs γ_{ij}, $ij = AB, AC, BC$, such that eq. (G.1) is fully inseparable. Since it is biseparable by construction, it is not genuinely multipartite entangled.

A two-mode vacuum CM is given by

$$\gamma_{jk}^{TMSV} = \begin{pmatrix} a\mathbb{I}_2 & c\sigma_z \\ c\sigma_z & a\mathbb{I}_2 \end{pmatrix}, \tag{G.2}$$

and where $a = \cosh(2r), c = \sinh(2r)$ and $\sigma_z = \mathrm{diag}(1,-1)$, the usual Pauli-z matrix; r is the squeezing parameter. Let now $\gamma_{jk} = \gamma_{jk}^{TMSV}$ for $jk = AB, AC, BC$. To show that eq. (G.1) is fully inseparable we show that there is a squeezing value, r, such that the CM is not separable across any bipartition[1].

Expanding the CM fully, we have

$$\begin{aligned}\gamma_{ABC} &= \frac{1}{3}\left(\gamma_{AB}^{TMSV} \oplus \mathbb{I}_C + \gamma_{AC}^{TMSV} \oplus \mathbb{I}_B + \gamma_{BC}^{TMSV} \oplus \mathbb{I}_A\right) \\ &= \frac{1}{3}\begin{pmatrix} (2a+1)\mathbb{I} & c\sigma_z & c\sigma_z \\ c\sigma_z & (2a+1)\mathbb{I} & c\sigma_z \\ c\sigma_z & c\sigma_z & (2a+1)\mathbb{I} \end{pmatrix}.\end{aligned} \tag{G.3}$$

To test separability across all bipartitions, we check all symplectic eigenvalues of the covariance matrix under partial transposition [145]. For a given partition across which the partial transposition is taken: if the symplectic eigenvalues [2] are equal to or greater than one then the state is separable across that partition (see Thm. 5.6). If this does not hold for any partition, the state is fully inseparable. Since the state is invariant under mode swapping, any bipartition is sufficient.

As a function of the squeezing parameter, the magnitude of the smallest symplectic eigenvalue after partial transposition of the density matrix is given by

$$\nu_{min}^{PT} = \frac{1}{6}\sqrt{|9 + 16\cosh(2r) + 11\cosh(4r) - \sqrt{2(199 + 256\cosh(2r) + 121\cosh(4r))}\sinh 2r|},$$

which is smaller than one for the squeezing parameter in the range $0 < r \leq 1.24275$.

This example shows that the set of Gaussian biseparable covariance matrices is not equal to the set of fully inseparable covariance matrices.

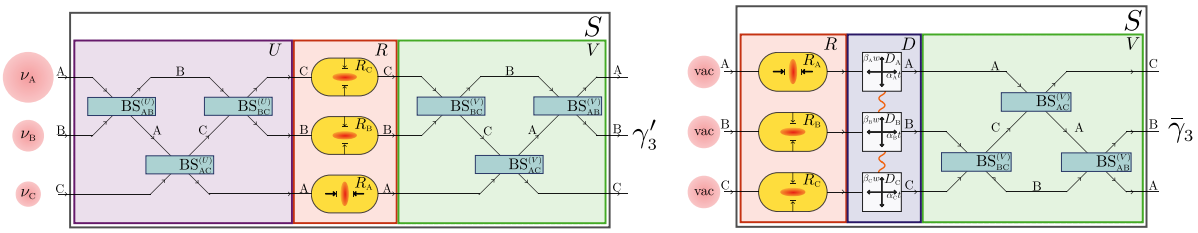
[1] Due to the hierarchy of multipartite entanglement. Showing that a CM is not 2-separable subsumes k-separability for all $k > 2$.

[2] The symplectic eigenvalues of γ are the absolute values of the eigenvalues of $i\Omega\gamma$. For a covariance matrix γ, the requirement for the symplectc eigenvalues to be less than one is equivalent to not satisfying the uncertainty principle: $\gamma + i\Omega \ngeq 0$.

APPENDIX H

Circuits in figs. 6.3 and 6.4 are equivalent

We prove that the covariance matrices of the output states produced by circuits in figs. 6.3 and 6.4 are the same. They are copied in this appendix in fig. H.1. Since the last beam-splitter array coincides in both circuits, we only need to show that the covariance matrices just before that (after R in fig. 6.3 and after D in fig. 6.4) are the same.



(a) Circuit to produce $\gamma^{(3)}$ with rounded parameters (fig. 6.3) **(b)** Circuit to produce $\bar{\gamma}^{(3)}$. (fig. 6.4)

Figure H.1: Equivalent circuits that output γ' as defined in section 6.5

Describe by $\boldsymbol{\xi}$ a vector of canonical operators, $\boldsymbol{d}$ a displacement of quadratures, by B the mixing due to a beam-splitter array, and by S a squeezing transformation. The effect of the circuit in fig. 6.3 (until after squeezing operation R) on a quadratures contained in $\boldsymbol{\xi}$ is

$$\mathcal{P}_1 : \quad \boldsymbol{\xi} \mapsto \boldsymbol{\xi} + \boldsymbol{d} \mapsto B\boldsymbol{\xi} + B\boldsymbol{d} \mapsto SB\boldsymbol{\xi} + SQB\boldsymbol{d} = \boldsymbol{\xi}^1. \tag{H.1}$$

The same end may be achieved through the process

$$\mathcal{P}_2 : \quad \boldsymbol{\xi} \mapsto S\boldsymbol{\xi} \mapsto S\boldsymbol{\xi} + \boldsymbol{d}' \mapsto S\boldsymbol{\xi} + \boldsymbol{d}' = \boldsymbol{\xi}^2. \tag{H.2}$$

where $\boldsymbol{d}' = SB\boldsymbol{d}$. This corresponds to the two first steps in fig. 6.4. Define then the two covariance matrices due to the circuits $\mathcal{P}_1$ and $\mathcal{P}_2$ as $\gamma_{\mathcal{P}_1}$ and $\gamma_{\mathcal{P}_2}$ respectively. Let also γ_0 be the covariance matrix of the input which is the vacuum in all three modes. Therefore, the elements may be given by

$$(\gamma_0)_{ij} = \langle\{\xi_i, \xi_j\}\rangle = \delta_{ij}, \tag{H.3}$$

where we used the fact that the first moments are chosen to be at the origin (equivalently, the input is a vacuum): $\langle\xi_i\rangle = 0$ for all $i \in [0, 2N]$.

To see that the two processes are equivalent with respect to entanglement properties of the states generated one may verify that they produce the same covariance matrix. Using Def. 5.14 (Covariance matrix), the covariance matrix produced after circuit $\mathcal{P}_1$ is

$$(\gamma_{\mathcal{P}_1})_{ij} = \langle\{\xi_i^1, \xi_j^1\}\rangle - 2\langle\xi_i^1\rangle\langle\xi_j^1\rangle. \tag{H.4}$$

Let's consider the second term first. Begin by noting that

$$\begin{aligned}\langle \xi_i^1 \rangle &= \langle S_{i\alpha} B_{\alpha\beta} \xi_\beta + S_{i\alpha} B_{\alpha\beta} d_\beta \rangle \\ &= \langle S_{i\alpha} B_{\alpha\beta} \xi_\beta \rangle + \langle d_i' \rangle \\ &= S_{i\alpha} B_{\alpha\beta} \langle \xi_\beta \rangle + \langle d_i' \rangle \\ &= d_i',\end{aligned}$$

where we used that $\xi_\beta = 0$ for all β and $\langle d_\beta \rangle = d_\beta \langle \mathbb{1} \rangle = d_\beta \cdot 1$. Then, the only component that remains in the second term of eq. (H.3) is

$$-2 S_{i\alpha} B_{\alpha\beta} d_\beta S_{i\mu} B_{\mu\nu} d_\nu = -2 \langle d_i' \rangle \langle d_j' \rangle. \tag{H.5}$$

Now consider the first term of eq. (H.3):

$$\begin{aligned}\langle \{\xi_i^1, \xi_j^1\} \rangle &= \langle \{S_{i\alpha} B_{\alpha\beta} \xi_\beta + d_i', S_{j\mu} B_{\mu\nu} \xi_\nu + d_j'\} \rangle \\ &= \langle \{S_{i\alpha} B_{\alpha\beta} \xi_\beta, S_{j\mu} B_{\mu\nu} \xi_\nu\} \rangle + \underbrace{\langle \{S_{i\alpha} B_{\alpha\beta} \xi_\beta, d_j'\} \rangle}_{=0} + \underbrace{\langle \{d_i', S_{j\mu} B_{\mu\nu} \xi_\nu\} \rangle}_{=0} + \langle \{d_i', d_j'\} \rangle \\ &= S_{i\alpha} B_{\alpha\beta} S_{j\mu} B_{\mu\nu} \langle \{\xi_\beta, \xi_\nu\} \rangle + \langle \{d_i', d_j'\} \rangle \\ &= S_{i\alpha} B_{\alpha\beta} S_{j\mu} B_{\mu\nu} \delta_{\beta\nu} + \langle \{d_i', d_j'\} \rangle \\ &= S_{i\alpha} S_{j\mu} B_{\mu\beta} B_{\alpha\beta} + \langle \{d_i', d_j'\} \rangle \\ &= S_{i\alpha} S_{j\mu} \delta\alpha\mu + \langle \{d_i', d_j'\} \rangle,\end{aligned}$$

where we used the fact that B is orthogonal ($BB^T = \mathbb{1}$ so $(BB^T)_{ij} = B_{i\alpha}(B^T)_{\alpha j} = B_{i\alpha} B_{j\alpha} = \delta_{ij}$) to get the last line.

Putting both terms together we get that

$$\begin{aligned}(\gamma_{\mathcal{P}_1})_{ij} &= \langle \{\xi_i^1, \xi_j^1\} \rangle - 2 \langle \xi_i^1 \rangle \langle \xi_j^1 \rangle. \\ &= S_{i\alpha} S_{j\mu} \delta\alpha\mu + \langle \{d_i', d_j'\} \rangle - 2 \langle d_i' \rangle \langle d_j' \rangle \\ &= S_{i\alpha} \langle \{\xi_\alpha, \xi_{mu}\} \rangle S_{j\mu} + \langle \{d_i', d_j'\} \rangle - 2 \langle d_i' \rangle \langle d_j' \rangle, \\ &= \langle \{S_{i\alpha} \xi_\alpha, S_{j\mu} \xi_\mu\} \rangle + \langle \{d_i', d_j'\} \rangle - 2 \langle d_i' \rangle \langle d_j' \rangle,\end{aligned}$$

where the penultimate line followed from using $S_{\alpha\beta} = S_{\beta\alpha}$ since it is diagonal.

Now, to find that this is the same as the covariance matrix due to circuit $\mathcal{P}_2$ we use a number of times that $\langle \xi_i \rangle$ for all i. In particular, we add the (zero) terms $\langle \{S_{i\alpha} \xi_\alpha, d_j'\} \rangle, \langle \{d_i', S_{j\mu} \xi_\mu\} \rangle$, to join the two first terms and append $-2\langle S_{i\alpha} \xi_\alpha \rangle \langle d_j' \rangle, -2\langle d_1' \rangle \langle S_{j\mu} \xi_\mu \rangle$, and $-2\langle S_{i\alpha} \xi_\alpha \rangle \langle S_{j\mu} \xi_\mu \rangle$ to the last term.

The above equation then reads

$$\begin{aligned}(\gamma_{\mathcal{P}_1})_{ij} &= \langle \{S_{i\alpha} \xi_\alpha, S_{j\mu} \xi_\mu\} \rangle + \langle \{d_i', d_j'\} \rangle - 2 \langle d_i' \rangle \langle d_j' \rangle && \text{(H.6)} \\ &= \langle \{S_{i\alpha} \xi_\alpha + d_i', S_{j\mu} \xi_\mu + d_j'\} \rangle - 2 \langle S_{i\alpha} \xi_\alpha + d_i' \rangle \langle S_{j\mu} \xi_\mu + d_j' \rangle && \text{(H.7)} \\ &= \langle \{\xi_i^2, \xi_j^2\} \rangle - 2 \langle \xi_i^2 \rangle \langle \xi_j^2 \rangle && \text{(H.8)} \\ &= (\gamma_{\mathcal{P}_2})_{ij}, && \text{(H.9)}\end{aligned}$$

which completes the proof.

For numerical calculation purposes, the correlation parameters given in table 6.11 are calculated from the outer product of $\boldsymbol{d}'$ with itself. Since the variables t and w are independent and have zero mean, terms involving their product $\langle t \rangle \langle w \rangle$ can be set to zero.

Bibliography

References for Introduction

[1] A. I. M. Rae. *Quantum Mechanics*. Fifth edition. CRC Press, 2007 (cit. on p. 3).

[2] B. H. Bransden and C. J. Joachain. *Quantum Mechanics*. Second edition. Pearson, 2000 (cit. on p. 3).

[3] J. J. Sakurai. *Modern Quantum Mechanics*. Ed. by S. F. Tuan. First revised edition. Addison Wesley Longman, 1993 (cit. on p. 3).

[4] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Reprint 2003. Cambridge University Press, 2000 (cit. on pp. 3, 8, 20, 27).

[5] M. Reed and B. Simon. *I: Functional Analysis*. Academic Press, 1980 (cit. on p. 4).

[6] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Trans. by R. T. Beyer. Original in German (1932). Princeton, New Jersey, United States: Princeton University Press, 1996 (cit. on p. 5).

[7] S. Barnett. *Quantum Information*. Oxford Master Series in Physics. Oxford: Oxford University Press, 2009, p. 314. ISBN: 9780198527626. DOI: 10.1093/oso/9780198527626.001.0001 (cit. on pp. 5–8, 19).

[8] P. Busch. ""No Information Without Disturbance": Quantum Limitations of Measurement". In: *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*. Dordrecht: Springer Netherlands, 2009, pp. 229–256. DOI: 10.1007/978-1-4020-9107-0_13 (cit. on p. 5).

[9] W. Heisenberg. *The Physical Principles of the Quantum Theory*. Trans. by C. Eckart and F. C. Hoyt. Republication of original by University of Chicago press (1930). Dover, 1949 (cit. on pp. 5, 12).

[10] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* 47 (10 May 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777 (cit. on p. 7).

[11] B. Coecke. *Kindergarten Quantum Mechanics*. 2005. arXiv: quant-ph/0510032 [quant-ph] (cit. on p. 7).

[12] B. Coecke. *The logic of entanglement*. 2004. arXiv: quant-ph/0402014 [quant-ph] (cit. on p. 7).

[13] L. Gurvits. "Classical Deterministic Complexity of Edmonds' Problem and Quantum Entanglement". In: *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*. STOC '03. San Diego, CA, USA: Association for Computing Machinery, 2003, pp. 10–19. ISBN: 1581136749. DOI: 10.1145/780542.780545 (cit. on p. 7).

[14] J. S. Bell. "On the Einstein Podolsky Rosen paradox". *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195 (cit. on p. 8).

[15] D. Esteve, J. Dalibard, and J.-M. Raimond, eds. *Proceedings, Les Houches Summer School of Theoretical Physics, Session 79: Quantum Entanglement and Information Processing: Les Houches, France, July 30 - August 25, 2003*. Vol. 79. 2004, pp.1–608 (cit. on p. 8).

[16] E. H. Kennard. "Zur Quantenmechanik einfacher Bewegungstypen". *Zeitschrift für Physik* 44.4 (Apr. 1927), pp. 326–352. ISSN: 0044-3328. DOI: 10.1007/BF01391200 (cit. on p. 9).

[17] H. P. Robertson. "The Uncertainty Principle". *Phys. Rev.* 34 (1 July 1929), pp. 163–164. DOI: 10.1103/PhysRev.34.163 (cit. on p. 9).

[18] A. Peres. "Separability Criterion for Density Matrices". *Phys. Rev. Lett.* 77 (8 Aug. 1996), pp. 1413–1415. DOI: 10.1103/PhysRevLett.77.1413 (cit. on pp. 9, 74).

[19] M. Horodecki, P. Horodecki, and R. Horodecki. "Separability of mixed states: necessary and sufficient conditions". *Physics Letters A* 223.1 (1996), pp. 1–8. ISSN: 0375-9601. DOI: 10.1016/S0375-9601(96)00706-2 (cit. on pp. 9, 74, 76, 77).

[20] P. Horodecki. "Separability criterion and inseparable mixed states with positive partial transposition". *Physics Letters A* 232.5 (1997), pp. 333–339. ISSN: 0375-9601. DOI: 10.1016/S0375-9601(97)00416-7 (cit. on pp. 9, 74).

[21] E. Størmer. "Decomposable Positive Maps on C^*-Algebras". *Proceedings of the American Mathematical Society* 86.3 (1982), pp. 402–404. DOI: https://doi.org/10.2307/2044436 (cit. on p. 9).

[22] S. Woronowicz. "Positive maps of low dimensional matrix algebras". *Reports on Mathematical Physics* 10.2 (1976), pp. 165–183. ISSN: 0034-4877. DOI: https://doi.org/10.1016/0034-4877(76)90038-0 (cit. on p. 9).

[23] U. Leonhardt. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge: Cambridge University Press, 2010. DOI: 10.1017/CBO9780511806117 (cit. on pp. 9, 16).

[24] C. Gerry and P. Knight. *Introductory Quantum Optics*. Cambridge: Cambridge University Press, 2004. DOI: 10.1017/CBO9780511791239 (cit. on pp. 10, 48).

[25] S. Barnett and P. Radmore. *Methods in Theoretical Quantum Optics*. Oxford Series in Optical and Imaging Sciences 15. Oxford: Oxford University Press, 1997, p. 292. DOI: 10.1093/acprof:oso/9780198563617.001.0001 (cit. on pp. 10, 11, 13, 17, 18).

[26] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. 1st ed. Boca Raton: CRC Press, 2017. DOI: 10.1201/9781315118727 (cit. on pp. 10, 43, 46, 62, 66–70, 79, 105).

[27] C. Weedbrook et al. "Gaussian quantum information". *Rev. Mod. Phys.* 84 (2 May 2012), pp. 621–669. DOI: 10.1103/RevModPhys.84.621 (cit. on p. 10).

[28] S. L. Braunstein and P. van Loock. "Quantum information with continuous variables". *Rev. Mod. Phys.* 77 (2 June 2005), pp. 513–577. DOI: 10.1103/RevModPhys.77.513 (cit. on p. 10).

[29] Quantumwhisp (https://physics.stackexchange.com/users/102243/quantumwhisp). *Is there any plausible reason for the existence of conjugate variables in quantum mechanics?* Physics Stack Exchange. URL: https://physics.stackexchange.com/q/377201 (cit. on p. 12).

[30] D. I. Bondar, R. R. Lompay, and W.-K. Liu. "Quantum mechanics of a free particle from properties of the Dirac delta function". *American Journal of Physics* 79.4 (2011), pp. 392–394. DOI: 10.1119/1.3533715 (cit. on p. 12).

[31] S. Lloyd and S. L. Braunstein. "Quantum Computation over Continuous Variables". *Phys. Rev. Lett.* 82 (8 Feb. 1999), pp. 1784–1787. DOI: 10.1103/PhysRevLett.82.1784 (cit. on pp. 14, 16, 17, 28, 30, 41, 65).

[32] S. D. Bartlett et al. "Efficient Classical Simulation of Continuous Variable Quantum Information Processes". *Phys. Rev. Lett.* 88 (9 Feb. 2002), p. 097904. DOI: 10.1103/PhysRevLett.88.097904 (cit. on pp. 14, 15, 29).

[33] D. Gottesman. "The Heisenberg representation of quantum computers". In: *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics* (Cambridge, USA). Ed. by S. Corney. International Press, 1998, p. 32. arXiv: quant-ph/9807006 (cit. on p. 15).

[34] B. W. Shore and P. L. Knight. "The Jaynes-Cummings Model". *Journal of Modern Optics* 40.7 (1993), pp. 1195–1238. DOI: 10.1080/09500349314551321 (cit. on p. 18).

[35] J. Gauthier et al. "A brief history of bioinformatics". *Briefings in Bioinformatics* 20.6 (Aug. 2018), pp. 1981–1996. ISSN: 1477-4054. DOI: 10.1093/bib/bby063 (cit. on p. 19).

[36] C. H. Bennett. "The thermodynamics of computation—a review". *International Journal of Theoretical Physics* 21.12 (Dec. 1982), pp. 905–940. DOI: 10.1007/BF02084158 (cit. on p. 19).

[37] A. E. Hirsh and D. M. Gordon. "Distributed problem solving in social insects". *Annals of Mathematics and Artificial Intelligence* 31.1 (Oct. 2001), pp. 199–221. DOI: 10.1023/A:1016651613285 (cit. on p. 19).

[38] D. Chu, M. Prokopenko, and J. C. J. Ray. "Computation by natural systems". *Interface Focus* 8.20180058 (2018). DOI: 10.1098/rsfs.2018.0058 (cit. on p. 19).

[39] M. Fernández. *Models of Computation. An introduction to computability theory*. Undergraduate Topics in Computer Science. London, UK: Springer, 2009. DOI: 10.1007/978-1-84882-434-8 (cit. on pp. 19, 30).

[40] A. Adamatzky. "Unconventional Computing, Introduction to". In: *Encyclopedia of Complexity and Systems Science*. Ed. by R. A. Meyers. New York, NY: Springer New York, 2009, pp. 9705–9706. ISBN: 978-0-387-30440-3. DOI: 10.1007/978-0-387-30440-3_574 (cit. on p. 19).

[41] A. Adamatzky and T. Schubert. "Slime mold microfluidic logical gates". *Materials Today* 17.2 (2014), pp. 86–91. ISSN: 1369-7021. DOI: 10.1016/j.mattod.2014.01.018 (cit. on p. 19).

[42] A. Adamatzky. "Towards fungal computer". *Interface Focus* 8.20180029 (2018). DOI: http://doi.org/10.1098/rsfs.2018.0029 (cit. on p. 19).

[43] R. Blümel et al. "Power-optimal, stabilized entangling gate between trapped-ion qubits". *npj Quantum Information* 7.1 (Oct. 2021), p. 147. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00489-w (cit. on pp. 19, 38).

[44] X. Gu et al. "Microwave photonics with superconducting quantum circuits". *Physics Reports* 718-719 (2017). Microwave photonics with superconducting quantum circuits, pp. 1–102. ISSN: 0370-1573. DOI: 10.1016/j.physrep.2017.10.002 (cit. on pp. 19, 41, 45).

[45] J. Yoshikawa et al. "Invited Article: Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing". *APL Photonics* 1.6 (2016), p. 060801. DOI: 10.1063/1.4962732 (cit. on p. 19).

[46] P. Wang et al. "Single ion qubit with estimated coherence time exceeding one hour". *Nature Communications* 12.1 (Jan. 2021), p. 233. ISSN: 2041-1723. DOI: 10.1038/s41467-020-20330-w (cit. on p. 19).

[47] Y. Chen et al. "Qubit Architecture with High Coherence and Fast Tunable Coupling". *Phys. Rev. Lett.* 113 (22 Nov. 2014), p. 220502. DOI: 10.1103/PhysRevLett.113.220502 (cit. on p. 19).

[48] V. Danos, E. Kashefi, and P. Panangaden. "Parsimonious and robust realizations of unitary maps in the one-way model". *Phys. Rev. A* 72 (6 Dec. 2005), p. 064301. DOI: 10.1103/PhysRevA.72.064301 (cit. on pp. 20, 28).

[49] J. Zhang et al. "Geometric theory of nonlocal two-qubit operations". *Phys. Rev. A* 67 (4 Apr. 2003), p. 042313. DOI: 10.1103/PhysRevA.67.042313 (cit. on pp. 20, 21).

[50] B. Kraus and J. I. Cirac. "Optimal creation of entanglement using a two-qubit gate". *Phys. Rev. A* 63 (6 May 2001), p. 062309. DOI: 10.1103/PhysRevA.63.062309 (cit. on p. 20).

References for Part I

[4] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Reprint 2003. Cambridge University Press, 2000 (cit. on pp. 3, 8, 20, 27).

[24] C. Gerry and P. Knight. *Introductory Quantum Optics*. Cambridge: Cambridge University Press, 2004. DOI: 10.1017/CBO9780511791239 (cit. on pp. 10, 48).

[26] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. 1st ed. Boca Raton: CRC Press, 2017. DOI: 10.1201/9781315118727 (cit. on pp. 10, 43, 46, 62, 66–70, 79, 105).

[31] S. Lloyd and S. L. Braunstein. "Quantum Computation over Continuous Variables". *Phys. Rev. Lett.* 82 (8 Feb. 1999), pp. 1784–1787. DOI: 10.1103/PhysRevLett.82.1784 (cit. on pp. 14, 16, 17, 28, 30, 41, 65).

[32] S. D. Bartlett et al. "Efficient Classical Simulation of Continuous Variable Quantum Information Processes". *Phys. Rev. Lett.* 88 (9 Feb. 2002), p. 097904. DOI: 10.1103/PhysRevLett.88.097904 (cit. on pp. 14, 15, 29).

[39] M. Fernández. *Models of Computation. An introduction to computability theory*. Undergraduate Topics in Computer Science. London, UK: Springer, 2009. DOI: 10.1007/978-1-84882-434-8 (cit. on pp. 19, 30).

[43] R. Blümel et al. "Power-optimal, stabilized entangling gate between trapped-ion qubits". *npj Quantum Information* 7.1 (Oct. 2021), p. 147. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00489-w (cit. on pp. 19, 38).

[44] X. Gu et al. "Microwave photonics with superconducting quantum circuits". *Physics Reports* 718-719 (2017). Microwave photonics with superconducting quantum circuits, pp. 1–102. ISSN: 0370-1573. DOI: 10.1016/j.physrep.2017.10.002 (cit. on pp. 19, 41, 45).

[48] V. Danos, E. Kashefi, and P. Panangaden. "Parsimonious and robust realizations of unitary maps in the one-way model". *Phys. Rev. A* 72 (6 Dec. 2005), p. 064301. DOI: 10.1103/PhysRevA.72.064301 (cit. on pp. 20, 28).

[51] J. Watrous. *The Theory of Quantum Information*. Cambridge,UK: Cambridge University Press, 2018. DOI: 10.1017/9781316848142 (cit. on pp. 25, 26).

[52] M. J. Bremner et al. "Practical Scheme for Quantum Computation with Any Two-Qubit Entangling Gate". *Phys. Rev. Lett.* 89 (24 Nov. 2002), p. 247902. DOI: 10.1103/PhysRevLett.89.247902 (cit. on pp. 28, 50).

[53] J.-L. Brylinski and R. Brylinski. *Universal quantum gates*. 2001. arXiv: quant-ph/0108062 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0108062 (cit. on p. 28).

[54] N. C. Menicucci et al. "Universal Quantum Computation with Continuous-Variable Cluster States". *Phys. Rev. Lett.* 97 (11 Sept. 2006), p. 110501. DOI: 10.1103/PhysRevLett.97.110501 (cit. on pp. 28, 30, 31, 43, 50–52, 128, 130).

[55] B. Heim et al. "Quantum programming languages". *Nature Reviews Physics* 2.12 (Dec. 2020), pp. 709–722. ISSN: 2522-5820. DOI: 10.1038/s42254-020-00245-7 (cit. on p. 30).

[56] N. Killoran et al. "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum* 3 (2019), p. 129. DOI: 10.22331/q-2019-03-11-129. arXiv: 1804.03159 (cit. on p. 30).

[57] M. S. Anis et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2021. DOI: 10.5281/zenodo.2573505 (cit. on p. 30).

[58] J. Anders et al. "Ancilla-driven universal quantum computation". *Phys. Rev. A* 82 (2 Aug. 2010), p. 020301. DOI: 10.1103/PhysRevA.82.020301 (cit. on pp. 30, 31, 33, 34, 44, 49, 74).

[59] W. J. Munro et al. "Qubus computation". In: *Quantum Communications and Quantum Imaging IV*. Ed. by R. E. Meyers, Y. Shih, and K. S. Deacon. Vol. 6305. International Society for Optics and Photonics. SPIE, 2006, pp. 78–86. DOI: 10.1117/12.675938 (cit. on pp. 30, 31).

[60] T. Albash and D. A. Lidar. "Adiabatic quantum computation". *Rev. Mod. Phys.* 90 (1 Jan. 2018), p. 015002. DOI: 10.1103/RevModPhys.90.015002 (cit. on p. 30).

[61] C. Nayak et al. "Non-Abelian anyons and topological quantum computation". *Rev. Mod. Phys.* 80 (3 Sept. 2008), pp. 1083–1159. DOI: 10.1103/RevModPhys.80.1083 (cit. on p. 30).

[62] D. Deutsch. "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117. DOI: 10.1098/rspa.1985.0070 (cit. on p. 30).

[63] R. Raussendorf and H. J. Briegel. "A One-Way Quantum Computer". *Phys. Rev. Lett.* 86 (22 May 2001), pp. 5188–5191. DOI: 10.1103/PhysRevLett.86.5188 (cit. on pp. 30, 74, 113).

[64] H. J. Briegel et al. "Measurement-based quantum computation". *Nature Physics* 5 (19-26 2009). DOI: 10.1038/nphys1157 (cit. on p. 30).

[65] P. Walther et al. "Experimental one-way quantum computing". *Nature* 434.7030 (Mar. 2005), pp. 169–176. ISSN: 1476-4687. DOI: 10.1038/nature03347 (cit. on p. 30).

[66] X. Zhou, D. W. Leung, and I. L. Chuang. "Methodology for quantum logic gate construction". *Phys. Rev. A* 62 (5 Oct. 2000), p. 052316. DOI: 10.1103/PhysRevA.62.052316 (cit. on pp. 30, 31).

[67] H. J. Briegel and R. Raussendorf. "Persistent Entanglement in Arrays of Interacting Particles". *Phys. Rev. Lett.* 86 (5 Jan. 2001), pp. 910–913. DOI: 10.1103/PhysRevLett.86.910 (cit. on p. 30).

[68] N. C. Menicucci. "Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States". *Phys. Rev. Lett.* 112 (12 Mar. 2014), p. 120504. DOI: 10.1103/PhysRevLett.112.120504 (cit. on pp. 31, 44).

[69] H. Vahlbruch et al. "Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency". *Phys. Rev. Lett.* 117 (11 Sept. 2016), p. 110801. DOI: 10.1103/PhysRevLett.117.110801 (cit. on pp. 31, 102).

[70] D. Gottesman, A. Kitaev, and J. Preskill. "Encoding a qubit in an oscillator". *Phys. Rev. A* 64 (1 June 2001), p. 012310. DOI: 10.1103/PhysRevA.64.012310 (cit. on p. 31).

[71] M. V. Larsen et al. "Fault-Tolerant Continuous-Variable Measurement-based Quantum Computation Architecture". *PRX Quantum* 2 (3 Aug. 2021), p. 030325. DOI: 10.1103/PRXQuantum.2.030325 (cit. on p. 31).

[72] T. P. Spiller et al. "Quantum computation by communication". *New Journal of Physics* 8.2 (Feb. 2006), pp. 30–30. DOI: 10.1088/1367-2630/8/2/030 (cit. on p. 31).

[73] C. Gerry and P. Knight. "Derivation of the effective Hamiltonian for dispersive (far off-resonant) interactions". In: *Introductory Quantum Optics*. Cambridge University Press, 2004, pp. 308–311. DOI: 10.1017/CBO9780511791239.014 (cit. on pp. 31, 38, 39, 48).

[74] E. Kashefi et al. "Twisted Graph States for Ancilla-driven Universal Quantum Computation". *Electronic Notes in Theoretical Computer Science* 249 (2009). Proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009), pp. 307–331. ISSN: 1571-0661. DOI: 10.1016/j.entcs.2009.07.096 (cit. on pp. 31, 34).

[75] J. Anders et al. "Ancilla-driven quantum computation with twisted graph states". *Theoretical Computer Science* 430 (2012). Mathematical Foundations of Programming Semantics (MFPS XXV), pp. 51–72. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2012.02.007 (cit. on pp. 31–33, 46).

[76] T. J. Proctor and V. Kendon. "Hybrid quantum computing with ancillas". *Contemporary Physics* 57.4 (2016), pp. 459–476. DOI: 10.1080/00107514.2016.1152700 (cit. on pp. 31, 33, 34, 45, 50).

[77] T. Proctor et al. "Ancilla-driven quantum computation for qudits and continuous variables". *Phys. Rev. A* 95 (5 May 2017), p. 052317. DOI: 10.1103/PhysRevA.95.052317 (cit. on pp. 31, 33, 44, 46).

[78] T. J. Proctor, E. Andersson, and V. Kendon. "Universal quantum computation by the unitary control of ancilla qubits and using a fixed ancilla-register interaction". *Phys. Rev. A* 88 (4 Oct. 2013), p. 042330. DOI: 10.1103/PhysRevA.88.042330 (cit. on pp. 31, 32, 34, 35, 44, 46).

[79] T. J. Proctor and V. Kendon. "Minimal ancilla mediated quantum computation". *EPJ Quantum Technology* 1 (13 2014). DOI: 10.1140/epjqt13 (cit. on pp. 31, 34, 44, 46).

[80] A. J. Roncaglia et al. "Sequential measurement-based quantum computing with memories". *Phys. Rev. A* 83 (6 June 2011), p. 062332. DOI: 10.1103/PhysRevA.83.062332 (cit. on pp. 33–35).

[81] C. B. Gallagher and A. Ferraro. "Relative resilience to noise of standard and sequential approaches to measurement-based quantum computation". *Phys. Rev. A* 97 (5 May 2018), p. 052305. DOI: 10.1103/PhysRevA.97.052305 (cit. on pp. 33, 46).

[82] M. Giulian. "Continuous and Hybrid Variable Ancilla Driven Quantum Computation". MA thesis. University of St Andrews, 2015 (cit. on pp. 35, 47).

[83] X. Wang. "Continuous-variable and hybrid quantum gates". *Journal of Physics A: Mathematical and General* 34.44 (Oct. 2001), pp. 9577–9584. DOI: 10.1088/0305-4470/34/44/316 (cit. on p. 35).

[84] G. Kurizki et al. "Quantum technologies with hybrid systems". *Proceedings of the National Academy of Sciences* 112.13 (2015), pp. 3866–3873. ISSN: 0027-8424. DOI: 10.1073/pnas.1419326112 (cit. on pp. 38, 39, 41, 42, 45).

[85] Q. Cai, J. Liao, and Q. Zhou. "Entangling two microwave modes via optomechanics". *Phys. Rev. A* 100 (4 Oct. 2019), p. 042330. DOI: 10.1103/PhysRevA.100.042330 (cit. on p. 38).

[86] M. D. LaHaye et al. "Nanomechanical measurements of a superconducting qubit". *Nature* 459.7249 (June 2009), pp. 960–964. ISSN: 1476-4687. DOI: 10.1038/nature08093 (cit. on p. 38).

[87] W. K. Hensinger et al. "Ion trap transducers for quantum electromechanical oscillators". *Phys. Rev. A* 72 (4 Oct. 2005), p. 041405. DOI: 10.1103/PhysRevA.72.041405 (cit. on p. 38).

[88] F. Lenzini et al. "Integrated photonic platform for quantum information with continuous variables". *Science Advances* 4.12 (2018), eaat9331. DOI: 10.1126/sciadv.aat9331 (cit. on p. 38).

[89] S. Slussarenko and G. J. Pryde. "Photonic quantum information processing: A concise review". *Applied Physics Reviews* 6.4 (2019), p. 041303. DOI: 10.1063/1.5115814 (cit. on p. 38).

[90] J. C. Bardin, D. H. Slichter, and D. J. Reilly. "Microwaves in Quantum Computing". *IEEE Journal of Microwaves* 1.1 (2021), pp. 403–427. DOI: 10.1109/JMW.2020.3034071 (cit. on p. 38).

[91] A. Blais et al. "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation". *Phys. Rev. A* 69 (6 June 2004), p. 062320. DOI: 10.1103/PhysRevA.69.062320 (cit. on p. 38).

[92] M. Kjaergaard et al. "Superconducting Qubits: Current State of Play". *Annual Review of Condensed Matter Physics* 11.1 (2020), pp. 369–395. DOI: 10.1146/annurev-conmatphys-031119-050605 (cit. on p. 38).

[93] F. Arute et al. "Quantum supremacy using a programmable superconducting processor". *Nature* 574.7779 (Oct. 2019), pp. 505–510. ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5 (cit. on p. 38).

[94] F. Arute et al. "Hartree-Fock on a superconducting qubit quantum computer". *Science* 369.6507 (2020), pp. 1084–1089. DOI: 10.1126/science.abb9811 (cit. on p. 38).

[95] G. J. Mooney et al. "Generation and verification of 27-qubit Greenberger-Horne-Zeilinger states in a superconducting quantum computer". *Journal of Physics Communications* 5.9 (Sept. 2021), p. 095004. DOI: 10.1088/2399-6528/ac1df7 (cit. on p. 38).

[96] J. I. Cirac and P. Zoller. "Quantum Computations with Cold Trapped Ions". *Phys. Rev. Lett.* 74 (20 May 1995), pp. 4091–4094. DOI: 10.1103/PhysRevLett.74.4091 (cit. on p. 38).

[97] I. Pogorelov et al. "Compact Ion-Trap Quantum Computing Demonstrator". *PRX Quantum* 2 (2 June 2021), p. 020343. DOI: 10.1103/PRXQuantum.2.020343 (cit. on p. 38).

[98] C. J. Ballance et al. "High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits". *Phys. Rev. Lett.* 117 (6 Aug. 2016), p. 060504. DOI: 10.1103/PhysRevLett.117.060504 (cit. on p. 38).

[99] K. Wright et al. "Benchmarking an 11-qubit quantum computer". *Nature Communications* 10.1 (Nov. 2019), p. 5464. ISSN: 2041-1723. DOI: 10.1038/s41467-019-13534-2 (cit. on p. 38).

[100] R. T. Sutherland and R. Srinivas. "Universal hybrid quantum computing in trapped ions". *Phys. Rev. A* 104 (3 Sept. 2021), p. 032609. DOI: 10.1103/PhysRevA.104.032609 (cit. on p. 38).

[101] L. Hu et al. "Quantum error correction and universal gate set operation on a binomial bosonic logical qubit". *Nature Physics* 15.5 (May 2019), pp. 503–508. ISSN: 1745-2481. DOI: 10.1038/s41567-018-0414-3 (cit. on p. 38).

[102] S. Rosenblum et al. "A CNOT gate between multiphoton qubits encoded in two cavities". *Nature Communications* 9.1 (Feb. 2018), p. 652. ISSN: 2041-1723. DOI: 10.1038/s41467-018-03059-5 (cit. on p. 38).

[103] T. Hillmann et al. "Universal Gate Set for Continuous-Variable Quantum Computation with Microwave Circuits". *Phys. Rev. Lett.* 125 (16 Oct. 2020), p. 160501. DOI: 10.1103/PhysRevLett.125.160501 (cit. on p. 38).

[104] C. Bonizzoni et al. "Storage and retrieval of microwave pulses with molecular spin ensembles". *npj Quantum Information* 6.68 (2020). DOI: 10.1038/s41534-020-00296-9 (cit. on p. 38).

[105] C. Bonizzoni, A. Ghirri, and M. Affronte. "Coherent coupling of molecular spins with microwave photons in planar superconducting resonators". *Advances in Physics: X* 3.1 (2018), p. 1435305. DOI: 10.1080/23746149.2018.1435305 (cit. on p. 38).

[106] N. Gisin et al. "Quantum cryptography". *Rev. Mod. Phys.* 74 (1 Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145 (cit. on p. 38).

[107] S. Kolkowitz et al. "Coherent Sensing of a Mechanical Resonator with a Single-Spin Qubit". *Science* 335.6076 (2012), pp. 1603–1606. DOI: 10.1126/science.1216821 (cit. on pp. 38, 39, 45).

[108] O. Arcizet et al. "A single nitrogen-vacancy defect coupled to a nanomechanical oscillator". *Nature Physics* 7.11 (Nov. 2011), pp. 879–883. ISSN: 1745-2481. DOI: 10.1038/nphys2070 (cit. on pp. 38, 39, 45).

[109] A. A. Clerk et al. "Hybrid quantum systems with circuit quantum electrodynamics". *Nature Physics* 16.3 (Mar. 2020), pp. 257–267. ISSN: 1745-2481. DOI: 10.1038/s41567-020-0797-9 (cit. on p. 38).

[110] C. Gerry and P. Knight. "Emission and absorption of radiation by atoms". In: *Introductory Quantum Optics*. Cambridge University Press, 2004, pp. 74–114. DOI: 10.1017/CBO9780511791239.004 (cit. on p. 38).

[111] A. Blais et al. "Circuit quantum electrodynamics". *Rev. Mod. Phys.* 93 (2 May 2021), p. 025005. DOI: 10.1103/RevModPhys.93.025005 (cit. on pp. 39, 41, 45).

[112] G. M. Reuther et al. "Two-resonator circuit quantum electrodynamics: Dissipative theory". *Phys. Rev. B* 81 (14 Apr. 2010), p. 144510. DOI: 10.1103/PhysRevB.81.144510 (cit. on pp. 39, 41, 45).

[113] M. Boissonneault, J. M. Gambetta, and A. Blais. "Dispersive regime of circuit QED: Photon-dependent qubit dephasing and relaxation rates". *Phys. Rev. A* 79 (1 Jan. 2009), p. 013819. DOI: 10.1103/PhysRevA.79.013819 (cit. on pp. 39, 45).

[114] A. Blais et al. "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation". *Phys. Rev. A* 69 (6 June 2004), p. 062320. DOI: 10.1103/PhysRevA.69.062320 (cit. on pp. 39, 45).

[115] L. Tian et al. "Interfacing Quantum-Optical and Solid-State Qubits". *Phys. Rev. Lett.* 92 (24 June 2004), p. 247902. DOI: 10.1103/PhysRevLett.92.247902 (cit. on pp. 39, 45).

[116] A. Wallraff et al. "Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics". *Nature* 431 (162-167 2004). DOI: 10.1038/nature02851 (cit. on pp. 39, 45).

[117] M. Wallquist et al. "Hybrid quantum devices and quantum engineering". *Physica Scripta* T137 (Dec. 2009), p. 014001. DOI: 10.1088/0031-8949/2009/t137/014001 (cit. on pp. 39, 45).

[118] M. J. Bremner et al. "Practical Scheme for Quantum Computation with Any Two-Qubit Entangling Gate". *Phys. Rev. Lett.* 89 (24 Nov. 2002), p. 247902. DOI: 10.1103/PhysRevLett.89.247902 (cit. on p. 41).

[119] M. Mariantoni et al. "Two-resonator circuit quantum electrodynamics: A superconducting quantum switch". *Phys. Rev. B* 78 (10 Sept. 2008), p. 104508. DOI: 10.1103/PhysRevB.78.104508 (cit. on pp. 41, 45).

[120] L. Ortiz-Gutiérrez et al. "Continuous variables quantum computation over the vibrational modes of a single trapped ion". *Optics Communications* 397 (2017), pp. 166–174. ISSN: 0030-4018. DOI: 10.1016/j.optcom.2017.04.011 (cit. on p. 42).

[121] D. Babusci, G. Dattoli, and D. Sacchetti. "The Airy transform and associated polynomials". *Open Physics* 9.6 (2011), pp. 1381–1386. DOI: 10.2478/s11534-011-0057-9 (cit. on pp. 50, 128).

[122] D. V. Widder. "The Airy Transform". *The American Mathematical Monthly* 86.4 (2022/03/24/1979). Full publication date: Apr., 1979, pp. 271–277. DOI: 10.2307/2320744 (cit. on pp. 50, 128).

References for Part II

[18] A. Peres. "Separability Criterion for Density Matrices". *Phys. Rev. Lett.* 77 (8 Aug. 1996), pp. 1413–1415. DOI: 10.1103/PhysRevLett.77.1413 (cit. on pp. 9, 74).

[19] M. Horodecki, P. Horodecki, and R. Horodecki. "Separability of mixed states: necessary and sufficient conditions". *Physics Letters A* 223.1 (1996), pp. 1–8. ISSN: 0375-9601. DOI: 10.1016/S0375-9601(96)00706-2 (cit. on pp. 9, 74, 76, 77).

[20] P. Horodecki. "Separability criterion and inseparable mixed states with positive partial transposition". *Physics Letters A* 232.5 (1997), pp. 333–339. ISSN: 0375-9601. DOI: 10.1016/S0375-9601(97)00416-7 (cit. on pp. 9, 74).

[26] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. 1st ed. Boca Raton: CRC Press, 2017. DOI: 10.1201/9781315118727 (cit. on pp. 10, 43, 46, 62, 66–70, 79, 105).

[31] S. Lloyd and S. L. Braunstein. "Quantum Computation over Continuous Variables". *Phys. Rev. Lett.* 82 (8 Feb. 1999), pp. 1784–1787. DOI: 10.1103/PhysRevLett.82.1784 (cit. on pp. 14, 16, 17, 28, 30, 41, 65).

[58] J. Anders et al. "Ancilla-driven universal quantum computation". *Phys. Rev. A* 82 (2 Aug. 2010), p. 020301. DOI: 10.1103/PhysRevA.82.020301 (cit. on pp. 30, 31, 33, 34, 44, 49, 74).

[63] R. Raussendorf and H. J. Briegel. "A One-Way Quantum Computer". *Phys. Rev. Lett.* 86 (22 May 2001), pp. 5188–5191. DOI: 10.1103/PhysRevLett.86.5188 (cit. on pp. 30, 74, 113).

[69] H. Vahlbruch et al. "Detection of 15 dB Squeezed States of Light and their Application for the Absolute Calibration of Photoelectric Quantum Efficiency". *Phys. Rev. Lett.* 117 (11 Sept. 2016), p. 110801. DOI: 10.1103/PhysRevLett.117.110801 (cit. on pp. 31, 102).

[123] P. Hyllus and J. Eisert. "Optimal entanglement witnesses for continuous-variable systems". *New J. Phys.* 51.8 (2006) (cit. on pp. 57, 74, 76–80, 85, 86, 89, 96, 97, 101, 103, 112, 114).

[124] L. Cohen. "The Weyl Operator". In: *The Weyl Operator and its Generalization*. Basel: Springer Basel, 2013, pp. 25–46. ISBN: 978-3-0348-0294-9. DOI: 10.1007/978-3-0348-0294-9_3 (cit. on p. 66).

[125] J. Williamson. "On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems". *American Journal of Mathematics* 58.1 (1936), pp. 141–163. ISSN: 00029327, 10806377 (cit. on p. 67).

[126] K. Ikramov. "On the Symplectic Eigenvalues of Positive Definite Matrices." *MoscowUniv.Comput.Math.Cybern.* 42 (2018), pp. 1–4. DOI: 10.3103/S0278641918010041 (cit. on p. 67).

[127] S. L. Braunstein. "Squeezing as an irreducible resource". *Phys. Rev. A* 71 (5 May 2005). DOI: 10.1103/PhysRevA.71.055801 (cit. on p. 67).

[128] P. van Loock. "Quantum Communication with Continuous Variables". *Fortschritte der Physik* 50.12 (2002), pp. 1177–1372. DOI: 10.1002/1521-3978(200212)50:12<1177::AID-PROP1177>3.0.CO;2-T (cit. on pp. 68, 108).

[129] M. Reck et al. "Experimental realization of any discrete unitary operator". *Phys. Rev. Lett.* 73 (1 July 1994), pp. 58–61. DOI: 10.1103/PhysRevLett.73.58 (cit. on pp. 68, 108).

[130] Á. Rivas and S. F. Huelga. *Quantum Open Systems. An introduction*. 1st ed. Berlin, Heidelberg: Springer, 2012. DOI: 10.1007/978-3-642-23354-8 (cit. on p. 74).

[131] S. Matern et al. "Coherent backaction between spins and an electronic bath: Non-Markovian dynamics and low-temperature quantum thermodynamic electron cooling". *Phys. Rev. B* 100 (13 Oct. 2019), p. 134308. DOI: 10.1103/PhysRevB.100.134308 (cit. on p. 74).

[132] K. B. Arnardottir et al. "Multimode Organic Polariton Lasing". *Phys. Rev. Lett.* 125 (23 Dec. 2020), p. 233603. DOI: 10.1103/PhysRevLett.125.233603 (cit. on p. 74).

[133] L. Hollberg et al. "Quantum optics and quantum entanglement". *Journal of Optics B: Quantum and Semiclassical Optics* 5.4 (Aug. 2003), pp. 457–457. DOI: 10.1088/1464-4266/5/4/001 (cit. on p. 74).

[134] D. B. Horoshko et al. "Nonlinear Mach–Zehnder interferometer with ultrabroadband squeezed light". *Journal of Modern Optics* 67.1 (2020), pp. 41–48. DOI: 10.1080/09500340.2019.1674394 (cit. on p. 74).

[135] M. J. Padgett and R. W. Boyd. "An introduction to ghost imaging: quantum and classical". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 375.2099 (2017), p. 20160233. DOI: 10.1098/rsta.2016.0233 (cit. on p. 74).

[136] M. Thornton et al. "Continuous-variable quantum digital signatures over insecure channels". *Phys. Rev. A* 99 (3 Mar. 2019), p. 032341. DOI: 10.1103/PhysRevA.99.032341 (cit. on p. 74).

[137] M. Pereira, M. Curty, and K. Tamaki. "Quantum key distribution with flawed and leaky sources". *npj Quantum Information* 5.1 (July 2019), p. 62. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0180-9 (cit. on p. 74).

[138] J. Yin et al. "Entanglement-based secure quantum cryptography over 1,120 kilometres". *Nature* 582.7813 (June 2020), pp. 501–505. DOI: 10.1038/s41586-020-2401-y (cit. on p. 74).

[139] Q. Zhuang and J. H. Shapiro. "Ultimate Accuracy Limit of Quantum Pulse-Compression Ranging". *Phys. Rev. Lett.* 128 (1 Jan. 2022), p. 010501. DOI: 10.1103/PhysRevLett.128.010501 (cit. on p. 74).

[140] O. Gühne and G. Tóth. "Entanglement detection". *Physics Reports* 474.1 (2009), pp. 1–75. ISSN: 0370-1573. DOI: 10.1016/j.physrep.2009.02.004 (cit. on pp. 75, 76, 139).

[141] M. Paraschiv et al. "Proving genuine multiparticle entanglement from separable nearest-neighbor marginals". *Phys. Rev. A* 98 (6 Dec. 2018), p. 062102. DOI: 10.1103/PhysRevA.98.062102 (cit. on pp. 77, 95, 96, 103, 105, 106, 112).

[142] B. M. Terhal. "Bell inequalities and the separability criterion". *Physics Letters A* 271.5 (2000), pp. 319–326. ISSN: 0375-9601. DOI: 10.1016/S0375-9601(00)00401-1 (cit. on p. 76).

[143] M. Lewenstein et al. "Optimization of entanglement witnesses". *Phys. Rev. A* 62 (5 Oct. 2000), p. 052310. DOI: 10.1103/PhysRevA.62.052310 (cit. on p. 77).

[144] R. E. Edwards. *Functional Analysis; Theory and Applications*. The Hahn-Banach theorem is presented in analytic form in section 1.7 and in geometric form in chapter 2. USA: Holt, Rinehart and Winston, 1965 (cit. on p. 77).

[145] R. F. Werner and M. M. Wolf. "Bound Entangled Gaussian States". *Phys. Rev. Lett.* 86 (16 Apr. 2001), pp. 3658–3661. DOI: 10.1103/PhysRevLett.86.3658 (cit. on pp. 79, 103, 140).

[146] H. F. Hofmann and S. Takeuchi. "Violation of local uncertainty relations as a signature of entanglement". *Phys. Rev. A* 68 (3 Sept. 2003), p. 032103. DOI: 10.1103/PhysRevA.68.032103 (cit. on p. 79).

[147] R. Simon. "Peres-Horodecki Separability Criterion for Continuous Variable Systems". *Phys. Rev. Lett.* 84 (12 Mar. 2000), pp. 2726–2729. DOI: 10.1103/PhysRevLett.84.2726 (cit. on p. 79).

[148] B. Gärtner and J. Matousek. *Approximation Algorithms and Semidefinite Programming*. 1st ed. Berlin, Heidelberg: Springer, 2012. ISBN: 978-3-642-22015-9. DOI: 10.1007/978-3-642-22015-9 (cit. on pp. 80–83, 114).

[149] S. Boyd and L. Vandenberghe. *Convex Optimization*. Relevant sections: Sec. 5.1; Sec. 5.2; Sec. 5.4 on the min-max characterisation of Lagrangian duality (p.237); Sec. 5.9.1 on the Lagrange Dual of SDPs, in particular Example 5.11 (p.265) Sections and pages referenced obtained through the URL provided. Cambridge University Press, 2004. DOI: 10.1017/CBO9780511804441 (cit. on pp. 80, 82, 83, 105).

[150] A. Klyachko. *Quantum marginal problem and representations of the symmetric group*. 2004. DOI: 10.48550/arXiv.quant-ph/0409113. arXiv: quant-ph/0409113 [quant-ph] (cit. on p. 95).

[151] C. Schilling. "The Quantum Marginal Problem". In: *Proceedings of the Conference QMath 12*. Berlin, Germany (Sep. 2013), 2014. DOI: 10.48550/arXiv.1404.1085. arXiv: quant-ph/1404.1085 [quant-ph] (cit. on p. 95).

[152] L. Chen et al. "Role of correlations in the two-body-marginal problem". *Phys. Rev. A* 90 (4 Oct. 2014), p. 042314. DOI: 10.1103/PhysRevA.90.042314 (cit. on pp. 95, 96, 112).

[153] N. Miklin, T. Moroder, and O. Gühne. "Multiparticle entanglement as an emergent phenomenon". *Phys. Rev. A* 93 (2 Feb. 2016), p. 020104. DOI: 10.1103/PhysRevA.93.020104 (cit. on pp. 95, 96, 103, 106, 112).

[154] M. Mičuda et al. "Verifying genuine multipartite entanglement of the whole from its separable parts". *Optica* 6.7 (July 2019), pp. 896–901. DOI: 10.1364/OPTICA.6.000896 (cit. on pp. 95, 96, 103, 106).

[155] T. O'Connor. "Emergent Properties". In: *The Stanford Encyclopedia of Philosophy*. Ed. by E. N. Zalta. Winter 2021. Metaphysics Research Lab, Stanford University, 2021 (cit. on p. 95).

[156] D. Galas. *Systems biology*. https://www.britannica.com/science/systems-biology. Encyclopedia entry, Accessed 18 March 2022 (cit. on p. 95).

[157] G. M. Hodgson. "The Concept of Emergence in Social Sciences: Its History and Importance". *Emergence* 2.4 (2000), pp. 65–77. DOI: 10.1207/S15327000EM0204_08 (cit. on p. 95).

[158] V. Nordgren et al. "Convicting emergent multipartite entanglement with evidence from a partially blind witness" (2021). arXiv: 2103.07327 [quant-ph] (cit. on p. 101).

[159] J. Löfberg. "YALMIP : a toolbox for modeling and optimization in MATLAB". In: *2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No.04CH37508)*. 2004, pp. 284–289. DOI: 10.1109/CACSD.2004.1393890 (cit. on p. 101).

[160] J. F. Sturm. "Using SeDuMi 1.02, A Matlab toolbox for optimization over symmetric cones". *Optimization Methods and Software* 11.1-4 (1999). Version 1.05 available from http://fewcal.kub.nl/sturm, pp. 625–653. DOI: 10.1080/10556789908805766 (cit. on p. 101).

[161] MOSEK ApS. *The MOSEK optimization toolbox for MATLAB manual. Version 9.2*. 2019. URL: http://docs.mosek.com/9.2/toolbox/index.html (cit. on p. 101).

[162] J. DiGuglielmo et al. "Experimental Unconditional Preparation and Detection of a Continuous Bound Entangled State of Light". *Phys. Rev. Lett.* 107 (24 Dec. 2011), p. 240503. DOI: 10.1103/PhysRevLett.107.240503 (cit. on p. 103).

[163] L. Vandenberghe and S. Boyd. "Semidefinite Programming". *SIAM Review* 38.1 (1996), pp. 49–95. DOI: 10.1137/1038003 (cit. on p. 105).

[164] A. Serafini, G. Adesso, and F. Illuminati. "Unitarily localizable entanglement of Gaussian states". *Phys. Rev. A* 71 (3 Mar. 2005), p. 032349. DOI: 10.1103/PhysRevA.71.032349 (cit. on p. 108).

[165] S. Pirandola, A. Serafini, and S. Lloyd. "Correlation matrices of two-mode bosonic systems". *Phys. Rev. A* 79 (5 May 2009), p. 052327. DOI: 10.1103/PhysRevA.79.052327 (cit. on p. 108).

[166] O. Leskovjanová et al. *[Work in progress]*. 2022 (cit. on pp. 113, 114).

[167] K. Kreis and P. van Loock. "Classifying, quantifying, and witnessing qudit-qumode hybrid entanglement". *Phys. Rev. A* 85 (3 Mar. 2012), p. 032307. DOI: 10.1103/PhysRevA.85.032307 (cit. on p. 113).

[168] G. Massé et al. "Implementable hybrid entanglement witness". *Phys. Rev. A* 102 (6 Dec. 2020), p. 062406. DOI: 10.1103/PhysRevA.102.062406 (cit. on p. 113).

[169] L. Kuepfer, U. Sauer, and P. A. Parrilo. "Efficient classification of complete parameter regions based on semidefinite programming". *BMC Bioinformatics* 8.1 (Jan. 2007), p. 12. ISSN: 1471-2105. DOI: 10.1186/1471-2105-8-12 (cit. on p. 114).

References for Appendices

[54] N. C. Menicucci et al. "Universal Quantum Computation with Continuous-Variable Cluster States". *Phys. Rev. Lett.* 97 (11 Sept. 2006), p. 110501. DOI: 10.1103/PhysRevLett.97.110501 (cit. on pp. 28, 30, 31, 43, 50–52, 128, 130).

[121] D. Babusci, G. Dattoli, and D. Sacchetti. "The Airy transform and associated polynomials". *Open Physics* 9.6 (2011), pp. 1381–1386. DOI: 10.2478/s11534-011-0057-9 (cit. on pp. 50, 128).

[122] D. V. Widder. "The Airy Transform". *The American Mathematical Monthly* 86.4 (2022/03/24/1979). Full publication date: Apr., 1979, pp. 271–277. DOI: 10.2307/2320744 (cit. on pp. 50, 128).

[140] O. Gühne and G. Tóth. "Entanglement detection". *Physics Reports* 474.1 (2009), pp. 1–75. ISSN: 0370-1573. DOI: 10.1016/j.physrep.2009.02.004 (cit. on pp. 75, 76, 139).

[145] R. F. Werner and M. M. Wolf. "Bound Entangled Gaussian States". *Phys. Rev. Lett.* 86 (16 Apr. 2001), pp. 3658–3661. DOI: 10.1103/PhysRevLett.86.3658 (cit. on pp. 79, 103, 140).

[170] E. B. Dynkin. "Selected papers of E. B. Dynkin with commentary." In: ed. by G. S. A.A. Yushkevich and A. Onishchik. American Mathematical Society, 2000 (cit. on p. 117).

[171] R. Achilles and A. Bonfiglioli. "The early proofs of the theorem of Campbell, Baker, Hausdorff, and Dynkin". *Archive for History of Exact Sciences* 66.3 (May 2012), pp. 295–358. DOI: 10.1007/s00407-012-0095-8 (cit. on p. 117).

[172] R. Stratonovich. ""On a Method of Calculating Quantum Distribution Functions"". Russian. *Doklady Akad. Nauk S.S.S.R.* 115 (1097 1957). translation: Soviet Phys. Doklady 2, 416 (1958) (cit. on p. 118).

[173] J. Hubbard. "Calculation of Partition Functions". *Phys. Rev. Lett.* 3 (2 July 1959), pp. 77–78. DOI: 10.1103/PhysRevLett.3.77 (cit. on p. 118).