Gaussian and Covariant Processes In Discrete And Continuous Variable Quantum Information

Hulya Yadsan-Appleby

Department of Physics and Astronomy, University College London

Thesis submitted in partial fulfillment
of the requirements of
University College London
for the degree of
Doctor of Philosophy

September 2012

Declaration

The studies presented in this thesis were performed by the author whilst a member of Quantum Information Group, Department of Physics and Astronomy, University College London, United Kingdom.

I, Hulya Yadsan-Appleby, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

Quantum information theory has attracted much interest in the last decade. The cause of this interest is twofold: the exciting applications that the theory promises, such as the realization of quantum computers, but also the possibility that perhaps the theory will enable us to solve the mysteries of quantum physics. In this thesis we touched a wide variety of topics with the modest motivation that perhaps, at the very least, one could get a little more insight into the conceptual problems. Our motivation led us to carry out the work presented in this thesis. We explore entanglement properties of light in the context of quantum memories. Quantum memories are set to be a crucial component of future quantum computers. In the short and medium term, the development of effective quantum memories would pave the way for the implementation of a variety of quantum information protocols. For the applications it is important to be able to store entanglement. In this thesis we investigate the storage of two mode Gaussian states of light in a QND feedback quantum memory and we examine the question whether it is better to store the state already entangled or whether is better to store a squeezed state which is only entangled after storage. We then turn to a study of some aspects of the theory of SIC-POVMs (Symmetric Informationally Complete Positive Operator Valued Measures). SIC-POVMs potentially have numerous application in quantum information. They have been constructed mathematically in every dimension ≤ 67. But it remains an open question whether they can be constructed in every finite dimension. In this thesis we describe an analogy between coherent states of a continuous variables systems and SIC-POVMs in a discrete system. We then go on to examine the Galois group of the extension field generated by the components of the SIC-POVM fiducial vector. We prove a number of theorems about this group. We then go on to actually calculate the group for a SIC-POVM in dimension 6 and show that it has a number of interesting properties. We speculate that this line of research may make a useful contribution to an eventual proof of the existence of SIC-POVMs. Finally we investigate quantum communication via spin chains. One of the key requirements for a functioning quantum information processor is the ability to transport quantum information from one location to another. Spin chains are a tool which might be used for this purpose. There have been many proposals recently which showed that under fairly general conditions spin chains communicate quantum information with arbitrarily high fidelity. However, so far there have not been many proposals addressing the problem of communicating as much quantum information as possible. In this thesis we address this problem and describe a method which achieves a high transmission rate for long spin chains.

Contents

List of Tables

List of Figures

Acknowledgements

I would like to express my gratitude to my supervisor Alessio Serafini who encouraged me to continue with my wide range of research interests, especially at times that were crucial for bringing this thesis about. I would also like to thank my family and friends for their continual support during my studies. In particular, I would like to give my thanks to Marcus who had been tormented by his conflicting roles of being a husband and a collaborator simultaneously during my studies.

Intimate

Knowledge always deceives.

It always limits the Truth, every concept and image does.

From cage to cage the caravan moves,
but I give thanks, for at each divine juncture

my wings expand
and I

touch Him more
intimately.

Meister Eckhart

CHAPTER 1

Overview

1.1. Motivation

The interpretation of quantum mechanics is one of the most controversial topics in science. There are numerous interpretations each opposing all the others. Perhaps the controversy surrounding quantum mechanics is best expressed by Christopher Fuchs in [**1**]:

> But how did this come about? What is the cause of this year-after-year sacrifice to the "great mystery?" Whatever it is, it cannot be for want of a self-ordained solution: Go to any meeting, and it is like being in a holy city in great tumult. You will find all the religions with all their priests pitted in holy war—the Bohmians [**2**], the Consistent Historians [**3**], the Transactionalists [**4**], the Spontaneous Collapseans [**5**], the Einselectionists [**6**], the Contextual Objectivists [**7**, **8**], the outright Everettics [**9**, **10**] and many more beyond that. They all declare to see the light, the ultimate light. Each tells us that if we will accept their solution as our savior, then we too will see the light.

He suggests that the reason for all this disagreement is because of a failure to realize that quantum mechanics is a theory of information:

> So, throw the existing axioms of quantum mechanics away and start afresh! But how to proceed? I myself see no alternative but to contemplate deep and hard the tasks, the techniques, and the implications of quantum information theory. The reason is simple, and I think inescapable. Quantum mechanics has always

> been about information. It is just that the physics community has somehow forgotten this.

So as Fuchs sees it, quantum information is not just a branch of quantum mechanics but almost is quantum mechanics ("almost" because he does think that there is a "little more" to quantum mechanics than just information). Whether one accepts Fuchs' view or not quantum information is certainly very important.

Information theory began in the 1940s with discussions between Shannon and Turing during the Second World War [**11**]. At the time, Shannon and Turing were both engaged in military work on cryptography. However, they were both looking forward into the future and thinking about communication, computation and more speculatively artificial intellegence. Their work has had a major impact on the subsequent development of science and technology. In particular, it led to Shannon's classical information theory. Shannon gave his famous formula for measuring the amount the information:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i, \tag{1.1.1}$$

where n is the number of possible messages and p_i is the probability of the ith message. The striking fact is that this formula is nothing but the formula for classical entropy, and indeed H is often called the *Shannon entropy*. His theory gives rise to the idea that information can be viewed as something physical. Like any other physical quantity, it has a unit called the *bit* (short for "binary digits") defined to be the information content of a message consisting of a single symbol equal to 0 or 1 and occurring with equal probability.

After the pioneering work of Shannon and Turing, the field of information grew explosively. During the course of this development devices were made smaller and smaller. This led to a worry about what would happen when the size of the individual components approached atomic dimensions so that quantum effects became important. However, in the 1980s a number of people began to think that the quantum effects can be turned into an advantage [**11**]. This led to the three key

papers by Feynman which discussed the simulation of physics using a quantum computer [**12**], by Deutsch which showed that a quantum computer could be much faster than classical computer for some calculations [**13**] and by Bennett and Brassard which showed that quantum mechanics could be used to give a much more secure method for key-distribution in cryptography [**14**]. These papers founded the field of quantum information.

Quantum information exploits the distinctive features of quantum mechanics to perform tasks which would be either impossible to perform classically or which, at least, is not known how to achieve classically. In particular, quantum information exploits superposition principle. A classical bit can be only one of two states: 0 or 1. A quantum bit (a qubit) by contrast can be in an arbitrary superposition of these states $\alpha|0\rangle + \beta|1\rangle$ where α and β are arbitrary complex numbers satisfying the condition $|\alpha|^2 + |\beta|^2 = 1$. It also exploits entanglement. Suppose Alice and Bob both have a classical bit, then their bit can be in one of the 4 states: 00, 01, 10 or 11. In quantum mechanics other states are possible. For example the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This state cannot even be written as a product of two quantum superposition states of Alice's qubit and Bob's qubit. A state of this kind is said to be entangled. The possibility of entanglement plays a crucial role in quantum information.

1.2. Plan of this thesis

In this thesis we examine three particular problems that arise in quantum information theory: entanglement storage with Gaussian states in continuous variable systems, SIC-POVMs (symmetric informationally complete positive operator valued measures) and quantum communication using spin chains.

The plan of the thesis is as follows. In Part 1 we give an introduction to Gaussian states and discrete and continuous variable systems. However, we would like to point out that Section 4.3, although in the introduction, contains (unpublished)

original material. Specifically, we argue that a SIC-POVM can be regarded as a discrete analogue of a coherent state POVM (positive operator valued measure). The reason we put this in the introduction is that it is foundational and highly relevant to the elementary properties of Gaussian states. It is also one of the motivations for the work in Part 3.

In Part 2, we treat the first of our three problems. The problem is concerned with quantum memories. One important application of a quantum memory is to quantum communication over long distances. In such communication a quantum memory is used as part of a quantum repeater to counter the effects of attenuation. In our research we considered the problem whether it is better to entangle a state before storing it or whether, instead, it is better to entangle it after storing it in a quantum memory. We present our results in two sections. The first of these, Section 5.3.1, has been published. The second part of our results in Section 5.3.2 is original, unpublished work.

In Part 3 we discuss the application of Galois theory to SIC-POVMs. SIC-POVMs are interesting for many reasons. One reason is that they are a central part of the programme of Chris Fuchs mentioned above to formulate quantum mechanics as a theory of information [**15**, **16**]. This reveals many interesting properties of the known SIC-POVMs. We illustrate these properties for the case of dimension 6 in Section 6.4. A more detailed analysis of dimensions $4-16$ and $19, 24, 28, 35, 48$ can be found in our paper [**17**].

In Part 4 we discuss quantum communication using a spin chain. In Section 7.2 we present a result for maximizing the fidelity of an arbitrarily long spin chains. Although this was a significant result it was not published. This was due to the fact that we later discovered that a very similar result had already been published in [**18**]. However we think that it is worth presenting this result in this thesis since it is independent work. We then present another result in Section 7.3 which has been published in [**19**]. In this work we considered communicating qubits along a chain where the state of the chain is represented by a superposition of approximate

Gaussian wavepackets. We found a bound for maximum achievable transmission rate. This also is a significant result as it is an important problem to increase the number of signals that one can put on the chain successively to achieve efficient quantum communication.

Part 1

Introduction to Discrete and Continuous Variable Systems

CHAPTER 2

Continuous variable systems

Quantum Mechanical systems are described by operators on a Hilbert space. The state of a system is represented by a density matrix ρ which has two defining properties

$$\rho \geq 0, \tag{2.0.1}$$

$$Tr[\rho] = 1. \tag{2.0.2}$$

The first property expressed in Eq. (2.0.1) states that the eigenvalues of any density matrix ρ are equal to or greater than zero. Such matrices are said to be *positive semi-definite positive* matrices. The second property states that the trace of a density matrix is always 1.

The observables of a quantum system are described by operators. An important property of these operators is that they are *Hermitian*. An operator $\hat{A}$ is said to be Hermitian if it is equal to its Hermitian-adjoint where by the Hermitian-adjoint we mean the transpose of the matrix obtained by taking the complex conjugate of the matrix elements of the original matrix $\hat{A}$. That is

$$\hat{A} = \hat{A}^{\dagger}, \tag{2.0.3}$$

where $\hat{A}^{\dagger}$ is the Hermitian-adjoint of $\hat{A}$. This implies that the eigenvalues of a Hermitian operator are real and therefore can be interpreted as a possible outcomes of a measurement. The expectation value of a measurement of an observable $\hat{A}$ is given by

$$\langle \hat{A} \rangle = Tr[\rho \hat{A}]. \tag{2.0.4}$$

The operators describing the observables may have finitely or infinitely many eigenvectors depending on the given observable. If one is interested in the spin of an electron, for instance, then the corresponding operator will have finitely many eigenvalues. If, on the other hand one is interested in position or momentum observables then the corresponding operators will have a continuum of eigenvalues. The former case is referred to as *discrete variables* systems and the latter as *continuous variables* (CV) systems. The fundamental distinction between discrete and CV systems is that for a discrete system the Hilbert space is finite dimensional while for a CV system it is infinite dimensional and therefore hard to handle mathematically.

2.1. Hilbert space representation

CV systems can be described in terms of creation and annihilation operators. In this thesis we are concerned with the states of the radiation field with a finite number of modes. Let N be the number of modes. For the kth mode we have a creation operator $\hat{a}_k^\dagger$ and an annihilation operator $\hat{a}_k$. The creation and annihilation operators are non-Hermitian and satisfy the commutation relation

$$[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{jk}. \tag{2.1.1}$$

The product $\hat{a}_k^\dagger \hat{a}_k$ is Hermitian and it is defined to be the photon number operator $\hat{n}_k$. The eigenvectors of the number operators are the number states $|n_1, \ldots, n_N\rangle$ and they form a countable basis for an infinite dimensional Hilbert space. Therefore any other state can be written in terms of number sates $|n_1, \ldots, n_N\rangle$ such that

$$\hat{n}_k |n_1, \ldots, n_N\rangle = n_k |n_1, \ldots, n_N\rangle. \tag{2.1.2}$$

Number states can be generated by acting on the vacuum state $|0 \ldots 0\rangle$ by the creation operators $\hat{a}_k^\dagger$:

$$|n_1, \ldots, n_N\rangle = \frac{(\hat{a}_1^\dagger)^{n_1} \ldots (\hat{a}_N^\dagger)^{n_N}}{\sqrt{n_1! \ldots n_N!}} |0 \ldots 0\rangle. \tag{2.1.3}$$

The effect of creation and annihilation operators on number states is given by

$$\hat{a}_k^\dagger|n_1,\ldots,n_N\rangle = \sqrt{n_k+1}|n_1,\ldots,n_k+1,\ldots,n_N\rangle,$$
$$\hat{a}_k|n_1,\ldots,n_N\rangle = \sqrt{n_k}|n_1,\ldots,n_k-1,\ldots,n_N\rangle. \tag{2.1.4}$$

Number states are useful if one is interested in the number of photons of a given system. However in a number state the expectation values of the electric and the magnetic field strengths are zero everywhere. We would like to find a state in which the expectation values of the electric and magnetic field strengths are non zero and oscillate sinusoidally as in a classical electromagnetic wave. *Coherent states* $|\alpha_1,\ldots,\alpha_N\rangle$ have this property and such states are given by

$$|\alpha_1,\ldots,\alpha_N\rangle = e^{-\frac{1}{2}(|\alpha_1|^2+\cdots+|\alpha_N|^2)} \sum_{n_1,\ldots,n_N=0}^{\infty} \frac{\alpha_1^{n_1}\ldots\alpha_N^{n_N}}{\sqrt{n_1!\ldots n_N!}}|n_1,\ldots,n_N\rangle, \tag{2.1.5}$$

The parameters $\alpha_1,\ldots,\alpha_N$ are complex and they are related to the amplitude of the field. The expectation value of the photon number operator $\hat{n}_k$ is

$$\langle\alpha_1,\ldots,\alpha_N|\hat{n}_k|\alpha_1,\ldots,\alpha_N\rangle = |\alpha_k|^2, \tag{2.1.6}$$

and so $|\alpha_k|^2$ is the average photon number of the field. Coherent states are the eigenstates of the annihilation operator. Although they span the Hilbert space they do not form a basis because they are overcomplete (in other words, they are not linearly independent).

For every mode of a given quantized bosonic field there is a pair of operators, called quadratures $\hat{x}$ and $\hat{p}$. The quadratures are associated with the amplitude of the field, they are dimensionless and, unlike creation and annihilation operators, they can be measured. They can be expressed in terms of $\hat{a}_k$ and $\hat{a}_k^\dagger$

$$\hat{x}_k = \hat{a}_k + \hat{a}_k^\dagger, \tag{2.1.7}$$
$$\hat{p}_k = -i(\hat{a}_k - \hat{a}_k^\dagger), \tag{2.1.8}$$

with the *canonical commutation relations* (CCR)

$$[\hat{x}_j, \hat{p}_k] = 2i\delta_{jk}, \tag{2.1.9}$$

where j, k label the mode. It is often convenient to group quadratures of an n-mode field as a *canonical vector* in the following way

$$\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_n, \hat{p}_n)^T. \tag{2.1.10}$$

The CCR can be written as

$$[\hat{\mathbf{r}}_k, \hat{\mathbf{r}}_l] = 2i\Omega_{kl}, \tag{2.1.11}$$

where Ω is the *symplectic form*

$$\Omega = \bigoplus_{i=1}^{n} \omega, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.1.12}$$

Displacement Operators are an important set of unitary operators defined in terms of quadratures and the symplectic form by

$$\hat{D}_{\mathbf{r}} = e^{i\mathbf{r}^T \Omega \hat{\mathbf{r}}}, \tag{2.1.13}$$

where $\mathbf{r}$ is a real vector with $2n$ components

$$\mathbf{r} = (x_1, p_1, \ldots, x_n, p_n)^T \tag{2.1.14}$$

Alternatively, displacement operators can be expressed in terms of creation and annihilation operators as

$$\hat{D}_{\boldsymbol{\alpha}} = e^{i\boldsymbol{\alpha}^T \Omega \hat{\boldsymbol{\alpha}}}, \tag{2.1.15}$$

where $\boldsymbol{\alpha}$ is a complex vector with $2n$ components

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_1^*, \ldots, \alpha_n, \alpha_n^*)^T, \tag{2.1.16}$$

with

$$\alpha_i = x_i + ip_i, \tag{2.1.17}$$

where x_i and p_i are being the components of real vector $\mathbf{r}$ given in (2.1.14). The operator vector $\hat{\boldsymbol{\alpha}}$ is

$$\hat{\boldsymbol{\alpha}} = (\hat{a}_1, \hat{a}_1^\dagger, \ldots, \hat{a}_n, \hat{a}_n^\dagger)^T. \tag{2.1.18}$$

Fig.1 shows the action of a displacement operator $\hat{D}_{x,p}$ in phase space. It displaces the vacuum state at $(0, 0)$ to (x, p).

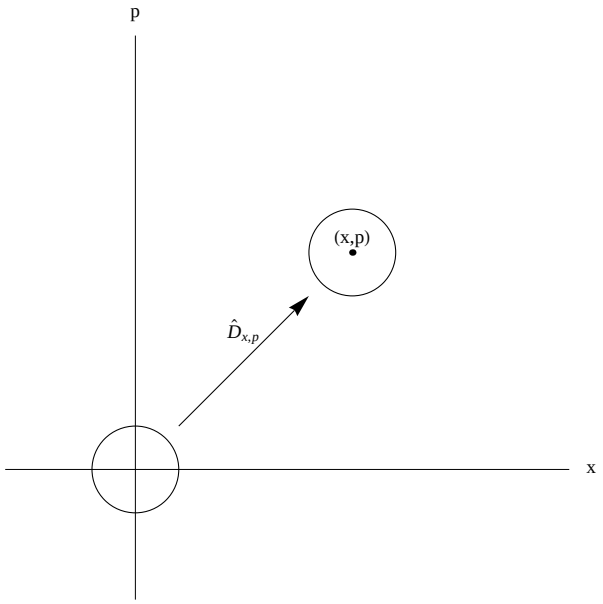


FIGURE 1. The displacement operator $\hat{D}_{x,p}$ takes the vacuum state at the origin to a point (x, p) in phase space.

All operators of the form $e^{i\theta}\hat{D}_{\mathbf{r}}$ form a group called the Weyl-Heisenberg group [**20**].

Displacement operators form a basis in the operator space that is orthogonal relative to the Hilbert-Schmidt inner product. For any two operators $\hat{A}$ and $\hat{B}$ the Hilbert-Schmidt inner product is

$$\langle \hat{A}, \hat{B} \rangle = Tr[\hat{A}^{\dagger}\hat{B}]. \tag{2.1.19}$$

If $\hat{A}$ and $\hat{B}$ are Hermitian, then the Hibert-Schmidt inner product is

$$\langle \hat{A}, \hat{B} \rangle = Tr[\hat{A}\hat{B}]. \tag{2.1.20}$$

The inner product for the displacement operators is given by

$$\langle \hat{D}_{\mathbf{r}}^{\dagger}, \hat{D}_{\mathbf{r}'} \rangle = (2\pi)^n \delta(\mathbf{r} - \mathbf{r}'). \tag{2.1.21}$$

So we have the following orthogonality condition

$$Tr[\hat{D}_{\mathbf{r}}^{\dagger}\hat{D}_{\mathbf{r}'}] = (2\pi)^n \delta(\mathbf{r} - \mathbf{r}'). \tag{2.1.22}$$

The displacement operators correspond to the shifting of the quadratures in phase space:

$$\hat{D}_{\mathbf{r}}\hat{\mathbf{r}}\hat{D}_{\mathbf{r}}^{\dagger} = \hat{\mathbf{r}} + \mathbf{r}. \tag{2.1.23}$$

In terms of the creation and annihilation operator vector $\hat{\boldsymbol{\alpha}}$:

$$\hat{D}_{\boldsymbol{\alpha}}\hat{\boldsymbol{\alpha}}^{\dagger}\hat{D}_{\boldsymbol{\alpha}}^{\dagger} = \hat{\boldsymbol{\alpha}}^{\dagger} + \boldsymbol{\alpha}^*, \tag{2.1.24}$$

and

$$\hat{D}_{\boldsymbol{\alpha}}\hat{\boldsymbol{\alpha}}\hat{D}_{\boldsymbol{\alpha}}^{\dagger} = \hat{\boldsymbol{\alpha}} + \boldsymbol{\alpha}. \tag{2.1.25}$$

2.2. Phase space representation

We now turn our attention to the phase space representation of continuous variables systems. Another way of formulating quantum mechanics with continuous variables systems is to represent the system in a real valued, $2n$-dimensional phase space. This formulation is analogous to classical mechanics. Classically a probability distribution on phase space $\Gamma(x, p)$ where x is the position and p is the momentum, describes the state of a stochastic system. The time evolution of this function is given by Liouville equation

$$\frac{\partial \Gamma}{\partial t} = \{H, \Gamma\}, \tag{2.2.1}$$

where H is the classical Hamiltonian and $\{.,.\}$ is the Poisson bracket:

$$\{H, \Gamma\} = \frac{\partial H}{\partial x}\frac{\partial \Gamma}{\partial p} - \frac{\partial \Gamma}{\partial x}\frac{\partial H}{\partial p}. \tag{2.2.2}$$

In analogy to a classical mechanical probability distribution $\Gamma(x, p)$, there are functions on phase space that can be interpreted as a probability distribution for quantum-mechanical continuous variable systems. One such function is the Husimi function discovered by [**21**] and studied extensively in connection with quantum mechanical systems. It can be shown that the Husimi function is a positive valued function and can be interpreted as a probability distribution for an arbitrary quantum state (see references [**22**–**24**] and the references cited therein). In this thesis, however, we are interested in a quasi-probabability distribution, the Wigner function. The Wigner function may have negative values and this is why it is referred to as a quasi-probability distribution. However, for Gaussian states the Wigner function is always positive as will be explained in the next section.

The Wigner function is defined to be the Weyl transform of the density matrix ρ

$$W(x, p) = \rho_W(x, p), \tag{2.2.3}$$

where the Weyl transform $\rho_{W(x,p)}$ is given by

$$\rho_{W(x,p)} = \int dy e^{\frac{i}{\hbar}py} \langle x - \frac{1}{2}y|\rho|x + \frac{1}{2}y\rangle, \tag{2.2.4}$$

where $x, y, p \in \mathbb{R}$. The expectation value of an observable $\hat{A}$ in the phase space representation is given by

$$\langle \hat{A} \rangle = \int dx dp W(x,p) \hat{A}_{W(x,p)}. \tag{2.2.5}$$

The fact that the displacement operators form a basis in the operator space provides us with another way of looking at the Wigner function. Since the displacement operators are a basis, any operator $\hat{A}$ can be expanded in terms of them as

$$\hat{A} = \int f(\mathbf{r}) \hat{D}_{\mathbf{r}} d\mathbf{r}. \tag{2.2.6}$$

First multiplying both sides by $\hat{D}^{\dagger}_{\mathbf{r}'}$ then taking the trace of the product of the operators on both sides we get

$$Tr[\hat{D}^{\dagger}_{\mathbf{r}'} \hat{A}] = \int f(\mathbf{r}) Tr[\hat{D}^{\dagger}_{\mathbf{r}'} \hat{D}_{\mathbf{r}}] d\mathbf{r}. \tag{2.2.7}$$

By using the orthogonality condition in (2.1.22), we obtain the following expression for $f(\mathbf{r})$

$$f(\mathbf{r}') = \frac{1}{(2\pi)^n} Tr[\hat{D}^{\dagger}_{\mathbf{r}'} \hat{A}]. \tag{2.2.8}$$

Substituting this into eqn (2.2.6) we have

$$\hat{A} = \frac{1}{(2\pi)^n} \int Tr[\hat{D}^{\dagger}_{\mathbf{r}} \hat{A}] \hat{D}_{\mathbf{r}} d\mathbf{r}. \tag{2.2.9}$$

Note that $\hat{D}^{\dagger}_{\mathbf{r}} = \hat{D}_{-\mathbf{r}}$ and similarly $\hat{D}_{\mathbf{r}} = \hat{D}^{\dagger}_{-\mathbf{r}}$. This follows immediately from the fact that in Eqn. (2.1.13) all the operators in the exponential are Hermitian. Using this property of $\hat{D}_{\mathbf{r}}$ together with changing the dummy index $-\mathbf{r}$ to $\mathbf{r}$ and replacing

the operator $\hat{A}$ by the density operator ρ we obtain

$$\rho = \frac{1}{(2\pi)^n} \int Tr[\hat{D}_{\mathbf{r}}\rho]\hat{D}_{\mathbf{r}}^{\dagger} d\mathbf{r}. \tag{2.2.10}$$

The expression $Tr[\hat{D}_{\mathbf{r}}\rho]$ is known as the *characteristic function* and plays an important role in CV systems. For every density operator there is a characteristic function χ associated with it

$$\chi_\rho(\mathbf{r}) = Tr[\hat{D}_{\mathbf{r}}\rho]. \tag{2.2.11}$$

It is possible to obtain the characteristic function by taking the Fourier transform of the Wigner function by applying a general formula given by

$$W(\mathbf{r}') = \frac{1}{\pi^2} \int \chi_\rho(\mathbf{r}) e^{i\mathbf{r}^T \Omega \mathbf{r}'} d\mathbf{r} \tag{2.2.12}$$

This expression can be derived by taking the Weyl transform given in Eq. (2.2.4) of the density matrix ρ.

2.3. Symplectic transformations in CV systems

A matrix S is a real symplectic matrix iff

$$S^T \Omega S = \Omega. \tag{2.3.1}$$

The set of all such operators acting on phase space form a group. The set is closed under matrix multiplication:

$$(SS')^T \Omega SS' = S'^T S^T \Omega SS' = S'^T \Omega S' = \Omega. \tag{2.3.2}$$

If we take the determinant of both sides of Eq. (2.3.1) we find that S is non-singular:

$$\begin{aligned} &\det S^T \Omega S = \det \Omega \\ &\Rightarrow (\det S)^2 = 1 \Rightarrow \det S = \pm 1. \end{aligned} \tag{2.3.3}$$

Since S is non-singular it has an inverse S^{-1}. It is easy to see that S^{-1} is in the symplectic group:

$$(S^{-1})^T \Omega S^{-1} = (S^{-1})^T S^T \Omega S S^{-1} = (SS^{-1})^T \Omega S S^{-1} = \Omega. \tag{2.3.4}$$

The operators $\hat{D}_{\mathbf{r}}$ perform translations in phase space. So we have

$$\chi_{\hat{D}_{\mathbf{r}'} \rho \hat{D}^\dagger_{\mathbf{r}'}}(\mathbf{r}) = \chi_\rho(\mathbf{r} + \mathbf{r}'). \tag{2.3.5}$$

Corresponding to every $S \in S_p(2n, \mathbb{R})$ there is a unitary U_S such that

$$\chi_{U_S \rho U_S^\dagger}(\mathbf{r}) = \chi_\rho(S\mathbf{r}). \tag{2.3.6}$$

We also have

$$U_S \hat{D}_{\mathbf{r}} U_S^\dagger = \hat{D}_{S\mathbf{r}}. \tag{2.3.7}$$

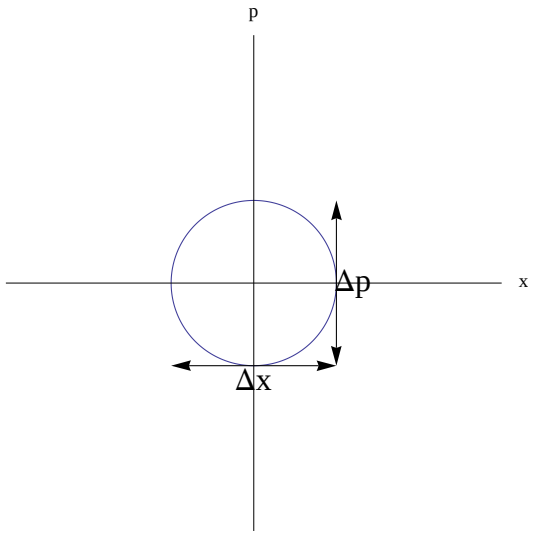
One important example of such an operator is the *squeezing operator* $U_S(\eta)$. For a one-mode state we have

$$U_S(\eta) = e^{\eta(\hat{a}^{\dagger 2} - \hat{a}^2)}.$$

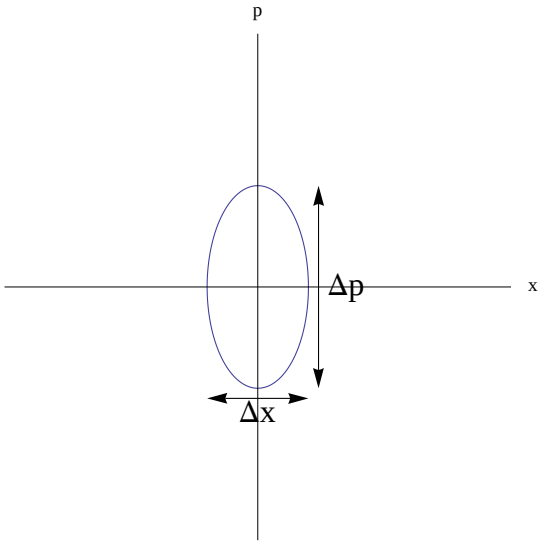
where η is the squeezing parameter and in general it can be complex. However, here we consider a real parameter for simplicity. The main ingredient to generate entanglement in CV systems is squeezed light. In laboratories it is generated by optical processes such as optical parametric oscillation and four-wave mixing. Theoretically we apply a squeezing operator on the state of light. Squeezing light corresponds to increasing uncertainty in one quadrature while decreasing it in the other. Heisenberg's uncertainty relation tells us

$$\Delta x \Delta p \geq 1.$$

A coherent state is a minimum uncertainty state with $\Delta x = \Delta p = 1$. Acting on a coherent state with $U_S(\eta)$ generates a squeezed state with $\Delta x = \eta$ and $\Delta p = \frac{1}{\eta}$. These states have simple representations in the phase space. For instance this graph



shows a single-mode coherent state with $\Delta p = \Delta x$, while this one



shows a single-mode squeezed coherent state with $\Delta p = 2\Delta x$.

We now give the following theorem [**25**] which plays an important role in manipulation of Gaussian states.

THEOREM 1. *Williamson Theorem. For any $2n$-dimensional real, symmetric, positive matrix $\boldsymbol{\sigma}$ there exists $S \in \mathbb{S}_p(2n, \mathbb{R})$ such that a symplectic diagonalization defined as*

$$S^T \boldsymbol{\sigma} S = \boldsymbol{\nu} \tag{2.3.8}$$

is possible, with

$$\boldsymbol{\nu} = \bigoplus_{i=1}^{n} \begin{pmatrix} \nu_i & 0 \\ 0 & \nu_i \end{pmatrix} \tag{2.3.9}$$

where $\boldsymbol{\nu}$ is a positive definite $2n$-dimensional matrix. The ν_i are the symplectic eigenvalues of $\boldsymbol{\sigma}$.

PROOF. Define an anti-symmetric matrix $M = \boldsymbol{\sigma}^{-\frac{1}{2}} \Omega \boldsymbol{\sigma}^{-\frac{1}{2}}$. Then there exists an orthogonal matrix R such that

$$R^T M R = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \tag{2.3.10}$$

where E is a positive semi-definite $n \times n$ diagonal matrix. It is straightforward to obtain the following

$$F \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} F = \Omega \quad \text{where} \quad F = \begin{pmatrix} E^{-\frac{1}{2}} & 0 \\ 0 & E^{-\frac{1}{2}} \end{pmatrix} \tag{2.3.11}$$

In terms of $\boldsymbol{\sigma}$ this reads

$$F R^T \boldsymbol{\sigma}^{-\frac{1}{2}} \Omega \boldsymbol{\sigma}^{-\frac{1}{2}} R F = \Omega \tag{2.3.12}$$

Define $S = \boldsymbol{\sigma}^{-\frac{1}{2}} R F$. Then $S^T = F R^T \boldsymbol{\sigma}^{-\frac{1}{2}}$ and so

$$S^T \Omega S = \Omega \tag{2.3.13}$$

It follows from the definition of S that

$$S^T \boldsymbol{\sigma} S = F R^T I R F = F^2. \tag{2.3.14}$$

So if we define

$$\boldsymbol{\nu} = F^2 = \begin{pmatrix} E^{-1} & 0 \\ 0 & E^{-1} \end{pmatrix}, \tag{2.3.15}$$

we have

$$S^T \boldsymbol{\sigma} S = \boldsymbol{\nu}. \tag{2.3.16}$$

□

In our investigation of entanglement storage in quantum memories, described in Chapter 5.2 we often need to calculate the symplectic eigenvalues. This can be done using the following result.

PROPOSITION 1. *The symplectic eigenvalues of $\boldsymbol{\sigma}$ are the (ordinary) eigenvalues of the matrix $|i\Omega\boldsymbol{\sigma}|$.*

PROOF. This follows from the definition of a symplectic matrix given in Eq. (2.3.1) and from the symplectic diagonalization in Eq. (2.3.8). First note that $S^T(-\Omega^2)\boldsymbol{\sigma} S = \boldsymbol{\nu}$ since $-\Omega^2 = I$. Then multiplying both sides by $-i\Omega$ on the left, we get

$$-i\Omega S^T \Omega(-\Omega\boldsymbol{\sigma})S = -i\Omega\boldsymbol{\nu}. \tag{2.3.17}$$

Multiplying Eq. (2.3.1) by S^{-1} on the right both sides we get $S^T\Omega = \Omega S^{-1}$ then multiplying it again by Ω on the left on both sides we have $\Omega S^T \Omega = -S^{-1}$. Substituting this in the above equation we get

$$-i(-S^{-1})(-\Omega\boldsymbol{\sigma})S = -i\Omega\boldsymbol{\nu},$$

$$S^{-1}(-i\Omega\boldsymbol{\sigma})S = -i\Omega\boldsymbol{\nu}.$$

On the LHS we have a similarity transformation which leaves the eigenvalues of $i\Omega\boldsymbol{\sigma}$ unchanged. □

2.4. Bosonic Gaussian states

A state ρ is said to be Gaussian if its characteristic function χ is Gaussian. In other words, if

$$\chi_\rho(\mathbf{r}) = e^{i\mathbf{r}^T\Omega\mathbf{d}}e^{-\mathbf{r}^T\Omega^T\boldsymbol{\sigma}\Omega\mathbf{r}}, \tag{2.4.1}$$

where the vector $\mathbf{r}$ is the points in phase space given in Eq. (2.1.14) and Ω is the symplectic form given in Eq. (2.1.12) and $\mathbf{d}$ is the vector whose length is the distance between the origin and the peak of the Gaussian state in phase space. The matrix $\boldsymbol{\sigma}$ is called the *covariance matrix* and is a real, symmetric matrix whose entries are given in terms of the expectation values of the canonical operators $\hat{\mathbf{r}}$ described in Eq. (2.1.10).

One of the nice features of a Gaussian state is that it is fully determined by the first and second moments:

$$\begin{aligned} d_k &= \langle\hat{\mathbf{r}}_k\rangle, \\ \sigma_{kl} &= \frac{\langle\hat{\mathbf{r}}_k\hat{\mathbf{r}}_l + \hat{\mathbf{r}}_l\hat{\mathbf{r}}_k\rangle}{2} - \langle\hat{\mathbf{r}}_k\rangle\langle\hat{\mathbf{r}}_l\rangle. \end{aligned} \tag{2.4.2}$$

The d_k are the components of vector $\mathbf{d}$. The second moments, σ_{kl} are the components of the covariance matrix, $\boldsymbol{\sigma}$ in Eq. (2.4.1). The covariance matrix $\boldsymbol{\sigma}$ describes the shape of the Gaussian wavepacket. It also gives the "distortion" in the Gaussian wavepacket which determines the entanglement in systems with many modes. In other words, entangling a Gaussian state affects only the covariance matrix and therefore knowledge of the covariance matrix suffices to measure entanglement. The uncertainty relation for a multi-mode system is given by

$$\boldsymbol{\sigma} + i\Omega \geq 0. \tag{2.4.3}$$

PROPOSITION 2. *The positivity of the density matrix and the commutation relation given in Eq. (2.1.11) impose the following condition on the covariance matrix: a real, symmetric matrix $\boldsymbol{\sigma}$ is a covariance matrix if and only if it satisfies the uncertainty relation given in Eq. (2.4.3).*

PROOF. Let $\hat{y} = \sum_k (\hat{\mathbf{r}}_k - \mathbf{r}_k) v_k$ be a non-Hermitian operator where v_k is a complex vector with $2n$ components. Then $\hat{y}^\dagger = \sum_l v_l^* (\hat{\mathbf{r}}_l - \mathbf{r}_l)$ and $\hat{y}^\dagger \hat{y}$ is a Hermitian operator, and $Tr[\rho \hat{y}^\dagger \hat{y}] \geq 0$. This means that we have

$$\begin{aligned} Tr[\rho \hat{y}^\dagger \hat{y}] &= \sum_{k,l} v_l^* Tr[\rho (\hat{\mathbf{r}}_k - \mathbf{r}_k)(\hat{\mathbf{r}}_l - \mathbf{r}_l)] v_k \geq 0 \\ &= \sum_{k,l} v_l^* (Tr[\rho \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l] - \mathbf{r}_k \mathbf{r}_l) v_k \geq 0 \\ &= \sum_{k,l} v_l^* (\langle \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l \rangle - \mathbf{r}_k \mathbf{r}_l) v_k \geq 0 \end{aligned}$$

We define an operator $\boldsymbol{\tau}$ with elements $\tau_{kl} = (\langle \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l \rangle - \mathbf{r}_k \mathbf{r}_l)$. Then

$$Tr[\rho \hat{y}^\dagger \hat{y}] \geq 0 \Rightarrow \langle v, \boldsymbol{\tau} v \rangle \geq 0 \Rightarrow \boldsymbol{\tau} \geq 0. \tag{2.4.4}$$

It is easy to see that $\boldsymbol{\tau} = \boldsymbol{\sigma} + i\Omega$. We have $\hat{\mathbf{r}}_l \hat{\mathbf{r}}_k = \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l - 2i\Omega_{kl}$ from the commutation relation in Eq. (2.1.11). Substituting this into Eq. (2.4.2), we get

$$\begin{aligned} &\sigma_{kl} = \langle \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l \rangle - i\Omega_{kl} - \mathbf{r}_k \mathbf{r}_l \\ &\Rightarrow \langle \hat{\mathbf{r}}_k \hat{\mathbf{r}}_l \rangle - \mathbf{r}_k \mathbf{r}_l = \sigma_{kl} + i\Omega_{kl} \\ &\Rightarrow \hat{\tau}_{kl} = \sigma_{kl} + i\Omega_{kl}. \end{aligned} \tag{2.4.5}$$

□

Together the uncertainty principle and the Williamson theorem imply $\boldsymbol{\nu} + i\Omega \geq 0$. To see this, we take the symplectic transformation of Eq. (2.4.3):

$$S^T \boldsymbol{\sigma} S + i S^T \Omega S \geq 0 \implies \boldsymbol{\nu} + i\Omega \geq 0 \tag{2.4.6}$$

This amounts to

$$\nu_i \geq 1 \quad \forall\, i = 1, \ldots n. \tag{2.4.7}$$

In this thesis, we are interested in two-mode Gaussian states. The covariance matrix for such states is

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\alpha} & \boldsymbol{\gamma} \\ \boldsymbol{\gamma}^T & \boldsymbol{\beta} \end{pmatrix}, \tag{2.4.8}$$

where $\boldsymbol{\alpha}, \boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ can be any 2×2 matrices in general. However, there is a convenient way of writing $\boldsymbol{\sigma}$: For any CM $\boldsymbol{\sigma}$ we can find a local symplectic operator [**26**] $S_l = S_1 \oplus S_2$ such that

$$S_l^T \boldsymbol{\sigma} S_l = \boldsymbol{\sigma}_{sf} = \begin{pmatrix} a & 0 & c_+ & 0 \\ 0 & a & 0 & c_- \\ c_+ & 0 & b & 0 \\ 0 & c_- & 0 & b \end{pmatrix}. \tag{2.4.9}$$

In this form $\boldsymbol{\alpha}, \boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ are simple matrices: $\boldsymbol{\alpha} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \boldsymbol{\beta} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ and $\boldsymbol{\gamma} = \begin{pmatrix} c_+ & 0 \\ 0 & c_- \end{pmatrix}$. The quantity $\det \boldsymbol{\sigma}$ is invariant under symplectic transformations [**27**]. This means that $\det \boldsymbol{\sigma}$ is determined by the parameters a, b and $c_\pm$. Another symplectic invariant that is determined by these parameters is $\Delta(\boldsymbol{\sigma})$ given by

$$\Delta(\boldsymbol{\sigma}) = \det \boldsymbol{\alpha} + \det \boldsymbol{\beta} + 2 \det \boldsymbol{\gamma}. \tag{2.4.10}$$

The symplectic eigenvalues can be expressed in terms of $\Delta(\boldsymbol{\sigma})$:

$$\nu_\pm(\boldsymbol{\sigma}) = \sqrt{\frac{\Delta(\boldsymbol{\sigma}) \pm \sqrt{\Delta(\boldsymbol{\sigma})^2 - 4 \det \boldsymbol{\sigma}}}{2}}. \tag{2.4.11}$$

This expression together with Eq. (2.4.7) imply

$$\Delta(\boldsymbol{\sigma}) \leq 1 + \det \boldsymbol{\sigma}. \tag{2.4.12}$$

In Chapter 5.2 we will use these result to quantify the amount of entanglement in two-mode Gaussian states.

Gaussian states are an important ingredient of quantum optical processes for both their mathematical simplicity and experimental feasibility. The Wigner function described in the previous section is a classical probability distribution for all Gaussian states. We can easily calculate the characteristic function and then the Wigner function of any state but this significantly simplifies for Gaussian states since we only have a quadratic expression in the exponential. Below we illustrate the correspondence between the density matrix, the characteristic function and the Wigner function of a single mode coherent state.

2.4.1. Example: Wigner and characteristic functions of a coherent state. The simplest example of a Gaussian state is a one-mode coherent state. For a one-mode coherent state we have $\alpha = (\alpha, \alpha^*)^T$, $\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\hat{\alpha} = (\hat{a}, \hat{a}^\dagger)^T$ Eq. (2.1.15) becomes

$$D_\alpha = e^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}} = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha \hat{a}^\dagger} e^{-\alpha^* \hat{a}}, \tag{2.4.13}$$

where we used Baker-Campbell-Haussdorf formula $e^{[\hat{A},\hat{B}]} = e^{\hat{A}} e^{\hat{B}} e^{-\frac{1}{2}[\hat{A},\hat{B}]}$ to obtain the final expression. The density matrix ρ for such a system is

$$\rho = |\alpha\rangle\langle\alpha|. \tag{2.4.14}$$

The characteristic function is

$$\chi_\rho(\alpha') = Tr[D_{\alpha'} |\alpha\rangle\langle\alpha|]. \tag{2.4.15}$$

First, we find an expression for $D_{\alpha'}|\alpha\rangle$:

$$D_{\alpha'}|\alpha\rangle = e^{-\frac{1}{2}|\alpha'|^2} e^{-\alpha^{*\prime}\alpha} e^{\alpha'\hat{a}^\dagger}|\alpha\rangle, \tag{2.4.16}$$

where we used the fact that the coherent states are the eigenstates of $\hat{a}$ so that $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. To evaluate $e^{\alpha'\hat{a}^\dagger}|\alpha\rangle$ we use the definition of a coherent state in terms of number states as given in Eq. (2.1.5) and expand the exponential:

$$e^{\alpha'\hat{a}^\dagger}|\alpha\rangle = \Big(1 + \alpha'\hat{a}^\dagger + \frac{1}{2!}(\alpha'\hat{a}^\dagger)^2 + \frac{1}{3!}(\alpha'\hat{a}^\dagger)^3 + \cdots + \frac{1}{m!}(\alpha'\hat{a}^\dagger)^m + \ldots\Big) e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle.$$

Using Eq. (2.1.4) we have

$$e^{\alpha'}\hat{a}^\dagger|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n,m=0}^{\infty} \frac{\alpha^n \alpha'^m}{\sqrt{n!}m!} \sqrt{(n+1)(n+2)\ldots(n+m)}|n+m\rangle \tag{2.4.17}$$

$$= e^{-\frac{1}{2}|\alpha|^2} \sum_{n,m=0}^{\infty} \frac{\alpha^n \alpha'^m}{\sqrt{n!}m!} \sqrt{\frac{(n+m)!}{n!}}|n+m\rangle \tag{2.4.18}$$

$$= e^{-\frac{1}{2}|\alpha|^2} \sum_{n,m=0}^{\infty} \frac{\alpha^n \alpha'^m}{n!m!} \sqrt{(n+m)!}|n+m\rangle, \tag{2.4.19}$$

where we used the fact that

$$(n+1)(n+2)\ldots(n+m-1)(n+m) = \frac{(n+m)!}{n!}.$$

We can simplify this by defining a new index $k = n+m$ with $k : 0 \to \infty$ since both $n, m : 0 \to \infty$. Also, $m = k - n$ and $n : 0 \to k$, and we have

$$e^{\alpha'\hat{a}^\dagger}|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \sum_{n=0}^{k} \frac{\alpha^n \alpha'^{k-n}}{n!(k-n)!} \sqrt{k!}|k\rangle$$

$$= e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \Big(\sum_{n=0}^{k} \frac{k!}{n!(k-n)!} \alpha^n \alpha'^{k-n} \Big) \frac{1}{\sqrt{k!}}|k\rangle,$$

where the sum in brackets is a binomial expansion of the form: $(x+y)^s = \sum_{r=0}^{s} \frac{s!}{r!(s-r)!} x^r y^{s-r}$, so we have

$$e^{\alpha' a^\dagger}|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha+\alpha')^k}{\sqrt{k!}}|k\rangle. \tag{2.4.20}$$

We can write Eq. (2.1.5) as follows

$$|\alpha+\alpha'\rangle = e^{-\frac{1}{2}|\alpha+\alpha'|^2}\sum_{n=0}^{\infty}\frac{(\alpha+\alpha')^n}{\sqrt{n!}}|n\rangle$$
$$\Rightarrow \sum_{n=0}^{\infty}\frac{(\alpha+\alpha')^n}{\sqrt{n!}}|n\rangle = e^{\frac{1}{2}|\alpha+\alpha'|^2}|\alpha+\alpha'\rangle,$$

by simply replacing α by $\alpha+\alpha'$. Substituting this into the RHS of Eq. (2.4.20) we get

$$e^{\alpha' a^\dagger}|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}e^{\frac{1}{2}|\alpha+\alpha'|^2}|\alpha+\alpha'\rangle. \tag{2.4.21}$$

Going back to the Eq. (2.4.16) we now have

$$D_{\alpha'}|\alpha\rangle = e^{-\frac{1}{2}|\alpha'|^2}e^{-\alpha'^*\alpha}e^{-\frac{1}{2}|\alpha|^2}e^{\frac{1}{2}|\alpha+\alpha'|^2}|\alpha+\alpha'\rangle. \tag{2.4.22}$$

The terms in the exponential simplify to $-\frac{1}{2}(\alpha\alpha'^* - \alpha^*\alpha')$, which is equal to $-\frac{1}{2}\langle\alpha,\alpha'\rangle$. So we have

$$D_{\boldsymbol{\alpha'}}|\alpha\rangle = e^{-\frac{1}{2}\langle\alpha,\alpha'\rangle}|\alpha+\alpha'\rangle, \tag{2.4.23}$$

and so

$$\chi_\rho(\alpha') = e^{-\frac{1}{2}\langle\alpha,\alpha'\rangle}\langle\alpha|\alpha+\alpha'\rangle. \tag{2.4.24}$$

The overlap in the above expression is

$$\begin{aligned}\langle\alpha|\alpha+\alpha'\rangle &= e^{-\frac{1}{2}|\alpha|^2}e^{-\frac{1}{2}|\alpha+\alpha'|^2}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\frac{\alpha'^{*n}(\alpha+\alpha')^m}{\sqrt{n!m!}}\langle n|m\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2}e^{-\frac{1}{2}|\alpha+\alpha'|^2}\sum_{n=0}^{\infty}\frac{\left(\alpha^*(\alpha+\alpha')\right)^n}{n!} \\ &= e^{-\frac{1}{2}|\alpha|^2}e^{-\frac{1}{2}|\alpha+\alpha'|^2}e^{\alpha^*(\alpha+\alpha')} \\ &= e^{\frac{1}{2}(\alpha^*\alpha'-\alpha\alpha'^*)}e^{-\frac{1}{2}|\alpha'|^2},\end{aligned} \tag{2.4.25}$$

and

$$e^{-\frac{1}{2}\langle\alpha,\alpha'\rangle}\langle\alpha|\alpha+\alpha'\rangle = e^{\alpha^*\alpha'-\alpha\alpha'^*}e^{-\frac{1}{2}|\alpha'|^2}. \tag{2.4.26}$$

So

$$\chi_\rho(\alpha') = e^{\alpha^*\alpha'-\alpha\alpha'^*}e^{-\frac{1}{2}|\alpha'|^2}. \tag{2.4.27}$$

In the phase space representation the characteristic function above can be written as a function of x' and p' by simply replacing $\alpha' = x' + ip'$ and $\alpha = x + ip$

$$\chi_\rho(x',p') = e^{i(xp'-x'p)}e^{-\frac{1}{2}(x'^2+p'^2)} \tag{2.4.28}$$

We can now obtain the Wigner function of $\chi_\rho(x',p')$ by using Eq. (2.2.12)

$$W(x'',p'') = \frac{1}{\pi^2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\chi_\rho(x',p')e^{i(x',p')\Omega(x'',p'')^T}dx'dp' \tag{2.4.29}$$

Evaluating this Gaussian integral we obtain the Wigner function

$$W(x'',p'') = \frac{2}{\pi}e^{-\frac{1}{2}\left((x-x'')^2+(p-p'')^2\right)}. \tag{2.4.30}$$

In Fig.2 we give an example of a graph of $W(x'',p'')$.

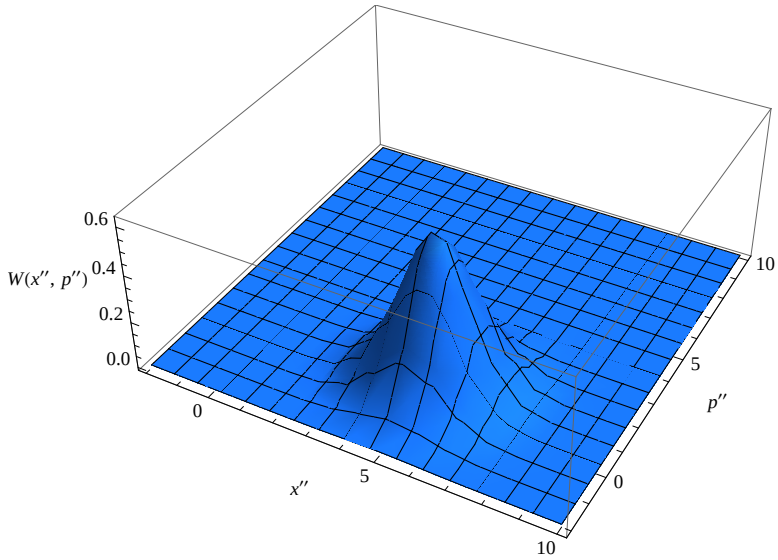


FIGURE 2. Wigner function, $W(x'', p'')$, with $x = 5, p = 1$.

CHAPTER 3

Discrete systems

In the last chapter we introduced the phase space representation of a CV system. It is interesting to ask how much of this generalizes to the case of a discrete system. The short answer is quite a lot but not entirely.

One of the differences is that the canonical commutation relations do not hold in discrete systems. Nevertheless, we can define discrete displacement operators and symplectic unitaries.

3.1. Discrete displacement operators

There is no perfect analogy between the discrete systems and the CV systems. The CCR in Eq. (2.1.9) cannot be satisfied in discrete systems. This is easily seen as follows. Suppose Eq. (2.1.9) could be satisfied in discrete systems. Then

$$\hat{x}_k\hat{p}_k - \hat{p}_k\hat{x}_k = 2iI,$$

taking the trace of both sides we have

$$Tr[\hat{x}_k\hat{p}_k] - Tr[\hat{p}_k\hat{x}_k] = 2id,$$

where d is the dimension of the Hilbert space. From the cyclic property of trace we have $Tr[\hat{x}_k\hat{p}_k] = Tr[\hat{p}_k\hat{x}_k]$ so we have

$$0 = 2id,$$

which is impossible. So for a finite dimension d there is no analogue of the CCR.

We can, however, have displacement operators in discrete systems whose action is similar to the operators, $e^{ip\hat{x}}, e^{-ix\hat{p}}$ in CV systems. In a CV system we have

$$\begin{aligned} e^{ip\hat{x}}|x\rangle &= e^{ipx}|x\rangle, \\ e^{-ix'\hat{p}}|x\rangle &= |x+x'\rangle. \end{aligned} \tag{3.1.1}$$

Suppose we have a finite dimensional system with a basis $|0\rangle, \ldots, |d-1\rangle$. Define X as

$$\begin{aligned} X|0\rangle &= |1\rangle, \\ X|1\rangle &= |2\rangle, \\ &\cdots, \\ X|d-1\rangle &= X|0\rangle. \end{aligned}$$

So

$$X^{r'}|r\rangle = |r+r'\rangle, \tag{3.1.2}$$

in analogy to Eq. (3.1.1). Similarly, we can define an operator Z such that

$$Z|r\rangle = \omega^r|r\rangle, \tag{3.1.3}$$

where $\omega = e^{\frac{2\pi i}{d}}$ and $Z^{r'}|r\rangle = \omega^{r'r}|r\rangle$. So the operator $Z^{r'}$ is like $e^{ip\hat{x}}$ of Eqn. (3.1.1). For CV systems the CCR imply

$$e^{ip\hat{x}}e^{-ix\hat{p}} = e^{ixp}e^{-ix\hat{p}}e^{ip\hat{x}}, \tag{3.1.4}$$

where we used Baker–Campbell–Hausdorff formula. For discrete systems we have

$$Z^r X^s = \omega^{rs} X^s Z^r. \tag{3.1.5}$$

So although we don't have a discrete analogue of $\hat{x}, \hat{p}$ we do have a discrete analogue of the unitaries $e^{ip\hat{x}}, e^{-ix\hat{p}}$.

The displacement operators in the discrete case are defined as

$$D_{\mathbf{p}} = \tau^{p_1 p_2} X^{p_1} Z^{p_2}, \tag{3.1.6}$$

where $\tau = -e^{\frac{i\pi}{d}}$ and the subscript $\mathbf{p}$ is a vector whose components are p_1, p_2 and is the position vector of a point in discrete phase space. Notice that when d is even $\tau^d = -1$. It is therefore convenient to define $\bar{d}$:

$$\bar{d} = \begin{cases} d & \text{if } d \text{ is odd} \\ 2d & \text{if } d \text{ is even} \end{cases}. \tag{3.1.7}$$

Then the components p_1 and p_2 run from 0 to $\bar{d} - 1$.

There are several reasons for introducing τ in the definition of displacement operators in Eq. (3.1.6). If we did not introduce it the expression for the product of two displacement operators in Eq. (3.1.8) below would not involve the symplectic form but instead some more complicated expression involving vectors $\mathbf{p}$ and $\mathbf{q}$. The role of τ becomes even more important when we go on to consider discrete symplectic transformations in the next section. It can be seen from the Eq. (3.2.6) that τ enters into the definition of a symplectic unitary in an essential way.

We have the following relationships,

$$D_{\mathbf{p}} D_{\mathbf{q}} = \tau^{\langle \mathbf{p}, \mathbf{q} \rangle} D_{\mathbf{p}+\mathbf{q}} \doteq D_{\mathbf{p}+\mathbf{q}}, \tag{3.1.8}$$

where the notation, $\doteq$, means 'up to a phase', and

$$D_{\mathbf{p}}^{\dagger} = D_{-\mathbf{p}}, \tag{3.1.9}$$

where the symplectic form in Eq. (3.1.8) is defined by

$$\langle \mathbf{p}, \mathbf{q} \rangle = p_2 q_1 - p_1 q_2, \tag{3.1.10}$$

with $\langle \mathbf{p}, \mathbf{p} \rangle = 0$. Notice also that the symplectic form is anti-symmetric, that is $\langle \mathbf{p}, \mathbf{q} \rangle = -\langle \mathbf{q}, \mathbf{p} \rangle$. It is also worth remarking that the symplectic form in a discrete

variable system is the same as the symplectic form in a CV system, given by Eq. (2.1.12). Although one can have multi-mode discrete variable systems [**28**], in this thesis we are considering one-mode discrete variable systems only. For such a system we can see that

$$\begin{pmatrix} p_1 & p_2 \end{pmatrix} \Omega \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = p_2 q_1 - p_1 q_2 = \langle \mathbf{p}, \mathbf{q} \rangle, \tag{3.1.11}$$

so the expression for the symplectic form in the discrete case is formally the same as in the CV case.

As in the CV case the displacement operators form a group called the Weyl-Heisenberg group or sometimes the generalized Pauli group [**20**,**29**]. They also form a basis for operator space. Thus an arbitrary operator $\hat{A}$ is uniquely expressed as

$$\hat{A} = \sum_{p_1, p_2 = 0}^{d-1} A_{\mathbf{p}} D_{\mathbf{p}}. \tag{3.1.12}$$

We also have

$$Tr[D_{\mathbf{p}} D_{\mathbf{q}}^{\dagger}] = d\delta_{\mathbf{p},\mathbf{q}}, \tag{3.1.13}$$

and so

$$\hat{A}_{\mathbf{p}} = \frac{1}{d} Tr[\hat{A} D_{\mathbf{p}}^{\dagger}]. \tag{3.1.14}$$

For a density matrix ρ,

$$\rho_{\mathbf{p}} = \frac{1}{d} Tr[\rho D_{\mathbf{p}}^{\dagger}], \tag{3.1.15}$$

is a discrete analogue of the characteristic function. It is possible to obtain the Wigner function by taking the Fourier transform of $\rho_{\mathbf{p}}$ [**30**]. It may seem that the analogy between the discrete and CV systems is perfect. However this is not the case. The discrete analogue of the Wigner function may not be a real valued function for even dimensions. Suppose we try to write down the Eq. (2.2.4) for a

finite dimension d:

$$W(x,p) = \sum_{y=0}^{d-1} \omega^{py} \langle x - \frac{1}{2}y|\rho|x + \frac{1}{2}y\rangle \tag{3.1.16}$$

where $x, y, p \in \mathbb{Z}_d$. The problem here is the number $\frac{1}{2}$. We need to find a number $a \in \mathbb{Z}_d$ such that $2a = 1 \mod d$. If d is odd this question can be solved. For instance, if $d = 5$ we can take $a = 3$, if $d = 7$ we can take $a = 4$ etc. However if d is even then the equation $2a = 1 \mod d$ has no solution. There has been considerable effort to get around this problem [**31**]. However, these efforts have not led a satisfactory definition of the Wigner function for even dimensions.

3.2. Symplectic transformations in discrete systems

In the CV case we introduced symplectic matrices S with the property that $S^T \Omega S = \Omega$. We define symplectic matrices in the discrete case in the same way to be matrices

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{3.2.1}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_{\bar{d}}$, such that

$$F^T \Omega F = \Omega \mod \bar{d}, \tag{3.2.2}$$

or, equivalently,

$$\langle F\mathbf{p}, F\mathbf{q}\rangle = \langle \mathbf{p}, \mathbf{q}\rangle, \quad \forall\, \mathbf{p}, \mathbf{q}. \tag{3.2.3}$$

The necessary and sufficient condition for F to have this property is

$$\det F = 1 \mod \bar{d}. \tag{3.2.4}$$

We denote the group of symplectic matrices $\mathrm{SL}(2, \mathbb{Z}_{\bar{d}})$.

We saw that in the CV case for each symplectic matrix S there is a unitary U_S such that $U_S D_{\mathbf{r}} U_S^\dagger = D_{S\mathbf{r}}$. It can be shown [**32**] that the same is true in the

discrete case: for each $F \in SL(2, \mathbb{Z}_{\bar{d}})$ there is a unitary U_F such that

$$U_F D_{\mathbf{p}} U_F^{\dagger} = D_{F\mathbf{p}}, \tag{3.2.5}$$

for all $\mathbf{p}$. This equation relates the action of 2×2 matrix F on the points $\mathbf{p}$ in discrete phase space to the action of unitary operator U_F on the Hilbert space. To give an explicit expression for U_F consider first symplectic matrices such that β, in Eq. (3.2.1), is relatively prime to $\bar{d}$ (we say F is a *prime matrix* in that case). The fact that β is relatively prime to $\bar{d}$ means that $\exists\ \beta^{-1} \in \mathbb{Z}_{\bar{d}}$ such that $\beta\beta^{-1} = 1$ mod $\bar{d}$. We have

$$U_F = \frac{1}{\sqrt{d}} \sum \tau^{\beta^{-1}(\alpha s^2 - 2rs + \delta r^2)} |r\rangle\langle s|, \tag{3.2.6}$$

where d is the dimension of the Hilbert space and $|r\rangle, |s\rangle$ are the standard basis vectors. Notice that the only matrix element of F, in Eq. (3.2.1), that does not appear in Eq. (3.2.6) is γ. This is not so surprising if we consider the fact that β is coprime with $\bar{d}$ together with the property in Eq. (3.2.4) determines γ. In other words, γ is fixed by α, β, δ.

REMARK 1. *Note that number β in Eq.(3.2.6) is not a fraction. We will explain this point by a simple example. Suppose $\bar{d} = d = 5$ and $\beta = 3$. If we were dealing with ordinary integers we would argue:*

$$3x = 0 \implies x = 0 \times \frac{1}{3} \implies x = 0. \tag{3.2.7}$$

where $\frac{1}{3}$ is the inverse of 3. In $\mathbb{Z}_5$, however, inverse of 3 is not a fraction. So what is the inverse of 3 in $\mathbb{Z}_5$? To answer this question we need to see how $\mathbb{Z}_5$ is defined. We say two numbers are equivalent if their difference is a multiple of 5 e.g. if 15-10=5 then 10 and 15 are equivalent. An equivalence class is a set of all integers equivalent to some given integer e.g. the equivalence class of 10 (denoted as $\bar{10}$ is $\bar{10} = \{\cdots -10, -5, 0, 5, 10, \dots\}$. $\mathbb{Z}_5$ consists of five equivalence classes

$$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

where

$$\bar{0} = \{0, 5, 10, 15, \dots\} \cup \{0, -5, -10, -15, \dots\},$$

$$\bar{1} = \{1, 6, 11, 16, \dots\} \cup \{-4, -9, -14, -19, \dots\},$$

$$\bar{2} = \{2, 7, 12, 17, \dots\} \cup \{-3, -8, -13, -18 \dots\},$$

$$\bar{3} = \{3, 8, 13, 18, \dots\} \cup \{-2, -7, -12, -17 \dots\},$$

$$\bar{4} = \{4, 9, 14, 19, \dots\} \cup \{-1, -6, -11, -16 \dots\}.$$

Any element $\bar{a}$ *has an inverse in* $\mathbb{Z}_{\bar{d}}$ *iff* $\bar{a} \times \bar{a}^{-1} = 1$ *since* $\bar{1}$ *is the identity element. To find the inverse of* 3 *in* $\mathbb{Z}_5$ *we solve the equation*

$$\bar{3}\bar{a} = \bar{1}. \tag{3.2.8}$$

In other words for some element $\bar{a}$ *in the set* $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ *we will obtain* $\bar{1}$ *when multiplied by* $\bar{3}$*. We'll do it by trial and error:*

$$\bar{3} \times \bar{0} = \bar{0},$$

$$\bar{3} \times \bar{1} = \bar{3},$$

$$\bar{3} \times \bar{2} = \bar{6} = \bar{1}.$$

So we found the inverse of $\bar{3}$ *to be* $\bar{2}$ *in* $\mathbb{Z}_5$*. This means that if we take any element in the set* $\bar{3}$ *and another in the set* $\bar{2}$ *and multiply them we will always get an element in the set* $\bar{1}$*. In general we drop the bar on the integer and use* a *instead of* $\bar{a}$*, e.g. we write* $3a = 1 \mod 5$ *rather than* $\bar{3}\bar{a} = \bar{1}$*. In general we can find the inverse of a number* $a \mod \bar{d}$ *if and only if* a *is coprime to* $\bar{d}$ *[**33, 34**].*

If F is a non-prime symplectic matrix then we can always find two symplectic prime matrices F_1, F_2 such that $F = F_1 F_2$ and so $U_F = U_{F_1} U_{F_2}$ [**32**]. We can then use Eq. (3.2.6) together with the relation given below in Eq. (3.2.18) to calculate $U_{F_1} U_{F_2}$.

In this thesis, we will also need the concept of an anti-symplectic matrix. This is a matrix

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{3.2.9}$$

with

$$\det F = -1 \mod \bar{d}. \tag{3.2.10}$$

For every such F there is a corresponding anti-unitary U_F such that

$$U_F D_{\mathbf{p}} U_F^\dagger = D_{F\mathbf{p}}. \tag{3.2.11}$$

REMARK 2. *Recall that a unitary is linear,*

$$U(z|\psi\rangle + w|\phi\rangle) = zU|\psi\rangle + wU|\phi\rangle. \tag{3.2.12}$$

An anti-unitary is anti-linear,

$$U(z|\psi\rangle + w|\phi\rangle) = z^*U|\psi\rangle + w^*U|\phi\rangle. \tag{3.2.13}$$

In fact if U is an anti-unitary there is always a unitary V such that

$$\begin{aligned} U|\psi\rangle &= V|\psi^*\rangle \\ U^\dagger|\psi\rangle &= V^T|\psi^*\rangle. \end{aligned} \tag{3.2.14}$$

Basically, an anti-unitary is a complex conjugation followed by a unitary.

The set of all symplectic and anti-symplectic matrices is denoted $\mathrm{ESL}(2, \mathbb{Z}_{\bar{d}})$.If F is anti-symplectic we have

$$U_F = U_{FJ} U_J, \tag{3.2.15}$$

where

$$J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.2.16}$$

and

$$U_J|\psi\rangle = |\psi^*\rangle. \tag{3.2.17}$$

FJ is symplectic, so the unitary U_{FJ} can be calculated using Eqn. (3.2.6).

For any two arbitrary symplectic or anti-symplectic matrices, $F, G \in \mathrm{ESL}(2, \mathbb{Z}_{\bar{d}})$, we have the following relations:

$$U_F U_G \doteq U_{FG}, \tag{3.2.18}$$

$$U_F^\dagger \doteq U_{F^{-1}}, \tag{3.2.19}$$

$$U_F D_{\mathbf{p}} = D_{F\mathbf{p}} U_F, \tag{3.2.20}$$

$$U_F^\dagger D_{\mathbf{p}} U_F = D_{F^{-1}\mathbf{p}}. \tag{3.2.21}$$

We have introduced two kinds of unitaries: the displacement operators $D_{\mathbf{p}}$ and the symplectic unitaries U_F. If we act with both kinds of unitaries we obtain a larger group called the *Clifford Group*, $\mathrm{C}(d)$ [**35**–**41**], which consists of all unitaries of the form

$$e^{i\theta} D_{\mathbf{p}} U_F, \tag{3.2.22}$$

where $e^{i\theta}$ is an arbitrary phase. If we allow F in this expression to be any matrix in $\mathrm{ESL}(2, \mathbb{Z}_{\bar{d}})$, this gives us the *extended Clifford group*, $\mathrm{EC}(d)$ [**32**]. This definition is for the single-mode case in discrete phase space. The Clifford group is also defined for multi-mode discrete systems. For a good discussion of the differences between the single-mode and multi-mode cases see [**28**]. The Clifford group was originally introduced into quantum information in connection with quantum error correction

by [**35**–**41**]. The application to quantum error correction depends on the multi-mode Clifford group. The application of the single-mode Clifford group to the SIC problem is discussed in [**32**].

CHAPTER 4

Measurements

It is an interesting question to ask if there is a finite dimensional analogue of Gaussian states for discrete systems. In this chapter we show that *symmetric informationally complete positive operator valued measures* (SIC-POVMs) in discrete systems are analogous to coherent state POVMs in CV systems. [**42**].

We first give a brief introduction to POVMs in general. Then in Section 4.2 we introduce SIC-POVMS and in Section 4.3 we draw an analogy between the coherent states in CV case and SIC-POVMs in the discrete case.

4.1. Generalized observables: PVMs and POVMs

Traditionally, an observable was considered to be a self-adjoint operator, $\hat{A}$. Such an operator can be written in terms of its eigenvalues. If the eigenvalues of $\hat{A}$ are discrete then we can write,

$$\hat{A} = \sum_r \lambda_r |r\rangle\langle r|, \tag{4.1.1}$$

where λ_r is the nth eigenvalue and $|r\rangle$ is the corresponding eigenvector. If, on the other hand, the eigenvalues are continuous then we can write,

$$\hat{A} = \int \lambda |\lambda\rangle\langle\lambda| d\lambda, \tag{4.1.2}$$

where we now write the eigenvector corresponding to λ as $|\lambda\rangle$. For simplicity we are confining ourselves to the case where the eigenvectors are non-degenerate and spectrum is either purely discrete or purely continuous.

If the state of the system described by the density matrix ρ, then:

(1) In the discrete case the probability of getting measurement outcome λ_r is $\langle r|\rho|r\rangle$.
(2) In the continuous case the probability of getting measurement outcome λ is $\langle\lambda|\rho|\lambda\rangle$.

In the 1970s [**43**, **44**] a more general concept of observable was introduced. To understand this let us go back to our consideration of a self-adjoint operator and in the discrete case write

$$E_r = |r\rangle\langle r|. \tag{4.1.3}$$

The E_r are a set of rank-1 projection operators with the following properties:

(1) The number of E_r is equal to the dimension of the Hilbert space.
(2) The E_r are orthogonal,

$$Tr[E_r E_s] = \delta_{rs}. \tag{4.1.4}$$

.

(3) The E_r satisfy the completeness relation,

$$\sum E_r = I \tag{4.1.5}$$

.

(4) If the system is in a state described by the density matrix ρ then the probability, P_r, of getting measurement outcome λ_r is

$$P_r = Tr[\rho E_r] \tag{4.1.6}$$

In the continuous case we have the same statements except that the Kronecker-delta is replaced by the Dirac-delta and the sum is replaced with an integral. Such a set of operators E_r is called a PVM (*Projection Valued Measure*). The corresponding measurement is called a Von Neumann measurement [**45**].

In the more general concept of observable introduced in he 1970s, the PVM is replaced with a POVM (*Positive Operator Valued Measure*). In a POVM we drop the requirement that the E_r be the projection operators and only require that they be positive semi-definite. We no longer require that the number of E_r be equal to the dimension of the Hilbert space. However, we still do require items (3) and (4) on the above list. Thus a discrete POVM is a set of positive semi-definite operators E_r with the properties

(1) The E_r satisfy the completeness relation, $\sum E_r = I$.
(2) If the system is in a state described by the density matrix ρ then the probability of getting measurement outcome λ_r is $Tr[\rho E_r]$.

A continuous POVM is defined similarly replacing the sum with an integral. Notice that it is essential for the E_r the positive semi-definite since otherwise the probability of a measurement outcome could be negative. It is also essential that the E_r satisfy the completeness relation since otherwise the probabilities would not sum to 1.

4.1.1. Informationally complete POVMs. The more general concept of a POVM measurement has many applications [**43**,**44**,**46**]. In this thesis we are interested in POVMs with the property of informational completeness. A Von Neumann measurement does not give enough information to reconstruct the density matrix. However, there exist POVMs such that a knowledge of probabilities is sufficient to reconstruct the density matrix. Such POVMs are said to be *informationally complete* (IC) [**47**–**49**].

Assume the system is discrete with Hilbert space dimension d. For an IC POVM we must have at least d^2 elements, i.e. we must have $n \geq d^2$. To see this consider the number of real independent parameters needed to specify ρ. Diagonally there are d real parameters $r_1, \ldots, r_d$. There are $2 \times \frac{1}{2}d(d-1)$ real parameters in the upper triangle: $d-1$ complex parameters in the first row, $d-2$ in the second row and so on, all with 2 real numbers. The numbers in the lower triangle are the conjugates of the numbers in the upper triangle so the real numbers in upper

triangle are the same as the real numbers in the lower triangle. So in total there are $d + d(d-1) = d^2$ real parameters. However, they are not all independent because $Tr[\rho] = 1$ means $r_1 + \cdots + r_d = 1 \implies r_d = 1 - r_1 - \cdots - r_{d-1}$. So in total there are $d^2 - 1$ real independent parameters that fix ρ. The equations $P_0 = Tr[\rho E_0], \ldots, P_{n-1} = Tr[\rho E_{n-1}]$ are not independent either because

$$Tr[\rho \sum_r E_r] = Tr[\rho] = 1. \tag{4.1.7}$$

So there are no more than $n-1$ independent equations. If the POVM is informationally complete the number of independent equations must be the same as the number of independent parameters. So we must have $n \geq d^2$. An IC-POVM is said to be *minimal* if $n = d^2$.

4.1.2. Weyl-Heisenberg POVMs. An important class of POVMs are POVMs that are covariant under the action of Weyl-Heisenberg (WH) group which we introduced in Chapter 2 (CV case) and Chapter 3 (discrete case).

A WH covariant POVM is one in which all the POVM elements are obtained from a single POVM element by acting with displacement operators. The single POVM element which is used to generate the POVM is called the fiducial element. Thus in the CV case the POVM elements are

$$E_{\mathbf{r}} = D_{\mathbf{r}} E D_{\mathbf{r}}^\dagger \tag{4.1.8}$$

while in the discrete case they are

$$E_{\mathbf{p}} = D_{\mathbf{p}} E D_{\mathbf{p}}^\dagger \tag{4.1.9}$$

where E is the fiducial element.

4.1.3. The coherent state POVM. One important example of a WH POVM in the CV case is the coherent state POVM. In the one-mode case we take the fiducial element to be

$$E = K|0\rangle\langle 0| \tag{4.1.10}$$

where $|0\rangle$ is the vacuum state and K is a normalization constant (which we show below in Section 4.3, Eq. (4.3.13) to be $\frac{1}{2\pi}$). Since we are restricting ourselves to the one-mode case $\mathbf{r}^T = (x, p)$ and so acting with displacement operators we get

$$E_{x,p} = K|x, p\rangle\langle x, p|. \tag{4.1.11}$$

If the state of the system is described by the density matrix ρ then the corresponding probability distribution is

$$Q(x, p) = Tr[\rho E_{x,p}] = K\langle x, p|\rho|x, p\rangle. \tag{4.1.12}$$

This is the well-known Q-function of quantum optics [**50**, **51**].

4.2. SIC-POVMs

It is interesting to ask if one can define a discrete analogue of a coherent state POVM. We are going to argue in the next section that a SIC-POVM (*Symmetric Informationally Complete* POVM) can be considered to be a such an analogue. SIC-POVMs were first introduced by Zauner in his dissertation [**52**]. Subsequently it attracted much interest [**32**, **52**–**61**] in the literature.

A SIC-POVM is a special kind of minimal IC POVM. It has the following properties

(1) Each E_r is rank-1.

(2) $Tr[E_r] = A \ \forall r$, where A is a fixed constant.

(3) $Tr[E_r E_s] = B \ \forall r \neq s$, where B is a fixed constant.

The symmetry requirement (2) and (3) means that the E_r are spread out evenly over the generalized Bloch body, which means SIC-POVMs are the best minimal

IC POVMs from the point of view of tomography. It is also the reason why they are useful in the other applications listed in the Section 1.1 of this thesis.

We will first show that $A = \frac{1}{d}$ and $B = \frac{1}{d^2(d+1)}$ then prove that any POVM with the properties 1–3 is informationally complete. Properties (1) and (2) imply that we can write

$$E_r = A|\psi_r\rangle\langle\psi_r|, \tag{4.2.1}$$

where $|\psi_r\rangle$ are normalized vectors. Taking the trace of both sides of Eq. (4.1.5) we have

$$d^2 A = d \Rightarrow A = \frac{1}{d}. \tag{4.2.2}$$

Multiplying both sides of Eq. (4.1.5) by E_s and taking the trace we have

$$\sum_r Tr[E_r E_s] = Tr[E_s],$$
$$Tr[E_s^2] + \sum_{r \neq s} Tr[E_r E_s] = Tr[E_s].$$

Using both Eq. (4.2.1) and Eq. (4.2.2) we get

$$\frac{1}{d^2} + (d^2 - 1)B = \frac{1}{d} \Rightarrow B = \frac{1}{d^2(d+1)}$$

The Eq. (4.1.6) holds for any POVM. We now derive an expression for the density matrix ρ in terms of probabilities to show that for a SIC-POVM we have a bijection. First we define an operator $\bar{E}_r$ such that $Tr[\bar{E}_r E_s] = \delta_{rs}$. It is straightforward algebra to show that this is true if $\bar{E}_r = d(d+1)E_r - I$. Since E_r are a basis for the operator space we can write $\rho = \sum_r \lambda_r E_r$ for some λ_r. So we have

$$Tr[\rho \bar{E}_s] = \sum_r \lambda_r Tr[E_r \bar{E}_s] = \sum_r \lambda_r \delta_{rs} = \lambda_s. \tag{4.2.3}$$

We also have

$$Tr[\rho \bar{E}_s] = Tr[\rho(d(d+1)E_s - I)] = d(d+1)Tr[\rho E_s] - Tr[\rho I] = d(d+1)P_s - 1$$

$$\Rightarrow \lambda_s = d(d+1)P_s - 1$$

$$\Rightarrow \rho = \sum_s \big(d(d+1)P_s - 1\big)E_s. \tag{4.2.4}$$

where P_s is given by Eq. (4.1.6).

A nice way of thinking about SIC-POVMs is to consider the geometry of a quantum state space. For a 2 dimensional Hilbert space an arbitrary quantum state can be represented by a real vector in a 3 dimensional Bloch sphere. A SIC-POVM in $d = 2$ has 4 elements which are represented as vectors on Bloch sphere. These vectors form a tetrahedron on the Bloch sphere. In higher dimensions the situation is a little more complicated. One can still represent a quantum state by a real vector [**55**,**62**–**65**]. However, the vectors no longer lie in a sphere but in a much more geometrically complicated convex body which is sometimes called the Bloch body. The Bloch body is contained in side a hyper-sphere. The pure states are the points where the Bloch body meets the inclosing hyper-sphere. A SIC-POVM is a regular symplex inside the body. The vertices are the rank-1 projectors dE_r and they lie on the manifold of pure states (i.e. the intersection of Bloch body with the enclosing hyper-sphere) [**55**].

The vast majority of known SIC-POVMs are in fact WH POVMs. To construct a WH SIC-POVM we find a single vector $|\psi\rangle$ such that

$$|\langle\psi|D_{\mathbf{p}}|\psi\rangle| = \begin{cases} 1 & \text{if } \mathbf{p} = \mathbf{0} \\ \frac{1}{\sqrt{d+1}} & \text{if } \mathbf{p} \neq \mathbf{0}. \end{cases} \tag{4.2.5}$$

Applying the displacement operators gives us a WH SIC-POVM

$$E_{\mathbf{p}} = \frac{1}{d} D_{\mathbf{p}}|\psi\rangle\langle\psi|D_{\mathbf{p}}^{\dagger}. \tag{4.2.6}$$

The vector $|\psi\rangle$ is called the fiducial vector.

4.3. A finite dimensional analogue of coherent states: SIC-POVMs

We are now going to argue that a WH SIC-POVM is a discrete analogue of a coherent state POVM. This means that if we write the elements of a WH SIC-POVM in the form

$$E_{\mathbf{p}} = \frac{1}{d}|\psi_{\mathbf{p}}\rangle\langle\psi_{\mathbf{p}}|, \tag{4.3.1}$$

then the vectors $|\psi_{\mathbf{p}}\rangle$ can be considered to be discrete analogues of the coherent states $|x, p\rangle$. It also means that the probability distribution $Tr[\rho E_{\mathbf{p}}]$ can be considered to be a discrete analogue of the Q-function. Note that the informational completeness means that this probability distribution completely determines the state.

The crucial point in our analogy is that within the class of WH POVMs the elements of SIC-POVMs in the discrete case and the coherent states in the CV case are as nearly orthogonal as possible, in a sense we will, now, explain. Recall that for a PVM one has $Tr[E_r E_s] = 0$, whenever $r \neq s$. Distinct PVM elements thus orthogonal. It is impossible to construct a WH POVM for which this is true. However, one might ask for a WH POVM for which the overlaps between distinct elements is as small as possible. We will say that the POVM that satisfies this condition is as nearly orthogonal as possible.

We need to make this statement quantitative. For the discrete case we consider the sum

$$\sum_{\mathbf{p}\neq\mathbf{q}} (Tr[E_{\mathbf{p}} E_{\mathbf{q}}])^2. \tag{4.3.2}$$

We will say that a POVM which minimizes this sum is as nearly orthogonal as possible.

In the CV case we cannot simply replace the sum by an integral as the expression which results is infinite. So instead we consider the following quantities

$$\epsilon_x = \Big(\int x^2 Tr[E E_{x,p}] dx dp \Big)^{\frac{1}{2}},$$

$$\epsilon_p = \Big(\int p^2 Tr[E E_{x,p}] dx dp \Big)^{\frac{1}{2}}. \tag{4.3.3}$$

We will say that a POVM which minimizes the product $\epsilon_x \epsilon_p$ is as nearly orthogonal as possible. We also require the POVM to be symmetric in the sense that $\epsilon_x = \epsilon_p$.

4.3.1. Discrete case. We restrict ourselves to one-mode WH POVMs. First note that the index vector $\mathbf{r}$ in Eq. (4.1.8) is $(x, p)^T$ for a one-mode system. Then we have Eq. (4.1.8) as

$$E_{x,p} = D_{x,p} E D^\dagger_{x,p}. \tag{4.3.4}$$

Using this expression we write an expression for the overlap between two arbitrary POVM elements corresponding to $\mathbf{r} = (x, p)^T$ and $\mathbf{r'} = (x', p')^T$

$$E_{x+x',p+p'} = D_{x',p'} E_{x,p} D^\dagger_{x',p'}. \tag{4.3.5}$$

Furthermore, we require the following properties:

(1) The fiducial element E is proportional to a rank-1 projector, so that

$$E = K|\psi\rangle\langle\psi|, \tag{4.3.6}$$

for some normalization constant K and pure state $|\psi\rangle$.

(2) The POVM elements are as close to orthogonal as possible, in the sense that the sum

$$\sum_{x' \neq x, p' \neq p} \Big(Tr[E_{x,p} E_{x'p'}] \Big)^2 \tag{4.3.7}$$

is as small as possible.

We then use the following result, proved in [**61**]:

THEOREM 2. *Suppose A_i is a positive semi-definite operator and $Tr[A_i^2] = 1$ then*

$$\sum_{i \neq j} (Tr[A_i A_j])^2 \geq \frac{d^2(d-1)}{d+1}, \tag{4.3.8}$$

with the equality if and only if

(1) *A_i is a rank 1 projector*
(2) $Tr[A_iA_j] = \frac{1}{d+1}$, $\forall i \neq j$.

We use this result to show that $\sum_{x,p}(Tr[E_{x,p}E_{x',p'}])^2 \geq \frac{d-1}{d^2(d+1)}$ and that the lower bound is achieved if and only if $Tr[E_{x,p}E_{x',p'}] = \frac{1}{d^2(d+1)}$ when $x \neq x'$ and $p \neq p'$.

First note that $Tr[E^2]$ is not 1 but it is $Tr[E] = K$. Moreover the trace of every other POVM element is also K since

$$Tr[E_{x,p}] = Tr[D_{x,p}ED^\dagger_{x,p}] = Tr[E], \tag{4.3.9}$$

where we used the cyclic property of trace and the fact that $DD^\dagger = I$. Taking the trace of both sides of Eq. (4.1.5) we obtain

$$\begin{aligned}
&\sum_{x,p} Tr[E_{x,p}] = Tr[I],\\
&\sum_{x,p} Tr[E] = d,\\
&d^2 Tr[E] = d,\\
&d^2 K = d,\\
&K = \frac{1}{d},\\
&\Rightarrow Tr[E^2_{x,p}] = \frac{1}{d^2}.
\end{aligned}$$

So if we define $A_i = dE_{x,p}$ then we get $Tr[E^2_{x,p}] = 1$ as required by the theorem. Then substituting $E_{x,p}$ for A_i in the Eq. (4.3.8) we have

$$\begin{aligned}
&\sum_{x\neq x',p\neq p'} (Tr[dE_{x,p}dE_{x',p'}])^2 = \sum_{x\neq x',p\neq p'} d^4(Tr[E_{x,p}E_{x',p'}])^2 \geq \frac{d^2(d-1)}{d+1}\\
&\Rightarrow \sum_{x\neq x',p\neq p'} (Tr[E_{x,p}E_{x',p'}])^2 \geq \frac{d-1}{d^2(d+1)}.
\end{aligned} \tag{4.3.10}$$

The lower bound for $E_{x,p}$ follows from Eq. (2)

$$Tr[dE_{x,p}dE_{x',p'}] = \frac{1}{d+1} \Rightarrow Tr[E_{x,p}E_{x',p'}] = \frac{1}{d^2(d+1)}. \tag{4.3.11}$$

When we substitute Eq. (4.3.6) into Eq. (4.3.11) we find that the following condition is imposed on the fiducial vector $|\psi\rangle$:

$$|\langle\psi|D_{x,p}|\psi\rangle|^2 = \begin{cases} 1 & \text{if } x = p = 0 \\ \frac{1}{d+1} & \text{otherwise} \end{cases} \tag{4.3.12}$$

This shows that the elements of a WH POVM are rank-1 and as close to orthogonal as possible if and only if it is a WH SIC-POVM.

4.3.2. CV case. Now we turn to CV systems. In CV systems the first requirement expressed in Eq. (4.3.6) remains almost exactly the same except $K \neq \frac{1}{d}$. So for the CV system we have

$$E = K'|\psi\rangle\langle\psi|. \tag{4.3.13}$$

where

$$\begin{aligned} K' &= Tr[E] = \int Tr[EE_{x,p}]dxdp, \\ K' &= K'^2 \int |\langle\psi|D_{x,p}|\psi\rangle|^2 dxdp, \\ &= K'^2 \int e^{i(x''-x')}\langle\psi|x'\rangle\langle x+x'|\psi\rangle\langle\psi|x+x''\rangle\langle x''|\psi\rangle dxdpdx'dx'', \\ &= 2\pi K'^2, \\ \Rightarrow K' &= \frac{1}{2\pi}. \end{aligned} \tag{4.3.14}$$

So the Eq. (4.3.13) is

$$E = \frac{1}{2\pi}|\psi\rangle\langle\psi|. \tag{4.3.15}$$

The second condition expressed in Eq. (4.3.7), however, needs to be changed slightly because the sum in Eq. (4.3.7) becomes a divergent integral. First note that

$Tr[E_{x,p}E_{x',p'}] = Tr[EE_{x,p}]$. This follows from Eq. (4.3.5) and from the cyclic property of the trace. Substituting Eq. (4.3.15) into Eq. (4.3.3) gives

$$\epsilon_x^2 = \frac{1}{4\pi^2}\int x^2 |\langle\psi|D_{x,p}|\psi\rangle|^2 dxdp. \tag{4.3.16}$$

We can rewrite the displacement operator D_α given in Eq. (2.4.13) replacing α by $x + ip$ and $\hat{a}$ by $\frac{1}{2}(\hat{x} + i\hat{p})$ in the LHS of Eq.(2.4.13) then using Baker-Campbell-Hausdorff formula together with Eq.(2.1.11) to get $D_{x,p} = e^{-2ixp}e^{ix\hat{p}}e^{-ip\hat{x}}$. Also note that $\langle\psi|D_{x,p}|\psi\rangle = \int\langle\psi|x'\rangle\langle x'|D_{x,p}|\psi\rangle dx'$, where $\langle x'|D_{x,p}|\psi\rangle = e^{-2ixp}e^{-ix'p}\langle x' + x|\psi\rangle$. In the final step we used $\langle x|\hat{x}|\psi\rangle = x\langle x|\psi\rangle$ and $\langle x|\hat{p}|\psi\rangle = -2i\frac{\partial}{\partial x}\langle x|\psi\rangle$ together with the Taylor series. So, now we have

$$\epsilon_x^2 = \frac{1}{4\pi^2}\int x^2 e^{i(x''-x')}\langle\psi|x'\rangle\langle x + x'|\psi\rangle\langle\psi|x + x''\rangle\langle x''|\psi\rangle dxdpdx'dx''. \tag{4.3.17}$$

The result of this integral is

$$\epsilon_x^2 = \frac{1}{\pi}(\Delta x)^2. \tag{4.3.18}$$

Similarly

$$\epsilon_p^2 = \frac{1}{\pi}(\Delta p)^2. \tag{4.3.19}$$

So we have

$$\epsilon_x\epsilon_p = \frac{1}{\pi}\Delta x\Delta p. \tag{4.3.20}$$

So the requirement for minimizing $\epsilon_x\epsilon_p$ amounts to the requirement for minimizing $\Delta x\Delta p$. So $|\psi\rangle$ must be a minimum uncertainty state. Since we also require $\epsilon_x = \epsilon_p$ it follows that $|\psi\rangle$ must be a coherent state.

WH SICs in a discrete system and coherent states in a CV system have in common the property that they are the rank-1 WH covariant POVMs for which the POVM elements are as near to orthogonal as possible.

4.4. Conclusion

We have shown that there is a sense in which WH SIC vectors $|\psi_{\mathbf{p}}\rangle$ can be regarded as a discrete analogue of coherent states $|x, p\rangle$. They are both covariant under the action of the WH group (discrete in the one case, continuous in the other). Also the vectors are as close to orthogonal as possible in the sense we have explained. Of course, one should not make too much of this analogy as there are also some important differences. One obvious difference is that, while there is a simple analytic expression for a coherent state, no such expression is known for a SIC. Although a SIC is highly symmetric in the sense that the overlaps $Tr[E_{\mathbf{p}}E_{\mathbf{q}}]$ are constant for $\mathbf{p} \neq \mathbf{q}$, the expressions for the known SIC vectors are very complicated. Of course it is possible that a simple analytic expression will eventually be found, however, no such expression is currently known.

Our analogy means in particular that the SIC probabilities $Tr[\rho E_{\mathbf{p}}]$ can be regarded as a discrete analogue of the Q-function. However, this analogy should not be pushed too far. Although it is true that the coherent state POVM is informationally complete in a mathematical sense, in actual practice the Wigner function is much more suitable for tomography. This is because the Q-function is obtained by smoothing the Wigner function and as a result it is insensitive to a lot of the fine detail in the quantum state [**50**, **51**]. On the other hand a SIC-POVM, when it can be experimentally realized, is very suitable for tomography. So from the point of view of tomograpohy the probability distribution $Tr[\rho E_{\mathbf{p}}]$ might be considered more analogous to the Wigner function than it is to Q-function.

Part 2

Quantum Information Processes with Gaussian States

CHAPTER 5

Entanglement with continuous variable systems

The concept of entanglement was first discussed in the EPR paper in 1935 [**66**]. It should be noted, however, the word entanglement was first explicitly used by Schrödinger in a paper [**67**] which appeared a few months after the EPR paper and in which Schrödinger further developped the implications. In their paper, Einstein-Podolsky-Rosen considered a system with continuous variables. However early experiments in entanglement used discrete variables (typically, polarization of photons). The first experiments on entanglement came in the 1980s, whereas the EPR thought experiment was demonstrated only in 1992 [**68**]. In general there had been a bias for working with discrete variables rather than continuous variables in the early development of quantum information and quantum computation fields. One of the main reasons for this is the fact that qubits are analogues of the classical bits in digital classical computers. Another reason for working with discrete variables is that they only involve a finite dimensional Hilbert space which is easier to handle mathematically. However, although infinite dimensional Hilbert space for a CV system is in general hard to handle mathematically, there is a class of CV states, Gaussian states, which are much easier to handle mathematically. They are also easy to implement in the laboratory. Consequently, in recent years there has been a lot of interest and developments in CV systems [**27**,**69**–**77**]. They have been used to demonstrate quantum teleportation [**78**], teleportation networks [**79**], quantum key distribution [**80**] as well as quantum memories [**81**, **82**]. The generation of CV entanglement has also seen spectacular advances. Furthermore, CV systems such as optomechanical [**83**, **84**] and nano-electro-mechanical resonators [**85**] hold cosiderable promise for high precision sensing at the quantum limit. Although

there are theoretical reasons why it would be desirable to explore non-Gaussian resources [**86**], all such advances are still mainly centred on Gaussian states (essentially because first and second-order interactions in the field operators are easier to implement in practice).

Entangled quantum states are important resources for quantum information processing. Gaussian states have nice properties that enable us to generate and manipulate entanglement in the laboratory, and whose separability can be assessed analytically. In fact, an important criterion for entanglement is the Peres-Horodecki criterion which states that the positivity of the partial transpose is, in general, necessary but not sufficient for separability. In other words $\rho^{PT} \ngeq 0$ then ρ is entangled. If, on the other hand, $\rho^{PT} \geq 0$ then ρ may or may not be separable. However, for two-mode Gaussian states the positivity of the partially transposed density matrix is necessary and sufficient for the separability of the state. This has very nice implications for the covariance matrix and its symplectic eigenvalues. It has been shown that one of the implications is that if at least one of the symplectic eigenvalues ν_j of the covariance matrix $\boldsymbol{\sigma}$ of the partially transposed ρ is less than 1 then the Gaussian state corresponding to the covariance matrix is entangled. Moreover, the entanglement increases as the symplectic eigenvalue (that are < 1) decrease. In this chapter we review some essential background material regarding the entanglement of two-mode Gaussian states. In Section 5.2 we go on to apply these ideas to obtain some results concerning entanglement storage in a quantum memory (published in Yadsan-Appleby and Serafini [**87**]).

5.1. Entanglement criterion for Gaussian states

It was shown in [**88**, **89**] that the negativity of the partially transposed density matrix is a sufficient condition for the corresponding state to be entangled. This is called the Peres-Horodecki criterion. Reference [**89**] showed that this was not only a sufficient but also a necessary condition for all 2×2 and 2×3 systems. However, in general if the partial transposition of the density matrix is positive then the state

may or may not be entangled. In other words, in general, it is not straightforward to say whether a state is separable or not. However this problem greatly simplifies for Gaussian states. It can be seen from Eq. (2.2.4) that if we work in the position basis then the effect of transposition on the Wigner function is given by

$$\rho \to \rho^T \iff W(q,p) \to W(q,-p).$$

So in the position basis transposition of the density matrix is equivalent to reflecting phase space in the x-axis. Similarly, for a two-mode Gaussian state the effect of partial transposition (in the position basis) on the Wigner function is

$$\rho \to \rho^{PT} \iff W(q_1,p_1,q_2,p_2) \to W(q_1,p_1,q_2,-p_2).$$

This together with the uncertainty relation imply that Peres-Horodecki separability criterion is a necessary and sufficient condition for all Gaussian states to be separable and therefore it is also necessary and sufficient condition for all Gaussian states to be entangled [**90**].

The partial transposition matrix that takes $\begin{pmatrix} p_1 \\ q_1 \\ p_2 \\ q_2 \end{pmatrix}$ to $\begin{pmatrix} p_1 \\ q_1 \\ p_2 \\ -q_2 \end{pmatrix}$ is

$$T = \text{Diag}[1,1,1,-1]. \tag{5.1.1}$$

Or,

$$T = I \oplus \sigma_z, \tag{5.1.2}$$

where σ_z is the usual Pauli matrix. The following theorem is the crucial result proved in [**27**, **90**]. For the convenience of the reader we give the version of the proof given in [**27**].

THEOREM 3. ***PPT Criterion for two-mode Gaussian states***. *A two-mode Gaussian state is separable if and only if its partial transposition is positive semi-definite.*

Let $\tilde{\rho} = \rho^{PT}$. The Peres-Horodecki criterion tells us that if $\tilde{\rho}$ is negative then ρ is entangled. We need to prove that for a Gaussian state it is also true that if $\tilde{\rho}$ positive semi-definite then ρ is separable. Let $\boldsymbol{\sigma}$ and $\tilde{\boldsymbol{\sigma}}$ be the covariance matrices corresponding to ρ and $\tilde{\rho}$ respectively. Recall Eq. (2.4.8)

$$\boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\alpha} & \boldsymbol{\gamma} \\ \boldsymbol{\gamma}^T & \boldsymbol{\beta} \end{pmatrix}. \tag{5.1.3}$$

We then have

$$\tilde{\boldsymbol{\sigma}} = T\boldsymbol{\sigma}T = \begin{pmatrix} \tilde{\boldsymbol{\alpha}} & \tilde{\boldsymbol{\gamma}} \\ \tilde{\boldsymbol{\gamma}}^T & \tilde{\boldsymbol{\beta}} \end{pmatrix}, \tag{5.1.4}$$

with

$$\tilde{\boldsymbol{\alpha}} = \boldsymbol{\alpha}, \qquad \tilde{\boldsymbol{\gamma}} = \boldsymbol{\gamma}\sigma_z, \qquad \tilde{\boldsymbol{\beta}} = \sigma_z\boldsymbol{\beta}\sigma_z, \tag{5.1.5}$$

where we used the Eq. (5.3.14) for T. Note that this means $\det\tilde{\boldsymbol{\alpha}} = \det\boldsymbol{\alpha}, \det\tilde{\boldsymbol{\beta}} = \det\boldsymbol{\beta}$ and $\det\tilde{\boldsymbol{\gamma}} = -\det\boldsymbol{\gamma}$. We then need to prove the following lemma.

LEMMA 1. *Two-mode Gaussian states with* $\det\boldsymbol{\gamma} \geq 0$ *are separable.*

PROOF. We first assume $\det\boldsymbol{\gamma} > 0$. We use a local symplectic operation to reduce $\boldsymbol{\sigma}$ to the standard form of Eq. (2.4.9):

$$\boldsymbol{\sigma}_{sf} = \begin{pmatrix} a & 0 & c_+ & 0 \\ 0 & a & 0 & c_- \\ c_+ & 0 & b & 0 \\ 0 & c_- & 0 & b \end{pmatrix}, \tag{5.1.6}$$

where it can be assumed that $a \geq b$ and $c_+ \geq c_- > 0$. Now define the local symplectic operation $S_l = \text{Diag}[\sqrt{xy}, \frac{1}{\sqrt{xy}}, \sqrt{\frac{y}{x}}, \sqrt{\frac{x}{y}}]$ where

$$x = \sqrt{\frac{c_+ a + c_- b}{c_- a + c_+ b}},$$

$$y = \sqrt{\frac{\frac{a}{x} + bx - \left((\frac{a}{x} - bx)^2 + 4c_-^2\right)^{\frac{1}{2}}}{ax + \frac{b}{x} - \left((ax - \frac{b}{x})^2 + 4c_-^2\right)^{\frac{1}{2}}}},$$

and let

$$\boldsymbol{\sigma}' = S_l^T \boldsymbol{\sigma}_{sf} S_l \tag{5.1.7}$$

It can now be shown by direct calculation that $\boldsymbol{\sigma'}$ can be diagonalized by a rotation matrix of the form

$$R = \begin{pmatrix} \cos\theta & 0 & -\sin\theta & 0 \\ 0 & \cos\theta & 0 & -\sin\theta \\ \sin\theta & 0 & \cos\theta & 0 \\ 0 & \sin\theta & 0 & \cos\theta \end{pmatrix}. \tag{5.1.8}$$

Notice that this is only possible because c_+ and c_- have the same sign. Also the smallest eigenvalue of $\boldsymbol{\sigma}'$ is degenerate:

$$\boldsymbol{\sigma}_d = R\boldsymbol{\sigma}' R^T = \text{Diag}[\kappa_1, \kappa_2, \kappa_-, \kappa_-] \tag{5.1.9}$$

with $\kappa_1 \geq \kappa_-$ and $\kappa_2 \geq \kappa_-$. The uncertainty principle, $\boldsymbol{\sigma}_d + i\Omega \geq 0$ implies that $\kappa_- \geq 1$. So all the eigenvalues of $\boldsymbol{\sigma}_d$ are greater than 1, that is $\boldsymbol{\sigma}_d \geq I$.

We now appeal to the fact [**91**,**92**] that if the ordinary eigenvalues of a CM are all ≥ 1 (as is the case with $\boldsymbol{\sigma}_d$) then the P-function is nonnegative and not more singular than δ-function. This means that if ρ_d is the density matrix corresponding to the $\boldsymbol{\sigma}_d$ then we can write

$$\rho_d = \int_{\mathbb{C}^2} d^2\alpha_1 d^2\alpha_2 P(\alpha_1, \alpha_2)(|\alpha_1\rangle\langle\alpha_1| \otimes |\alpha_2\rangle\langle\alpha_2|), \tag{5.1.10}$$

where P is nonnegative. It follows that ρ_d is a convex combination of the separable states $|\alpha_1\rangle\langle\alpha_1| \otimes |\alpha_2\rangle\langle\alpha_2|$. Since ρ is obtained from ρ_d by applying local unitaries we conclude that ρ is separable.

We now need to consider the case when $\det \boldsymbol{\gamma} = 0$. For this case we can use a slightly modified version of the above argument. In Eq. (5.1.6) we can assume that $c_- = 0$. We then define $S_l = \mathrm{Diag}[\sqrt{a}, \frac{1}{\sqrt{a}}, \sqrt{b}, \frac{1}{\sqrt{b}}]$ and

$$\boldsymbol{\sigma}' = S_l^T \boldsymbol{\sigma}_{sf} S_l = \begin{pmatrix} a^2 & 0 & \sqrt{ab}c_+ & 0 \\ 0 & 1 & 0 & 0 \\ \sqrt{ab}c_+ & 0 & b^2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{5.1.11}$$

We then apply the uncertainty principle $\boldsymbol{\sigma}' + i\Omega \geq 0$ to deduce $\boldsymbol{\sigma}' \geq I$. The rest of the argument goes exactly as before. □

We now are ready to prove Theorem 3.

PROOF. Suppose $\tilde{\rho}$ is a state. Then there are 2 possibilities: 1. $\det \boldsymbol{\gamma} \geq 0$. Then we know ρ is separable by the Lemma 1. 2. $\det \boldsymbol{\gamma} < 0$. Then $\det \tilde{\boldsymbol{\gamma}} > 0$ since $\det \tilde{\boldsymbol{\gamma}} = -\det \boldsymbol{\gamma}$. So $\tilde{\rho}$ is separable by the Lemma 1. We now appeal to the fact that the partial transposition of a separable state is also a separable state. Since ρ is the partial transpose of $\tilde{\rho}$, and since $\tilde{\rho}$ is a separable state, it follows that ρ is a separable state. □

We can use the Theorem just proved to give the criterion for ρ to be entangled in terms of the symplectic eigenvalues of $\tilde{\boldsymbol{\sigma}}$. We know that ρ is separable if and only if $\tilde{\rho}$ is positive semi-definite, i.e. if and only if $\tilde{\boldsymbol{\sigma}} + i\Omega \geq 0$. In view of Eq. (2.4.7) this means that ρ is separable if and only if $\tilde{\nu}_i \geq 1$ for all i, where $\tilde{\nu}_i$ are the symplectic eigenvalues of $\tilde{\boldsymbol{\sigma}}$. Equivalently, ρ is entangled if and only if $\tilde{\nu}_i < 1$ for some i.

5.1.1. A measure of entanglement: logarithmic negativity. The partial transposition does not change the trace so that $Tr[\rho] = Tr[\tilde{\rho}] = 1$, however, it does

change the eigenvalues (the state is entangled if at least one of the eigenvalues of $\tilde{\rho}$ is negative). The *negativity* $\mathcal{N}(\rho)$, is defined to be the sum of the moduli of the negative eigenvalues of $\tilde{\rho}$ and is used to quantify the entanglement in ρ [**93**]. Let $\lambda_1, \ldots, \lambda_j$ be the non-negative eigenvalues and $\mu_1, \ldots, \mu_k$ be the negative eigenvalues of $\tilde{\rho}$. Then,

$$\begin{aligned} &Tr[\tilde{\rho}] = (\lambda_1 + \cdots + \lambda_j) + (\mu_1 + \cdots + \mu_k) = 1 \\ &\implies Tr[\tilde{\rho}] = (\lambda_1 + \cdots + \lambda_j) - (|\mu_1| + \cdots + |\mu_k|) = 1. \end{aligned} \tag{5.1.12}$$

The negativity of a quantum state with a density matrix ρ is defined to be

$$\mathcal{N}(\rho) = \frac{Tr[|\tilde{\rho}|] - 1}{2} \tag{5.1.13}$$

where $|\tilde{\rho}| = \sqrt{\tilde{\rho}^2} \implies Tr[|\tilde{\rho}|] = (\lambda_1 + \cdots + \lambda_j) + (|\mu_1| + \cdots + |\mu_k|)$. Substituting this and Eq. (5.1.12) into Eq. (5.1.13) we have

$$\begin{aligned} &\mathcal{N}(\rho) = \frac{1}{2}\Big((\lambda_1 + \cdots + \lambda_j) + (|\mu_1| + \cdots + |\mu_k|)\Big) - \Big((\lambda_1 + \cdots + \lambda_j) - (|\mu_1| + \cdots + |\mu_k|)\Big) \\ &\implies \mathcal{N}(\rho) = |\mu_1| + \cdots + |\mu_k|. \end{aligned} \tag{5.1.14}$$

The *logarithmic negativity* $E_{\mathcal{N}}(\rho)$ is defined to be

$$E_{\mathcal{N}}(\rho) = \log[Tr[|\tilde{\rho}|]]. \tag{5.1.15}$$

We now prove the following theorem which expresses $\mathcal{N}(\rho)$ and $E_{\mathcal{N}}(\rho)$ for a two-mode Gaussian state in terms of the symplectic eigenvalues of $\tilde{\boldsymbol{\sigma}}$. To prove this we follow the discussion in [**27**].

THEOREM 4. *Let $\tilde{\nu}_+ \geq \tilde{\nu}_-$ be the symplectic eigenvalues of $\tilde{\boldsymbol{\sigma}}$. Then*

$$\mathcal{N}(\tilde{\rho}) = Max\Big(0, \frac{1 - \tilde{\nu}_-}{2\tilde{\nu}_-}\Big), \tag{5.1.16}$$

$$E_{\mathcal{N}}(\tilde{\rho}) = Max\Big(0, -\log \tilde{\nu}_-\Big). \tag{5.1.17}$$

PROOF. Suppose first of all that $\det \boldsymbol{\gamma} \geq 0$ then as shown in the previous section there is no entanglement and $\tilde{\nu}_- \geq 1$. So the result holds in this case.

For the case $\det \boldsymbol{\gamma} < 0$, first note that for a partially transposed ρ the symplectic invariants given in Eq. (2.4.10) and Eq. (2.4.11) become

$$\Delta(\boldsymbol{\sigma}) = \det \boldsymbol{\alpha} + \det \boldsymbol{\beta} + 2 \det \boldsymbol{\gamma}, \tag{5.1.18}$$

$$\Delta(\tilde{\boldsymbol{\sigma}}) = \det \boldsymbol{\alpha} + \det \boldsymbol{\beta} - 2 \det \boldsymbol{\gamma}, \tag{5.1.19}$$

and

$$\tilde{\nu}_\pm = \sqrt{\frac{\Delta(\tilde{\boldsymbol{\sigma}}) \pm \sqrt{\Delta(\tilde{\boldsymbol{\sigma}})^2 - 4 \det \boldsymbol{\sigma}}}{2}}. \tag{5.1.20}$$

As was shown in Eq. (2.4.7), the uncertainty relation implies $\nu_- \geq 1$. It is easy to see that $\tilde{\nu}_+ \geq \nu_- \geq 1$:

$$\sqrt{\frac{\Delta(\tilde{\boldsymbol{\sigma}}) + \sqrt{\Delta(\tilde{\boldsymbol{\sigma}})^2 - 4 \det \boldsymbol{\sigma}}}{2}} \geq \sqrt{\frac{\Delta(\tilde{\boldsymbol{\sigma}})}{2}} > \sqrt{\frac{\Delta(\boldsymbol{\sigma})}{2}} \geq \sqrt{\frac{\Delta(\boldsymbol{\sigma}) - \sqrt{\Delta(\boldsymbol{\sigma})^2 - 4 \det \boldsymbol{\sigma}}}{2}} \tag{5.1.21}$$

where we also used the fact that $\det \boldsymbol{\gamma} < 0 \implies \Delta(\boldsymbol{\sigma}) \geq \Delta(\tilde{\boldsymbol{\sigma}})$.

Now, to calculate $E_{\mathcal{N}}$ we apply a symplectic transformation to diagonalize $\boldsymbol{\sigma}$:

$$\tilde{\boldsymbol{\sigma}}_D = S^T \tilde{\boldsymbol{\sigma}} S = \mathrm{Diag}[\tilde{\nu}_-, \tilde{\nu}_-, \tilde{\nu}_+, \tilde{\nu}_+]. \tag{5.1.22}$$

Let $\tilde{\rho}$ and $\tilde{\rho}_D$ be the matrices (not necessarily density matrices) corresponding to $\tilde{\boldsymbol{\sigma}}$ and $\tilde{\boldsymbol{\sigma}}_D$ respectively. We have $Tr[|\tilde{\rho}_D|] = Tr[|\tilde{\rho}|]$ since $\tilde{\rho}_D = U_S^\dagger \tilde{\rho} U_S$. Also,

$$\tilde{\rho}_D = \tilde{\rho}_- \otimes \tilde{\rho}_+ \implies Tr[|\tilde{\rho}_D|] = Tr[|\tilde{\rho}_-|] Tr[|\tilde{\rho}_+|] \tag{5.1.23}$$

where $\tilde{\rho}_\pm$ is a thermal state given by

$$\tilde{\rho}_\pm = \frac{2}{\tilde{\nu}_\pm + 1} \sum_{n=0}^{\inf} \Big(\frac{\tilde{\nu}_\pm - 1}{\tilde{\nu}_\pm + 1} \Big)^n |n\rangle\langle n|. \tag{5.1.24}$$

Using the binomial theorem we find that

$$Tr[|\tilde{\rho}_{\pm}|] = \frac{2}{|\tilde{\nu}_{\pm}+1| - |\tilde{\nu}_{\pm}-1|}. \tag{5.1.25}$$

By inspection we can see that if $\tilde{\nu}_{+} \geq 1$ then $Tr[\tilde{\rho}_{+}] = 1$ and if $\tilde{\nu}_{-} \geq 1$ then $Tr[\tilde{\rho}_{-}] = 1$. If $\tilde{\nu}_{-} < 1$ then $|\tilde{\nu}_{-}+1| = \tilde{\nu}_{-}+1$ because $\tilde{\nu}_{-} \geq 0$ by theorem 1 and $|\tilde{\nu}_{-}-1| = 1-\tilde{\nu}_{-}$. So substituting this into the expression above we obtain $Tr[|\tilde{\rho}_{-}|] = \frac{1}{\tilde{\nu}_{-}}$. To summarize, we have

$$Tr[|\tilde{\rho}_{+}|] = 1 \text{ always}, \tag{5.1.26}$$

and

$$Tr[|\tilde{\rho}_{-}|] = \begin{cases} 1 & \text{if} \quad \tilde{\nu}_{-} \geq 1 \\ \frac{1}{\tilde{\nu}_{-}} & \text{if} \quad \tilde{\nu}_{-} < 1 \end{cases}. \tag{5.1.27}$$

So

$$Tr[|\tilde{\rho}|] = \text{Max}\left(1, \frac{1}{\tilde{\nu}_{-}}\right), \tag{5.1.28}$$

implying

$$\mathcal{N}(\tilde{\rho}) = \text{Max}\Big(0, \frac{1-\tilde{\nu}_{-}}{2\tilde{\nu}_{-}}\Big), \tag{5.1.29}$$

and

$$E_{\mathcal{N}}(\tilde{\rho}) = \text{Max}\Big(0, -\log \tilde{\nu}_{-}\Big). \tag{5.1.30}$$

□

In Section 5.2 we calculate amount of entanglement for storage in quantum memories using the expression above. We also rely on a result shown in [**94**] for a two-mode Gaussian state:

THEOREM 5. *Let $\tilde{\nu}_+ \geq \tilde{\nu}_-$ be the symplectic eigenvalues of $\tilde{\boldsymbol{\sigma}}$. Then*

$$\tilde{\nu}_-^2 \geq \lambda_1 \lambda_2. \tag{5.1.31}$$

where λ_1 and λ_2 are the smallest ordinary eigenvalues of $\boldsymbol{\sigma}$.

PROOF. First note that from Proposition 1 we have that the symplectic eigenvalues $\tilde{\nu}_\pm$ are the ordinary eigenvalues of $|i\Omega\tilde{\boldsymbol{\sigma}}|$. Also the $\tilde{\nu}_-^2$ is smallest eigenvalue of both $\tilde{\Omega}^T\boldsymbol{\sigma}\tilde{\Omega}\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}^{\frac{1}{2}}\tilde{\Omega}^T\boldsymbol{\sigma}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}$ with $\tilde{\Omega} = T\Omega T$. This means that the quantity $\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}\tilde{\Omega}^T\boldsymbol{\sigma}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle$ is a function of a set of all unit vectors $|e\rangle$ in $\mathbb{R}^n$ (in $\mathbb{R}^4$ for a two-mode Gaussian state). Moreover as we vary $|e\rangle$ the smallest value of this function is $\tilde{\nu}_-^2$. So that we can define $\tilde{\nu}_-^2$ as follows:

$$\tilde{\nu}_-^2 = \inf_{|||e\rangle||=1} \langle e|\boldsymbol{\sigma}^{\frac{1}{2}}\tilde{\Omega}^T\boldsymbol{\sigma}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle. \tag{5.1.32}$$

We can also define $\tilde{\nu}_-^2$ as

$$\tilde{\nu}_-^2 = \inf_{|||e\rangle=1||} \langle e_\sigma|\boldsymbol{\sigma}^{\frac{1}{2}}|e_\sigma\rangle\langle e|\boldsymbol{\sigma}|e\rangle, \tag{5.1.33}$$

where

$$|e_\sigma\rangle = \frac{1}{\sqrt{\langle e|\boldsymbol{\sigma}|e\rangle}}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle, \tag{5.1.34}$$

with $\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle = 0$ and $\langle e_\sigma|e_\sigma\rangle = 0$. Then we have

$$\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}|e_\sigma\rangle = \frac{1}{\sqrt{\langle e|\boldsymbol{\sigma}|e\rangle}}\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle = 0. \tag{5.1.35}$$

since $\boldsymbol{\sigma}^{\frac{1}{2}}\tilde{\Omega}\boldsymbol{\sigma}^{\frac{1}{2}}$ is antisymmetric. We can define a bigger set varying a more general vector, that is independent of $|e\rangle$, $|e'\rangle$ but still imposing the same condition as we imposed on $|e_\sigma\rangle$: $\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}|e'\rangle = 0$. Then we have the following inequality

$$\tilde{\nu}_-^2 \geq \inf_{|||e\rangle||=|||e'\rangle||=1} \langle e'|\boldsymbol{\sigma}|e'\rangle\langle e|\boldsymbol{\sigma}|e\rangle. \tag{5.1.36}$$

The RHS of this inequality is in fact product of the two smallest ordinary eigenvalues of $\boldsymbol{\sigma}$. This is straightforward to see. We write $|e\rangle$ and $|e'\rangle$ as a superposition of

vectors $|1\rangle$ and $|2\rangle$ corresponding to the eigenvectors of the smallest eigenvalues λ_1 and λ_2 respectively. So $|e\rangle = \cos\theta|1\rangle + \sin\theta|2\rangle$ and $|e'\rangle = \cos\phi|1\rangle + \sin\phi|2\rangle$. Then,

$$\langle e|\boldsymbol{\sigma}^{\frac{1}{2}}|e\rangle = \lambda_1 \cos^2\theta + \lambda_2 \sin^2\theta \tag{5.1.37}$$

and

$$\langle e'|\boldsymbol{\sigma}^{\frac{1}{2}}|e'\rangle = \lambda_1 \cos^2\phi + \lambda_2 \sin^2\phi. \tag{5.1.38}$$

We can eliminate $\cos\phi$ and $\sin\phi$ using

$$\langle e|\boldsymbol{\sigma}|e'\rangle = \sqrt{\lambda_1}\cos\theta\cos\phi + \sqrt{\lambda_2}\sin\theta\sin\phi = 0, \tag{5.1.39}$$

implying

$$\cos\phi = -\frac{k\sqrt{\lambda_2}}{\cos\theta}, \tag{5.1.40}$$

and

$$\sin\phi = \frac{k\sqrt{\lambda_1}}{\sin\theta}, \tag{5.1.41}$$

for some k. So we have

$$\cos^2\phi + \sin^2\phi = k^2\Big(\frac{\lambda_2}{\cos^\theta} + \frac{\lambda_1}{\sin^2\theta}\Big) = 1, \tag{5.1.42}$$

implying

$$k^2 = \frac{\sin^2\theta\cos^2\theta}{\lambda_1\cos^2\theta + \lambda_2\sin^2\theta}. \tag{5.1.43}$$

Substituting this into $\langle e'|\boldsymbol{\sigma}^{\frac{1}{2}}|e'\rangle$ we get

$$\langle e'|\boldsymbol{\sigma}^{\frac{1}{2}}|e'\rangle = k^2\lambda_1\lambda_2\Big(\frac{1}{\cos^2\theta} + \frac{1}{\sin^2\theta}\Big) \tag{5.1.44}$$

$$= \frac{\sin^2\theta\cos^2\theta}{\lambda_1\cos^2\theta + \lambda_2\sin^2\theta}\lambda_1\lambda_2\Big(\frac{1}{\cos^2\theta} + \frac{1}{\sin^2\theta}\Big) \tag{5.1.45}$$

$$= \frac{\lambda_1 \lambda_2}{\lambda_1 \cos^2\theta + \lambda_2 \sin^2\theta} \tag{5.1.46}$$

Then

$$\langle e'|\boldsymbol{\sigma}|e'\rangle\langle e|\boldsymbol{\sigma}|e\rangle = \frac{\lambda_1 \lambda_2}{\lambda_1 \cos^2\theta + \lambda_2 \sin^2\theta}(\lambda_1 \cos^2\theta + \lambda_2 \sin^2\theta) \tag{5.1.47}$$

$$= \lambda_1 \lambda_2. \tag{5.1.48}$$

Hence the inequality in Eq. (5.1.36) becomes

$$\tilde{\nu}_-^2 \geq \lambda_1 \lambda_2. \tag{5.1.49}$$

□

In Chapter 5.2 we use this inequality to identify a region for which the entanglement is maximum in the context of quantum memories.

5.1.2. Gaussian channels. A Gaussian channel is a channel which gives a Gaussian state as output whenever a Gaussian is fed in as input. In this section we are going to derive an expression for the most general possible Gaussian channel on the CM $\boldsymbol{\sigma}$.

The effect of a general Gaussian channel on the density matrix ρ is given by

$$\rho \to Tr_A[U^\dagger \rho \otimes \rho_A U], \tag{5.1.50}$$

where ρ_A is the Gaussian state of an ancilla and U is a symplectic unitary. The role of ρ_A is to allow us to model interaction with the environment. In particular, it allows us to model the effect of decoherence. Note that, since in the CM description tensor products correspond to direct sums, partial tracing is equivalent to taking the main submatrix corresponding to the reduced degrees of freedom. Thus in terms of covariance matrices we have

$$\boldsymbol{\sigma} \to [S^T(\boldsymbol{\sigma} \oplus \boldsymbol{\sigma}_A)S]_{11} \tag{5.1.51}$$

where $\boldsymbol{\sigma}$ is the CM of ρ, $\boldsymbol{\sigma}_A$ is the CM of ρ_A, S is the symplectic matrix corresponding to the unitary U and subscript 11 signifies that we take the top left hand block of the matrix. Let

$$S = \begin{pmatrix} \mathbf{x} & \mathbf{y} \\ \mathbf{z} & \mathbf{w} \end{pmatrix}, \qquad \boldsymbol{\sigma} = \begin{pmatrix} \boldsymbol{\sigma}_0 & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\sigma}_A \end{pmatrix}. \tag{5.1.52}$$

Then we have

$$\begin{aligned} S^T\boldsymbol{\sigma}S &= \begin{pmatrix} \mathbf{x}^T & \mathbf{z}^T \\ \mathbf{y}^T & \mathbf{w}^T \end{pmatrix} \begin{pmatrix} \boldsymbol{\sigma}_0 & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\sigma}_A \end{pmatrix} \begin{pmatrix} \mathbf{x} & \mathbf{y} \\ \mathbf{z} & \mathbf{w} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{x}^T & \mathbf{z}^T \\ \mathbf{y}^T & \mathbf{w}^T \end{pmatrix} \begin{pmatrix} \boldsymbol{\sigma}_0\mathbf{x} & \boldsymbol{\sigma}_0\mathbf{y} \\ \boldsymbol{\sigma}_A\mathbf{z} & \boldsymbol{\sigma}_A\mathbf{w} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{x}^T\boldsymbol{\sigma}_0\mathbf{x} + \mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{z} & \mathbf{x}^T\boldsymbol{\sigma}_0\mathbf{y} + \mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{w} \\ \mathbf{y}^T\boldsymbol{\sigma}_0\mathbf{x} + \mathbf{w}^T\boldsymbol{\sigma}_A\mathbf{z} & \mathbf{y}^T\boldsymbol{\sigma}_0\mathbf{y} + \mathbf{w}^T\boldsymbol{\sigma}_A\mathbf{w} \end{pmatrix} \end{aligned} \tag{5.1.53}$$

So,

$$\left[\begin{pmatrix} \mathbf{x}^T\boldsymbol{\sigma}_0\mathbf{x} + \mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{z} & \mathbf{x}^T\boldsymbol{\sigma}_0\mathbf{y} + \mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{w} \\ \mathbf{y}^T\boldsymbol{\sigma}_0\mathbf{x} + \mathbf{w}^T\boldsymbol{\sigma}_A\mathbf{z} & \mathbf{y}^T\boldsymbol{\sigma}_0\mathbf{y} + \mathbf{w}^T\boldsymbol{\sigma}_A\mathbf{w} \end{pmatrix}\right]_{11} = \mathbf{x}^T\boldsymbol{\sigma}_0\mathbf{x} + \mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{z} \tag{5.1.54}$$

where $\mathbf{x} = X$ and $\mathbf{z}^T\boldsymbol{\sigma}_A\mathbf{z} = Y$. So the most general Gaussian channel is given by

$$\boldsymbol{\sigma} \to X^T\boldsymbol{\sigma}X + Y. \tag{5.1.55}$$

This is the expression we wanted to derive. However, we are still not finished because we cannot put just any pair of matrices X and Y in this equation as the uncertainty principle Eq. (2.4.3) imposes some restrictions. To see this observe first of all Eq. (2.3.1) implies

$$S^T \begin{pmatrix} \Omega_0 & 0 \\ 0 & \Omega_A \end{pmatrix} S = \begin{pmatrix} \Omega_0 & 0 \\ 0 & \Omega_A \end{pmatrix}. \tag{5.1.56}$$

Evaluating the RHS of this equation we find

$$S^T \begin{pmatrix} \Omega_0 & 0 \\ 0 & \Omega_A \end{pmatrix} S = \begin{pmatrix} \mathbf{x}^T & \mathbf{z}^T \\ \mathbf{y}^T & \mathbf{w}^T \end{pmatrix} \begin{pmatrix} \Omega_0 \mathbf{x} & \Omega_0 \mathbf{y} \\ \Omega_A \mathbf{z} & \Omega_A \mathbf{w} \end{pmatrix} \tag{5.1.57}$$

implying

$$\begin{pmatrix} \mathbf{x}^T \Omega_0 \mathbf{x} + \mathbf{z}^T \Omega_A \mathbf{z} & \mathbf{x}^T \Omega_0 \mathbf{y} + \mathbf{z}^T \Omega_A \mathbf{w} \\ \mathbf{y}^T \Omega_0 \mathbf{x} + \mathbf{w}^T \Omega_A \mathbf{z} & \mathbf{y}^T \Omega_0 \mathbf{y} + \mathbf{w}^T \Omega_A \mathbf{w} \end{pmatrix} = \begin{pmatrix} \Omega_0 & 0 \\ 0 & \Omega_A \end{pmatrix}. \tag{5.1.58}$$

So

$$\mathbf{x}^T \Omega_0 \mathbf{x} + \mathbf{z}^T \Omega_A \mathbf{z} = \Omega_0 \tag{5.1.59}$$

From $\boldsymbol{\sigma}_A + i\Omega_A \geq 0$ we have

$$\begin{aligned} & \mathbf{z}^T \boldsymbol{\sigma}_A \mathbf{z} + i \mathbf{z}^T \Omega_A \mathbf{z} \geq 0 \\ \implies & Y + i \mathbf{z}^T \Omega_A \mathbf{z} \geq 0 \\ \implies & i \mathbf{z}^T \Omega_A \mathbf{z} \geq -Y. \end{aligned} \tag{5.1.60}$$

Multiplying both sides of Eq. (6.3.84) by i we get

$$\begin{aligned} & i \mathbf{x}^T \Omega_0 \mathbf{x} + i \mathbf{z}^T \Omega_A \mathbf{z} = i \Omega_0 \\ \implies & i \mathbf{z}^T \Omega_A \mathbf{z} = i \Omega_0 - i \mathbf{x}^T \Omega_0 \mathbf{x}. \end{aligned} \tag{5.1.61}$$

Eq. (5.1.60) implies

$$i \Omega_0 - i \mathbf{x}^T \Omega_0 \geq -Y, \tag{5.1.62}$$

or

$$i \Omega_0 - i \mathbf{x}^T \Omega_0 + Y \geq 0. \tag{5.1.63}$$

This is the constraint that X and Y have to satisfy due to the uncertainty principle. These results will play a crucial role in our discussion in the next section of entanglement storage in an atomic cloud.

We describe the evolution inside the atomic cloud by the equation $\sigma \rightarrow X^T \boldsymbol{\sigma} X +$ Y where

$$X = \text{Diag}[e^{-\frac{\Gamma_1}{2}t}, e^{-\frac{\Gamma_1}{2}t}, e^{-\frac{\Gamma_2}{2}t}, e^{-\frac{\Gamma_1}{2}t}], \tag{5.1.64}$$

$$Y = \text{Diag}[(2n+1)(1-e^{-\Gamma_1 t}), (2n+1)(1-e^{-\Gamma_1 t}), (2m+1)(1-e^{-\Gamma_2 t}), (2m+1)(1-e^{-\Gamma_2 t})], \tag{5.1.65}$$

with

$$n = \frac{1}{e^{\frac{\omega_s t}{kT_n}} - 1}, \qquad\qquad m = \frac{1}{e^{\frac{\omega_s t}{kT_m}} - 1}. \tag{5.1.66}$$

The X and Y operators model the interaction of the two modes with independent Markovian baths with average photon numbers n and m, respectively, and loss rates Γ_1 and Γ_2 (depending on the strength of the system-bath interaction). Eq. (5.1.66) gives the relationship between the temperatures of the two independent baths and their average numbers of excitations (according to the standard Bose-Einstein statistics). We also describe the entanglement process using a beam splitter by the equation

$$\boldsymbol{\sigma} \rightarrow R^T \boldsymbol{\sigma} R, \tag{5.1.67}$$

where R is the rotation matrix given in Eq.(5.3.6). In the beam splitter the evolution is unitary. There is no interaction with the environment and so $Y = 0$.

5.2. Entanglement storage in CV quantum memories

In this chapter we investigate entanglement generation and storage in the context of QND-feedback quantum memories where we use symplectic eigenvalues of the covariance matrix of corresponding state to measure the amount of entanglement. In particular, we examine the question whether in a quantum memory it is

better to store states that are already entangled or whether it is better to only entangle them after storage. Some of the work in this Chapter has been published in Yadsan-Appleby and Serafini [**87**]. We are considering general Gaussian dissipative channels (encompassing the description of thermalisation by contact with reservoir) acting on Gaussian states. We describe two different quantum optical situations. In the context of quantum memories the first case is analogous to storing squeezing, while the second case would correspond to storing entanglement. In the former case, the squeezed light is entangled using a beam splitter after interacting with the environment. In the latter case, the squeezed light is entangled using a beam splitter and then it interacts with the environment. Given a fixed amount of noise, we then compare decoherence produced in the two cases in terms of final entanglement. This enables us to identify optimized strategies to create entanglement depending on the noise and system parameters.

5.2.1. Quantum memories. One of the foundational results of quantum information is the no cloning theorem. The theorem states that the quantum state of a system cannot be copied. This constitutes a challenge for quantum information processes where one wants to store information for later use. A quantum memory is such a system that stores quantum states faithfully. There are many different approaches to implement such a system, depending on the task that the memory is to perform. Some of these approaches are; optical delay lines and cavities, electromagnetic induced transparency (EIT) [**95**, **96**], Duan, Lukin, Cirac and Zoller (DLCZ) protocol which is the basis for Raman memory in atomic gases [**97**], photon-echo quantum memory [**98**–**100**], atomic frequency combs (AFC) [**101**], off-resonant Faraday interaction between light and atoms, also known as quantum nondemolition (QND)-Faraday intereaction [**102**, **103**]. Perhaps one of their most important application is quantum repeaters [**104**–**106**]. They have also applications in deterministic single photon sources [**107**–**109**], loophole-free Bell test [**110**,**111**], communication complexity and protocols requiring local operations and classical communication (LOCC) [**112**–**116**], precision measurements [**104**]. Performance

criteria for a quantum memory are the fidelity, the efficiency, storage time, bandwidth, capacity to store multiple photons and dimensionality, wavelength [**104**].

This thesis is concerned with the applications that exploit QND-Faraday interactions. Using this approach a protocol for storing a quantum state of photons in an atomic cloud has been constructed [**81**]. The incident light interacted with a two-level atomic cloud which consisted of caesium atoms. The transmitted light was measured and then the state of measured light was mapped back onto the atomic cloud. The fidelity achieved was 70%. This is better than what could be achieved classically, by measuring and re-preparing the state. The classical fidelity is the maximal fidelity that can be achieved by measure and prepare strategies. For a set of coherent states equally distributed in phase space, that equals to 1/2 [**76**]. For squeezed states and finite distributions of first moments, it can be calculated by semi-definite-programming [**117**, **118**].

The latest developments in this approach are discussed in [**103**]. Most recently, [**82**] implemented a quantum memory to store EPR entangled states. These were multi-photon states and two-mode squeezed by $6dB$. The storage time was about $1ms$ and the fidelity was 0.52 ± 0.02 which exceeds the best possible classical value.

The specific question we investigate in this thesis is whether the resulting state will be more entangled if we first store the light and entangle it only when we need to use it or first entangle it then store it. More explicitly "given that the state is squeezed, in the presence of noise can we improve the generation of entanglement by choosing the timing of a passive operation?" The answer turns out to be "yes the timing of the entanglement affects the amount of entanglement in the resulting state". In the next chapter, we investigate this protocol further and we identify optimized strategies to create entanglement depending on noise parameters. First we give a brief description of light storage in atomic clouds.

5.2.2. Storing light in atomic clouds. A cloud of atoms at room temperature can be used to store quantum continuous variables in certain conditions. Each atom of such clouds acts like a qubit, where the relevant two quantum levels are two

distinct electronic states. Such degrees of freedom are also called pseudo-spins, in analogy with the electron spin 1/2. By the Holstein-Primakoff construction, which we will now sketch, the angular momentum operators to which the field quadratures couple can be regarded as approximately canonical for a large number of pseudo-spins. In fact, collective pseudo-spins in the cloud are described by sums of Pauli operators, each defined in the Hilbert space of one atom:

$$\sigma_k^{(a)} = \sum_{j=1}^{N} \sigma_k^{(j)},$$

where $k = x, y, z$ and

$$[\sigma_+^{(a)}, \sigma_-^{(a)}] = 2\sigma_z^{(a)}.$$

Here, $\sigma_+^{(a)} = \sigma_x^{(a)} + i\sigma_y^{(a)}$ and $\sigma_-^{(a)} = \sigma_x^{(a)} - i\sigma_y^{(a)}$.

If N, the number of spins in the cloud, is very large and if the cloud is very polarised along the z axis (which may be achieved by preparing all the atoms in the ground state), then $\sigma_z^{(a)}$ can be replaced by its mean value:

$$[\sigma_+^{(a)}, \sigma_-^{(a)}] \approx 2\langle\sigma_z^{(a)}\rangle I \ .$$

Then we can define an operator a such that

$$a = \frac{1}{\sqrt{c}}\sigma_-^{(a)}, \qquad\qquad a^\dagger = \frac{1}{\sqrt{c}}\sigma_+^{(a)},$$

and so

$$\Rightarrow [a, a^\dagger] \approx I. \tag{5.2.1}$$

So, the system behaves like a CV system to a good approximation. Let us finally define the atomic canonical quadrature operators:

$$\hat{X}_A = \frac{a + a^\dagger}{\sqrt{2}},$$

$$\hat{P}_A = \frac{a - a^\dagger}{i\sqrt{2}}.$$

In the following, we will further approximate the description of the atoms as a continuum of canonical operators $\hat{X}(z)$ and $\hat{P}(z)$, where the variable z, representing the spatial direction along the direction of propagation of a light beam through the atomic ensemble.

5.2.3. The dynamics of a quantum memory. We will now briefly describe the operation (storage and retrieval) of an atomic cloud quantum memory. We will mainly follow the treatment found in [**103**].

A Quantum Non-Demolition interaction (or Faraday interaction) is an interaction between the light and atomic cloud in which every atom is a Λ system. In a Λ system each atom is a 3-level system as shown in Fig. 3 below. In this description there is no coupling between the states $|0\rangle$ and $|1\rangle$. The state $|0\rangle$ is coherently coupled to state $|e\rangle$ through the electromagnetic field, with a coupling constant g, and the state $|e\rangle$ is in turn coupled to another state $|1\rangle$. In a Λ system the levels of excited state $|e\rangle$ are only virtually populated and so can be eliminated via adiabatic elimination. After adiabatic elimination, the Hamiltonian for such a system is given by

$$\hat{H} = -\int \kappa(z)\hat{P}_L(z)\hat{P}_A(z)dz, \tag{5.2.2}$$

where $\hat{P}_A(z)$ is the collective atomic pseudo-spin operator defined in the previous section, and $\hat{P}_L$ is the quadrature of light at position z along the direction of propagation of light. The constant κ is the coupling constant given by

$$\kappa^2 = \int_0^T dt \frac{|\Omega(t)|^2}{2\Delta^2} \int dz |g(z)|^2, \tag{5.2.3}$$

T is the time that takes the light pulse to pass through the atomic cloud, Ω is the Rabi frequency driven by the classical laser while $g(z)$ is the coherent dipole coupling strength at position z.

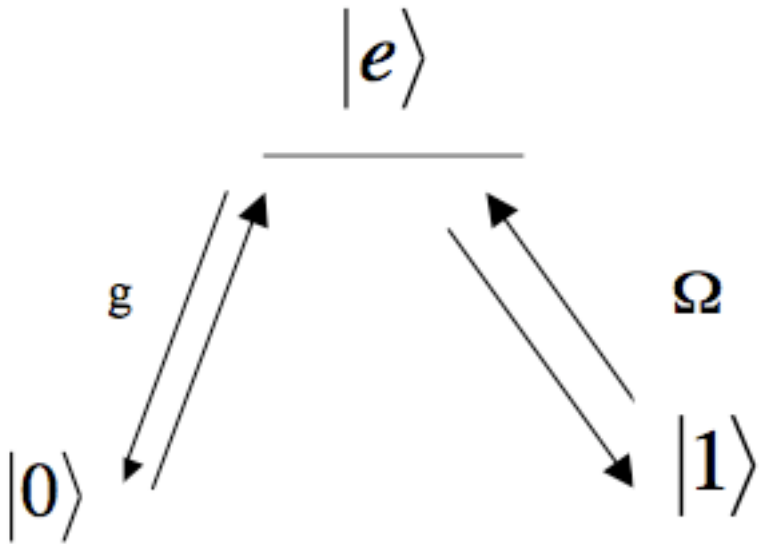


FIGURE 3. A three level atom.

As an aside, let us mention that the term "QND" interaction comes from the fact that, in principle, such an interaction would allow one to measure the state of the atoms by measuring the state of light. To see this, let the state of the atomic cloud be $|\psi_A\rangle$, suppose that we want to know $\hat{P}_A$ and that the atom-light Hamiltonian is given by $\hat{P}_A\hat{P}_L$. Assume that the initial combined state of the atomic cloud and the light is $|\psi_A\rangle \otimes |X'_L\rangle$, with $\hat{X}_L|X'_L\rangle = X'_L|X'_L\rangle$. Then after time t the combined state evolves as

$$\begin{aligned} e^{-i\hat{H}t}|\psi_A\rangle \otimes |X'_L\rangle &= \int dP_A \psi_A(P_A) e^{-i\kappa \hat{P}_A \hat{P}_L t}|P_A\rangle \otimes |X'_L\rangle \\ &= \int dP_A \psi_A(P_A)|P_A\rangle \otimes e^{-i\kappa P_A \hat{P}_L t}|X'_L\rangle \\ &= \int dP_A \psi_A(P_A)|P_A\rangle \otimes |X'_L + \kappa t P_A\rangle \ . \end{aligned} \tag{5.2.4}$$

So the resulting state of the measurement of $\hat{X}_L$ is $|X'_L + \kappa t P_A\rangle$. This means that the state of the atomic cloud $|\psi_A\rangle$ collapses into $|P_A\rangle$ with probability density $|\psi_A(P_A)|^2$, thus realising the quantum non demolition measurement process.

One passage of QND interacting light through the atomic ensemble leads to the following input-output relationships:

$$\begin{aligned}
\hat{X}_{L,out} &= \hat{X}_{L,in} + \kappa \hat{P}_{A,t_0} \,, \\
\hat{P}_{L,out} &= \hat{P}_{L,in} \,, \\
\hat{X}_{A,t_f} &= \hat{X}_{A,t_0} + \kappa \hat{P}_{L,in} \,, \\
\hat{P}_{A,t_f} &= \hat{P}_{A,t_0} \,,
\end{aligned}$$

where the subscripts *in* and *out* indicate the quadratures corresponding to the states of the light beam as it enters and leaves the atomic cloud respectively, and the times t_0 and t_f indicate the quadratures corresponding to the state of the atomic cloud initially (just before the light beam enters the cloud), and finally (after the light beam has left the cloud respectively).

An ideal storage process needs to map the input light operators into the final atomic ones. This is done by resorting to a feedback loop, where the output light is measured by a balanced homodyne detection to adjust the operators $\hat{X}_A$ and $\hat{P}_A$. The feedback loop is described by the following process. Firstly, $\hat{X}_{L,out}$ is measured, then $\hat{P}_{A,t_f}$ is displaced to $\hat{P}_{A,t_f} + h\zeta$, where h is the feedback gain and ζ is the measurement outcome. Including the feedback loop we hence have

$$\hat{P}_{A,t_f} \to \hat{P}_{A,t_f} + h\hat{X}_{L,out} = \hat{P}_{A,t_0} + h\hat{X}_{L,in} + h\kappa\hat{P}_{A,t_0}, \tag{5.2.5}$$

we choose $h = -\frac{1}{\kappa}$ so that

$$\hat{P}_{A,t_f} \to -\frac{1}{\kappa}\hat{X}_{L,in} \,. \tag{5.2.6}$$

So, for the storage with feedback we have

$$\hat{X}_{A,t_f} = \hat{X}_{A,t_0} + \kappa \hat{P}_{L,in}, \tag{5.2.7}$$

$$\hat{P}_{A,t_f} = -\frac{1}{\kappa}\hat{X}_{L,in}. \tag{5.2.8}$$

This input–output relations hold when spontaneous emission and losses are neglected, which we are referring to as the 'ideal memory' case.

For retrieval, two passages of light go through the cell, and a phase shifter is applied to light between the two passages through the cloud [**75**]. One has then (with primed operators referring to the retrieval step of the memory operation):

$$\hat{X}'_{L,out} = -\hat{X}'_{A,t_0}, \tag{5.2.9}$$

$$\hat{P}'_{L,out} = -\kappa \hat{X}'_{L,in} - \hat{P}'_{A,t_0}. \tag{5.2.10}$$

For the storage and retrieval, one has then simply to chain the two input-output relationships above, setting $\hat{X}_{A,t_f} = \hat{X}'_{A,t_0}$ and $\hat{P}_{A,t_f} = \hat{P}'_{A,t_0}$ to obtain

$$\hat{X'}_{L,out} = -\hat{X}_{A,t_0} - \kappa \hat{P}_{L,in}, \tag{5.2.11}$$

$$\hat{P'}_{L,out} = \kappa \hat{X}'_{L,in} + \frac{1}{\kappa}\hat{X}_{L,in}. \tag{5.2.12}$$

We also apply a final phase shift ($\hat{X}_{L,out} = \hat{P'}_{L,out}$ and $\hat{P}_{L,out} = -\hat{X'}_{L,out}$), for ease of notation:

$$\hat{X}_{L,out} = \kappa \hat{X}'_{L,in} + \frac{1}{\kappa}\hat{X}_{L,in}, \tag{5.2.13}$$

$$\hat{P}_{L,out} = \hat{X}_{A,t_0} + \kappa \hat{P}_{L,in}. \tag{5.2.14}$$

Let us now consider the corresponding CM:

$$\boldsymbol{\sigma}_{L,out} = \begin{pmatrix} 2\kappa^2\langle \hat{X}'^2_{L,in}\rangle + \frac{2}{\kappa^2}\langle \hat{X}^2_{L,in}\rangle & \langle\{\hat{X}_{L,t_0}, \hat{P}_{L,in}\}\rangle \\ \langle\{\hat{X}_{L,t_0}, \hat{P}_{L,in}\}\rangle & 2\langle \hat{X}^2_{A,t_0}\rangle + 2\kappa^2\langle \hat{P}^2_{L,in}\rangle \end{pmatrix}, \tag{5.2.15}$$

which can be written as

$$\boldsymbol{\sigma}_{L,out} = X\boldsymbol{\sigma}_{L,in}X^T + Y \ , \tag{5.2.16}$$

where $\boldsymbol{\sigma}_{L,in}$ is the CM of light before storage and retrieval in the memory, and

$$X = \begin{pmatrix} \frac{1}{\kappa} & 0 \\ 0 & \kappa \end{pmatrix}, \tag{5.2.17}$$

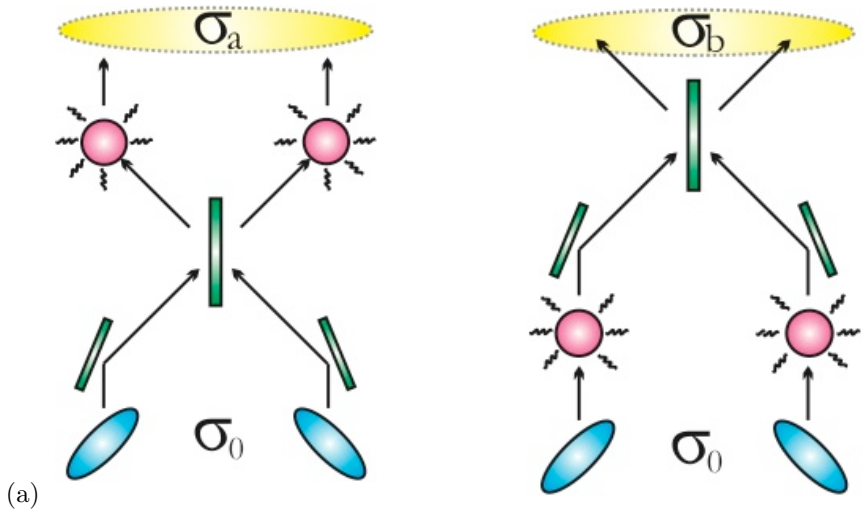
$$Y = \begin{pmatrix} 2\kappa^2\langle \hat{X}'_{L,in}\rangle & 0 \\ 0 & 2\langle \hat{X}^2_{A,t_0}\rangle \end{pmatrix}. \tag{5.2.18}$$

Ideally, one could set $Y = 0$ by squeezing the quadratures $\hat{X}_A$ and $\hat{X}_L$, thus obtaining perfect storage and retrieval upon setting $\kappa = 1$.

5.3. Would one rather store squeezing or entanglement in CV quantum memories?

We consider following two cases. One could either store an entangled state and retrieve it directly from the memory, or rather store two separate single-mode squeezed states and then combine them with a beam splitter to generate the final entangled state. The first case corresponds to entangling the squeezed light first and then storing it and the second case corresponds to storing the squeezed light first and only entangling it when we want to use the state. Let ρ_0 be the initial state, ρ_a be the final state for the first case and ρ_b be the final state of the second case where subscript a stands for *after* indicating storage after entanglement and subscript b stands for *before* indicating storage before entanglement. Let the CM corresponding to ρ_0 be $\boldsymbol{\sigma}_0$, the CM corresponding to ρ_a be $\boldsymbol{\sigma}_a$ and the CM corresponding to ρ_b be $\boldsymbol{\sigma}_b$. Then the noise in the two system is described as

$$\begin{aligned} \boldsymbol{\sigma}_a &= XR\boldsymbol{\sigma}_0R^TX^T + Y \\ \boldsymbol{\sigma}_b &= RX\boldsymbol{\sigma}_0X^TR^T + RYR^T \end{aligned} \tag{5.3.1}$$



(a)

FIGURE 4. The two cases being compared: in (a), the state is stored in the memory cells *after* the beam splitter has mixed and entangled the single-mode squeezed states; in (b), the state is stored *before* the entangling beam-splitting action. We assume that all the noise is imputable to the storage and retrieval processes.

where X and Y are given in Eq. (5.1.64) and Eq. (5.1.65) respectively. The matrix R describes the action of the beam-splitter.

In the following we first consider ideal or nearly ideal memories and then noisy memories.

5.3.1. Ideal memories. The work we present in this section has been presented in Yadsan-Appleby and Serafini [**87**]. For ideal memories [**77**] we define X and Y as follows:

$$X = \mathrm{Diag}[1, 1, 1, 1]$$
$$Y = \mathrm{Diag}[y_{q1}, 0, y_{q2}, 0] \tag{5.3.2}$$

where $y_{q1} = \big(1 - \frac{1}{Z_1^2}\big)\Delta_{AT1}$ is the noise in the first quadrature and $y_{q2} = \big(1 - \frac{1}{Z_2^2}\big)\Delta_{AT2}$ is the noise in the second quadrature. Here, the parameters Z_1 and Z_2 depend on the optical detuning of the swap interaction and take the value $\sqrt{6.4}$ [**82**] and Δ_{AT1}, Δ_{AT2} are the initial variances of one of the quadratures of the collective

atomic pseudo-spin in the two memory cells. We also define the CM $\boldsymbol{\sigma}_0$ as

$$\boldsymbol{\sigma}_0 = \mathrm{Diag}[sN_1, \frac{N_1}{s}, \frac{N_2}{s}, N_2 s] \tag{5.3.3}$$

with $s \geq 1$, $N_1 \geq 1$ and $N_2 \geq 1$. For $N_1 = N_2 = 1$ this CM describes two pure single-mode squeezed states with optical phases chosen so as to optimize the production of entanglement by a 50:50 beam-splitter [**94**]. Given that

$$\frac{1}{s^2} \leq \frac{N_2}{N_1} \leq s^2 \tag{5.3.4}$$

we have

$$y_{q2} \geq y_{q1} \iff E_{\mathcal{N}}(\rho_a) \geq E_{\mathcal{N}}(\rho_b). \tag{5.3.5}$$

Proof. Define

$$\begin{aligned} R_\theta &= \begin{pmatrix} \cos\theta I & \sin\theta I \\ -\sin\theta I & \cos\theta I \end{pmatrix}, \\ R_0 &= I, \\ R_{\frac{\pi}{4}} &= R = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ -I & I \end{pmatrix}. \end{aligned} \tag{5.3.6}$$

We also define following matrices

$$\begin{aligned} \boldsymbol{\sigma}_\theta &= R\boldsymbol{\sigma}_0 R^T + R_\theta Y R_\theta^T, \\ \boldsymbol{\sigma}_0 &= \boldsymbol{\sigma}_a, \\ \boldsymbol{\sigma}_{\frac{\pi}{4}} &= \boldsymbol{\sigma}_b, \end{aligned} \tag{5.3.7}$$

where $\boldsymbol{\sigma}_\theta$ interpolates over θ continuously between $\theta = 0$ and $\theta = \frac{\pi}{4}$. This means that the symplectic eigenvalues and hence the logarithmic negativity also interpolate over θ since they are functions of symplectic invariants $\Delta(\tilde{\boldsymbol{\sigma}}_\theta)$ and $\det \boldsymbol{\sigma}_\theta$.

From Eq. (5.1.20) we have

$$\tilde{\nu}_-^2(\theta) = \frac{\Delta(\tilde{\boldsymbol{\sigma}}_\theta) - \sqrt{\Delta^2(\tilde{\boldsymbol{\sigma}}_\theta) - 4\det\boldsymbol{\sigma}_\theta}}{2}. \tag{5.3.8}$$

Differentiating this we get

$$\frac{d\tilde{\nu}_-^2(\theta)}{d\theta} = k(y_{q_2} - y_{q1}), \tag{5.3.9}$$

where

$$k = \frac{N_1N_2(N_1s - \frac{N_2}{s}) - \tilde{\nu}_-^2(\theta)(\frac{N_1}{s} - N_2s)}{\sqrt{\Delta^2(\tilde{\boldsymbol{\sigma}}) - 4\det\boldsymbol{\sigma}_\theta}}\cos 2\theta. \tag{5.3.10}$$

First note that Eq. (5.3.4) implies $k \geq 0$. Then $y_{q2} \geq y_{q1}$ implies $\tilde{\nu}_-^2(\theta)$ is an increasing function and $y_{q2} \leq y_{q1}$ implies $\tilde{\nu}_-^2(\theta)$ is a decreasing function by Eq. (5.3.9). □

It follows from Eq. (5.3.5) that, under the adopted configuration of optical phases, storing entanglement is advantageous over storing single-mode squeezing if the noise acting on the second quadrature is larger than the noise acting on the first quadrature, and vice versa. In other words, the optimal storage is the one whereby the variance of the noisier quadrature is the larger before the storage takes place, and hence is the more robust in the face of the noise.

5.3.2. Noisy memories. In the work presented in this section we consider the same experimental situation as in Fig. 4 with the different region of parameter space and analyzing it using a different method. In this case we define the matrix Y in Eq. (5.1.65) as

$$Y = \mathrm{Diag}[1-\lambda^2, 1-\lambda^2, 1-\mu^2, 1-\mu^2], \tag{5.3.11}$$

taking $n = m = 0$ in Eq. (5.1.66) with $\lambda = e^{-\frac{\Gamma_1 t}{2}}$, $\mu = e^{-\frac{\Gamma_2 t}{2}}$. We also rewrite matrix X in Eq. (5.1.64) in terms of λ and μ:

$$X = \mathrm{Diag}[\lambda, \lambda, \mu, \mu]. \tag{5.3.12}$$

We take the initial CM $\boldsymbol{\sigma}_0$ to be

$$\boldsymbol{\sigma}_0 = \mathrm{Diag}[r, \frac{1}{r}, \frac{1}{s}, s], \tag{5.3.13}$$

where r and s are squeezing parameters. The effect of noise on the $\boldsymbol{\sigma}_0$ is described as before, in Eq. (5.3.1) with the resulting states with CMs $\boldsymbol{\sigma}_a$ and $\boldsymbol{\sigma}_b$. It follows from the Eq. (5.1.30) that the smallest symplectic eigenvalue of the CM, $\tilde{\boldsymbol{\sigma}}$, corresponding the partially transposed state is the state that has the maximum entanglement. The effect of partial transposition on $\boldsymbol{\sigma}_a$ and $\boldsymbol{\sigma}_b$ is

$$\begin{aligned} \tilde{\boldsymbol{\sigma}}_b &= T\boldsymbol{\sigma}_b T, \\ \tilde{\boldsymbol{\sigma}}_a &= T\boldsymbol{\sigma}_a T. \end{aligned} \tag{5.3.14}$$

where T is given in Eq. (5.1.1). In Proposition 1 we have shown that the symplectic eigenvalues of $\boldsymbol{\sigma}$ are the same as the ordinary eigenvalues of $|i\Omega\boldsymbol{\sigma}|$. Furthermore calculating the eigenvalues of $(i\Omega\boldsymbol{\sigma})^2$ rather than $|i\Omega\boldsymbol{\sigma}|$ of considerably reduces the amount of algebra. Multiplying Eq. (5.3.14) by $i\Omega$ then squaring it we get the partially transposed symplectic eigenvalues, $\tilde{\nu}_b^2$ and $\tilde{\nu}_a^2$:

$$\begin{aligned} \tilde{\nu}_b^2 &= (i\Omega\tilde{\boldsymbol{\sigma}}_b)^2 = -\Omega\tilde{\boldsymbol{\sigma}}_b\Omega\tilde{\boldsymbol{\sigma}}_b = -\Omega T\boldsymbol{\sigma}_b T\Omega T\boldsymbol{\sigma}_b T, \\ \tilde{\nu}_a^2 &= (i\Omega\tilde{\boldsymbol{\sigma}}_a)^2 = -\Omega\tilde{\boldsymbol{\sigma}}_a\Omega\tilde{\boldsymbol{\sigma}}_a = -\Omega T\boldsymbol{\sigma}_a T\Omega T\boldsymbol{\sigma}_a T. \end{aligned} \tag{5.3.15}$$

We found and simplified the following expressions. Note that the symplectic eigenvalues come in pairs by the definition given in Eq. (2.3.8). So for a two-mode Gaussian state we have two symplectic eigenvalues. Below are the expressions for the two systems we have described in section 5.2.

$$\begin{aligned} \tilde{\nu}_{b1}^2 &= (1 - \lambda^2 + r\lambda^2)(1 - \mu^2 + s\mu^2), \\ \tilde{\nu}_{b2}^2 &= \frac{(-r - \lambda^2 + r\lambda^2)(-s - \mu^2 + s\mu^2)}{rs}. \end{aligned}$$

and

$$\tilde{\nu}_{a1}^2 = \frac{1}{8rs}\Big(2s\lambda^2+\lambda^4-2s\lambda^4+2s\mu^2+2\lambda^2\mu^2+\mu^4-2s\mu^4+r^2s((-2+s)\lambda^4+2\mu^2 \\ +(-2+s)\mu^4+2\lambda^2(1+s\mu^2))+2r(\lambda^2-\lambda^4+\mu^2-\mu^4+s^2(\lambda^2-\lambda^4+\mu^2-\mu^4) \\ +s(4+3\lambda^4-4\mu^2+3\mu^4-2\lambda^2(2+\mu^2))\Big)-\Big((-16rs(-2r-\lambda^2+2r\lambda^2-rs\lambda^2 \\ +(-1+2r-rs+2(-1+r)(-1+s)\lambda^2)\mu^2)(-2s-\lambda^2+2s\lambda^2-rs\lambda^2 \\ +(-1+2s-rs+2(-1+r)(-1+s)\lambda^2)\mu^2)+((\lambda^2+\mu^2)^2+2s(\lambda^2-\lambda^4+\mu^2-\mu^4) \\ +r^2s((-2+s)\lambda^4+2\mu^2+(-2+s)\mu^4+2\lambda^2(1+s\mu^2))+2r(\lambda^2-\lambda^4+\mu^2-\mu^4 \\ +s^2(\lambda^2-\lambda^4+\mu^2-\mu^4)+s(4-4\lambda^2+3\lambda^4-2(2+\lambda^2)\mu^2+3\mu^4)))^2))\Big)^{\frac{1}{2}},$$

$$\tilde{\nu}_{a2}^2 = \frac{1}{8rs}\Big(2s\lambda^2+\lambda^4-2s\lambda^4+2s\mu^2+2\lambda^2\mu^2+\mu^4-2s\mu^4+r^2s((-2+s)\lambda^4+2\mu^2 \\ +(-2+s)\mu^4+2\lambda^2(1+s\mu^2))+2r(\lambda^2-\lambda^4+\mu^2-\mu^4+s^2(\lambda^2-\lambda^4+\mu^2-\mu^4) \\ +s(4+3\lambda^4-4\mu^2+3\mu^4-2\lambda^2(2+\mu^2))\Big)+\Big((-16rs(-2r-\lambda^2+2r\lambda^2-rs\lambda^2 \\ +(-1+2r-rs+2(-1+r)(-1+s)\lambda^2)\mu^2)(-2s-\lambda^2+2s\lambda^2-rs\lambda^2 \\ +(-1+2s-rs+2(-1+r)(-1+s)\lambda^2)\mu^2)+((\lambda^2+\mu^2)^2+2s(\lambda^2-\lambda^4+\mu^2-\mu^4) \\ +r^2s((-2+s)\lambda^4+2\mu^2+(-2+s)\mu^4+2\lambda^2(1+s\mu^2))+2r(\lambda^2-\lambda^4+\mu^2-\mu^4 \\ +s^2(\lambda^2-\lambda^4+\mu^2-\mu^4)+s(4-4\lambda^2+3\lambda^4-2(2+\lambda^2)\mu^2+3\mu^4)))^2))\Big)^{\frac{1}{2}}.$$

We could not simplify these expressions further. However, we investigated the numerical values of the entanglement in the two cases. First we calculated

$$f_{\tilde{\nu}_b^2}(\lambda,\mu) = \sqrt{\text{Min}[\text{Eigenvalues}[i\Omega\tilde{\boldsymbol{\sigma}}_b i\Omega\tilde{\boldsymbol{\sigma}}_b]]},$$

$$f_{\tilde{\nu}_a^2}(\lambda,\mu) = \sqrt{\text{Min}[\text{Eigenvalues}[i\Omega\tilde{\boldsymbol{\sigma}}_a i\Omega\tilde{\boldsymbol{\sigma}}_a]]},$$

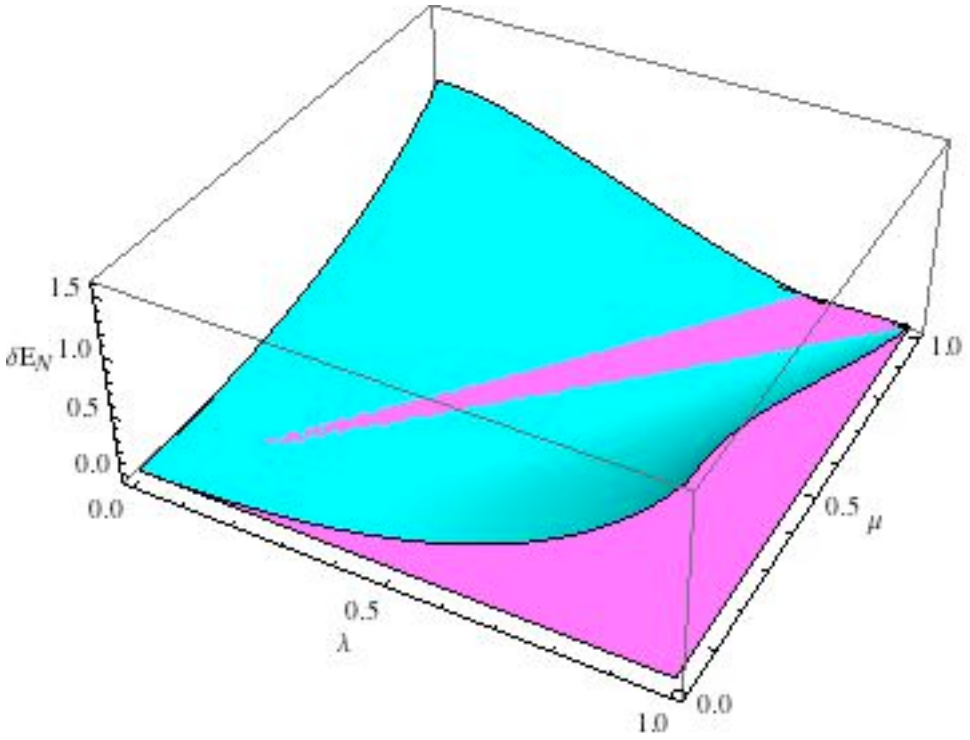


FIGURE 5. The difference in the amount of entanglement between the two cases where we used the values r=3,s=2

then

$$\delta E_{\mathcal{N}}(\lambda,\mu) = -\log_2[f_{\tilde{\nu}_b^2}(\lambda,\mu)] + \log_2[f_{\tilde{\nu}_a^2}(\lambda,\mu)].$$

5.3.3. First approach. The most direct approach is to simply plot the graphs of $\delta E_{\mathcal{N}}$ against λ and μ for different choices of r and s. A typical graph is given in Fig. 5.

The purple plane represents the zero plane. The blue graph is the difference in entanglement between the two cases. The region above the horizontal plane represents the region where $\delta E_{\mathcal{N}} > 0$ and therefore in this region it is better to store squeezing . The region below the purple plane is when $\delta E_{\mathcal{N}} < 0$ meaning that in this region it is better to store entanglement. The trouble with this approach is that one gets a wide variety of graphs and it is difficult to make any general statements.

5.3.4. Second approach. By making suitable approximations we find a simple analytic expression for a region in the λ, μ plane where it is certainly better to entangle after storage. For values of λ, μ outside of this region we cannot say (using this analysis) whether or not it is better to entangle after storage. Let $e_1 e_2$ be the product of two smallest *ordinary* eigenvalues of $\boldsymbol{\sigma}_b$. Then for definitions of X, Y given in Eq. (5.3.12) and Eq. (5.3.11) the inequality in Eq. (5.1.31) for the case $\boldsymbol{\sigma}_b$ becomes an equality (this can be seen by a direct calculation of Eq. (5.3.1)):

$$\tilde{\nu}_b^2 = e_1 e_2(\boldsymbol{\sigma}_b).$$

This means that if we can identify a region for which

$$e_1 e_2(\boldsymbol{\sigma}_a) > e_1 e_2(\boldsymbol{\sigma}_b), \tag{5.3.16}$$

holds then we also know the region $\tilde{\nu}_a^2 > \tilde{\nu}_b^2$ by the following inequality:

$$\tilde{\nu}_a^2 \geq e_1 e_2(\boldsymbol{\sigma}_a) > e_1 e_2(\boldsymbol{\sigma}_b) = \tilde{\nu}_b^2. \tag{5.3.17}$$

Note that for the region where $e_1 e_2(\boldsymbol{\sigma}_a) < e_1 e_2(\boldsymbol{\sigma}_b)$, Eq. (5.3.17) may or may not hold. This region had not been analyzed in this thesis. Below we give a brief summary of our strategy for identifying a region for which Eq. (5.3.16) holds.

- We consider the special case $n = m = 0$.
- We found the symplectic and ordinary eigenvalues of $\boldsymbol{\sigma}_b$ and $\boldsymbol{\sigma}_a$. They correspond to storing squeezing and storing entanglement respectively. In the former case there is decoherence before beamsplitter and in the latter there is decoherence after beamsplitter.
- We did a little algebra to get the expressions for the ordinary eigenvalues of $\boldsymbol{\sigma}_b$ and $\boldsymbol{\sigma}_a$.
- We identified the smallest two ordinary eigenvalues of $\boldsymbol{\sigma}_b$ with the condition $r > s > 1$.

- We showed that for $n = m = 0$ the square of the smallest symplectic eigenvalue of $\boldsymbol{\sigma}_b$ is equal to the product of the two smallest ordinary eigenvalues of $\boldsymbol{\sigma}_b$.
- Identifying the two smallest ordinary eigenvalues of $\boldsymbol{\sigma}_a$ was algebraically tricky. We had to impose another condition $s > 2 - \frac{1}{r}$ to simplify the problem.
- For this special case we looked at the difference between the product of two smallest eigenvalues of $\boldsymbol{\sigma}_a$ and the product of two smallest eigenvalues $\boldsymbol{\sigma}_b$. We found a boundary for the region where storing squeezing is better than storing entanglement.

The ordinary eigenvalues of $\boldsymbol{\sigma}_b$ are

$$\begin{aligned} e_{b_1} &= 1 + \lambda^2\Big(\frac{1}{r} - 1\Big), \\ e_{b_2} &= 1 + \lambda^2(r-1), \\ e_{b_3} &= 1 + \mu^2\Big(\frac{1}{s} - 1\Big), \\ e_{b_4} &= 1 + \mu^2(s-1). \end{aligned}$$

The ordinary eigenvalues of $\boldsymbol{\sigma}_a$ are

$$e_{a_1} = 1 + \frac{1-2r+rs}{4r}(\lambda^2+\mu^2) - \sqrt{\Big(\frac{1-2r+rs}{4r}\Big)^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2}, \tag{5.3.18}$$

$$\begin{aligned} e_{a_2} &= 1 + \frac{1-2r+rs}{4r}(\lambda^2+\mu^2) + \sqrt{\Big(\frac{1-2r+rs}{4r}\Big)^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2}, \\ e_{a_3} &= 1 + \frac{1-2s+rs}{4s}(\lambda^2+\mu^2) - \sqrt{\Big(\frac{1-2s+rs}{4s}\Big)^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{s}\lambda^2\mu^2}, \\ e_{a_4} &= 1 + \frac{1-2s+rs}{4s}(\lambda^2+\mu^2) + \sqrt{\Big(\frac{1-2s+rs}{4s}\Big)^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{s}\lambda^2\mu^2}. \end{aligned} \tag{5.3.19}$$

We impose the following conditions:

$$1) r > s > 1,$$

$$2) s > 2 - \frac{1}{r}. \tag{5.3.20}$$

First observe that Condition 1) implies $e_{b_1} < 1$ and $e_{b_3} < 1$ whereas $e_{b_2} > 1$ and $e_{b_2} > 1$. So we can immediately see that the smallest two eigenvalues of $\boldsymbol{\sigma}_b$ are e_{b_1} and e_{b_3}. After a little algebra the product of two smallest ordinary eigenvalues of $\boldsymbol{\sigma}_b$ can be written as

$$e_{b_1} e_{b_3} = 1 - (1 - \frac{1}{r})\lambda^2 - (1 - \frac{1}{s})\mu^2 + \frac{(r-1)(s-1)}{rs}\lambda^2\mu^2. \tag{5.3.21}$$

It is not as easy to inspect the smallest two ordinary eigenvalues of $\boldsymbol{\sigma}_a$. We use the following method. Observe that all the expressions in Eq. (5.3.19) are of the form:

$$\begin{aligned} e_{a_1} &= k - \sqrt{\Delta k}, \\ e_{a_2} &= k + \sqrt{\Delta k}, \\ e_{a_3} &= p - \sqrt{\Delta p}, \\ e_{a_4} &= p + \sqrt{\Delta p}. \end{aligned}$$

where we define

$$\begin{aligned} k &= 1 + \frac{1 - 2r + rs}{4r}(\lambda^2 + \mu^2), \\ p &= 1 + \frac{1 - 2s + rs}{4s}(\lambda^2 + \mu^2), \\ \Delta k &= \Big(\frac{1 - 2r + rs}{4r}\Big)^2 (\lambda^2 + \mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2, \\ \Delta p &= \Big(\frac{1 - 2s + rs}{4s}\Big)^2 (\lambda^2 + \mu^2)^2 + \frac{(r-1)(s-1)}{s}\lambda^2\mu^2. \end{aligned}$$

We now show that the smallest two eigenvalues are $k - \sqrt{\Delta k}$ and $p - \sqrt{\Delta p}$. We can immediately see that

$$\begin{aligned} k - \sqrt{\Delta k} &< k + \sqrt{\Delta k}, \\ p - \sqrt{\Delta p} &< p + \sqrt{\Delta p}. \end{aligned} \tag{5.3.22}$$

Next we notice that the Condition 1) in Eq. (5.3.20) implies $k < p$ and $\sqrt{\Delta k} < \sqrt{\Delta p}$. To see this we first rewrite k and p as

$$k = 1 + \frac{1}{4}\Big(\frac{1}{r} + s - 2\Big),$$
$$p = 1 + \frac{1}{4}\Big(\frac{1}{s} + r - 2\Big).$$

We only need to compare the terms $\frac{1}{r} + s$ and $\frac{1}{s} + r$ since all other terms are the same.

$$s < r \Rightarrow \frac{1}{r} < \frac{1}{s} \Rightarrow \frac{1}{r} + s < \frac{1}{s} + r.$$

So

$$k < p. \tag{5.3.23}$$

We also notice that Δk is of the form $k^2 + c$ and Δp is $p^2 + c'$. We now know that $k < p$. It is also easily seen that Condition 1 Eq. (5.3.20) implies $c < c'$ so that $k^2 + c < p^2 + c'$. That gives us:

$$\sqrt{\Delta k} < \sqrt{\Delta p}. \tag{5.3.24}$$

The inequalities in (5.3.23) and (5.3.24) together imply:

$$k + \sqrt{\Delta k} < p + \sqrt{\Delta p}.$$

We can now dismiss $p + \sqrt{\Delta p}$ as it is the greatest eigenvalue. Of the remaining 3 we can say that $k - \sqrt{\Delta k}$ is one of the smallest since it is smaller than both $p - \sqrt{\Delta p}$ and $k + \sqrt{\Delta k}$. We need to find out which of the remaining 2 is smaller. We do that by showing $k + \sqrt{\Delta k} > 1$ and $p - \sqrt{\Delta p} < 1$.

$$\begin{aligned}
&\sqrt{\Delta k} > \frac{1 - 2r + rs}{4r} \\
&\Rightarrow k + \sqrt{\Delta k} > k + \frac{1 - 2r + rs}{4r} = 1 + \frac{1 - 2r + rs}{4r} + \frac{1 - 2r + rs}{4r} \\
&= 1 + 2\frac{1 - 2r + rs}{4r}
\end{aligned}$$

$$\Rightarrow k+\sqrt{\Delta k} > 1+2\frac{1-2r+rs}{4r} \tag{5.3.25}$$
$$\Rightarrow k+\sqrt{\Delta k} > 1.$$

Similarly,

$$\sqrt{\Delta p} > \frac{1-2s+rs}{4s}$$
$$\Rightarrow -\sqrt{\Delta p} < -\frac{1-2s+rs}{4s} \Rightarrow p-\sqrt{\Delta p} < p-\frac{1-2s+rs}{4s}$$
$$\Rightarrow p-\sqrt{\Delta p} < 1+\frac{1-2s+rs}{4s}-\frac{1-2s+rs}{4s} = 1 \Rightarrow p-\sqrt{\Delta p} < 1.$$

So $k+\sqrt{\Delta k} > p-\sqrt{\Delta p}$. We conclude that the smallest two eigenvalues of $\boldsymbol{\sigma}_a$ are:

$$e_{a_1} = k-\sqrt{\Delta k},$$
$$e_{a_3} = p-\sqrt{\Delta p}.$$

and so, the product of 2 smallest ordinary eigenvalues of $\boldsymbol{\sigma}_a$:

$$e_{a_1}e_{a_3} = \left(1+\frac{1-2r+rs}{4r}(\lambda^2+\mu^2)-\sqrt{\Big(\frac{1-2r+rs}{4r}\Big)^2(\lambda^2+\mu^2)^2+\frac{(r-1)(s-1)}{r}\lambda^2\mu^2}\right)$$
$$\left(1+\frac{1-2s+rs}{4s}(\lambda^2+\mu^2)-\sqrt{\Big(\frac{1-2s+rs}{4s}\Big)^2(\lambda^2+\mu^2)^2+\frac{(r-1)(s-1)}{s}\lambda^2\mu^2}\right).$$

We now find the region of r and s for which $e_{a_1}e_{a_3} > e_{b_1}e_{b_3}$. We define A, B, C as follows:

$$A = 1-(1-\frac{1}{r})\lambda^2-(1-\frac{1}{s})\mu^2+\frac{(r-1)(s-1)}{rs}\lambda^2\mu^2,$$
$$B = \left(1+\frac{1-2r+rs}{4r}(\lambda^2+\mu^2)-\Big((\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2+\frac{(r-1)(s-1)}{r}\lambda^2\mu^2\Big)^{\frac{1}{2}}\right),$$
$$C = \left(1+\frac{1-2s+rs}{4s}(\lambda^2+\mu^2)-\Big((\frac{1-2s+rs}{4s})^2(\lambda^2+\mu^2)^2+\frac{(r-1)(s-1)}{s}\lambda^2\mu^2\Big)^{\frac{1}{2}}\right).$$

We want to identify the regions where

$$BC-A > 0$$

Note that B and C are of the form

$$\sqrt{a+b} \leq \sqrt{a} + \sqrt{b}.$$

The square roots in $e_{a_1} e_{a_3}$ have the same form as above. So we can say

$$\sqrt{(\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2} \leq \sqrt{(\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2} + \sqrt{\frac{(r-1)(s-1)}{r}\lambda^2\mu^2}$$

$$-\sqrt{\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2} \geq -\sqrt{\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2} + \sqrt{\frac{(r-1)(s-1)}{r}\lambda^2\mu^2}$$

$$\Rightarrow 1 + \frac{1-2r+rs}{4r}(\lambda^2+\mu^2) - \Big(\sqrt{(\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2 + \frac{(r-1)(s-1)}{r}\lambda^2\mu^2}\Big) \geq$$

$$1 + \frac{1-2r+rs}{4r}(\lambda^2+\mu^2) - \Big(\sqrt{(\frac{1-2r+rs}{4r})^2(\lambda^2+\mu^2)^2} + \sqrt{\frac{(r-1)(s-1)}{r}\lambda^2\mu^2}\Big)$$

$$\Rightarrow B \geq 1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{r}}.$$

Similarly,

$$C \geq 1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{s}}.$$

Then,

$$\begin{aligned} BC - A =& \Big(1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{r}}\Big)\Big(1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{s}}\Big) \\ & - \Big(1 - (1-\frac{1}{r})\lambda^2 - (1-\frac{1}{s})\mu^2 + \frac{(r-1)(s-1)}{rs}\lambda^2\mu^2\Big) \\ &= -\lambda\mu\Big(\sqrt{\frac{(r-1)(s-1)}{r}} + \sqrt{\frac{(r-1)(s-1)}{s}}\Big) + \lambda^2\mu^2(r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs}) \\ & + (1-\frac{1}{r})\lambda^2 + (1-\frac{1}{s})\mu^2. \end{aligned}$$

Consider the term with $\lambda^2\mu^2$:

$$\sqrt{rs} < rs \Rightarrow \frac{1}{\sqrt{rs}} > \frac{1}{rs} \Rightarrow \Big(\frac{1}{\sqrt{rs}} - \frac{1}{rs}\Big) > 0.$$

It follows that

$$BC - A > BC - A - \lambda^2\mu^2(r-1)(s-1)\Big(\frac{1}{\sqrt{rs}} - \frac{1}{rs}\Big).$$

which gives the following inequality below.

$$(\frac{r-1}{r})\lambda^2 + (\frac{s-1}{s})\mu^2 - \sqrt{\frac{(r-1)(s-1)}{rs}}(\sqrt{r}+\sqrt{s})\lambda\mu + (r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs})\lambda^2\mu^2 >$$
$$(\frac{r-1}{r})\lambda^2 + (\frac{s-1}{s})\mu^2 - \sqrt{\frac{(r-1)(s-1)}{rs}}(\sqrt{r}+\sqrt{s})\lambda\mu. \tag{5.3.26}$$

This is simpler to handle because RHS is a quadratic in λ and μ. We can now find a bound for λ and μ in terms of r and s. Define $x = \sqrt{\frac{r-1}{r}}\lambda \quad y = \sqrt{\frac{s-1}{s}}\mu$. Then we can write RHS of 5.3.26 as follows:

$$x^2 + y^2 - xy(\sqrt{r}+\sqrt{s}) = y^2(\frac{x^2}{y^2} - \frac{x}{y}(\sqrt{r}+\sqrt{s}) + 1).$$

Let $t = \frac{x}{y}$. Then,

$$t^2 - (\sqrt{r}+\sqrt{s})t + 1 = 0 \Rightarrow t = \frac{(\sqrt{r}+\sqrt{s}) \pm \sqrt{(\sqrt{r}+\sqrt{s})^2 - 4}}{2}.$$

Substituting λ and μ we have,

$$t = \frac{x}{y} = \frac{\sqrt{\frac{r-1}{r}}}{\sqrt{\frac{s-1}{s}}}\frac{\lambda}{\mu}$$
$$\Rightarrow \frac{\sqrt{\frac{r-1}{r}}}{\sqrt{\frac{s-1}{s}}}\frac{\lambda}{\mu} = \frac{(\sqrt{r}+\sqrt{s}) \pm \sqrt{(\sqrt{r}+\sqrt{s})^2 - 4}}{2}$$
$$\Rightarrow \frac{\lambda}{\mu} = \frac{\sqrt{\frac{s-1}{s}}}{\sqrt{\frac{r-1}{r}}}\frac{(\sqrt{r}+\sqrt{s}) \pm \sqrt{(\sqrt{r}+\sqrt{s})^2 - 4}}{2}.$$

This means that,

$$\frac{\lambda}{\mu} > \frac{\sqrt{\frac{s-1}{s}}}{\sqrt{\frac{r-1}{r}}}\frac{(\sqrt{r}+\sqrt{s}) + \sqrt{(\sqrt{r}+\sqrt{s})^2 - 4}}{2} \Rightarrow BC - A > 0,$$

$$\frac{\lambda}{\mu} < \frac{\sqrt{\frac{s-1}{s}}}{\sqrt{\frac{r-1}{r}}} \frac{(\sqrt{r}+\sqrt{s}) - \sqrt{(\sqrt{r}+\sqrt{s})^2 - 4}}{2} \Rightarrow BC - A > 0. \tag{5.3.27}$$

We conclude that given the Conditions 1) and 2) we have

$$e_{a_1} e_{a_3} > e_{b_1} e_{b_3} \Rightarrow \tilde{\nu}_a^2 > \tilde{\nu}_b^2.$$

for the regions of λ and μ given in (5.3.27). If λ and μ satisfy the Eq. (5.3.27) then storing squeezing is better than storing entanglement. In the next section we will derive an improved treatment which makes fewer approximations.

5.3.5. Improved second approach. If we let $r = s$ then Eq. (5.3.27) becomes,

$$\begin{aligned} &\frac{\lambda}{\mu} > \sqrt{r} + \sqrt{r-1} \Rightarrow BC - A > 0 \quad , \\ &\frac{\lambda}{\mu} < \sqrt{r} - \sqrt{r-1} \Rightarrow BC - A > 0. \end{aligned}$$

As r goes to infinity the first one of above equations will get bigger and bigger the second one will get nearer and nearer to zero. This suggests that our bound is not very good. We will try to improve it by not making some of the approximation we made previously. We had

$$\begin{aligned} BC - A =& \Big(1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{r}}\Big)\Big(1 - \lambda\mu\sqrt{\frac{(r-1)(s-1)}{s}}\Big) \\ &- \Big(1 - (1-\frac{1}{r})\lambda^2 - (1-\frac{1}{s})\mu^2 + \frac{(r-1)(s-1)}{rs}\lambda^2\mu^2\Big) \\ &= -\lambda\mu\Big(\sqrt{\frac{(r-1)(s-1)}{r}} + \sqrt{\frac{(r-1)(s-1)}{s}}\Big) + \lambda^2\mu^2(r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs}) \\ &+ (1-\frac{1}{r})\lambda^2 + (1-\frac{1}{s})\mu^2. \end{aligned} \tag{5.3.28}$$

where we dropped the $\lambda^2\mu^2$ term altogether because this term is always greater than zero. We have

$$BC - A > BC - A - \lambda^2\mu^2(r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs}). \tag{5.3.29}$$

We showed that

$$BC - A - \lambda^2\mu^2(r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs}) > 0. \tag{5.3.30}$$

We now want to include λ^2 and μ^2 term to identify the region for which the inequality $BC - A > 0$ holds. We can write 5.3.30 as follows:

$$\kappa(\lambda,\mu) = a^2\lambda^2 + b^2\mu^2 - 2c\lambda\mu + d^2\lambda^2\mu^2 > 0. \tag{5.3.31}$$

where

$$\begin{aligned}
a &= \sqrt{1 - \frac{1}{r}},\\
b &= \sqrt{1 - \frac{1}{s}},\\
c &= \frac{1}{2}\Big(\sqrt{\frac{(r-1)(s-1)}{r}} + \sqrt{\frac{(r-1)(s-1)}{s}}\Big),\\
d &= \sqrt{(r-1)(s-1)(\frac{1}{\sqrt{rs}} - \frac{1}{rs})}.
\end{aligned}$$

Eq. (5.3.31) is the difference between the product of two smallest eigenvalues the covariance matrices corresponding to the two cases; storage after entanglement and storage before entanglement. Completing the squares, this can be written as

$$\kappa(\lambda,\mu) = (a\lambda + b\mu)^2 + \Big(d\lambda\mu - \frac{c+ab}{d}\Big)^2 - \frac{(c+ab)^2}{d^2}. \tag{5.3.32}$$

Note that $\kappa(\lambda,\mu)$ has the form

$$x^2 + y^2 = z^2.$$

We display this information graphically in Fig. 6 and Fig. 7. Fig. 6 is a $3-D$ graph of $\kappa(\lambda,\mu)$ and Fig. 7 is a contour graph. The yellow region in Fig. 7 is the region

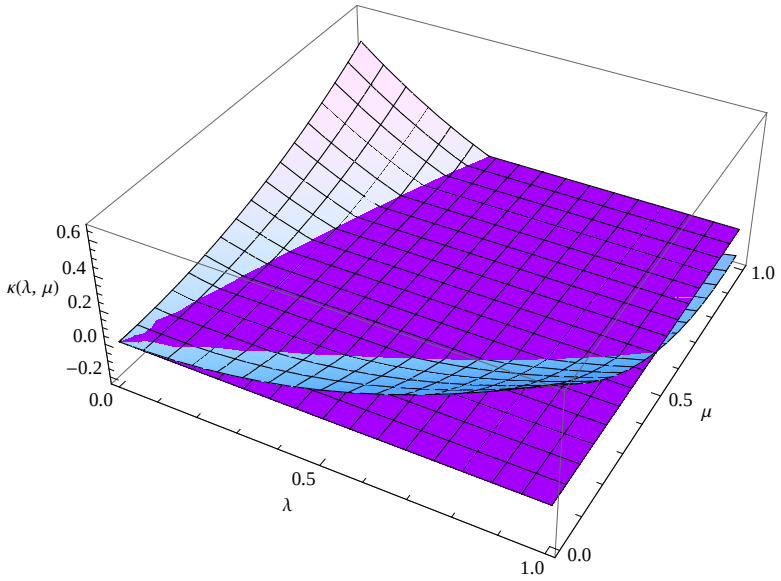


FIGURE 6. The blue graph is the graph of $\kappa(\lambda, \mu)$ with $r = 3, s = 2$ and $\lambda, \mu : 0 \to 1$. The purple plane is the zero plane and it is there so that we can see the regions of blue graph for which $\kappa(\lambda, \mu) \geq 0$ clearly.

where $\kappa(\lambda, \mu)$ is greater than zero and where we can consequently say for sure that it is better to store squeezing. In the purple region in Fig. 7 the approximations we made in deriving our inequality in Eq. (5.3.31) mean that we are unable to say for sure which is better: to store squeezing or entanglement. Of course we know from our first approach that there is a subset of purple region where it is better to store entanglement but approximations in this approach mean that we cannot give its boundary using this approach.

We conclude this section by deriving analytic parametric equations for the boundary curve dividing the purple and yellow regions in Fig. 7. Define

$$a\lambda + b\mu = R\cos\theta, \tag{5.3.33}$$

$$d\lambda\mu - \frac{c + ab}{d} = R\sin\theta, \tag{5.3.34}$$

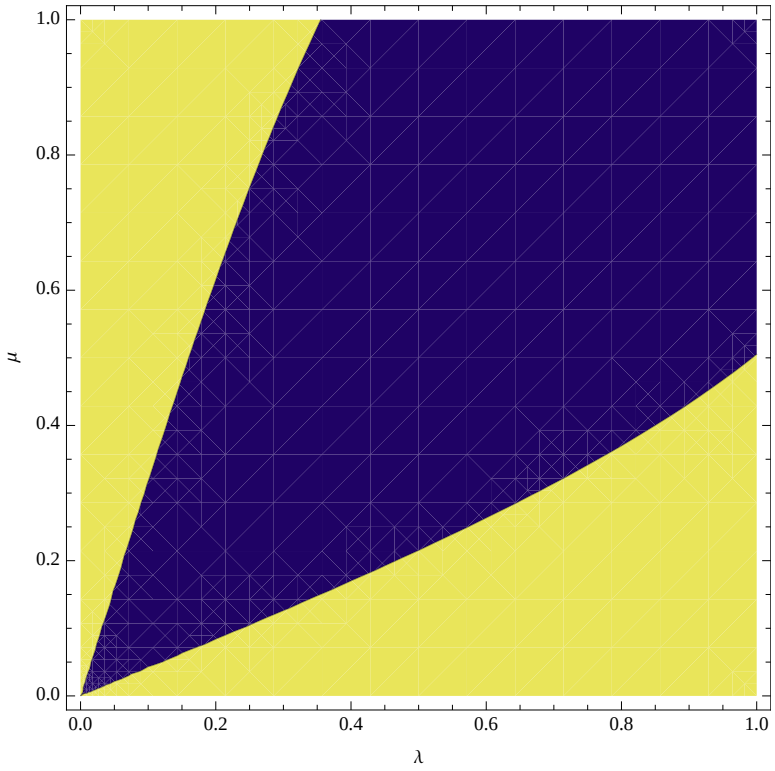


FIGURE 7. Contour graph of $\kappa(\lambda, \mu)$ with $r = 3, s = 2$ and $\lambda, \mu : 0 \to 1$. The yellow region is where $\kappa(\lambda, \mu) \geq 0$ and therefore it is the region for which storing squeezing yields more entanglement. The purple region is where $\kappa(\lambda, \mu) \leq 0$ which, due to our approximations we made in deriving $\kappa(\lambda, \mu) \geq 0$, does not necessarily imply that storing entanglement is better in this region.

with $0 \leq \theta \leq 2\pi$. Then we can write Eq. (5.3.31) as

$$\begin{aligned} & R^2 \cos^2\theta + R^2 \sin^2\theta \geq \frac{(c+ab)^2}{d^2} \\ & \Rightarrow R^2 \geq \frac{(c+ab)^2}{d^2} \\ & \Rightarrow R \geq \frac{c+ab}{d}. \end{aligned} \tag{5.3.35}$$

From Eq. (5.3.33) we have

$$\mu = \frac{R\cos\theta - a\lambda}{b}. \tag{5.3.36}$$

Substituting this into Eq. (5.3.34) we get

$$\lambda^2 - \frac{R\cos\theta}{a}\lambda + \frac{b}{ad}\Big(\frac{c+ab}{d} + R\sin\theta\Big) = 0.$$

Solving this for λ we get

$$\lambda = \frac{1}{2a}\Big(R\cos\theta \pm \sqrt{R^2\cos^2\theta - \frac{4ab}{d}\Big(\frac{c+ab}{d} + R\sin\theta\Big)}\Big).$$

Then substituting this into Eq. (5.3.36) we obtain the following expression for μ:

$$\mu = \frac{1}{2b}\Big(R\cos\theta \pm \sqrt{R^2\cos^2\theta - \frac{4ab}{d}\Big(\frac{c+ab}{d} + R\sin\theta\Big)}\Big).$$

We are particularly interested in the line for which

$$R = \frac{c+ab}{d}, \tag{5.3.37}$$

as this gives the boundary of the region in which (5.3.31) holds. We call this value R_0. Substituting this into equations for λ and μ we get

$$\begin{aligned}\lambda &= \frac{1}{2a}\Big(R_0\cos\theta \pm \sqrt{R_0^2\cos^2\theta - \frac{4ab}{d}R_0(1+\sin\theta)}\Big),\\ \mu &= \frac{1}{2b}\Big(R_0\cos\theta \mp \sqrt{R_0^2\cos^2\theta - \frac{4ab}{d}R_0(1+\sin\theta)}\Big).\end{aligned} \tag{5.3.38}$$

These two parametric equations giving λ and μ in terms of the parameter θ specify the boundary curve between the purple and yellow regions in Fig. 7. In Fig. 8 we plot the boundary curve. For one choice of the sign we get the equation for the lower boundary curve; with the other choice of the sign we get the upper boundary curve.

5.4. Summary

We have considered continuous variable quantum memories operated in spin clouds by QND feedback. We have shown that given that we impose the conditions

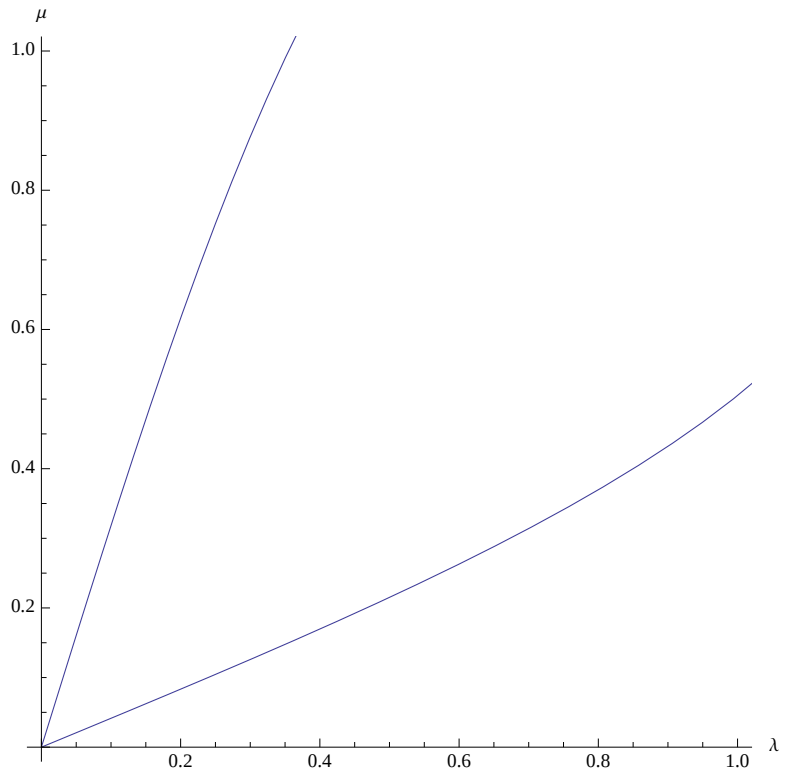


FIGURE 8. The boundary curve between yellow and purple region in Fig. 7 with $r = 3, s = 2$, $\lambda, \mu : 0 \to 1$ and $\theta : -\frac{\pi}{2} \to 0$. The lower boundary curve is obtained when we choose the first pair of signs ($+$ for λ and $-$ for μ) in Eq. (5.3.38) and the upper curve boundary is obtained when we choose the other pair ($-$ for λ and $+$ for μ) of signs.

in Eq. (5.3.20) on the squeezing parameters, in the presence of noise we can identify a region of the parameters, r, s, λ, μ where storing squeezing first yields more entanglement in the resulting state.

Our result could have significant impact as operational guidelines for the storage and retrieval of continuous variable entanglement, which will be an ubiquitous prerequisite in the areas of quantum communication and information processing alike.

Part 3

Application of Galois Theory to SIC-POVMs

CHAPTER 6

Galois theory and SIC-POVMs

6.1. SIC existence problem

In Chapter 4 we argued that a SIC-POVM can be regarded as a discrete analogue of a coherent state POVM and that a SIC fiducial vector can be regarded as a discrete analogue of a coherent state.

SIC-POVMs are interesting for many other reasons. In particular, they have applications to quantum tomography [**60**,**119**–**121**], quantum cryptography [**59**,**122**–**125**], quantum communication [**126**–**130**] and Kochen-Specker arguments [**131**]. They also have applications classically to high precision radar [**129**, **132**, **133**] and speech recognition [**134**]. They have been realized experimentally [**123**, **135**] and further experiments have been proposed [**136**, **137**]. They also play an important role in the "Qbist" approach to the interpretation of quantum mechanics [**15**, **16**, **138**–**140**]. Unfortunately, in spite of much effort, it is still not proven that they exist in every dimension. SICs have been constructed numerically in every dimension less than or equal to 67 and many dimensions greater than the 67 (this is still work in progress [**141**]). Exact expressions have been found in 2-15,19,24,35,48 (see [**142**] and references cited therein), dimension 16 [**143**] and dimension 28 [**144**]. This encourages the conjecture that SICs actually exist in every finite dimension. However, that is only a conjecture.

In this chapter we describe some work we did on the Galois symmetries of SIC-POVMs. We will give a review of Galois theory in Section 6.2. However, before going into details, we will explain in general terms, why Galois theory might be expected to be relevant to this problem.

A SIC fiducial vector is a solution to a set of equations

$$|\langle\psi|D_{\mathbf{p}}|\psi\rangle|^2 = \begin{cases} 1 & \text{if } \mathbf{p} = 0 \\ \frac{1}{d+1} & \text{if } \mathbf{p} \neq 0. \end{cases} \tag{6.1.1}$$

as we saw in Eq. (4.2.5). It can be seen that these are degree 4 polynomial equations in the real and imaginary parts of the components of $|\psi\rangle$. One can see at once that the system is greatly overdetermined for $d > 2$ since one has d^2 equations for only $2d$ real variables. It is therefore surprising that we are able to find solutions at all. The fact that we are, for at least $d \leq 67$, suggests there is some special feature of the equations that is responsible for a solution. Finding that special feature may be the key to proving existence.

The motivation for our work here is the striking fact [**142**–**144**] that all known exact fiducials are expressible in radicals. This tells us that the corresponding Galois group is of a very special kind, namely a solvable group. This suggested to us that we might find the special feature responsible for SICs existing in spite of the over-determination of the equations by studying the Galois group.

When we embarked on this work, we hoped that it might lead to a solution to the existence problem. This did not happen. However, we did find a lot of interesting mathematical structure which we hope will be found useful in future work on this problem.

We now give a brief introduction to Galois theory, stating the basic facts that we relied on in this problem.

6.2. Galois theory

Galois Theory is about polynomials and their solutions. The ancient Greeks originally assumed that every number can be written as a fraction (or rational number). But then they found that $\sqrt{2}$ (the solution to the polynomial $x^2 - 2$) cannot be written as a fraction. Subsequently it was found that the same is true of $\sqrt{n}$, for every integer n which is not a perfect square. Numbers like $\sqrt{2}$ or

$\sqrt[3]{2}$ or $\sqrt[5]{\sqrt{3}+\sqrt[3]{2+\sqrt[7]{11}}}$ which we build up by taking roots are called radicals. The question was: can the solution to every polynomial equation be written in radicals? It was found that polynomials up to degree 4 have solutions expressible in radicals [**145**].

Lagrange thought that it was possible to derive a general formula for degree 5 (and greater than 5) polynomials. However he could not find such a formula. Subsequently Galois showed that it was impossible to find a general formula for quintics because not all quintics had solutions in radicals. He did this by defining what is now called the Galois group of the polynomial. He then showed that the polynomial is solvable in radicals if and only if the Galois group is a solvable group (we define the term "solvable group" below). Then he showed that there are quintics such that their Galois group is not a solvable group.

Note that here the word "solvable" does not indicate the group itself is solvable in some special sense but only indicates that the polynomial corresponding to the group is solvable in radicals.

Let us now give the precise definition of a solvable group. The simplest example of a solvable group is an Abelian group—i.e. a group in which the multiplication is commutative so that for any two elements g_1, g_2 of the group $\mathcal{G}$ we have $g_1 g_2 = g_2 g_1$. To give a general definition of a solvable group we first need to introduce the concept of a *normal subgroup* and a *quotient group* [**146**].

Let $\mathcal{G}$ be any group and $\mathcal{H}$ subgroup. $\mathcal{H}$ is said to be a normal subgroup of $\mathcal{G}$ if, given any $h \in \mathcal{H}$ and $g \in \mathcal{G}$, $ghg^{-1} \in \mathcal{H}$.

If $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$ then we can define the quotient group $\mathcal{G}/\mathcal{H}$. We do this as follows. For each $g \in \mathcal{G}$ we define

$$g\mathcal{H} = \{gh : h \in \mathcal{H}\}. \tag{6.2.1}$$

The set $g\mathcal{H}$ is said to be a coset. The fact that $\mathcal{H}$ is a normal subgroup of $\mathcal{G}$ means that if $x_1 \in g_1\mathcal{H}$ and $x_2 \in g_2\mathcal{H}$ then $x_1 x_2 \in g_1 g_2 \mathcal{H}$. Consequently, we can define a

group multiplication law on the cosets:

$$g_1\mathcal{H}g_2\mathcal{H} = g_1g_2\mathcal{H}. \tag{6.2.2}$$

With this multiplication rule the set of all cosets, denoted $\mathcal{G}/\mathcal{H}$, becomes a group with identity $e\mathcal{H}$ (where e is the identity of $\mathcal{G}$) and where the inverse of $g\mathcal{H}$ is $g^{-1}\mathcal{H}$. $\mathcal{G}/\mathcal{H}$ is called quotient group of $\mathcal{G}$ with respect to $\mathcal{H}$.

We now return to the task of explaining what a solvable group is. After an Abelian group the next simplest example of a solvable group is a group $\mathcal{G}$ which has a normal subgroup $\mathcal{H}$ such that $\mathcal{H}$ and $\mathcal{G}/\mathcal{H}$ are both Abelian. More generally still, a group $\mathcal{G}$ is solvable if it has a chain of subgroups $\mathcal{H}_1, \mathcal{H}_2, \ldots \mathcal{H}_i$ such that

$$\mathcal{H}_1 \subseteq \mathcal{H}_2 \subseteq \cdots \subseteq \mathcal{H}_i \subseteq \mathcal{G}, \tag{6.2.3}$$

where each subgroup is a normal subgroup of the one immediately to the right, and if $\mathcal{H}_1$ together with the quotient groups,

$$\mathcal{G}/\mathcal{H}_i, \mathcal{H}_i/\mathcal{H}_{i-1} \ldots, \mathcal{H}_2/\mathcal{H}_1, \tag{6.2.4}$$

is Abelian. If there is no chain as in Eq. (6.2.3) then the group $\mathcal{G}$ is said to be not solvable.

After Galois there were many developments. Kronecker showed that an extension field has an Abelian group if and only if it is either a cyclotomic field or a subfield of a cyclotomic field (where by a cyclotomic field we mean a field generated by a number of the form $e^{i2n\pi}$, i.e. by a root of unity). He then wanted to have a similar characterization for the quadratic fields (which are the fields generated by numbers of the form $\sqrt{n}$ where n is an integer), however he could not manage it. He called this his "youthful dream". It was also discovered that numbers like e and π are not solutions to any polynomial equation. Such numbers are called transcendental.

However, the detailed analysis of these ideas is out of the scope of this thesis. Our interest in Galois Theory arises from the fact that the components of all known

fiducial vectors are expressible in terms of radicals. This suggests that the fields generated by these radicals have corresponding Galois groups that are solvable. Using this idea we have discovered some interesting features of the structure of SIC-POVMs in the discrete case.

In the next section we give some relevant definitions and explain with simple examples, how Galois Theory works in principle. After that we apply these ideas to the SIC problem.

6.2.1. Number fields and their extensions. The most familiar examples of number fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. However, these are not the only examples. Let us begin by giving a formal definition of a number field (or simply field as we shall call it from now on). A field $\mathbb{F}$ is a set of objects that satisfies the following axioms under the two binary operations, addition and multiplication.

(1) Multiplication is distributive over addition: $x(y+z) = xy + xz$
(2) Addition and multiplication are commutative: if $x, y \in \mathbb{F}$ then $x+y = y+x$ and $x \times y = y \times x$.
(3) Addition and multiplication are associative: if $x, y, z \in \mathbb{F}$ then $(x+y)+z = x + (y+z)$ and $(x \times y) \times z = x \times (y \times z)$.
(4) An additive identity $0 \in \mathbb{F}$ exists such that $x+0 = 0+x = x$ for all $x \in \mathbb{F}$. A multiplicative identity $1 \in \mathbb{F}$ exists such that $1 \times x = x \times 1 = x$ for all $x \in \mathbb{F}$.
(5) An additive and a multiplicative inverse $x^{-1} \in \mathbb{F}$ exists such that $x+x^{-1} = 0$ and $x \times x^{-1} = 1$ for all $x \in \mathbb{F}$.

If a field $\mathbb{F}$ is contained in a field $\mathbb{E}$ we say that $\mathbb{E}$ is an extension field of $\mathbb{F}$ and $\mathbb{F}$ is a subfield of $\mathbb{E}$. In this thesis we are concerned with extension fields $\mathbb{E}$ such that $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{C}$. There are other examples of fields, for instance, $\mathbb{Z}_p$ where p is a prime number. Galois theory also applies to them but we are not concerned with them in this thesis. We now list the kinds of complex numbers included in $\mathbb{C}$.

(1) The set of all rational numbers and the numbers of the form $a + bi$ where $a, b \in \mathbb{Q}$ included in the $\mathbb{C}$.
(2) Radicals, that is the numbers obtained from rational numbers by use of arithmetic operations: addition, subtraction, multiplication, division and taking by arbitrary roots (square roots, cube roots, etc.). For example: $\sqrt{\frac{\sqrt{2}+\sqrt{5}}{3+(2+3i)^{\frac{1}{3}}}}$.
(3) Algebraic numbers which are the roots of a polynomial. Not all algebraic numbers can be written in terms of radicals. For instance there are quintic polynomials whose roots are not expressible in radicals.
(4) Transcendental numbers are the numbers that are not algebraic, in other words, they are not the roots of any polynomial. For example: e or π.

If an extension of the rationals consists entirely of radicals then we say that it is a *radical extension*. If it consists entirely of algebraic numbers then we say that it is an *algebraic extension*. If it is not algebraic (meaning that some of its elements are transcendental) then we say that it is a *transcendental extension*.

6.2.1.1. *Field extensions.* The basic idea for constructing field extensions is present in the way we obtain complex numbers from the real numbers. The set of real numbers $\mathbb{R}$ does not contain the roots of $x^2 + 1$, so we define a number i. We then define the field of complex numbers to be $\mathbb{C} = \mathbb{R}(i)$ which contains the combination of all numbers of the form $a + bi$ where $a, b \in \mathbb{R}$. $\mathbb{R}(i)$ is closed under addition, subtraction, multiplication and division and therefore it is a field. This is easy to see by straightforward arithmetic. Suppose we multiply two arbitrary numbers in $\mathbb{R}(i)$: $(a + bi)(c + di) = ac + (bc + ad)i + bdi^2 = (ac - bd) + (bc + ad)i$ which is of the form $a' + b'i$. Similarly, it can be shown that addition, subtraction and division will produce numbers of the same form. Consider another polynomial for an example: $x^2 + x + 1$. The roots of this polynomial are $e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$ and are not in $\mathbb{Q}$. So we extend $\mathbb{Q}$ to include $\omega = e^{\frac{2\pi i}{3}}$. Define $\mathbb{E} = \mathbb{Q}(\omega)$ to consist of all combinations of the form $a + b\omega$ with $a, b \in \mathbb{Q}$. It can, again by simple arithmetic, be shown that $\mathbb{Q}(\omega)$ is closed under all four operations and therefore it is a field.

For instance multiplying two arbitrary elements in this field we have

$$\begin{aligned}(a+b\omega)(c+d\omega) &= ac+(bc+ad)\omega+bd\omega^2 \\ &= ac+(bc+ad)\omega+bd(-1-\omega) \\ &= (ac-bd)+(bc+ad-bd)\omega \end{aligned} \tag{6.2.5}$$

which is of the form $a'+b'\omega$.

This idea generalizes. Let $\mathbb{F}$ be an extension of the rationals and a be an algebraic number that is not in $\mathbb{F}$. We define the minimal polynomial of a over $\mathbb{F}$ which is the lowest degree polynomial with all its coefficients in $\mathbb{F}$ and a as one of its roots and for which the leading coefficient is equal to 1. The minimal polynomial is unique. This is easy to see. Suppose there were two such polynomials

$$x^n+c_1x^{n-1}+\cdots+c_{n-1}x+c_n \tag{6.2.6}$$

$$x^n+c'_1x^{n-1}+\cdots+c'_{n-1}x+c'_n \tag{6.2.7}$$

with $c_1,\ldots,c_n\in\mathbb{F}$. Then a would also be a root of the difference of these polynomials

$$(c_1-c'_1)x^{n-1}+\cdots+(c_{n-1}-c'_{n-1})x \tag{6.2.8}$$

implying that a is a root of a non-zero polynomial of degree less than n, contrary to assumption. We define $\mathbb{F}(a)$ to consist of all combinations of the form

$$r_0+r_1a+\cdots+r_{n-1}a^{n-1} \tag{6.2.9}$$

where $r_0,\ldots,r_{n-1}\in\mathbb{F}$. If we multiply two such expressions we get an expression involving powers of a up to a^{2n-2} but using the fact that $a^n=-c_1a^{n-1}-\cdots-c_{n-1}a-c_n$. We can rewrite it in terms of powers up to a^{n-1}. So $\mathbb{F}(a)$ is closed under multiplication. It can also be shown [**147**] that $\mathbb{F}(a)$ is closed under division. It is obviously closed under addition and subtraction. It is therefore a field generated

by a. We can repeat this construction to build a tower of the fields:

$$\begin{aligned}
&\mathbb{E}_1 = \mathbb{F}(a_1) \\
&\mathbb{E}_2 = \mathbb{E}_1(a_2) = \mathbb{F}(a_1, a_2) \\
&\dots \\
&\mathbb{E}_n = \mathbb{E}_{n-1}(a_n) = \mathbb{F}(a_1, a_2, \dots, a_n)
\end{aligned} \tag{6.2.10}$$

If we add the generators a_i in different order the resulting field will not be affected.

One important field property is the *degree* of a field. The degree of a field is determined by the minimal polynomial of its generators. For instance, consider a single generator a, generating the field $\mathbb{F}(a)$. Then the degree of this field is the same as the degree of the minimal polynomial of a. For a field $\mathbb{E}_n(a_1, \dots, a_n)$ with n generators let $d_1, \dots, d_n$ be the degrees of the field extensions. Then the degree d of the field $\mathbb{E}_n$ is given by $d = d_1 \times d_2 \times \cdots \times d_n$.

6.2.1.2. *Galois extensions.* We are particularly interested in extension fields with some special properties. Let $\mathbb{E}$ be an extension field of the base field $\mathbb{F}$.

$\mathbb{E}$ is said to be *separable* if the minimal polynomial of each element of $\mathbb{E}$ over $\mathbb{F}$ has no repeated roots.

REMARK 3. *It can be shown that all extensions of* $\mathbb{Q}$ *are automatically separable. [**145, 147**]*

An extension is said to be *normal* if every polynomial with coefficients in $\mathbb{F}$ which has one root in $\mathbb{E}$ has all its roots in $\mathbb{E}$.

A Galois extension is an extension which is both normal and separable.

Example. Consider the extension $\mathbb{Q}(2^{\frac{1}{4}})$. The minimal polynomial of $2^{\frac{1}{4}}$ over $\mathbb{Q}$ is $f(x) = x^4 - 2$. So $\mathbb{Q}(2^{\frac{1}{4}})$ consists of all combinations of the form $r_0 + r_1 2^{\frac{1}{4}} + r_2 2^{\frac{2}{4}} + r_3 2^{\frac{3}{4}}$ with $r_0, r_1, r_2, r_3 \in \mathbb{Q}$. The degree of the extension field is 4. Now $f(x)$ factors completely in $\mathbb{C}$. Consider its factors: $f(x) = (x + 2^{\frac{1}{4}})(x - 2^{\frac{1}{4}})(x + i2^{\frac{1}{4}})(x - i2^{\frac{1}{4}})$. However, $i \notin \mathbb{Q}(2^{\frac{1}{4}})$. The factorization of $f(x)$ over $\mathbb{Q}(2^{\frac{1}{4}})$ is

$f(x) = (x+2^{\frac{1}{4}})(x-2^{\frac{1}{4}})(x^2+2^{\frac{1}{4}})$. It follows that $\mathbb{Q}(2^{\frac{1}{4}})$ is not a normal extension of $\mathbb{Q}$. To construct a normal extension of $\mathbb{Q}$ containing i we use the following theorem.

THEOREM 6. *The field $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_n)$ is a normal extension if and only if the minimal polynomials of $a_1, \ldots, a_n$ over $\mathbb{F}$ factor completely in $\mathbb{E}$.*

In our example, $\mathbb{Q}(2^{\frac{1}{4}})$, suppose we add another generator, i, to get $\mathbb{E} = \mathbb{Q}(2^{\frac{1}{4}}, i)$. The minimal polynomial $g(x)$ of i over $\mathbb{Q}$ is $g(x) = x^2 + 1$. Now, both polynomials factor completely in $\mathbb{E}$: $f(x) = (x+2^{\frac{1}{4}})(x-2^{\frac{1}{4}})(x+i2^{\frac{1}{4}})(x-i2^{\frac{1}{4}})$ and $g(x) = (x+i)(x-i)$. So $\mathbb{E}$ is a normal extension of $\mathbb{Q}$. The degree of $\mathbb{E}$ is $4 \times 2 = 8$.

6.2.2. Galois group. In order to define the Galois group we need to introduce the idea of a *field automorphism*. The most familiar example of a field automorphism is complex conjugation. This is a map from $\mathbb{C}$ to $\mathbb{C}$ with the following properties. In the first place it is one-to-one (meaning that distinct elements are mapped to distinct elements) and onto (meaning that every element is the image of some element under the map). This is expressed by saying that the map is *bijective*. In the second place the map leaves the reals unchanged. In the third place, it preserves multiplication and addition (i.e. $(z_1 z_2)^* = z_1^* z_2^*$, $(z_1 + z_2)^* = z_1^* + z_2^*$). The only other automorphism of $\mathbb{C}$ which leaves $\mathbb{R}$ unchanged is the identity map. Complex conjugation and the identity form a group called the Galois group of $\mathbb{C}$ as an extension of $\mathbb{R}$. This generalizes to the case of an arbitrary field extension, the only difference being that in the general case the Galois group is usually more complicated.

Let $\mathbb{E}$ be an extension field of the base field $\mathbb{F}$. A Galois automorphism of $\mathbb{E}$ over $\mathbb{F}$ is a function g such that $g : \mathbb{E} \to \mathbb{E}$ with the following properties:

(1) It is bijective.
(2) It leaves the elements of $\mathbb{F}$ unchanged: $g(z) = z$, $\forall\ z \in \mathbb{F}$.
(3) It preserves the field operations: $g(z\omega) = g(z)g(\omega)$ and $g(z+\omega) = g(z) + g(\omega)$, $\forall\ z, \omega \in \mathbb{E}$.

Note that property 3 implies that

$$\begin{aligned} g(0) &= 0, \\ g(1) &= 1, \\ g\Big(\frac{1}{z}\Big) &= \frac{1}{g(z)} \\ g(-z) &= -g(z). \end{aligned} \tag{6.2.11}$$

The Galois group $\mathcal{G}$ of $\mathbb{E}$ over $\mathbb{F}$, denoted $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$, is the set of all Galois automorphisms that map $\mathbb{E}$ onto itself leaving the base field fixed.

The above definition of Galois group applies to all extensions. If, however, the extension $\mathbb{E}$ is a Galois extension of $\mathbb{F}$ then the degree of $\mathbb{E}$ is the same as the order of the Galois group $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$ (where by the order of group we mean the number of elements it contains).

Also, if $\mathbb{E}$ is a Galois extension of $\mathbb{F}$ then the subgroups of $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$ are in bijective correspondence with fields $\mathbb{K}$ such that $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$ (i.e. to each subgroup there corresponds exactly one $\mathbb{K}$ and vice versa). The correspondence is defined as follows. Let $\mathcal{H}$ be a subgroup of $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$. We associate to $\mathcal{H}$ the field

$$\mathbb{K}_{\mathcal{H}} = \{z \in \mathbb{E} : h(z) = z, \forall h \in \mathcal{H}\}. \tag{6.2.12}$$

where $\mathbb{K}_{\mathcal{H}}$ is the fixed field of $\mathcal{H}$. On the other hand let $\mathbb{K}$ be any field such that $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$. Then we associate to $\mathbb{K}$ the subgroup

$$\mathcal{H}_{\mathbb{K}} = \{h \in \mathcal{G}_{\mathbb{F}}(\mathbb{E}) : h(z) = z, \forall z \in \mathbb{K}\}. \tag{6.2.13}$$

The maps $\mathbb{K} \to \mathcal{H}_{\mathbb{K}}$ and $\mathcal{H} \to \mathbb{K}_{\mathcal{H}}$ are mutually inverse. The map is order reversing: $\mathcal{H}_1 \subseteq \mathcal{H}_2 \iff \mathbb{K}_{\mathcal{H}_1} \supseteq \mathbb{K}_{\mathcal{H}_2}$. In other words the bigger the field is the smaller the group gets. Also $\mathcal{H}$ is a *normal* subgroup of $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$ if and only if $\mathbb{K}_{\mathcal{H}}$ is a normal extension of $\mathbb{F}$.

6.2.3. Constructing the Galois group. Suppose we want to calculate the Galois group $\mathcal{G}_{\mathbb{F}}(\mathbb{E})$ of the Galois extension $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_n)$. Firstly, observe that each element in $\mathbb{E}$ can be written as a linear combination of the terms of the form $a_1^{m_1} \times \cdots \times a_n^{m_n}$ with coefficients in $\mathbb{F}$. So if we know the numbers $g(a_1), \ldots, g(a_n)$, where g is a Galois automorphism, we know $g(z)$ for every $z \in \mathbb{E}$.

Fact 1. A Galois automorphism is completely specified by its action on the field generatos. Secondly, let $f_j(x)$ be the minimal polynomial of a_j over $\mathbb{Q}$. Since the extension is Galois, $f_j(x)$ factors completely over $\mathbb{E}$ with no repeated roots:

$$f_j(x) = (x - a_j^{(1)})(x - a_j^{(2)}) \ldots (x - a_j^{(m)}), \tag{6.2.14}$$

where $a_j^{(1)} = a_j$. The numbers $a_j^{(1)}, \ldots, a_j^{(m)}$ are called *Galois conjugates* of a_j.

Fact 2. For each Galois conjugate $a_j^{(t)}$ there is a Galois automorphism g such that $g(a_j) = a_j^{(t)}$.

REMARK 4. *Another way of looking at the action of g on a_j is that each g permutes the roots of the polynomials $f_j(x)$. This gives us a useful check on our working.*

Using the facts 1 and 2 we can construct the Galois group. Note also that the number of automorphisms are the same as the degree of the extension field which gives us a useful check for our working. Constructing the Galois group is quite easy in principle but can be extremely tedious in practice. Galois himself commented on this as follows [**145**]

> If you now give me an equation that you have chosen at your pleasure, and if you want to know if it is or is not solvable by radicals, I need to do nothing more than to indicate to you the means of answering your question, without wanting to give myself or anyone else the task of doing it. In a word, the calculations are impractical.

This was also expressed by D.M. Appleby in a private conversation as follows

> In the 19th century no one in their right mind attempted to calculate a Galois group in any but the simplest cases. Kronecker (one of the major contributors to this subject) talked about calculations which could be done "theoretically", meaning that he himself had not attempted to do them.

However, now we have computers (classical) and for this thesis we used the computer program Magma. To illustrate these ideas we conclude this section with two simple examples where the calculations can be done on a paper.

Example 1. $\mathbb{E} = \mathbb{Q}(2^{\frac{1}{4}}, i)$. The minimal polynomial of $2^{\frac{1}{4}}$:

$$f_1(x) = x^4 - 2 = (x - 2^{\frac{1}{4}})(x + 2^{\frac{1}{4}})(x - i2^{\frac{1}{4}})(x + i2^{\frac{1}{4}}), \tag{6.2.15}$$

and the minimal polynomial of i:

$$f_2(x) = x^2 + 1 = (x + i)(x - i). \tag{6.2.16}$$

The degree of $\mathbb{E}$ is 8. So there are 8 automorphisms which are obtained by setting $g(2^{\frac{1}{4}})$ equal to one of the 4 roots of $f_1(x)$ and $g(i)$ equal to one of the 2 roots of $f_2(x)$. The group table is given below.

	$2^{\frac{1}{4}}$	i
g_1	$2^{\frac{1}{4}}$	i
g_2	$-2^{\frac{1}{4}}$	i
g_3	$i2^{\frac{1}{4}}$	i
g_4	$-i2^{\frac{1}{4}}$	i
g_5	$2^{\frac{1}{4}}$	$-i$
g_6	$-2^{\frac{1}{4}}$	$-i$
g_7	$i2^{\frac{1}{4}}$	$-i$
g_8	$-i2^{\frac{1}{4}}$	$-i$

TABLE 1. Galois group table of extension $\mathbb{E}$ in Example 1

We can read off from the table straight away that g_1 is the identity element and g_5 is complex conjugation. Notice also that the group elements can be written

in terms of g_3 and g_5:

$$\begin{aligned} g_1 &= g_3^4 & g_5 &= g_5 \\ g_2 &= g_3^2 & g_6 &= g_3^2 g_5 \\ g_3 &= g_3 & g_7 &= g_3 g_5 \\ g_4 &= g_3^3 & g_8 &= g_3^3 g_5 \end{aligned}$$

We say that the group is generated by g_3, g_5 and denote it as

$$\mathcal{G}_{\mathbb{Q}}(\mathbb{E}) = \langle g_3, g_5 \rangle. \tag{6.2.17}$$

Notice also that $g_3 g_5 = g_5 g_3^3$ and so the group is not Abelian. However it still is solvable. Define $\mathcal{H}_0 = \langle e \rangle$ where $e = g_1$ is the identity element, $\mathcal{H}_1 = \{e, g_1, g_3, g_3^2\}$ and $\mathcal{H}_2 = \mathcal{G}_{\mathbb{Q}}(\mathbb{E})$. Then $\mathcal{H}_1$ is a normal subgroup of $\mathcal{G}_{\mathbb{Q}}(\mathbb{E})$ because $g_5 g_3^r g_5^{-1} = g_3^{3r}$ and $\mathcal{H}_1, \mathcal{H}_2/\mathcal{H}_1$ are both Abelian. So the group is solvable. Of course we know in advance that the group is solvable because all the numbers in $\mathbb{E}$ are expressible in radicals.

Example 2. In this example we illustrate subtleties that are not present in the previous example. Let $\mathbb{E} = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}})$. We build the field up as a tower.

$$\begin{aligned} \mathbb{E}_1 &= \mathbb{Q}(\sqrt{2}) \\ \mathbb{E}_2 &= \mathbb{Q}(\sqrt{2+\sqrt{2}}). \end{aligned}$$

The minimal polynomial of $\sqrt{2}$ is $f_1(x) = x^2 - 2$ and of $\sqrt{2+\sqrt{2}}$ is $f_2(x) = x^2 - (2+\sqrt{2})$. The degree of $\mathbb{E}$ is 4. The subtlety is that $f_2(x)$ is the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{E}_1$, but not over $\mathbb{Q}$. To construct the Galois group we need the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$ and this is

$$\begin{aligned} &\tilde{f}_2(x) = x^4 - 4x + 2 = \big(x^2 - (2+\sqrt{2})\big)\big(x^2 - (2+\sqrt{2})\big) \\ &\Rightarrow \tilde{f}_2(x) = \Big(x - \sqrt{2+\sqrt{2}}\Big)\Big(x + \sqrt{2+\sqrt{2}}\Big)\Big(x - \sqrt{2-\sqrt{2}}\Big)\Big(x + \sqrt{2-\sqrt{2}}\Big). \end{aligned} \tag{6.2.18}$$

So the Galois conjugates of $\sqrt{2+\sqrt{2}}$ are $\pm\sqrt{2+\sqrt{2}}$ and $\pm\sqrt{2-\sqrt{2}}$. Notice that $\sqrt{2-\sqrt{2}}$ can be expressed in terms of $\sqrt{2+\sqrt{2}}$:

$$\sqrt{2-\sqrt{2}} = (\sqrt{2}-1)(\sqrt{2+\sqrt{2}}).$$

So the extension is normal. If g is a Galois automorphism then we must have

$$g(\sqrt{2}) = \pm\sqrt{2}. \tag{6.2.19}$$

Now consider the action of g on $\sqrt{2+\sqrt{2}}$.

Case 1. $g(\sqrt{2}) = \sqrt{2}$. Then g doesn't change the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{E}_1$. So $g(\sqrt{2+\sqrt{2}})$ must be one of the two roots of $f_2(x)$:

$$g(\sqrt{2+\sqrt{2}}) = \pm\sqrt{2+\sqrt{2}}. \tag{6.2.20}$$

Case 2. $g(\sqrt{2}) = -\sqrt{2}$. Then g changes $f_2(x)$ to $x^2-(2-\sqrt{2})$. So $g(\sqrt{2+\sqrt{2}})$ must be one of the two roots of $x^2-(2-\sqrt{2})$:

$$g(\sqrt{2+\sqrt{2}}) = \pm\sqrt{2-\sqrt{2}}. \tag{6.2.21}$$

So the Galois group consists of 4 automorphisms as shown in the table below. Notice that g_1 is the identity. Also, the group generator is $g_3 : g_2 = g_3^2$ and $g_4 = g_3^3$.

	$\sqrt{2}$	$\sqrt{2+\sqrt{2}}$
g_1	$\sqrt{2}$	$\sqrt{2+\sqrt{2}}$
g_2	$\sqrt{2}$	$-\sqrt{2+\sqrt{2}}$
g_3	$-\sqrt{2}$	$\sqrt{2-\sqrt{2}}$
g_4	$-\sqrt{2}$	$-\sqrt{2-\sqrt{2}}$

TABLE 2. Galois group table of extension $\mathbb{E}$ in Example 2

So

$$\mathcal{G}_{\mathbb{Q}}(\mathbb{E}) = \langle g_3 \rangle = \{e, g_3, g_3^2, g_3^3\}. \tag{6.2.22}$$

In particular the full group is Abelian.

6.3. Galois-Clifford correspondence

The work we present here is in Appleby, Yadsan-Appleby and Zauner [**17**].

Having explained the basic principles of Galois theory we now apply them to the SIC problem. As the reader will recall that exact fiducial vectors have been calculated in dimensions 2-16, 19, 24, 28, 35, 48 ([**32**, **52**–**54**, **142**–**144**]). It is a striking fact that the components of all these fiducials are expressible in terms of radicals. This means that the associated Galois group must be solvable. This suggested to us that it would be interesting to examine the Galois group. In particular, there are two groups in the problem: the Galois group and the extended Clifford group. We would like to understand the relationships between the actions of these two groups. When we embarked on this work we hoped that this would provide an insight which would enable us to prove existence. Unfortunately that did not happen but we did discover a lot of interesting structure which we feel may be useful in future investigations.

The extended Clifford group $EC(d)$ consists of all unitaries and anti-unitaries U of the form

$$U = e^{i\theta} D_{\mathbf{p}} U_F \tag{6.3.1}$$

where $D_{\mathbf{p}}$ is a displacement operator and U_F is a symplectic unitary or an anti-symplectic anti-unitary, with $\mathbf{p} = (p_1, p_2)^T$, a vector in discrete phase space with components $p_1, p_2 \in \mathbb{Z}_{\bar{d}}$ and $F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ whose entries $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_{\bar{d}}$ and $\det F = 1$ for a symplectic unitary and $\det F = -1$ for an anti-symplectic anti-unitary (please see Chapter 3 for more details).

Recall also that a WH SIC fiducial is a vector which satisfies the equation

$$|\langle\psi|D_{\mathbf{p}}|\psi\rangle| = \begin{cases} 1 & \text{if } \mathbf{p} = \mathbf{0} \\ \frac{1}{\sqrt{d+1}} & \text{if } \mathbf{p} \neq \mathbf{0}. \end{cases} \tag{6.3.2}$$

which therefore has he property that the operators

$$E_{\mathbf{p}} = \frac{1}{d} D_{\mathbf{p}} |\psi\rangle\langle\psi| D_{\mathbf{p}}^{\dagger}. \tag{6.3.3}$$

form a WH SIC-POVM.

If $|\psi\rangle$ is a WH SIC fiducial and U is any Extended Clifford unitary or anti-unitary then $U|\psi\rangle$ is also a SIC fiducial. We call the set of all fiducials obtained by acting on $|\psi\rangle$ with $U \in EC(d)$ the *orbit* of $|\psi\rangle$. This means that any two SIC vectors $|\psi\rangle$ and $|\phi\rangle$ are on the same orbit if and only if

$$\exists U \in EC(d) : |\psi\rangle = U|\phi\rangle. \tag{6.3.4}$$

The $EC(d)$ elements permute the fiducial vectors on the same orbit. In some dimensions there is only one orbit of the $EC(d)$ but usually there are several as can be seen in [**142**]. In the cases where there is more than one orbit, it can happen that there are Galois group elements which move the vector from one orbit to another, Scott and Grassl [**142**] noted that this happens in dimensions 9, 11, 13, 14, 16 (among the cases which have been studied).

We want to find the smallest extension field of $\mathbb{Q}$ which contains all the numbers appearing in the defining Eqs. (6.3.2) and (6.3.3). This means that we require it to contain the components of the fiducial (obtained from Scott and Grasl [**142**]), ω and $\sqrt{d+1}$. We also want it to contain the matrix elements of $U \in EC(d)$. Referring to Eq. (3.2.22) it can be seen that it must therefore contain $\sqrt{d}$ and τ. It will then contain not only the components of $|\psi\rangle$ but also the components of the every other vector on the same orbit as $|\psi\rangle$. Finally, we want it to be a Galois extension of $\mathbb{Q}$ so that we can apply the special results which hold for the Galois extension which are described in Section 6.2.1.2. Since extensions of $\mathbb{Q}$ are automatically separable. It is enough to require it to be a normal extension of $\mathbb{Q}$. (see Section 6.2.1.2. To summarize we define $\mathbb{E}$ to be the smallest normal extension of $\mathbb{Q}$ which contains components of $|\psi\rangle, \tau, \sqrt{d}, \sqrt{d+1}$.

We define $\mathcal{G}$ to be the Galois group of the extension $\mathbb{E}$ over $\mathbb{Q}$. We will be particularly interested in the subgroup of $\mathcal{G}$ consisting of all automorphisms which commute with complex conjugation. We denote this subgroup $\mathcal{G}_c$. This subgroup is important for a number of reasons. One reason is that it takes Hermitian operators to Hermitian operators. Another reason is that it takes normalized vectors to normalized vectors.

6.3.1. Action of $\mathcal{G}$ on the matrices $D_{\mathbf{p}}$ and U_F. Before considering the action of $\mathcal{G}$ on the fiducial vector we need to examine its action on the elements of $EC(d)$. For all $g \in \mathcal{G}$

$$g(\sqrt{d}) = \pm\sqrt{d}, \tag{6.3.5}$$

because

$$g\big((\sqrt{d})^2\big) = d \implies \big(g(\sqrt{d})\big)^2 = d \implies g(\sqrt{d}) = \pm\sqrt{d}.$$

We also have

$$g(\tau) = \tau^{k_g}. \tag{6.3.6}$$

and

$$g(\omega) = \omega^{k_g}. \tag{6.3.7}$$

for some k_g such that k_g and d are coprime. This is because g is an automorphism only if k_g and d are coprime. Since

$$\omega^d = 1, \tag{6.3.8}$$

we must have

$$\big(g(\omega)\big)^d = 1, \tag{6.3.9}$$

implying

$$g(\omega) = \omega^k, \tag{6.3.10}$$

for some integer k. We can now see why k_g and d are coprime by the following argument: suppose k and d are not coprime. Then there is a number n that divides both k and d. Let $k' = k/n$ and $d' = d/n$. Then,

$$g(\omega) = \omega^k = e^{\frac{2\pi i k}{d}} = e^{\frac{2\pi i k'}{d'}}.$$

implying $g(\omega^{d'}) = 1$ and consequently $\omega^{d'} = 1$ which is a contradiction.

There is a further question: given k coprime to d is there always a g such that $g(\omega) = \omega^{k_g}$? The answer is yes. It can be shown [**147**] that the degree of the minimal polynomial of ω is the same as the number of positive integers $< d$ which are relatively prime to d. It can also be shown that the order of the Galois group of $\mathbb{Q}(\omega)$ is equal to the degree of the minimal polynomial of ω. So the number of Galois automorphisms of $\mathbb{Q}(\omega)$ is equal to the number of integers relatively prime to d. So there is one automorphism for each k relatively prime to d.

We are now in a position to explain how a Galois automorphism g acts on the displacement operators $D_{\mathbf{p}}$ and unitaries and anti-unitaries U_F. The result is most conveniently stated as a theorem.

THEOREM 7. *We have*

$$g(D_{\mathbf{p}}) = D_{H_g \mathbf{p}}. \tag{6.3.11}$$

for all $\mathbf{p}$*, and*

$$g(U_F) \doteq U_{H_g F H_g^{-1}} \tag{6.3.12}$$

for all $F \in \mathrm{SL}(2,\mathbb{Z}_{\bar{d}})$*, where* $\doteq$ *means equal up to a phase and*

$$H_g = \begin{pmatrix} 1 & 0 \\ 0 & k_g \end{pmatrix}$$

where k_g *is given in Eq. (6.3.6). If* $g \in \mathcal{G}_c$ *we also have*

$$g(U_F) \doteq U_{H_g F H_g^{-1}}, \tag{6.3.13}$$

for all anti-symplectic matrices F*.*

REMARK 5. *Observe that* H_g *belongs to* $\mathrm{GL}(2,\mathbb{Z}_{\bar{d}})$*, the group of all* 2×2 *matrices with entries in* $\mathbb{Z}_{\bar{d}}$ *whose determinant is relatively prime to* $\bar{d}$ *(the requirement that the determinant is relatively prime to* $\bar{d}$ *means that the matrices are invertible). However, since* k_g *is not necessarily equal to* ± 1*,* H_g *will not necessarily belong to* $\mathrm{ESL}(2,\mathbb{Z}_{\bar{d}})$*.*

PROOF. We have

$$D_{\mathbf{p}} = \tau^{p_1 p_2} \sum_{r=0}^{d-1} \omega^{p_2 r} |r + p_1\rangle\langle r| \tag{6.3.14}$$

Acting on both sides of this equation with g we see that

$$g(D_{\mathbf{p}}) = D_{p_1, k_g p_2} = D_{H_g \mathbf{p}}. \tag{6.3.15}$$

Now suppose

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{6.3.16}$$

is a prime symplectic matrix so that

$$U_F = \frac{1}{\sqrt{d}} \sum \tau^{\beta^{-1}(\alpha s^2 - 2rs + \delta r^2)} |r\rangle\langle s|. \tag{6.3.17}$$

Applying g to both sides of this equation we find

$$g(U_F) = \pm\frac{1}{\sqrt{d}}\sum \tau^{k_g\beta^{-1}(\alpha s^2 - 2rs + \delta r^2)}|r\rangle\langle s| \tag{6.3.18}$$

$$\doteq U_{H_g F H_g^{-1}}. \tag{6.3.19}$$

Suppose on the other hand F is not a prime matrix. Then $F = F_1F_2$ where F_1, F_2 are both prime matrices. So

$$g(U_F) = g(U_{F_1})g(U_{F_2}) = U_{H_g F_1 H_g^{-1}} U_{H_g F_2 H_g^{-1}} = U_{H_g F H_g^{-1}}. \tag{6.3.20}$$

Finally suppose $g \in \mathcal{G}_c$ and suppose that F is anti-symplectic. Then for all $|\phi\rangle$

$$U_F|\phi\rangle \doteq U_{FJ}|g_c(\phi)\rangle. \tag{6.3.21}$$

where g_c is complex conjugation and where J is the matrix defined in Section 2.5. Applying g to both sides we find

$$g(U_F|\phi\rangle) = U_{H_g F J H_g^{-1}}|g_c g(\phi)\rangle = U_{H_g F H_g^{-1}}|g(\phi)\rangle. \tag{6.3.22}$$

Hence

$$g(U_F) = U_{H_g F H_g^{-1}}. \tag{6.3.23}$$

□

6.3.2. Action of $\mathcal{G}_c$ on the fiducial vector $|\psi\rangle$. We now come to the main point which is the action of Galois group on the fiducial vector $|\psi\rangle$. As we noted above if $\mathcal{G}$ does not commute with complex conjugation it does not necessarily preserve normalization. Since the fiducial vector is normalized by definition we confine ourselves to automorphisms in the subgroup $\mathcal{G}_c$. We begin by showing that $\mathcal{G}_c$ preserves the fiduciality property. The fiducial vector $|\psi\rangle$ satisfies

$$\langle\psi|D_{\mathbf{p}}|\psi\rangle = \begin{cases} 1 & \text{if } \mathbf{p} = 0 \\ \frac{e^{i\theta_{\mathbf{p}}}}{\sqrt{d+1}} & \text{if } \mathbf{p} \neq 0. \end{cases} \tag{6.3.24}$$

If $g \in \mathcal{G}_c$ then

$$g(\langle\psi|) = \langle g(\psi)|, \tag{6.3.25}$$

(notice this would not be true if g did not commute with complex conjugation). Also if $e^{i\theta}$ is any phase belonging to $\mathbb{F}$ then

$$|g(e^{i\theta})|^2 = g(e^{i\theta}g^{-i\theta}) = 1 \tag{6.3.26}$$

implying that $g(e^{i\theta})$ is also a phase. Consequently if we apply g to both sides of Eq. (6.3.24) we find

$$\langle g\psi|D_{H_g\mathbf{p}}|g\psi\rangle = \begin{cases} 1 & \text{if } \mathbf{p} = 0 \\ \pm\frac{g(e^{i\theta_{\mathbf{p}}})}{\sqrt{d+1}} & \text{if } \mathbf{p} \neq 0 \end{cases}. \tag{6.3.27}$$

or

$$\langle g\psi|D_{\mathbf{p}}|g\psi\rangle = \begin{cases} 1 & \text{if } \mathbf{p} = 0 \\ \pm\frac{e^{i\tilde{\theta}_{\mathbf{p}}}}{\sqrt{d+1}} & \text{if } \mathbf{p} \neq 0 \end{cases} \tag{6.3.28}$$

where $e^{i\tilde{\theta}_{\mathbf{p}}} = g\left(e^{i\theta_{H_g^{-1}\mathbf{p}}}\right)$. So $|g(\psi)\rangle$ is also a fiducial.

Now let $\mathcal{G}_o$ be the subset of $\mathcal{G}_c$ consisting of g's such that $g(|\psi\rangle)$ is on the same orbit of the extended Clifford group as $|\psi\rangle$ (where the subscript o stands for orbit). For each $g \in \mathcal{G}_o$ there is a $U_g \in \mathrm{EC}(d)$ such that

$$g(|\psi\rangle) = U_g|\psi\rangle. \tag{6.3.29}$$

We can write

$$U_g = D_{\mathbf{q}_g}U_{F_g}. \tag{6.3.30}$$

for some $\mathbf{q}_g$ and F_g.

Let $\mathcal{S}_\psi$ be the stabilizer of $|\psi\rangle$, i.e. the set of all unitaries and anti-unitaries V such that $V|\psi\rangle \doteq |\psi\rangle$. Then we can replace U_g with U_gV for any $V \in \mathcal{S}_\psi$. In

some dimensions every SIC vector lies on the same orbit. In such cases $\mathcal{G}_o = \mathcal{G}_c$. For other cases we want to show that $\mathcal{G}_o$ is a group. To see this observe that if $g_1, g_2 \in \mathcal{G}_o$ then

$$|g_1 g_2(\psi)\rangle = g_1(U_{g_2}|\psi\rangle) = g_1(U_{g_2})g_1|\psi\rangle = g_1(U_{g_2})U_{g_1}|\psi\rangle \tag{6.3.31}$$

It follows from Theorem 7 that $g_1(U_{g_2}) \in \mathrm{EC}(d)$. Therefore $g_1 g_2 \in \mathcal{G}_o$ and

$$U_{g_1 g_2} \doteqdot g_1(U_{g_2})U_{g_1}. \tag{6.3.32}$$

where the notation $V \doteqdot V'$ means $V = V'W$ for some $W \in \mathcal{S}_\psi$. Also if $g \in \mathcal{G}_o$ we find, by acting on both sides of

$$g(|\psi\rangle) = U_g|\psi\rangle \tag{6.3.33}$$

with g^{-1}, that

$$|\psi\rangle = g^{-1}(U_g)g^{-1}|\psi\rangle. \tag{6.3.34}$$

It follows from Theorem 7 that $g^{-1}(U_g) \in \mathrm{EC}(d)$. So $g^{-1} \in \mathcal{G}_o$ and

$$U_{g^{-1}} \doteqdot (g^{-1}(U_g))^\dagger = g^{-1}(U_g^\dagger). \tag{6.3.35}$$

6.3.3. Special form of the unitary U_g. In this section we will show if d is not divisible by 3 then under certain assumptions which hold in every known case, it can be assumed that the vector $\mathbf{q}_g$ in Eq. (6.3.30) is zero, so that

$$U_g = U_{F_g} \tag{6.3.36}$$

If on the other hand d is divisible by 3 then under the same assumptions it can be assumed that

$$U_g = D_{\mathbf{q}_g} U_{F_g} \tag{6.3.37}$$

where $\mathbf{q}_g = 0 \mod \frac{d}{3}$. Let us now explain the properties which must hold for this statement to be true. We need to give two definitions.

DEFINITION 1. ***Canonical Order 3 Unitary.*** *Let F be a symplectic matrix F such that*

$$Tr[F] = -1 \mod d. \tag{6.3.38}$$

with $F \neq I$. Then

$$(D_{\mathbf{p}} U_F)^3 = I, \tag{6.3.39}$$

for all $\mathbf{p}$. We say that $D_{\mathbf{p}} U_F$ is a canonical order 3 unitary.

REMARK 6. *The requirement that $F \neq I$ is only necessary in d=3 as $Tr[I] = -1$ mod d if and only if $d = 3$.*

It is an observed fact so far unexplained that for every known WH SIC fiducial vector $|\psi\rangle$ $\mathcal{S}_\psi$ contains a canonical order 3 unitary [**32**, **52**, **53**].

DEFINITION 2. ***Displacement Free.*** *We say $\mathcal{S}_\psi$ is displacement free if it entirely consists of unitaries and anti-unitaries of the form U_F.*

It is another observed though unexplained fact that for every known WH SIC fiducial $|\psi\rangle$ there is a SIC fiducial $|\psi'\rangle$ on the same orbit as $|\psi\rangle$ such that $\mathcal{S}_{\psi'}$ is displacement free.

The conditions for the statements made in the first paragraph of this section to be true are that $\mathcal{S}_\psi$ (a) contains a canonical order 3 unitary (b) is displacement free. To prove this we will need the following theorem [**32**].

THEOREM 8. *If d is odd then $D_{\mathbf{p}} U_G \doteq I$ if and only if $\mathbf{p} = 0$ and $G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. If d is even then $D_{\mathbf{p}} U_G \doteq I$ if and only if*

$$\mathbf{p} = \begin{pmatrix} \frac{sd}{2} \\ \\ \frac{td}{2} \end{pmatrix},$$

$$G = \begin{pmatrix} 1+rd & sd \\ td & 1+rd \end{pmatrix}, \tag{6.3.40}$$

for arbitrary integers r, s, t.

We are now ready to prove the main result of this section.

THEOREM 9. *Let $|\psi\rangle$ be a fiducial vector whose stability group $\mathcal{S}_\psi$ (a) contains canonical order 3 unitary and (b) is displacement free. Then, for all $g \in \mathcal{G}_o$, and taking into account the freedom expressed by Eq. (6.3.40), it is possible to choose $\mathbf{q}_g$ and F_g in Eq. (6.3.30) in such a way that*

$$\mathbf{q}_g = \begin{cases} \mathbf{0} & \text{if } d \text{ is not a multiple of 3} \\ \mathbf{0} \mod \frac{d}{3} & \text{if } d \text{ is a multiple of 3} \end{cases}. \tag{6.3.41}$$

PROOF. Let $\mathcal{S}_{g\psi}$ be the stability group of $g(|\psi\rangle)$. It is a straightforward consequence of the definitions that

$$U_g^\dagger \mathcal{S}_\psi U_g = \mathcal{S}_{g\psi} = g(\mathcal{S}_\psi). \tag{6.3.42}$$

It is also convenient to define

$$S_\psi = \{G \in \mathrm{ESL}(2, \mathbb{Z}_{\bar{d}}) : U_G \in \mathcal{S}_\psi\}. \tag{6.3.43}$$

Because $\mathcal{S}_\psi$ is displacement free it consists of operators U_G with $G \in S_\psi$.

Now choose a symplectic matrix $G \in S_\psi$ such that $Tr[G] = -1 \mod d$ and $G \neq I$ (this is possible because we are assuming that $\mathcal{S}_\psi$ contains a canonical order 3 unitary). It follows from Eq. (6.3.42) that there exist $G' \in S_\psi$ such that

$$g(U_G) \doteq U_g U_{G'} U_g^\dagger, \tag{6.3.44}$$

or

$$U_{H_g G H_g^{-1}} \doteq D_{\mathbf{q}_g} U_{F_g} U_{G'} U_{F_g^{-1}} D_{-\mathbf{q}_g} \tag{6.3.45}$$

After rearranging this becomes

$$D_{\tilde{G}\mathbf{q}_g-\mathbf{q}_g}U_{\tilde{G}F_gG'^{-1}F_g^{-1}}\doteq I \tag{6.3.46}$$

where $\tilde{G}=H_gGH_g^{-1}$. It follows from Theorem 8 that

$$\tilde{G}\mathbf{q}_g-\mathbf{q}_g=\begin{cases}\mathbf{0} \mod d & \text{if } d \text{ is odd}\\ \mathbf{0} \mod \frac{d}{2} & \text{if } d \text{ is even}\end{cases}. \tag{6.3.47}$$

Since $Tr[\tilde{G}]=Tr[G]=-1 \mod d$ we can write

$$\tilde{G}=\begin{pmatrix}\alpha & \beta\\ \gamma & -\alpha-1\end{pmatrix}. \tag{6.3.48}$$

The fact that $\det\tilde{G}=\det G=1$ means α,β,γ must satisfy

$$\alpha^2+\alpha+\beta\gamma+1=0 \mod \bar{d} \tag{6.3.49}$$

It is easily verified that

$$\begin{pmatrix}-(\alpha+2) & -\beta\\ -\gamma & (\alpha-1)\end{pmatrix}(\tilde{G}-I)=3I \mod \bar{d} \tag{6.3.50}$$

implying

$$3\mathbf{q}_g=\begin{cases}\mathbf{0} \mod d & \text{if } d \text{ is odd}\\ \mathbf{0} \mod \frac{d}{2} & \text{if } d \text{ is even}\end{cases}. \tag{6.3.51}$$

We now analyze this equation case by case.

Case 1 a: d is odd and not divisible by 3 We then have

$$\begin{aligned}&3\mathbf{q}_g=\mathbf{0} \mod d\\ \implies &\mathbf{q}_g=\mathbf{0} \mod d.\end{aligned} \tag{6.3.52}$$

Case 1 b: d is odd and divisible by 3. In this case we have

$$\begin{aligned} 3\mathbf{q}_g &= \mathbf{0} \mod d \\ \implies \mathbf{q}_g &= \mathbf{0} \mod \frac{d}{3}. \end{aligned} \tag{6.3.53}$$

This proves the result for odd dimensions.

For even dimensions we first note that Theorem 8 implies

$$U_g = D_{\mathbf{q}_g} U_{F_g} = D_{\mathbf{q}_g} D_{\mathbf{p}} U_F U_{F_g} = D_{\mathbf{q}_g + \mathbf{p}} U_{F F_g}, \tag{6.3.54}$$

So we are free to replace $\mathbf{q}_g$ by $\mathbf{q}_g + \mathbf{p}$ and F_g by $F F_g$ where

$$\mathbf{p} = \begin{pmatrix} \frac{sd}{2} \\ \frac{td}{2} \end{pmatrix}, \qquad\qquad F = \begin{pmatrix} 1 + rd & sd \\ td & 1 + rd \end{pmatrix} \tag{6.3.55}$$

for arbitrary integers r, s, t.

Case 2 a: d is even and not divisible by 3. We have

$$\begin{aligned} 3\mathbf{q}_g &= \mathbf{0} \mod \frac{d}{2} \\ \implies \mathbf{q}_g &= \mathbf{0} \mod \frac{d}{2} \\ \implies \mathbf{q}_g &= \begin{pmatrix} j\frac{d}{2} \\ k\frac{d}{2} \end{pmatrix}. \end{aligned} \tag{6.3.56}$$

So we now want to choose $\mathbf{p}$ in Eq. (6.3.55) such that $\mathbf{q}'_g = \mathbf{q}_g + \mathbf{p} = \mathbf{0} \mod d$. We have

$$\mathbf{q}'_g = \begin{pmatrix} j\frac{d}{2} \\ k\frac{d}{2} \end{pmatrix} + \begin{pmatrix} s\frac{d}{2} \\ t\frac{d}{2} \end{pmatrix} \tag{6.3.57}$$

We choose $s = -j$ and $t = -k$ to obtain $\mathbf{q}'_g = \mathbf{0} \mod d$.

Case 2b: d is even and divisible by 3:

$$3\mathbf{q}_g = \mathbf{0} \mod \frac{d}{2}$$

$$\implies \mathbf{q}_g = \mathbf{0} \mod \frac{d}{6}$$
$$\implies \mathbf{q}_g = \begin{pmatrix} jn \\ kn \end{pmatrix}. \tag{6.3.58}$$

where we defined $n = \frac{d}{6}$. We now want to choose $\mathbf{p}$ in Eq. (6.3.55) such that $\mathbf{q}'_g = \mathbf{q}_g + \mathbf{p} = \mathbf{0} \mod \frac{d}{3}$. We have

$$\mathbf{q}'_g = \begin{pmatrix} jn \\ kn \end{pmatrix} + \begin{pmatrix} 3sn \\ 3tn \end{pmatrix} = \begin{pmatrix} (j+3s)n \\ (k+3t)n \end{pmatrix} \tag{6.3.59}$$

If j is even (respectively odd) we choose s even (respectively odd) so that $j+3s$ is even. Similarly we can choose t so that $k+3t$ is even. With these choices $\mathbf{q}'_g = \mathbf{0}$ mod $\frac{d}{3}$ as required. □

6.3.4. Action of $\mathcal{G}_o$ on the overlaps. Up to now we have been looking at the action of $\mathcal{G}_o$ on the fiducial vector $|\psi\rangle$. In this section we examine the action of $\mathcal{G}_o$ on the phases

$$e^{i\theta_{\mathbf{p}}} = \sqrt{d+1}\langle\psi|D_{\mathbf{p}}|\psi\rangle. \tag{6.3.60}$$

This will lead us to an interesting relation between $\mathcal{G}_o$ and a subgroup of $GL(2, \mathbb{Z}_{\bar{d}})$ (see Theorem 11 below). We assume that $\mathcal{S}_\psi$ contains a canonical order 3 unitary and is displacement free. We also assume that $\mathbf{q}_g$ and F_g are chosen as described in the Theorem 9. We then have the following theorem.

THEOREM 10. *If $g \in \mathcal{G}_o$ then*

$$g(e^{i\theta_{\mathbf{p}}}) = s\omega^{-\langle \mathbf{q}_g, H_g\mathbf{p}\rangle} e^{i\theta \bar{F}_g \mathbf{p}} \tag{6.3.61}$$

where

$$s = \frac{g(\sqrt{d+1})}{\sqrt{d+1}} = \pm 1 \tag{6.3.62}$$

and

$$\tilde{F}_g = \begin{cases} F_g^{-1} H_g & \text{if } \det F_g = 1 \\ -F_g^{-1} H_g & \text{if } \det F_g = -1 \end{cases} . \tag{6.3.63}$$

PROOF. Suppose $\det F_g = 1$. Then

$$g(e^{i\theta_{\mathbf{p}}}) = s\sqrt{d+1}\langle g\psi | D_{H_g\mathbf{p}} | g\psi\rangle \tag{6.3.64}$$

$$= s\sqrt{d+1}\omega^{-\langle \mathbf{q}_g, H_g\mathbf{p}\rangle}\langle \psi | D_{\tilde{F}_g^{-1}H_g\mathbf{p}} | \psi\rangle \tag{6.3.65}$$

$$= s\omega^{-\langle \mathbf{q}_g, H_g\mathbf{p}\rangle} e^{i\theta_{\tilde{F}_g\mathbf{p}}} \tag{6.3.66}$$

Suppose on the other hand $\det F_g = -1$. Then

$$g(e^{i\theta_{\mathbf{p}}}) = s\sqrt{d+1}\langle g\psi | D_{H_g\mathbf{p}} | g\psi\rangle \tag{6.3.67}$$

$$= s\sqrt{d+1}\omega^{-\langle \boldsymbol{q}_g, H_g\mathbf{p}\rangle}\langle g_c\psi | D_{JF_g^{-1}H_g\mathbf{p}} | g_c\psi\rangle \tag{6.3.68}$$

$$= s\sqrt{d+1}\omega^{-\langle \boldsymbol{q}_g, H_g\mathbf{p}\rangle} g_c\langle \psi | D_{F_g^{-1}H_g\mathbf{p}} | \psi\rangle \tag{6.3.69}$$

$$= s\sqrt{d+1}\omega^{-\langle \boldsymbol{q}_g, H_g\mathbf{p}\rangle}\langle \psi | D_{-F_g^{-1}H_g\mathbf{p}} | \psi\rangle \tag{6.3.70}$$

$$= s\sqrt{d+1}\omega^{-\langle \boldsymbol{q}_g, H_g\mathbf{p}\rangle} e^{i\theta\tilde{F}_g\mathbf{p}} \tag{6.3.71}$$

□

6.3.5. Structure of the group $\mathcal{G}_o$. In this section we prove a result concerning the structure of the group $\mathcal{G}_o$. Let N_ψ be the normalizer of S_ψ (i.e. the set of all $G \in \mathrm{GL}(2, \mathbb{Z}_{\bar{d}})$ such that $GS_\psi G^{-1} \subseteq S_\psi$. We now prove the following lemma.

LEMMA 2. *Let $|\psi\rangle$ be a fiducial vector whose stability group $\mathcal{S}_\psi$ (a) contains a canonical order 3 unitary and (b) is displacement free. Then $\tilde{F}_g \in N_\psi$ for all g (where $\tilde{F}_g$ is the matrix defined by Eq. (6.3.63)).*

PROOF. Let $G \in S_\psi$ be arbitrary. Then by the same argument that led to Eqn. (6.3.46) there exists $G' \in S_\psi$ such that

$$D_{\tilde{G}\mathbf{q}_g - \mathbf{q}_g} U_{\tilde{G}F_g G'^{-1} F_g^{-1}} \doteq I, \tag{6.3.72}$$

where $\tilde{G} = H_g G H_g^{-1}$.

Case 1: d is odd.

It follows from Theorem 8 that

$$H_g G H_g^{-1} F_g G'^{-1} F_g^{-1} = I, \tag{6.3.73}$$

implying

$$\tilde{F}_g G \tilde{F}_g^{-1} = G' \tag{6.3.74}$$

So

$$\tilde{F}_g \in N_\psi \tag{6.3.75}$$

Case 2: d is even. It follows from Theorem 8 that

$$H_g G H_g^{-1} \mathbf{q}_g - \mathbf{q}_g = \begin{pmatrix} s\frac{d}{2} \\ t\frac{d}{2} \end{pmatrix} \mod d. \tag{6.3.76}$$

and

$$H_g G H_g^{-1} F_g G'^{-1} F_g^{-1} = \begin{pmatrix} 1+rd & sd \\ td & 1+rd \end{pmatrix} \mod 2d \tag{6.3.77}$$

where $r, s, t = 0, 1$. From Theorem 9 we have

$$H_g G H_g^{-1} \mathbf{q}_g - \mathbf{q}_g = \begin{cases} \mathbf{0} \mod d & \text{if } d \text{ is not divisible by 3} \\ \mathbf{0} \mod \frac{d}{3} & \text{if } d \text{ is divisible by 3} \end{cases} \tag{6.3.78}$$

It follows that $s = t = 0$ and

$$H_g G H_g^{-1} F_g G'^{-1} F_g^{-1} = P \tag{6.3.79}$$

where

$$P = \begin{pmatrix} 1+rd & 0 \\ 0 & 1+rd \end{pmatrix}, \tag{6.3.80}$$

implying

$$\tilde{F}_g G \tilde{F}_g^{-1} = PG' \tag{6.3.81}$$

where we used the fact that P commutes with F_g and G'. The fact that $U_P \doteq I$ means $|G' \in S_\psi$. So $\tilde{F}_g \in N_\psi$. □

We now prove the main result of this section.

THEOREM 11. *Let $|\psi\rangle$ be a fiducial vector whose stability group $\mathcal{S}_\psi$ (a) contains canonical order 3 unitary and (b) is displacement free. Then the map $f : g \to \tilde{F}_g S_\psi$ is a homomorphism of the group $\mathcal{G}_o$ into the quotient group N_ψ / S_ψ*

PROOF. Let $g_1, g_2 \in \mathcal{G}_o$ be arbitrary. By Eq. (6.3.32) we have

$$U_{g_1 g_2} \doteq g_1(U_{g_2}) U_{g_1} U_L, \tag{6.3.82}$$

for some $L \in S_\psi$. Hence

$$D_{H_{g_1}\mathbf{q}_{g_2} + H_{g_1} F_{g_2} H_{g_1}^{-1} \mathbf{q}_{g_1} - \mathbf{q}_{g_1 g_2}} U_{H_{g_1} F_{g_2} H_{g_1}^{-1} F_{g_1} L^{-1} F_{g_1 g_2}^{-1}} \doteq I. \tag{6.3.83}$$

By the same argument that led to Eq. (6.3.74) and Eq. (6.3.81) it follows that

$$H_{g_1} F_{g_2} H_{g_1}^{-1} F_{g_1} = F_{g_1 g_2} M, \tag{6.3.84}$$

where

$$M = \begin{cases} L & d \text{ odd} \\ PL & d \text{ even.} \end{cases}, \tag{6.3.85}$$

P being the matrix defined by Eq. (6.3.80). Hence

$$\tilde{F}_{g_1}\tilde{F}_{g_2} = M\tilde{F}_{g_1 g_2} = \tilde{F}_{g_1 g_2}M', \tag{6.3.86}$$

for some matrix $M' \in S_\psi$ (since $F_{g_1 g_2}$ is in the normalizer of S_ψ). Consequently

$$f(g_1 g_2) = f(g_1)f(g_2), \tag{6.3.87}$$

implying f is a homomorphism. □

Let $\mathcal{G}_o^0$ be the kernel of the homomorphism f. Then the result just proved shows that $\mathcal{G}_o/\mathcal{G}_o^0$ is isomorphic to a subgroup of N_ψ/S_ψ. In Appleby, Yadsan-Appleby and Zauner [**17**] we calculate $\mathcal{G}_o$ for all 27 known exact fiducials with $d > 3$. We find

(1) The subgroup of N_ψ/S_ψ is in fact always C_ψ/S_ψ where C_ψ is the centralizer of S_ψ (i.e. the set of all $G \in \mathrm{GL}(2, \mathbb{Z}_{\tilde{d}})$ which commute with every element of S_ψ).
(2) $\mathcal{G}_o^0$ is always isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

.

6.4. Dimension 6 analysis

In the previous sections we proved some general results. In this section we will illustrate these results by applying them to the exact fiducial in dimension 6 which is given in Appendix A. We constructed the following field tower

$$\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \mathbb{F}_3 \subseteq \mathbb{F}_4 \subseteq \mathbb{F}_5.$$

with

$$\mathbb{F} = \mathbb{Q}(a),$$

$$\mathbb{F}_1 = \mathbb{Q}(a, a_1),$$

$$\mathbb{F}_2 = \mathbb{Q}(a, a_1, a_2),$$

$$\mathbb{F}_3 = \mathbb{Q}(a, a_1, a_2, a_3),$$

$$\mathbb{F}_4 = \mathbb{Q}(a, a_1, a_2, a_3, a_4)$$

$$\mathbb{F}_5 = \mathbb{Q}(a, a_1, a_2, a_3, a_4, a_5). \tag{6.4.1}$$

where $\mathbb{F}_5$ is the smallest normal extension of $\mathbb{Q}$ containing the components of the fiducial, $\tau = -e^{\frac{\pi i}{6}}$ and $\sqrt{6}$ and $\sqrt{7}$ (i.e. the field denoted $\mathbb{F}$ in previous sections), and where the numbers $a, a_1, a_2, a_3, a_4, a_5$ are the field generators given by

$$a = \sqrt{21}, \tag{6.4.2}$$

$$a_1 = i, \tag{6.4.3}$$

$$a_2 = e^{\frac{\pi i}{3}}, \tag{6.4.4}$$

$$a_3 = \sqrt{9 + \sqrt{21}}, \tag{6.4.5}$$

$$a_4 = \sqrt{3}\big(2(-3i + \sqrt{7})\big)^{\frac{1}{3}} \tag{6.4.6}$$

$$a_5 = \sqrt{6} \tag{6.4.7}$$

In the appendix we give an expression for the unnormalized fiducial vector in terms of these generators. To calculate the full field extension $\mathbb{F}_5$ we examine the minimal polynomials of these numbers over $\mathbb{Q}$. They are

$$f_0(x) = x^2 - 21,$$

$$f_1(x) = x^2 + 1,$$

$$f_2(x) = x^2 - x + 1,$$

$$f_3(x) = x^4 - 18x^2 - 3,$$

$$f_4(x) = x^{12} + 432x^6 + 2985984,$$

$$f_5(x) = x^2 - 6. \tag{6.4.8}$$

We now factor every polynomial in every extension field until we have all the roots. We know that all above polynomials split linearly in $\mathbb{F}_5$ however we still need to analyze how each polynomial splits in every subfield. The reason for this is that the way these polynomials split in the subfields affect our construction of Galois group as we will see later. Our results are given in Table 3.

Generators	$\mathbb{Q}$	$\mathbb{F}$	$\mathbb{F}_1$	$\mathbb{F}_2$	$\mathbb{F}_3$	$\mathbb{F}_4$	$\mathbb{F}_5$
a	x^2-21	$x+a$, $x-a$	DNFF	DNFF	DNFF	DNFF	DNFF
a_1	x^2+1	DNFF	$x+a_1$, $x-a_1$	DNFF	DNFF	DNFF	DNFF
a_2	x^2-x+1	DNFF	DNFF	$x-a_2$, $x+a_2-1$	DNFF	DNFF	DNFF
a_3	x^4-18x^2-3	x^2-2a-9, x^2+2a-9	DNFF	DNFF	$x-a_3$, $x+a_3$, $x-\frac{1}{3}(2a-9)(2a_2-1)a_3$, $x+\frac{1}{3}(2a-9)(2a_2-1)a_3$	DNFF	DNFF
a_4	$x^{12}+432x^6+2985984$	x^6-12ax^3+1728, x^6+12ax^3+1728	DNFF	$x^3+36a_2-6a-18$, $x^3-36a_2-6a+18$, $x^3-36a_2+6a+18$, $x^3+36a_2+6a-18$	DNFF	$x-a_4$, $x+(1-a_2)a_4$, $x+a_2a_4$, $x-\frac{1}{24}(-3+a+6a_2)a_4^2$, $x+\frac{1}{24}(3+a+(3-a)a_2)a_4^2$, $x+\frac{1}{24}(-6+(3+a)a_2)a_4^2$, $x+a_4$, $x-a_2a_4$, $x+(a_2-1)a_4$, $x+\frac{1}{24}(-3+a+6a_2)a_4^2$, $x-\frac{1}{24}(-6+(3+a)a_2)a_4^2$, $x+\frac{1}{24}(a(a_2-1)-3(a_2+1))a_4^2$	DNFF
a_5	x^2-6	DNFF	DNFF	DNFF	DNFF	DNFF	$x-a_5, x+a_5$

TABLE 3. Factorization of defining polynomials over the subfields, where DNFF stands for 'does not factor further'.

6.4.1. Calculating the Galois group. To construct the Galois group for dimension 6 we use the same method in the two examples in section 6.2.3. The only difference is that the calculations are more complicated here and the use of a computer algebra program (Magma) is essential. The field is degree 96, so there are 96 automorphisms. The first step was to calculate all 96 automorphisms using Magma. We then selected a set of generators that would generate all 96 automorphisms. To do this we used a well known property of any group, namely the order of the full group is divisible by the order of any of its subgroups. In our case, using Magma we found that the orders of the group elements are 2,3,4,6. We want to find a set of group elements $g_1, \ldots, g_n$ such that every element of the group can be written as

$$g_1^{r_1} \ldots g_n^{r_n}. \tag{6.4.9}$$

where different choices of the integers $r_1, \ldots, r_n$ give different group elements. We then picked a list of candidates for which the equation below holds:

$$|g_1| \times \cdots \times |g_n| = 96, \tag{6.4.10}$$

where the notation $|g_i|$ denotes the order of group element g_i. We tried a few possible products of the orders that satisfied this equation: $2\times3\times4\times4$, $2\times2\times4\times6$ and $2\times2\times2\times2\times6$. We found that the last two of these combinations generate the full group. We chose the very last one because this combination included complex conjugation g_c as generator (which is convenient to have when constructing the subgroup $\mathcal{G}_c$). So the full group $\mathcal{G}$ is generated by

$$\mathcal{G} = \langle g_c, g_1, g_2, g_3, g_4 \rangle. \tag{6.4.11}$$

where g_c, g_1, g_2, g_3, g_4 are defined in Table 4 and where the orders of group elements are as follows:

$$|g_c| = 2,\ |g_1| = 2,\ |g_2| = 6,\ |g_3| = 2,\ |g_4| = 2. \tag{6.4.12}$$

	a	a_1	a_2	a_3	a_4	a_5
g_c	a	$-a_1$	$1-a_2$	a_3	$\Big(\frac{1}{4}a_2+\frac{1}{24}(a-3)\Big)a_4^2$	a_5
g_1	a	a_1	$1-a_2$	$-a_3$	$\Big(\frac{1}{4}a_2+\frac{1}{24}(a-3)\Big)a_4^2$	a_5
g_2	a	$-a_1$	a_2	a_3	$-a_2a_4$	a_5
g_3	$-a$	a_1	a_2	$\frac{1}{3}(4a-18)a_2+\frac{1}{3}(-2a+9)a_3$	$\Big(-\frac{1}{4}a_2+\frac{1}{24}(-a+3)\Big)a_4^2$	a_5
g_4	a	a_1	a_2	a_3	a_4	$-a_5$

TABLE 4. Action of the group generators g_c, g_1, g_2, g_3 and g_4 on the field generators $a, a_1, a_2, a_3, a_4, a_5$

Recall that we defined the subgroup $\mathcal{G}_o$ of $\mathcal{G}_c$ to be the group whose elements permute the fiduicals on the same orbit. In dimension 6 there is only one orbit and therefore

$$\mathcal{G}_o = \mathcal{G}_c$$

We found that complex conjugation g_c commutes with all generators except g_3. So we conclude that the subgroup $\mathcal{G}_c$ is generated by g_c, g_1, g_2, g_4. In other words,

$$\mathcal{G}_c = \langle g_c, g_1, g_2, g_4 \rangle. \tag{6.4.13}$$

We find that $\mathcal{G}_c$ is Abelian and is a normal subgroup of $\mathcal{G}$. Moreover, $\mathcal{G}/\mathcal{G}_c$ is also Abelian. So $\mathcal{G}$ is a solvable group (which, of course we already knew because the field $\mathbb{F}_5$ is a radical extension of $\mathbb{Q}$). Using the Galois correspondence, we found that corresponding to the series of groups

$$\langle e \rangle \subseteq \mathcal{G}_c \subseteq \mathcal{G}, \tag{6.4.14}$$

there is the series of fields

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{21}) \subseteq \mathbb{F}_5, \tag{6.4.15}$$

where $\mathbb{Q}(\sqrt{21})$ is the fixed field of $\mathcal{G}_c$. In our paper [**17**] we show that in all 27 cases of known exact fiducials for $d > 3$ $\mathcal{G}_c$ is always Abelian and the corresponding fixed

field is always

$$\mathbb{Q}(\sqrt{(d-3)(d+1)}). \tag{6.4.16}$$

We now turn to the problem of calculating the matrices F_g and $\tilde{F}_g$ and vectors q_g introduced earlier. We begin by calculating the matrices $\tilde{F}_g$. From the Eq. (6.3.61) we have

$$g\Big(\frac{\langle\psi|D_{\mathbf{p}}|\psi\rangle}{\langle\psi|\psi\rangle}\Big) = \omega^{\langle \mathbf{q}_g, H_g\mathbf{p}\rangle}\frac{\langle\psi|D_{\tilde{F}\mathbf{p}}|\psi\rangle}{\langle\psi|\psi\rangle}. \tag{6.4.17}$$

Using Eq. (6.3.6) and Magma we found that

$$H_{g_c} = \begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix}$$

$$H_{g_1} = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

$$H_{g_2} = \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$$

$$H_{g_4} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each generator g_k we then find the corresponding $\mathbf{q}_{g_k}, \tilde{F}_{g_k}$ by simply running through all the possible choices (using Magma) until we find one which satisfies Eq. (6.4.17). The result of our calculation is:

$$\mathbf{q}_{g_c} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

$$\mathbf{q}_{g_1} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

$$\mathbf{q}_{g_2} = \begin{pmatrix} 4 \\ 2 \end{pmatrix},$$

$$\mathbf{q}_{g_4} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

and

$$\tilde{F}_{g_c} = \begin{pmatrix} 11 & 0 \\ 0 & 11 \end{pmatrix},$$

$$\tilde{F}_{g_1} = \begin{pmatrix} 1 & 5 \\ 7 & 6 \end{pmatrix},$$

$$\tilde{F}_{g_2} = \begin{pmatrix} 3 & 10 \\ 2 & 1 \end{pmatrix},$$

$$\tilde{F}_{g_4} = \begin{pmatrix} 0 & 11 \\ 1 & 11 \end{pmatrix}.$$

Finally we calculate the matrices F_{g_k} using the Eq. (6.3.63):

$$F_{g_c} = \begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix},$$

$$F_{g_1} = \begin{pmatrix} 6 & 11 \\ 5 & 1 \end{pmatrix},$$

$$F_{g_2} = \begin{pmatrix} 7 & 2 \\ 10 & 3 \end{pmatrix},$$

$$F_{g_4} = \begin{pmatrix} 11 & 1 \\ 11 & 0 \end{pmatrix}.$$

We have shown that for dimension 6

- The group $\mathcal{G}_c$ is an Abelian, normal subgroup of $\mathcal{G}$

- The field $\mathbb{E}_c$ corresponding to the group $\mathcal{G}_c$ under the Galois correspondence is generated by $\sqrt{(d-3)(d+1)} = \sqrt{21}$:

$$\mathbb{E}_c = \mathbb{Q}(\sqrt{(d-3)(d+1)}) \tag{6.4.18}$$

In our paper we show that the same is true for the 26 other known exact fiducials for $d > 3$.

6.5. Conclusion

All the known exact fiducials are expressible in radicals implying that the associated Galois group must be solvable. This suggested to us it would be interesting to examine the structure of the Galois group and its relation to the extended Clifford group in more detail. We first showed that automorphisms in the subgroup $\mathcal{G}_c$ (i.e. automorphisms which commute with complex conjugation) take fiducial vectors to fiducial vectors. We then examined the subgroup $\mathcal{G}_o \subseteq \mathcal{G}_c$ consisting of all automorphisms which take $|\psi\rangle$ to another fiducial vector on the same orbit. For each $g \in \mathcal{G}_o$ there is a vector $\mathbf{q}_g$ and matrix F_g such that

$$g(|\psi\rangle) \doteq D_{\mathbf{q}_g} U_{F_g} |\psi\rangle. \tag{6.5.1}$$

We then showed that if the dimension is not divisible by 3 then subject to certain assumptions it can be assumed that $\mathbf{q}_g = 0$. If the dimension is divisible by 3 then subject to the same assumption $\mathbf{q}_g = \mathbf{0} \mod \frac{d}{3}$. We then examined the action of $\mathcal{G}_o$ on the overlaps. We showed that there is a natural homomorphism of $\mathcal{G}_o$ into the quotient group N_ψ / S_ψ. This means that if $\mathcal{G}_o^0$ is the kernel of the homomorphism then $\mathcal{G}_o / \mathcal{G}_o^0$ is isomorphic to a subgroup of N_ψ / S_ψ. Finally we looked at dimension 6 in more detail. We showed $\mathcal{G}_c$ is an Abelian, normal subgroup of $\mathcal{G}$ and that the field $\mathbb{E}_c$ corresponding to the group $\mathcal{G}_c$ is given by $\mathbb{E}_c = \mathbb{Q}(\sqrt{(d-3)(d+1)})$.

As we discussed earlier the problem of proving SIC existence (or non-existence) is a very hard one. It has not been solved in spite of all efforts since it was first

introduced more than 10 years ago. However, it seems possible that the striking properties of Galois group may contain some important clues.

One of our future interests is to search for other "magic numbers" apart from $\sqrt{(d-3)(d+1)}$. This is particularly exciting in view of a theorem in Galois theory which had no direct use in this thesis. The theorem states that every field can be obtained by using a non-unique single generator. For instance, the same field we generated for dimension 6 using the generators $a, a_1, a_2, a_3, a_4, a_5$ can be generated by a non-unique, single generator s for which $\mathbb{Q}(s) = \mathbb{Q}(a, a_1, a_2, a_3, a_4, a_5)$. It might be interesting to find single generators using magic numbers that could be predicted for an arbitrary dimension d. This would mean that we could write down the field and Galois group without first having have to calculate an exact fiducial. This could not, by itself solve the SIC existence problem. But it might, perhaps, take us closer to a solution.

Part 4

Quantum Information Processes with Spin Chains

CHAPTER 7

Spin chains

Quantum communication is an important area of quantum information. It is concerned with the problem of transferring a quantum state from one place to another. One of its applications is quantum key distribution. For this application, photons (what Bose [**148**] calls flying qubits) are very suitable as they can travel long distances through optical fibres or empty space. However, another area where quantum communication would be important is in connecting the different parts of a quantum computer. In this case the sender and the receiver are separated by a small distance, perhaps only a few nm. For this purpose Bose has proposed [**148**, **149**] the use of spin chains as an alternative to the flying qubit approach. His proposal has attracted much subsequent interest. The idea is to have a 1D array of spins and then to allow the state placed at one end to be propagated down the chain under the interactions between the spins. There are two mainstream ideas for exploiting the spin interactions on a chain. One is to control all the individual couplings, the other is to let the spins interact naturally under their intrinsic moments. The former is known as an *engineered* chain and the latter as an *unengineered* or *unmodulated* chain (the latter is sometimes also referred as a *wire* because of its similarity to a classical wire in the sense that the electrical signals sent through a classical wire are also not controlled). In this thesis we are entirely concerned with unengineered chains. In terms of achieving a high fidelity, of course, engineered chains would be preferable. However the price for that is that it is very difficult, in practice, to have access to individual couplings. For this reason unengineered chains are the subject of continuing interest. In this chapter we review some essential background material. Our discussion is mostly based on Bose [**148**, **149**].

7.1. Basic principles

We assume that the chain consists of spin-1/2 particles. In general one might consider a Hamiltonian of the form

$$-J_{ij}\boldsymbol{\sigma}_i\boldsymbol{\sigma}_j, \tag{7.1.1}$$

which allows for interactions between non-adjacent spins. However we assume that there are only nearest neighbour interactions and that the coupling constant is the same for every pair. So this reduces to

$$-\sum_{i=1}^{n-1} J\boldsymbol{\sigma}^i.\boldsymbol{\sigma}^{i+1} \tag{7.1.2}$$

where n is the length of the chain. Finally we assume that there is a constant magnetic field B acting in the z direction. This gives us the Hamiltonian

$$\mathbf{H} = -J\sum_{i=1}^{n-1} \boldsymbol{\sigma}^i\boldsymbol{\sigma}^{i+1} - \sum_{i=1}^{n} B\sigma_i^z + C. \tag{7.1.3}$$

where B is the magnetic field and C is a constant chosen to make the ground state energy zero (this is just for later convenience). The time evolution operator, describing the propagation down the chain is given by

$$T = e^{-i\mathbf{H}t}, \tag{7.1.4}$$

where t is time.

We now define a basis for the full Hilbert space. Let $|s_1, \ldots, s_n\rangle$ to be the state in which the jth spin is up if $s_j = 1$ and down if $s_j = 0$. The states $|s_1, \ldots, s_n\rangle$ then give us our desired basis. However we do not need to work with the full 2^n dimensional Hilbert space. It is enough to work with an $n + 1$ dimensional subspace defined as follows. Observe that the operator $S = \sum_{j=1}^{n} \boldsymbol{\sigma}_z^j$ commutes with the Hamiltonian. This means that if the state is an eigenstate of S to begin with, it will remain an eigenstate. In other words, the number of spin up sites (what we will call the excitation number) is constant. In this section and in Section

7.2 we confine ourselves to the zero-excitation subspace spanned by a single vector

$$|e_0\rangle = |0\dots0\rangle, \tag{7.1.5}$$

and the single excitation subspace spanned by the vectors

$$\begin{aligned} |e_1\rangle &= |10\dots0\rangle \\ &\dots \\ |e_n\rangle &= |00\dots1\rangle. \end{aligned} \tag{7.1.6}$$

We now consider the process of sending a single qubit down the chain. We assume that Alice at one end of the chain and Bob at the other each have a 2-dimensional ancilla in their possesion. Suppose that Alice's ancilla is in the state

$$|\psi_A\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{7.1.7}$$

Alice puts her qubit on the chain and allows it to propagate down the chain. Some time later Bob takes it off the chain and puts it onto his ancilla. We want to set things up so that the state Bob ends up with is as close as possible to $|\psi_A\rangle$, where we measure degree of closeness by a quantity, the fidelity, defined later. We assume that the state is initially in the state $|e_0\rangle$. There are then three steps we need to consider:

(1) The encoding process, in which Alice puts the qubit onto the chain.
(2) The propagation process, in which the qubit travels down the chain.
(3) The decoding process, in which Bob takes the qubit off the chain.

Encoding process. For the encoding process we assume some once and for all fixed state only involving the first m sites:

$$|\alpha\rangle = \sum_{j=1}^{m} \alpha_j |e_j\rangle. \tag{7.1.8}$$

We assume, for simplicity, that $m = 2$, so

$$|\alpha\rangle = \alpha_1|e_1\rangle + \alpha_2|e_2\rangle. \tag{7.1.9}$$

We then define an encoding unitary which takes

$$|\psi_A\rangle \otimes |e_0\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|e_0\rangle, \tag{7.1.10}$$

(the initial state of ancilla+chain) to

$$|0\rangle \otimes (\cos\frac{\theta}{2}|e_0\rangle + e^{i\phi}\sin\frac{\theta}{2}|\alpha\rangle, \tag{7.1.11}$$

(state of ancilla+chain after the qubit has been transferred to the chain). We can do this by defining

$$|\alpha'\rangle = -\alpha_2|e_1\rangle + \alpha_1|e_2\rangle, \tag{7.1.12}$$

orthogonal to $|\alpha\rangle$. We can then define a unitary U_A which takes

$$|0\rangle \otimes |e_0\rangle \to |0\rangle \otimes |e_0\rangle,$$

$$|1\rangle \otimes |e_0\rangle \to |0\rangle \otimes |\alpha\rangle,$$

$$|0\rangle \otimes |\alpha\rangle \to |1\rangle \otimes e_0\rangle,$$

$$|1\rangle \otimes |\alpha\rangle \to |1\rangle \otimes |\alpha\rangle,$$

and leaves the states $|0\rangle \otimes |\alpha'\rangle$, $|1\rangle \otimes |\alpha'\rangle$ and $|0\rangle \otimes |e_j\rangle, |1\rangle \otimes |e_j\rangle$ for $j = 3, \ldots, n$ unchanged. It is easily seen that U_A is our desired encoding unitary.

Propagation process. The effect of the time evolution operator is to take the state in Eq. (7.1.11) to the state

$$|0\rangle \otimes (\cos\frac{\theta}{2}|e_0\rangle + e^{i\phi}\sin\frac{\theta}{2}T|\alpha\rangle \tag{7.1.13}$$

where we used the fact that $e_0\rangle$ is the ground state so $T|e_0\rangle = |e_0\rangle$.

Decoding process. We assume Bob is equipped with a once and for all fixed state

$$|\beta\rangle = \beta_{n-1}|e_{n-1}\rangle + \beta_n|e_n\rangle. \tag{7.1.14}$$

As with the encoding process, we assume for simplicity that Bob only interacts with the last two spins; the generalization to the case where he interacts with the last m spins is straightforward. We also define a state

$$|\beta'\rangle = -\beta_n|e_{n-1} + \beta_{n-1}|e_n\rangle, \tag{7.1.15}$$

orthogonal to $|\beta\rangle$. By analogy with the encoding unitary U_A we then define unitary U_B which takes

$$|e_0\rangle \otimes |0\rangle \to |e_0\rangle \otimes |0\rangle,$$

$$|e_0\rangle \otimes |1\rangle \to |\beta\rangle \otimes |0\rangle,$$

$$|\beta\rangle \otimes |0\rangle \to |e_0\rangle \otimes |1\rangle,$$

$$|\beta\rangle \otimes |1\rangle \to |\beta\rangle \otimes |1\rangle,$$

and which leaves $|\beta'\rangle \otimes |0\rangle, |\beta'\rangle \otimes |1\rangle$ and $|e_j\rangle \otimes |0\rangle, |e_j\rangle \otimes |1\rangle$ for $j = 1, \ldots, n-2$ unchanged (where now $|0\rangle, |1\rangle$ are the basis states of Bob's ancilla). U_B is our decoding unitary. We assume that Bob's ancilla is initially in the state $|0\rangle$. Applying U_B to the state

$$(\cos\frac{\theta}{2}|e_0\rangle + e^{i\phi}\sin\frac{\theta}{2}T|\alpha\rangle) \otimes |0\rangle, \tag{7.1.16}$$

(where for compactness of notation we have omitted Alice's ancilla). We find the final state of the chain+Bob's ancilla is

$$|\psi_f\rangle = (\cos\frac{\theta}{2}|e_0\rangle + e^{i\phi}\sin\frac{\theta}{2}|\chi\rangle) \otimes |0\rangle + \langle\beta|T|\alpha\rangle e^{i\phi}\sin\frac{\theta}{2}|e_0\rangle \otimes |1\rangle, \tag{7.1.17}$$

where $|\chi\rangle = T|\alpha\rangle - \langle|T|\alpha\rangle|\beta\rangle$.

It can be seen that Bob's qubit will usually be entangled with the chain. So the reduced density matrix ρ_B will usually not be a pure state. To calculate ρ_B it is convenient to write $|\psi_f\rangle$ in the form

$$|\psi_f\rangle = |\chi_1\rangle \otimes |0\rangle + |\chi_2\rangle \otimes\rangle |1\rangle, \tag{7.1.18}$$

where

$$|\chi_1\rangle = \cos\frac{\theta}{2}|e_0\rangle + e^{i\phi}\sin\frac{\theta}{2}|\chi\rangle, \tag{7.1.19}$$

and

$$|\chi_2\rangle = \langle\beta|T|\alpha\rangle e^{i\phi}\sin\frac{\theta}{2}|e_0\rangle. \tag{7.1.20}$$

So

$$|\psi_f\rangle\langle\psi_f| = |\chi_1\rangle\langle\chi_1| \otimes |0\rangle\langle 0| + |\chi_1\rangle\langle\chi_2| \otimes |0\rangle\langle 1| + |\chi_2\rangle\langle\chi_1| \otimes |1\rangle\langle 0| + |\chi_2\rangle\langle\chi_2| \otimes |1\rangle\langle 1|. \tag{7.1.21}$$

Partially tracing out the chain we get

$$\rho_B = \langle\chi_1|\chi_1\rangle|0\rangle\langle 0| + \langle\chi_1|\chi_2\rangle|0\rangle\langle 1| + \langle\chi_2|\chi_1\rangle|1\rangle\langle 0| + \langle\chi_2|\chi_2\rangle|1\rangle\langle 1|. \tag{7.1.22}$$

Average fidelity. As our measure of closeness between Alice's initial state and $|\psi_A\rangle$ and Bob's final state ρ_B we use the fidelity

$$F = \langle\psi_A|\rho_B|\psi_A\rangle. \tag{7.1.23}$$

Using the definitions of $|\psi_A\rangle, |\chi_1\rangle, |\chi_2\rangle$ and defining $\langle\beta|T|\alpha\rangle = \sqrt{p}e^{i\gamma}$ we derive the following expression for the fidelity F.

$$\begin{aligned} F &= \cos^2\frac{\theta}{2}(1 - p\sin^2\frac{\theta}{2}) + \sqrt{p}e^{-i\gamma}\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2} + \sqrt{p}e^{i\gamma}\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2} + p\sin^4\frac{\theta}{2} \\ &= \cos^2\frac{\theta}{2} - p\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2} + \sqrt{p}\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2}(e^{i\phi} + e^{-i\phi}) + p\sin^4\frac{\theta}{2} \end{aligned}$$

$$= \cos^2\frac{\theta}{2} + \sqrt{p}\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2}2\cos\gamma + p(\sin^4\frac{\theta}{2} - \sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2}).$$

We want the average fidelity $\langle F\rangle$:

$$\langle F\rangle = \frac{1}{4\pi}\int F\sin\theta d\theta d\phi.$$

So integrating F term by term we have

$$\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi}\cos^2\frac{\theta}{2}\sin\theta d\theta d\phi = \frac{1}{2}$$
$$\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi}\sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2}\sin\theta d\theta d\phi = \frac{1}{3}$$
$$\frac{1}{4\pi}\int_0^{2\pi}\int_0^{\pi}(\sin^4\frac{\theta}{2} - \sin^2\frac{\theta}{2}\cos^2\frac{\theta}{2})\sin\theta d\theta d\phi = \frac{1}{6}.$$

So the average fidelity is

$$\langle F\rangle = \frac{1}{2} + \frac{1}{3}\cos\gamma\sqrt{p} + \frac{1}{6}p.$$

The maximum fidelity is given when $\gamma = 0$. This can be achieved by fixing the magnetic field B. So we have

$$\langle F\rangle = \frac{1}{2} + \frac{\sqrt{p}}{3} + \frac{p}{6}. \tag{7.1.24}$$

In the next chapter we maximize $p = |\langle\beta|T|\alpha\rangle|^2$.

7.2. Maximizing the average fidelity

7.2.1. Analysis. In the preceding chapter we saw that the average fidelity is given by

$$\langle F\rangle = \frac{1}{2} + \frac{\sqrt{p}}{3} + \frac{p}{6}, \tag{7.2.1}$$

where

$$p = |\langle\beta|T|\alpha\rangle|^2. \tag{7.2.2}$$

The average fidelity, therefore, depends on the states $|\alpha\rangle, |\beta\rangle$ and on the time t at which Bob takes the qubit off the chain (note that the time dependence of $\langle F\rangle$ comes through the time evolution operator T in Eq. (7.2.2)). In this chapter we address the problem of finding the maximum achievable fidelity for a suitable choice of $|\alpha\rangle, |\beta\rangle$ and t. After completing the work described in this chapter we discovered that this question had been previously answered by [**18**]. However, it still seems worth giving our analysis since our method is a little different.

We write T as follows

$$T = \sum_{r,s=1}^{n} T_{rs}|e_r\rangle\langle e_s|. \tag{7.2.3}$$

We find

$$\langle\beta|T|\alpha\rangle = \langle\bar{\beta}|M|\bar{\alpha}\rangle, \tag{7.2.4}$$

where $|\bar{\alpha}\rangle, |\bar{\beta}\rangle$ are the 2-dimensional vectors and M is the matrix given by

$$|\bar{\alpha}\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad |\bar{\beta}\rangle = \begin{pmatrix} \beta_{n-1} \\ \beta_n \end{pmatrix}, \quad M = \begin{pmatrix} T_{n-1,n} & T_{n-2,2} \\ T_{n1} & T_{n2} \end{pmatrix}. \tag{7.2.5}$$

We next observe that by the Schwarz Inequality we have

$$\langle\bar{\beta}|M|\bar{\alpha}\rangle \leq |||\bar{\beta}\rangle||||M|\bar{\alpha}\rangle|| = ||M|\bar{\alpha}\rangle||, \tag{7.2.6}$$

(since $|\bar{\beta}\rangle$ is normalized) where the upper bound is achieved if $|\bar{\beta}\rangle$ is parallel to $M|\bar{\alpha}\rangle$. So

$$\max_{\big|\big||\bar{\beta}\rangle\big|\big|=1} |\langle\bar{\beta}|M|\bar{\alpha}\rangle| = ||M|\bar{\alpha}\rangle|| = \sqrt{\langle\bar{\alpha}|M^\dagger M|\bar{\alpha}\rangle}. \tag{7.2.7}$$

Now let λ_t be the maximum eigenvalue of $M^\dagger M$ so that

$$\langle\bar{\alpha}|M^\dagger M|\bar{\alpha}\rangle \leq \lambda_t \qquad \text{for all normalized } |\bar{\alpha}\rangle, \tag{7.2.8}$$

where we insert the subscript t as a reminder that $M^\dagger M$, and therefore its maximum eigenvalue λ_t, depends on t. Moreover the upper bound is achieved if $|\bar{\alpha}\rangle$ is an eigenvector corresponding to λ_t. So

$$\max_{\big|\big||\langle\bar{\alpha}|\big|\big|,\big|\big||\bar{\beta}\rangle\big|\big|=1} |\langle\bar{\beta}|M|\bar{\alpha}\rangle| = \sqrt{\lambda_t}. \tag{7.2.9}$$

We conclude that the maximum achievable average fidelity for a given time t is

$$\max_{\big|\big||\langle\bar{\alpha}|\big|\big|,\big|\big||\bar{\beta}\rangle\big|\big|=1} \langle F\rangle = \frac{1}{2} + \frac{1}{3}\sqrt{\lambda_t} + \frac{1}{6}\lambda_t. \tag{7.2.10}$$

So the problem of maximizing the average fidelity reduces to finding the maximum of the RHS of Eq. (7.2.10) as t varies. We were not able to tackle this problem analytically. We were however able to tackle it numerically as described in the next section.

Note that although we derived this result on the assumption that $m = 2$, where m is the number of sites introduced in the states $|\alpha\rangle, |\beta\rangle$ (see Eq. (7.1.8) and Eq. (**??**)), this was only for the sake of simplicity. The result remains valid for $m > 2$.

7.2.2. Numerical results. We write the Hamiltonian in the form

$$H = -JH_0 - B\sum_{j=1}^{n} \sigma_z^j, \tag{7.2.11}$$

where

$$H_0 = \sum_{i=1}^{n-1} J\boldsymbol{\sigma}^i.\boldsymbol{\sigma}^{i+1}. \tag{7.2.12}$$

We have

$$\begin{aligned} |\langle\beta|T|\alpha\rangle| &= |\langle\beta|e^{-iHt}|\alpha\rangle| \\ &= |e^{iBt}\langle\beta|e^{iH_0\tilde{t}}|\alpha\rangle| \\ &= |\langle\beta|e^{iH_0\tilde{t}}|\alpha\rangle|, \end{aligned}$$

where $\tilde{t} = Jt$. So there is no loss of generality in taking the time evolution operator to be $T = e^{iH_0\tilde{t}}$ rather than $T = e^{iHt}$. To calculate T we use analytic expressions for the eigenvectors and eigenvalues of H_0 given in [**148**]. Let

$$H_0|\xi\rangle = E_j|\xi_j\rangle, \tag{7.2.13}$$

with $j = 1, \ldots, n$. Then

$$T = \sum_{j=1}^{n} e^{iE_j\tilde{t}}|\xi_j\rangle\langle\xi_j|. \tag{7.2.14}$$

Using this it is straight forward to calculate $M^\dagger M$, and its maximum eigenvalue $\lambda_{\tilde{t}}$ as a function of $\tilde{t}$ using Mathematica. We then used Mathematica to find the maximum value of $\lambda_{\tilde{t}}$ as $\tilde{t}$ goes to zero to $10,000$. We did this for all values of $n \leq 30$ and for $m = 2, 3, 4$ (where m is the number of sites contributing to the states $|\alpha\rangle$ and $|\beta\rangle$).

We tabulate our results in Table 5. It can be seen that the maximum achievable fidelity when $m = 4$ and $n = 30$ is 0.98. So the method is potentially a useful way of communicating quantum information. Of course achieving this in practice might be difficult because we have to take the qubit off the chain at exactly the right time. Also it might be difficult to prepare the states $|\alpha\rangle$ and $|\beta\rangle$ as required. Finally we have assumed only nearest neighbour couplings of the spins. In practice there might be longer range couplings which might significantly change our result. Nevertheless our data are useful as they give us an idea of what is achievable in principle.

Spin No.	$m=2$			$m=3$			$m=4$		
	$\tilde{t}$	p_{max}	$\langle F\rangle$	$\tilde{t}$	p_{max}	$\langle F\rangle$	$\tilde{t}$	p_{max}	$\langle F\rangle$
5	479.02	1.00000	1.00000	-	-	-	-	-	-
6	4572.588	1.00000	1.00000	-	-	-	-	-	-
7	2402.986	0.99992	0.99997	2402.979	1.00000	1.00000	-	-	-
8	2713.618	0.99986	0.99995	3721.22	1.00000	1.00000	-	-	-
9	6237.213	0.91887	0.97267	1904.294	0.99986	0.99995	493.197	1.00000	1.00000
10	4285.142	0.99666	0.99889	3411.520	0.99990	0.99997	3411.512	1.00000	1.00000
11	7698.164	0.99175	0.99725	5179.49	0.99773	0.99924	6131.218	0.99997	0.99999
12	2673.507	0.90996	0.96963	2673.48	0.99832	0.99944	3454.58	0.99960	0.99987
13	4948.996	0.96753	0.98913	4949.012	0.98693	0.99564	8076.42	0.99845	0.99948
14	2961.415	0.96795	0.98927	2537.684	0.99941	0.99980	2537.681	0.99945	0.99981
15	4.125	0.72195	0.90355	7908.177	0.94760	0.98241	6649.59	0.99808	0.99936
16	1912.723	0.94414	0.98125	5664.478	0.98090	0.99362	841.536	0.99659	0.99887
17	2816.947	0.92758	0.97563	2816.347	0.94608	0.98190	4.254	0.98650	0.99549
18	886.025	0.85915	0.95216	886.064	0.94776	0.98247	9520.661	0.99466	0.99822
19	4320.69	0.93798	0.97916	4320.65	0.95688	0.98555	4320.14	0.98097	0.99364
20	3494.027	0.85970	0.95235	5296.718	0.97537	0.99176	5296.7	0.98367	0.99455
21	2198.116	0.74474	0.91178	6399.815	0.92767	0.97566	5.318	0.97398	0.99130
22	9288.65	0.87742	0.95847	9288.692	0.93978	0.97977	5.582	0.97052	0.99014
23	4560.679	0.81969	0.93840	9193.457	0.89933	0.96600	5.846	0.96696	0.98894
24	8441.493	0.80753	0.93413	8441.546	0.88185	0.96000	6.109	0.96331	0.98771
25	1107.084	0.82959	0.94187	7505.908	0.87151	0.95643	6.37	0.95960	0.98646
26	8764.488	0.85267	0.94991	3784.929	0.89828	0.96564	6.635	0.95584	0.98520
27	8545.665	0.73901	0.90972	7.094	0.83307	0.94309	6.897	0.95202	0.98391
28	5140.542	0.0.75543	0.91563	5140.583	0.88387	0.96069	7.158	0.94817	0.98261
29	9084.933	0.72046	0.90301	7.614	0.81791	0.93778	7.42	0.94430	0.98130
30	6760.899	0.75931	0.91701	6760.884	0.85363	0.95024	7.681	0.94040	0.97998

TABLE 5. $\tilde{t} = Jt$ and $p_{max} = \lambda_{\tilde{t}}^2$ is the probability and $\langle F\rangle$ is the average fidelity.

7.3. Achievable transmission rates

The work presented in this section is published in Yadsan-Appleby and Osborne [**19**].

Yet another context where quantum information is manipulated in a Gaussian form is the use of Gaussian wavepackets in the theory of spin chains. There has been much interest in spin chains in recent years as they constitute a kind of "quantum wire" which can be used to connect the different parts of a quantum computer. For long wires it is advantageous to transmit qubits encoded as Gaussian wave-packets of delocalized degrees of freedom, where the profile of the probability amplitude on

the different sites of the chain is a Gaussian distribution. The question then arise as to how the transmission rate depends on the length of the wire. In this section, we show that the rate scales like $n^{-\frac{1}{3}}$ where n is the length of the wire. This means that although the transmission rate falls off with increasing length it only falls off quite slowly. For instance increasing the length by a factor of 1000 only reduces the rate by a factor of 10 [**19**].

7.3.1. Communicating Gaussian wavepackets via spin chains. In Section 7.2 we discussed the problem of maximizing the average fidelity. However, we said nothing about the rate at which qubits can be transmitted down the chain. The most straight forward procedure would be for Alice to put a qubit on the wire and then to wait for Bob to take it off before transmitting another. However this procedure will obviously be slow if the chain is long, since the transmission rate will scale like $\frac{1}{n}$ where n is the length of the chain. We can try to improve on this by having more than one qubit on the chain at any time. The more qubits we have on the chain at once the greater is the transmission rate. On the other hand we cannot have too many qubits on the chain at once since otherwise they will interfere and there will be a reduction in fidelity. The problem is therefore how many qubits can we put on the chain at once and still achieve an acceptable fidelity.

Since the question of transmission rate becomes most important with long chains we will assume a long chain in this section. As we saw in the previous section this means that m, length of the encoding and decoding regions, also needs to be large. We will in fact assume $|\alpha\rangle$ and $|\beta\rangle$ defined in the last chapter are discrete Gaussian wavepackets.

Instead of the Hamiltonian used in the last section, we take the Hamiltonian to be,

$$H = J\sum_{j=1}^{n-1}(\sigma_x^j\sigma_x^{j+1} + \sigma_y^j\sigma_y^{j+1}). \tag{7.3.1}$$

We define

$$\sigma_{\pm}^{j} = \frac{1}{2}(\sigma_x^j \pm i\sigma_y^j). \tag{7.3.2}$$

So we can write the Hamiltonian H as

$$H = J\sum_{j=1}^{n-1}(\sigma_+^j\sigma_-^{j+1} + \sigma_-^j\sigma_+^{j+1}). \tag{7.3.3}$$

This is often called an XY chain.

It is convenient to reformulate this problem by considering a different physical situation with electrons hopping on a regular lattice of n sites [**150**]. This situation is mathematically equivalent to the many spins on a XY chain. The fact that the electrons are fermions means that the number of fermions at a given site is either 0 or 1. Let $|s_1, \ldots, s_n\rangle$ be the state where the number of fermions at site j is s_j. It is in strict analogy to the state $|s_1, \ldots, s_n\rangle$ for the spin chain model where $s_j = 0$ if spin j down and $s_j = 1$ if spin j is up.

Define creation and annihilation operators $a_j^\dagger, a_j$ for each site which satisfy the anti-commutation relation

$$\begin{aligned}\{a_j, a_k^\dagger\} &= \delta_{jk},\\ \{a_j, a_k\} &= \{a_j^\dagger, a_k^\dagger\} = 0.\end{aligned} \tag{7.3.4}$$

$a_j^\dagger$ creates an electron at site j, a_j annihilates an electron at site j. We define $|\Omega\rangle$ to be the vacuum state, in which there are no electrons on the lattice and we assume that $a_j|\Omega\rangle = 0$ for all j. Then

$$|s_1 \ldots s_n\rangle = (a_1^\dagger)^{s_1} \ldots (a_n^\dagger)^{s_n}|\Omega\rangle. \tag{7.3.5}$$

It may be worth comparing this model with the photon creation and annihilation operators. In an n mode system we have

$$[a_j, a_k^\dagger] = \delta_{jk},$$

$$[a_j, a_k] = [a_j^\dagger, a_k^\dagger] = 0. \tag{7.3.6}$$

where $a_j^\dagger$ and a_j are the photon creation and annihilation operators for mode j. In the case of photons we can have arbitrarily many photons in mode j. However for electrons the fact that we have anti-commutation relations instead of CCR means that $(a_j^\dagger)^2$ is zero which in turn means we cannot have more than one electron at site j. This is because electrons are fermions whereas photons are bosons. For our electron model we take the Hamiltonian to be

$$H = J\sum_{j=1}^{n-1} a_j^\dagger a_{j+1} + a_{j+1}^\dagger a_j. \tag{7.3.7}$$

The XY spin chain model and the electron lattice model are physically very different. However from a mathematical point of view they are really the same. To see the essential reason why consider the case when there are only two sites. The spin chain Hamiltonian is then

$$H = J(\sigma_+^1\sigma_-^2 + \sigma_+^2\sigma_-^1). \tag{7.3.8}$$

For the electron lattice model the Hamiltonian is

$$H = J(a_1 a_2^\dagger + a_2 a_1^\dagger). \tag{7.3.9}$$

In both cases one has

$$H|00\rangle = 0,$$

$$H|11\rangle = 0,$$

$$H|01\rangle = |10\rangle,$$

$$H|10\rangle = |01\rangle.$$

So the action of the two Hamiltonians on the basis states is identical. It is easily seen that the same continues to be true when we have n sites instead of only two

sites. However, although the two models are equivalent, it is easier to work with the creation and annihilation operators of the electron model.

We next consider the encoding and decoding states $|\alpha\rangle$ and $|\beta\rangle$.We take m to be an integer of order $n^{\frac{1}{3}}$. This is based on the analysis in [**151**] where it is shown that the spreading of Gaussian wavepacket is independent of number of sites n, if m is chosen to be $n^{\frac{1}{3}}$. Define $|\alpha\rangle$ to be the truncated discrete Gaussian wavepacket

$$|\alpha\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{m} e^{\frac{-(j-\frac{m}{2})^2}{2\Delta^2} + 2\pi i k j} a_j^\dagger |\Omega\rangle, \tag{7.3.10}$$

where $\frac{1}{\sqrt{N}}$ is a normalization constant and where we assume that $1 \ll \Delta \ll m$. It is convenient to define an operator

$$g = \frac{1}{\sqrt{N}} \sum_{j=1}^{m} e^{\frac{-(j-\frac{m}{2})^2}{2\Delta^2} + 2\pi i k j} a_j. \tag{7.3.11}$$

We then have

$$|\alpha\rangle = g^\dagger |\Omega\rangle. \tag{7.3.12}$$

Similarly, we define

$$|\beta\rangle = h^\dagger |\Omega\rangle, \tag{7.3.13}$$

where

$$h = \frac{1}{\sqrt{N}} \sum_{j=n-m+1}^{m} e^{\frac{-\left(j-(n-\frac{m}{2})\right)^2}{2\Delta^2} + 2\pi i k j} a_j. \tag{7.3.14}$$

The fact that $1 \ll \Delta \ll m$ means [**19, 151**] we can take the continuum limit to deduce that the discrete Gaussian wavepacket propagates, to a good approximation, without change of shape at group velocity v:

$$e^{-Ht}|\alpha\rangle = g^\dagger(t)|\Omega\rangle, \tag{7.3.15}$$

where

$$g^\dagger(t) = e^{-iHt} g^\dagger e^{iHt} \approx \frac{1}{\sqrt{N}} \sum_{j=1}^{m} e^{\frac{-(j-\frac{m}{2}-vt)^2}{2\Delta^2} + 2\pi i k j} a_j^\dagger. \tag{7.3.16}$$

We will need an expression for the overlap between two such wavepackets $g^\dagger(t_1)|\Omega\rangle$ and $g^\dagger(t_2)|\Omega\rangle$. We have

$$\langle\Omega|g(t_1)g^\dagger(t_2)|\Omega\rangle = \langle\Omega|\{g(t_1), g^\dagger(t_2)\}|\Omega\rangle = \{g(t_1), g^\dagger(t_2)\}, \tag{7.3.17}$$

where

$$\{g(t_1), g^\dagger(t_2)\} = \frac{1}{\sqrt{N}} \sum_{j=1}^{m} e^{\frac{-(j-\frac{m}{2}-vt_1)^2}{2\Delta^2} - \frac{-(j-\frac{m}{2}-vt_2)^2}{2\Delta^2}}. \tag{7.3.18}$$

Using the continuum limit to approximate this expression by an integral we find

$$\{g(t_1), g^\dagger(t_2)\} \approx e^{-\frac{v^2}{4\Delta^2}(t_1-t_2)^2}. \tag{7.3.19}$$

Notice that when $t_1 = t_2 = t$ this means $\{g(t), g^\dagger(t)\} = 1$ (this is actually exact).

7.3.2. Encoding and decoding. We already discussed encoding and decoding unitaries in chapter 7. However we were there working with the assumption that the number of excitations ≤ 1. We no longer make that assumption so we need to define the unitaries differently. Suppose the chain interacts with an ancilla consisting of a single qubit with basis states $|0\rangle_A, |1\rangle_A$. Let $\sigma_\pm$ be the ladder operators

$$\sigma_\pm = \frac{1}{2}(\sigma_x \pm i\sigma_y), \tag{7.3.20}$$

acting on the ancilla (σ_x, σ_y being the Pauli matrices as usual). So

$$\{\sigma_+, \sigma_-\} = I,$$

$$\sigma_+|0\rangle = |1\rangle,$$

$$\sigma_-|1\rangle = |0\rangle,$$

$$\sigma_+|1\rangle = \sigma_-|0\rangle = 0. \tag{7.3.21}$$

We now consider the interaction Hamiltonian H_I:

$$H_I = \sigma_- g^\dagger + \sigma_+ g, \tag{7.3.22}$$

describing the interaction between the ancilla and the chain. Using the fact that

$$g^2 = (g^\dagger)^2 = \sigma_\pm^2 = 0, \tag{7.3.23}$$

and

$$\{\sigma_+, \sigma_-\} = 1, \tag{7.3.24}$$

$$\{g, g^\dagger\} = 1. \tag{7.3.25}$$

We find

$$\begin{aligned} H_I^2 &= \sigma_-\sigma_+ g^\dagger g + \sigma_+\sigma_- g g^\dagger, \\ H_I^3 &= H_I. \end{aligned} \tag{7.3.26}$$

We now define the encoding unitary U_A to be

$$\begin{aligned} U_A = e^{i\frac{\pi}{2}H_I} &= 1 + \Big(\sum_{n=0}^{\infty} \frac{(i\frac{\pi}{2})^{2n+1}}{(2n+1)!}\Big) H_I + \Big(\sum_{n=1}^{\infty} \frac{(i\frac{\pi}{2})^{2n}}{(2n+1)!}\Big) H_I^2 \\ &= 1 + (\cos\frac{\pi}{2} - 1) H_I^2 + i \sin\frac{\pi}{2} H_I \\ &= I - H_I^2 + i H_I. \end{aligned} \tag{7.3.27}$$

Similarly, we define the decoding unitary U_B to be

$$U_B = e^{i\frac{\pi}{2}H_I'} = I - H_I' + i H_I', \tag{7.3.28}$$

with

$$H_I' = \sigma_- h^\dagger + \sigma_+ h, \tag{7.3.29}$$

where h is the operator defined in Eq. (7.3.14) and $\sigma_\pm$ now refer to Bob's ancilla. We find

$$\begin{aligned} U_A(|0\rangle \otimes |\Omega\rangle) &= |0\rangle \otimes |\Omega\rangle \\ U_A(|1\rangle \otimes |\Omega\rangle) &= i|0\rangle \otimes g^\dagger|\Omega\rangle. \end{aligned} \tag{7.3.30}$$

So if Alice's qubit is initially in the state

$$|\psi_A\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{7.3.31}$$

After the action of U_A we would like the state of the combined system (chain and ancilla) to be

$$\cos\frac{\theta}{2}|\Omega\rangle + e^{i\phi}\sin\frac{\theta}{2}g^\dagger|\Omega\rangle. \tag{7.3.32}$$

However, in fact, we have

$$U_A(|\psi_A\rangle \otimes |\Omega\rangle) = |0\rangle \otimes (\cos\frac{\theta}{2}|\Omega\rangle + ie^{i\phi}\sin\frac{\theta}{2}g^\dagger|\Omega\rangle), \tag{7.3.33}$$

which has an additional i. We fix this problem by applying the unitary matrix $\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$ to $|\psi_A\rangle$ before applying U_A. We will ignore this complication from now on.

If we adopt the same procedure described in chapter 7, Bob and Alice now wait for the center of wavepacket to propagate from the position $\frac{m}{2}$ to $n - \frac{m}{2}$. This will take time $t = \frac{n-m}{v}$ where v is the group velocity. Bob then applies the decoding unitary U_B. For the reasons explained in [**151**] this will give us high fidelity if $1 \ll \Delta \ll m$. We now want to consider a situation where Alice does not wait

for Bob to take his first qubit off the chain before putting another one on, as this should give us as a higher transmission rate.

7.3.3. Putting many qubits on the chain. Suppose Alice puts qubits on the chain at the time intervals of τ, without waiting for Bob to take them off. From Eq. (7.3.19) we get

$$\{g(r\tau), g^\dagger(s\tau)\} \approx e^{-\frac{(r-s)^2 v^2 \tau^2}{4\Delta^2}}. \tag{7.3.34}$$

This is non-zero. Suppose, to begin with, that it were in fact zero when $r \neq s$. Then it can be seen that after Alice has put M qubits on the chain the state of the first M ancilla+chain is

$$|0\rangle \otimes \cdots \otimes |0\rangle \otimes \big(\cos\frac{\theta}{2} + e^{i\phi}\sin\frac{\theta}{2} g^\dagger(M\tau)\big) \ldots \big(\cos\frac{\theta}{2} + e^{i\phi}\sin\frac{\theta}{2} g^\dagger(\tau)\big)|\Omega\rangle. \tag{7.3.35}$$

It is straightforward (though tedious) to confirm that when Bob takes the qubits off the chain he achieves the same fidelity that he would achieve if there was only ever one qubit on the chain. In short there is no interference between the qubits. The trouble is, of course, that $\{g(r\tau), g^\dagger(s\tau)\} \neq 0$, and so we do get interference. We find that the state of the chain with M qubits on it is the state given in Eq. (7.3.35) together with a correction term. The problem is to put a bound to the correction term.

To simplify the working we confine ourselves to the case where Alice sends a sequence of states all either $|0\rangle$ or $|1\rangle$. One can recover the general case by constructing the appropriate superposition. If Alice sends all $|1\rangle$'s then, on the (wrong!) assumption that $\{g(r\tau), g^\dagger(s\tau)\} = 0$ the state of the chain after M qubits have been added will be

$$g^\dagger(M\tau) \ldots g^\dagger(\tau)|\Omega\rangle. \tag{7.3.36}$$

If she sends $|0\rangle$'s as well as $|1\rangle$'s the state will be similar to this except that some of the $g^\dagger$'s will be missing. We therefore anticipate that the interference problem

is worst when Alice sends all $|1\rangle$'s, as this is when the most Gaussian wavepackets are packed on to the chain. We therefore focus on the case where Alice sends all $|1\rangle$'s.

We define

$$\epsilon = \{g(0), g^\dagger(\tau)\} \approx e^{-\frac{v^2\tau^2}{4\Delta^2}}, \tag{7.3.37}$$

so

$$\{g(r\tau), g^\dagger(s\tau)\} \approx \epsilon^{(r-s)^2}. \tag{7.3.38}$$

We now build up the state sequentially. Initially the state of the combined system of Alice's M ancilla and the chain is

$$|1\dots1\rangle \otimes |\Omega\rangle, \tag{7.3.39}$$

where the first factor is the state of the first M ancilla. After swapping the first qubit onto the chain and allowing it to evolve for time τ the state is

$$|1\dots0\rangle \otimes ig^\dagger(\tau)|\Omega\rangle. \tag{7.3.40}$$

After swapping the second qubit onto the chain and allowing it to evolve for a further time τ the state is

$$i^2|1\dots100\rangle \otimes g^\dagger(\tau)g^\dagger(2\tau)|\Omega\rangle + i\epsilon|1\dots110\rangle \otimes g^\dagger(\tau)|\Omega\rangle. \tag{7.3.41}$$

As we swap more and more qubit the state gets more and more complicated. However we do not need to give its detailed form. It is enough to observe that after M qubits have been swapped in we will have a leading term of the form

$$|0\dots0\rangle \otimes ig^\dagger(\tau)\dots ig^\dagger(M\tau)|\Omega\rangle, \tag{7.3.42}$$

and a series of additional terms of the form

$$\epsilon^r |s_1 \dots s_M\rangle \otimes ig^\dagger(j_1\tau) \dots ig^\dagger(j_l\tau)|\Omega\rangle, \tag{7.3.43}$$

such that $r \geq 1$, and such that in the ancilla state $|s_1 \dots s_M\rangle$ the s_j are not all zero. This means that we can write the state in the form

$$|\psi\rangle = |P\rangle + |E\rangle, \tag{7.3.44}$$

where

$$|P\rangle = |0 \dots 0\rangle \otimes ig^\dagger(\tau) \dots ig^\dagger(M\tau)|\Omega, \tag{7.3.45}$$

and $|E\rangle$ is an error term which is order ϵ and orthogonal to $|P\rangle$. The problem now is to put a bound on the error term.

7.3.4. Bounding the error term. We state our result in the form of a theorem:

THEOREM 12. *For small ϵ,*

$$\langle E|E\rangle \leq (M-1)\epsilon^2. \tag{7.3.46}$$

PROOF. The fact that $|\psi\rangle$ is normalized and $|P\rangle$ and $|E\rangle$ are orthogonal means that

$$\begin{aligned} 1 &= \langle\psi|\psi\rangle = \langle P|P\rangle + \langle E|E\rangle, \\ \langle E|E\rangle &= 1 - \langle P|P\rangle. \end{aligned} \tag{7.3.47}$$

This is a nice result because it means if we are only interested in the norm of the state $|E\rangle$ we do not need to pay any attention to its detailed structure (which is very complicated), instead we can just calculate it from the norm of $|P\rangle$. To calculate $\langle P|P\rangle$ consider first the case when $M = 2$. We have

$$\langle P|P\rangle = \langle\Omega|g(2\tau)g(\tau)g^\dagger(\tau)g^\dagger(2\tau)|\Omega\rangle$$

$$= \{g(\tau), g^\dagger(\tau)\}\{g(2\tau), g^\dagger(2\tau)\} - \{g(2\tau), g^\dagger(\tau)\}\{g(\tau), g^\dagger(2\tau)\}$$
$$= 1 - \epsilon^2.$$

When $M = 3$ we have

$$\begin{aligned}\langle P|P\rangle &= \langle\Omega|g(3\tau)g(2\tau)g(\tau)g^\dagger(\tau)g^\dagger(2\tau)g^\dagger(3\tau)|\Omega\rangle \\ &= \{g(\tau), g^\dagger(\tau)\}\{g(2\tau), g^\dagger(2\tau)\}\{g(3\tau), g^\dagger(3\tau)\} \\ &\qquad - \{g(2\tau), g^\dagger(\tau)\}\{g(\tau), g^\dagger(2\tau)\}\{g(3\tau), g^\dagger(3\tau)\} + 6\text{more terms} \\ &= 1 - 2\epsilon^2 + 2\epsilon^6 - \epsilon^8.\end{aligned}$$

These two calculations are examples of Wick's theorem [**152**]. The theorem states that for arbitrary M

$$\begin{aligned}\langle P|P\rangle &= \langle\Omega|g(M\tau)\dots g(\tau)g^\dagger(\tau)\dots g^\dagger(M\tau)|\Omega\rangle \\ &= \sum_\sigma s_\sigma \{g(\tau), g^\dagger(\sigma_1\tau)\}\{g(2\tau), g^\dagger(\sigma_2\tau)\}\dots\{g(M\tau), g^\dagger(\sigma_M\tau)\} \\ &= \sum_\sigma s_\sigma \prod_{\sigma=1}^{M} \epsilon^{(r-\sigma_r)^2}, \end{aligned} \tag{7.3.48}$$

where the sum over all permutations σ of the integers $1, \dots, M$ and s_σ is the sign of the permutation ($s_\sigma = 1$ if σ is even and $s_\sigma = -1$ if σ is odd). In other words

$$\langle P|P\rangle = \det L, \tag{7.3.49}$$

where

$$L = \begin{pmatrix} 1 & \epsilon & \epsilon^4 & \dots & \epsilon^{(M-1)^2} \\ \epsilon & 1 & \epsilon & \dots & \epsilon^{(M-2)^2} \\ \epsilon^4 & \epsilon & 1 & \dots & \epsilon^{(M-3)^2} \\ \vdots & \vdots & \vdots & & \vdots \\ \epsilon^{(M-1)^2} & \epsilon^{(M-2)^2} & \epsilon^{(M-3)^2} & \dots & 1 \end{pmatrix}. \tag{7.3.50}$$

So

$$\langle E|E\rangle = 1 - \det L. \tag{7.3.51}$$

Define

$$f(\epsilon) = \frac{1 - \det L}{\epsilon^2}. \tag{7.3.52}$$

We will show that $f(\epsilon) \leq M-1$ for sufficiently small ϵ. The only way of generating an ϵ^2 term when calculating $\det L$ is by multiplying two elements $= \epsilon$ with $M-2$ elements $= 1$. So the ϵ^2 terms are all of the form

$$-(L_{i,i+1}L_{i+1,i})(\prod_{j\neq i,i+1}^{M} L_{jj}),$$

the minus sign is because $i \iff i+1$ is a negative permutation. It is easy to see that number of such terms is $M-1$. Similarly all ϵ^4 terms are of the form

$$(L_{i,i+1}L_{i+1,i}L_{j,j+1}L_{j+1,j})(\prod_{k=i,i+1,j,j+1} L_{kk}).$$

The number of such terms is

$$1 + 2 + \cdots + (M-3) = \frac{1}{2}(M-3)(M-2).$$

It is easily seen that there are no ϵ or ϵ^3 terms in $\det L$. So to order ϵ^4

$$\det L = 1 - (M-1)\epsilon^2 + \frac{1}{2}(M-3)(M-2)\epsilon^4 + O(\epsilon^6)$$

Then

$$f(\epsilon) = (M-1) - \frac{(M-3)(M-2)}{2}\epsilon^2 + O(\epsilon^4)$$

Since $f'(0) = 0$ and $f''(0) < 0$ we have a maximum at $\epsilon = 0$. So in the vicinity of $\epsilon = 0$

$$f(\epsilon) \leq M-1$$

□

7.3.5. Transmission rate. The transmission rate is $R = \frac{1}{\tau}$. The spacing between the adjacent wavepackets is $v\tau$. So the number of wavepackets on the chain at any given time is $M = \frac{n}{v\tau} = \frac{nR}{v}$. For the sake of example suppose $\Delta = \kappa n^{\frac{1}{3}}$ and $M = n^{\frac{2}{3}}$ for some constant κ to be fixed later. The spacing between the qubits is $v\tau$, so

$$v\tau = \frac{n}{M} = n^{\frac{1}{3}} \tag{7.3.53}$$

and

$$\epsilon = e^{-\frac{(v\tau)^2}{4\Delta^2}} = e^{-\frac{1}{4\kappa^2}} \tag{7.3.54}$$

We now choose κ small enough for Theorem 12 to apply. For the sake of example suppose that Theorem 12 is true when $\kappa = 0.1$ and $\epsilon \approx 10^{-11}$. Then

$$\langle E|E\rangle \leq (M-1)\epsilon^2 < n^{\frac{2}{3}} e^{-50} \approx (10^{-33}n)^{\frac{2}{3}}. \tag{7.3.55}$$

So the error term will be negligible for $n \ll 10^{33}$—a condition which will certainly be satisfied in every physically realistic situation (our spin chains aren't cosmic). The fidelity therefore will be high. From Eq. (7.3.53) we see that the transmission rate R is given by

$$R = \frac{1}{\tau} = vn^{-\frac{1}{3}}. \tag{7.3.56}$$

If it should happen that Theorem 12 is not satisfied for $\kappa = 0.1$ we simply choose a smaller value of κ. This will not change our conclusion in that we get a high fidelity with a transmission rate that scales like $n^{-\frac{1}{3}}$.

We see from this analysis that making the spin chain longer reduces the achievable transmission rate. However, the rate decreases very slowly. For instance making the chain 1000 times longer only reduces the rate by a factor of 10.

7.4. Conclusion

In this chapter we have considered quantum communication with unmodulated spin chains. We began by reviewing the encoding and decoding processes by which information is put on the chain at one end and taken off at the other end. We also described how one calculates the fidelity. We then went on to address the question what is the maximal fidelity in Section 7.2. It turned out that this question had already been answered in [**18**]. However, our method is different from theirs.

In Section 7.3 we turned our attention to a different situation where the state of the chain was approximated as a Gaussian wavepacket. On the basis of this description we addressed the question as to what is the achievable transmission rate. We showed that we get a high fidelity with a transmission rate that scales like $n^{-\frac{1}{3}}$. Thus, although the rate decrease with increasing chain length, it decreases quite slowly. This work has been published [**19**].

Part 5

Summary

CHAPTER 8

Summary

We have explored a wide range of topics and we made a few discoveries which we hope may prove a moderately useful contribution to the subject.

Firstly, we have investigated a question concerning the CV quantum memories. Quantum memories are likely to play a very important role in future quantum computers. On a shorter time scale they are likely to make possible the implementation of a number of quantum information protocols. For instance in quantum communication quantum repeaters assisted by good quantum memories may solve the problem of entanglement distribution. Recently squeezed and entangled states of light have been successfully stored in quantum memories. In Sections 5.3.1 and 5.3.2 we addressed the question when it is best to store squeezed states and only entangle them later, and when it is best to store the states already entangled. We gave an answer to this question in the case of ideal memories. In the case of noisy memories we gave for a certain class of parameter choice a simple analytical expression which enables one to determine cases where it is better to entangle after storage. It would be interesting to develop this approach and give a criterion for when it is definitely better to entangle before storage. It would also be interesting to extend our results to other regions of parameter space.

Secondly, we investigated the SIC-POVMs. We began by showing that SIC fiducials can be regarded as discrete analogs of coherent states in a CV system. We then turned to an examination of Galois automorphisms of a SIC-POVM. This work was motivated by the observation that with the exception of dimension 3 the components of SIC fiducials turn out to be expressible in radicals in every case where an exact fiducial has been calculated. This tells us that the associated Galois

group must be solvable. We set out to see if there is anything more one can say about the Galois group. We identified a subgroup $\mathcal{G}_c$, the automorphisms of which take SIC fiducials to SIC fiducials. We then focused on a subgroup of $\mathcal{G}_c$, $\mathcal{G}_o$ for which the automorphisms take the SIC fiducial onto another SIC fiducial on the same orbit of the extended Clifford group. For each automorphism in this subgroup one can associate a unitary or anti-unitary in the extended Clifford group. We also examined the effect of the Galois automorphisms on the overlaps $\langle\psi|D_{\mathbf{p}}|\psi\rangle$. We used this to show that there is a homomorphism of $\mathcal{G}_o$ into the quotient group N_ψ/S_ψ. Finally we made a detailed study of dimension 6 case. We found that for this case $\mathcal{G}_c$ is Abelian and that the field corresponding to $\mathcal{G}_c$under the Galois corespondence is $Q(\sqrt{(d-3)(d+1)})$. It turns out that the same is true for every other exact solution for $d > 3$ (although we did not show this here).

Finally, we have addressed the question of transmission rate on a spin chain. We described a protocol whereby Alice and Bob, using a long XY spin chain can communicate quantum information with arbitrarily high fidelity at a rate of $n^{-\frac{1}{3}}$ qubits per unit time. The rate we achieve here for an unengineered chain is much greater than the previously described rate by [**153**] for a specially engineered chain.

APPENDIX A

Fiducial Vector in Dimension 6

The exact fiducial vector for dimension 6 can be found in [**142**]. However, we calculated the exact fiducial vector $|\psi\rangle$ ourselves and used it for our calculations in this thesis. We calculated the following expression for $|\psi\rangle$:

$$|\psi\rangle = \psi_0|e_0\rangle + \psi_{1p}|e_1\rangle + \psi_{2p}|e_2\rangle. \tag{A.0.1}$$

where

$$\psi_0 = \sqrt{\frac{1}{14}(7-\sqrt{21})}, \tag{A.0.2}$$

$$\psi_{1p} = \frac{\sqrt{7+\sqrt{21}+\sqrt{14(-3+\sqrt{21})}}\Big(-2(-7+\sqrt{21})+(1-i\sqrt{3})\sqrt{14(-3+\sqrt{21})}\Big)^{\frac{1}{3}}}{2\times 14^{\frac{2}{3}}(1+\sqrt{-9+2\sqrt{21}})^{\frac{1}{6}}}, \tag{A.0.3}$$

$$\psi_{2p} = \frac{1}{2\times 2^{\frac{2}{3}}}\sqrt{1+\sqrt{\frac{3}{7}}-\sqrt{\frac{2}{7}(-3+\sqrt{21}}}\Big(\sqrt{23-3\sqrt{21}-3\sqrt{6(-3+\sqrt{21})}} + i\sqrt{3(3+\sqrt{21}+\sqrt{6(-3+\sqrt{21})})}\Big)^{\frac{1}{3}}, \tag{A.0.4}$$

$$|e_0\rangle = \begin{pmatrix} e_{01} \\ e_{02} \\ e_{03} \\ e_{04} \\ e_{03} \\ e_{02} \end{pmatrix}, |e_1\rangle = \begin{pmatrix} e_{11} \\ e_{12} \\ e_{13} \\ e_{12} \\ e_{11} \\ e_{14} \end{pmatrix}, |e_2\rangle = \begin{pmatrix} e_{11} \\ e_{14} \\ e_{11} \\ e_{12} \\ e_{13} \\ e_{12} \end{pmatrix},$$

with

$$e_{01} = \frac{1}{3}\sqrt{\frac{1}{2}(3+\sqrt{3})}, \tag{A.0.5}$$

$$e_{02} = -\frac{\frac{1}{6}(1+i)(3i+\sqrt{3})}{\sqrt{2(3+\sqrt{3})}}, \tag{A.0.6}$$

$$e_{03} = -\frac{\frac{1}{6}(1+i)(3+(2+i)\sqrt{3})}{\sqrt{2(3+\sqrt{3})}}, \tag{A.0.7}$$

$$e_{04} = \frac{1+i}{\sqrt{6(3+\sqrt{3})}}, \tag{A.0.8}$$

$$e_{11} = \frac{1}{2}\sqrt{\frac{1}{3}(3+\sqrt{3})} - \frac{\sqrt{3+\sqrt{3}}}{6}, \tag{A.0.9}$$

$$e_{12} = -\frac{1}{6}(1+i)\sqrt{3+\sqrt{3}}, \tag{A.0.10}$$

$$e_{13} = -\frac{1}{4}\sqrt{\frac{1}{3}(3+\sqrt{3})} + \frac{\sqrt{3+\sqrt{3}}}{12} + i\Big(-\frac{1}{4}\sqrt{\frac{1}{3}(3+\sqrt{3})} + \frac{\sqrt{3+\sqrt{3}}}{4}\Big), \tag{A.0.11}$$

$$e_{14} = \frac{1}{4}\sqrt{\frac{1}{3}(3+\sqrt{3})} + \frac{\sqrt{3+\sqrt{3}}}{12} + i\Big(-\frac{1}{4}\sqrt{\frac{1}{3}(3+\sqrt{3})} + \frac{\sqrt{3+\sqrt{3}}}{12}\Big). \tag{A.0.12}$$

We then used the components of the first column of the projector $\Pi = |\psi\rangle\langle\psi|$ to generate the field $\mathbb{F}_5$ described in chapter 6.4. The reason for using the unnormalized fiducial vector rather than the normalized one was that the field that contains the components of the normalized fiducial is bigger than $\mathbb{F}_5$ and we wanted to reduce the size of the field. Let the first column of Π be

$$\Pi = \begin{pmatrix} \Pi_{11} \\ \Pi_{21} \\ \Pi_{31} \\ \Pi_{41} \\ \Pi_{51} \\ \Pi_{61} \end{pmatrix}. \tag{A.0.13}$$

Then the components of Π in terms of $\mathbb{F}_5$ generators a_1, a_2, a_3, a_4, a_5 are given by

$$\Pi_{11} = \frac{1}{6048}\{(756 + 36a + 84a_1 - 60aa_1 - 168a_1a_2 + 120aa_1a_2 - 252a_3 + 36aa_3 + 252a_1a_3 - 36aa_1a_3$$

$$
\begin{aligned}
&- 504a_1a_2a_3 + 72aa_1a_2a_3 + 42a_1a_4 + 2aa_1a_4 - 84a_1a_2a_4 + 8aa_1a_2a_4 + 42a_3a_4 \\
&- 6aa_3a_4 + 168a_2a_3a_4 - 36aa_2a_3a_4 + 7a_1a_4^2 + aa_1a_4^2 + 7a_1a_2a_4^2 - 5aa_1a_2a_4^2 \\
&- 21a_3a_4^2 + 5aa_3a_4^2 + 63a_2a_3a_4^2 - 13aa_2a_3a_4^2)\}
\end{aligned}
$$

$$
\begin{aligned}
\Pi_{21} = \frac{1}{6048}\{&(168 + 24a - 168a_1 - 24aa_1 - 84a_2 - 12aa_2 + 84a_1a_2 + 12aa_1a_2 + 504a_3 - 120aa_3 \\
&+ 504a_1a_3 - 120aa_1a_3 - 252a_2a_3 + 60aa_2a_3 - 252a_1a_2a_3 + 60aa_1a_2a_3 - 42a_4 \\
&- 2aa_4 + 42a_1a_4 - 10aa_1a_4 + 84a_2a_4 - 8aa_2a_4 + 42a_1a_2a_4 + 2aa_1a_2a_4 \\
&+ 210a_3a_4 - 42aa_3a_4 - 42a_1a_3a_4 + 6aa_1a_3a_4 - 42a_2a_3a_4 + 6aa_2a_3a_4 \\
&- 168a_1a_2a_3a_4 + 36aa_1a_2a_3a_4 + 14a_4^2 - 4aa_4^2 + 7a_1a_4^2 + aa_1a_4^2 \\
&- 7a_2a_4^2 - aa_2a_4^2 + 7a_1a_2a_4^2 - 5aa_1a_2a_4^2 - 21a_3a_4^2 + 5aa_3a_4^2 \\
&- 42a_1a_3a_4^2 + 8aa_1a_3a_4^2 + 63a_2a_3a_4^2 - 13aa_2a_3a_4^2 \\
&- 21a_1a_2a_3a_4^2 + 5aa_1a_2a_3a_4^2)\}
\end{aligned}
$$

$$
\begin{aligned}
\Pi_{31} = \frac{1}{6048}\{&(-672a_1 + 48aa_1 + 72aa_2 + 336a_1a_2 - 24aa_1a_2 - 504a_3 + 120aa_3 + 504a_1a_3 - 72aa_1a_3 \\
&- 24aa_2a_3 - 1008a_1a_2a_3 + 216aa_1a_2a_3 + 168a_1a_4 - 16aa_1a_4 - 84a_1a_2a_4 + 20aa_1a_2a_4 \\
&+ 7a_1a_4^2 - 5aa_1a_4^2 - 14a_1a_2a_4^2 + 4aa_1a_2a_4^2 + 63a_3a_4^2 - 13aa_3a_4^2 - 42a_2a_3a_4^2 + 8aa_2a_3a_4^2)\}
\end{aligned}
$$

$$
\begin{aligned}
\Pi_{41} = \frac{1}{6048}\{&(-84 + 60a + 84a_1 - 60aa_1 + 168a_2 - 120aa_2 - 168a_1a_2 + 120aa_1a_2 - 252a_3 + 36aa_3 \\
&- 252a_1a_3 + 36aa_1a_3 - 42a_4 + 10aa_4 - 84a_1a_4 + 8aa_1a_4 - 42a_2a_4 - 2aa_2a_4 + 42a_1a_2a_4 \\
&- 10aa_1a_2a_4 + 168a_3a_4 - 36aa_3a_4 - 210a_1a_3a_4 + 42aa_1a_3a_4 - 210a_2a_3a_4 + 42aa_2a_3a_4 \\
&+ 42a_1a_2a_3a_4 - 6aa_1a_2a_3a_4 - 7a_4^2 + 5aa_4^2 - 14a_1a_4^2 + 4aa_1a_4^2 + 14a_2a_4^2 - 4aa_2a_4^2 + 7a_1a_2a_4^2 \\
&+ aa_1a_2a_4^2 - 42a_3a_4^2 + 8aa_3a_4^2 + 63a_1a_3a_4^2 - 13aa_1a_3a_4^2 - 21a_2a_3a_4^2 + 5aa_2a_3a_4^2 - 42a_1a_2a_3a_4^2 \\
&+ 8aa_1a_2a_3a_4^2)\}
\end{aligned}
$$

$$
\begin{aligned}
\Pi_{51} = \frac{1}{6048}\{&(-168a_1 - 24aa_1 - 756a_2 + 180aa_2 + 84a_1a_2 + 12aa_1a_2 + 504a_3 - 120aa_3 - 252a_2a_3 + 60aa_2a_3 \\
&+ 756a_1a_2a_3 - 180aa_1a_2a_3 - 84a_1a_4 + 8aa_1a_4 + 42a_1a_2a_4 - 10aa_1a_2a_4 - 168a_3a_4 + 36aa_3a_4 \\
&+ 210a_2a_3a_4 - 42aa_2a_3a_4 + 7a_1a_4^2 - 5aa_1a_4^2 - 14a_1a_2a_4^2 + 4aa_1a_2a_4^2 + 63a_3a_4^2 - 13aa_3a_4^2
\end{aligned}
$$

$$- 42a_2a_3a_4^2 + 8aa_2a_3a_4^2)\}$$

$$\Pi_{61} = \frac{1}{6048}\{(672 - 48a - 672a_1 + 48aa_1 - 336a_2 + 24aa_2 + 336a_1a_2 - 24aa_1a_2 - 504a_3 + 120aa_3$$

$$- 504a_1a_3 + 120aa_1a_3 - 24aa_2a_3 - 24aa_1a_2a_3 + 84a_4 + 4aa_4 - 84a_1a_4 + 20aa_1a_4 - 168a_2a_4$$

$$+ 16aa_2a_4 - 84a_1a_2a_4 - 4aa_1a_2a_4 + 14a_4^2 - 4aa_4^2 + 7a_1a_4^2 + aa_1a_4^2 - 7a_2a_4^2$$

$$- aa_2a_4^2 + 7a_1a_2a_4^2 - 5aa_1a_2a_4^2 - 21a_3a_4^2 + 5aa_3a_4^2 - 42a_1a_3a_4^2 + 8aa_1a_3a_4^2 + 63a_2a_3a_4^2$$

$$- 13aa_2a_3a_4^2 - 21a_1a_2a_3a_4^2 + 5aa_1a_2a_3a_4^2)\}$$

List of Publications

1. Hulya Yadsan-Appleby, A. Serafini, *Would one rather store squeezing or entanglement in continuous variable quantum memories?*, Phys. Lett. A Volume **375**, Issue 18, Pages 1864-1869 (2011)

2. Hulya Yadsan-Appleby, T. Osborne, *Achievable Qubit Rates for Quantum Information Wires* Phys. Rev. A, **85**, 012310, (2012)

3. D.M. Appleby, Hulya Yadsan-Appleby, Gerhard Zauner, *Galois Automorphisms of a Symmetric Measurement*, arXiv:1209.1813 (2012). Accepted for publication in Quantum Information and Computation.

Bibliography

[1] C. A. Fuchs, Quantum Foundations in the Light of Quantum Information, in Decoherence and its Implications in Quantum Computation and Information Transfer: Proceedings of the NATO Advanced Research Workshop, Mykonos Greece, June 2530, 2000, edited by A. Gonis and P. E. A. Turchi (IOS Press, Amsterdam, 2001), pp. 3882. Also posted at quant-ph/0106166.

[2] J. T. Cushing, A. Fine, and S. Goldstein, editors, *Bohmian Mechanics and Quantum Theory: An Appraisal*, (Kluwer, Dordrecht, 1996).

[3] R. B. Griffiths and R. Omn'es, *Consistent Histories and QuantumMeasurements*,Phys. Today **52** (8), 2631 (1999).

[4] J. G. Cramer, *An Overview of the Transactional Interpretation of Quantum Mechanics*, Int. J. Theor. Phys. **27**, 227236 (1988).

[5] G. C. Ghirardi and P. Pearle, *Dynamical Reduction Theories: Changing Quantum Theory so the Statevector Represents Reality*, PSA 1990: Proceedings of the Biennial Meeting of the Philosophy of Science Association, **Vol. I**, edited by A. Fine, M. Forbes, and L. Wessels (Philosophy of Science Association, East Lansing, MI, 1990), pp. 1934.

[6] W. H. Zurek, *Decoherence, Einselection and the Existential Interpretation (The Rough Guide)*, Phil. Trans. R. Soc. Lond. A **356**, 17931821 (1998).

[7] P. Grangier, *Contextual Objectivity: A Realistic Interpretation of Quantum Mechanics*, quant-ph/ 0012122.

[8] P. Grangier, *Reconstructing the Formalism of Quantum Mechanics in the Contextual Objectivity Point of View*, quant-ph/0111154.

[9] D. Deutsch, *The Fabric of Reality: The Science of Parallel Universesand its Implications*, (Allen Lane, New York, 1997).

[10] L. Vaidman, *The Many-Worlds Interpretation of QuantumMechanics*, in The Stanford Encyclopedia of Philosophy (Summer 2002 Edition), edited by E. N. Zalta (Stanford University, Stanford, CA, 2002). Available at http:// plato.stanford.edu/entries/qm-manyworlds/.

[11] James Gleick, *The Information*, Fourth Estate, London, 2011.

[12] R. P. Feynman *Simulating physics with computers*, Int. J. Theor. Phys. **21**, pg 467 (1982)

[13] D. Deutsch Proceedings of the Royal Society of London. Series A, **Vol. 400**, No. 1818 (Jul. 8, 1985), pp. 97-117

[14] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public key distribution and coin tossing*, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984)

[15] C. A. Fuchs (2010), *QBism, the Perimeter of Quantum Bayesianism*, eprint arXiv:1003.5209.

[16] C. A. Fuchs and R. Schack (2011), *A quantum-Bayesian route to quantum state space*, Found. Phys.**41**, 345–356.

[17] D.M. Appleby, Hulya Yadsan-Appleby, Gerhard Zauner, *Galois Automorphisms of a Symmetric Measurement*, arXiv:1209.1813. Accepted for publication in Quantum Information and Computation.

[18] Henry L. Haselgrove, *Optimal state encoding for quantum walks and quantum communication over spin systems*, Phys. Rev. A **72**, 062326 (2005)

[19] Hulya Yadsan-Appleby, T. Osborne, *Achievable Qubit Rates for Quantum Information Wires* Phys. Rev. A, **85**, 012310, (2012).

[20] Hermann Weyl, *The Theory of Groups and Quantum Mechanics*, Dover (1950).

[21] K. Husimi, *Some Formal Properties of the Density Matrix* Proc. Phys. Math. Soc. Jpn. **22**, 264 (1940).

[22] D. M. Appleby, *Quantum Mechanics on Phase Space*, Ph.D Thesis, Queen Mary and Westfield College (1997).

[23] D. M. Appleby, *Optimal Joint Measurements of Position and Momentum*, Int.J.Theor.Phys. **38**, 807-825, (1999) .

[24] D. M. Appleby, *The Error Principle*, Int.J.Theor.Phys. **37**, 2557-2572, (1998).

[25] John Williamson, *On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems*,American Journal of Mathematics, Vol. **58**, No.1 (Jan.,1936),pp.141-163.

[26] A. Serafini, F. Illuminati and S. De Siena, J.Phys.B:At.Mol.Opt.Phys **37** (2004).

[27] Alessio Serafini, *Ph.D. Thesis*, University of Solerno, Italy, (2004).

[28] D. Gross (2006), *Hudson's theorem for finite dimensional quantum systems*, J. Math. Phys., **47**, 122107.

[29] M.A. Nielsen, M.J. Bremner, J.L. Dodd, A.M. Childs and C.M. Dawson, *Universal simulation of Hamiltonian dynamics for qudits*, Phys. Rev. A **66**, 022317 (2002)

[30] William K Wootters, *A Wigner-function formulation of finite-state quantum mechanics*, Annals of Physics, Volume **176**, Pages 1-21 (1987).

[31] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, R. Simon, *Wigner distributions for finite dimensional quantum systems: An algebraic approach*, Pramana , **65**, Pages 981-985, (2005)

[32] D.M. Appleby, *Symmetric informationally complete-positive operator valued measures and extended Clifford group*, J.Math.Phys., **46**, 052107 (2005).

[33] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, (Oxford University Press, 1979).

[34] H. E. Rose, *A Course in Number Theory*, (Oxford University Press, 1994).

[35] D. Gottesman, *A theory of fault-tolerant computation*, Phys. Rev. A **57**, 127–137 (1998).

[36] D. Gottesman, *Fault-tolerant quantum computation with higher-dimensional systems*, in C. Williams (ed.) *Quantum Computing and Quantum Communications*, Proceedings of the First NASA International Conference on Quantum Computing and Quantum Communications(QCQC), Palm Springs, California, 302–313.

[37] D. Gottesman, *The Heisenberg representation of quantum computers*, quant-ph/9807006.

[38] J. Dehaene, B. de Moor, *Clifford Group, stabilizer states, and linear and quadratic operations over* GF(2), Phys. Rev. A **68**, 042318 (2003).

[39] E. Hostens, J. Dehaene, B. de Moor, *Stabilizer states and Clifford operations for systems of arbitrary dimensions, and modular arithmetic*, Phys. Rev. A **71**, 042315 (2005).

[40] M. van den Nest, J. Dehaene, B. de Moor, *The invariants of the local Clifford group*, Phys. Rev. A **71**, 022310 (2005).

[41] M. van den Nest, J. Dehaene, B. de Moor, *Finite set of invariants to characterize local Clifford equivalence of stabilizer states*, Phys. Rev. A **72**, 014307 (2005).

[42] D.M. Appleby *Talk at Workhop on Quantum Foundations in the Light of Quantum Information III, CRM, Universite de Montreal*, December 6-9, 2011.

[43] E.B.Davies, *Quantum Theory of Open Systems*, Academic Press (1976).

[44] A.S. Holevo, *Probabilistic and statistical aspects of quantum theory*, North-Holland Publ. Cy., Amsterdam (1982).

[45] John von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, (1955)

[46] M.A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, (2000).

[47] E. Prugovecki, *Information-theoretical aspects of quantum measurement*, International Journal of Theoretical Phyics, **16**, 321-331 (1977).

[48] P. Busch, International Journal of Theoretical Physics, *Informationally complete sets of physical quantities*, **30**, 1217 (1991).

[49] F. E. Schroek, *Quantum Mechanics on Phase Space*, Kluwer, Dordrecht, the Netherlands, (1996).

[50] Stephen M. Barnett and Paul M. Radmore, *Methods in Theoretical Quantum Optics*, Clarendon Press, Oxford (1997).

[51] Ulf Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press, (1997).

[52] G. Zauner, *Quantendesigns. Grundzuge einer nichtkommutativen designtheorie*, PhD thesis, University of Vienna (1999). Published in English translation: G. Zauner, *Quantum designs: foundations of a noncommutative design theory*, Int. J. Quantum Inf., **9**, pp. 445-507 (2011).

[53] M. Grassl, *On SIC-POVMs and MUBs in dimension 6*, quant-ph/0406175 (2004).

[54] M. Grassl, *Tomography of quantum states in small dimensions*, Electronic Notes in Discrete Mathematics, **20**, 151-164 (2005).

[55] D.M. Appleby, *Symmetric informationally complete measurements of arbitrary rank*, Opt. Spect., **103**, pp.416-428 (2007).

[56] S.N. Flippov and V.I. Man'ko, *Symmetric informationally complete positive operator valued measure and probability representation of quantum mechanics*, J. Russian Laser Research, **31**, pp. 211-231 (2011).

[57] D.M. Appleby, S.T. Flammia and C.A. Fuchs, *The Lie Algebraic Significance of Symmetric Informationally Complete Measurements*, J.Math.Phys., **52**, 022202 (2011).

[58] J.M. Renes, R. Blume-Kohout, A.J. Scott and C.M. Caves, *Symmetric Informationally Complete Quantum Measurements*, J. Math. Phys., **45**, pp. 2171-2180 (2004).

[59] J.M. Renes, *Equiangular spherical codes in quantum cryptography*, Quantum Inf. Comput., **5**, pp. 81–92 (2005).

[60] A. J. Scott, *Tight informationally complete quantum measurements*, J. Phys. A, **39**, pp. 13507–13530 (2006).

[61] D.M. Appleby, Hoan Bui Dang, Christopher A. Fuchs, *Symmetric informationally complete quantum states as analogues to orthonormal bases and minimum uncertainty states*, arXiv:0707.2071 (2007).

[62] G. Kimura, *The Bloch vector for N-level systems* Phys. Lett. A **314**, 339 (2003).

[63] M.S. Byrd and N. Khaneja, *Characterization of the positivity of the density matrix in terms of the coherence vector representation*, Phys. Rev. A **68**, 062322 (2003).

[64] S.G. Schirmer, T. Zhang and J.V. Leahy, *Orbits of quantum states and geometry of Bloch vectors for N-level systems* J. Phys. A, **37**, 1389 (2004).

[65] G. Kimura and A. Kossakowski, *The Bloch-Vector Space for N-Level Systems: the Spherical-Coordinate Point of View* Open Sys. Information Dyn. **12**, 207 (2005).

[66] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review, **47**:777-780 (1935).

[67] E. Schrödinger, *Discussion of Probability Relations between Separated Systems*, Proceedings of the Cambridge Philosophical Society, **31**:555-562 (1935b).

[68] Z.Y. Ou, S.F. Pereira,H.J. Kimble and K.C. Peng *Realization of the Einstein-Podolsky-Rosen paradox for continuous variables*, Phys. Rev. Lett. **68**,3663, (1992b).

[69] Alessandro Ferraro, Stefano Olivares,Matteo G.A. Paris, *Gaussian states in continuous variable quantum information*, ISBN 88-7088-483-X Bibliopolis, Napoli, 2005 and arXiv: quant-ph/0503237v1.

[70] S.L. Braunstein and P. van Loock, *Rev. mod. Phys.* **77**, 513 (2005).

[71] Geza Giedke *Dissertation* Innsbruck, (2001).

[72] A. Serafini,O.C.O. Dahlsten,D. Gross and M.B. Plenio,*Canonical and micro-canonical typical entanglement of continuous variable systems*, J.Phys.A.Math.Theor. **40**, 9551-9576 (2007).

[73] A. Serafini, *Multimode Uncertainty Relations and Separability of Continuous Variable States*, Phys.Rev.Lett. **96**, 110402 (2006).

[74] Ulrik L. Andersen, Gerd Leuchs, Christine Silberhorn, *Continuous Variable Quantum Information Processing*, Laser & Photonics Reviews, **Vol.4**, 337-354 (2010).

[75] A. Kuzmich, E. Polzik, *Atomic continuous variable processing and light-atoms quantum interface, Quantum Information with Continuous Variables*, pp. 231265 (Kluwer Academics,2003).

[76] K. Hammerer, M. M. Wolf, E.S. Polzik and J. I. Cirac, *Quantum benchmark for storage and transmission of coherent states*, Phys. Rev. Lett. 94 150503 (2005).

[77] Klemens Hammerer, Anders S. Sorensen and Eugene S. Polzik, *Quantum interface between light and atomic ensembles*, Rev. Mod. Phys. 82, 10411093 (2010)

[78] A. Furusawa, J. L. Srensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik, *Unconditional Quantum Teleportation*, Science 23 October 1998: **Vol. 282** no. 5389 pp. 706-709.

[79] Yonezawa H, Aoki T, Furusawa A. *Demonstration of a quantum teleportation network for continuous variables*, Nature. 2004 Sep 23;431(7007):430-3.

[80] Lars S. Madsen, Vladyslav C. Usenko, Mikael Lassen, Radim Filip, Ulrik L. Andersen, *Continuous variable quantum key distribution with modulated entangled states*, Nature Communications 3, Article number: 1083 (2012).

[81] Brian Julsgaard, Jacob Sherson, J. Ignacio Cirac, Jaromr Fiurasek, Eugene S. Polzik1 *Experimental demonstration of quantum memory for light*, Nature **432**, 482-486 (2004).

[82] K. Jensen, W. Wasilewski, H. Krauter, T. Fernholz, B. M. Nielsen, M. Owari, M. B. Plenio, A. Serafini, M. M. Wolf, E. S. Polzik *Quantum memory for entangled continuous-variable states*, Nature Physics **7**, 1316 (2011).

[83] T.J. Kippenberg and K. J. Vahala, *Cavity optomechanics: back-action at the mesoscale*, Science **321** 1172 (2008).

[84] F. Marquardt and S. M. Girvin, *Optomechanics*, Physics 2, **40** (2009).

[85] K. L. Ekinci and M. L. Roukes, *Nanoelectromechanical systems*, Rev. Sci. Instrum. **76**, 061101 (2005).

[86] A. Mari, J. Eisert, *Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient*, Phys. Rev. Lett. **109**, 230503 (2012).

[87] Hulya Yadsan-Appleby, A. Serafini, *Would one rather store squeezing or entanglement in continuous variable quantum memories?*, Phys. Lett. A Volume **375**, Issue 18, Pages 1864-1869 (2011).

[88] Asher Peres, *Separability Criterion for Density Matrices* Phys. Rev. Lett. **77**,8 (1996).

[89] Michal Horodecki, Pawel Horodecki, Ryszard Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Phys. Lett. A, **223**, 1-8, (1996).

[90] R. Simon, *Peres-Horodecki separability criterion for continuous variable systems*, Phys. Rev. Lett. **84**, 2726-2729, (2000).

[91] C. T. Lee, Phys. Rev. A **44**, R2275 (1991).

[92] R. Simon, N. Mukunda, and B. Dutta, Phys. Rev. A **49**, 1567 (1994).

[93] G. Vidal and R.F. Werner, Phys. Rev. A, **65**, 032314 (2002).

[94] Michael M. Wolf, Jens Eisert and Martin B. Plenio *The entangling power of passive optical elements*, Phys.Rev.Lett, **90**, 047904 (2003).

[95] M. Fleischhauer, A. Imamoglu, and J. P. Marangos, *Electromagnetically induced transparency: Optics in Coherent Media*, Reviews Modern Physics, **77**, 633 (2005).

[96] M. D. Lukin, Rev. Mod. Phys. **75**(2), 457, (2003).

[97] Duan, L.-M., M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) 414, 413 (2001).

[98] S. A Moiseev, W. Tittel, *Optical quantum memory with generalized time-reversible atom-light interactions*, arXiv 0812. 1730

[99] G. Hetet, M. Hosseini, B. M. Sparkes, D. Oblak, P. K. Lam, and B. C. Buchler, Opt. Lett. **33** 2323 (2008)

[100] J. L. Le Gouet, P. Berman, Phys. Rev. A **80** 012320 (2009)

[101] M. Afzelius, C. Simon, H. de Riedmatten, N. Gisin, Phys. Rev. A **79**, 052329, (2009).

[102] Alexander I. Lvovsky, Barry C. Sanders and Wolfgang Tittel *Optical quantum memory*, Nature Photonics, **3**, 706-714 (2009).

[103] Klemens Hammerer, Anders S. Sorensen and Eugene S. Polzik, *Quantum interface between light and atomic ensembles*, Reviews of Modern Physics **82**, 1041 (2010).

[104] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S.J. Dewhurst, N. Gisin, C.Y. Hu, F. Jelezko, S. Kroll, J.H. Muller, J. Nunn, E. Polzik, J. Rarity, H. de Riedmatten, W. Rosenfeld, A.J. Shields, N. Scold, R.M. Stevenson, R. Thew, I. Walmsley, M. Weber, H. Weinfurter, J. Wrachtrup and R.J. Young, *Quantum memories*, Eur. Phys. J. D **58**, 1 (2010).

[105] Briegel, H.-J., W. Du r, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[106] Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[107] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, Nicolas Gisin, Rev. Mod. Phys. **83** (2011).

[108] E. Knill, R. Laflamme, G. J. Milburn, Nature, **409**, 46 (2001).

[109] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).

[110] K. Saucke, *Diploma Thesis*, University of Munich (2002).

[111] C. Simon, W. T. M. Irvine, Phys. Rev. Lett. **91**, 110405 (2003).

[112] H. Buhrman, R. Cleve, S. Massar, R. de Wolf, arXiv: 0907.3584v1.

[113] Daniel E. Browne, Jens Eisert, Stefan Scheel, and Martin B. Plenio, *Driving non-Gaussian to Gaussian states with linear optics*, Phys. Rev. A **67**, 062320 (2003)

[114] N. C. Menicucci et al. Phys. Rev. Lett. **97**, 110501 (2006).

[115] L. P. Lamoureux et al. Phys. Rev. Lett. **94**, 050503 (2005).

[116] S. Lloyd, Science **321**, 1463 (2008).

[117] M. Owari, M. B. Plenio, E. S. Polzik, A. Serafini, M. M. Wolf, *Squeezing the limit: Quantum benchmarks for the teleportation and storage of squeezed states*, New J. Phys. 10, 113014, (2008).

[118] J. Calsamiglia, M. Aspachs, R. Muoz-Tapia, and E. Bagan, *Phase-covariant quantum benchmarks*, Phys. Rev. A 79, 050301(R) (2009).

[119] M.A. Ballester, *Optimal estimation of $SU(d)$ using exact and approximate 2-designs*, quant-ph/0507073 (2005).

[120] D. Petz and L. Ruppert, *Efficient quantum tomography needs complementary measurements*, arXiv:1011.5210 (2010).

[121] H. Zhu and B.-G. Englert, *Quantum state tomography with fully symmetric measurements and product measurements*, Phys. Rev. A, **84**, 022327 (2011).

[122] T. Durt, C. Kurtsiefer, A. Lamas-Linares and A. Ling, *Wigner tomography of two-qubit states and quantum cryptography*, Phys. Rev. A, **78**, 042338 (2008).

[123] J. Du, M. Sun, X. Peng and T. Durt (2006), *Realization of entanglement assisted qubit-covariant symmetric-informationally-complete positive-operator-valued measurements*, Phys. Rev. A, **74**, 042341.

[124] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček and J. Anders, *Efficient and robust quantum key distribution with minimal state tomography*, quant-ph/0412075 (2004).

[125] J. Řeháček, B.-G. Englert and D. Kaszlikowski, *Minimal qubit tomography* Phys. Rev. A, **70**, 052321 (2004).

[126] C.A. Fuchs and M. Sasaki, *Squeezing quantum information through a classical channel: measuring the quantumness of a set of quantum states*, Quantum Inf. Comput., **3**, pp. 377–404 (2003).

[127] C. A. Fuchs, *On the quantumness of a Hillbert space*, Quantum Inf. Comput. **4**, pp. 467–478 (2004).

[128] I.H. Kim, *Quantumness, generalized spherical 2-design and symmetric informationally complete POVM*, Quantum Inf. Comput., **7**, pp. 730–737 (2007).

[129] B. G. Bodmann, D. W. Kribs and V. I. Paulsen, *Decoherence-insensitive quantum communication by optimal C^*-encoding*, IEEE Trans. Inf. Theory, **53**, pp. 4738–4749.

[130] O. Oreshkov, J. Calsamiglia, R. Muñoz-Tapia and E. Bagan, *Optimal signal states for quantum detectors*, New J. Phys., **13**, 073032 (2011).

[131] I. Bengtsson, K. Blanchfield and A. Cabello, *A Kochen-Specker inequality from a SIC*, arXiv:1109.6514 (2011).

[132] S. D. Howard, A. R. Calderbank and W. Moran, *The finite Heisenberg-Weyl groups in radar and communications*, EURASIP J. Appl. Sig. Process., **2006**, 85865 (2006).

[133] M. A. Hermann and T. Strohmer, *High-resolution radar via compressed sensing*, IEEE Trans. on Sig. Process., **57**, pp. 2275–2284 (2009).

[134] R. Balan, B. G. Bodmann, P. G. Casazza and D. Edidin, *Painless reconstruction from magnitudes of frame coefficients*, J. Fourier Anal. Appl., **15**, pp. 488–501 (2009).

[135] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs and A. M. Steinberg, *Experimental characterization of qutrits using SIC-POVMs*, Phys. Rev. A, **83**, 051801R (2011).

[136] A. Kalev, J. Shang and B.-G. Engert, *Symmetric Minimal Quantum Tomography by Successive Measurements*, eprint arXiv:1203.1677 (2012).

[137] G. N. M. Tabia, *Experimental Scheme for qubit and qutrit SIC-POVMs using Multiport Devices*, eprint arXiv:1207.6035 (2012).

[138] C. A. Fuchs and R. Schack, *Quantum-Bayesian coherence*, eprint arXiv:0906.2187 (2009).

[139] C. A. Fuchs, *QBism, the Perimeter of Quantum Bayesianism*, eprint arXiv:1003.5209 (2010).

[140] D. M. Appleby, Å. Ericsson and C. A. Fuchs, *Properties of QBist state spaces*, Found. Phys., **41**, pp. 564–579 (2011).

[141] E. Schnetter, *To Appear*.

[142] A.J. Scott and M. Grassl, *SIC-POVMs: a new computer study*, J.Math.Phys. **51**, 042203 (2010).

[143] D.M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross and J.-Å-Larsson, *The Monomial Representations of the Clifford Group*, Quantum Inf. Comput., **12**, 404-431 (2012).

[144] D.M. Appleby, I. Bengtsson, S. Brierley, Å. Ericsson, M. Grassl and J.-Å-Larsson, *Systems of Imprimitivity for the Clifford Group*, arXiv: 1210. 1055 (2012).

[145] Harold M. Edwards, *Galois Theory*, Springer-Verlag, New York, Berlin, Heidelberg, (1984).

[146] Garrett Birkhoff and Saunders MacLane, *A Survey of Modern Algebra*, The Macmillan Company, New York (1941).

[147] Steven Roman, *Field Theory* Springer-Verlag, New York, Berlin, Heidelberg, (1995).

[148] Sougato Bose, *Quantum Communication through an Unmodulated Spin Chain*, Phys. Rev. Lett. **91** (20) (2003).

[149] Sougato Bose, *Quantum Communication Through Spin Chain Dynamics: An Introductory Overview*,Contemporary Physics, **48**, pages 13 - 30, (2007).

[150] N. W. Ashcroft and N. D. Mermin, *Solid State Physics*, Harcourt College Publishers, Fort Worth, (1976).

[151] Tobias J. Osborne and Noah Linden, *Propagation of quantum information through a spin system*, Phys. Rev. A, **69**, 052315 (2004).

[152] S. S. Schweber, An Introduction to Relativistic Quantum Field Theory, Harper and Row, New York (1962)

[153] A. Kay, Int. J. Q. Inform. **8**, 641 (2010)

.