Limiting behaviours in physics:
From duality to super-resolution

Kevin Piché

A thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfilment of the requirements for the
MSc degree in Physics

Department of Physics
Faculty of Science
University of Ottawa

Contents

List of Figures

List of Tables

Acronyms

BQC Blind Quantum Computation.

CCD Charge-Coupled Devices.

LG Laguerre-Gaussian.

MMF Multi-Mode Fibre.

NPBS Non-Polarizing Beam Splitter.

OAM Orbital Angular Momentum.

PBS Polarizing Beam Splitter.

QCED Quantum Computation on Encrypted Data.

SLM Spatial Light Moduator.

SVD Singular Value Decomposition.

Symbols

A: Object, light at the input of the imaging system.

B: Image, light at the output of the imaging system.

S_r: Super-resolution factor.

Φ: Eigenmode.

$\hat{\rho}$: density matrix.

$\hat{\sigma}$: Pauli matrix.

λ: Eigenvalue.

$\mathcal{A}$: Accessible environment.

$\mathcal{C}$: Coherence of quantum state, best recoverable degree of superposition.

$\mathcal{D}$: Distinguishability of quantum state, best recoverable 'which alternative information'.

$\mathcal{E}$: Environment.

$\mathcal{I}$: Inaccessible environment.

$\mathcal{P}$: Predictability of quantum state, 'which alternative information'.

$\mathcal{Q}$: Qubit.

$\mathcal{V}$: Visibility of quantum state, degree of superposition.

c: Space-bandwidth product.

f: Focal length of a lens.

Abstract

In this thesis, we discuss several phenomena exhibiting 'limiting behaviour' in physics. This includes the duality principle, delegated quantum computation, and super-resolution. The duality principle places a limit on the coexistence of wave and particle behaviours. We develop a framework that explains apparent violations of this principle while staying within the scope of quantum mechanics. In addition, we relate the duality principle to the sub-fidelity and weak-values. We also show that the maximum recoverable coherence of a qubit has a sharp transition from 0 to 1 when we have access to half of the environment to which the qubit is correlated. Delegated quantum computation consists of a computational weak client who wishes to delegate a complex quantum computation to a powerful quantum server. We develop a new protocol for delegated quantum computation requiring less quantum power than its predecessor. Finally, we develop and test a new theory for eigenmode super-resolution.

Acknowledgements

I would like to acknowledge and thank Robert W. Boyd and Anne Broadbent for their support during the course of this work. This would not have happened without them.

This work was supported by NSERC, CERC and the Bank of Montréal.

I acknowledge Eliot Bolduc, Jonathan Leach, and Filippo M. Miatto for their help in the development of the framework describing apparent violations of the duality principle and in the theoretical analysis of the experiment. In addition, Jonathan Leach and Eliot Bolduc also performed the experimental test of this theory including the data analysis. I would like to acknowledge Filippo M. Miatto for his support and guidance in the subsequent theoretical analysis of the duality principle including its relation to weak values and the sub-fidelity. He also provided the derivation for the recoverable coherence as a function of the dimensions of the accessible and inaccessible environment.

I would like to acknowledge Anne Broadbent for providing guidance and support throughout the development of the new delegated quantum computing protocol.

I acknowledge Jonathan Leach for his support in the first experimental test of eigenmode super-resolution. I would also like to acknowledge Allan S. Johnson and Jeff Z. Salvail for developing the technique to numerically determine the eigenmodes of optical imaging systems and their application to super-resolution. I acknowledge Robert Fickler for building the experimental setup for the second experiment: the application of the generalised theory to the $4f$ system. Finally, I would like to acknowledge Frédéric Bouchard for his help in setting up the last super-resolution experiment: eigenmode super-resolution through a multimode fibre.

I would also like to thank Filippo M. Miatto and Jonathan Leach.

Copyrighted Contents

This thesis does not contain copyrighted content from other authors.

Chapter 1

Introduction

There are many interesting phenomena in physics. There exists a class of phenomena involving *limited behaviours*. By this we mean that there exists a one-way or two-way bounded relationship between two quantities. In this thesis, we will be discussing three of these behaviours: the first is the duality principle, the second is delegated quantum computation, and the final phenomenon is super-resolution.

The first chapter will be discussing the duality principle which limits the simultaneous existence of 'which-alternative information' and a coherent super-position of said alternatives. This principle is one of the building blocks of quantum mechanics. However, in a recent paper by Menzel, they reported simultaneous high-visibility fringes and high which-alternative information in a single system which is in apparent violation of the duality principle [1]. We provide a framework to explain such apparent violations of the duality principle using post-selection and provide experimental support for this. We also relate duality to weak values and show that these values perfectly describe the system even for strong coupling for a certain class of coupling Hamiltonians. In addition, we derive the behaviour of the visibility (coherent super-position) of a qubit when we only have access to a subspace of the environment to which it is entangled. By access, we mean that we have the ability to manipulate and measure this subspace. In contrast, inaccessible environments cannot be manipulated, nor measured. We show that the visibility in this case is related to the sub-fidelity of the inaccessible environment. This provides the first operational interpretation of the sub-fidelity. Finally, we also show the surprising result that it is possible to restore full coherence of a qubit while only having access to half of its environment. These derivations are a significant step towards linking the duality principle to generalized measurements which is one of the most powerful tools for describing quantum measurements. This allows us to better predict the behaviour of quantum systems under complex situations.

In the second chapter of this thesis, we will be looking at our next dual behaviour:

that of security and quantum power in a delegated quantum computation scheme. Here a client (often named Alice) wishes to delegate a complex quantum computation to a server (often named Bob). In recent work, it was shown that a purely classical client cannot delegate a quantum computation to a quantum server with security. At the other end of the spectrum, we have a quantum client that has infinite quantum power. In this case, no delegation is required as the client can perform the computation on its own. More interesting cases fall in-between these two extremes and one example is quantum computing on encrypted data (QCED). In QCED, the client can delegate a computation if it can generate four ancillary states. In this work, we reduce the number of required states to two non-orthogonal states as well as provide a proof of input privacy for an honest server. This can be viewed as a reduction of required quantum power on the client's side without compromising input privacy. From this it is clear that the relationship between privacy and quantum power is not quite straightforward. Here we are interested in taking the first step towards a complete understanding to the minimal requirement for information theoretic security as current research is focused not on minimal requirements but instead purely on functionality of quantum circuits and security from various powerful adversaries. Future work will be looking into the complete dual behaviour for clients with quantum power below this requirement.

In optics, we have the diffraction limit which restricts the resolution of images. Due to the power of optics in various fields, an entire field of research is dedicated to going beyond this limit. In the final chapter, we present a new technique for super-resolution called eigenmode super-resolution. This technique corrects diffraction and aberrations by finding the eigenmodes of an optical system and then compensating for the eigenvalues after propagation. We present here simulated and experimental results of its application to various optical systems including a multi-mode fibre. This method of achieving super-resolution has many advantages over its competitors: it is easily applicable to many pre-existing optical systems without having to make many modifications to the system and it does not require many specialized optical components and finally it is not restricted in the types of images it can resolve.

The following is a summary of my research contributions along with those of my co-contributors. My contribution to the duality principle project is the following: I provided minor aid in the development of the framework describing apparent violations of the duality principle due to post-selection. Jonathan Leach, Eliot Bolduc and Filippo M. Miatto provided this framework. Jonathan Leach and Eliot Bolduc performed the experimental test of this theory. Filippo M. Miatto and I, developed the theory relating the coherence to the sub-fidelity. I developed the theory relating weak values and the duality principle with the

guidance of Filippo M. Miatto. Filippo M. Miatto developed the theory for recovering coherence as a function of the dimensions of the accessible and inaccessible environment as well as developing the examples with limited assistance on my part. Three separate papers are currently being written for this project: one for the experimental test of the duality principle in the presence of post-selection [2], one on the relation between the duality principle and the sub-fidelity [3], and one of the optimal bound of quantum erasure with limited means [4].

I developed the new protocol for delegated quantum computation and derived the proof for an honest server. Anne Broadbent provided guidance and support throughout this work. I performed a literature review of super-resolution and introduced our group to its basics. I also performed the first eigenmode super-resolution experiment with the support of Jonathan Leach [5]. Allan S. Johnson and Jeff Z. Salvail developed the technique to numerically determine the eigenmodes of optical imaging systems. I performed the numerical simulations implementing this technique for a variety of systems and objects [6]. Allan S. Johnson and Jeff Z. Salvail provide help in development of the simulations. Robert Fickler built the experimental setup for the second experiment: the application of the generalised theory to the $4f$ system. I took and analysed the data. I also performed a simulation of this system. Frederic Bouchard and I performed the final experiment: super-resolution throught a multi-mode fibre. I analysed the data from this experiment as well.

Chapter 2

The duality principle

The duality principle is one of the building blocks of quantum mechanics. Essentially, it is a quantitative version of the wave-particle duality. In other words, the duality principle limits the coexistence of wave and particle behaviours of quantum systems. If we consider a qubit, a quantum system living in a two-dimensional Hilbert space, the duality principle is given by an equation of the following form:

$$(\text{wave-like})^2 + (\text{particle-like})^2 \leq 1, \tag{2.1}$$

where we have two quantities: one describing a *wave-like* property and the other describing a *particle-like* property. The wave-like property, denoted by $\mathcal{V}$, is called the *visibility* and it is a measure of the degree of interference between the two alternatives of the qubit. The particle-like property, denoted by $\mathcal{P}$, is called the *predictability* and it is a measure of how well one can predict the outcome of a measurement on the two alternatives [7]. This is also called which-alternative information. In the context of the double slit experiment, the visibility is a measure of the clearness of the interference fringes and the predictability is a measure of our knowledge of which slit the photons went through. The clearer the fringes, the less we know about which slit the photons went through and vice versa. We can call this a limiting behaviour because one quantity places an upper bound or limit on the value of the other and vice versa. These two quantities are of great importance to quantum mechanics and more specifically to quantum optics. Most applications of quantum optics require photons that are in a state of superposition. Thus our ability to measure the visibility allows us to better calibrate our experiments and make sure that the photons are in the desired state. The predictability is used less often compared to the visibility; however, the ability to predict outcomes is often useful.

Quantum systems such as qubits can interact with their surrounding environment and

become coupled to it. This coupling can be of a classical or a quantum nature. It may be intentional such as the coupling of polarization to the path of an interferometer. It may also be detrimental and lead to decoherence. Decoherence is a term widely used in physics and has different meanings in different contexts. Here we mean loss in the visibility of a quantum system. In other words, decoherence is a process where the interference of the alternatives of a qubit is lost. This is of great interest as it can be viewed as a transition from quantum to classical physics. It is also important from a practical point-of-view as maintaining coherence throughout a quantum protocol is essential to its success [8, 9, 10, 11, 12, 13]. Quantum erasure is one of the many techniques available for restoring coherence in quantum systems. The technique consists of measuring the environment to which the system of interest is coupled in such a way that the information stored within it is erased and thereby coherence is recovered [14]. A great example of this phenomenon is given by Young's double-slit experiment. If we were to place two orthogonal polarizers in front of the slits, the interference fringes will disappear. Quantum erasure would consist of adding a polarizer diagonally before the screen. This will erase the path information contained in the polarization of the light and restore the interference fringes.

The duality principle has been tested, directly and indirectly, many times and for many regimes [15, 16, 17, 18, 19, 20]. In all of these tests, the duality principle was consistent with the experimental results. In a recent paper, Menzel et al. reported simultaneous high-visibility fringes and high which-alternative information in a single system [1]. This work is not in conflict with the duality principle as we will see in the following section [21]. In brief, this apparent violation of the duality principle is due to post-selection. The high-visibility fringes were measured with respect to a particular post-selection and the high which-alternative information was measured with respect to another.

In this thesis, we develop a framework for understanding apparent violations of the duality principle. This framework is based on post-selection. Post-selection is the act of ignoring the results of a measurement given the outcome of another. The experiment is repeated many times until the desired outcome for the second measurement is achieved. We also perform an experiment to demonstrate the validity of this theory and found the results to be consistent. In addition, we explored the duality principle by applying it to multiple scenarios. First, we derive the visibility and the predictability of a qubit in terms of weak values describing the coupling between the qubit and its environment. We find that these equations apply even when the coupling is not weak for Hamiltonians of a given form. We also look at the scenario where we have access to only a two-dimensional sub-space of the environment. For this type of system we derived a relation between the maximal recoverable visibility of a qubit and the sub-fidelity of the states of the inaccessible environment conditioned on the alternatives of

the qubit. This is the first operational interpretation of the sub-fidelity [22]. Finally, we look at quantum erasure for the case where we only have access to a subset of the environment to which the system is coupled. We derive the maximum average visibility that can be achieved as a function of the dimension of the accessible and inaccessible environments. We demonstrate the surprising result that there is a sharp transition in the average visibility from 0 to 1 when we have access to approximately half of the environment.

2.1 Introduction to density matrices

In quantum mechanics, quantum states are often described using state vectors $|\psi\rangle$. However, this is only possible for pure states. For mixed states, quantum states that are correlated to an environment, this is no longer possible and a new description is required. The more general way to describe quantum systems is with the density matrix $\hat{\rho}$. Because interactions with environments are a crucial part of this chapter we will need to use the density matrix formalism.

The density matrix $\hat{\rho}$ of a qubit is given by the following matrix:

$$\hat{\rho} = \begin{pmatrix} p_0 & \sqrt{p_0 p_1}\epsilon \mathrm{e}^{i\theta} \\ \sqrt{p_0 p_1}\epsilon^* \mathrm{e}^{-i\theta} & p_1 \end{pmatrix}, \tag{2.2}$$

where p_0 and p_1 are the probabilities of the system being in the state $|0\rangle$ and $|1\rangle$ respectively, θ is the relative phase of the two states, and ϵ is the complex cross-term. This cross-term determines the purity of the system. The qubit is in a pure state if and only if $|\epsilon| = 1$ and in this case the density matrix can be written as $\hat{\rho} = |\psi\rangle\langle\psi|$ where $|\psi\rangle = \sqrt{p_0}|0\rangle + \sqrt{p_1}\mathrm{e}^{i\theta}|1\rangle$. The density matrix has the following property: $\mathrm{Tr}\hat{\rho} = 1$ where the trace (Tr) is the sum of the diagonal.

For composite systems, we need to take the tensor product of the density matrices of the individual systems to get the composite density matrix: $\hat{\rho}_{ab} = \hat{\rho}_a \otimes \hat{\rho}_b$. As stated previously, interactions will be important in this section. Interactions lead to correlations and correlated systems have more complicated composite density matrices. For the case where one of the systems is a qubit, the composite density matrix can be written as:

$$\hat{\rho} = \begin{pmatrix} p_0\hat{\rho}_0 & \sqrt{p_0 p_1}\mathrm{e}^{i\theta}\hat{\chi} \\ \sqrt{p_0 p_1}\mathrm{e}^{-i\theta}\hat{\chi}^\dagger & p_1\hat{\rho}_1 \end{pmatrix}, \tag{2.3}$$

where ρ_0 and ρ_1 are the states of the second system given that the qubit is in the state $|0\rangle$ and $|1\rangle$ respectively and $\hat{\chi}$ is the cross-term. If we want to find the individual density matrices

from the composite density matrix, we must take the partial trace over all other systems. While taking the partial trace, one ignores the system of interest while taking the trace over all of the others. Consider for example a density matrix of the form $\hat{\rho}_{ab} = \frac{1}{2}(\hat{\psi}_a \otimes \hat{\psi}_b + \hat{\phi}_a \otimes \hat{\phi}_b)$, where $\hat{\psi}_a$ and $\hat{\phi}_a$ are density matrices for system a and $\hat{\psi}_b$ and $\hat{\phi}_b$ are density matrices for system b. The state of system a is given by $\hat{\rho}_a = \mathrm{Tr}_b \hat{\rho}_{ab} = \frac{1}{2}(\hat{\psi}_a \mathrm{Tr}(\hat{\psi}_b) + \hat{\phi}_a \mathrm{Tr}(\hat{\phi}_b)) = \frac{1}{2}(\hat{\psi}_a + \hat{\phi}_a)$.

Furthermore, the trace norm of a matrix $\hat{X}$ will be important in our analysis. It is given by the sum of the square root of the d eigenvalues of the matrix $\hat{X}^\dagger \hat{X}$:

$$\mathrm{Tr}|\hat{X}| = \sum_{i=1}^{d} \sqrt{\lambda_i(\hat{X}^\dagger \hat{X})}, \tag{2.4}$$

where d is the dimensionality of $\hat{X}$.

As a final note, it is often important to know how 'close' a given density matrix is to another. By 'close', we mean how much overlap there is between the two density matrices. For example, orthogonal states have no overlap and identical density matrices are perfectly overlapped. Uhlmann's fidelity is one such measure and is given by [22]:

$$F(\hat{\rho}_1, \hat{\rho}_1) = \left(\mathrm{Tr}\left|\sqrt{\hat{\rho}_1}\sqrt{\hat{\rho}_2}\right|\right)^2 = \left(\mathrm{Tr}\sqrt{\sqrt{\hat{\rho}_1}\hat{\rho}_2\sqrt{\hat{\rho}_1}}\right)^2 \tag{2.5}$$

The sub-fidelity, $E(\hat{\rho}_1, \hat{\rho}_2)$, is a lower bound to this measure of closeness. It is given by $E(\hat{\rho}_1, \hat{\rho}_2) = \mathrm{Tr}(\hat{\rho}_1\hat{\rho}_2) + \sqrt{2}\sqrt{[\mathrm{Tr}(\hat{\rho}_1\hat{\rho}_2)]^2 - \mathrm{Tr}(\hat{\rho}_1\hat{\rho}_2\hat{\rho}_1\hat{\rho}_2)}$. Our work suggests that the sub-fidelity has a deeper meaning then simply being a lower bound (see section 2.5).

2.2 Theoretical framework

The duality principle is of fundamental importance to quantum mechanics. It states that the existence of 'which-alternative information' places an upper bound on the possible degree of superposition for these alternatives and vice versa. The fundamentals of this have been examined in detail by Englert and Bergou [7]. We provide a quick overview here. We first note that there is a nice visual representation of the duality principle which is provided by the Bloch sphere, see Figure 2.1. Here we have an arbitrary qubit in the state $\hat{\psi} = \frac{1}{2}(\hat{\mathbb{1}} + \mathbf{v} \cdot \overrightarrow{\hat{\sigma}})$ where $\overrightarrow{\hat{\sigma}} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$ is a vector of Pauli matrices and $\mathbf{v} = (x, y, z)$ is the Bloch vector. The z coordinate being the distance along the North-South line ($|0\rangle$-$|1\rangle$ line). The visibility $\mathcal{V}$ can be written as $x^2 + y^2$ and the predictability is given by z^2. From this it is clear why $\mathcal{V}^2 + \mathcal{P}^2 \leq 1$: from these relations, the duality principle can be rewritten as $x^2 + y^2 + z^2 \leq 1$

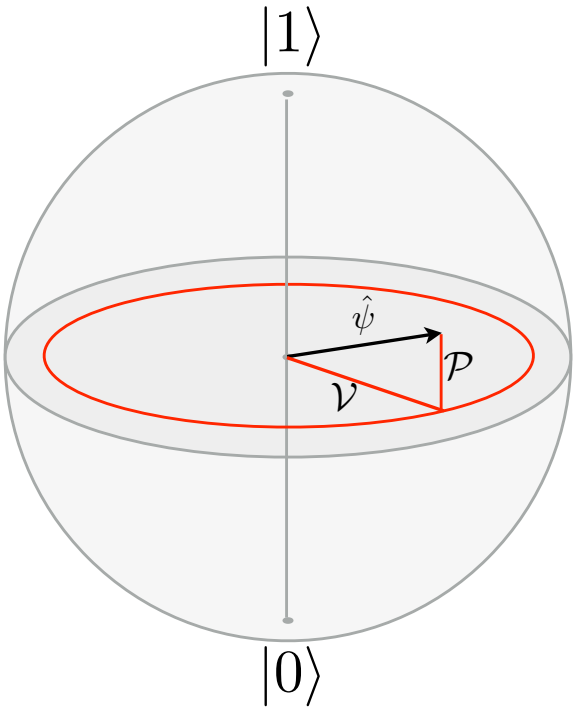

Figure 2.1: The duality principle can be visualized using the Bloch sphere. Here, the visibility $\mathcal{V}$ of a quantum state $\hat{\psi}$ is given by the distance from the North-South line and the predictability $\mathcal{P}$ is given by the distance from the equatorial plane. The North-South line is determined by the chosen alternatives $|0\rangle$ and $|1\rangle$. This representation makes it clear why the squared sum of these quantities is bounded by one: the Bloch sphere is a unit sphere. Real physical systems do not exist outside the Bloch sphere.

which is true from the definition of a density matrix. It is also clear from this picture that the duality principle is saturated only for pure states as these states and these states alone lie on the surface of the Bloch sphere which is a unit sphere.

More formally, for a qubit $\mathcal{Q}$ with a density matrix given by $\hat{\rho}$, $\mathcal{V}$ and $\mathcal{P}$ are given by:

$$\mathcal{V} = |\mathrm{Tr}\left[(\hat{\sigma}_x + i\hat{\sigma}_y)\hat{\rho}\right]|, \tag{2.6}$$

$$\mathcal{P} = |\mathrm{Tr}\left[\hat{\sigma}_z\hat{\rho}\right]|. \tag{2.7}$$

These quantities are real positive numbers taking a value between 0 and 1. Here, a value of 0 indicates no coherent superposition or knowledge of the alternatives and a value of 1 indicates a perfect superposition or a complete knowledge of the alternatives. These equations do not take into account any environment $\mathcal{E}$ to which the qubit may be coupled. This information is traced out when calculating $\hat{\rho}$. Let us now consider the combined density matrix of $\mathcal{Q}$ and $\mathcal{E}$: $\hat{\rho}_{\mathcal{Q}\mathcal{E}}$. The new question is, what happens to $\mathcal{V}$ and $\mathcal{P}$ if we make a measurement on the

environment $\mathcal{E}$ and get the result $\hat{\pi}$, where $\hat{\pi}$ is the density matrix of the environment after the measurement. First, the state of the qubit $\mathcal{Q}$ is reduced to

$$\hat{\rho}_{\mathcal{Q}|\hat{\pi}} = \frac{\mathrm{Tr}_{\mathcal{E}}[(\hat{\mathbb{1}} \otimes \hat{\pi})\hat{\rho}_{\mathcal{Q}\mathcal{E}}]}{p}, \tag{2.8}$$

where $p = \mathrm{Tr}[(\hat{\mathbb{1}} \otimes \hat{\pi})\hat{\rho}_{\mathcal{Q}\mathcal{E}}]$ is the probability of measuring $\hat{\pi}$. Substituting this into equations 2.6 and 2.7 gives us the values of the visibility and predictability conditioned on the measurement outcome $\hat{\pi}$,

$$\mathcal{V}_{\hat{\pi}} = |\mathrm{Tr}\left[(\hat{\sigma}_x + i\hat{\sigma}_y)\hat{\rho}_{\mathcal{Q}|\hat{\pi}}\right]|, \tag{2.9}$$

$$\mathcal{P}_{\hat{\pi}} = |\mathrm{Tr}\left[\hat{\sigma}_z\hat{\rho}_{\mathcal{Q}|\hat{\pi}}\right]|. \tag{2.10}$$

The process of measuring the environment and waiting for a particular measurement result $\hat{\pi}$ is post-selection. If we repeat the measurement multiple times on identical copies of the joint system $\hat{\rho}_{\mathcal{Q}\mathcal{E}}$, rejecting the cases where the result was not $\hat{\pi}$. These new conditional values define the conditional duality relation:

$$\mathcal{V}_{\hat{\pi}}^2 + \mathcal{P}_{\hat{\pi}}^2 \leq 1. \tag{2.11}$$

Post-selection can be achieved when one has access to the measurement outcomes. This does not need to be immediate. The measurement outcomes can be saved and read at a later date. Sometimes, we wish to make a measurement on $\mathcal{E}$ but we do not wish to or can't post-select on particular outcomes. In this case we must take an average over the outcomes $\{\hat{\pi}_k\}$ to:

$$\overline{\mathcal{V}} = \sum_k p_k \mathcal{V}_{\hat{\pi}_k}, \tag{2.12}$$

$$\overline{\mathcal{P}} = \sum_k p_k \mathcal{P}_{\hat{\pi}_k}, \tag{2.13}$$

where $p_k = \mathrm{Tr}[(1 \otimes \hat{\pi}_k)\hat{\rho}_{\mathcal{Q}\mathcal{E}}]$. These quantities define the most stringent test of the duality principle:

$$\overline{\mathcal{V}}^2 + \overline{\mathcal{P}}^2 \leq 1. \tag{2.14}$$

The minimum values for these quantities are given by the case where no measurement was

made, $\hat{\pi} = \hat{\mathbb{1}}$. The result is

$$\min_{\{\hat{\pi}\}} \overline{\mathcal{V}} = \mathcal{V}, \tag{2.15}$$

$$\min_{\{\hat{\pi}\}} \overline{\mathcal{P}} = \mathcal{P}. \tag{2.16}$$

We therefore have that any information about the alternatives contained within the state of the qubit $\mathcal{Q}$ itself cannot be lost by making some measurement on the environment. Note that this is only true for the case where no post-selection is made. When we include post-selection, the state of the qubit can be of any form.

Let us now turn to the maximum values for $\overline{\mathcal{V}}$ and $\overline{\mathcal{P}}$. These quantities are given by the *coherence* $\mathcal{C}$ and the *distinguishability* $\mathcal{D}$, respectively. They are defined as

$$\mathcal{C} = \sup_{\{\hat{\pi}\}} \overline{\mathcal{V}} = \mathrm{Tr}|\hat{X}_{\mathcal{E}}|, \tag{2.17}$$

$$\mathcal{D} = \sup_{\{\hat{\pi}\}} \overline{\mathcal{P}} = \mathrm{Tr}|\hat{W}_{\mathcal{E}}|, \tag{2.18}$$

where 'sup' stands for the supremum and:

$$\hat{X}_{\mathcal{E}} = \mathrm{Tr}_{\mathcal{Q}} \left([(\hat{\sigma}_x + i\hat{\sigma}_y) \otimes \hat{\mathbb{1}}] \hat{\rho}_{\mathcal{Q}\mathcal{E}} \right), \tag{2.19}$$

$$\hat{W}_{\mathcal{E}} = \mathrm{Tr}_{\mathcal{Q}} \left([\hat{\sigma}_z \otimes \hat{\mathbb{1}}] \hat{\rho}_{\mathcal{Q}\mathcal{E}} \right). \tag{2.20}$$

These two quantities correspond to two different kinds of quantum steering. Here, quantum steering is the process of setting a preferred basis for a quantum system by acting on its entangled partner [23]. This steering is what Einstein referred to as 'spooky action at a distance' [24].

In the case of the coherence $\mathcal{C}$, the measurements on the environment are chosen such that any information it contained about the two alternatives of the qubit are erased and thus leave the qubit with a high degree of superposition. This is called quantum erasure [14]. Alternatively, when achieving the distinguishability $\mathcal{D}$, the information about the superposition is lost and the qubit is left with a large degree of which-alternative information.

We can now define two new relations: the erasure relation $\mathcal{C}^2 + \mathcal{P}^2 \leq 1$ and the duality relation $\mathcal{V}^2 + \mathcal{D}^2 \leq 1$. The erasure relation is a quantitative statement about the wave-particle duality as it places an upper bound on the recoverable visibility given that the qubit has a given $\mathcal{P}$. It provides an upper limit to the effectiveness of quantum erasure. Similarly, the duality relation provides an upper limit on the recoverable which-alternative information given that the qubit has a given $\mathcal{V}$.

The relations given above provide tests of the duality principle under both steering scenarios. We can also write the following hierarchy for the degree of superposition of a qubit $\mathcal{Q}$: $\mathcal{V} \leq \overline{\mathcal{V}} \leq \mathcal{C}$ where $\mathcal{C}$ represents nature's knowledge about the superposition of the alternatives, $\overline{\mathcal{V}}$ represents man's knowledge after a measurement of the environment, and $\mathcal{V}$ represents man's knowledge before the measurement. We have an analogous hierarchy for the which-alternative information: $\mathcal{P} \leq \overline{\mathcal{P}} \leq \mathcal{D}$.

Finally, weak values [25, 26] have found many applications, from weak amplification [27] to direct measurements of the wave-function [28]. We will be deriving the conditional values for $\mathcal{V}$ and $\mathcal{P}$ in terms of weak values for a special Hamiltonian. In the language of weak values, a system s (in our case the qubit $\mathcal{Q}$) is coupled to a pointer p (in our case the environment $\mathcal{E}$) with some coupling Hamiltonian $\mathcal{H}$. The weak value for an operator $\hat{A}$ is given by

$$A^w = \frac{\langle \pi | \hat{A} | s \rangle}{\langle \pi | s \rangle} \tag{2.21}$$

where $|s\rangle$ is the initial state of the system before the coupling and $|\pi\rangle$ is the post-selection state.

2.3 The duality principle in the presence of post-selection

In this section, we provide a framework for explaining apparent violations of the duality principle. We were motivated by the work of Menzel et al., who measured both high visibility and high which-alternative information in a single experiment [1]. At first glance, this appears to violate the duality principle. However, recent work has shown that this result was due to an unintentional violation of fair-sampling [21]. Fair-sampling is an assumption which states that the measurement results are representative of the system. In addition, we experimentally realize apparent violations of the duality principle in a controlled manner. These apparent violations are possible due to a fair-sampling-like loophole that can be enforced with post-selection.

The framework is very simple. We will take as our starting point the conditional duality principle,

$$\mathcal{V}_{\hat{\pi}}^2 + \mathcal{P}_{\hat{\pi}}^2 \leq 1. \tag{2.22}$$

Notice that both the visibility and predictability are conditioned on the same outcome $\hat{\pi}$. However, this does not need to be the case. We can choose to measure the visibility condi-

tioned on some outcome $\hat{\pi}_1$ and the predictability conditioned on some other outcome $\hat{\pi}_2$. In this case, if we put them together we get

$$\mathcal{V}^2_{\hat{\pi}_1} + \mathcal{P}^2_{\hat{\pi}_2} \leq 2. \tag{2.23}$$

The value of 2 comes from the fact that each of these quantities can individually reach 1. From this it is clear how apparent violations can occur. If one chooses $\hat{\pi}_1$ such that the measured visibility is large and if $\hat{\pi}_2$ is similarly chosen such that the measured predictability is large as well, the squared sum of these quantities may exceed 1. If care is not taken in explicitly showing the post-selections, this may appear as a violation of the duality principle. Of course, this is a violation of the fair-sampling criterion.

We now demonstrate this apparent violation of the duality principle by considering the coupling between two internal degrees-of-freedom of a single photon. In our setup, we produced the following coupled state for orbital angular momentum (OAM) and polarization of a photon:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|\ell\rangle|V\rangle + \sin\left(\frac{\theta}{2}\right)|-\ell\rangle\left(\cos\left(\frac{\alpha}{2}\right)|H\rangle + \sin\left(\frac{\alpha}{2}\right)|V\rangle\right), \tag{2.24}$$

where we use the subset $|\ell\rangle$ and $|-\ell\rangle$ to define the two dimensional Hilbert space of our qubit $\mathcal{Q}$. The polarization constitutes the environment $\mathcal{E} = \text{Pol}$ where $|V\rangle$ is the vertical polarization and $|H\rangle$ is the horizontal polarization. The density matrix for this state is given by $\hat{\Psi} = |\Psi\rangle\langle\Psi|$. The visibility and predictability of the state of the OAM when we ignore the polarization is given by $\mathcal{V} = |\sin(\alpha/2)\sin\theta|$ and $\mathcal{P} = |\cos\theta|$. The duality principle states that

$$\mathcal{V}^2 + \mathcal{P}^2 = \sin^2\left(\frac{\alpha}{2}\right)\sin^2\theta + \cos^2\theta \leq 1. \tag{2.25}$$

This is clearly correct for all values of θ and α.

Let us now make a post-selection on the polarisation and look at the resulting state of the OAM. We will use $\hat{\pi}_V = |V\rangle\langle V|$ and $\hat{\pi}_H = |H\rangle\langle H|$ as our two post-selection operators. In our experiment, we measure the visibility and the predictability of the OAM conditioned on a successful post-selection of the vertical and horizontal polarizations, respectively. These are given by

$$\mathcal{V}_{\hat{\pi}_V} = \frac{|\sin\theta\sin(\frac{\alpha}{2})|}{\cos^2(\frac{\theta}{2}) + \sin^2(\frac{\theta}{2})\sin^2(\frac{\alpha}{2})}, \tag{2.26}$$

$$\mathcal{P}_{\hat{\pi}_H} = 1. \tag{2.27}$$

Given that the visibility is a real positive number, the squared sum of these two quantities is clearly greater than or equal to 1. This is in apparent violation of the duality principle. However, we have clearly violated the fair-sampling criterion in order to do so. To include fair-sampling, one must take the averages of the visibility and predictability for all measurement outcomes. In our case, these are given by

$$\overline{\mathcal{V}} = |\sin\theta \sin(\alpha/2)|, \tag{2.28}$$

$$\overline{\mathcal{P}} = \sin^2(\theta/2)\cos^2(\alpha/2) + |\cos^2(\theta/2) - \sin^2(\theta/2)\sin^2(\alpha/2)|. \tag{2.29}$$

The sum of the squares of these quantities is indeed bounded by 1.

Let us now take a look at the setup for the experiment outlined above, see Figure 2.3. We first generate the OAM mode with $\ell = +3$ using a collimated HeNe laser and a spatial light modulator. We then send this through a polarizing beam splitter (PBS) and a half-wave plate to generate a beam in the state $|\ell\rangle \otimes [\cos(\theta/2)|V\rangle + \sin(\theta/2)|H\rangle]$. This state is sent into a Mach-Zehnder interferometer with a dove prism and a second half-wave plate with the H arm. This interferometer entangles the OAM to the polarization of the photon. The first and second half-wave plates control θ and α respectively. We then send this state through a PBS and measure the outputs with a standard CCD camera. This PBS projects the state onto the vertical and horizontal polarization states. Each of these output ports corresponds to a post-selection of the polarization. It is clear from our state, Eq. 2.24, that the horizontal polarization output is always composed of a single OAM mode and that the vertical polarization output is composed of some superposition of the two OAM modes defined by the parameters θ and α.

Figure 2.3(a) gives an example of a typical output measured by the CCD camera. To achieve an apparent violation of the duality principle, we measure the visibility and predictability of the vertical and horizontal polarization outputs of the PBS, respectively. The predictability of the output modes were determined by measuring the relative intensity contributions from each arm of the interferometer. The difference is these intensities gives $\mathcal{P}_{\hat{\pi}_H}$. Finally, we integrate the vertical polarization output radially and plot this as a function of the angle. The visibility of the interference fringes of this plot gives $\mathcal{V}_{\hat{\pi}_V}$, see Figure 2.3(b).

Our results are summarized in Figure 2.4. We plotted both $\mathcal{V}^2_{\hat{\pi}_V} + \mathcal{P}^2_{\hat{\pi}_H}$ and $\overline{\mathcal{V}}^2 + \overline{\mathcal{P}}^2$ as a function of θ for $\alpha = \pi/12$ (a) and as a function of α for $\theta = \pi/2$ (b). We see that apparent violations of the duality principle do occur for the post-selected measurements but do not occur for the average values. This is in agreement with our theoretical predictions. Note that we have an apparent violation of the duality principle for all non-separable states including weakly coupled states. In conclusion, we report the observation of both high visibility and

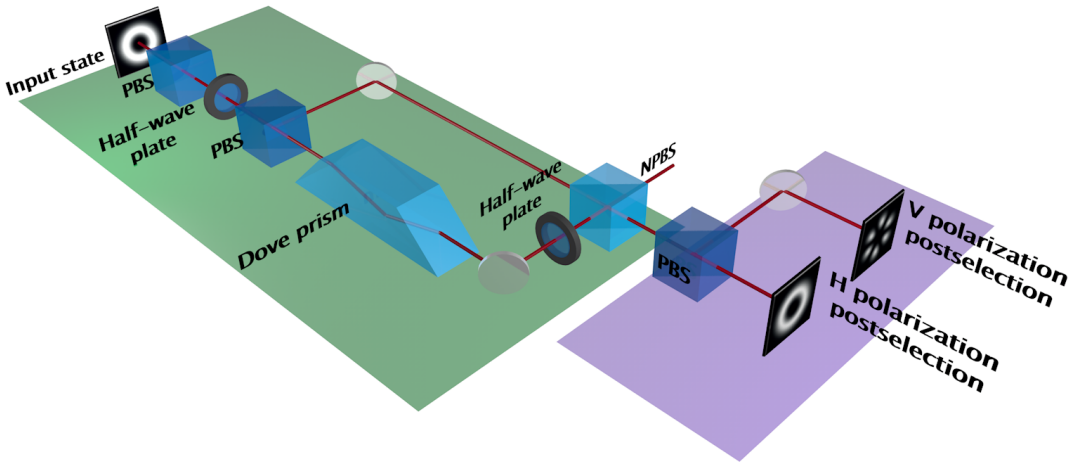

Figure 2.2: Our experimental setup can be split into two parts. The first, indicated in green, is the state preparation phase where the desired non-separable state is generated. The interferometer produces a coupling between the orbital angular momentum (OAM) and the polarization of the light passing through it. The second, indicated in purple, is the post-selection phase. Here we measure the outputs of a polarizing beam splitter (PBS). This PBS performs a post-selection on the polarization. The input to the interferometer is generated by a HeNe laser and a spatial light modulator (not shown). The outputs of the final PBS were measured with a CCD camera.

high predictability originating from measurements on a single system without violating the duality principle. We've also developed a framework to explain apparent violations of the duality principle, one of the building blocks of quantum mechanics.

2.4 Relation to weak-values

In the previous section, we have seen that the duality principle can appear to be violated even for weakly coupled states with the use of post-selection. In brief, if one measures the visibility with respect to a particular post-selection and measures the predictability with respect to another, then the sum of the squares of these quantities can exceed the limit of 1 prescribed by the duality principle. This is called a fair-sampling violation and falls completely within the scope of standard quantum mechanics. This motivated us to investigate the connection between weak values and the duality principle.

In this section, we consider a *system* S that is weakly coupled to some *pointer* P through some interaction Hamiltonian. The pointer is equivalent to the environment from the previous sections. Our goal is to find the visibility and predictability of the system in terms of

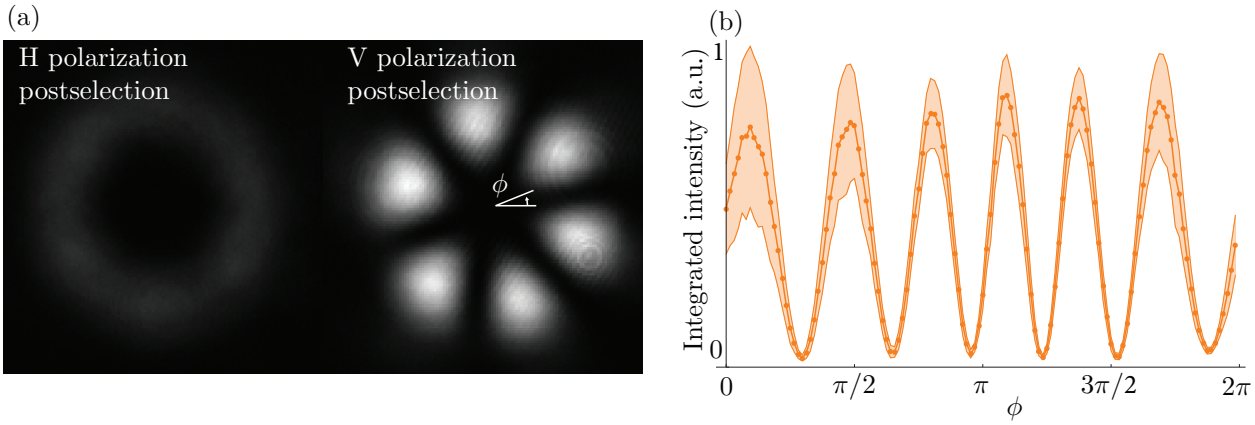

Figure 2.3: This figure demonstrates the method used to measure the visibility of the post-selected states. (a) A typical image of the post-selected outputs. The H polarization post-selection is given by a very faint $\ell = -3$ mode due to its low post-selection probability. This image has a high predictability of $\mathcal{P}_{\hat{\pi}_H} = 0.98$. The V polarisation post-selection, is a superposition of $\ell = -3$ and $\ell = +3$ modes. The visibility of this output is $\mathcal{V}_{\hat{\pi}_V} = 0.93$. This value is calculated by azimuthally integrating the intensity pattern and measuring the visibility of the resulting fringes (b). Each data point (given in arbitrary units, a.u., since the scaling is not important) corresponds to the average intensity in a 3° angular window. The shaded region indicates the error band, which is at one σ. The value of $\mathcal{V}^2_{\hat{\pi}_V} + \mathcal{P}^2_{\hat{\pi}_H}$ is equal to 1.83.

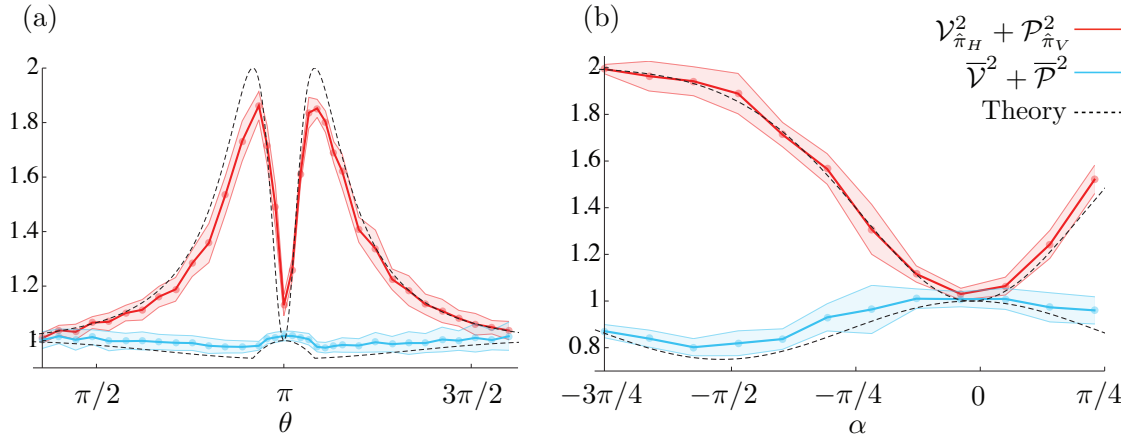

Figure 2.4: This figure is a summary of the results of the experiment. (a) We scan over multiple inputs θ with a fixed coupling parameter $\alpha = \pi/12$. (b) We scan over the coupling parameter α with a fixed $\theta = \pi/2$. These results show that if care is not taken in the measurement process, the visibility and predictability may be measured with respect to different post-selections leading to an apparent violation of the duality principle (red curve). When we take an average over all possible post-selections, no violation occurs (blue curve). For the plots given above, the error band is at one σ.

the weak values of this interaction Hamiltonian.

Let us start with a system qubit whose states are elements of the Hilbert space $\mathcal{H}_S$. Similarly, a pointer qubit (or environment) can be described by the Hilbert space $\mathcal{H}_P$. Note that the pointer does not necessarily need to be a qubit. However, due to the Schmidt decomposition, we can treat it as such for simplicity. Initially their joint state is separable, $|s,p\rangle$, however a coupling is created from an interaction. This interaction is governed by the Hamiltonian $\hat{U} = \exp\left(-i\frac{\alpha}{2}\hat{J}\right)$ where α is the coupling parameter which determines the strength of the interaction and $\hat{J}$ is the coupling operator which determines the nature of the interaction. This Hamiltonian is a generating function and therefore can be expanded as a power series. For weak coupling (small values of α), we can keep the first two terms and ignore higher powers of α. Doing this gives us the weak coupling Hamiltonian $\hat{H} = \hat{\mathbb{1}} - i\frac{\alpha}{2}\hat{J}$. We can rewrite this as $\hat{H} = \hat{\mathbb{1}} - it\hat{A}\otimes\hat{B}$ where $\hat{A}$ and $\hat{B}$ are the local parts of the Hamiltonian acting on the system and the pointer respectively and $t = \frac{\alpha}{2}$ is the weak coupling parameter. The (unnormalized) joint state after a weak coupling interaction can be written as

$$|\psi_{SP}\rangle = |s,p\rangle - it\,\hat{A}\otimes\hat{B}|s,p\rangle. \tag{2.30}$$

The conditional visibility and predictability of the system S are given by

$$\mathcal{V}_{\hat{\pi}} = \frac{|\langle\psi_{SP}|(\hat{\sigma}_x + i\hat{\sigma}_y)\otimes\hat{\pi}|\psi_{SP}\rangle|}{\langle\psi_{SP}|\pi\rangle\langle\pi|\psi_{SP}\rangle}, \tag{2.31}$$

$$\mathcal{P}_{\hat{\pi}} = \frac{|\langle\psi_{SP}|\hat{\sigma}_z\otimes\hat{\pi}|\psi_{SP}\rangle|}{\langle\psi_{SP}|\pi\rangle\langle\pi|\psi_{SP}\rangle}, \tag{2.32}$$

where $\hat{\sigma}_x + i\hat{\sigma}_y = 2|0\rangle\langle 1|$. Here $|0\rangle$ and $|1\rangle$ are the two alternatives of the system S. Note that we can still ignore the normalization of $|\psi_{SP}\rangle$ because it is in both the numerator and denominator. By substituting the definition of $|\psi_{SP}\rangle$, Eq. 2.30, into the above equations and dividing both the numerator and denominator by $\langle\pi|p\rangle\langle p|\pi\rangle$, we get the final result directly:

$$\mathcal{V}_{\hat{\pi}} = \frac{\mathcal{V}\left|1 - it\,(A_1^w B^w - A_0^{w*}B^{w*}) + t^2\,A_1^w A_0^{w*}\,|B^w|^2\right|}{1 + 2t\langle\hat{A}\rangle\,\mathrm{Im}\,[B^w] + t^2\langle\hat{A}^2\rangle|B^w|^2}, \tag{2.33}$$

$$\mathcal{P}_{\hat{\pi}} = \frac{\left|\tilde{\mathcal{P}} + 2t\,\mathrm{Im}\left[\langle\hat{\sigma}_z\hat{A}\rangle B^w\right] + t^2\langle\hat{A}\hat{\sigma}_z\hat{A}\rangle|B^w|^2\right|}{1 + 2t\langle\hat{A}\rangle\,\mathrm{Im}\,[B^w] + t^2\langle\hat{A}^2\rangle|B^w|^2}, \tag{2.34}$$

where $\tilde{\mathcal{P}} = \langle\hat{\sigma}_z\rangle$, $\mathcal{V} = |\langle\hat{\sigma}_x + i\hat{\sigma}_y\rangle|$, $B^w = \frac{\langle\pi|\hat{B}|p\rangle}{\langle\pi|p\rangle}$, and $A_j^w = \frac{\langle j|\hat{A}|s\rangle}{\langle j|s\rangle}$. B^w is nothing else than the weak value of $\hat{B}$ with respect to the initial state $|p\rangle$ and the final state $|\pi\rangle$. Similarly, A_j^w is the weak value of $\hat{A}$ with respect to the initial state $|s\rangle$ and final state $|j\rangle$. Note that we wrote $\mathcal{V}_{\hat{\pi}}$ and $\mathcal{P}_{\hat{\pi}}$ in terms of weak values of $\hat{A}$ but no post-selection is ever made on the

system at any point. Also note that the expectation values with $\hat{\sigma}_z$ were not expanded for clarity. These expectation values can be expanded as follows:

$$\langle \hat{A} \rangle = A_0^w |\alpha_0|^2 + A_1^w |\alpha_1|^2, \tag{2.35}$$

$$\langle \hat{A}^2 \rangle = |A_0^w|^2 |\alpha_0|^2 + |A_1^w|^2 |\alpha_1|^2, \tag{2.36}$$

$$\langle \hat{\sigma}_z \hat{A} \rangle = A_0^w |\alpha_0|^2 - A_1^w |\alpha_1|^2, \tag{2.37}$$

$$\langle \hat{A} \hat{\sigma}_z \hat{A} \rangle = |A_0^w|^2 |\alpha_0|^2 - |A_1^w|^2 |\alpha_1|^2, \tag{2.38}$$

where $\alpha_j = \langle j|s\rangle$.

Above, we have found the conditional visibility $\mathcal{V}_{\hat{\pi}}$ and predictability $\mathcal{P}_{\hat{\pi}}$ of the system S for a weak coupling Hamiltonian. Again, this Hamiltonian was found by taking the first two terms in the generating function $\hat{U} = \exp\left(-i\frac{\alpha}{2}\hat{J}\right)$ where $\hat{J} = \hat{A} \otimes \hat{B}$ and $t = \alpha/2$. This method of expansion can only be done for weak coupling. Applying the complete generating function would give us the joint state of S and P for arbitrary coupling strengths. This is not generally possible. However, for the special case where $\hat{A}$ is a projector and $\hat{B}$ is a Pauli matrix, the exact conditional visibility and predictability can be calculated for arbitrary interaction strength. This is due to the following properties of the Hamiltonian $\hat{J} = \hat{A} \otimes \hat{B}$:

$$\begin{aligned} \hat{J}^0 &= \hat{\mathbb{1}} \otimes \hat{\mathbb{1}}, \\ \hat{J}^{2n} &= \hat{A} \otimes \hat{\mathbb{1}}, \\ \hat{J}^{2n+1} &= \hat{A} \otimes \hat{B}, \end{aligned} \tag{2.39}$$

where n is an integer larger than 0. This leads to

$$\begin{aligned} \hat{U}(\alpha) &= \exp\left(-i\frac{\alpha}{2}\hat{J}\right) \\ &= \sum_{n=0}^{\infty} \frac{\left(-i\frac{\alpha}{2}\hat{J}\right)^n}{n!} \\ &= \hat{\mathbb{1}} - \hat{A} \otimes \hat{\mathbb{1}} + \underbrace{\sum_{n=0}^{\infty} \frac{\left(-i\frac{\alpha}{2}\right)^{2n}}{2n!}}_{\cos\frac{\alpha}{2}} \hat{A} \otimes \hat{\mathbb{1}} + \underbrace{\sum_{n=0}^{\infty} \frac{\left(-i\frac{\alpha}{2}\right)^{2n+1}}{(2n+1)!}}_{-i\sin\frac{\alpha}{2}} \hat{A} \otimes \hat{B} \\ &= \hat{\mathbb{1}} + (\cos\frac{\alpha}{2} - 1)\hat{A} \otimes \hat{\mathbb{1}} - i\sin\frac{\alpha}{2}\hat{A} \otimes \hat{B}, \end{aligned} \tag{2.40}$$

and finally

$$
\begin{aligned}
|\psi_{SP}\rangle &= \hat{U}(\alpha)|s,p\rangle \\
&= \left[\hat{\mathbb{1}} + (\cos\frac{\alpha}{2} - 1)\hat{A}\otimes\hat{\mathbb{1}} - i\sin\frac{\alpha}{2}\hat{A}\otimes\hat{B}\right]|s,p\rangle. \qquad (2.41)
\end{aligned}
$$

Substituting this state into the definitions of the conditional visibility and predictability given above (2.31 and 2.32) and dividing the numerator and denominator by $\langle\pi|p\rangle\langle p|\pi\rangle$, we get

$$\mathcal{V}_{\hat{\pi}} = \frac{\mathcal{V}\left|\left(1 + D_\alpha^{w*}A_1^{w*}\right)\left(1 + D_\alpha^{w}A_2^{w}\right)\right|}{1 + \left(\left|D_\alpha^w + 1\right|^2 - 1\right)\langle\hat{A}\rangle} \qquad (2.42)$$

$$\mathcal{P}_{\hat{\pi}} = \frac{\left|\tilde{\mathcal{P}} + 2\mathrm{Re}\left[D_\alpha^w\langle\hat{\sigma}_z\hat{A}\rangle\right] + \left|D_\alpha^w\right|^2\langle\hat{A}\hat{\sigma}_z\hat{A}\rangle\right|}{1 + \left(\left|D_\alpha^w + 1\right|^2 - 1\right)\langle\hat{A}\rangle} \qquad (2.43)$$

where $D_\alpha^w = \cos\frac{\alpha}{2} - i\sin\frac{\alpha}{2}B^w - 1$. It is clear from these equations that if the system and pointer are uncorrelated, $\alpha = 0$, then the visibility and predictability that are observed are those measured while ignoring the pointer. This is due to the fact that for $\alpha = 0$, we have $D_\alpha^w = 0$.

In summary, we have derived the conditional visibility and predictability of a qubit in terms of the weak value of the coupling Hamiltonian for general weak couplings. We also derive these quantities for a coupling of arbitrary strength for coupling operators of the form $\hat{\Pi}\otimes\hat{\sigma}$ where $\hat{\Pi}$ is a projector and $\hat{\sigma}$ is a Pauli matrix. This is an important building block between the duality principle and generalized measurements.

2.5 Relation to the sub-fidelity

In this section, we will look at the problem of quantum erasure with minimal access to the environment. In other words, we wish to recover the coherence of our qubit $\mathcal{Q}$ which is entangled with an environment of which we only have access to a two-dimensional subspace $\mathcal{A}$, see Figure 2.5. The rest of the environment $\mathcal{I}$ is inaccessible. This is closely related to quantum steering [23] , see Figure 2.6. In this scenario, we have two parties, Alice and Bob, sharing an entangled qubit pair. Alice wishes to set a preferred basis for Bob's qubit $\mathcal{Q}$ by making a measurement on her qubit $\mathcal{A}$. This setting of a preferred basis is what Einstein referred to as 'spooky action at a distance'. In our case, the preferred basis would be a high visibility basis. An example of such a basis would be the diagonal and anti-diagonal basis for polarization.

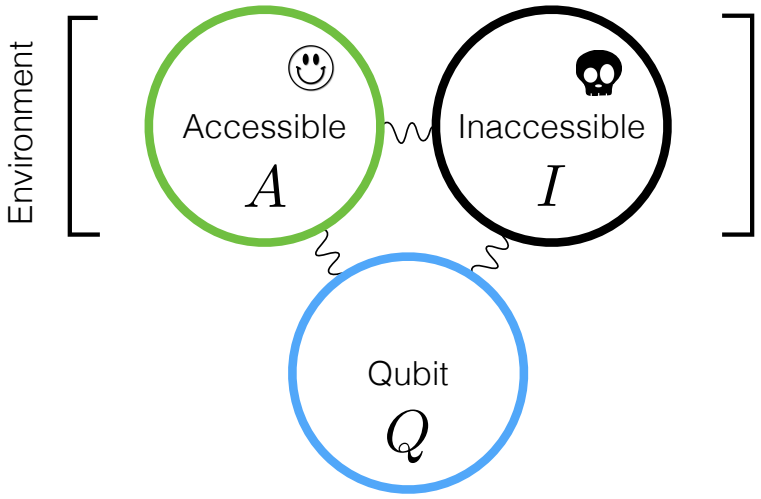

Figure 2.5: This schematic provides a visual representation of the type of system we are considering. The environment (upper circles) is split into an accessible subspace $\mathcal{A}$ and an inaccessible subspace $\mathcal{I}$. The squiggly lines represent the possible interaction and subsequent coupling between the different parts. We wish to perform quantum erasure and restore coherence in $\mathcal{Q}$ by acting solely on the accessible subspace $\mathcal{A}$.

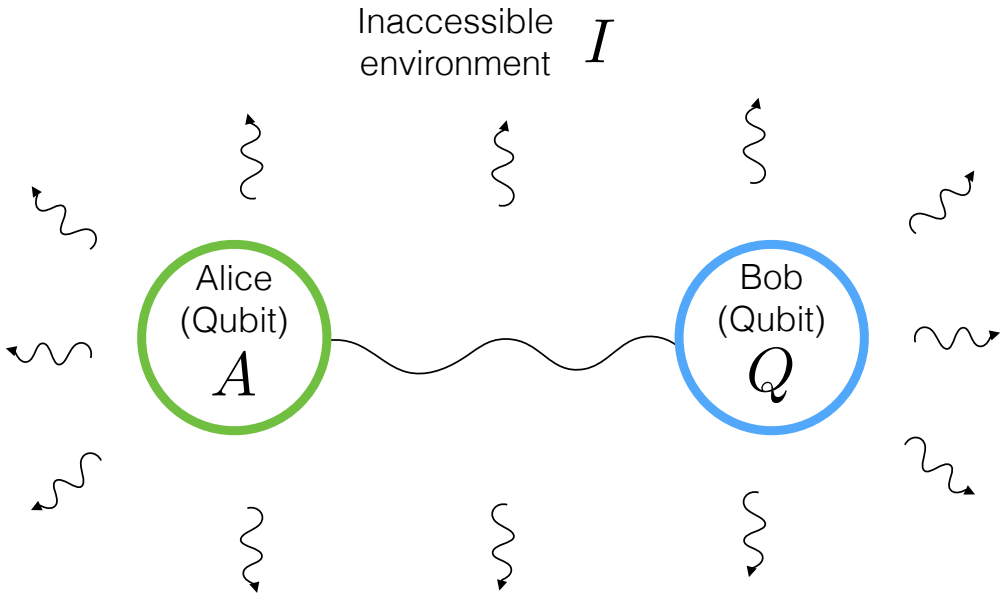

Figure 2.6: This schematic provides an alternative scenario for the system given above. Here Alice wishes to perform quantum steering on the state of Bob's qubit $\mathcal{Q}$ while some information about the joint system $\mathcal{AQ}$ could leak to an inaccessible environment.

Before deriving the main result, let us first look at the trivial case of quantum erasure when we do not have any access to the environment. Here we can write the joint state as

$|\psi\rangle = \alpha|0, e_0\rangle + \beta|1, e_1\rangle$, where $|e_0\rangle$ and $|e_1\rangle$ are the states of the environment conditioned on the state of the qubit. The coherence of this qubit $\mathcal{C}_1$ is given by the visibility $\mathcal{V}$:

$$\mathcal{C}_1 = \mathcal{V} = 2|\alpha\beta^*\langle e_0|e_1\rangle| = 2\sqrt{p_0 p_1 F(\hat{\psi}_{\mathcal{E}|0}, \hat{\psi}_{\mathcal{E}|1})}, \tag{2.44}$$

where $p_0 = |\alpha|^2$ and $p_1 = |\beta|^2$ are the probabilities of finding $\mathcal{Q}$ in the state $|0\rangle$ and $|1\rangle$ respectively. $\hat{\psi}_{\mathcal{E}|k} = |e_k\rangle\langle e_k|$ is the pure state of the environment conditioned on the state of $\mathcal{Q}$. $F(x, y) = \mathrm{Tr}(x^\dagger y)$ is the Hilbert-Schmidt inner product.

Let us now look at the case where we have access to a two-dimensional subspace of the environment. In this case, we can write the coherence as

$$\mathcal{C}_2 = 2\mathrm{Tr}|\hat{X}_{\mathcal{A}}|, \tag{2.45}$$

where $\hat{X}_{\mathcal{A}} = \mathrm{Tr}_{\mathcal{QI}}\left([(\hat{\sigma}_x + i\hat{\sigma}_y) \otimes \hat{\mathbb{1}}_{\mathcal{A}} \otimes \hat{\mathbb{1}}_{\mathcal{I}}]\hat{\rho}_{\mathcal{QAI}}\right)$. This differs from our original definition of $\hat{X}_{\mathcal{A}}$, Eq. 2.19, by tracing out the inaccessible environment $\mathcal{I}$. The subscript of 2 is to indicate that we only have access to 2 dimensions of the environment. After a bit of algebra (see the Appendix), we get the final result

$$\mathcal{C}_2 = 2\sqrt{p_0 p_1 E(\hat{\psi}_{\mathcal{I}|0}, \hat{\psi}_{\mathcal{I}|1})} \tag{2.46}$$

where $\hat{\psi}_{\mathcal{I}|k}$ is the state of the inaccessible environment conditioned on the qubit and $E(\hat{\psi}_{\mathcal{I}|0}, \hat{\psi}_{\mathcal{I}|1})$ is the sub-fidelity of these states. The sub-fidelity gives a lower bound to Uhlmann's fidelity and is defined as $E(x, y) = \mathrm{Tr}(xy) + \sqrt{2}\sqrt{[\mathrm{Tr}(xy)]^2 - \mathrm{Tr}(xyxy)}$ [22].

The method used to derive Eq. 2.46 can, in principle, be extended to larger dimensions of the accessible environment $\mathcal{A}$. From Eqs. 2.44 and 2.46, we conjecture that the form of $\mathcal{C}_a$ for higher dimensions is given by

$$\mathcal{C}_a = 2\sqrt{p_0 p_1 F_a(\hat{\psi}_{\mathcal{I}|0}, \hat{\psi}_{\mathcal{I}|1})}, \tag{2.47}$$

where the functions F_a involve only traces of products of $\psi_{\mathcal{I}|0}$ and $\psi_{\mathcal{I}|1}$. These functions give a measure of the overlap between the conditional states of the environment while also taking into account the number of dimensions of $\mathcal{A}$. In other words, they give a measure of the amount of information that the environment $\mathcal{I}$ has about the qubit $\mathcal{Q}$.

In summary, we have investigated the effects of decoherence on quantum steering. Decoherence dissipates information about a qubit to the environment. By making an appropriate measurement on this environment, it is possible to erase this information and recover coherence. We found that the maximum recoverable coherence is proportional to the sub-fidelity

of the states of the environment conditioned on the qubit. This provides the first operational interpretation of sub-fidelity. This suggests that the sub-fidelity is more than just a lower bound on Uhlmann's fidelity. Finally, we provide a conjecture as to the form of the coherence with increased access to the environment.

2.6 Quantum erasure with partial access to the environment

In this final section on the duality principle, we will be looking at the maximum recoverable coherence of a qubit when we only have partial access to the environment with which it is entangled. This is an extension of the problem given in the previous section to higher dimensions. However, instead of looking for an exact solution, we will be looking at the statistical average of the coherence for all possible states. We will show that this statistical average is a good representation of the ensemble for large environments.

Consider the following, we have a qubit $\mathcal{Q}$ embedded in an AK-dimensional environment with Hilbert space $\mathcal{A}\otimes\mathcal{I}$. This environment is divided into two parts: an accessible subspace $\mathcal{A}$ of dimension A and an inaccessible subspace $\mathcal{I}$ of dimension K. The pure states of this system are sampled uniformly in a Hilbert space $\mathcal{Q}\otimes\mathcal{A}\otimes\mathcal{I}$ of dimension $2AK$. Since $\mathcal{I}$ is inaccessible, we must trace this away. This leaves us with a $2A$-dimensional state in $\mathcal{Q}\otimes\mathcal{A}$ which can always be written as a $2A\times 2A$ density matrix:

$$\hat{\rho} = \begin{pmatrix} \hat{R}_0 & \hat{X} \\ \hat{X}^\dagger & \hat{R}_1 \end{pmatrix}, \tag{2.48}$$

where $\mathrm{Tr}(\hat{R}_0)$ and $\mathrm{Tr}(\hat{R}_1)$ are the probabilities of measuring the qubit in the alternatives $|0\rangle$ and $|1\rangle$, respectively, and $\hat{X}$ is the cross-term. The largest visibility of $\mathcal{Q}$, the coherence, that can be recovered with an optimal measurement of $\mathcal{A}$ is given by twice the trace norm of the cross-term $\hat{X}$: $\mathcal{C} = 2\mathrm{Tr}|\hat{X}|$. Again, this differs from Eq. 2.19 by a partial trace over $\mathcal{I}$. The trace norm of $\hat{X}$ is given by the sum of the square root of the A eigenvalues of the matrix $\hat{X}^\dagger\hat{X}$:

$$\mathrm{Tr}|\hat{X}| = \sum_{i=1}^{A} \sqrt{\lambda_i(\hat{X}^\dagger\hat{X})}. \tag{2.49}$$

Due to the trace over $\mathcal{I}$, the ensemble of states $\hat{\rho}$ in $\mathcal{Q}\otimes\mathcal{A}$ is not uniformly distributed. They are distributed according to the induced trace measure $P_{2A,K}(\hat{\rho})$. This is a Ginibre ensemble [29]. Sampling from this ensemble can be done by generating a $2A\times K$ complex

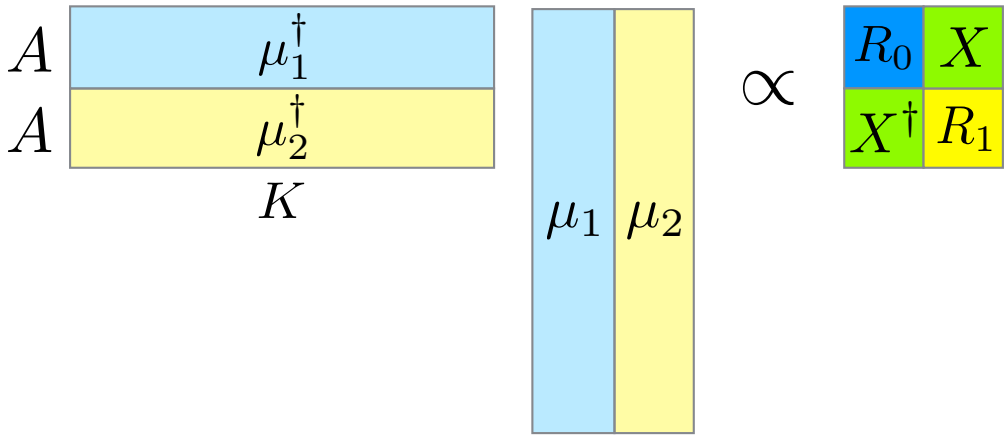

Figure 2.7: Here we show a visual representation of the matrix multiplication $\mu^\dagger\mu$. However, we are only interested in the $A \times A$ cross-term X which is proportional to the product between two independent random matrices μ_1 and μ_2 that make up μ.

Gaussian random matrix μ (with entries sampled from the complex normal distribution centred on the origin and with unit variance) and then building the $2A \times 2A$ density matrix

$$\hat{\rho} = \frac{\mu^\dagger\mu}{\mathrm{Tr}(\mu^\dagger\mu)}. \tag{2.50}$$

However, since we are only interested in calculating $\mathcal{C}$, which depends only on the $A \times A$ cross-term $\hat{X}$, we do not require the whole matrix $\hat{\rho}$.

From Figure 2.7, we see that $\hat{X}$ is proportional to the product $M = \mu_1^\dagger\mu_2$ of two independent $A \times K$ complex Gaussian random matrices μ_1 and μ_2. Recall that we are interested in the average value of $\mathcal{C}$. The proportionality factor is therefore given by the average value of the denominator in 2.50: $\langle \mathrm{Tr}(\mu^\dagger\mu)\rangle = 4AK$.

Let us now turn our attention to finding the average of $\mathrm{Tr}|M|$. We do this through the use of the moments m_ℓ of the marginal distribution for the eigenvalues of M. Specifically, the average square root of the eigenvalues of M is given by the moment of order $\ell = 1/2$. Therefore, we have $\langle \mathrm{Tr}|M|\rangle = Am_{\frac{1}{2}}$. We can compute this moment by applying Equation 57 of Ref. [30] to our matrices. We find

$$m_{\frac{1}{2}} = \frac{4\pi^{5/2}(-1)^K\, {}_4\tilde{F}_3\left(\begin{matrix}\frac{1}{2},1-A,1-A,1-K\\ \frac{1}{2}-A,\frac{1}{2}-A,\frac{1}{2}-K\end{matrix}\middle|1\right)}{A!\,\Gamma(A)\Gamma(K)} \tag{2.51}$$

where the function ${}_4\tilde{F}_3$ is a regularized Hypergeometric function. We therefore have that the

average coherence $\langle \mathcal{C} \rangle$ is given by

$$\langle \mathcal{C} \rangle = 2\langle \mathrm{Tr}|\hat{X}| \rangle = 2\frac{\langle \mathrm{Tr}|M| \rangle}{4AK} = \frac{m_{\frac{1}{2}}}{2K}. \tag{2.52}$$

Let us now look at a few examples. We evaluate Eq. 2.52 explicitly for several values of A. In addition, we also show the behaviour of these solutions for $K \to \infty$ and for $1 \leq K \leq A$.

Let us first consider the case where we have no control over the environment. This is equivalent to having no accessible environment ($A = 1$). We find that

$$\langle \mathcal{C}_1 \rangle = \frac{\pi^{3/2}(-1)^K}{2K!\Gamma\left(\frac{1}{2} - K\right)} \sim \frac{\sqrt{\pi}}{2\sqrt{K}} \quad (\text{as } K \to \infty) \tag{2.53}$$

Therefore, the visibility scales like $\mathcal{O}(1/\sqrt{K})$ at a rate of $\sqrt{\pi}/2$. Let's now consider the case where we have an accessible environment $\mathcal{A}$. Specifically, we will be looking at the case of a two- and three-dimensional $\mathcal{A}$. Setting $A = 2$ and $A = 3$ into equation 2.52 gives us

$$\langle \mathcal{C}_2 \rangle = \frac{\pi^{3/2}(-1)^K(13 - 22K)}{32K!\Gamma\left(\frac{3}{2} - K\right)} \sim \frac{11\sqrt{\pi}}{16\sqrt{K}} \ (\text{as } K \to \infty), \tag{2.54}$$

$$\langle \mathcal{C}_3 \rangle = \frac{(-1)^K\pi^{3/2}(433 - 936K + 428K^2)}{512K!\Gamma\left(\frac{5}{2} - K\right)} \sim \frac{107\sqrt{\pi}}{128\sqrt{K}} \quad (\text{as } K \to \infty). \tag{2.55}$$

We can keep going for even larger accessible spaces. These examples suggest that the high-K scaling is always $\mathcal{O}(1/\sqrt{K})$. Let us now look at the scaling for low values of K. We find a linear behaviour

$$\langle \mathcal{C} \rangle = 1 - \frac{K}{4A} \qquad 0 \leq K \leq A. \tag{2.56}$$

A transition away from this linear behaviour occurs rather sharply at $A = K$. In Figure 2.8, we show an explicit example of these behaviours with $A = 100$.

As our final example, let's consider a qubit $\mathcal{Q}$ immersed in an environment composed of n other qubits where a qubits are accessible and the remaining $k = n - a$ are not, see Figure 2.9. In this scenario, we have $A = 2^a$ and $K = 2^{n-a}$. In Figures 2.10 and 2.11, we plot the average coherence $\langle \mathcal{C} \rangle$ as we gain access to more and more environment qubits. From these plots, we see that $\langle \mathcal{C} \rangle$ is close to 0 when we have access to less than half the environment qubits $a \lesssim k$ and transitions quickly to 1 as the number of accessible qubits grows beyond this point $a \gtrsim k$.

We must now ask ourselves the following question: How typical is the value of $\langle \mathcal{C} \rangle$? In other words, is this representative of the majority of the states in the ensemble. To get an

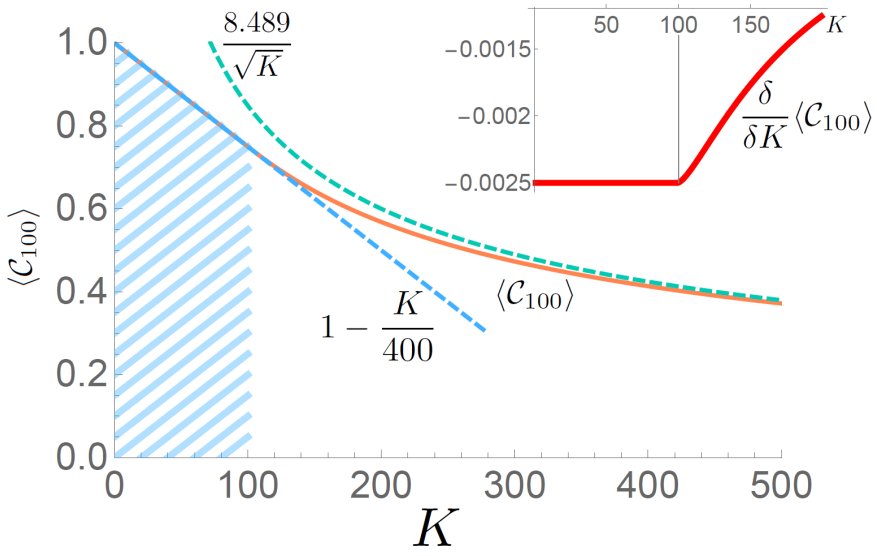

Figure 2.8: Here we show the behaviour of the average coherence $\langle \mathcal{C} \rangle$ as a function of K for $A = 100$. For values of K up to $K = A$, the behaviour of $\langle \mathcal{C} \rangle$ is purely linear ($1 - \frac{K}{4A}$, see inset). For $K > A$ the behaviour changes dramatically and is asymptotic to $\mathcal{O}(1/\sqrt{K})$. The shading indicates the linear region.

idea of this, we generated thousands of random states for a qubit embedded in environments with n ranging from 3 to 11. The results are plotted in Figure 2.10. From them, it is clear that $\langle \mathcal{C} \rangle$ becomes a typical property of the ensemble because they fall closer and closer to $\langle \mathcal{C} \rangle$. Note that we do not need large environments for $\langle \mathcal{C} \rangle$ to become a typical property of the ensemble. With only a handful of qubits, the 99th percentile is squeezed around the mean.

In summary, we have looked at the behaviour of the average recoverable visibility, the coherence, for qubits embedded in environments to which we only have partial access. In other words, we can only make measurements on a subspace of the total environment. We find that the average coherence increases sharply form 0 to 1 once we have access to half of the environment. We have also found the behaviours for this quantity when we have access to less than half the qubits and for very large inaccessible environments. Finally, we show that the average becomes a typical representation for the entire ensemble for large environments. As with previous sections, this is further expanding on the relation between the duality principle and generalized measurements.

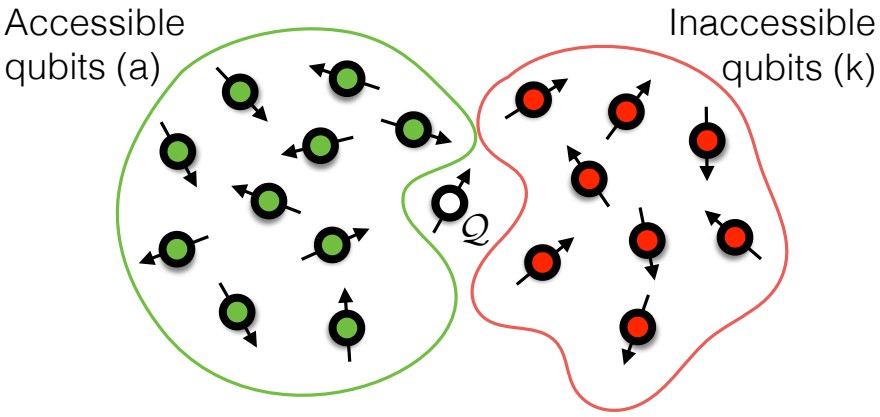

Figure 2.9: This schematic is a visual representation of the final scenario we will be considering. Here we have a qubit $\mathcal{Q}$ within an environment comprising n other qubits where a of them are accessible. The remaining $k = n - a$ are inaccessible. This can be viewed as a generalization of the scenario given in Figure 2.5.

2.7 Conclusions

In summary, the duality principle is one of the most important statements about quantum mechanics. It is one of the most striking examples of limited behaviours in physics. In this thesis chapter, we have explored the duality principle in detail for a multitude of different scenarios. We provided a framework to explain apparent violations of the duality principle and we demonstrated this experimentally. These apparent violations are due to the measurement of the visibility and predictability with respect to different post-selections.

We also provide the first operational interpretation of the sub-fidelity as a function of the maximum recoverable visibility of a qubit while only having access to a two-dimensional sub-space of the environment. We derived the visibility and predictability of a qubit in terms of the weak values describing its coupling with the environment. These equations are applicable even for large degrees of coupling. Finally, we show that there is a sharp transition in the maximum recoverable visibility from 0 to 1 when we have access to approximately half of the environment to which the qubit is coupled.

This work has contributed much to this topic. However, much work is still left to be done in this field. For instance, very little is known about duality for quantum systems with Hilbert spaces of dimensionality larger than 2. This future work would give us new tools to deal with high-dimensional quantum systems. In addition, much work is left to be done with the predictability. It is largely underdeveloped in comparison to the visibility.

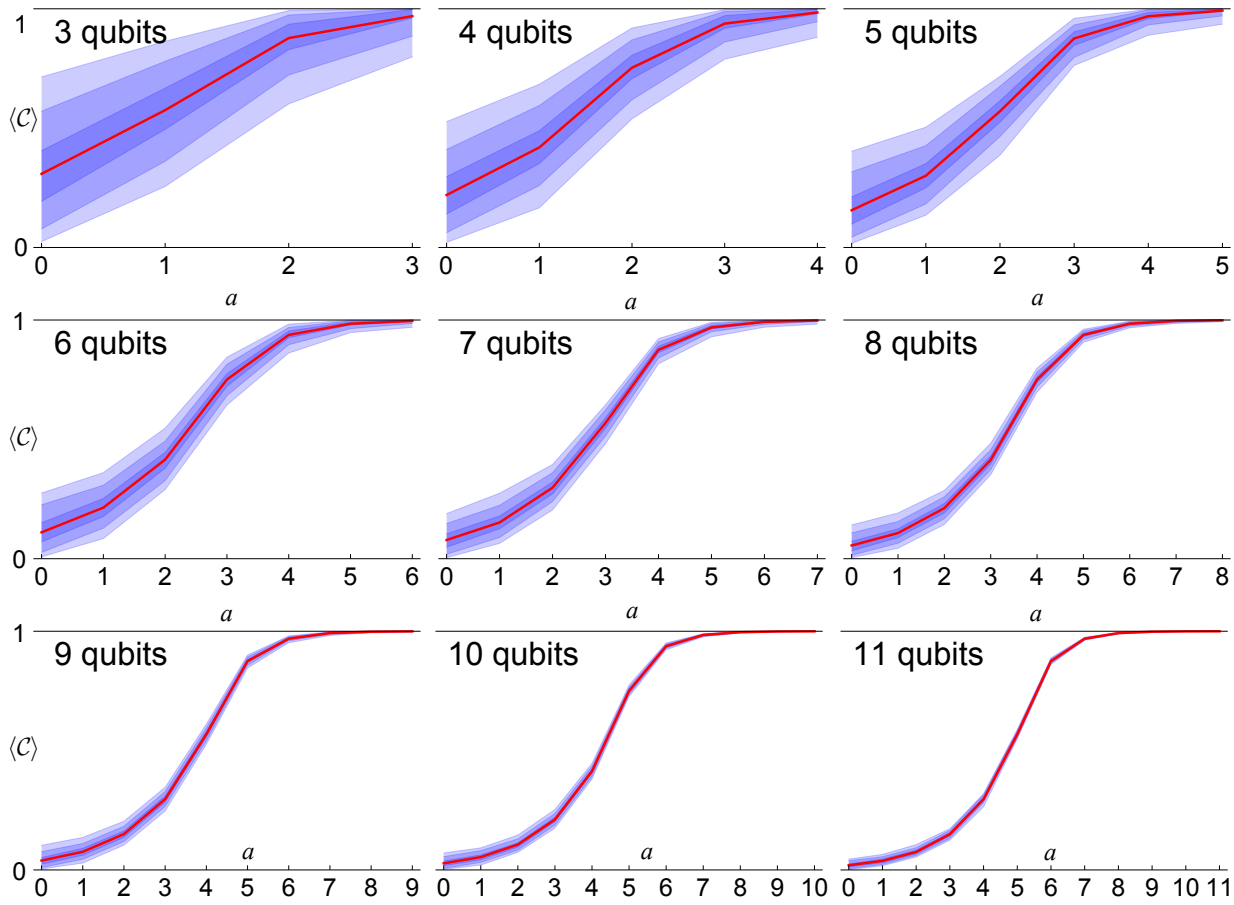

Figure 2.10: Here we provide several graphs showing the average recoverable coherence $\langle \mathcal{C} \rangle$ of a qubit $\mathcal{Q}$ as a function of the number a of environment qubits that we can control. The total number of environment qubits n is displayed on each graph. There is a clear transition from no recoverable coherence to perfectly recoverable coherence. This transition occurs when we gain access to approximately half of the environment. All of these plots range from 0 to 1 and the blue regions show the 50, 90 and 99 percentiles around the mean (red line). Notice that the mean becomes a better representation of the whole ensemble as we increase the total number of qubits n.

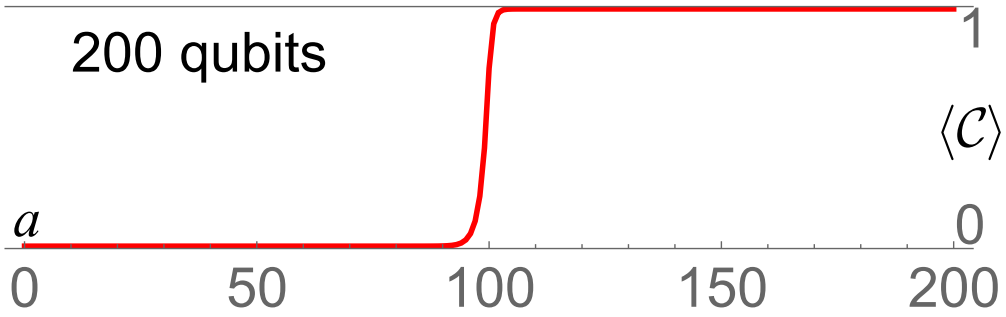

Figure 2.11: Here we show the average recoverable coherence $\langle \mathcal{C} \rangle$ of a qubit $\mathcal{Q}$ as a function of the number of accessible environment qubits a where the environment is comprised of a total of $n = 200$ qubits. We see an incredibly sharp transition from 0 to 1 when one has access to more than half of the environment qubits. The percentiles for this graph as not shown as the mean gives a very good representation for the whole ensemble of states.

Chapter 3

Novel protocol for delegated quantum computation

The previous chapter of this thesis focused on topics involving fundamental quantum mechanics. Specifically, we have looked at phenomena involving entanglement. We now turn our attention to the related field of quantum information [31]. Quantum computers, which are an application of quantum information, promise to revolutionize computing by providing increased performance and allowing to solve problems that were previously impossible to solve [32, 33]. For example, they would allow us to simulate quantum systems [34, 35]. However, practical applications of quantum computing are still in their infancy and the first quantum computers are very likely going to be expensive and not widely available. This will lead to a delegated scheme similar to those of modern super-computers where a remote client would like to query a quantum server. In other words, a client (often named Alice) wishes to delegate a complex quantum computation which it cannot perform itself to a powerful quantum server (often named Bob). Such delegated schemes are of interest to the scientific community for several reasons, one of which was mentioned above: the first quantum computers will be utilizing such schemes. Another reason is that these schemes pose some interesting questions. For example, is it possible for the client to delegate a computation without the server ever finding out what the inputs and outputs are or even what the computation is? As it turns out, such a scheme is possible and one protocol of achieving this is called blind quantum computing (BQC) [36]. Another protocol for delegated quantum computing is called quantum computing on encrypted data (QCED) [37]. This protocol keeps the input and output perfectly secure. However, unlike BQC, it does not keep the computation a secret.

The *quantum power* of a party in a protocol can be viewed as its ability to generate, manipulate and measure quantum particles such as qubits. A complete theoretical description

of quantum power has yet to be developed and our work can be viewed as a first step towards this. In recent work, it was shown that a purely classical client cannot delegate a quantum computation to a quantum server with information theoretic security [38]. At the other end of the spectrum, we have a quantum client that has infinite quantum power. In this case, no delegation is required as the client can perform the computation on its own. More interesting cases fall in-between these two extremes and one example is QCED. This continues our overall theme of limited behaviours in physics. In this scenario, we have a trade-off between the quantum power required on the client's side and the security of the protocol. Once a certain threshold in quantum power is reached, information theoretic security is achievable and additional quantum power is not necessary. Here we concern ourselves with finding this threshold. In other words, how 'classical' can a client be before it starts losing security.

In this work, we provide a novel protocol for generating the ancillary qubits required for the implementation of the R-gate in the QCED protocol. Ancillary qubits are extra qubits that are not part of the quantum state to which you wish to apply a quantum gate but are required in the quantum circuit to apply said quantum gate. This new method lowers the quantum power required on the clients side by lowering the number of states the ancillary qubits are generated in from four to two. The original method required the generation of two mutually unbiased bases, for a total of four states ($|+\rangle$, $|-\rangle$, $|+i\rangle$, and $|-i\rangle$) while our method only requires the generation of two non-orthogonal states ($|+\rangle$ and $|+i\rangle$). This reduction in the number of states comes at the price of increasing the number of ancillary qubits per R-gate (from one to three) and also requires post-selection (with a probability of success of 50%). We also provide a security proof for an honest server as well as provide a framework for generalizing this method to other sets of non-orthogonal states and to different numbers of ancillary qubits.

3.1 Preliminary definitions

This section includes a brief introduction to the mathematical definitions of quantum states and quantum gates used in this work. For an in-depth introduction to quantum information, see [31].

We keep our analysis general and independent of particular applications. We therefore define $\{|0\rangle,|1\rangle\}$ as the computational basis where these can be anything from electron spin

to photon polarization. The two mutually unbiased bases given above are defined as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3.1}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{3.2}$$

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \tag{3.3}$$

$$|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \tag{3.4}$$

The quantum gates that will be of use to us are the following: the Pauli X and Z gates, the Hadamard gate H, the phase gate P, the CNOT gate, and finally the R-gate. They are defined as follows:

$$X : |j\rangle \mapsto |j \oplus 1\rangle, \tag{3.5}$$

$$Z : |j\rangle \mapsto (-1)^j |j\rangle, \tag{3.6}$$

$$H : |j\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j |1\rangle), \tag{3.7}$$

$$P : |j\rangle \mapsto i^j |j\rangle, \tag{3.8}$$

$$\text{CNOT} : |j\rangle|k\rangle \mapsto |j\rangle|j \oplus k\rangle, \tag{3.9}$$

$$R : |j\rangle \mapsto \mathrm{e}^{ij\pi/4} |j\rangle. \tag{3.10}$$

Here we use the notation $O : |\psi\rangle \mapsto |\phi\rangle$. This notation means that, if we apply the quantum gate O to the state $|\psi\rangle$, we will end up with the state $|\phi\rangle$. In other words: $O|\psi\rangle = |\phi\rangle$. This operation is linear and therefore we also have $O(|\psi_1\rangle + |\psi_2\rangle) = |\phi_1\rangle + |\phi_2\rangle$. The Pauli gates are simply the application of a Pauli matrix to the quantum state. The Hadamard gate is the application of the Hadamard matrix to the quantum state. This is equivalent to a change of basis from $\{|0\rangle,|1\rangle\}$ to $\{|+\rangle,|-\rangle\}$. The P and R gates have a simple physical meaning: they do nothing to the state $|0\rangle$ and the add a phase to the state $|1\rangle$. Finally, the CNOT gate is the controlled-not gate.

The delegated quantum computing protocol that we are interested in is the QCED protocol [37]. It comprises a set of circuits that provide input privacy. By input privacy, we mean that the server gains no knowledge of the client's input apart from inevitable leakage of the size (number of qubits) of the input. This leakage of input size is trivial and applies to all protocols. This type of security is different from the security provided by the BQC protocol [36]. In this protocol the server gains no information regarding the input, nor does it learn any information regarding the algorithm it is performing. The only leakage of information

would be the size of the computation. We do not require this type of security and are content with input privacy.

In quantum information protocols, one wishes to transfer information in such a way that unauthorized access is not possible. Adversaries therefore constitute a large part of quantum information science. Malicious adversaries will actively attempt to gain unauthorized knowledge and will probably not follow any protocol you set for them. In our scheme of delegated quantum computation, the only adversary we consider is the server. No external adversaries will be considered. However, for our proof in input privacy we assume an honest server. This is a server that will always follow the protocol exactly and will not deviate in an attempt to gain information.

3.2 Quantum computing on encrypted data and the Clifford group

The Clifford group is a well known set of quantum operators or gates with a wide array of applications. It is defined as the set of quantum operators that conjugate the Pauli operators into other Pauli operators. This set comprises the single qubit Pauli gates (X, Y, Z), the Hadamard gate (H), the Phase gate (P), and the two-qubit controlled not $(CNOT)$ gate. In order to perform universal quantum computation, it is not necessary to be capable of implementing any quantum operation [39]. It is sufficient to be able to implement all of the gates in the Clifford group along with any one additional gate such as the Toffoli gate or the R-gate. This is due to the fact that any unitary operation can be approximated to any desired degree of accuracy by a circuit of these gates. We will be using the R-gate as our additional gate due to its simplicity and its relation to previous work [37]. Strictly speaking, not all of the Clifford group gates are required for universality due to the relations between these operators ($P = R^2$,$Z = P^2$, and $X = HZH$). If one uses the R-gate as its additional gate, universality only requires the Hadamard gate and the CNOT gate. However, current protocols for the implementation of non-Clifford group gates such as the R-gate require ancillary qubits to implement. The Clifford group gates on the other hand do not require such ancillary qubits due to their commutation relations with the Pauli gates. Thus, including the Pauli X and Z gates along with the P-gate into a protocol significantly reduces the required number of ancillaries. Since a Pauli Y gate can be implemented as a Pauli Z followed by a Pauli X (up to an irrelevant global phase), we do not require a protocol for this gate. Applying XZ is sufficient.

One protocol for delegated quantum computing is quantum computing on encrypted data

(QCED) [37]. It allows a client to delegate a complex quantum computation to a server while keeping its input private. However, the client must divulge the circuit it wishes to compute via classical messages to the server. For example, the server will know that it is factoring a number but it will not know what that number is, nor the output. This protocol provides a circuit for all of the Clifford group gates and for the R-gate. A brief outline of the protocol, along with proofs of correctness, follows.

The circuits for the implementation of the Clifford group gates are simple and straightforward. They are given in Figures 3.1 to 3.5. We start by encrypting the input $|\psi\rangle$ with the keys a and b. We then send the encrypted input state to the server which directly applies the desired Clifford group gate. The server then sends the output back to the client who decrypts it.

The circuits for the Pauli gates given in Figures 3.1 and 3.2 are correct because $ZX = XZ$ up to an irrelevant global phase. The circuit for the Hadamard gate, Figure 3.3, is correct because $HX = ZH$ (up to global phase). The Phase-gate circuit, Figure 3.4, is correct because $PZ = ZP$ and $PX = -iZXP$ (up to global phase). And finally, the CNOT circuit in Figure 3.5 is correct following a similar analysis.

For non-Clifford group gates, no simple circuits exist due to the lack of simple relations between these gates and the Clifford group gates. Here we must use ancillary qubits. The

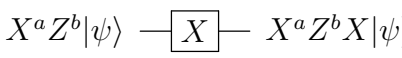

Figure 3.1: Protocol for the implementation of the Pauli-X gate where a and b are the encryption keys.

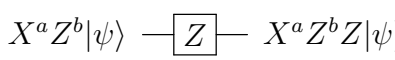

Figure 3.2: Protocol for the implementation of the Pauli-Z gate where a and b are the encryption keys.

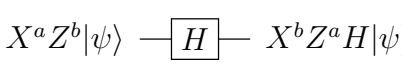

Figure 3.3: Protocol for the implementation of the Hadamard gate, H-gate, where a and b are the encryption keys.

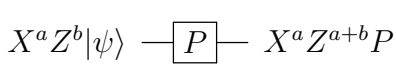

Figure 3.4: Protocol for the implementation of the Phase gate, P-gate, where a and b are the encryption keys.

original circuit for the R-gate in [37] is given in Figure 3.6. The client encrypts the input ψ as before and sends it to the server. The server applies the R-gate to this input. From here, it is not sufficient for the server to send the result back to the client. Instead, the client generates an ancillary qubit randomly from $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$. In the circuit, this is portrayed as generating the ancillary in the state $|+\rangle$ and then randomly applying P and Z gates as determined by the values y and d respectively, where y and d are the encryption keys for the ancillary qubit. These values are chosen to be 0 or 1 at random by the client. The client then sends this ancillary qubit and the classical bit $x = a \oplus y$ to the server. The server then applies a controlled not between the two qubits with the ancillary as the control. Afterwards, the server measures the input qubit and applies the P^x correction to the ancillary. This leaves the ancillary in the state $(X^a Z^{b+d} \otimes X^{a+c} Z^d) CNOT |\psi\rangle$. Correctness follows from all of the above relations along with the following: $RZ = ZR$, $RX = XZPR$, $P^2 = Z$ and $P^{a \oplus b} = Z^{a \cdot b} P^{a \oplus b}$ for $a, b \in \{0, 1\}$.

3.3 Novel protocol for the R-gate

In this section, we describe our novel protocol for the implementation of the R-gate required for QCED. The general idea is the following: we desire to generate a qubit randomly from the set $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ starting with ancillary qubits generated in the states $\{|+\rangle, |+i\rangle\}$. We then apply the original QCED protocol for the R-gate with this qubit as the new ancillary. In other words, we've developed a new protocol for the generation of the ancillary qubit. The purpose of this is to lower the demand on the client. In other words, this new protocol is easier to implement compared to the original protocol. For example, if one uses the polarization states of photons as their qubits, the original protocol would require the use of two Pockels cells (an expensive piece of equipment) but our new technique would only require one.

A schematic of our protocol can be found in Figure 3.7. We define $|\theta_j\rangle = (|0\rangle + e^{i\theta_j}|1\rangle)/\sqrt{2}$ as the state of the jth ancillary qubit. The protocol starts with the client generating three qubits randomly from $|+\rangle$ ($\theta_j = 0$) and $|+i\rangle$ ($\theta_j = \pi/2$). The client then sends the qubits to

$$(X^a Z^b \otimes X^c Z^d)|\psi\rangle \quad \left\{ \quad \right\} \quad (X^a Z^{b+d} \otimes X^{a+c} Z^d) CNOT |\psi\rangle$$

Figure 3.5: Protocol for the implementation of the controlled-not gate, $CNOT$, where a and b are the encryption keys for the first qubit and c and d are the encryption keys for the second qubit.

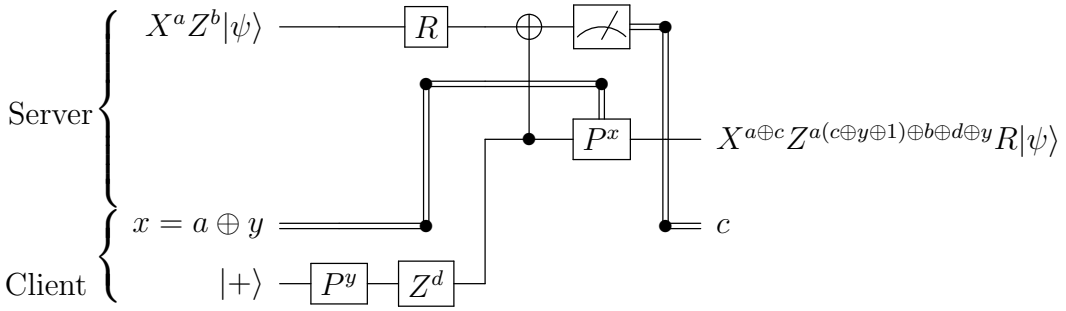

Figure 3.6: The original protocol for the implementation of the R-gate in the quantum computing on encrypted data scheme, where a and b are the encryption keys for the qubit and y and d are the encryption keys for the ancillary qubit.

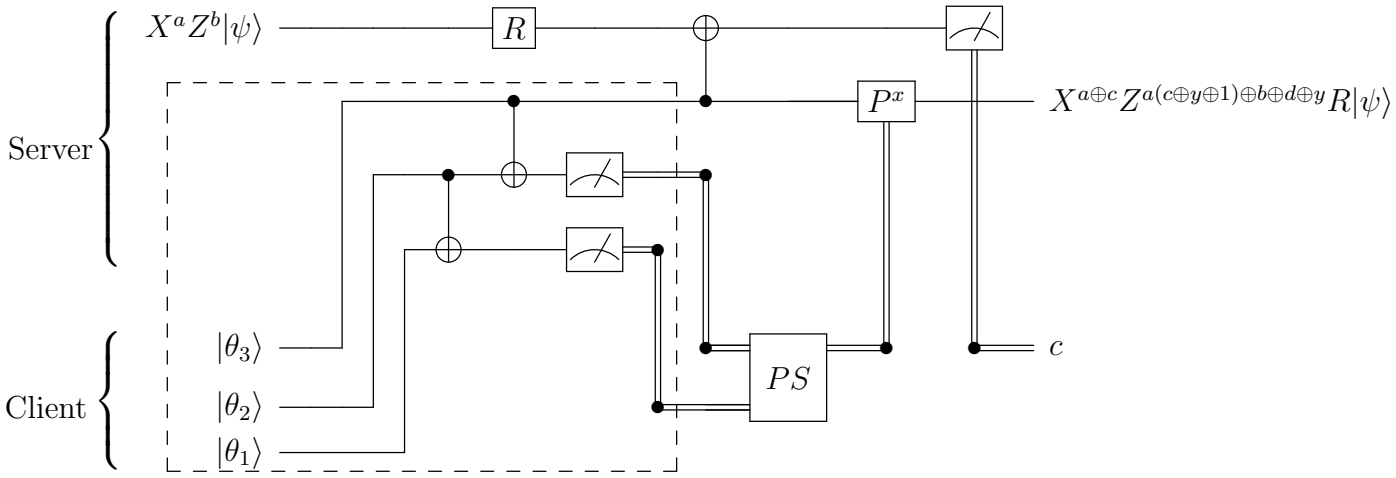

Figure 3.7: Novel protocol for the implementation of the R-gate, where a and b are the encryption keys for the qubit. The ancillary qubits are in the state $|\theta_j\rangle = (|0\rangle + \mathrm{e}^{i\theta}|1\rangle)/\sqrt{2}$ where $\theta \in \{0, \pi/2\}$. The dotted line designates the ancillary state preparation circuit and the classical 'PS-gate' corresponds to post-selection. The output of the 'PS-gate' is the classical bit x.

the server which applies two CNOTs: the first between the first and second qubits and the other between the second and third qubits with the second and the third qubits as the controls respectively. The server then measures the first and second qubits in the computational basis leaving the third qubit in the state

$$|0\rangle + e^{i\{(-1)^{c_2}[(-1)^{c_1}\theta_1 + \theta_2] + \theta_3\}}|1\rangle, \tag{3.11}$$

where c_1 and c_2 are the measurement results for qubits one and two respectively and θ_i is the phase of the ith qubit (0 for $|+\rangle$ and $\pi/2$ for $|+i\rangle$). The server then sends the measurement results c_1 and c_2 to the client. A derivation of Eq. 3.11 follows. We start with the initial

Input state			Measurement results, c_1 and c_2			
θ_1	θ_2	θ_3	0,0	0,1	1,0	1,1
0	0	0	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
0	0	$\frac{\pi}{2}$	$\|+i\rangle$	$\|+i\rangle$	$\|+i\rangle$	$\|+i\rangle$
0	$\frac{\pi}{2}$	0	$\|+i\rangle$	$\|-i\rangle$	$\|+i\rangle$	$\|-i\rangle$
$\frac{\pi}{2}$	0	0	$\|+i\rangle$	$\|-i\rangle$	$\|-i\rangle$	$\|+i\rangle$
0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$
$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$
$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$
$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\frac{\pi}{2}$	$\|-i\rangle$	$\|-i\rangle$	$\|+i\rangle$	$\|+i\rangle$

Table 3.1: Table of the resulting ancillary qubit after the first step of the R-gate circuit. The states marked with a grey background are the cases that correspond to a successful post-selection. All other outcomes are rejected.

state given by $|\theta_1\rangle|\theta_2\rangle|\theta_3\rangle$. After the first CNOT, we have:

$$\frac{1}{2}\left[|0\rangle(|0\rangle + \mathrm{e}^{i\theta_1}|1\rangle) + \mathrm{e}^{i\theta_2}|1\rangle(\mathrm{e}^{i\theta_1}|0\rangle + |1\rangle)\right]|\theta_3\rangle. \tag{3.12}$$

This can be rewritten as

$$\frac{1}{2}\left[(|0\rangle + \mathrm{e}^{i(\theta_2+i\theta_1)}|1\rangle)|0\rangle + \mathrm{e}^{i\theta_1}(|0\rangle + \mathrm{e}^{i(\theta_2-\theta_1)})|1\rangle\right]|\theta_3\rangle. \tag{3.13}$$

For simplicity, we will at this point perform the measurement of the first qubit. We can do this because the outcome will be same regardless of when we applied the second CNOT. The state after the measurement (ignoring a global phase) is

$$(|0\rangle + \mathrm{e}^{i(\theta_2+(-1)^{c_1}\theta_1)}|1\rangle)|\theta_3\rangle. \tag{3.14}$$

The state of the second ancillary qubit is the result of a CNOT and a measurement. The second half of this procedure is exactly the same but using the second and third qubits instead. We can therefore apply this equation but substituting θ_3 for θ_1 and $\theta_2 + (-1)^{c_1}\theta_1$ for θ_2. This results in a relative phase of $(-1)^{c_2}[\theta_2 + (-1)^{c_1}\theta_1] + \theta_3$.

Equation 3.11 above has been expanded out in Table 3.1. Each row corresponds to one of the possible inputs $\{\theta_i\}$ which the client chooses randomly with an even distribution. The three left columns determine the state of the input ancillary qubits and the last four columns correspond to the measurement outcomes c_1, c_2. We therefore have a clear table to determine which cases to keep during the post-selection phase indicated as a classical PS-gate in Figure 3.7. The states marked with a grey background are outcomes that are accepted. From this table, one finds that, in order to generate each of the four desired states

with equal probability, one can only accept half of the cases. Note that the accepted cases have been selected such that each input (row) has an equal probability of being accepted (50%). Upon successful post-selection, we are left in a situation that is analogous to the old protocol where we have an ancillary in one of the states $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ and $x = a \oplus y$ is determined by this state ($y = 0$ for $|\pm\rangle$, and $y = 1$ for $|\pm i\rangle$). The remainder of the circuit is identical to the original protocol described in the previous section and will not be repeated here. If the post-selection is unsuccessful, the client informs the server and must start over until the post-selection is successful.

From Table 3.1, correctness of the ancillary state preparation is clear. After successful post-selection, the state is left in one of the four desired states. Correctness of the remainder of the protocol follows an identical proof to the original R-gate protocol since the two circuits are equivalent at this point. Combining these two, we clearly have that the whole protocol is correct. In summary, we have a new protocol for QCED which is more easily implemented due to lowering the required quantum power of the client.

3.4 Correctness and security of novel protocol for an honest server

In the previous sections, we have shown that the protocols for the individual gates are correct. It follows that any circuit built up of these gates is also correct since the client simply needs to update its encryption keys after each individual gate. This is possible as the output of each gate is of the form $X^{a'}Z^{b'}O|\psi\rangle$ where O is the quantum gate and a' and b' are the decryption keys of the output. These decryption keys are used as the new encryption keys if further gates are applied. For example, if we first apply the P gate, the decryption keys are $a' = a$ and $b' = a + b$. If we then apply the Hadamard gate H, new decryption keys become $a'' = b' = a + b$ and $b'' = a' = a$.

We now provide a proof of the security of the protocol for an honest server. Given this honest server and assuming that the client implemented the protocol correctly, the state of the remaining ancillary qubit after the post-selection is one of $\{|+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ and we have $x = a \oplus y$ where $y = 0$ for $|\pm\rangle$ and $y = 1$ for $|\pm i\rangle$. We also define d as the following: $d = 0$ for $\{|+\rangle,|+i\rangle\}$ and $d = 1$ for $\{|-\rangle,|-i\rangle\}$. The encryption keys a and b are secure at this point since the only information the server has are the values of c_1 and c_2 and these values are uncorrelated to the state of the system after post-selection. The lack of correlations between c_1 and c_2 and the remaining ancillary state is crucial for security. We must post-select so that this is the case. The state of the system after post-selection

according to the server is

$$\frac{1}{4}|c_1,c_2\rangle\langle c_1,c_2|\otimes(|+\rangle\langle+|+|-\rangle\langle-|+|+i\rangle\langle+i|+|-i\rangle\langle-i|)=\frac{1}{2}|c_1,c_2\rangle\langle c_1,c_2|\otimes\hat{\mathbb{1}}, \quad (3.15)$$

where $\hat{\mathbb{1}}$ is the completely mixed state of the ancillary qubit and the summation was over all of the accepted states given c_1, c_2. The server therefore cannot determine the state of the ancillary qubit from c_1 and c_2 as they are separable. We therefore have that the protocol is secure for the ancillary state preparation and, as stated previously, the remainder of the circuit is identical to the original version of the protocol. Thus the original proof applies from this point.

A brief review of one of the many proofs follows. It was recently shown that it is sufficient that the client can always locally reconstruct its input to have input privacy in a protocol [40]. Consider a protocol for a circuit involving r R-gates. After the successful post-selection, the state sent from the client to the server is given by

$$\sum_{a,b=0}^{2^n-1}|ab\rangle(X^aZ^b\otimes\hat{\mathbb{1}})|\psi\rangle\bigotimes_{i=1}^{r}\left(\sum_{d_i,y_i=0}^{1}|d_i\rangle|y_i\rangle Z^{d_i}P^{y_i}|+\rangle|a_i'\oplus y_i\rangle\right), \quad (3.16)$$

where a_i' is the updated key for the Pauli-X encryption on its respective wire. Here we have that $|\psi\rangle$ is the shared state of the client and the server, where the client's part consists of its input into the protocol and the server's part includes anything that is correlated to this input. Also, we used the short hand X^aZ^b to mean the encryption of the entire input. This can be written out as: $X^aZ^b=X^{a_1}Z^{b_1}\otimes X^{a_2}Z^{b_2}\otimes\cdots\otimes X^{a_n}Z^{b_n}$. We then apply the auxiliary state identity and get

$$\sum_{a,b=0}^{2^n-1}|ab\rangle(X^aZ^b\otimes\hat{\mathbb{1}})|\psi\rangle\bigotimes_{i=1}^{r}\left(\sum_{d_i,y_i=0}^{1}|d_i\rangle|y_i\rangle|d_i\rangle|a_i'\oplus y_i\rangle\right), \quad (3.17)$$

where the auxiliary state identity is given by:

$$(Z^yP^yH\otimes 1)\frac{1}{\sqrt{2}}\sum_{d=0}^{1}|d\rangle P^yZ^d|+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \quad (3.18)$$

Its proof is straightforward. All one must do is expand the sum on the left-hand-side and simplify. This concludes our preliminary definitions. This is accurate up to a local operation

on the client's side. We now apply the change of variables $a'_i \oplus y_i \to x_i$:

$$\sum_{a,b=0}^{2^n-1} |ab\rangle(X^a Z^b \otimes \hat{\mathbb{1}})|\psi\rangle \bigotimes_{i=1}^{r} \left(\sum_{d_i,y_i=0}^{1} |d_i\rangle|x_i \oplus a'_i\rangle|d_i\rangle|x_i\rangle \right). \tag{3.19}$$

The client can then apply the local operation $a'_i \otimes x_i \mapsto x_i$ and get:

$$\sum_{a,b=0}^{2^n-1} |ab\rangle(X^a Z^b \otimes \hat{\mathbb{1}})|\psi\rangle \bigotimes_{i=1}^{r} \left(\sum_{d_i,y_i=0}^{1} |d_i\rangle|x_i\rangle|d_i\rangle|x_i\rangle \right). \tag{3.20}$$

We now have that the ancillary qubits are separable from the rest of the system and can be traced out. We are now left with

$$\sum_{a,b=0}^{2^n-1} |ab\rangle(X^a Z^b \otimes \hat{\mathbb{1}})|\psi\rangle \tag{3.21}$$

which is the problem of the quantum one-time pad [41]. The security for a quantum one-time pad is well known and we therefore have input privacy. As a final note, we conjecture that, in this protocol, the honest server corresponds to a specious adversarial server [42]. This conjecture has yet to be proven. In conclusion, we have a new secure protocol for quantum computation on encrypted data that is less demanding on the client and thus more widely available.

3.5 Generalization of the method to other states

Before we can generalize this protocol to different sets of (pure) states, we must first describe how to add qubits to the protocol. Same as before, the client prepares her qubits randomly from her chosen set of states and sends them to the server. The server then cascades CNOTs from the first qubit to the second, from the second to the third, then from the third to the fourth, etc. until he reaches the last qubit. The server then measures all but the last qubit and sends the measurement results to the client. We can now build a table similar to the one given above for this new protocol and determine which states are accepted and which are rejected during the post-selection.

This new protocol works for sets of two non-orthogonal states other than the one given above so long as there are enough ancillary qubits. For simplicity and without loss of generality, we can assume that one of the states is $|+\rangle$ and that the other is given by $|\theta\rangle = (|0\rangle + \mathrm{e}^{i\theta}|1\rangle)/\sqrt{2}$ where $\theta \neq 0$. Note that this protocol is exact only for states of the

form $(|0\rangle + e^{i\pi/2^k}|1\rangle)/\sqrt{2}$. For sets of states that are not of this form, the output of the protocol is only approximately the desired set. For the exact case, the minimum number of qubits required N is given by the relative phase of the second state: $N\theta = \frac{3\pi}{2}$. This can be seen by the fact that we require the state $|-i\rangle$. We therefore need that the sum of all of the phases of the ancillaries be at least $3\pi/2$. This sum is at its maximum of $N\theta$ when the input ancillaries are all in the state $|\theta\rangle$. This is the first step towards a general theory quantifying 'quantum power' and determining the trade-off between security and quantum power.

3.6 Conclusions

In summary, we have developed a novel method for the implementation of a non-Clifford group gate, in this case the R-gate, which is required for universal quantum computing. This method is a modified version of a delegated quantum computing scheme known as quantum computing on encrypted data (QCED). More specifically, we provide a new circuit for the generation of the ancillary states. Our new method differs from its predecessor by reducing the number of states the ancillary qubits are generated in from four to two. In effect, this reduces the quantum power required on the client's end at the cost of requiring more ancillary qubits per gate. We also provide a proof of correctness and security for this new circuit for an honest server. Finally, we demonstrated a method of generalizing this circuit to other states and to larger numbers of ancillary qubits. Future work will focus on the formalization of this method. A theoretical model quantifying the error in this method for approximate cases is also required. A proof of our conjecture that specious and honest servers are identical is still needed. Finally, an examination of the input security of this technique for a malicious server or even an eavesdropper is also needed.

Along with all of the other topics discussed in this thesis, this chapter focused on a limiting behaviour in physics. For delegated quantum computation, it is the limiting behaviour between the quantum power required by a client and the amount of security provided. In our specific case, we looked at lowering the quantum power of the client while keeping perfect input privacy. In other words, we want to know how 'classical' a client can be without sacrificing security. Further reductions in the client's quantum power would result in a loss of security. This work can be viewed as a first step towards a complete theory describing the duality between these two quantities and the transition from classical to quantum information.

Chapter 4

Eigenmode super-resolution

In this final chapter, we will be moving away from quantum phenomena and into the classical regime. More specifically, we will be discussing diffraction, its effect on optical imaging resolution, and how to correct it. Optical imaging plays a crucial role in many fields including chemistry, biology, physics, and engineering. This is due to the relative ease of generating, manipulating, and measuring light. Diffraction is a detriment to optical imaging in that it lowers the resolution of images.

As optical imaging was first developing, it was widely believed that the resolution of an image was limited by Abbe's diffraction limit [43]. This limit is quantified as

$$d = \frac{\lambda}{2n \sin\theta}, \tag{4.1}$$

where λ is the wavelength of the light, n is the index of refraction of the material in which the light is propagating, θ is the convergence angle, and d is the spot size of the image. In words, this equation provides a limit to how small a spot d can be given that the incoming light has a convergence angle of θ. However, this equation looks only at the focussing of a spot while many applications have more complex objects where this limit cannot be applied. Note that we will be using the term 'object' to mean the complex light field at the input of an optical imaging system and use the term 'image' to mean the output field unless stated otherwise.

Another quantitative measure of diffraction is Rayleigh's criterion [44]. It determines the minimum separation required between two points for them to be distinguishable upon propagation through the optical system. Rayleigh's criterion for a lens is

$$d = 1.22\frac{f\lambda}{D}, \tag{4.2}$$

where λ is again the wavelength, and f and D are the focal length and diameter of the lens, respectively. Similarly to Abbe's diffraction limit, this criterion is limited to a predetermined object, in this case two spots, and is not applicable to many imaging systems. It is however a good starting point for a more generally applicable diffraction limit as it directly provides a quantity that describes our ability to distinguish inputs.

Diffraction, along with finite-aperture optics, results in the loss of high spatial frequency information contained in the object. This 'loss of information' leads to blurry images where fine details in the original object are lost. In other words, diffraction reduces the fidelity of an optical imaging system. We can also view this from the point-of-view of degrees-of-freedom of objects and imaging systems [45]. By degrees-of-freedom of an imaging system, we mean the number of degrees-of-freedom of a light field that can be transmitted through the system. For example, single-mode fibres have a single degree-of-freedom. If the number of degrees-of-freedom of an object is larger than that of the image-forming apparatus, then the resulting image will be diffraction-limited. These degrees-of-freedom along with the concept of the detection of ambiguous images were introduced as key concepts for quantifying the resolution limit of optical systems. When two distinct objects have identical images upon propagation, they are indistinguishable unless one has some a priori information. The identical images after propagation through the optical system are called ambiguous images. Certain optical systems have an interesting property: finite sized objects do not have ambiguous images [46]. The resolution of these systems is therefore only limited by noise assuming that one can measure the images accurately.

It is now well known that it is possible to achieve resolutions beyond the diffraction limits described above. Discussion into achieving these resolutions began in the 1960s and have been of great interest ever since [46, 47]. Super-resolution imaging is the field of research dedicated to the generation of images with resolutions beyond the Abbe diffraction limit. In other words, super-resolution techniques allow one to resolve details in images with very high precision. Due to the vast number of applications of optical imaging, numerous techniques for super-resolution have been developed. However, we will refer to super-resolution imaging as any technique which provides an increase in resolution, regardless of whether it is applied to sub-diffraction or aberration-free imaging. We do this because aberrations can significantly degrade the resolution of images in a similar fashion to diffraction.

A priori information stands for information that is known ahead of time. Having a priori information about the object improves and is sometimes required for super-resolution. It is also well known that the maximum degree of super-resolution is limited by the signal-to-noise ratio (SNR). Many techniques for achieving super-resolution exist. Examples include near field imaging with hyperlenses [48, 49, 50, 51], super-oscillating lenses [52], compressive

sensing [53, 54], non-linear fluorescence imaging [55, 56], photon-counting techniques [57, 58, 59], and compressive sensing [53, 54]. Super-resolution has also found some applications in lithography [57, 60, 61]. However, several key issues of super-resolution remain. One of these is the absence of a complete theory describing the relation between the amount of a priori information available and the degree of super-resolution that is achievable.

Despite the theoretical interest in super-resolution, its applications are quite limited. This is due to multiple factors such as the requirement of complex apparati or that the technique can only be applied to a small class of images. A technique that can resolve arbitrary images without the use of complex apparati and in the presence of turbulence, imperfect optics, and diffraction which will be encountered in real world scenarios would be advantageous.

Eigenmode super-resolution is a super-resolution technique which utilizes the eigenmodes of the optical imaging system of interest to achieve resolutions above the diffraction limit. The eigenmodes of an imaging system are a special type of mode that retain their spatial distribution upon propagation [45, 62, 63]. They do however experience an attenuation in amplitude and a global phase shift [64]. This technique achieves super-resolution by expanding the image as a sum of eigenmodes and then compensating for the known attenuation and phase shift of the individual eigenmodes. It provides a method to realize super-resolution which is not reliant on non-linear optics, nor specialized equipment making it easily applicable to pre-existing set-ups. This technique can be applied to arbitrary objects so long as they can be written as a sum of eigenmodes. Also, the technique is inherently robust due to the fact that eigenmodes are capable of imaging through aberrations as well as diffraction, aberrations being undesired phase additions. The primary limit to eigenmode super-resolution is the signal-to-noise ratio (SNR) of the transmitted images. Originally, eigenmode imaging in this manner, and its extension to singular value decomposition, was considered infeasible due to its high computational cost [65]. The lack of a method to determine the eigenmodes of an optical system was also a problem until recently [6]. These problems led to a shift towards indirect methods of achieving super-resolution including scanning microscopy [66, 67] and the use of pupil-plane marks [68].

Most studies into super-resolution have been in the classical regime. However, there has been some recent theoretical work into the quantum limit to eigenmode resolution, this quantum limit being due to quantum fluctuation. These studies looked into the case of both one-dimensional and two-dimentional images [69, 70, 71, 72, 73]. We are motivated by the goal of reaching the quantum limit to super-resolution experimentally and measuring the degree of super-resolution as a function of the SNR. The work presented in this thesis chapter can be viewed as a first step towards achieving this goal.

In this thesis chapter, we present the first experimental demonstration of eigenmode

super-resolution. The optical system used in this experiment was a $4f$ system with a circular aperture. This system was chosen because it has known eigenmodes. We find that we can achieve super-resolution in certain cases [5]. We then provide a method to determine the eigenmodes of an arbitrary linear optical system and show how to utilize them for super-resolution even if they are non-orthogonal [6]. We then demonstrate the technique numerically for several diffraction-limited and aberrated optical systems and show its viability for a range of objects. Finally, we apply this new technique experimentally for two optical systems. First, we apply it to a $4f$ system similar to the original experiment. Second, we apply it to a multi-mode fibre. We find that we can achieve super-resolution for a limited number of cases.

4.1 Basic theory

This section provides the basics of eigenmode super-resolution imaging for linear optical imaging systems [5]. First and foremost, we need to define an eigenmode for such a system. An eigenmode Φ_i is a complex field of light that, upon propagation through the imaging system, remains unchanged apart from a global amplitude attenuation and a global phase shift. This attenuation and phase shift are given by the eigenvalue λ_i of the eigenmode. More formally, the eigenmodes Φ_i satisfy the following eigenvalue equation:

$$S[\Phi_i] = \lambda_i \Phi_i, \tag{4.3}$$

where $S[X]$ represents the output field of the imaging system given the input field X. In this section, we will assume that these eigenmodes are orthonormal and that they, along with their respective eigenvalues, are known.

The input to an optical imaging system is called the object which we denote as A. The output is called the image and we denote this as B. We can express the complex fields of both the object A and the image B as a super-position of the eigenmodes:

$$A = \sum_i a_i \Phi_i, \tag{4.4}$$

$$B = \sum_i b_i \Phi_i, \tag{4.5}$$

where a_i and b_i are the complex coefficients that define the object and image respectively. The intensity distributions of the object and image are given by $|A|^2$ and $|B|^2$ respectively. The coefficients above can be obtained from complex overlap integrals. We define the overlap

between two fields X and Y as

$$\langle X, Y \rangle = \int_D XY^* d\sigma \tag{4.6}$$

where D is total area spanned by X and Y and $d\sigma$ is the differential area. From this and the assumption that the eigenmodes are orthonormal, we have $a_i = \langle A, \Phi_i \rangle$ and $b_i = \langle B, \Phi_i \rangle$. We will generalize this to remove the orthonormality assumption in a later chapter. Our goal is to recover the values of a_i from b_i. Due to the properties of eigenmodes, we have a simple relationship between these coefficients. To find this relationship, let us first recognise that

$$S[A] = B. \tag{4.7}$$

We can expand this out with the use of Eq. 4.17 and 4.5 along with the eigenvalue equation 4.3:

$$\sum_i a_i S[\Phi_i] = \sum_i a_i \lambda_i \Phi_i = \sum_i b_i \Phi_i, \tag{4.8}$$

where we used the fact that our imaging system is linear, $S\left[\sum_i X_i\right] = \sum_i S[X_i]$. Finally, we have that

$$a_i = \frac{b_i}{\lambda_i}. \tag{4.9}$$

This equation gives us the coefficients that define the object a_i in terms of known quantities: b_i and λ_i. In other words, the coefficients of the object can be recovered by measuring the coefficients of the image and compensating for the attenuation and phase shift of the individual eigenmodes. Therefore, we are able to determine the desired object from the diffraction-limited and aberrated image. This reconstruction is eigenmode super-resolution.

We have previously stated that the Abbe diffraction limit and Rayleigh's criterion are not easily applicable to arbitrary systems and general input objects. We therefore need a different quantity to define the amount of improvement in resolution that is obtained from the reconstruction. We define the super-resolution factor S_r as

$$S_r = \frac{|\langle B', A \rangle|^2 - |\langle B, A \rangle|^2}{|\langle B, A \rangle|^2} = \left| \frac{\langle B', A \rangle}{\langle B, A \rangle} \right|^2 - 1, \tag{4.10}$$

where B' is the reconstructed image. Remember that A, B and B' are the complex fields and not the intensities. The reason we use fields instead of intensities is that we wish to be able

to distinguish different modes. For example, we want to be capable of distinguishing images with an orbital angular momentum of +1 from images with an orbital angular momentum of −1. Positive values indicate an improvement in resolution and that we have achieved super-resolution. Note that by 'achieve super-resolution' we mean a diffraction and/or aberration correction. We therefore may not necessarily have a resolution above the diffraction limit as the improvement in resolution may be due to the correction of other factors (aberrations) degrading the image. The maximum value of S_r is given by $|\langle B, A\rangle|^{-2} - 1$ and corresponds to the case where the reconstruction is perfect, $\langle B', A\rangle = 1$. A value of 0 indicates that there was no improvement in resolution. Negative values indicate that the resolution of the reconstructed image is lower than that of the diffracted image and therefore that the reconstruction failed.

In a real world scenario, an image measured at the output of an imaging system will be affected by noise. The signal-to-noise ratio places an upper limit on the achievable resolution. This is due to the fact that noise adds to the measured coefficients b_i and the subsequent division by λ_i will amplify this noise. We therefore have that any reconstruction including eigenmodes with λ_i approaching 0 will be dominated by noise. Also, if too few eigenmodes are included in the reconstruction, the resulting image may no longer accurately depict the object. This is because coefficients with a significant contribution to the object may be omitted in the reconstruction. We therefore need to balance the noise introduced and the number of coefficients used in the reconstruction. This can be done by placing a threshold on λ_i. Any eigenmode with an eigenvalue below the threshold is not included in the reconstruction. We can set this threshold to be the inverse of the signal-to-noise ratio [73]. Any object that can be expanded as a super-position of eigenmodes with eigenvalues lower than the threshold is distinguishable after the reconstruction.

This super-resolution technique requires the ability to measure the complex field at the output of the imaging system. This cannot be measured directly with a single measurement and we must rely on some phase retrieval protocol. We present here a simple protocol to determine the complex field of images [64]. The first step is to interfere our image at the output of the imaging system with a reference mode E_{ref} and measure the resulting intensity distribution I. We then shift the relative phase between these two beams by $2\pi/N$ where N is some integer greater than 3 and measure the new interference pattern. This process is repeated until we have measured all of the interference patterns with a relative phase of up to 2π. The complex field of the image is then calculated to be

$$B = \frac{1}{N|E_{ref}|} \sum_{k=0}^{N-1} \mathrm{e}^{i2\pi k/N} I_k, \tag{4.11}$$

where I_k is the intensity distribution with a relative phase of $2\pi k/N$ between the image and the reference beam. This method of phase retrieval can be applied to many systems. All one needs is to have a reference beam with which to interfere the images and the capability of changing the relative phase. This can be easily achieved with the use of spatial light modulators (SLM). In summary, we have a method to achieve super-resolution that is easily applied to a large number of optical systems while requiring few assumptions or specialized optical components.

4.2 Eigenmodes of a $4f$ system with a circular aperture

An optical imaging system that is of particular interest to us is given in Figure 4.1. Here we have a 4f imaging system with a circular aperture in the focal plane of the two lenses. This aperture absorbs the incident light producing diffraction. This is one of the simplest systems introducing diffraction and our interest in the system comes from the fact that its eigenmodes are known [74]. We define the space-bandwidth product c as

$$c = 2\pi \frac{R_o R_p}{\lambda f}, \tag{4.12}$$

where λ is the wavelength of the incident light, f is the focal length of the lenses, R_o is the radius of the object and image, and R_p is the radius of the aperture. The product gives a rough estimate of the number of degrees-of-freedom of the system. This can also be viewed as a measure of the amount of information that is transmitted. By this, we mean that there are approximately c eigenmodes with eigenvalues approaching 1.

The eigenmodes of this system are the prolate spheroidal modes [73]:

$$\Phi_{\ell,p}(r,\theta) = \varphi_{\ell,p}(r,c)\mathrm{e}^{-i\ell\theta} \tag{4.13}$$

where $\varphi_{\ell,p}$ is a generalized prolate spheroidal function. These functions were originally developed and analysed by Slepian [74] and Heurley [75]. Since their initial development, they have found a variety of applications in both physics [76, 77, 78] and mathematics [79, 80, 81, 82]. We calculated these functions along with their respective eigenvalues using a numerical method elaborated in [73]. In brief, the functions are expanded as a summation over radial Zernike polynomials weighted by coefficients determined by a three-term recurrence relation. The intensity and phase distributions of a few prolate spheroidal modes for a system with $c = 10$ are given in Figure 4.2. The eigenvalues for this system are real. The eigenmodes therefore experience an attenuation but no relative phase shift upon propagation through the

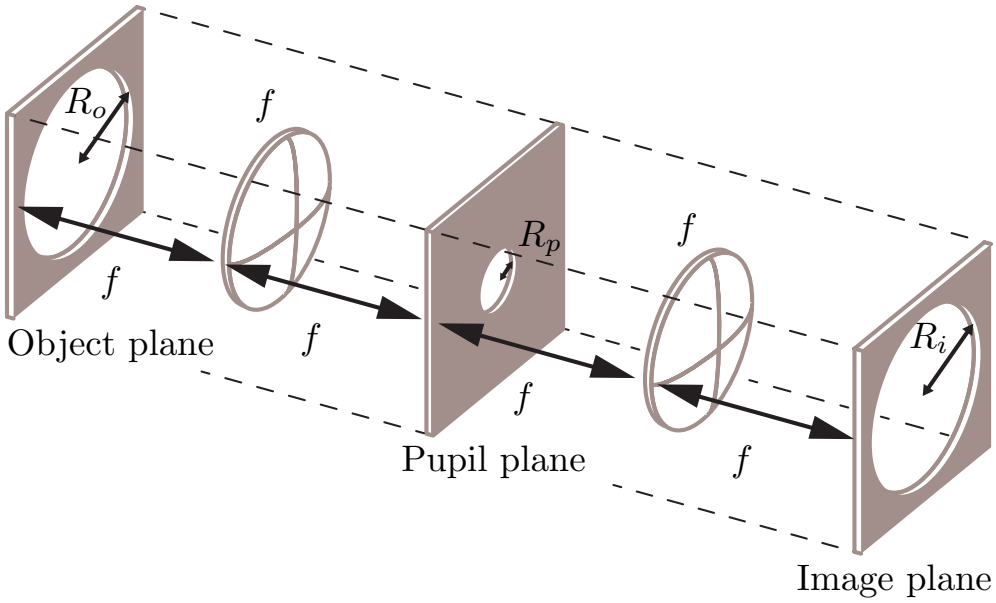

Figure 4.1: A schematic of a simple diffraction-limited optical imaging system is given here. This system consists of a $4f$ system with a circular aperture in the center producing diffraction. In order to find the eigenmodes of this system, we were required to fix a finite radius in the both the object and pupil planes. We set $R_o = R_i$.

$4f$ system. A visual representation of this, along with a subset of eigenvalues for a system with $c = 10$, are shown in Figure 4.3. This particular imaging system has also been used in the theoretical investigation into the quantum limit to super-resolution [72, 73].

4.3 Experiment #1: $4f$ system with known eigenmodes

In this section, we detail the experimental procedure along with the results for our first experiment [5]. The goal is to perform super-resolution through a $4f$ system containing a circular aperture, see Figure 4.4. We start with a spatially-filtered 670 nm diode laser illuminating a spatial light modulator (SLM, Holoeye Pluto) placed in the object plane of the $4f$ system. This SLM generates the objects that we wish to input into the system. We then send the first diffraction order of the light reflected off of the SLM through a $4f$ system with an adjustable iris placed at the focal point. This adjustable iris serves a dual purpose: it produces diffraction in the image and filters out the other diffraction orders reflected off the SLM. The output images are recorded by a CCD camera (Dalsa Genie) placed at the focal point of the second lens. The space-bandwidth product c for this set-up can be adjusted by changing the radius of iris R_p and the radius of the object R_o generated by the SLM. We chose $R_p = 0.5$ mm and $R_o = 1$ mm so that $c \approx 10$. In this setup, an independent reference

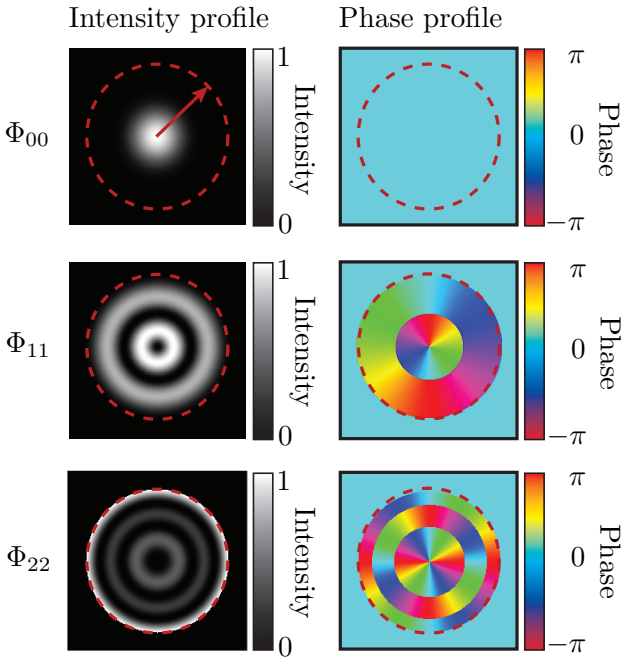

Figure 4.2: These are normalized intensity and phase profiles of three eigenmodes of the system described above with $c = 10$. The red arrow indicates R_o and the corresponding dashed red circles indicate the region in which the images are contained.

beam was not required. In order to determine the phase of the images, we generated the superposition of the object and a reference plane wave directly on the SLM.

A summary of our results is given in Figure 4.5. We chose the objects to be superpositions of prolate spheroidal modes $\Phi_{\ell,p}$. We find a significant improvement in the resolution of the images after the reconstruction as shown in the super-resolution factors: (i) 0.89, (ii) 0.49, and (iii) 0.45. The recorded diffraction-limited images are severely affected by loss and the reconstructed images look almost identical to their respective objects. In Figure 4.6, we plot the modulus squared of the coefficients defining the images from Figure 4.5. These are normalized such that the maximum value is 1. It is clear that the coefficients of the high-order $\Phi_{\ell,p}$ modes are attenuated in the diffraction-limited image and recovered after the division by $\lambda_{\ell,p}$. In this experiment, we have found that a good threshold for the eigenvalues $\lambda_{\ell,p}$ was given by 0.05. In conclusion, we have successfully performed super-resolution imaging in a $4f$ system containing a circular aperture. This is, to the author's knowledge, the first experimental implementation of eigenmode super-resolution.

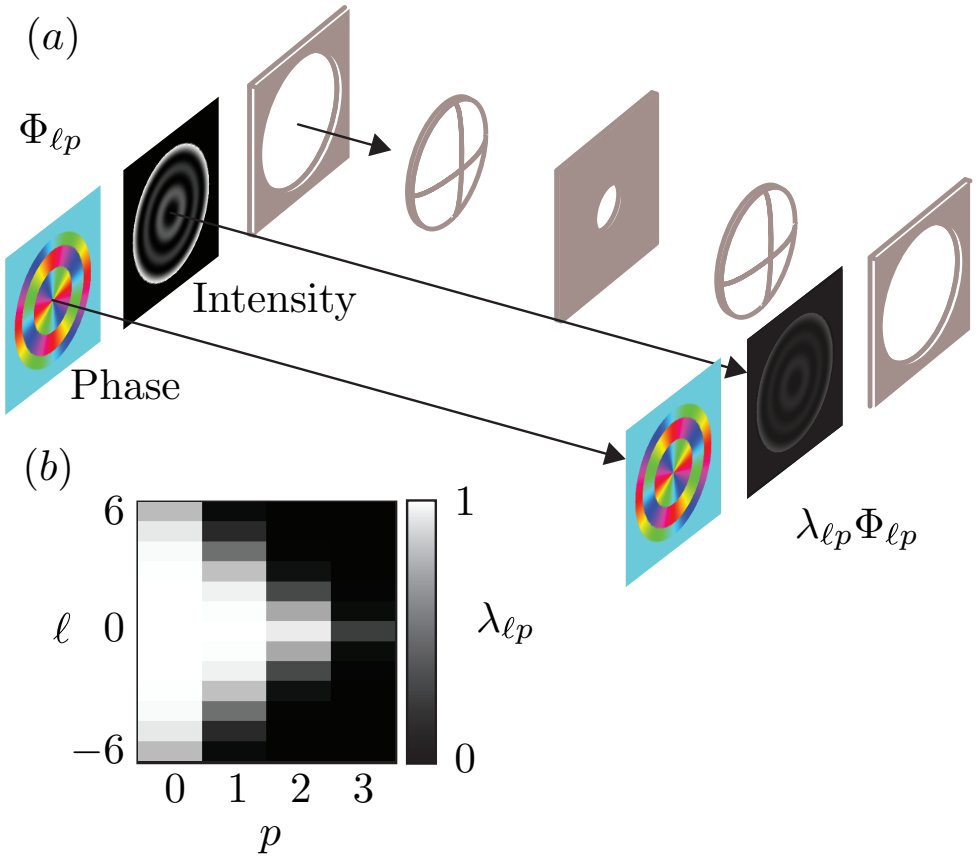

Figure 4.3: (a) This provides a visual demonstration of the transmission of eigenmodes through a $4f$ system (Φ_{22} is shown here). Upon transmission, the eigenmodes are unchanged apart from an attenuation in amplitude: $\Phi_{\ell p} \mapsto \lambda_{\ell p}\Phi_{\ell p}$. (b) This is a subset of the eigenvalues $\lambda_{\ell p}$ with $c = 10$. These values decay rapidly with increasing ℓ and p.

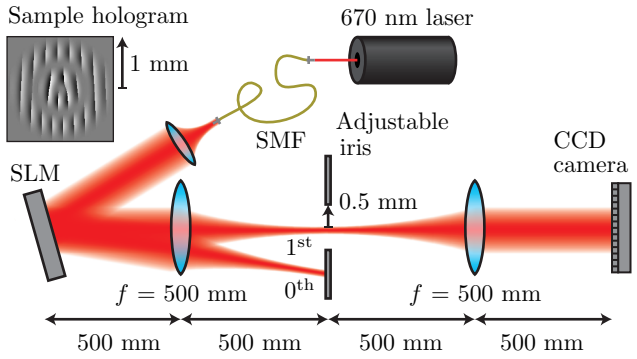

Figure 4.4: This is a schematic of the experimental setup used in our first experiment involving eigenmode super-resolution. Here, we use the known eigenmodes of the $4f$ system to achieve super-resolution.

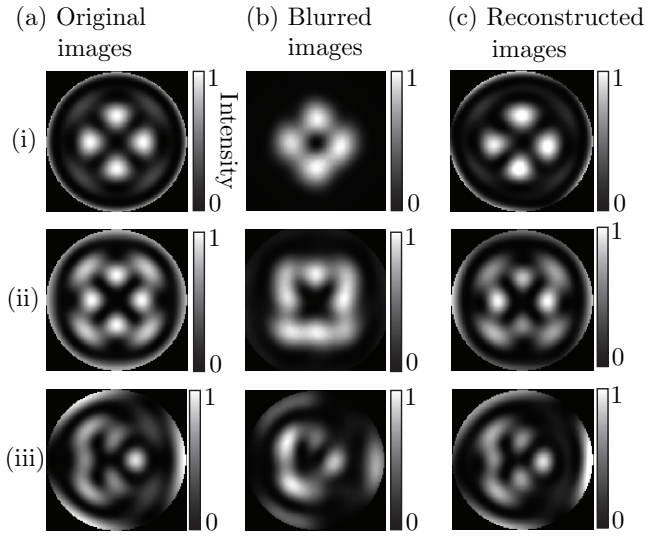

Figure 4.5: These are the results of our first eigenmode super-resolution experiment. (a) The objects or 'original images' that were generated by the SLM and propagated through the system. (b) The recorded diffraction-limited images. (c) The images after the reconstruction. These images are contained within a 1 mm radius. The super-resolution factors for these images are (i) 0.89, (ii) 0.49, and (iii) 0.45.

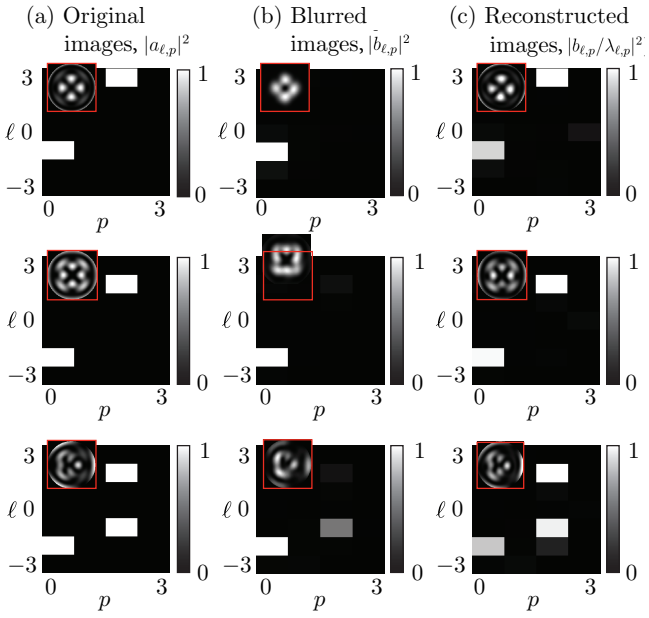

Figure 4.6: These are the moduli squared of the coefficients defining the images in Fig. 4.5 normalized to 1: (a) $\{|a_{\ell,p}|^2\}$, (b) $\{|b_{\ell,p}|^2\}$, (c) $\{|b_{\ell,p}/\lambda_{\ell,p}|^2\}$. The insets indicate the corresponding image at each stage.

4.4 Generalization to arbitrary optical systems

In the previous sections, we have assumed that the eigenmodes of the imaging system of interest are known. However, this is not always the case and a numerical method is required

to find them. In this section, we develop our technique for numerically determining the eigenmodes of an arbitrary linear optical imaging system and show how to apply it to achieve super-resolution [6].

Linear optical systems can be described as a matrix mapping the input fields (objects) to output fields (images). Finding the eigenvectors of this characteristic matrix is equivalent to finding the eigenmodes of the optical system. In order to do this, we first need to define a complete orthonormal basis $\{\psi_i\}$ of complex fields. Using this basis, we can write any arbitrary field Ψ as

$$\Psi = \sum_i c_i \psi_i, \tag{4.14}$$

where $\{c_i\}$ is a set of complex numbers. This set also defines the column vector ψ associated with the field Ψ.

The transmission matrix T of the imaging system can be found by propagating each of the basis modes ψ_i through the system one by one and recording the output. The elements of the transmission matrix are given by

$$T_{ij} = \langle S[\psi_i], \psi_j \rangle, \tag{4.15}$$

where $S[\psi_i]$ is the image at the output of the system given that the object is ψ_i. We are now set to find the eigenvalues and eigenvectors of the system. This is done by solving the eigenvalue equation $T\varphi_i = \lambda_i \varphi_i$ where φ_i are the eigenvectors and λ_i are the eigenvalues. With these, one can easily determine the eigenmodes Φ_i of the imaging system:

$$\Phi_i = \sum_{j=1}^{N} \varphi_{ij} \psi_j, \tag{4.16}$$

where N is the number of eigenmodes and φ_{ij} is the jth complex element of φ_i. We note that singular value decomposition (SVD) could have been used here instead at the cost of increased computation time [63]. In that case, the image must be decomposed with the right singular vectors and then reconstructed with the left singular vectors.

In the previous sections, it was assumed that the eigenmodes are orthonormal. This is not generally the case as is indicated from non-normal transmission matrices [83]. We now provide a method to reconstruct the object with non-orthonormal eigenmodes (this is not required for SVD since singular vectors are by definition orthogonal). We can still write the

object A as a super-position of eigenmodes

$$A = \sum_{i=1}^{N} a_i \Phi_i. \tag{4.17}$$

The set $\{a_i\}$ is unique since the eigenmodes are linearly independent. The image $S[A] = B$ of this object after propagation through the system is

$$B = \sum_{i=1}^{N} \lambda_i a_i \Phi_i. \tag{4.18}$$

We can no longer directly measure the coefficients of B to determine the values of a_i as we did in the previous sections because the eigenmodes are not guaranteed to be orthogonal. Instead, consider the overlap between the image B and the eigenmode Φ_j:

$$\left\langle \sum_{i=1}^{N} \lambda_i a_i \Phi_i, \Phi_j \right\rangle = \langle B, \Phi_j \rangle. \tag{4.19}$$

This can be expanded as

$$\lambda_1 \varphi_1 \cdot \varphi_j a_1 + \cdots + \lambda_N \varphi_N \cdot \varphi_j a_N = b \cdot \varphi_j = \langle B, \Phi_j \rangle, \tag{4.20}$$

where b is the column vector for B in ψ_i basis. We must now look at the full system of equations for these overlap equations. This can be expressed as a matrix multiplication:

$$\begin{bmatrix} \lambda_1 \varphi_1 \cdot \varphi_1 & \cdots & \lambda_N \varphi_N \cdot \varphi_1 \\ \vdots & \ddots & \vdots \\ \lambda_1 \varphi_1 \cdot \varphi_N & \cdots & \lambda_N \varphi_N \cdot \varphi_N \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_N \end{bmatrix} = \begin{bmatrix} b \cdot \varphi_1 \\ \vdots \\ b \cdot \varphi_N \end{bmatrix}. \tag{4.21}$$

This can be expressed more succinctly as

$$\Lambda a = \Gamma, \tag{4.22}$$

where Λ is the matrix of overlaps between eigenmodes weighted by the corresponding eigenvalue, a is the column vector defining the object, and Γ is the column vector of the overlap between the image B and the eigenvectors. Solving this equation for the column vector a allows us to reconstruct the object A through the use of Eq. 4.17.

Let us now take into account the noise introduced in real imaging systems. Again, we can define some noise threshold n_{thres} where any eigenmode with an eigenvalue below this

is ignored. The number of eigenmodes used in the reconstruction is therefore given by $N_{\text{thres}} \leq N$ with $\lambda_i \geq n_{\text{thres}}$. We must therefore solve a modified version of Eq. 4.21 where we only keep the first N_{thres} by N_{thres} block for Λ' and both A' and Γ' are column vectors with N_{thres} entries: $\Lambda' A' = \Gamma'$. The effects of discarding eigenmodes in the reconstruction of objects has been discussed in great detail in other works [62, 45, 63, 72, 73]. Some calibration will be required to find the proper threshold for a particular imaging system. In summary, we have removed two key assumptions from the original eigenmode super-resolution technique thus making it more widely applicable.

4.5 Numerical simulations of various optical systems

In this section, we show and discuss the results of numerical simulations of our new technique for eigenmode super-resolution outlined above [6]. The imaging system that we simulated consisted of a $4f$ system with an aperture or aberration in the central plane, see Figure 4.7. We also set a finite radius R in the object and image planes. The eigenmodes of these imaging systems are not known and we must use our method to determine them in order to achieve super-resolution. The diffraction in this system is determined by the size and shape of the aperture. For our first simulation, we chose a 1 mm by 1 mm square aperture. We then simulated aberrations using the Zernike polynomials, Z_2^0 and Z_2^2. These correspond to defocusing and astigmatism respectively. The magnitude of these aberrations are given by the amplitude of the polynomials z.

We chose the Laguerre-Gaussian (LG) basis $\{\psi_i\} = \{LG_{\ell,p}\}$ with $-5 \leq \ell \leq 5$ and $0 \leq p \leq 10$ as our characterization basis. A basis must be selected such that it probes all the degrees-of-freedom of the imaging system. Apart from a select few imaging systems, the number of degrees-of-freedom is not known analytically. In these cases, it is sufficient to select a basis that shares symmetry characteristics with the imaging system and include all modes with a significant transmission through the system. The closer the initial basis is to the eigenmodes, the fewer modes are required in the analysis. For example, to obtain the same results as with 121 LG modes, we required to use approximately 900 plane waves.

Results for the system with the square aperture are given in Figure 4.8. Here we use 56 eigenmodes in the reconstruction and get a super-resolution factor $S_r = 0.32$. Comparing the diffraction-limited and the reconstructed image, it is clear that this level of super-resolution is significant. The reconstructed image is clearly a ring, but no such conclusion can be said about the blurred image. The eigenmodes of this system were found to be non-orthogonal and we therefore required Eq. 4.21 to reconstruct the image.

The results for a system in the presence of defocus with a magnitude of $z = 48$ radians

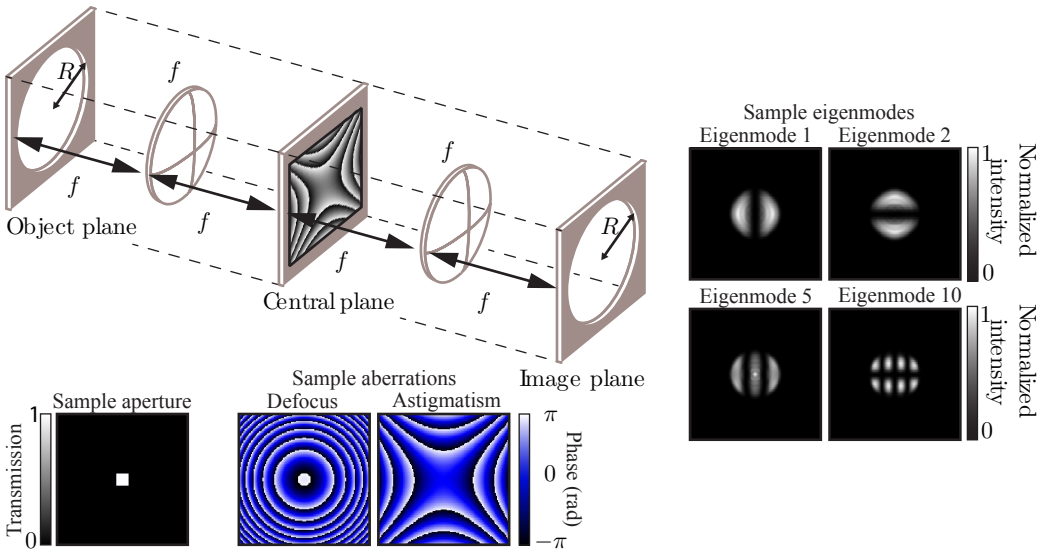

Figure 4.7: Schematic of the $4f$ optical imaging system used in the numerical simulations of our new technique for eigenmodes super-resolution. Here the central plane was modified to contain either a diffracting aperture or aberrations. We set $f = 1$ m, $R = 2$ mm, and the wavelength to 633 nm. We also show the first, second, fifth and tenth eigenmodes of the system in the presence of astigmatism of amplitude $z = 100$ radians across the simulation region along with a sample aperture and sample aberrations for defocus and astigmatism.

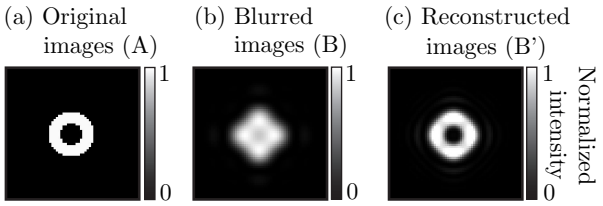

Figure 4.8: Results of our numerical simulation of a $4f$ system with a square aperture of size 1 mm by 1 mm. 56 eigenmodes are used in the reconstruction and the super-resolution factor is $S_r = 0.32$.

across the simulation region is given in Figure 4.9. It is clear from these results that, despite the introduction of some noise in the reconstructed image, there is a drastic increase in image quality. The main features of the objects which are lost upon propagation though the aberration are recovered. These reconstructions were done with 59 eigenmodes and the super-resolution factors S_r are (i) 1.7 and (ii) 1.2.

Finally, the results for a system with astigmatism of amplitude $z = 100$ radians are shown in figure 4.10. Again, we have a striking amount of resolution gain. For this case, the reconstructed images used 49 eigenmodes and the super-resolution factors S_r are (i) 1.3 and (ii) 1.0. A subset of the eigenmodes for this system are given in Figure 4.4.

Figure 4.11 shows the super-resolution factors S_r for two images (a. two lines and b. a

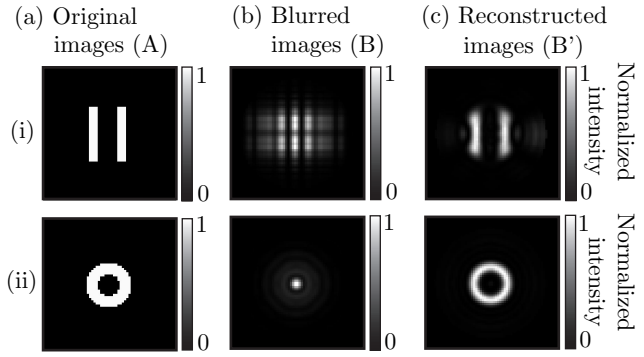

Figure 4.9: Results of our numerical simulation in the presence of defocus of amplitude $z = 48$ radians across the simulation region. 59 eigenmodes are used in each reconstruction and the super-resolution factors S_r are (i) 1.7 and (ii) 1.2.

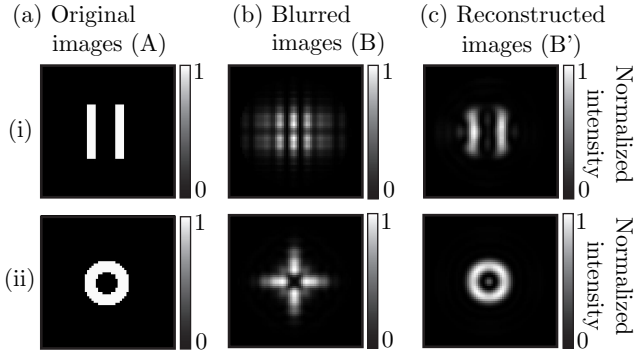

Figure 4.10: Results of our numerical simulation in the presence of astigmatism of amplitude $z = 100$ radians across the simulation region. 49 eigenmodes are used in each reconstruction and the super-resolution factors S_r are (i) 1.3 and (ii) 1.0.

circle) as a function of the total number of eigenmodes used in the reconstruction N_{thres} and the magnitude of the astigmatism z. It is clear that both images have a range in which super-resolution occurs. Since these are different objects, the overlap with each eigenmode is different, and this will lead to different optimal values for N_{thres}. However, an effective operating point N_{thres} can be chosen such that both images achieve super-resolution. We therefore have that eigenmode super-resolution is neither object nor imaging system specific.

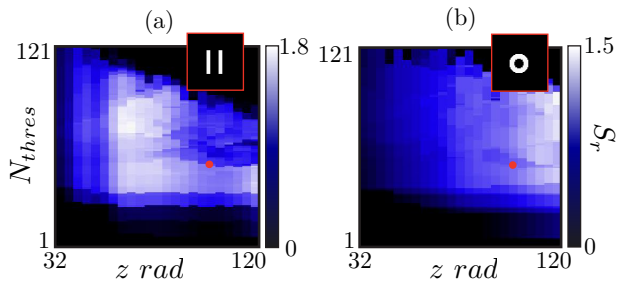

Figure 4.11: These graphs show the super-resolution factors S_r for two reconstructed images (object shown as inset) as a function of amplitude of astigmatism z and the number of eigenmodes used in the reconstruction, N_{thres}. The red dots indicates the images in Figure 4.10 (colour online). It is clear from these graphs that the super-resolution factor depends on both the imaging system and the object. However, it is also clear that there is a large area of overlap where both objects are super-resolved. This demonstrates the object independence of optical eigenmode imaging.

4.6 Experiment #2: $4f$ system using the generalized method

In this section, we go back and apply our new technique of eigenmode super-resolution imaging to the $4f$ system given in Figure 4.1. A schematic of the experimental setup is given in Figure 4.12. We start by splitting the output of a 633 nm HeNe laser into a reference beam and an imaging beam with a PBS. The relative intensity of these arms is controlled by a half-wave plate before the PBS. The imaging arm is reflected onto a SLM (Holoeye Pluto) and then sent through a $4f$ system with a circular aperture in the focal plane of the lens. Similarly to the previous experiment, this aperture introduces diffraction into the system and filters out the first diffraction order reflected off of the SLM. The field at the output of the $4f$ system is then demagnified using two lenses. This demagnification is required to have the reference beam completely cover the image. The two beams are finally brought together using a non-polarizing beam splitter NPBS. A Glan-Taylor polarizer is then used to project both beams onto the same polarization allowing interference. The output is measured with a CCD camera (Thorlabs). The focal length of the lenses in the $4f$ system are 50 mm, the aperture has a radius of 15μ m and the beam waist of the object incident on the system is 1.5 mm. The space-bandwidth product of this system is $c \approx 10$. We used the LG modes as our basis with $-6 \leq \ell \leq 6$ and $0 \leq p \leq 2$. We also used the LG modes and superpositions of LG modes as objects.

Our results are summarized in Figure 4.13. Here, we do not have a striking increase in resolution like in the previous experiment and simulations. By comparing the measured

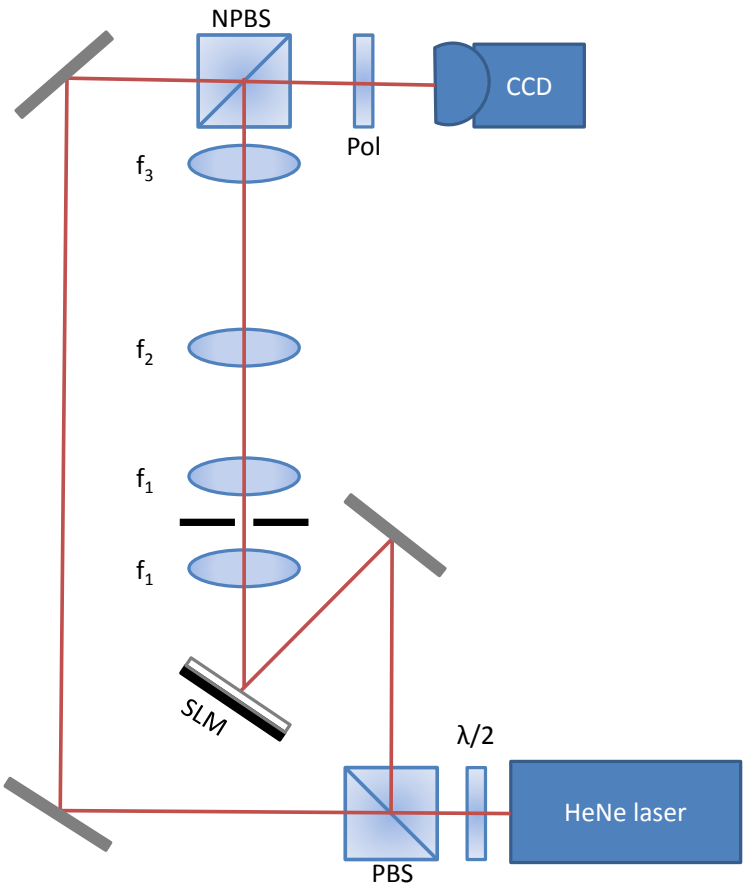

Figure 4.12: Schematic of the experimental set-up for our second experiment. Here we apply our new technique for eigenmode super-resolution imaging to a $4f$ system similar to the one used in the first experiment. We set $f_1 = 50$ mm, $f_2 = 35$ mm, and $f_3 = 100$ mm.

images and the reconstructed images we find a small amount of increased resolution in the first two images ($LG_{1,0}$ and $LG_{-1,0}$). This is reinforced by the super-resolution factors S_r of (i) 0.61 and (ii) 0.26. We have therefore achieved super-resolution for these images. However, looking at images (iii) and (iv), there is no clear increase in resolution. The super-resolution factors S_r for these images are given by (iii) -0.06 and (iv) 0.006. We therefore have a decrease in resolution for our third object and no significant change to the resolution for the fourth object. These images are included to demonstrate that objects composed of superpositions of the basis modes (objects iii and iv) are more sensitive to noise than individual basis modes used as objects (objects i and ii). In addition, by looking at the diffracted-limited images we see some distortions that are not expected from this system. One of the rings is cut and the two lobes of object (iv) are not evenly distributed at the output. We attribute these to a misalignment in the setup.

Next, we simulated this same system numerically and received drastically different re-

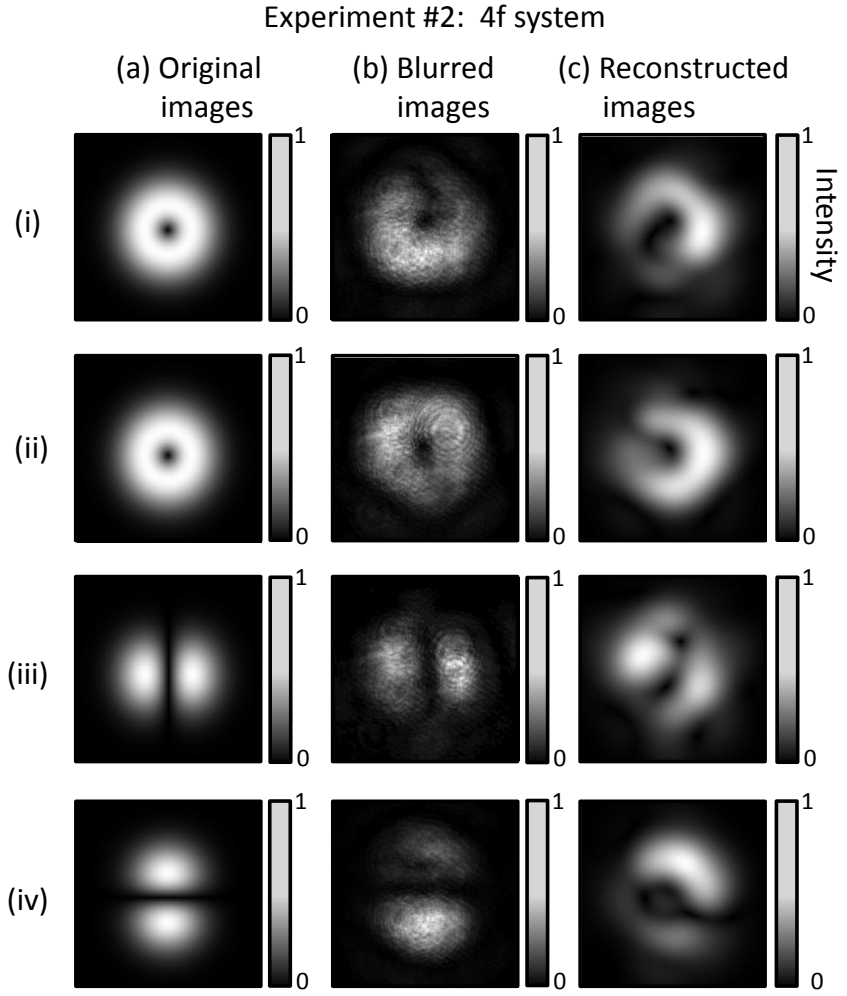

Figure 4.13: Results of our second experiment where we applied our new technique for eigenmode super-resolution imaging to the same system used in the original experiment. Four eigenmodes were used in the reconstruction and the super-resolution factors are (i) 0.61, (ii) 0.26, (iii) -0.06, and (iv) 0.006.

sults, see Figure 4.14. In our simulation, we achieve perfect super-resolution. However, this required almost all of the eigenmodes to reconstruct the object. This was not possible in the experiment as noise was already becoming a significant factor after the first few eigenmodes. This is why only 4 eigenmodes are used in the reconstruction. This is the main limiting factor to our ability to reconstruct the objects. Notice that we achieved super-resolution in the experiment with a super-resolution factor greater than the maximum given in the simulation. This is due to noise and misalignments introducing errors that are not present in the simulation. This increases the maximum achievable super-resolution factor.

In summary, we have experimentally achieved super-resolution in a $4f$ system using our

new eigenmode imaging technique for a select few objects. However, some objects are still unrecoverable due to the significant amount of noise in the system. We have also simulated this experiment and achieved perfect super-resolution for all input images (objects) indicating that this technique is applicable assuming that one can increase the signal-to-noise ratio.

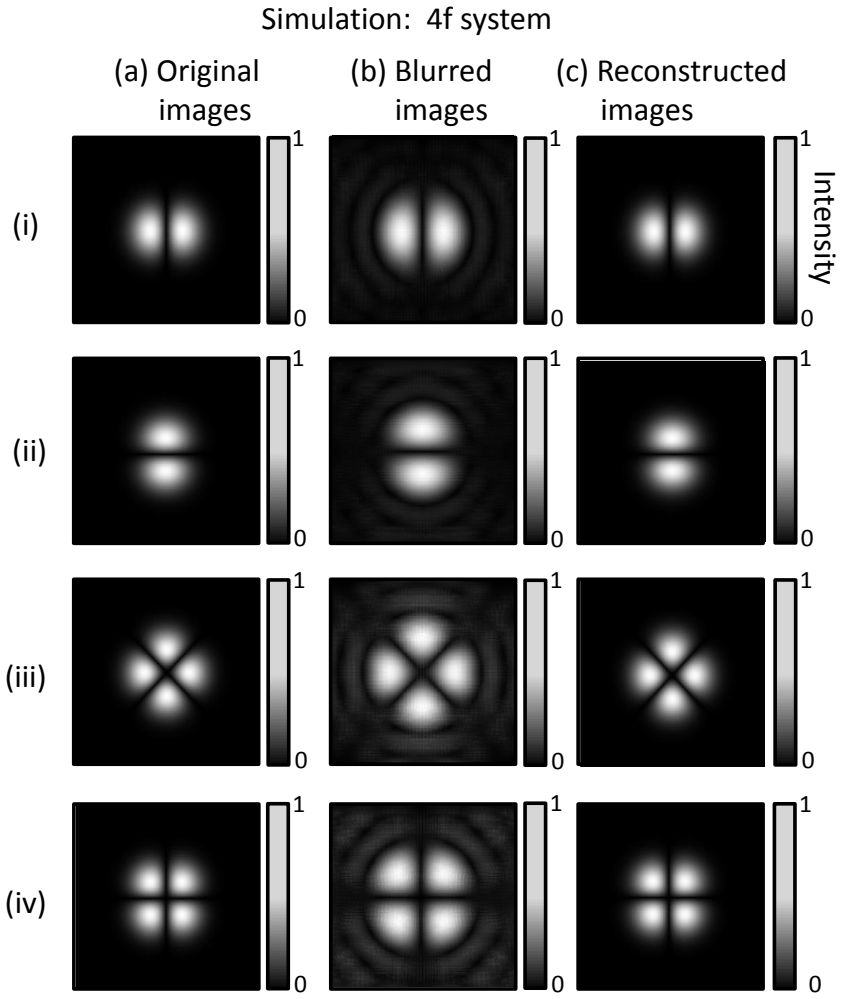

Figure 4.14: Results from our simulation of the experiment in Figure 4.12. Here, 33 eigenmodes were used in the reconstruction and the super-resolution factors are (i) 0.14, (ii) 0.14, (iii) 0.43, and (iv) 0.43. These super-resolution factors are the maximum values as we have achieved perfect super-resolution.

4.7 Experiment #3: Application to a multi-mode fibre

Multi-mode fibres (MMF) have many potential applications. However, they introduce a large degree of aberration and diffraction and, for this reason, remain largely unused. Eigenmode

super-resolution imaging provide a method for aberration and diffraction correction and are therefore a natural fit to work with MMFs. In this final section, we provide a proof of concept for applying eigenmode imaging to a MMF. The experimental setup is shown in Figure 4.15. We start by expanding the beam of the 633 nm HeNe laser to a radius of $R_o = 1$ mm using two lenses. We then split the beam with a half-wave plate and a PBS. The half-wave plate gives us control over the relative power of the two beams. The imaging beam is sent to a SLM (Holoeye Pluto) and then filtered by a $4f$ system with an aperture. This aperture is small enough to filter out the other diffraction orders but large enough not to cause diffraction. The $4f$ system also images the SLM onto a 20x objective coupling into a 20 cm long, 10 μm core multi-mode optical fibre. The output of the fibre is expanded and columnized by a second 20x objective and then sent through a half-wave plate and a quarter-wave plate. After these wave plates, the two beams are brought back together with a second PBS with a Glan-Taylor polarizer (Pol) at the output. We adjust the waveplates before the second PBS such that the majority of the light is transmitted through the PBS. This step is required as multi-mode fibres are not necessarily polarization preserving. The first wave plate is adjusted so that the image (output of fibre) and reference beams have approximately the same intensity for as many basis modes and images as possible. The ouput is recorded with a CCD camera (Thorlabs). Again, we used the LG modes as our basis with $-5 \leq \ell \leq 5$ and $0 \leq p \leq 2$.

The results are given in Figure 4.16. Comparing the objects with their respective recorded image and the reconstructed image is difficult due to the large degree of aberration. This comparison is more easily done with the use of the super-resolution factor S_r. The measured values for S_r are (i) 1.1, (ii) -0.57, (iii) 0.87, and (iv) 15.0. We therefore have super-resolution in three of the four images with comparatively large S_r. However, despite these large S_r's, the reconstructed images are still not accurately depicting the objects. This is because S_r depends on the overlap between the image and the object which is very small for MMFs. In other words, the more diffracted an image is, the larger S_r needs to be before the reconstructed image starts to look like the object. We also showed the result of a failed reconstruction. This is to highlight that, for systems with large aberrations like MMFs, it is not simple to tell apart a successful reconstruction from a failed one.

In summary, we have achieved limited super-resolution in a MMF. This work is a proof-of-concept for the application of eigenmode imaging to MMFs and can be viewed as a first step towards new applications involving MMFs.

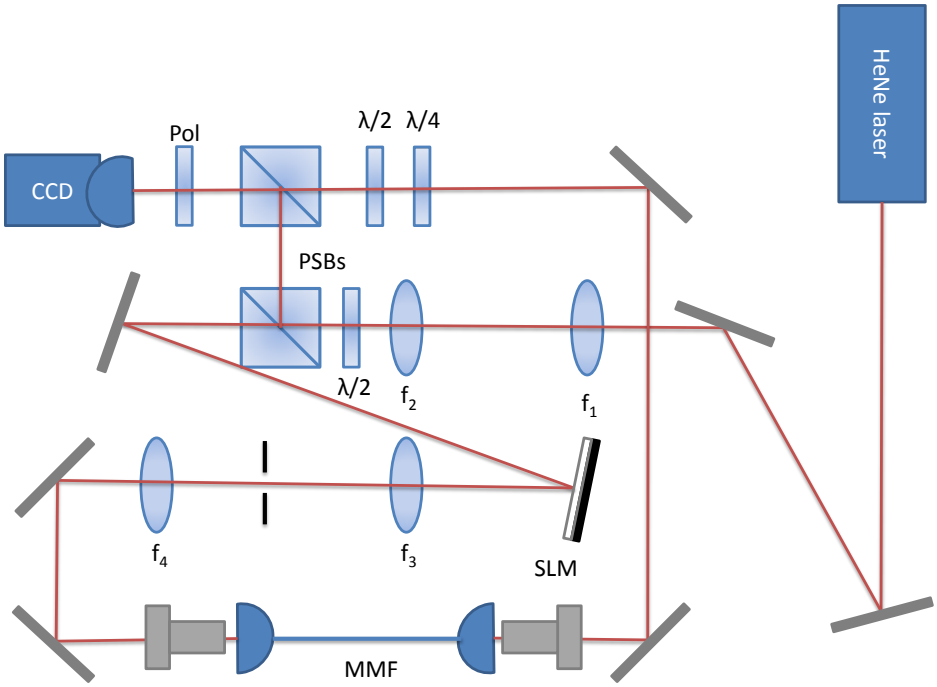

Figure 4.15: Experimental setup for our final experiment. Here we apply our technique to a multi-mode fibre (MMF). We set $f_1 = f_3 = f_4 = 100$ mm and $f_2 = 50$ mm. The MMF we used was 20 cm long and had a 10 μm core. The objectives have a 20x magnification

4.8 Conclusions

In summary, we have looked at our final limiting behaviour in physics. Diffraction and aberrations limit the resolution of imaging systems. Techniques that correct for this diffraction and aberration are called super-resolution techniques.

We report the first experimental realization of eigenmode super-resolution. The system used in this experiment was a diffraction-limited $4f$ system with a circular aperture [5]. This system is of particular importance as the theory for its quantum limit to resolution is already developed [72, 73]. Thus, this work represents a step towards realizing this experiment. In addition, we also provide a method to find the eigenmodes of arbitrary linear optical systems [6]. We also generalize the eigenmode super-resolution method for non-orthogonal eigenmodes. Furthermore, we numerically simulated various diffraction-limited and aberrated optical systems and applied this new technique. The result was a significant improvement in image quality. Finally, we apply our technique experimentally for the case of a $4f$ system and a multi-mode fibre. In these final experiments, we achieve limited super-resolution. However, they serve as a nice proof-of-concept. The signal-to-noise ratio of an

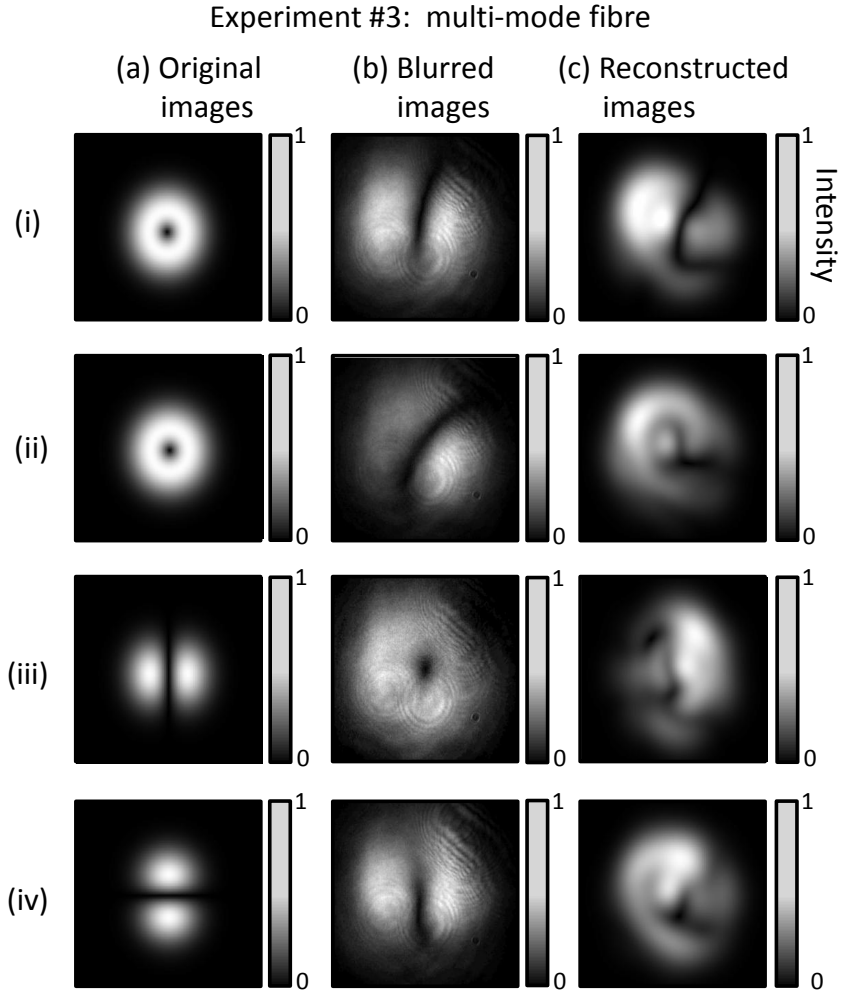

Figure 4.16: Experimental results for the multi-mode fibre experiment. Here we used 4 eigenmodes in the reconstruction and the super-resolution factors are (i) 1.1, (ii) -0.57, (iii) 0.87, and (iv) 15.0.

imaging system is what limits our ability to perform super-resolution.

Future research will focus on examining the quantum limits to resolution in optical system due to quantum fluctuations. In addition, eigenmodes will eventually enable imaging through turbulence, allow for quantum key distribution through optical fibres, and finally form an optimal basis for lithography.

Chapter 5

Conclusions

In this thesis, we have taken a comprehensive look at several phenomena. These include the duality principle, delegated quantum computation, and super-resolution. All of these phenomena exhibit limiting behaviour, that is, certain properties of the system of interest are bounded by another. In the case of the duality principle, this bounded behaviour is mutual, meaning that the two properties bound each other. The duality principle prohibits the coexistence of degree of interference and which-alternative information of a qubit. In the other two cases, delegated quantum computation and super-resolution, the bound is one-sided. This is clearly seen in the case of super-resolution. Here, the quantity of interest is the resolution of images. Diffraction lowers the resolution of these images, but increased resolution does not necessarily mean less diffraction. This increased resolution can be due to super-resolution. Finally, in delegated quantum computation, a client wishes to make a query to a quantum server. The quantity of interest is security. However, the highest achievable security depends on the quantum power of the client. With too little quantum power, the client cannot have perfect information theoretic security. However, if a certain threshold of quantum power is reached, perfect security is achievable.

The first topic of discussion was the duality principle. Here we developed a general framework to explain any apparent violation of the duality principle and demonstrated it experimentally. We also found a relation between the sub-fidelity and the maximum recoverable visibility as well as a relation between the duality principle and weak values. Finally we show that on average the coherence of a qubit can be completely recovered if one has access to half of the environment to which it is coupled. Future work will be focused on developing a comprehensive theory for the duality principle of quantum systems with Hilbert spaces of dimension larger than 2.

Our second topic was that of delegated quantum computing. We developed a new technique for generating the ancillary states required for the quantum computation on encrypted

data protocol. We also provide a proof of input-privacy for this new technique with an honest server. This can be viewed as a reduction in the quantum power required on the clients end and is a step towards a complete theory describing the minimum required power for perfect information theoretic security. Future work will also look into the transition away from perfect security due to lowered quantum power on the client's side.

The final topic was super-resolution. Here we performed the first experimental implementation of eigenmode super-resolution [5]. In addition, we developed a method to determine the eigenmodes of a system numerically and generalize the reconstruction algorithm to include non-orthogonal eigenmodes [6]. Finally, we apply this method numerically and experimentally for multiple optical systems, including a multi-mode fibre, with various degrees of success. Future work will be focused in reaching the quantum limit to eigenmode super-resolution.

Appendix: Calculation of $\mathcal{C}_2$

What follows is our derivation of $\mathcal{C}_2$. The first step is to recall that the trace norm of a matrix x is given by the sum of the singular values of x. These singular values are the eigenvalues of the positive matrix $|x| = \sqrt{x^\dagger x}$. Let's denote the two eigenvalues of $x^\dagger x$ by α and β. It then holds that $\mathrm{Tr}|\hat{X}_\mathcal{A}| = \sqrt{\alpha} + \sqrt{\beta}$. Next, we express the sum of two square roots in terms of the elementary symmetric polynomials in two variables $s_1 = \alpha + \beta$ and $s_2 = \alpha\beta$ as

$$\mathrm{Tr}|\hat{X}_\mathcal{A}| = \sqrt{\alpha} + \sqrt{\beta} = \sqrt{s_1 + 2\sqrt{s_2}}. \tag{5.1}$$

The last step is to express the symmetric polynomials in terms of traces, which can be done elegantly via Newton's identities:

$$s_1 = \mathrm{Tr}(y), \tag{5.2a}$$
$$2s_2 = \mathrm{Tr}(y)^2 - \mathrm{Tr}(y^2), \tag{5.2b}$$
$$6s_3 = \mathrm{Tr}(y)^3 - 3\mathrm{Tr}(y)\mathrm{Tr}(y^2) + 2\mathrm{Tr}(y^3), \tag{5.2c}$$
$$\text{etc.}$$

We have $y = \hat{X}_\mathcal{A}^\dagger \hat{X}_\mathcal{A}$. Let's now expand $\hat{X}_\mathcal{A}$ in its most general form:

$$\hat{X}_\mathcal{A} = \frac{1}{\sqrt{p_0 p_1}} \begin{pmatrix} \sqrt{r_0 s_0}\langle e_{10}|e_{00}\rangle & e^{i\theta'}\sqrt{r_0 s_1}\langle e_{11}|e_{00}\rangle \\ e^{-i\theta}\sqrt{r_1 s_0}\langle e_{10}|e_{01}\rangle & e^{-i(\theta-\theta')}\sqrt{r_1 s_1}\langle e_{11}|e_{01}\rangle \end{pmatrix}, \tag{5.3}$$

where $|e_{qa}\rangle$ are the states of $\mathcal{I}$ conditioned on the alternatives of qubits $\mathcal{Q}$ and $\mathcal{A}$. The positive numbers r_a and s_a are the relative probabilities of $|e_{0a}\rangle$ and $|e_{1a}\rangle$, respectively. θ and θ' are the phases of the states of $\mathcal{A}$ conditioned on the alternatives of $\mathcal{Q}$. For simplicity, we rewrite this as

$$\hat{X}_\mathcal{A} = \begin{pmatrix} a & c \\ d & b \end{pmatrix}. \tag{5.4}$$

Plugging this into Eq. 5.1 gives us

$$\mathrm{Tr}|\hat{X}_{\mathcal{A}}|^2 = |a|^2 + |b|^2 + |c|^2 + |d|^2 + 2|ab - cd|. \tag{5.5}$$

We now expand $|a|^2 + |b|^2 + |c|^2 + |d|^2$ in terms of the quantities given in Eq. 5.3:

$$\mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|00}\tilde{\psi}_{\mathcal{I}|10}) + \mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|00}\tilde{\psi}_{\mathcal{I}|11}) + \mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|01}\tilde{\psi}_{\mathcal{I}|10}) + \mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|01}\tilde{\psi}_{\mathcal{I}|11}) = \mathrm{Tr}(\hat{\psi}_{\mathcal{I}|0}\hat{\psi}_{\mathcal{I}|1}), \tag{5.6}$$

where $\tilde{\psi}_{\mathcal{I}|0a} = r_a|e_{0a}\rangle\langle e_{0a}|$ and $\tilde{\psi}_{\mathcal{I}|1a} = s_a|e_{1a}\rangle\langle e_{1a}|$ are *unnormalized* states. Consequently, $\hat{\psi}_{\mathcal{I}|q} = \tilde{\psi}_{\mathcal{I}|q0} + \tilde{\psi}_{\mathcal{I}|q1}$ are the normalized states of $\mathcal{I}$ conditioned on $\mathcal{Q}$ while ignoring (tracing away) $\mathcal{A}$.

To evaluate the final term, we first begin by rewriting $|ab-cd|$ as $\sqrt{(ab-cd)(a^*b^*-c^*d^*)}$. We then expand what is under the square root and then add and subtract the following term:

$$\mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|00}\tilde{\psi}_{\mathcal{I}|11})\mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|01}\tilde{\psi}_{\mathcal{I}|11}) + \mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|00}\tilde{\psi}_{\mathcal{I}|10})\mathrm{Tr}(\tilde{\psi}_{\mathcal{I}|01}\tilde{\psi}_{\mathcal{I}|10}). \tag{5.7}$$

Finally, simplifying the result using the identity $\mathrm{Tr}(XY)\mathrm{Tr}(XZ) = \mathrm{Tr}(XYXZ)$, which holds for any X with rank-1, gives us

$$\mathrm{Tr}|\tilde{\chi}_A|^2 = \mathrm{Tr}(\hat{\psi}_E^{(0)}\hat{\psi}_E^{(1)}) + \sqrt{2}\sqrt{[\mathrm{Tr}(\hat{\psi}_E^{(0)}\hat{\psi}_E^{(1)})]^2 - \mathrm{Tr}[(\hat{\psi}_E^{(0)}\hat{\psi}_E^{(1)})^2]} = E(\hat{\psi}_E^{(0)}, \hat{\psi}_E^{(1)}) \tag{5.8}$$

We can extend this analysis to the case of higher dimensions of the accessible qubit $\mathcal{A}$. As an example, consider the generalization to $\dim(\mathcal{A}) = 3$. In this case, we have three singular values and by following similar steps to the original solution, we find that

$$\begin{aligned}\mathrm{Tr}|\tilde{\chi}_A| &= \sqrt{\alpha} + \sqrt{\beta} + \sqrt{\gamma} \\ &= \sqrt{s_1 + 2\sqrt{s_2 + 2\sqrt{s_3}\,\mathrm{Tr}|\tilde{\chi}_A|}},\end{aligned} \tag{5.9}$$

where the symmetric polynomials are now in three variables: $s_1 = \alpha+\beta+\gamma$, $s_2 = \alpha\beta+\beta\gamma+\gamma\alpha$ and $s_3 = \alpha\beta\gamma$ and they still satisfy Eq. 5.2. Now, one can solve equation Eq. 5.9 for $\mathrm{Tr}|\tilde{X}_{\mathcal{A}}|$ and find $\mathcal{C}_3$. In principle, it is possible to extend this method to higher dimensions and find a whole family of distinguishability measures F_a. However, the problem becomes quickly intractable due to the fact that the number of terms that are necessary grows very rapidly and the degree of the equations to solve increases.

Bibliography

[1] R. Menzel, D. Puhlmann, A. Heuer, and W.P. Schleich. Wave-particle dualism and complementarity unraveled by a different mode. *PNAS*, 109(24):9314, 2012.

[2] J. Leach, E. Bolduc, F.M. Miatto, K. Piché, G. Leuchs, and R.W. Boyd. The duality principle in the presence of postselection. *ArXiv*, 2:1406.4300, 2014.

[3] F.M. Miatto, K. Piché, T. Brougham, and R.W. Boyd. The optical bound of quantum erasure with limited means. *ArXiv*, 1:1410.2313, 2014.

[4] F.M. Miatto, K. Piché, T. Brougham, and R.W. Boyd. Recovering full coherence in a qubit by measuring half of its environment. *ArXiv*, 2:1502.07030, 2015.

[5] K. Piché, J. Leach, A.S. Johnson, J.Z. Salvail, M.I. Kolobov, and R.W. Boyd. Experimental realization of optical eigenmode super-resolution. *Opt. Express*, 20:26424, 2012.

[6] A.S. Johnson, K. Piché, J.Z. Salvail, J. Leach, and R.W. Boyd. Eigenmode super-resolution imaging in arbitrary optical systems. *J. Mod. Opt.*, 60:1932, 2014.

[7] B.G. Englert and J.A. Bergou. Quantitative quantum erasure. *Opt. Comm.*, 179:337, 2000.

[8] M .O. Scully and H. Walther. Quantum optical test of observation and complementarity in quantum mechanics. *Phys. Rev. A*, 39(10):5229, 1989.

[9] M. Brune, E. Hagley, J. Dreyer, X. Maître, A. Maali, C. Wunderlich, J.M. Raimond, and S. Haroche. Observing the progressive decoherence of the "meter" in a quantum measurement. *Phys. Rev. Lett.*, 77:4887, 1996.

[10] C.J. Myatt, B.E. King, Q.A. Turchette, C.A. Sackett, D. Kielpinski, W.M. Itano, C.W. Monroe, and D.J. Wineland. Decoherence of quantum superpositions through coupling to engineered reservoirs. *Nature*, 403(6767):269, 2000.

[11] W.H. Zurek. Decoherence, einselection, and the quantum origins of the classical. *Rev. Mod. Phys.*, 75:715, 2003.

[12] A. D'Arrigo, R.L. Franco, G. Benenti, E. Paladino, and G. Falci. Recovering entanglement by local operations. *Annals of Physics*, 350:211, 2014.

[13] A. Orieux, A. D'Arrigo, G. Ferranti, R.L. Franco, G. Benenti, E. Paladino, G. Falci, F. Sciarrino, and P. Mataloni. Experimental on-demand recovery of entanglement by local operations within non-markovian dynamics. *Sci. Rep.*, 5:8575, 02 2015.

[14] D.M. Greenberger and A. Yasin. Simultaneous wave and particle knowledge in a neutron interferometer. *Phys. Lett. A*, 128(8):391, 1988.

[15] A. Aspect and P. Grangier. Wave-particle duality for single photons. *Hyperfine Interactions*, 37(1-4):1, 1987.

[16] S. Dürr, T. Nonn, and G. Rempe. Fringe visibility and which-way information in an atom interferometer. *Phys. Rev. Lett.*, 81(26):5705, 1998.

[17] P.D.D. Schwindt, P.G Kwiat, and B.G. Englert. Quantitative wave-particle duality and nonerasing quantum erasure. *Phys. Rev. A*, 60(6):4285, 1999.

[18] M. Arndt, O. Nairz, J. Vos-Andreae, C. Keller, G. van der Zouw, and A. Zeilinger. Wave-particle duality of c60 molecules. *Nature*, 401:680, 1999.

[19] R. Kolesov, B. Grotz, G. Balasubramanian, R.J. Stohr, A.A.L. Nicolet, P.R. Hemmer, F. Jelezko, and J. Wrachtrup. Wave-particle duality of single surface plasmon polaritons. *Nature Physics*, 5:470, 2011.

[20] S. Kocsis, B. Braverman, S. Ravets, M.J. Stevens, R.P. Mirin, L.K. Shalm, and A.M. Steinberg. Observing the average trajectories of single photons in a two-slit interferometer. *Science*, 332(6034):1170, 2011.

[21] E. Bolduc, J. Leach, F.M. Miatto, G. Leuchs, and R.W. Boyd. Fair sampling perspective on an apparent violation of duality. *PNAS*, 111(34):12337, 2014.

[22] J. Adam Miszczak, M. Zbigniew, P. Horodecki, A. Uhlmann, and K. Zyczkowski. Sub- and super-fidelity as bounds for quantum fidelity. *Quantum Inf. Comput.*, 9:103, 2009.

[23] E. Schrödinger. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge Univ Press, 1935.

[24] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[25] J. Dressel and A.N. Jordan. Significance of the imaginary part of the weak value. *Phys. Rev. A*, 85(1):012107, 2012.

[26] J. Dressel and A.N. Jordan. Weak values are universal in von neumann measurements. *Phys. Rev. Lett.*, 109(23):230402, 2012.

[27] S. Pang, J. Dressel, and T.A. Brun. Entanglement-assisted weak value amplification. *Phys. Rev. Lett.*, 113:030401, 2014.

[28] J.S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber. Direct measurement of the quantum wavefunction. *Nature*, 474(7350):188, 2011.

[29] K. Życzkowski and I. Bengtsson. *Geometry of quantum states*. Cambridge University Press, 2006.

[30] G. Akemann, J.R. Ipsen, and M. Kieburg. Products of rectangular random matrices: Singular values and progressive scattering. *Phys. Rev. E*, 88:052118, 2013.

[31] S. M. Barnett. *Introduction of quantum information*. Oxford Master Series in Physics, 2009.

[32] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A*, 439:553, 1992.

[33] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484, 1997.

[34] R.P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[35] I.M. Georgescu, S. Ashhab, and F. Nori. Quantum simulation. *Rev. Mod. Phys.*, 86:153, 2014.

[36] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, 2009.

[37] K.A.G. Fisher, A. Broadbent, L.K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K.J. Resch. Quantum computing on encrypted data. *Nature Communications*, 5:3074, 2014.

[38] T. Morimae and T. Koshiba. Impossibility of secure cloud quantum computing for classical client. *ArXiv*, 1:1407.1636, 2014.

[39] D. Gottesman. The heisenberg representation of quantum computers. In *Proceedings of the 22nd International Colloquium on Group Theoretical Methods in Physics*, 1999.

[40] Anne Broadbent and Serge Fehr. A purification approach to input privacy.

[41] F.G.S.L. Brandao and J. Oppenheim. The quantum one-time pad in the presence of an eavesdropper. *Phys. Rev. Lett.*, 108:040504, 2012.

[42] F. Dupuis, J.B. Nielsen, and L. Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. *Advances in Cryptology - CRYPTO 2010*, 6223:685, 2010.

[43] E. Abbe. Beitrage zur theorie des mikroskops und der mikroskopischen wahrnehmung. *Arch. Mikrosk. Anat.*, 9:413, 1873.

[44] J.W.S. Rayleigh. Collected optics papers of lord rayleigh. *J. Op. Soc. Am.*, 9:413, 1994.

[45] G.T. DiFrancia. Degrees of freedom of an image. *J. Op. Soc. Am.*, 59(7):799, 1969.

[46] J.L. Harris. Diffraction and resolving power. *J. Op. Soc. Am.*, 54(7):931, 1964.

[47] W. Lukosz. Optical systems with resolving powers exceeding the classical limit. *J. Op. Soc. Am.*, 56(11):1463, 1966.

[48] J.B. Pendry. Negative refraction makes a perfect lens. *Phys. Rev. Lett.*, 85:3966, 2000.

[49] D.R. Smith. How to build a superlens. *Science*, 308:502, 2005.

[50] N. Fang, H. Lee, C. Sun, and X. Zhang. Sub-diffraction-limited optical imaging with a silver superlens. *Science*, 308:534, 2005.

[51] Z. Liu, H. Lee, Y. Xiong, C. Sun, and X. Zhang. Far-field optical hyperlens magnifying sub-diffraction-limited objects. *Science*, 315(5819):1686, 2007.

[52] E.T.F. Rogers, J. Lindberg, T. Roy, S. Savo, J.E. Chad, M.R. Dennis, and N.I. Zheludev. A super-oscillatory lens optical microscope for subwavelength imaging. *Nature Materials*, 11:432, 2012.

[53] S. Gazit, A. Szameit, Y.C. Eldar, and M. Segev. Super-resolution and reconstruction of sparse sub-wavelength images. *Opt. Express*, 17(26):23920, 2009.

[54] Y. Shechtman, Y.C. Eldar, A. Szameit, and M. Segev. Sparsity based sub-wavelength imaging with partially incoherent light via quadratic compressed sensing. *Opt. Express*, 19(16):14807, 2011.

[55] S.W. Hell and J. Wichmann. Breaking the diffraction resolution limit by stimulated emission: stimulated-emission-depletion fluorescence microscopy. *Opt. Lett.*, 19:780, 1994.

[56] S.W. Hell. Far-field optical nanoscopy. *Science*, 316(5828):1153, May 2007.

[57] H. Shin, K.W.C. Chan, H.J. Chang, and R.W. Boyd. Quantum spatial superresolution by optical centroid measurements. *Phys. Rev. Lett.*, 107:083603, 2011.

[58] V. Giovannetti, S. Lloyd, L. Maccone, and J.H. Shapiro. Sub-rayleigh-diffraction-bound quantum imaging. *Phys. Rev. A*, 79:013827, 2009.

[59] F. Guerrieri, L. Maccone, F.N.C. Wong, J.H. Shapiro, S. Tisa, and F. Zappa. Sub-rayleigh imaging via n-photon detection. *Phys. Rev. Lett.*, 105:163602, 2010.

[60] P. Kok, A.N. Boto, D.S. Abrams, C.P. Williams, S.L. Braunstein, and J.P. Dowling. Quantum-interferometric optical lithography: Towards arbitrary two-dimensional patterns. *Phys. Rev. A*, 63:063407, 2001.

[61] R.W. Boyd and J.P. Dowling. Quantum lithography: status of the field. *Quantum Inf. Process.*, 11:891, 2012.

[62] C.K. Rushforth. Restoration, resolution, and noise. *J. Op. Soc. Am.*, 58:539, 1968.

[63] M. Bertero and E. R. Pike. Resolution in diffraction-limited imaging, a singular value analysis. *Optica Acta*, 29:727, 1982.

[64] A.C. De Luca, S. Kosmeier, K. Dholakia, and M. Mazilu. Optical eigenmode imaging. *Phys. Rev. A*, 84:021803, 2011.

[65] D.A. Fish, J. Grochmalicki, and E.R. Pike. Scanning singular-value-decomposition method for restoration of images with space-variant blur. *J. Op. Soc. Am. A*, 13(3):464, 1996.

[66] R. Pike, D. Chana, P. Neocleous, and S.-H. Jiang. Superresolution in scanning optical systems. *Opt. Imaging and Microscopy*, 87:113, 2007.

[67] B. Huang, W. Wang, M. Bates, and X. Zhuang. Three-dimensional super-resolution imaging by stochastic optical reconstruction microscopy. *Science*, 319(5864):810, 2008.

[68] I. Akduman, U. Brand, J. GrochmBrand, and G. Hester. Superresolving masks for incoherent high-numerical-aperture scanning microscopy in three dimensions. *J. Op. Soc. Am. A*, 15(9):2275, 1998.

[69] M.I. Kolobov and C. Fabre. Quantum limits on optical resolution. *Phys. Rev. Lett.*, 85(18):3789, 2000.

[70] I.V. Sokolov and M.I. Kolobov. Squeezed-light source for superresolving microscopy. *Opt. Lett.*, 29:703, 2004.

[71] V.N. Beskrovnyy and M.I. Kolobov. Quantum limits of super-resolution in reconstruction of optical objects. *Phys. Rev. A*, 71(4):043802, 2005.

[72] M.I. Kolobov and V.N. Beskrovnyy. Quantum theory of super-resolution for optical systems with circular apertures. *Opt. Comm.*, 264(1):9, 2006.

[73] V.N. Beskrovny and M.I. Kolobov. Quantum-statistical analysis of superresolution for optical systems with circular symmetry. *Phys. Rev. A*, 78:043824, 2008.

[74] D. Slepian. Prolate spheroidal wave functions, fourier analysis and uncertainty iv. *Bell System Tech. J.*, 43:3009, 1964.

[75] J.C. Heurtley. Hyperspheroidal functions-optical rresonator with circular mirrors. In *Proceedings of the Symposium on Quasi-Optics*, 1964.

[76] B.R. Frieden. Band-unlimited reconstruction of optical objects and spectra. *J. Op. Soc. Am.*, 57:1013, 1967.

[77] B.R. Frieden. Evaluation, design and extrapolation methods for optical signals, based on use of the prolate functions. *Prog. Optics*, 9:311, 1971.

[78] C.S. Hu. Prolate spheroidal wave functions of large frequency parameters c = kf and their applications in electromagnetic theory. *IEEE Trans. Antennas Propag.*, AP-34:114, 1986.

[79] I.C. Moore and M. Cada. Prolate spheroidal wave functions, an introduction to the slepian series and its properties. *Appl. Comput. Harmon. Anal.*, 16:208, 2004.

[80] G. Walter and T. Soleski. A new friendly method of computing prolate spheroidal wave functions and wavelets. *Appl. Comput. Harmon. Anal.*, 19:432, 2005.

[81] H. Xiao, V. Rokhlin, and N. Yarvin. Prolate spheroidal wavefunctions, quadrature and interpolation. *IOPScience*, 17:805, 2000.

[82] D. Slepian and E. Sonnenblick. Eigenvalues associated with prolate spheroidal wave functions of zero order. *Bell System Tech. J.*, 44:1745, 1965.

[83] A.E. Siegman. Orthogonality properties of optical resonator eigenmodes. *Opt. Comm.*, 31(3):369, 1979.