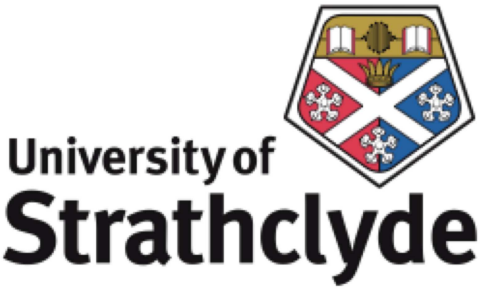
Measurements in Quantum Theory

Craig S. Hamilton

A thesis presented in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy



Department of Physics
University of Strathclyde

September 2009

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has lead to the award of a degree.

Signed: Date:

Acknowledgements

I would first like to express my thanks and appreciation to my supervisor Dr. John Jeffers for all his help over the course of my studies. I am also very grateful to the rest of the CNQO group for the assistance provided to me during my project. A big thanks goes to Ian and Kenny for their friendship during our years together at University. Also, I would like to thank my family that helped me, in many ways, over the course of my studies. Finally, I would like to thank Mariana for her love and support during our time together.

Abstract

Measurement of quantum systems contrasts markedly with that of classical systems and as such there are remarkable phenomena associated with the former. Quantum states can be intrinsically indistinguishable, in that no measurement, however perfect, can decide between two non-orthogonal states with absolute certainty all of the time. This is closely related to the no-cloning theorem in quantum mechanics that states that a general quantum state cannot be copied perfectly all of the time. In this thesis we examine some models that relate to measurements in quantum theory.

The first case we will look at are postselecting devices, which condition the output quantum state of the device after a measurement has been made. We describe a measure of successful-operation for these devices based on the mixed state fidelity.

Next, we look at a means to improve confidence in measurement results made by lossy photodetectors by placing a photon amplifier before the detector. This method only works in certain scenarios and we discuss these.

We then apply both of these techniques to an example of a postselecting device that encodes the quantum state within photons. This device forms part of a quantum key distribution network where two quantum states have to be compared with one another.

Finally, we look at a equation for the evolution of a quantum system undergoing measurements in phase-space and how this evolution is changed by the frequency and strength of these measurements.

List of Publications

This thesis is based in the following publications:

1. C. S. Hamilton and J. Jeffers, **Fidelity for imperfect postselection**, *Phys. Rev. A* 76, 052106 (2007)

2. C. S. Hamilton, H. Lavička, E. Andersson, J. Jeffers, and I. Jex, **Quantum public key distribution with imperfect device components**, *Phys. Rev. A* 79, 023808 (2009)

3. C. S. Hamilton and J. Jeffers, **Noisy preamplified photodetection for high-fidelity postselection**, *J. Phys. B: At. Mol. Opt. Phys.* 42, 114012 (2009)

Contents

1 Introduction **1**

1.1 Quantum states and density operators 1

1.1.1 Multi-mode states and entanglement 4

1.1.2 Operators 6

1.2 Quantum measurements 8

1.2.1 Von Neumann and Generalised Quantum Measurements 8

1.2.2 Conditional probabilities 10

1.3 Quantum evolution 11

1.3.1 Time evolution for open quantum systems 13

1.4 Quantum optics 15

1.4.1 Coherent states 18

1.4.2 Theory of beamsplitters 20

1.5 Overview of thesis 24

2 Fidelity for postselecting devices **26**

2.1 Introduction 26

2.2 Quantum computing 27

2.3 Linear optical quantum computing 28

2.4 Quantum distance measures and fidelity 30

2.4.1 Fidelity of two quantum states 31

2.5 Fidelity of correct output 33

2.5.1 Detection element 36

2.6 Examples of postselecting devices 38

2.6.1 Two-photon generation with a lossy beamsplitter . . . 38
2.6.2 Comparison of two coherent states 42
2.7 Conclusions 44

3 Fidelity increase by pre-amplification 46
3.1 Quantum theory of amplifiers and attenuators 46
3.1.1 Attenuation 47
3.1.2 Noise in an attenuator model 49
3.1.3 Amplification 50
3.1.4 Noise in an amplifier model 51
3.2 Pre-amplification method 52
3.3 Pre-amplification based on recording zero photocounts with a flat photon distribution 55
3.4 Pre-amplification based on recording zero photocounts with a Poisson photon distribution 62
3.5 Probability cost of pre-amplification 69
3.6 Pre-amplification based on recording a single photocount . . . 71
3.7 Postselection based on recording a single photo-count when there is no vacuum component 75
3.8 Discussion 76

4 Analysis of quantum key distribution network 79
4.1 Quantum cryptography 79
4.2 Quantum key distribution with coherent states 81
4.2.1 Key states 82
4.2.2 Analysis of QKD scheme as a postselecting device . . . 83
4.3 Results 84
4.3.1 Lossy beamsplitters 84
4.3.2 Imperfect detection: lossy detection and noisy amplification 89
4.4 Conclusions 92

5 Measurement master equation **95**
5.1 Measurement master equation 95
5.2 Measurement master equation with number states 98
5.2.1 Imperfect measurements in the number state basis . . . 99
5.2.2 Computational modelling 101
5.3 Measurement master equation with coherent states 103
5.3.1 Phase space methods in quantum optics 104
5.3.2 Derivation of the measurement master equation solution 105
5.3.3 Calculating observable values using the characteristic function 108
5.3.4 Computational modelling of the measurement master equation 110
5.3.5 Imperfect Measurements in the coherent state basis . . 114
5.4 Conclusions 115

6 Conclusions **116**
6.1 Summary of thesis 116

List of Figures

1.1 A ladder of energy levels of the quantum harmonic oscillator and the action of $\hat{a}$ and $\hat{a}^\dagger$. 17

1.2 A coherent state plotted in phase space. 19

1.3 Poisson distribution for 3 values of the mean, $|\alpha|^2$. Full line $|\alpha|^2 = 0.5$, dotted line $|\alpha|^2 = 1$, and dashed line $|\alpha|^2 = 5$. The distribution is only defined at integer values of n. 20

1.4 A beamsplitter. Two input modes are coupled to two output modes. 21

2.1 A non-linear sign shift gate. The gate works correctly when the detectors in the ancilla modes click with the desired results, as shown. 29

2.2 A typical postselecting device. This two-arm model can easily be generalized to many-arms. 34

2.3 **a)** The Hong-Ou-Mandel experimental setup and **b)** the result from the experiment. This result shows that pairs of perfectly-overlapping photons interfere at the beamsplitter to always leave in the same output arm. 39

2.4 Correct output fidelity for a two-photon generator with loss in the beam splitter vs. transmission coefficient of the beam splitter ($|t| = |r|$). 41

3.1 A model of the pre-amplification scheme: We have an amplifier followed by a lossy detector, which is modeled by an attenuator and a perfect detector. 54
3.2 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$. It can be seen from the graph that $P^{\mathrm{r}}(0|0)$ always increases for any level of amplifier gain and non-unit efficiency detector. 58
3.3 A two-dimensional slice of Figure 3.2 of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 58
3.4 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$. The graph shows improvement in measurement confidence when $\eta < 1/2$ and a decrease in confidence when $\eta > 1/2$. 59
3.5 A two-dimensional slice of Figure (3.4) of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 2$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 59
3.6 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 5$. The graph shows improvement in measurement confidence when $\eta < 1/5$ and a decrease in confidence when $\eta > 1/5$. 60
3.7 A two-dimensional slice of of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 5$ and the lines, from top to bottom, are η =0.5, 0.4, 0.2 and 0.1. 60
3.8 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 0.1$. This graph shows improvement for all lossy detectors and no change for a perfect detector. 64
3.9 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 0.1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 64

3.10 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 3$. . . 65
3.11 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 65
3.12 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ and $\lambda = 0.1$ . . 66
3.13 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$, $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 66
3.14 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ and $\lambda = 3$ . . . 67
3.15 $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$, $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 67
3.16 $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\mathrm{amp}} = 1$ (full line) and $N_{\mathrm{amp}} = 10$ (dashed line) with a uniform distribution of *a priori* input photons. 70
3.17 $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\mathrm{amp}} = 1$ (full line) and $N_{\mathrm{amp}} = 10$ (dashed line) with a Poisson distribution with $\lambda = 0.1$ of input photons. 70
3.18 $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\mathrm{amp}} = 1$ (full line) and $N_{\mathrm{amp}} = 10$ (dashed line) with a Poisson distribution with $\lambda = 3$ of input photons. 71
3.19 $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$. 73
3.20 A two-dimensional slice of of $P^{\mathrm{r}}(1|1)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 73
3.21 $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$. 74

3.22 A two-dimensional slice of of $P^{\mathrm{r}}(1|1)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 2$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25. 74
3.23 $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ for a uniform distribution with no vacuum component. The lines are, from top to bottom, η=1, 0.75 0.5 and 0.25. 77
3.24 $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ for a uniform distribution with no vacuum component. The lines are, from top to bottom, η=1, 0.75 0.5 and 0.25. 77

4.1 Quantum Key Distribution setup. If photons are detected in output arms 2 and/or 3 by the recipients, then the coherent states $|\alpha\rangle$ and $|\beta\rangle$ were necessarily different. 81
4.2 Quadrature plots of quantum key states. This figure shows two possible sets of key states. 82
4.3 F_{J}, the fidelity between an ideal output state and the state in equation 4.3, for three different values of α. The solid line refers to $|\alpha| = 1$, the dotted line refers to $|\alpha| = 2$ and the dashed line refers to $|\alpha| = 5$. 85
4.4 A plot of the Gaussian distribution (dotted line) and the top-hat distribution (full line), with $\sigma = B/2$. 87
4.5 F_{J} with a Gaussian deviation equation 4.5, dashed line, and with a flat distribution equation 4.6, full line, plotted as a function of width. Here width corresponds to the Gaussian's standard deviation, σ, or the top-hat distribution's bandwidth halved, $B/2$. 88
4.6 F, the fidelity given by Eq. (4.9), with both amplitude and phase noise present, plotted as a function of σ. 89

4.7 $P^{\mathrm{r}}(0|0)$ from equation 4.15 for different values of η, from top to bottom, 1, 0.5, 1/3 ($= N_{amp}^{-1}$), 0.25 and 0.1. Here $N_{amp} = 1$ and $|\alpha| = 0.5$. 93
4.8 $P^{\mathrm{r}}(0|0)$ from equation 4.15 for different values of η, from top to bottom, 1, 0.5, 1/3 ($= N_{amp}^{-1}$), 0.25 and 0.1. Here $N_{amp} = 3$ and $|\alpha| = 0.5$. 93

5.1 The photon-number distribution after a certain number of measurements. The solid line is the initial distribution, whereas the next distributions are after 3, 6 and 9 measurements each. The distribution becomes more peaked after each measurement. 102
5.2 The photon-number distribution after a single measurement with varying values of σ. A lower σ induces more collapse onto a single number state. 103
5.3 A single evolution of the trajectory in phase space. 112
5.4 The average of 10 trajectories in phase space 112
5.5 The average of 100 trajectories in phase space 113
5.6 The average of 2000 trajectories in phase space 113

Chapter 1

Introduction

In this introductory chapter we explain some of the background theory from quantum physics that we will use throughout this thesis. We start by describing a quantum state and why it is different from a classical state, and then explain the operators that act upon them. Then we explain how measurements affect quantum states and how states evolve in time. Finally we will describe quantum optics, which is the quantization of the electromagnetic field.

1.1 Quantum states and density operators

Physical systems can be characterized by their state, for example a particle can have a position and momentum, which corresponds to a point in phase space or an atom can have a certain electron configuration. In classical physics the state is described by a probability vector whereas a quantum state has a vector of amplitudes [1].

Mathematically quantum systems are described by Hilbert spaces, which can be composed of discrete states, such as photon number, or continuous states, such as position, and may have a finite or infinite dimension. A system with n-dimensions is also said to be a n-levels. A general quantum state, $|\psi\rangle$, can be written as a superposition of basis vectors that span the Hilbert space

of the system considered,

$$|\psi\rangle = \sum_n a_n |\phi_n\rangle. \tag{1.1}$$

Here the a_n are called the amplitudes of the individual basis states. The modulus-squared of the amplitudes, $|a_n|^2$, corresponds to the probability that the system will be found in that basis state upon a projective measurement. Thus, for the quantum state to be normalized, the amplitudes should satisfy the condition,

$$\sum_n^{\infty} |a_n|^2 = 1,$$

which is simply that probabilities should sum to unity. The $a_n$are complex numbers and contain phase information on different components of the state. The basis vectors themselves are generally orthonormal i.e. $\langle \phi_m | \phi_n \rangle = \delta_{nm}$, but do not have to be.

For discrete dimensional systems, such as photon number, states can be written as column vectors where the entries are the corresponding amplitudes. For continuous dimensional systems, such as particle position, states are typically written as a function normalizable over all space,

$$|\phi\rangle = \int_{-\infty}^{\infty} dx f(x) \, |x\rangle \quad \text{with} \quad \int_{-\infty}^{\infty} dx |f(x)|^2 = 1. \tag{1.2}$$

A quantum state can also be written in another way using the density operator [2]. The density operator for the state $|\psi\rangle$ is constructed as,

$$\hat{\rho} = |\psi\rangle \langle\psi| \, , \tag{1.3}$$

and can be written as a matrix as $\langle\psi|$ is a row vector. For example if we have the two-level system,

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle. \tag{1.4}$$

the density matrix will be,

$$\hat{\rho} = \begin{bmatrix} |a_0|^2 & a_0\, a_1^* \\ a_1\, a_0^* & |a_1|^2 \end{bmatrix} = \begin{bmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{bmatrix}. \tag{1.5}$$

The diagonal elements contain the probabilities that the state will be in that basis state, whereas the off-diagonal elements are called the coherences and contain the quantum phase information in the state. The density operator is a Hermitian operator, which means, in matrix formalism, that it is equal to its complex transpose,

$$\hat{\rho} = \hat{\rho}^\dagger = (\hat{\rho}^*)^T. \tag{1.6}$$

Density operators are useful because they can be used to describe a quantum system in the presence of decoherence [3], which is when the off-diagonal matrix elements of the density matrix tend to zero and we are left with a classical probability distribution for the state. For example, if a density matrix can be written as $|\psi\rangle\langle\psi|$ then that state is called a pure state. A pure state satisfies the following criteria,

$$\rho_{11}\rho_{22} = \rho_{12}\rho_{21}. \tag{1.7}$$

A state that is not pure is called a mixed state and cannot be written as $|\psi\rangle\langle\psi|$ and satisfies the following condition,

$$\rho_{11}\rho_{22} > \rho_{12}\rho_{21}. \tag{1.8}$$

These show that a pure state maximizes the coherence possible in a quantum state; any less and we say that the state has decohered. We can quantify this decoherence by a measure called the purity, which is defined for a state $\hat{\rho}$ as,

$$\mathrm{Tr}[\hat{\rho}^2], \tag{1.9}$$

where Tr[.] is the trace operation, defined as,

$$\mathrm{Tr}[\hat{\rho}] = \sum_n \langle \phi_n | \, \hat{\rho} \, | \phi_n \rangle \, . \tag{1.10}$$

The trace operation is cyclical i.e. $\mathrm{Tr}[\hat{A}\hat{B}\hat{C}] = \mathrm{Tr}[\hat{B}\hat{C}\hat{A}]$. For a pure state, $\hat{\rho} = |\psi\rangle \langle\psi|$, and $\hat{\rho}^2 = |\psi\rangle \langle\psi| \, \psi\rangle \langle\psi| = |\psi\rangle \langle\psi| = \hat{\rho}$, thus $\mathrm{Tr}[\hat{\rho}^2] = 1$, whereas for a mixed state $0 \leq \mathrm{Tr}[\hat{\rho}^2] < 1$. The purity can therefore be seen to be a suitable measure of a state's 'mixed-ness'.

Decoherence occurs when one quantum system couples to another and the two become entangled, thereby we need both systems to fully characterize the quantum state. If we only have access to one of the quantum systems then we will lose the phase information that the off-diagonal coherence elements provide. We will describe this in more detail in the next section on multi-mode states.

1.1.1 Multi-mode states and entanglement

When we have two or more quantum systems, such as two atoms or spatial modes of light beams, we can write the composite state of both subsystems as,

$$|\psi\rangle = \sum_{n,m} a_{n,m} |\phi_n\rangle_1 \otimes |\phi_m\rangle_2 = \sum_{n,m} a_{n,m} |\phi_n, \phi_m\rangle, \tag{1.11}$$

where the subscripts refer to the individual sub-system and $\otimes$ is the tensor product. The density operator is formed from this state as before. In general, these two-modes states can have correlations between different subsystems that classical physics cannot explain, known as entanglement.

This is an amazing feature of quantum systems, and was highlighted by Einstein, Podolsky and Rosen (EPR) [4], and has come to be known as the EPR paradox. When we have a quantum state composed of two subsystems such as,

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle \right), \tag{1.12}$$

EPR postulated that measurements on one component of the state would have a non-local effect on the other component and argued that this meant that quantum mechanics was not a locally real physical theory. States of this form are known as entangled states and have many interesting properties that are not found in classical physics, such as stronger correlations than allowed in classical physics leading to violations of Bell's inequalities [5, 6, 7], uses in quantum computation and cryptography [8] and quantum teleportation [9].

A useful operation to perform on such a state is the partial trace, which is where the trace is taken over one (or more) of the subsystem's modes. For our two-mode system the partial trace over the second mode would be defined as,

$$\mathrm{Tr}_2[\hat{\rho}_{12}] = \sum_n {}_2\langle\phi_n|\,\hat{\rho}_{12}\,|\phi_n\rangle_2\,, \tag{1.13}$$

and we are left with a state in the remaining mode 1. Such an operation would occur in the theory of open systems where we would sum over the environment modes and are then left with a density operator that describes the modes of our system of interest. Generally the remaining density operator will be a mixed state, as the trace procedure removes information about correlations between different modes of the complete system. We are only left with a pure state in one sub-system if the initial two-system state was separable,

$$|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \tag{1.14}$$

i.e. there was no entanglement between the two sub-systems.

Another mathematical technique referred to later in this thesis is that of purifying a mixed state. Purification intends to take a mixed state and extend the Hilbert space so that the new state is pure. For example, if we have the mixed state $\hat{\rho}$ in Hilbert space H_1 we can extend to another Hilbert space H_2 so that,

$$\hat{\rho} = \mathrm{Tr}_2[|\psi\rangle\langle\psi|], \tag{1.15}$$

where $|\psi\rangle$ is a pure state in the Hilbert space $H_1 \otimes H_2$.

We can now demonstrate the effect of decoherence on a 2-mode quantum

state. If we have the entangled state (1.12) from above, the density matrix is,

$$\begin{pmatrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \langle 00| \\ \langle 01| \\ \langle 10| \\ \langle 11| \end{pmatrix}.$$

$$= \frac{1}{2}\left[|01\rangle\langle 01| + |10\rangle\langle 10| - |10\rangle\langle 01| - |01\rangle\langle 01|\right]. \tag{1.16}$$

If we take the partial trace over one of the two modes, the state in the remaining mode,

$$\frac{1}{2}\left[|0\rangle\langle 0| + |1\rangle\langle 1|\right]. \tag{1.17}$$

This is proportional to the identity operator for the system and these states are termed the maximally-mixed states, as all off-diagonal elements are zero. Removing the phase information from the original density matrix has reduced our quantum state to a classical state.

The partial trace operation removed the phase information; there are operators that remove some of the coherence, perhaps per unit time, such as in the theory of open quantum systems evolving in time. The quantum state, characterised by the density operator, evolves mathematically by a master equation. This is discussed in a following section. In the next section we describe some of the general theory of operators.

1.1.2 Operators

Now we have defined the states of our quantum systems we would now like to define how they change when operators act upon them on. We can write an operator $\hat{A}$ using the basis states of a system as,

$$\hat{A} = \sum_{m,n} c_{m,n} |\phi_m\rangle\langle\phi_n|, \tag{1.18}$$

and this acts on a state $|\psi\rangle = \sum_s a_s |\phi_s\rangle$ as,

$$\hat{A}|\psi\rangle = \sum_{m,n} c_{m,n} |\phi_m\rangle \langle\phi_n| \sum_s a_s |\phi_s\rangle = \sum_{m,n,s} c_{m,n} a_s |\phi_m\rangle \langle\phi_n| \phi_s\rangle. \quad (1.19)$$

If we have orthonormal eigenstates, $\langle\phi_n| \phi_s\rangle = \delta_{ns}$, this gives,

$$\hat{A}|\psi\rangle = \sum_{m,n} c_{m,n} a_n |\phi_m\rangle . \quad (1.20)$$

An important class of operators are called unitary operators, $\hat{U}$, represented by a unitary matrix. When they act upon a quantum state they produce a new, normalized quantum state and as such can describe the time-evolution of quantum systems. A unitary operator, $\hat{U}$, satisfies the following conditions,

$$\begin{aligned} \hat{U}^\dagger &= \hat{U}^{-1} \\ \hat{U}\hat{U}^\dagger &= \hat{U}^\dagger\hat{U} = \hat{1}, \end{aligned} \quad (1.21)$$

where $\hat{1}$ is the identity operator for the system. This is an important operator which is written as,

$$\hat{1} = \sum_n |\phi_n\rangle \langle\phi_n| , \quad (1.22)$$

where the sum is over a complete set of basis states of the system. This operator does not change the state it acts upon. It can sometimes be useful to introduce the identity operator into a calculation to allow for re-arranging.

A projective operator is an operator that satisfies the following condition, $\hat{P}^2 = \hat{P}$. This makes it of the form $|\phi_n\rangle \langle\phi_n|$, where $|\phi_n\rangle$ is an eigenstate of the system. Pure states can be written as projective operators and projective measurements will be discussed in the next section on quantum measurements.

1.2 Quantum measurements

In this section we describe measurements made upon quantum states. We start this section by explaining Von Neumann, or projective measurement, and then move on to explain generalized measurements. We will then talk about conditional measurement probabilities that link the preparation of a state and subsequent measurement results obtained from that state. These will be useful in determining the likelihood of various measurements outcomes when certain states are produced, as well as what can be inferred about a state given a certain measurement outcome has occurred.

1.2.1 Von Neumann and Generalised Quantum Measurements

A measurement in quantum mechanics can be described by a set of operators $\{\hat{\pi}_n\}$ known as a Probability Operator Measure (POM), or Positive Operator Valued Measure (POVM) and the individual $\hat{\pi}_j$ are called elements. Each measurement operator corresponds to a potential result from that measurement. The probability of obtaining result j, corresponding to POM element $\hat{\pi}_j$, given a state $\hat{\rho}$, is,

$$P_j = \mathrm{Tr}[\hat{\rho}\,\hat{\pi}_j]. \tag{1.23}$$

The first case of quantum measurements are known as Von Neumann or projective measurements. Projective measurements form a complete set of eigenstates of the system, for example photon number, $\{\hat{\pi}_n = |n\rangle\langle n|\}$. After measurement, projective measurements leave the quantum system in the eigenstate corresponding to the measurement result. The measurement operators, $\hat{\pi}_n$, satisfy the following conditions:

1. $\sum_n \hat{\pi}_n = \hat{1}$
2. $\mathrm{Tr}[\hat{\rho}\,\hat{\pi}] \geq 0 \;\forall\, \hat{\rho}$
3. $\hat{\pi} = \hat{\pi}^\dagger$

4. $\hat{\pi}_n\hat{\pi}_m = \delta_{nm}\hat{\pi}_n$

The first two conditions have meaningful physical properties relating to completeness and positive definiteness, the third condition imposes hermiticity while the fourth condition, that POM elements are orthogonal to one another, can be discarded altogether. Removing this condition leads to generalised measurements.

With generalised measurements the POM elements can be decomposed into $\hat{\pi}_j = \hat{A}_j^\dagger \hat{A}_j$, where the $\hat{A}$ are called Kraus effect operators [10]. The POM elements obey rules 1-3 above. These operators are useful because they can be used to describe the density operator after a measurement takes place. The state after measurement, $\hat{\rho}'$, if the measurement result is known is given by,

$$\hat{\rho}' = \frac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{\mathrm{Tr}[\hat{A}_j\hat{\rho}\hat{A}_j^\dagger]} = \frac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{\mathrm{Tr}[\hat{\rho}\hat{\pi}_j]} = \frac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{P_j}, \tag{1.24}$$

using the cyclic property of the trace. If the measurement result is not known then the state becomes a sum of all possible post-measurement states, weighted by probability of observing that result,

$$\hat{\rho}' = \sum_j P_j \frac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{\mathrm{Tr}[\hat{A}_j\hat{\rho}\hat{A}_j^\dagger]} = \sum_j \mathrm{Tr}[\hat{A}_j\hat{\rho}\hat{A}_j^\dagger]\frac{\hat{A}_j\hat{\rho}\hat{A}_j^\dagger}{\mathrm{Tr}[\hat{A}_j\hat{\rho}\hat{A}_j^\dagger]} = \sum_j \hat{A}_j\hat{\rho}\hat{A}_j^\dagger. \tag{1.25}$$

In order to distinguish between two quantum states there are a few measurement criteria to decide what a 'best' measurement is [11]. There is minimum error discrimination [12], which aims to minimise the overlap between the measurement operators corresponding to each state and the other states. Unambiguous measurement has measurement operators orthogonal to certain states, so an observer will know that when they definitely do not have a certain state. This comes at the cost of sometimes having an ambiguous measurement result that gives no information about what state was present. Maximum confidence measurements [13] aim to maximise the conditional probability that given we measured a state and obtained the result corresponding to that state, we actually have that state present.

1.2.2 Conditional probabilities

Conditional probabilities highlight how the chance of an event occurring is altered after we learn more information concerning that event. For example, consider a set of quantum states, $\{\hat{\rho}_i\}$, each with an *a priori* probability of occurring, $P(i)$, and a set of POM elements, $\{\hat{\pi}_j\}$, that describes our measuring device. We can define the conditional probability that we obtain result j given we had state i, $P^{\mathrm{p}}(j|i)$, as [14],

$$P^{\mathrm{p}}(j|i) = \mathrm{Tr}[\hat{\rho}_i \hat{\pi}_j]. \tag{1.26}$$

We use the superscript 'P' to highlight that this is a predictive formula because the measurement result follows the process of state preparation, and so this is the probability of a later event given an earlier one. If we now use Bayes' Theorem [15], which relates conditional probabilities between two events, A and B, occurring,

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{P(B|A)P(A)}{\sum_A P(B|A)P(A)}, \tag{1.27}$$

where $P(A|B)$ is the conditional probability that event A will occur given that event B has occurred, likewise for $P(B|A)$ and $P(A)$ ($P(B)$) is the *a priori* probability of event A (B) occurring, we can now obtain a retrodictive conditional probability [16] from the predictive conditional probability, equation (1.26),

$$P^{\mathrm{r}}(i|j) = \frac{P^{\mathrm{p}}(j|i)P(i)}{\sum_i P^{\mathrm{p}}(j|i)P(i)} = \frac{P(i)\mathrm{Tr}[\hat{\rho}_i \hat{\pi}_j]}{\sum_i P(i)\mathrm{Tr}[\hat{\rho}_i \hat{\pi}_j]}. \tag{1.28}$$

This is a retrodictive formula because the probability of a past event occurring, a particular state being prepared, is conditioned on a future event, measurement. This formula tells us how the probability of a state being prepared is modified after learning the result of a measurement performed on that state. We will use this retrodictive probability as a measure of how well

our detectors work in future chapters as we are interested in the probability that we have the correct state in our device given we have measured the result corresponding to this state.

1.3 Quantum evolution

In this section we describe how quantum systems evolve in time. We start by describing how closed quantum systems evolve and then how open quantum systems evolve. A closed system has no interactions with an outside system, commonly called an environment, and this therefore ensures that evolution in the system is reversible. Reversible dynamics can be described by unitary operators. Systems that include a larger environment in their evolution are called 'open systems' and are their evolution is described by a master equation, which includes the interaction terms between the system and environment. Another definition of a closed system is that we can characterise all the degrees of freedom of the system with a Hamiltonian and that we have access to measure these degrees.

The quantum evolution of a closed system is described by the Hamiltonian operator, $\hat{H}$, which is the same as the classical Hamiltonian with the canonical variables replaced by the corresponding quantum operators i.e. for position and momentum we replace $x \rightarrow \hat{x}$ and $p \rightarrow i\hbar\partial/\partial\hat{x}$, with the commutator for operators, $[\hat{x}, \hat{p}] = i\hbar$. There are 3 pictures in which the quantum states can evolve, which we will discuss below.

The first picture of quantum evolution is known as the Schrödinger picture, where the state of the system evolves in time according to the familiar Schrödinger equation,

$$i\hbar\frac{d}{dt}\left|\psi(t)\right\rangle = \hat{H}\left|\psi(t)\right\rangle. \tag{1.29}$$

If a quantum system is expressed in terms of a set of eigenstates, then it is the amplitudes that change with respect to time, for example in a two-level system,

$$\left|\psi(t)\right\rangle = a(t)\left|0\right\rangle + b(t)\left|1\right\rangle, \tag{1.30}$$

and at all times the condition $|a(t)|^2 + |b(t)|^2 = 1$ must be satisfied. The solution to the Schrödinger equation is given by

$$|\psi(t)\rangle = \hat{U}\,|\psi(0)\rangle \tag{1.31}$$

where $|\psi(0)\rangle$ is the initial state and $\hat{U} = \exp[-i\hat{H}t/\hbar]$, provided that $\hat{H}$ is time-independent. The exponential of an operator $\hat{O}$ can be defined as,

$$\exp[\hat{O}] = \sum_{n=0}^{\infty} \frac{\hat{O}^n}{n!} = \hat{1} + \hat{O} + \frac{\hat{O}^2}{2!} + ... \,, . \tag{1.32}$$

The corresponding evolution for the density operator is the Liouville equation,

$$\dot{\hat{\rho}} = \frac{-i}{\hbar}[\hat{H}, \hat{\rho}], \tag{1.33}$$

whose solution is,

$$\hat{\rho}(t) = \hat{U}\hat{\rho}(0)\hat{U}^{\dagger}. \tag{1.34}$$

The second picture, and an alternative to the Schrödinger picture, is where the operators acting on the quantum state change with respect to time. This is the called the Heisenberg picture. The time evolution for an operator $\hat{O}$ is,

$$\dot{\hat{O}}(t) = \frac{i}{\hbar}[\hat{H}, \hat{O}(t)]. \tag{1.35}$$

The third picture is where both the state and operators change with respect to time and this is called the interaction picture. This would commonly be used if the total Hamiltonian for the system could be divided into time-dependent and -independent parts.

If we have two quantum systems that interact with one each other through a Hamiltonian $\hat{H}_{\text{int}}$, then the total Hamiltonian for the combined system is written as,

$$\hat{H}_{\text{tot}} = \hat{H}_1 + \hat{H}_2 + \hat{H}_{\text{int}}, \tag{1.36}$$

where $\hat{H}_i$ is the Hamiltonian of system i. If we are only interested of the dynamics of the interaction we can transform the density operator into the

interaction picture by applying the unitary operators,

$$\hat{\rho}_{\text{int}}(t) = \exp[i(\hat{H}_1 + \hat{H}_2)/\hbar]\, \hat{\rho}(t)\, \exp[-i(\hat{H}_1 + \hat{H}_2)/\hbar]. \tag{1.37}$$

In general, interactions between different quantum systems will lead to entanglement between the two systems. This is important for the theory of open quantum systems in the next section.

1.3.1 Time evolution for open quantum systems

A closed system is one in which we can, in principle, measure all modes of the system and that the Hamiltonian of the system only acts on those modes. In contrast to this, an open quantum system is an initial system of interest coupled to a larger system with many degrees of freedom that cannot be measured. These unobservable modes are usually called an environment or heat bath. For the complete evolution of the combined system we now have to include the Hamiltonians that describe the environmental modes and also the interaction between the system and environment. As the environment will have many degrees of freedom we cannot hope to solve this Liouville expression analytically and we must make some assumptions that allow us to simplify the interaction between the system and environment, as well as the state of the system and enviroment. These assumptions lead to a master equation for the evolution of the system. We briefly derive the master equation for an open quantum system [17, 18, 19].

We start with the Hamiltonian for the system, environment and interaction between the two,

$$\hat{H} = \hat{H}_{\text{sys}} + \hat{H}_{\text{int}} + \hat{H}_{\text{env}}, \tag{1.38}$$

where the individual $\hat{H}$ are the Hamiltonians for the system, interaction between the system and environment and environment itself respectively and we assume that they are time independent. As we are interested in the

dynamics of the interaction, we can transform the density operator of the system and environment, $\hat{\rho}$, into a density operator where the effects of $\hat{H}_{\text{sys}}$ and $\hat{H}_{\text{env}}$ are removed, know as the interaction picture,

$$\hat{\rho}_{\text{int}}(t) = e^{i(\hat{H}_{\text{sys}}+\hat{H}_{\text{env}})t/\hbar}\hat{\rho}\, e^{-i(\hat{H}_{\text{sys}}+\hat{H}_{\text{env}})t/\hbar}, \tag{1.39}$$

and for the interaction Hamiltonian,

$$\hat{H}_{\text{int}}(t) = \exp[i(\hat{H}_{\text{sys}} + \hat{H}_{\text{env}})t/\hbar]\hat{H}\ \exp[-i(\hat{H}_{\text{sys}} + \hat{H}_{\text{env}})t/\hbar]. \tag{1.40}$$

The density operator in the interaction picture evolves according to the equation,

$$\dot{\hat{\rho}}_{\text{int}}(t) = \frac{-i}{\hbar}[\hat{H}_{\text{int}}(t), \hat{\rho}_{\text{int}}(t)]. \tag{1.41}$$

If we integrate this once we obtain the expression,

$$\hat{\rho}_{\text{int}}(t) = \hat{\rho}_{\text{int}}(0) - \frac{i}{\hbar}\int_0^t dt'[\hat{H}_{\text{int}}(t'), \hat{\rho}_{\text{int}}(t')], \tag{1.42}$$

and if we substitute this solution into the expression for the evolution of the interaction density matrix, (1.41), we obtain,

$$\dot{\hat{\rho}}_{int}(t) = \frac{-i}{\hbar}[\hat{H}_{\text{int}}(t), \hat{\rho}_{\text{int}}(0)] - \frac{1}{\hbar^2}\int_0^t dt'[\hat{H}_{\text{int}}(t), [\hat{H}_{\text{int}}(t'), \hat{\rho}_{int}(t')]. \tag{1.43}$$

This expression is exact but in general will not be readily solved due to the complexity of $\hat{H}_{\text{int}}$ and so approximations must be applied. There are several standard approximations made, which lead to the well-known Born-Markov master equation. The first is that we can neglect terms in high-order $\hat{H}_{\text{int}}$, the next is that the initial state of the system and environment is separable and the third is that the system dynamics depend only upon the state at that instant in time and not upon the history of the state. Using these, and

taking $\hat{H}_{\rm int}$ to be of the form,

$$\hat{H}_{\rm int}(t) = \hbar \sum_i \hat{A}_i(t) \otimes \hat{b}_i(t), \tag{1.44}$$

where $\{\hat{A}_j(t)\}$ are operators acting only on the system and $\{\hat{b}_j(t)\}$ acting only on the environment.

Including these environmental operators into the master equation and taking the trace over environmental modes leads to factors of the form,

$$\langle \hat{b}_i(t)\hat{b}_j(t')\rangle = {\rm Tr}_{\rm env}[\hat{b}_i(t)\hat{b}_j(t')\hat{\rho}_{\rm env}]. \tag{1.45}$$

These factors are correlation functions for the environment. The Markov approximation leads to short-time effects where these correlation functions are replaced by delta functions, $\gamma_k\,\delta(t-t')$, where the γ_k are decay rates. This all leads to a master equation for the state of the system,

$$\hat{\rho}_{\rm sys} = \frac{-i}{\hbar}[\hat{H}_{\rm sys}, \hat{\rho}_{\rm sys}] + \sum_k \gamma_k \left[\hat{A}_k\hat{\rho}\hat{A}_k^\dagger - \frac{1}{2}\left(\hat{\rho}\hat{A}_k^\dagger\hat{A}_k + \hat{A}_k^\dagger\hat{A}_k\hat{\rho}\right)\right]. \tag{1.46}$$

Physically, this equation preserves the positive nature of the density matrix for all purifications of the density matrix. This is known as complete-positivity [20] and Lindblad has shown that this is the most general form of a completely-positive equation [21].

1.4 Quantum optics

Quantum optics is the study of the quantum mechanical properties of light, the electromagnetic field, and its interaction with matter [22, 23]. This field of study really came to its own with the development of the laser, a high-powered coherent source of photons that made experimental tests of the theory possible.

Maxwell's equations show that inside an optical cavity, an arrangement

of mirrors that reflects light such as a Fabry-Perot cavity, the electromagnetic field can be described by a collection of harmonic oscillators, one for each allowed frequency and polarization. The Hamiltonian of a harmonic oscillator,

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2, \tag{1.47}$$

is then quantized by replacing the canonical variables with their quantum operators, $p \to \hat{p} = -i\hbar d/d\hat{x}$ and $x \to \hat{x}$ along with the quantum commutation relation

$$[\hat{x}, \hat{p}] = i\hbar, \tag{1.48}$$

to give,

$$\hat{H} = \frac{-\hbar^2}{2m}\frac{d^2}{d\hat{x}^2} + \frac{1}{2}m\omega^2\hat{x}^2. \tag{1.49}$$

We can now introduce the operator,

$$\hat{a} = \sqrt{\frac{m\omega}{2\hbar}}\left(\hat{x} + \frac{i}{m\omega}\hat{p}\right), \tag{1.50}$$

and the Hamiltonian becomes,

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{1.51}$$

This operator, $\hat{a}$, is the bosonic annihilation operator for a quantum harmonic oscillator and its conjugate, $\hat{a}^\dagger$, is the creation operator. They have the commutator,

$$[\hat{a}, \hat{a}^\dagger] = 1, \tag{1.52}$$

and together they define a ladder of energy levels for the system, as shown in fig. 1.1. These operators act to change the number of quanta in the system; $\hat{a}$ will remove a quantum of energy in the system and $\hat{a}^\dagger$ will create a quantum of energy. In quantum optics these quanta are photons.

The photon number states, or Fock states, $\{|n\rangle\}$, form an orthonormal,

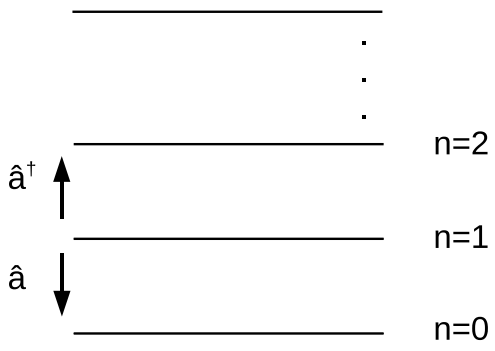


Figure 1.1: A ladder of energy levels of the quantum harmonic oscillator and the action of $\hat{a}$ and $\hat{a}^\dagger$.

complete set of basis vectors for the Hilbert space of photons,

$$\langle n|m\rangle = \delta_{nm}, \tag{1.53}$$

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \hat{1}, \tag{1.54}$$

where $\hat{1}$ is the unit operator of the state space. The creation and annihilation operators have the following representations using number states,

$$\hat{a} = \sum_{n=1}^{\infty} \sqrt{n}|n-1\rangle\langle n| \tag{1.55}$$

$$\hat{a}^\dagger = \sum_{n=0}^{\infty} \sqrt{n+1}|n+1\rangle\langle n| \tag{1.56}$$

and they act upon the number states in the following manner,

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \tag{1.57}$$

$$\hat{a}|0\rangle = 0, \tag{1.58}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{1.59}$$

These two operators combine to a third one called the number operator,

$$\hat{n} = \hat{a}^\dagger \hat{a}, \tag{1.60}$$

$$\hat{n} = \sum_n^\infty n \, |n\rangle \langle n| \, , \tag{1.61}$$

with an eigenvalue relation $\hat{n}|n\rangle = n|n\rangle$. The mean number of photons in a state $\hat{\rho}$ is then given by $\langle \hat{n} \rangle = \mathrm{Tr}[\hat{n}\,\hat{\rho}]$. The photon number variance of a state is,

$$\Delta n^2 = \langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2. \tag{1.62}$$

1.4.1 Coherent states

A set of states useful in quantum optics, and refered to in this thesis, are the Glauber coherent states [24, 25, 26], which can be defined either by their expansion in the number state basis,

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{1.63}$$

or by the eigenrelation with the annihilation operator,

$$\hat{a} \, |\alpha\rangle = \alpha \, |\alpha\rangle \, . \tag{1.64}$$

Here α is a complex number, which, using phase space co-ordinates of position and momentum for the harmonic oscillator is,

$$\alpha = \sqrt{\frac{m\omega}{2\hbar}} \left(x + \frac{i}{m\omega} p \right). \tag{1.65}$$

Another useful definition of a coherent state is in terms of the displacement operator, $\hat{D}$, acting on the zero photon number state,

$$|\alpha\rangle = \exp[\alpha \hat{a}^\dagger - \alpha^* \hat{a}] \, |0\rangle = \hat{D}(\alpha) \, |0\rangle \, . \tag{1.66}$$

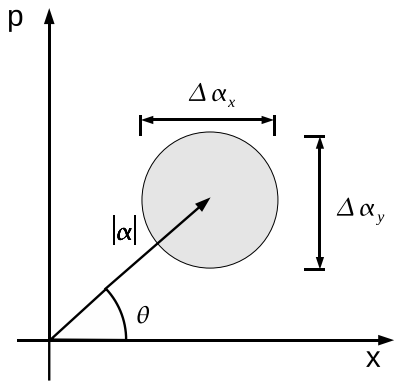


Figure 1.2: A coherent state plotted in phase space.

This is a unitary operator with the relation,

$$\hat{D}^{\dagger}(\alpha) = \hat{D}(-\alpha). \tag{1.67}$$

It can also act upon a non-zero coherent state,

$$\hat{D}(\alpha)\left|\beta\right\rangle = e^{\frac{1}{2}(\alpha\beta^{*}-\alpha^{*}\beta)}\left|\alpha+\beta\right\rangle = e^{iIm(\alpha\beta^{*})}\left|\alpha+\beta\right\rangle. \tag{1.68}$$

Coherent states are known as the most classical of states, as they come closest to a classical point in phase space, though when measured in phase space there will be a typical spread of values about the point (x, y). Fig. 1.2 shows a coherent state plotted in phase space, with a shaded area highlighting the spread of measurement values. Coherent states are minimum-uncertainty states, which means that they saturate a Heisenberg Uncertainty relation,

$$\Delta x \Delta y = \hbar/2. \tag{1.69}$$

The coherent states form an over-complete basis for the Hilbert space,

$$\frac{1}{\pi}\int d^{2}\alpha\left|\alpha\right\rangle\left\langle\alpha\right| = \hat{1}, \tag{1.70}$$

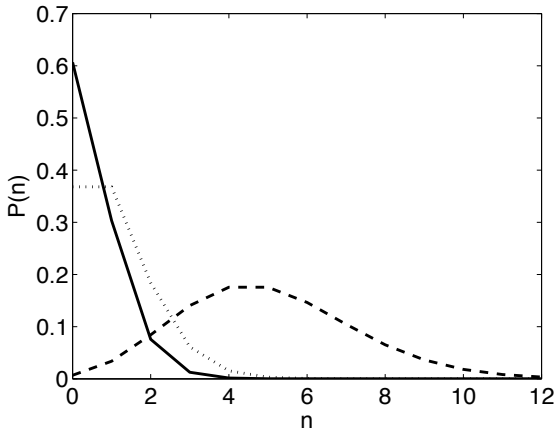


Figure 1.3: Poisson distribution for 3 values of the mean, $|\alpha|^2$. Full line $|\alpha|^2 = 0.5$, dotted line $|\alpha|^2 = 1$, and dashed line $|\alpha|^2 = 5$. The distribution is only defined at integer values of n.

and are non-orthogonal states,

$$\langle \alpha \, | \beta \rangle = \exp\left[-\frac{1}{2} \left(|\alpha|^2 + |\beta|^2 - 2\alpha^* \beta \right) \right], \tag{1.71}$$

although for large values of $|\alpha - \beta|^2$ they are approximately orthogonal.

The number of photons in a coherent state $|\alpha\rangle$ follows a Poisson distribution,

$$P(n) = \frac{e^{-|\alpha|^2} |\alpha|^{2n}}{n!}, \tag{1.72}$$

where the mean, $\bar{n}$, and variance, Δn^2, of the photon number are equal to $|\alpha|^2$. In fig. 1.3 we have plotted a Poisson distribution for mean = 0.5, 1 and 5. Note that this distribution is only defined at integer values of n, and the continuous lines are only for clarity.

1.4.2 Theory of beamsplitters

A beamsplitter is a device in quantum optics that linearly transforms two input modes into two output modes. We will use the theory of beamsplitters in later chapters of this thesis. A typical beamsplitter is shown in fig. 1.4

below, with the two modes labelled as a and b. From the figure we can see

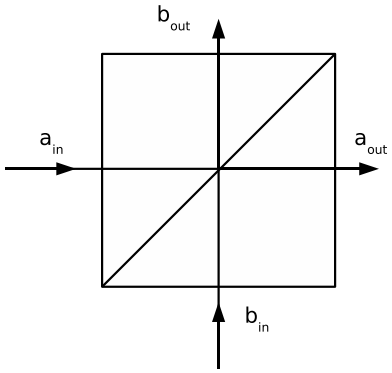


Figure 1.4: A beamsplitter. Two input modes are coupled to two output modes.

the the input modes are reflected and transmitted as they pass through the beamsplitter. This transformation can be written as,

$$\hat{a}_{\rm out} = t_a \hat{a}_{\rm in} + r_b \hat{b}_{\rm in} \,, \tag{1.73}$$

$$\hat{b}_{\rm out} = t_b \hat{b}_{\rm in} + r_a \hat{a}_{\rm in} \,, \tag{1.74}$$

where the coefficients represent transmission and reflection and are, in general, complex numbers. The mode operators satisfy the bosonic commutation relations,

$$[\hat{a}_{\rm in}, \hat{a}^\dagger_{\rm in}] = 1,$$

$$[\hat{b}_{\rm in}, \hat{b}^\dagger_{\rm in}] = 1,$$

$$[\hat{a}_{\rm in}, \hat{b}^\dagger_{\rm in}] = 0.$$

The output operators must satisfy similar conditions and this ensures unitarity in the beamsplitter transformation.

There are a variety of ways of mathematically representing the beamsplitter transformation, all equivalent, and here we will describe these.

Firstly, we can write a Hamiltonian describing the beamsplitter,

$$\hat{H}_{\mathrm{BS}} = \theta \left(e^{i\phi} \hat{a}^{\dagger} \hat{b} + e^{-i\phi} \hat{a} \hat{b}^{\dagger} \right), \tag{1.75}$$

where θ and ϕ are parameters of the beamsplitter that relate to the transmission and reflection coefficients. The unitary transformation of the beamsplitter is then simply,

$$\hat{U}_{\mathrm{BS}} = \exp \left[\frac{-i \hat{H}_{\mathrm{BS}}\, t}{\hbar} \right]. \tag{1.76}$$

A two-mode state will change under the action of the beamsplitter according to the Schrödinger equation,

$$|\phi\rangle_{\mathrm{out}} = \hat{U}_{\mathrm{BS}} \, |\phi\rangle_{\mathrm{in}} \,, \tag{1.77}$$

and the mode operators will change according to the Heisenberg equation,

$$\hat{a}_{\mathrm{out}} = \hat{U}_{\mathrm{BS}}^{\dagger} \hat{a}_{\mathrm{in}} \hat{U}_{\mathrm{BS}}. \tag{1.78}$$

Using the Heisenberg equation for the input operators $\hat{a}$ and $\hat{b}$ will give us equations of the form of (1.73) and (1.74) for our output operators [27].

The equations, (1.73) and (1.74), can also be written in matrix formalism,

$$\begin{pmatrix} \hat{a}_{\mathrm{out}} \\ \hat{b}_{\mathrm{out}} \end{pmatrix} = \begin{pmatrix} t_a & r_b \\ r_a & t_b \end{pmatrix} \begin{pmatrix} \hat{a}_{\mathrm{in}} \\ \hat{b}_{\mathrm{in}} \end{pmatrix}. \tag{1.79}$$

The beamsplitter matrix must be unitary and thus conditions are imposed

upon the transmission and reflection coefficients. These are,

$$\left.\begin{array}{c} t_a t_b^* + r_a r_b^* = 1, \\ t_a r_b^* + t_b^* r_a = 0, \\ t_a r_a^* + t_b^* r_b = 0, \\ |r_a| = |r_b|, \\ |t_a| = |t_b|. \end{array}\right\} \tag{1.80}$$

The beamsplitter is called symmetric if the matrix can be written as,

$$\begin{pmatrix} t & r \\ r & t \end{pmatrix}, \tag{1.81}$$

and unitarity conditions lead to,

$$\begin{aligned} |t|^2 + |r|^2 &= 1 \\ tr^* + t^* r &= 0\,. \end{aligned} \tag{1.82}$$

A simple way to calculate the output state using equations (1.73) and (1.74) is to invert them and express $\hat{a}_{\rm in}^\dagger, \hat{b}_{\rm in}^\dagger$ in terms of the output operators,

$$\hat{a}_{\rm in}^\dagger = t\hat{a}_{\rm out}^\dagger + r\hat{b}_{\rm out}^\dagger \tag{1.83}$$

$$\hat{b}_{\rm in}^\dagger = t\hat{b}_{\rm out}^\dagger + r\hat{a}_{\rm out}^\dagger. \tag{1.84}$$

The general input state to our beamsplitter, $|n_1, m_2\rangle$ (n photons in input mode 1, m photons in input mode 2), is written as,

$$|n_1, m_2\rangle = \frac{(\hat{a}_{\rm in}^\dagger)^n}{\sqrt{n!}} \frac{(\hat{b}_{\rm in}^\dagger)^m}{\sqrt{m!}} |0, 0\rangle, \tag{1.85}$$

and then the input operators are replaced with the output mode operators according to equation (1.83) and (1.84). This gives us a state in terms of the output photon modes. To transform coherent states we can use the displacement operator, equation 1.66. Starting with a general input of a

coherent state in each mode,

$$\begin{aligned} |\alpha\rangle_a |\beta\rangle_b &= \hat{D}(\alpha)\hat{D}(\beta)|0\rangle_{ab} = \exp\left[\alpha\hat{a}_{\rm in}^\dagger - \alpha^*\hat{a}_{\rm in}\right]\exp\left[\beta\hat{b}_{\rm in}^\dagger - \beta^*\hat{b}_{\rm in}\right]|0\rangle_{ab} \\ &= \exp\left[\alpha\hat{a}_{\rm in}^\dagger + \alpha^*\hat{a}_{\rm in} + \beta\hat{b}_{\rm in}^\dagger + \beta^*\hat{b}_{\rm in}\right]|0\rangle_{ab}\,, \end{aligned} \tag{1.86}$$

where we can obtain the last term because operators from different modes commute. We then replace the input operators with the output operators, which leads to,

$$\begin{aligned} &\exp\left[(t\alpha + r\beta)\hat{a}_{\rm out}^\dagger - (t\alpha + r\beta)^*\hat{a}_{\rm out} + (t\beta + r\alpha)\hat{b}_{\rm out}^\dagger - (t\beta + r\alpha)^*\hat{b}_{\rm out}\right]|0\rangle_{ab} \\ &= \hat{D}_a(t\alpha + r\beta)\hat{D}_b(t\beta + r\alpha)|0\rangle_{ab} \\ &= |t\alpha + r\beta\rangle_{\rm a}|t\beta + r\alpha\rangle_{\rm b}\,, \end{aligned} \tag{1.87}$$

which is a separable state at the output, again, highlighting how classical coherent states are. We will use this result in subsequent chapters.

1.5 Overview of thesis

In this thesis we will examine some various applications of quantum measurements applied to different situations in quantum computing, cryptography and open quantum systems, using the theory of quanutm optics and photons as the physical implementation.

In Chapter 2 we discuss a measure of success for postselecting devices. These are necessary components for scalable linear optical quantum computing that create certain quantum states conditioned on measurements made on some modes of that state. The measure discussed here is based on the standard quantum fidelity, the overlap of two states.

In Chapter 3 we discuss a method to improve the confidence of measurement results from lossy photo-detectors by placing an optical amplifier in front of them. We show this pre-amplification method to work even when the amplifier adds excess noise photons to the amplified signal.

In Chapter 4 we apply the work from the previous two chapters to an example of a postselecting device for quantum key distribution and calculate the success of this device when imperfect device components are present.

In Chapter 5 we analyse an evolution equation for a quantum system undergoing repeated quantum measurements. This master equation is shown to be of Lindblad form and we analyse different forms of measurement operators acting upon it.

Chapter 6 contains our conclusions.

Chapter 2

Fidelity for postselecting devices

2.1 Introduction

In the previous chapter we discussed some of the theory of quantum mechanics, touching upon measurements, evolution and the quantum mechanical description of light.

In this chapter we analyse a device known as a postselecting device, providing a measure of success for its operation. These devices are important for Linear Optical Quantum Computing (LOQC). We first begin by explaining LOQC, and quantum computing in general, and the use of postselecting devices within it. The measure presented here will be based on the fidelity of quantum states, which is a distance measure for quantum states, and so we will then explain what distance measures are for quantum states. Then we introduce our measure of fidelity for a postselecting device, and explain why it is a more accurate measure of how well a quantum device operates than the straight-forward fidelity. Finally we will provide two examples of postselecting devices and use our measure to quantify how well they work.

2.2 Quantum computing

Traditional computations are carried out by adding and subtracting 'bits' in various ways to form algorithms, where a bit has either the value '0' or '1'. Quantum computers use two level states, know as qubits, to represent classical bits. A qubit state would look like,

$$a\,|0\rangle + b\,|1\rangle\,, \tag{2.1}$$

where $|a|^2 + |b|^2 = 1$. The difference between the qubit and the classical bit is that the former has coherence: it can take part in interference.

It was Deutsch [28] who first showed that a quantum algorithm could be faster than a classical algorithm. The Deutsch algorithm calculates whether or not a function, $f(x)$, of a single qubit, is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$), with a single call of the function. In classical physics this would take two calls of the function. This algorithm was then generalised to many qubits by Deutsch and Jozsa [29].

Although these algorithms showed that quantum computation could be faster than classical computation, the first algorithm to have important practical implications was Shor's factoring algorithm [30]. This algorithm yields an exponential speed-up in finding the factors of prime numbers and has implications in cryptography protocols such as RSA [31] that rely on the difficulty in factoring large primes for their security. Another useful algorithm is Grover's search algorithm [32, 33] which can reduce the number of times an un-structured database of N entries has to accessed by a factor of $O(\sqrt{N})$.

The circuit-based model of quantum computation resembles the classical model of computation. The 'computer', we are not specifying a physical representation yet, consists of gates connected by wires, where the wires transport the qubits and the gates act upon them. A gate in quantum computing has a logic table in much the same way as a classical gate, for example the controlled-not gate in quantum computing is an entangling gate of two

qubits that performs the operation,

$$\alpha\,|0\rangle + \beta\,|1\rangle \otimes |0\rangle \rightarrow \alpha\,|00\rangle + \beta\,|11\rangle\,, \tag{2.2}$$

where it flips the bit of the second qubit if the first qubit is $|1\rangle$. It has been shown that the only multi-qubit gates quantum computation needs are two-qubit operations [34].

An alternative to the circuit model of quantum computing is the measurement driven model [35, 36] that uses a special state known as a cluster state [37]. This model starts by entangling a large number of qubits and then performing measurements on some qubits. The results of those measurements then determine what gates are applied to the qubits to obtain the desired algorithm. The advantage here is that all the entangling operations are carried out at the start and afterwards the only operations needed are single qubit gates and measurement.

Research into the physical realisation of quantum computers has many potential systems that could be used for the qubits and quantum gates. These include ion traps [38] that use two levels of an ion contained by magnetic and electric fields, optical lattices [39], spin systems and quantum dots [40]. In this thesis we will look at an aspect of one implementation using photons and linear optical devices.

2.3 Linear optical quantum computing

LOQC is a physical implementation of quantum computing that uses photons as the qubits and gates that are composed of linear optical elements such as beamsplitters [41]. The qubits are either encoded in the spatial modes of the photon, termed 'dual-rail', or in the polarization modes of the photons, which can be horizontally or vertically polarized.

There is a problem, however, with using photons as qubits. While single qubit operations are easy, two qubit operations and gates are difficult. This is due to the fact photons do not readily interact with each other. For example,

a Kerr medium allows for non-linear interactions between photons with the Kerr effect parametrized by a value $\chi^{(2)}$. The Hamiltonian for the cross-Kerr interaction is,

$$\hat{H} = \chi^{(2)}\hat{b}^\dagger\hat{b}\hat{a}^\dagger\hat{a} = \chi^{(2)}\hat{n}_b\hat{n}_a, \tag{2.3}$$

and this Hamiltonian yields a controlled-z gate between photons. Unfortunately, the values of $\chi^{(2)}$ in materials are not large enough to be of reliable use in a quantum computer, while other effects from the Kerr medium distort the output state.

Knill, Laflamme and Milburn (KLM) [42] provided a solution to the lack of non-linearities. They demonstrated how linear optical devices could be used to perform non-linear tasks, such as a C-NOT gate. The non-linear element is introduced by the process of measuring ancilla modes of the system and after the result is known using the remaining modes accordingly. This process of dynamics conditioned on measurement is know as postselection. The down-side of this is that the gate is non-deterministic, meaning that we know when it works but that it does not work on every run of the device.

In their paper they first showed how to produce a non-linear sign shift (NSS) gate, shown in fig. 2.1 which performs the transformation,

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \rightarrow |\psi'\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle. \tag{2.4}$$

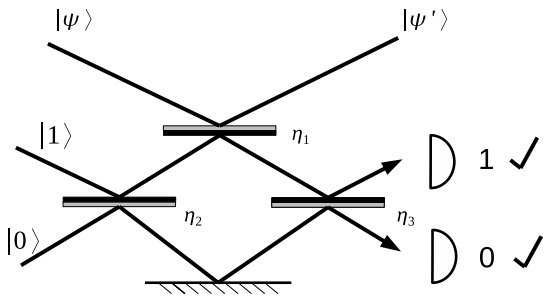


Figure 2.1: A non-linear sign shift gate. The gate works correctly when the detectors in the ancilla modes click with the desired results, as shown.

The lack of a normalization factor here reflects the fact that this transformation is non-deterministic, although we would know when the transformation has occurred by measuring ancillary modes in the device. It has a probability of 25% to work. By combining two of these CSS gates together, the C-NOT gate can be obtained, but again this gate is non-deterministic and operates with probability 1/16 (25% $\times$ 25%).

As these non-linear gates are probabilistic, operating with probability p, the chance of N gates working together in sequence is at best p^N, which tends to zero for large N. KLM employed the 'teleportation trick' devised by Gottesman and Chaung [9, 43]. They teleported the probabilistic part of the gate into circuit after it had been shown to work, thus turning the gate into a deterministic one. This requires the use of entangled qubits, for example the four Bell states, and a scheme to perform this with photonic qubits was devised by by Yoran and Reznik [44], using both the spatial and polarization modes as the qubits. This scheme allows all four measurements in the Bell basis to be performed in LOQC, which was not possible in previous schemes [45].

Quantum computation will only work if errors in the scheme are not above a certain rate, thus classing the scheme as fault-tolerant. Thus quantifying how well individual parts operate is crucial to examining the overall success of the scheme. In the rest of this chapter we will describe a measure of successful operation for postselecting devices, which will be used in other chapters. This measure will be based on the fidelity of quantum states, a distance measure for quantum states. We describe the fidelity in the next section before we introduce our postselection measure.

2.4 Quantum distance measures and fidelity

In information theory it is useful to quantify how similar two messages are to one another by use of a measure giving quantitative answers. This would be termed a distance measure, with two messages that are similar being 'close'

and another two messages that are dis-similar being far apart. The exact measure used will depend on how the messages are encoded. For example Euclidean distance is such a measure for points in space.

In quantum physics, distance measures can be used to quantify how accurately two quantum states can be distinguished from each other or how well a quantum process creates a particular state. In the first example we are concerned with how 'far apart' two states are and in the second example we want to see how 'close' two states are. There are various measures of quantum distance between two states [46, 47]. The first one is the trace distance, and for two pure quantum states, $\hat{\rho}$ and $\hat{\sigma}$, it is defined as,

$$D(\hat{\rho}, \hat{\sigma}) = \mathrm{Tr}\left[|\hat{\rho} - \hat{\sigma}|\right]. \tag{2.5}$$

The trace distance fulfils the required properties of a metric,

1. $D(\hat{\rho}, \hat{\sigma}) = D(\hat{\sigma}, \hat{\rho})$
2. $D(\hat{\rho}, \hat{\sigma}) \geq 0$
3. $D(\hat{\rho}, \hat{\rho}) = 0$
4. $D(\hat{\rho}_1, \hat{\rho}_2) \leq D(\hat{\rho}_1, \hat{\rho}_3) + D(\hat{\rho}_3, \hat{\rho}_2)$.

The last property is the Cauchy-Schwarz inequality (the 'triangle inequality').

The second quantum distance measure is the quantum fidelity. This is used as a basis for measuring how accurately a postselecting device creates a desired state and is described in the next section.

2.4.1 Fidelity of two quantum states

The fidelity for two pure quantum states, $|\phi_1\rangle$ and $|\phi_2\rangle$, is defined as,

$$F(|\phi\rangle_1, |\phi\rangle_2) = |\langle\phi_1|\phi_2\rangle|^2, \tag{2.6}$$

and satisfies the following conditions,

1. $F(|\phi_1\rangle, |\phi_2\rangle) = F(|\phi\rangle_2, |\phi\rangle_1)$

2. $1 \geq F(|\phi_1\rangle, |\phi_2\rangle) \geq 0$

3. $F(|\phi_1\rangle, |\phi_1\rangle) = 1$

The quantum fidelity is not a metric because for identical quantum states it equals unity (not zero).

The above definition for quantum fidelity is for pure states; to include mixed states we require a definition in terms of density matrices. Using the density matrices for the states we can write the fidelity as,

$$F(\hat{\rho}_1, \hat{\rho}_2) = \mathrm{Tr}[\hat{\rho}_1 \hat{\rho}_2], \tag{2.7}$$

where at least one of the states must be pure. If both states are mixed then the expression for the fidelity was given by Jozsa [48] and is based on Uhlmann's transition probability [49] for mixed states. Uhlmanns's work obtained a transition probability for mixed states by taking the supremum overlap over all purifications of both mixed states.

Jozsa showed that the quantum fidelity when both states were mixed is defined by,

$$F(\hat{\rho}_1, \hat{\rho}_2) = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\rho}_1}\hat{\rho}_2\sqrt{\hat{\rho}_1}}\right]. \tag{2.8}$$

Although this expression looks unusual it satisfies the criteria above for pure state fidelities. One note is that the square-root of a density matrix $\hat{\rho}$ can be found by diagonalizing the density operator (using a unitary transformation) and then taking the square root of the diagonal matrix and unitary matrices,

$$\sqrt{\hat{\rho}} = \sqrt{\hat{U}\,\hat{\rho}_D\,\hat{U}^\dagger} = \hat{U}\,\sqrt{\hat{\rho}_\mathrm{D}}\,\hat{U}^\dagger. \tag{2.9}$$

The square root of a diagonal matrix is simply the square root of the entries (in the case of the density operator, they are all real) along the diagonal and the unitary matrix is its own square root.

In the next section we describe our measure for the successful operation of a postselecting device and demonstrate that this measure depends on two factors. The first factor depends upon the output state itself. It should be perfectly correlated in order that there is a one-to-one correspondence between measurement results in the detector arm and the remaining state in the other arms. The next factor depends upon the detector arm properties. Here, we should have a detector that distinguishes between different outcomes perfectly. That means that the relevant POM elements should be orthogonal to one another (in a subsequent chapter we will describe a method to improve confidence in measurements results in the case of imperfect detection). Our measure of success will quantify these two factors and will provide a means to maximize the fidelity.

2.5 Fidelity of correct output

In this section we describe a measure of success for the operation of a mixed state postselecting device. We have called this measure fidelity of correct output [50, 51]. This measure is based on the mixed state fidelity of two quantum states and it is most appropriate to use for postselectors that require a particular state to be successful.

In general, a postselector will have an output state correlated across several modes, or arms. In this derivation we will assume only two arms without loss of generality, as it is quite simple to group two or more modes into a single mode without changing the physics of the situation. Such a postselector is shown in fig. 2.2. We will label the arms of the postselector 1 and 2, and in arm 2 we will have a detector, which in an optical setup will be a photo-detector, and in arm 1 will be a quantum state that will be used for further computing/communication. The output state will therefore be labeled as $|\phi\rangle^{12}$, where the superscripts refer to the individual arms, and will

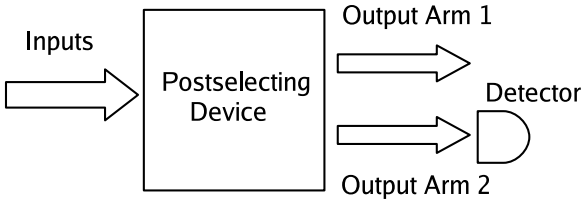


Figure 2.2: A typical postselecting device. This two-arm model can easily be generalized to many-arms.

be of the form,

$$|\phi\rangle^{12} = \sqrt{p_{\rm c}}\,|\phi\rangle_{\rm c}^{1} \otimes |\phi\rangle_{\rm c}^{2} + \sqrt{p_{\rm i}}\,|\phi\rangle_{\rm i}^{1} \otimes |\phi\rangle_{\rm i}^{2} \tag{2.10}$$

where the subscripts are for a 'correct' state and an 'incorrect' state and $p_{\rm c}$ is the *a priori* probability for the correct state and likewise for $p_{\rm i}$.

For the device to be able to operate perfectly, $|\phi\rangle_{\rm c}^{2}$ should be orthogonal to $|\phi\rangle_{\rm i}^{2}$. If not, say,

$$|\phi\rangle_{\rm i}^{2} = \sqrt{p}\,|\phi\rangle_{\rm c}^{2} + \sqrt{(1-p)}\,|\phi\rangle_{\bar{c}}^{2}\,, \tag{2.11}$$

then we can re-write the output state as,

$$|\phi\rangle^{12} = \sqrt{p_{\rm c}}\,|\phi\rangle_{\rm c}^{1} \otimes |\phi\rangle_{\rm c}^{2} + \sqrt{p_{\rm i}}\,|\phi\rangle_{\rm i}^{1} \otimes \left(\sqrt{p}\,|\phi\rangle_{\rm c}^{2} + \sqrt{(1-p)}\,|\phi\rangle_{\bar{c}}^{2}\right). \tag{2.12}$$

and we can see that the correct result in the detector arm is not perfectly correlated with the correct state in the output mode 1. Note that we do not require the possible states in mode 1 to be orthogonal and in general they will not be. Our device strictly requires the output state to be $|\phi\rangle_{\rm c}^{1}$ and no other state will suffice, even one with a non-zero overlap with $|\phi\rangle_{\rm c}^{1}$ (we term this $|\phi\rangle_{\rm c}^{1}$ 'sacred').

The detector in arm 2 can be described by a set of POM elements, $\{\hat{\pi}_m\}$. When we obtain the measurement result 'm' in the detector arm then the

state remaining in arm 1 will be defined by,

$$\hat{\rho}_m^1 = \frac{\mathrm{Tr}_2[\hat{\rho}^{12}\hat{\pi}_m]}{\mathrm{Tr}_{12}[\hat{\rho}^{12}\hat{\pi}_m]}. \tag{2.13}$$

We will assume, again without loss of generality, that there are only two measurement outcomes; the measurement result that corresponds to the state we want to produce, 'correct', and an 'incorrect' outcome. We will label these measurement outcomes as $\hat{\pi}_\mathrm{c}$ and $\hat{\pi}_\mathrm{i}$ respectively and note that $\hat{\pi}_\mathrm{c} + \hat{\pi}_\mathrm{i} = \hat{1}$. For a perfect postselector $\hat{\pi}_\mathrm{c}$ and $\hat{\pi}_\mathrm{i}$ must be orthogonal and,

$$\hat{\rho}_\mathrm{c}^2 = \frac{\hat{\pi}_\mathrm{c}}{\mathrm{Tr}[\hat{\pi}_\mathrm{c}]} \quad \hat{\rho}_\mathrm{i}^2 = \frac{\hat{\pi}_\mathrm{i}}{\mathrm{Tr}[\hat{\pi}_\mathrm{i}]}. \tag{2.14}$$

The output state that we want to produce in arm 1 is defined as $\hat{\rho}_\mathrm{c}$. Using the general fidelity for mixed states, the straight-forward overlap fidelity for our postselecting devices is,

$$F(\hat{\rho}_\mathrm{c}, \hat{\rho}_m^1) = \mathrm{Tr}\left[\sqrt{\sqrt{\hat{\rho}_m^1}\hat{\rho}_\mathrm{c}\sqrt{\hat{\rho}_m^1}}\,\right]. \tag{2.15}$$

We now look at what happens when the output state produced is not perfect i.e. $\hat{\rho}_m^1 \neq \hat{\rho}_\mathrm{c}$, even if the detector is perfect. This would happen if our output state was not perfectly correlated e.g. if the state was of the form of the one shown in equation 2.12. We could then write our output state after measurement as a combination of the correct state and some other, useless, state,

$$\hat{\rho}_m^1 = P^{\max}\hat{\rho}_\mathrm{c} + \hat{\gamma}, \tag{2.16}$$

where $P^{\max}$ is the weight of $\hat{\rho}_\mathrm{c}$ that can be obtained from $\hat{\rho}_m^1$ and $\hat{\gamma}$ is a operator that represents the useless components of the density operator. Although this second term may have a non-zero overlap with the correct state $\hat{\rho}_\mathrm{c}$, we are only concerned with keeping terms that contribute to the correct operation of the device. Terms of this kind would be included in the full overlap fidelity, artificially increasing its value. If we remove this term from

our output state then we can write the fidelity of correct output, $F_{\rm c}$, as,

$$F(\hat{\rho}_{\rm c}, \hat{\rho}_m^1) \geq F_{\rm c}(\hat{\rho}_{\rm c}, \hat{\rho}_m^1) = P^{\max} F(\hat{\rho}_{\rm c}, \hat{\rho}_{\rm c}) = P^{\max} \tag{2.17}$$

which will, in general, be less than unity and provides a lower bound on the fidelity of this device. In the next section we will include the effects of imperfect detection.

2.5.1 Detection element

In this section we will show how imperfect detection affects the confidence in measurement results. If we take a postselecting device that works on detection of result 'c' then for perfect detection we would require that the measurement operator corresponding to this result, $\hat{\pi}_{\rm c}$, be orthogonal to any other measurement operators describing the detector. We can write the other possible measurement results in a single operator (as we are only concerned with two results; 'c' or 'not c'),

$$\hat{\pi}_{\rm i} = \hat{1} - \hat{\pi}_{\rm c}, \tag{2.18}$$

and so we require that $\mathrm{Tr}[\hat{\pi}_{\rm c}\, \hat{\pi}_{\rm i}] = 0$ for a perfect detector. With an imperfect detector the measurement outcomes are no longer orthogonal,

$$\begin{aligned} \hat{\pi}'_{\rm c} &= P^{\rm p}({\rm c}|{\rm c})\hat{\pi}_{\rm c} + P^{\rm p}({\rm c}|{\rm i})\hat{\pi}_{\rm i} \\ \hat{\pi}'_{\rm i} &= P^{\rm p}({\rm i}|{\rm c})\hat{\pi}_{\rm c} + P^{\rm p}({\rm i}|{\rm i})\hat{\pi}_{\rm i}, \end{aligned}$$

where the '$P^{\rm p}$' are predictive conditional probabilities e.g. $P^{\rm p}({\rm c}|{\rm i})$ is the probability that the measurement operator $\hat{\pi}_{\rm i}$ is mistaken for $\hat{\pi}_{\rm c}$. Here $P^{\rm p}({\rm c}|{\rm i})$ is the predictive probability that an incorrect result will be recorded as a correct result by the measurement device.

We note that the new measurement operators satisfy $\hat{\pi}'_{\rm c} + \hat{\pi}'_{\rm i} = \hat{1}$, where $\hat{1}$ is the identity operator of the system. Thus $P^{\rm p}({\rm c}|{\rm c}) + P^{\rm p}({\rm i}|{\rm c}) = 1$ and $P^{\rm p}({\rm c}|{\rm i}) + P^{\rm p}({\rm i}|{\rm i}) = 1$ satisfying the completeness relation for POMs.

When we substitute this imperfect POM element into the expression for the output state, equation 2.13, we obtain,

$$\begin{aligned}\hat{\rho}_{\mathrm{c}}^{\prime 1} &= \frac{\mathrm{Tr}_2\left(\hat{\rho}^{12}\hat{\pi}_{\mathrm{c}}^{\prime}\right)}{\mathrm{Tr}_{12}\left(\hat{\rho}^{12}\hat{\pi}_{\mathrm{c}}^{\prime}\right)} \\ &= \frac{P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})p_{\mathrm{c}}\hat{\rho}_{\mathrm{c}}^{1} + P^{\mathrm{p}}(\mathrm{c}|\mathrm{i})p_{\mathrm{i}}\hat{\rho}_{\mathrm{i}}^{1}}{P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})p_{\mathrm{c}} + P^{\mathrm{p}}(\mathrm{c}|\mathrm{i})p_{\mathrm{i}}} \\ &= P^{\mathrm{r}}(n|n)\hat{\rho}_{n}^{1} + \sum_{m\neq n} P^{\mathrm{r}}(m|n)\hat{\rho}_{m}^{1}, \end{aligned} \tag{2.19}$$

where $P^{\mathrm{r}}(\mathrm{c}|\mathrm{c})$ is the retrodictive conditional probability that we had state 'c' in the detector given we registered result 'c' and p_{c} and p_{i} are defined in equation 2.10. The last line is obtained by using Bayes' Theorem, which relates conditional probabilities $P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})$ with $P^{\mathrm{r}}(\mathrm{c}|\mathrm{c})$ [15] (see also section 1.2.2).

We now include the effects of an imperfect postselector by substituting the form of the output density matrix from equation 2.16 into the expression for the state in mode 1 after an imperfect correct measurement has been made, equation 2.19, to arrive at,

$$\hat{\rho}_{\mathrm{c}}^{\prime 1} = \frac{P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})P^{\max}\hat{\rho}_{\mathrm{c}} + P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})\hat{\gamma} + P^{\mathrm{p}}(\mathrm{c}|\mathrm{i})\hat{\rho}_{\mathrm{i}}}{P^{\mathrm{p}}(\mathrm{c}|\mathrm{c})p_{\mathrm{c}} + P^{\mathrm{p}}(\mathrm{c}|\mathrm{i})p_{\mathrm{i}}} \tag{2.20}$$

We discard the second two terms in this expression, as they do not meaningfully contribute to the successful operation of the device, and calculating the fidelity, equation 2.8, of the remaining term with $\hat{\rho}_{\mathrm{c}}$ we obtain an expression for the fidelity of correct output as,

$$F_{\mathrm{c}} = P^{\max}P^{\mathrm{r}}(\mathrm{c}|\mathrm{c}), \tag{2.21}$$

and we see that the fidelity for correct output, F_{c}, depends on two factors. The first factor, $P^{\max}$, depends on the quality of the output state only and can be seen as the fidelity between the correct state and the state that we produce when we obtain result 'c' in the detector arm. The second factor

depends on the properties of the detection arm and the POM elements used to describe the measurements, and is unity for a perfect detector. In the following section we will provide examples using this measure to determine the fidelity of postselecting devices.

2.6 Examples of postselecting devices

In the following sections we will demonstrate how our measure of fidelity works for various postselecting devices. The first device we will examine is one that generates a two-photon state and the next is one that compares two Glauber coherent states to determine if they are identical or not.

2.6.1 Two-photon generation with a lossy beamsplitter

We first explain the use of our measure on a simple system. A 50/50 beamsplitter with a single photon in each input mode will produce the well known two photon interference effect, shown experimentally by Hong, Ou and Mandel [52]. In their experiment they used a photon-down conversion source to prepare pairs of photons that were then directed onto the arms of a beamsplitter, as shown in fig. 2.3(a). By altering the position of the beamsplitter and thus the overlap of the two photons entering it, the number of coincidence counts in the two output arms moved from a maximum to zero, shown in fig. 2.3(b). This is known as the Hong-Ou-Mandel dip.

Using the beamsplitter theory described in section 1.4.2, we can explain this effect. When two photons enter different arms, which we label a and b, of a symmetric beamsplitter with transmission and reflection coefficients $t = 1/\sqrt{2}, r = i/\sqrt{2}$, the input state is,

$$\hat{a}^{\dagger}_{in}\hat{b}^{\dagger}_{in}\left|0,0\right\rangle_{ab},$$

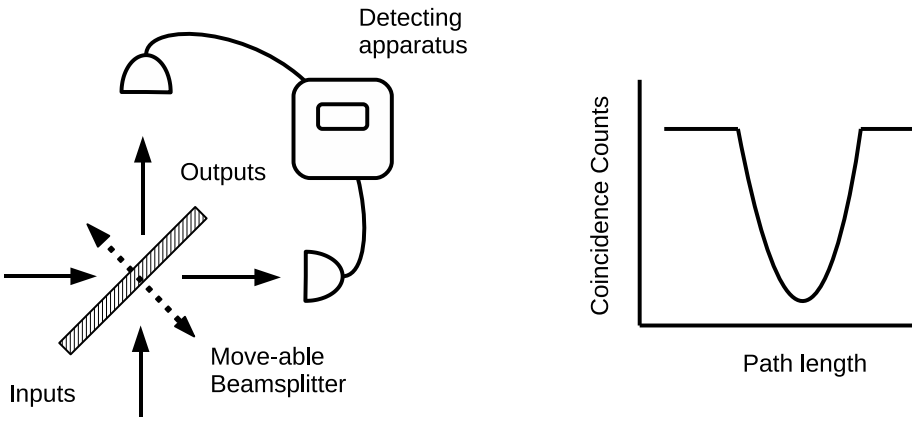


Figure 2.3: **a)** The Hong-Ou-Mandel experimental setup and **b)** the result from the experiment. This result shows that pairs of perfectly-overlapping photons interfere at the beamsplitter to always leave in the same output arm.

and substituting the output operators for the input operators,

$$\begin{aligned}
& \left(t\hat{a}^{\dagger}_{out} + r\hat{b}^{\dagger}_{out}\right)\left(t\hat{b}^{\dagger}_{out} + r\hat{a}^{\dagger}_{out}\right)|0,0\rangle_{ab} \\
= & \left(\frac{1}{\sqrt{2}}\,\hat{a}^{\dagger}_{out} + \frac{i}{\sqrt{2}}\,\hat{b}^{\dagger}_{out}\right)\left(\frac{1}{\sqrt{2}}\,\hat{b}^{\dagger}_{out} + \frac{i}{\sqrt{2}}\,\hat{a}^{\dagger}_{out}\right)|0,0\rangle_{ab} \\
= & \left(t^2 + r^2\right)\hat{a}^{\dagger}_{out}\hat{b}^{\dagger}_{out} + tr\left(\hat{a}^{\dagger 2}_{out} + \hat{b}^{\dagger 2}_{out}\right)|0,0\rangle_{ab} \\
= & \frac{i}{\sqrt{2}}\left(|2,0\rangle_{ab} + |0,2\rangle_{ab}\right),
\end{aligned}$$

and we can see that the amplitude of the state with photons leaving in both output arms is zero. Thus both photons leave in the same arm and we can consider such a device as a two-photon state generator. This effect is due to the photons being bosonic (an alternative effect occurs when fermionic particles are used, with both particles leaving in different arms [53]) and has uses in LOQC gates as it is the only way that photons can influence one another in linear optical elements [41].

However if we have a lossy beamsplitter then the output state will contain other terms, such as $|1,0\rangle_{ab}$ and $|0,0\rangle_{ab}$, that will also have a vacuum component in the detector arm, but do not produce the correct state in the other

arm. Such a situation would be a problem for gate operations in a quantum computer, as it would either induce gate errors or project the system out of the computational space. In order to calculate the operation of the device, we need to now the output probabilities for the various states that can occur. We use results obtained by Barnett *et. al.* [54] that calculate the required probabilities. We summarise briefly their model of a lossy beamsplitter.

To calculate the output state from a lossy beamsplitter, we replace the beamsplitter equations from section 1.4.2 with,

$$\begin{aligned} \hat{a}_{out} &= t\hat{a}_{in} + r\hat{b}_{in} + \hat{F}_a \\ \hat{b}_{out} &= t\hat{b}_{in} + r\hat{a}_{in} + \hat{F}_b \end{aligned}$$

where $\hat{F}$ is a Langevin term that will allow for loss terms and has the following averages,

$$\langle \hat{F}_a, \hat{F}_a^\dagger \rangle = 1 - |t|^2 - |r|^2$$

$$\langle \hat{F}_a, \hat{F}_b^\dagger \rangle = tr^* + t^* r,$$

and the single operator averages, $\langle \hat{F} \rangle$, are all zero.

The probabilities for certain photon-number components can be obtained using counting formulae [54, 55, 56], and are just stated here,

$$\begin{aligned} p_{20} &= p_{02} = 2|t|^2|r|^2 \\ p_{11} &= |t|^4 + |r|^4 + t^2 r^{*^2} + r^2 t^{*^2} \\ p_{10} &= p_{01} = (|t|^2 + |r|^2)(1 - |t|^2 - |r|^2) - (tr^* + rt^*)^2 \\ p_{00} &= (1 - |t|^2 - |r|^2)^2 + (tr^* + rt^*)^2, \end{aligned}$$

where p_{nm} is the probability that the beamsplitter produces the state $|n, m\rangle_{ab} \langle m, n|$. These terms depends on the magnitude and phase of t and r, the transmission and reflection coefficients of the beam splitter.

If we now assume that the desired state we wish to create is $\hat{\rho}_c = |2, 0\rangle_{ab} \langle 2, 0|$ i.e. two photons leaving the a mode and zero photons in the

b mode, which has our photodetector. When we measure zero photocounts in the b arm the state in the a arm is,

$$\hat{\rho}_a = \frac{p_{20}|2\rangle\langle 2| + p_{10}|1\rangle\langle 1| + p_{00}|0\rangle\langle 0|}{p_{20} + p_{10} + p_{00}} = P^{\max}\hat{\rho}_{\rm c} + \hat{\gamma}, \tag{2.22}$$

given a perfect detector, such that $P^{\rm r}(n|n) = 1 \; \forall \; n$. We can equate $P^{\max}$ with the correct output fidelity,

$$F_{\rm c} = P^{\max} = \frac{p_{20}}{p_{20} + p_{10} + p_{00}} \tag{2.23}$$

Note that in the denominator the phase dependent terms, $(tr^* + rt^*)^2$, cancel from p_{10} and p_{00}, meaning that the expression for $F_{\rm c}$ only depends on $|t|$ and $|r|$. Equation (2.23) is plotted in fig. (2.4) where we have assumed that $|t| = |r|$. This shows that the fidelity tends to unity as the beam splitter approaches 50/50. For this system the Jozsa fidelity, equation 2.8, is equal

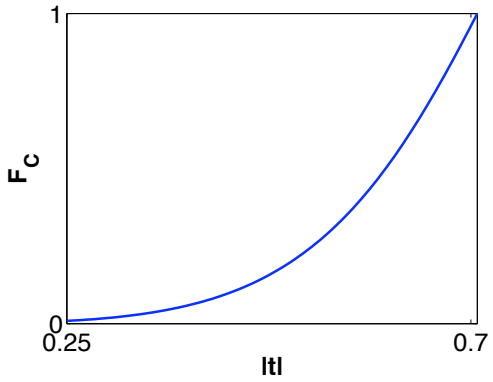


Figure 2.4: Correct output fidelity for a two-photon generator with loss in the beam splitter vs. transmission coefficient of the beam splitter ($|t| = |r|$).

to the fidelity of correct output due to the orthogonal nature of the number states. In the next section we will discuss a postselecting device where this is not the case.

2.6.2 Comparison of two coherent states

In this section we will discuss a postselecting device that seeks to determine if two coherent states are identical or not. Glauber coherent states, first introduced in section 1.4.1, are superpositions of Fock number states and are non-orthogonal. This means that any two coherent states cannot be perfectly distinguished.

Andersson *et. al.* [57] devised a test to determine if two coherent states were identical or not. This test involves interfering two coherent states at a beamsplitter and measuring the output from one arm to determine if the states are identical or not, a typical postselecting setup. Depending on the result from the measurement the state in the other arm can be manipulated to recover the two original states. This test has uses in searching a database [58] and, as will be discussed in a later Chapter, quantum key distribution.

The transformation for two coherent states of light entering a beamsplitter is straight-forward and we described it in section 1.4.2. For two arbitrary coherent states the transformation is,

$$\begin{aligned} &|\alpha\rangle_a \langle\alpha| \quad \otimes |\beta\rangle_b \langle\beta| \\ &\quad \rightarrow \quad |t_b\beta + r_a\alpha\rangle_b \langle t_b\beta + r_a\alpha| \otimes |t_a\alpha + r_b\beta\rangle_a \langle t_a\alpha + r_b\beta| \,, \end{aligned} \tag{2.24}$$

where the state on the left hand side of this equation is the state of light entering the beamsplitter and the right hand side is the output state. It can be seen that if appropriate choices of t and r are made then when we have identical coherent states as inputs to the device then the output will be the vacuum state in one arm and a combination of the coherent states in the other. The choice we make for $t_a = t_b = 1/\sqrt{2}$, $r_a = 1/\sqrt{2}$ and $r_b = -1/\sqrt{2}$, which satisfy the conditions for beamsplitters, equations 1.80.

When identical coherent states enter each arm of the beamsplitter, say $|\alpha\rangle$, the output state across the two arms is,

$$|\alpha\rangle_a \otimes |\alpha\rangle_b \rightarrow \left|\sqrt{2}\alpha\right\rangle_a \otimes |0\rangle_b \,. \tag{2.25}$$

Upon measuring the vacuum in the second arm we will know that the two states were identical. We can then split the coherent state of light in the first arm at another beamsplitter to regain the state $|\alpha\rangle \otimes |\alpha\rangle$ at the output. When different coherent states, i.e. $|\alpha\rangle$ and $|\beta\rangle$, form the input there will be a finite-amplitude coherent state in the second output arm,

$$|\alpha\rangle_a \otimes |\beta\rangle_b \rightarrow \left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_a \otimes \left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_b \tag{2.26}$$

and photo-counts can be recorded by the detector in this second arm, signalling that the states were different.

Unfortunately, as all coherent states have a vacuum state component, it is possible for this to be the outcome when measuring a non-zero coherent state in the detector arm. When this occurs we will mistake two different states as being identical. This means that when we detect zero photocounts we cannot determine with certainty whether or not two states are different or identical. The setup therefore has the form of an unambiguous measurement scheme [59] where we can distinguish between two non-orthogonal quantum states if we accept the possibility of an inconclusive result. Here we know for definite if the two states are different but the result that corresponds to the states being identical, zero photo-counts, is ambiguous.

To calculate the fidelity of correct output of this device we assume that the input to the beamsplitter is,

$$|\alpha\rangle_a \langle\alpha| \otimes \frac{1}{2}\left[|\alpha\rangle_b \langle\alpha| + |\beta\rangle_b \langle\beta|\right], \tag{2.27}$$

and that we have a photo-detector that differentiates between zero photo-counts and non-zero photo-counts. Our output state from the beamsplitter described above is then,

$$\begin{aligned}\hat{\rho}_{ab} = \frac{1}{2}\Bigg[&\left|\sqrt{2}\alpha\right\rangle_a \left\langle\sqrt{2}\alpha\right| \otimes |0\rangle_b \langle 0| \\ &+ \left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_a \left\langle\frac{\alpha+\beta}{\sqrt{2}}\right| \otimes \left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_b \left\langle\frac{\alpha-\beta}{\sqrt{2}}\right|\Bigg].\end{aligned} \tag{2.28}$$

Our photodetector has measurement operators $\hat{\pi}_0 = |0\rangle\langle 0|$ and $\hat{\pi}_{\bar{0}} = \hat{1} - |0\rangle\langle 0|$, i.e zero and not zero. Our state in the a arm after detecting zero photo-counts in the b arm is,

$$\hat{\rho}_a = \frac{\mathrm{Tr}_b[\hat{\rho}_{ab}\hat{\pi}_0]}{\mathrm{Tr}_{ab}[\hat{\rho}_{ab}\hat{\pi}_0]}$$

$$= \frac{\left|\sqrt{2}\alpha\right\rangle_a \left\langle\sqrt{2}\alpha\right| + \exp\left[-\frac{1}{2}|\alpha-\beta|^2\right] \left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_a \left\langle\frac{\alpha-\beta}{\sqrt{2}}\right|}{1+\exp\left[-\frac{1}{2}|\alpha-\beta|^2\right]}. \tag{2.29}$$

We can write this state as,

$$\hat{\rho}_0 = P_{\max}\left|\sqrt{2}\alpha\right\rangle\left\langle\sqrt{2}\alpha\right| + \hat{\gamma}, \tag{2.30}$$

where $P_{\max} = 1/(1+e^{-\frac{1}{2}|\alpha-\beta|^2})$. The fidelity of correct output, with perfect detectors so that $P^{\mathrm{r}}(0|0) = 1$, is simply,

$$F_{\mathrm{c}} = P_{\max}. \tag{2.31}$$

We can see that even though our device has no imperfections the F_{c} is not unity. This is because we are trying to distinguish between two non-orthogonal quantum states, which is impossible to do with certainty in quantum mechanics. We also note that if we increase the amplitudes of the coherent states, or modify their phases, in order to increase the value of $|\alpha-\beta|$ then we succeed more often. This is because the states are now further apart, have a lower overlap and are therefore more distinguishable. We will comment on this aspect with regards to the quantum key distribution in the next section.

2.7 Conclusions

In this chapter we have described a measure of success for a postselecting device, termed the fidelity of correct output F_{c}. This measure is based on

the mixed-state fidelity, F, and intends to measure how close the state that the device produces is to the desired state we wish to produce. To derive $F_{\rm c}$ we assume that the desired state is 'sacred' and so discard other terms in the output state. These discarded terms may have a non-zero overlap with the desired state and so may inflate the strict mixed-state fidelity. Thus, $F_c \leq F$. We showed that $F_{\rm c}$ can be split into two factors; one which depends upon the output state from the device and another which depends upon detector arm properties. (In the next Chapter we discussed a method to improve the second factor.)

We then demonstrated the use of $F_{\rm c}$ with two examples of postselecting devices. The first was a two-photon generator and the second was a coherent state comparison device. In the latter example it was shown that $F_{\rm c} < F$ due to the inclusion of a term that was an intrinsic error in trying to distinguish non-orthogonal states.

Chapter 3

Fidelity increase by pre-amplification

In this Chapter we will describe and explain a method to improve our confidence in photo-detection measurement results with a lossy detector. This method involves placing an phase-insensitive optical amplifier in front of the lossy photo-detector, offsetting the loss of the detector using the gain of the amplifier [60, 61].

We will first describe the model of amplifiers and attenuators used in this Chapter, which is based on optical beamsplitters, and next describe the theory behind the pre-amplification method. We will then evaluate the usefulness of the method at improving confidence in measurement results in various scenarios, along with the downsides of such a method, discussing when the method works best.

3.1 Quantum theory of amplifiers and attenuators

In this section we will describe the phase-insensitive model of amplification and attenuation of optical quantum channels used in the rest of this chapter. We use the model of optical amplifiers and attenuators described in [22, 62],

where they are modelled by beamsplitters. There are also single mode theories that use noise operators [63, 64] to describe the channel that is amplified/attenuated. The fact that the models are phase-insensitve means that the output photon number distribution will only depend upon the input photon number distribution and not any off-diagonal coherence elements. This will mean that we can replace the density matrices by real-valued probability distributions later in the chapter.

We have discussed beamsplitters in a previous section, 1.4.2. For the following models, the quantum channel that is either amplified or attenuated enters and leaves the beamsplitter in the a-modes. The b-modes are the modes to which we lose or gain photons in the case of an attenuator/amplifier. They are typically considered to be a thermal environment coupled to our channel that we do not have access to. In the following sections we state the relationship between input and output photon number for attenuators and amplifiers and derive conditional probabilities for these events.

3.1.1 Attenuation

There are two equivalent ways to describe the effects of lossy detection. Either we can change the measurement operators of the detector to mixtures of photon number states [54] or we place an attenuator in front of a perfect detector that 'mixes' the state before it reaches the detector. In this chapter we will choose the latter, as the attenuation factor of the detector can then be compared to the amplification factor.

An attenuating photon channel is modeled by a beamsplitter with, for example, the following beamsplitter relations,

$$\hat{a}_{\text{out}} = \sqrt{\eta}\,\hat{a}_{\text{in}} + i\sqrt{1-\eta}\,\hat{b}_{\text{in}} \tag{3.1}$$

$$\hat{b}_{\text{out}} = i\sqrt{1-\eta}\,\hat{a}_{\text{in}} + \sqrt{\eta}\,\hat{b}_{\text{in}}, \tag{3.2}$$

where we have set,

$$t = \sqrt{\eta} \tag{3.3}$$

$$r = i\sqrt{1-\eta}, \tag{3.4}$$

and η is the probability for a photon to be successfully transmitted through the channel and $1-\eta$ as the probability for a photon to be reflected, which amounts to absorption by the attenuating channel. Equations 3.1 and 3.2 satisfy the beamsplitter relations in 1.80. If the attenuating channel is an inefficient detector then this parameter η is called the quantum efficiency of the detector.

We can write the input state of m photons in the a-mode and the vacuum entering the b-mode as,

$$\begin{aligned} |m\rangle_{a_{\rm in}} |0\rangle_{b_{\rm in}} &= \frac{(\hat{a}^\dagger_{\rm in})^m}{\sqrt{m!}} |0\rangle_{a_{\rm in}} |0\rangle_{b_{\rm in}} \\ &= \frac{\left(\sqrt{\eta}\,\hat{a}^\dagger_{\rm out} + i\sqrt{1-\eta}\,\hat{b}^\dagger_{\rm out}\right)^m}{\sqrt{m!}} |0\rangle_{a_{\rm out}} |0\rangle_{b_{\rm out}} . \end{aligned} \tag{3.5}$$

We now trace over the b-mode of the device (as this represents modes of an environment which we cannot observe), thus giving us an output state in mode a only. The diagonal density matrix elements of the output state are given by the expression,

$$\rho^{\rm out}_{nn} = \sum_{m=n}^{\infty} \left(\begin{array}{c} m \\ n \end{array} \right) \eta^n (1-\eta)^{m-n} \rho^{\rm in}_{mm}, \tag{3.6}$$

which only depends upon the input diagonal density matrix elements because we have a phase-insensitve attentuator. We will only be concerned with the diagonal elements as we intend to measure photon number, which these represent. (If we were to use homodyne detection, to measure phase, we would need the off-diagonal elements also.) The predictive conditional probability

that n photons exit the attenuator given that m photons entered is then,

$$P_{\rm att}^{\rm p}(n|m) = \left(\begin{array}{c} m \\ n \end{array} \right) \eta^n (1-\eta)^{m-n}, m \geq n. \tag{3.7}$$

The effect of the attenuation is equivalent to Bernoulli sampling the input distribution of photons. It has been shown that this type of sampling only reduces the mean of the original distribution by a factor η when the distribution is classical but it may alter the distribution of non-classical distributions like squeezed light [27].

3.1.2 Noise in an attenuator model

We now turn to noise in an attenuator model. As well as removing photons at random from the quantum channel an attenuator can also add noise photons, which enter the channel from the b-mode. We no longer set $|0\rangle_{\rm in} = |0\rangle_{\rm out}$ but that $|0\rangle_{\rm in}$ is now some superposition of all number states, typically one that yields a thermal distribution of output photon numbers. If we look at average values from the number operators of the output channel we have,

$$\begin{aligned} \langle \hat{a}_{\rm out}^\dagger \hat{a}_{\rm out} \rangle &= |t|^2 \langle \hat{a}_{\rm in}^\dagger \hat{a}_{\rm in} \rangle + |r|^2 \langle \hat{b}_{\rm in}^\dagger \hat{b}_{\rm in} \rangle \\ &= \eta \langle \hat{a}_{\rm in}^\dagger \hat{a}_{\rm in} \rangle + (1-\eta) \langle \hat{b}_{\rm in}^\dagger \hat{b}_{\rm in} \rangle, \end{aligned} \tag{3.8}$$

where the second term depends on the number of photons entering from the environment and can be considered a noise term. Typically this term will correspond to thermal light, and is therefore represented by a Planck thermal excitation function with a characteristic temperature T,

$$\langle \hat{b}_{\rm in}^\dagger \hat{b}_{\rm in} \rangle = \frac{1}{e^{\frac{\hbar\omega}{k_b T}} - 1} = N_{\rm att}(T). \tag{3.9}$$

This is the population factor for a thermal distribution of photons. At zero temperature $N_{\rm att}(0) = 0$, thus an attenuator can be noiseless.

3.1.3 Amplification

The simplest way to model an amplifier is to change the b_{in} mode to an inverted harmonic oscillator [65, 66], which leads to photons being added to the a-mode. Thus, an amplifying photon channel is modelled by a beamsplitter with the following beamsplitter relations,

$$\hat{a}_{\text{in}} = \sqrt{G}\,\hat{a}_{\text{out}} - \sqrt{G-1}\,\hat{b}^{\dagger}_{\text{out}} \tag{3.10}$$

$$\hat{b}_{\text{in}} = \sqrt{G}\,\hat{b}_{\text{out}} - \sqrt{G-1}\,\hat{a}^{\dagger}_{\text{out}}. \tag{3.11}$$

where G is the amplifier gain, $G \geq 1$, and the commutation relation leads to,

$$|t|^2 - |r|^2 = 1. \tag{3.12}$$

We can write an arbitrary input mode of n photons in the same way as an attenuator,

$$|n\rangle_{a_{\text{in}}} |0\rangle_{b_{\text{in}}} = \frac{(\hat{a}^{\dagger}_{\text{in}})^n}{\sqrt{n!}} |0\rangle_{a_{\text{in}}} |0\rangle_{b_{\text{in}}} = \frac{\left(t\hat{a}^{\dagger}_{\text{out}} + r\hat{b}_{\text{out}}\right)^n}{\sqrt{n!}} |0\rangle_{a_{\text{in}}} |0\rangle_{b_{\text{in}}}. \tag{3.13}$$

however in this case we cannot set $|0\rangle_{\text{in}} = |0\rangle_{\text{out}}$. This is due to the fact that an amplifier must add noise photons to the output mode that enter from the b-mode. To model the noise a thermal distribution is again chosen,

$$|0\rangle_{a_{\text{in}}} |0\rangle_{b_{\text{in}}} = \frac{1}{\sqrt{G}} \sum_{n=0}^{\infty} \left(\frac{\sqrt{G-1}}{\sqrt{G}}\right)^n |n\rangle_{\text{out}} |n\rangle_{b_{\text{out}}}. \tag{3.14}$$

If we use the last two expressions, 3.13 and 3.14, we can obtain a quantum state for the two output modes. We then trace across the environment b-mode which gives us the output density operator. The diagonal elements of $\hat{\rho}$ in the a-mode output are,

$$\rho^{\text{out}}_{nn} = \sum_{m=0}^{n} \begin{pmatrix} n \\ m \end{pmatrix} \frac{(G-1)^{n-m}}{G^{n+1}} \rho^{\text{in}}_{mm}. \tag{3.15}$$

This formula yields the predictive conditional probability that n photons leave the amplifier given that m photons entered it [67],

$$P^{\mathrm{p}}_{\mathrm{amp}}(n|m) = \left(\begin{array}{c} n \\ m \end{array} \right) \frac{(G-1)^{n-m}}{G^{n+1}},\ n \geq m. \tag{3.16}$$

In the next section we look at how noise is present in the output distribution of an amplifier.

3.1.4 Noise in an amplifier model

Unlike an attenuator an amplifier must add photons to the output in both the a and b modes. The average number of photons in the output channel of the a mode is given by,

$$\langle \hat{a}^{\dagger}_{\mathrm{out}} \hat{a}_{\mathrm{out}} \rangle = G \langle \hat{a}^{\dagger}_{\mathrm{in}} \hat{a}_{\mathrm{in}} \rangle + (G-1) \langle \hat{b}_{\mathrm{in}} \hat{b}^{\dagger}_{\mathrm{in}} \rangle, \tag{3.17}$$

and, as for attenuation, the second term can be considered a noise term as the photons enter from the environmental modes. We can re-arrange this term using the boson commutator,

$$\langle \hat{b}_{\mathrm{in}} \hat{b}^{\dagger}_{\mathrm{in}} \rangle = \langle \hat{b}^{\dagger}_{\mathrm{in}} \hat{b}_{\mathrm{in}} + 1 \rangle, \tag{3.18}$$

which shows that the expectation value contains a constant term. This indicates that the noise in an amplifier cannot be set to zero, unlike attenuation. Again we assume that the noise expectation value is thermal, as in 3.9,

$$\langle \hat{b}^{\dagger}_{\mathrm{in}} \hat{b}_{\mathrm{in}} + 1 \rangle = \frac{1}{e^{\frac{\hbar\omega}{kT}} - 1} + 1 = \frac{e^{\frac{\hbar\omega}{kT}}}{e^{\frac{\hbar\omega}{kT}} - 1} = N_{\mathrm{amp}}(T) \geq 1. \tag{3.19}$$

The amplifier's noise parameter is related to the attenuator's noise parameter $N_{\mathrm{amp}}(T) = 1 - N_{\mathrm{att}}(T)$. The mean number of output photons of the

amplifying channel is given by,

$$G\,\bar{n}_a + N_{\rm amp}(G-1) = G\,\bar{n}_a + n_{\rm ex}, \tag{3.20}$$

where the first term is the amplified input channel, with a mean number of photons $\bar{n}_a$ and the second term, $n_{\rm ex} = N_{\rm amp}(G-1)$, is the average number of noise photons added. An amplifier with $N_{\rm amp} > 1$ is termed an excess noise amplifier.

Taking excess noise photons into account, the predictive conditional probability that n photons leave the amplifier given that m photons entered it is given by [67],

$$\begin{aligned} P^{\rm p}_{\rm amp}(n|m) &= \sum_{s=0}^{min[n,m]} \left(\begin{array}{c} n \\ s \end{array} \right) \left(\begin{array}{c} m \\ s \end{array} \right) \frac{n_{\rm ex}^{n-s}}{(n_{\rm ex}+1)^{n+1}} \\ &\times \left(\frac{G}{n_{\rm ex}+1} \right)^{s} \left(1 - \frac{G}{n_{\rm ex}+1} \right)^{m-s}. \end{aligned} \tag{3.21}$$

For $N_{\rm amp} = 1$ this expression reduces to the ideal amplifier, equation 3.16. For an amplifier with $N_{\rm amp} > 1$ we do not have the condition $n \geq m$, and the excess amplifier can have *fewer* output photons than input photons. The addition of noise by an amplifier is physically acceptable. If the amplifier did not add noise then if would be possible to violate quantum mechanics by perfectly copying a state multiple times thus leading to perfect measurements and superluminal communication [68].

In the next section we explain how the method of placing an amplifier in front of a lossy detector can aid photodetection results.

3.2 Pre-amplification method

In this section we explain the setup of the pre-amplification method [60] and present the analytical expression we will use to quantify confidence in our measurement results.

In the previous Chapter, section 2.3, we described Linear Optical Quantum Computing (LOQC) and how it relies on postselection. This postselection is a crucial aspect of LOQC because it provides the non-linearities necessary for the gates that operate in an optical quantum computer. When we require a certain result from postselection we want to be as sure as possible that the result is exactly what we believe it to be. In probability terms we want the retrodictive conditional probability that we have the correct state in the measurement arm given we measured the correct state in our detection device to be close to unity.

However, in quantum computing gates, the signal that the gate has operated successfully is usually a few photocounts at most. Sometimes the trigger for a gate to operate can be a single photon, or none at all. Therefore loss in these systems can cause false positive results to occur, where by the action of the attenuator in removing photons projects some of the incorrect state to the correct state. This is where amplification can assist us in making more confident measurements. To overcome this effect of losing photons, we amplify the photon number states before they enter the photo-detector. As will be shown, this can improve our retrodictive conditional probability that the state we detected was indeed the correct state. Naturally this might be assumed to be of no benefit, as quantum mechanics says that we cannot decrease the overlap between two states that we are trying to distinguish. However this method appears to work under certain circumstances, which we will comment on later.

Our setup for detection is shown in fig. 3.1, where we have an amplifier followed by a lossy detector. The lossy detector is modelled by an attenuator followed by a perfect detector. Here, a perfect detector is one described by the set of POM elements, $\{\hat{\pi}_n = |n\rangle \langle n|\}$, which are orthogonal projective operators in the number state basis. The amplifier and attenuator are modeled as described in the previous section. As our detector can only measure photon number, we only need to describe the diagonal elements of the density matrix entering it, which in turn can be described by a classical probability

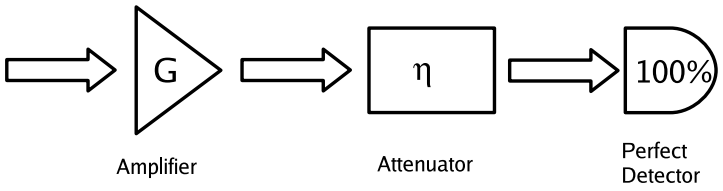


Figure 3.1: A model of the pre-amplification scheme: We have an amplifier followed by a lossy detector, which is modeled by an attenuator and a perfect detector.

distribution, which we label as $P(n)$. Following this, as we are only using phase-insensitive optical components (amplifier, attenuator) we only need to start with the input photon number probability distribution.

We have shown in the previous Chapter that this confidence in measurement results can be parametrized by the retrodictive conditional probability, $P^{\mathrm{r}}(c|c)$. This is the probability that we had the 'correct' state present in our device in the detector arm given we obtained the measurement outcome associated with the 'correct' state. In this chapter our desired, correct state is heralded by the detection of n photo-counts at the detector. Our measure of confidence is the retrodictive conditional probability that we had n photons as input to our detector given we obtained n photo-counts at our detector,

$$P^{\mathrm{r}}(n|n) = \frac{P^{\mathrm{p}}(n|n)P(n)}{\sum_m P^{\mathrm{p}}(n|m)P(m)}, \tag{3.22}$$

where $P^{\mathrm{p}}(n|m)$ is the predictive conditional probability that we detect n photo-counts given that m photons enter our detection setup and $P(m)$ is the *a priori* probability of m photons in the detector arm. We can obtain the factor $P^{\mathrm{p}}(m|n)$ as follows.

Upon amplification our initial photon number probability, $P(n)$, becomes,

$$P_{\mathrm{amp}}(k) = \sum_n P^{\mathrm{p}}_{\mathrm{amp}}(k|n)P(n), \tag{3.23}$$

which is then attenuated to become,

$$P_{\rm att}(m) = \sum_k P^{\rm p}_{\rm att}(m|k) P_{\rm amp}(k) = \sum_{k,n} P^{\rm p}_{\rm att}(m|k) P^{\rm p}_{\rm amp}(k|n) P(n), \qquad (3.24)$$

where $P^{\rm p}_{\rm att}(m|k)$ and $P^{\rm p}_{\rm amp}(k|n)$ are given by equations 3.7 and 3.21 respectively. We then detect the state with a perfect photo-detector. We will write the term,

$$\sum_k P^{\rm p}_{\rm att}(m|k) P^{\rm p}_{\rm amp}(k|n), \qquad (3.25)$$

simply as $P^{\rm p}(m|n)$, where the superscripts indicate that these are predictive conditional probabilities. This is the conditional probability that we will measure m photo-counts given we have n photons entering the detection setup. Equation 3.22 can now be written as,

$$P^{\rm r}(n|n) = \frac{\sum_k P_{\rm att}(n|k) P_{\rm amp}(k|n) P(n)}{\sum_m \sum_k P_{\rm att}(n|k) P_{\rm amp}(k|m) P(m)}. \qquad (3.26)$$

In the following sections we will look at two different initial photon number distributions to demonstrate when this method can improve results and then discuss conditions under which this scheme will help to distinguish different states.

3.3 Pre-amplification based on recording zero photocounts with a flat photon distribution

Output states from postselecting devices are particular to the specific device considered, as is the desired measurement result in the detector arm. When the undetected output is traced over this will provide a state in the detector arm with a specific *a priori* photon number distribution. Given that this distribution is required in order to calculate the retrodictive fidelity, particular

distributions will be assumed here. In this section we will examine a simple flat distribution, in which all photon numbers are *a priori* equally likely. We will also assume that the 'trigger' result for our postselection device is zero photo-counts. In reality a flat distribution is an infeasible distribution of photons but we choose it as it is simple to calculate and provides a worst case scenario where all photon numbers are equally likely.

We calculate the value $P^{\mathrm{r}}(0|0)$ using equation (3.26),

$$P^{\mathrm{r}}(0|0) = \frac{P^{\mathrm{p}}(0|0)P(n)}{\sum_m P^{\mathrm{p}}(0|m)P(m)} = \frac{\sum_k P_{\mathrm{att}}(0|k)P_{\mathrm{amp}}(k|0)}{\sum_m \sum_n P_{\mathrm{att}}(0|n)P_{\mathrm{amp}}(n|m)}, \tag{3.27}$$

where $P_{\mathrm{att}}(0|k)$ and $P_{\mathrm{amp}}(n|m)$ are given by equations 3.7 and 3.21 respectively. Explicitly these two are,

$$P_{\mathrm{att}}(0|k) = (1-\eta)^k, \tag{3.28}$$

$$P_{\mathrm{amp}}(k|0) = \frac{n_{\mathrm{ex}}^k}{(n_{\mathrm{ex}}+1)^{k+1}}, \tag{3.29}$$

and we repeat $P^{\mathrm{p}}_{\mathrm{amp}}(n|m)$ here for completeness,

$$\begin{aligned} P^{\mathrm{p}}_{\mathrm{amp}}(n|m) &= \sum_{s=0}^{min[n,m]} \left(\begin{array}{c} n \\ s \end{array} \right) \left(\begin{array}{c} m \\ s \end{array} \right) \frac{n_{\mathrm{ex}}^{n-s}}{(n_{\mathrm{ex}}+1)^{n+1}} \\ &\times \left(\frac{G}{n_{\mathrm{ex}}+1} \right)^s \left(1 - \frac{G}{n_{\mathrm{ex}}+1} \right)^{m-s}. \end{aligned} \tag{3.30}$$

When included in 3.27 we obtain,

$$P^{\mathrm{r}}(0|0) = \frac{\sum_n (1-\eta)^n \frac{n_{\mathrm{ex}}^n}{(n\mathrm{ex}+1)^{n+1}}}{\sum_m \sum_n (1-\eta)^n P^{\mathrm{p}}_{\mathrm{amp}}(n|m)}. \tag{3.31}$$

In figs. 3.2 - 3.7 we have plotted this expression for $P^{\mathrm{r}}(0|0)$ for various values of amplifier noise N_{amp}, amplifier gain G and detector efficiency η.

In fig. 3.2, equation 3.31 for $P^{\mathrm{r}}(0|0)$ is plotted with $N_{\mathrm{amp}} = 1$. This value represents an ideal amplifier, which is one that adds the minimum number

of noise photons, $(G-1)$, to the signal. We can see that the confidence in our measurement results is improved as we increase the amplifier gain when $\eta < 1$. We can also see that when we have a perfect detector, $\eta = 1$, we cannot improve results by using an amplifier. Fig. 3.3 is a two-dimensional slice of fig. 3.2 and shows the same conclusions.

In fig. 3.4 $P^{\mathrm{r}}(0|0)$ is plotted with $N_{\mathrm{amp}} = 2$. In this case we can see two different areas of the graph. When our detector loss, η, is less then 0.5 we see improvement in confidence and $P^{\mathrm{r}}(0|0)$ increases with amplifier gain. However, when $\eta > 0.5$ we now see that increasing amplifier gain causes $P^{\mathrm{r}}(0|0)$ to decrease. When $\eta = 0.5$ there is no change in $P^{\mathrm{r}}(0|0)$ with respect to amplifier gain. These conclusions are also shown in fig. 3.5, a two-dimensional graph using the same value of $N_{\mathrm{amp}} = 2$. From figs. 3.4 and 3.5 we can see that we can improve detection confidence even in the presence of excess noise, $N_{\mathrm{amp}} > 1$ but that this depends upon the level of detector efficiency.

Finally, in figs. 3.6 and 3.7 we have plotted $P^{\mathrm{r}}(0|0)$ with $N_{\mathrm{amp}} = 5$. Similar results are obtained, showing that amplification with excess noise can improve $P^{\mathrm{r}}(0|0)$ if detector efficiency is low enough.

We will now provide some analysis on this situation. The graph suggests that when our amplifier noise, N_{amp}, is less than the reciprocal of the detector loss, η^{-1}, we can improve our measurement confidence by including a noisy amplifier. This conclusion is reinforced when $P^{\mathrm{r}}(0|0)$ with no amplifier is compared to $P^{\mathrm{r}}(0|0)$ as amplifier gain tends to ∞. At $G = 1$ there is (effectively) no amplifier present and equation 3.30 simplifies to (with $n_{\mathrm{ex}} = N_{\mathrm{amp}}(G-1) = 0$),

$$\begin{aligned} P^{\mathrm{p}}_{\mathrm{amp}}(n|m) &= \sum_{s=0}^{min[n,m]} \left(\begin{array}{c} n \\ s \end{array} \right) \left(\begin{array}{c} m \\ s \end{array} \right) \frac{n_{\mathrm{ex}}^{n-s}}{(n_{\mathrm{ex}}+1)^{n+1}} \\ &\times \left(\frac{G}{n_{\mathrm{ex}}+1} \right)^{s} \left(1 - \frac{G}{n_{\mathrm{ex}}+1} \right)^{m-s} = \delta_{nm}, \end{aligned} \tag{3.32}$$

which means that the output distribution of the amplifier equals the input

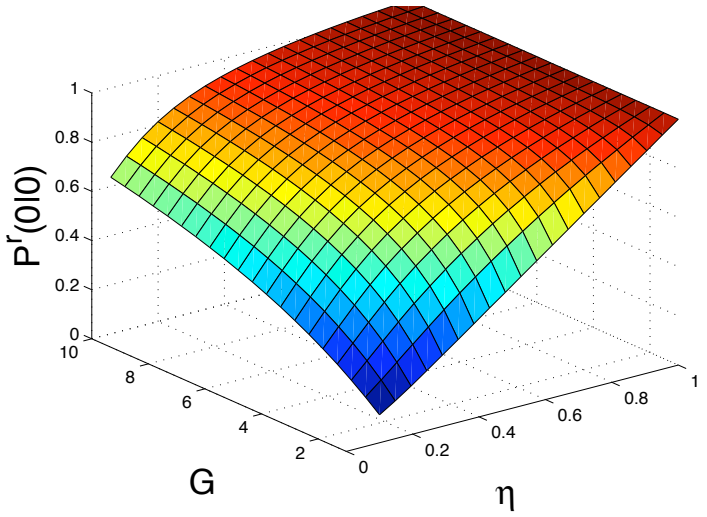


Figure 3.2: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$. It can be seen from the graph that $P^{\mathrm{r}}(0|0)$ always increases for any level of amplifier gain and non-unit efficiency detector.

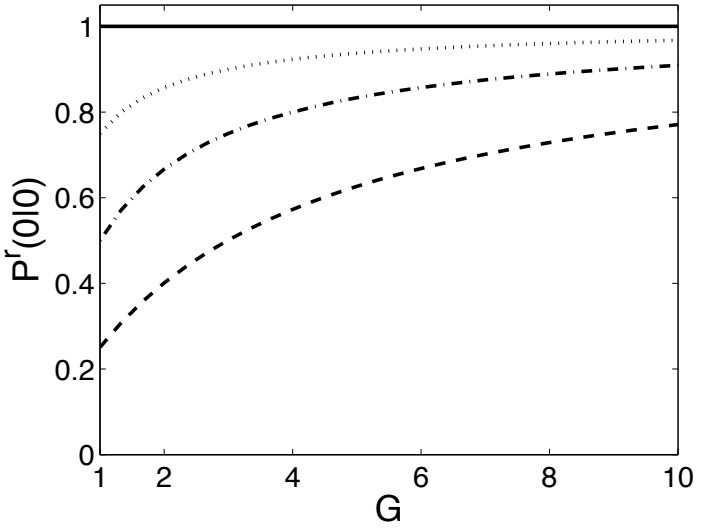


Figure 3.3: A two-dimensional slice of Figure 3.2 of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

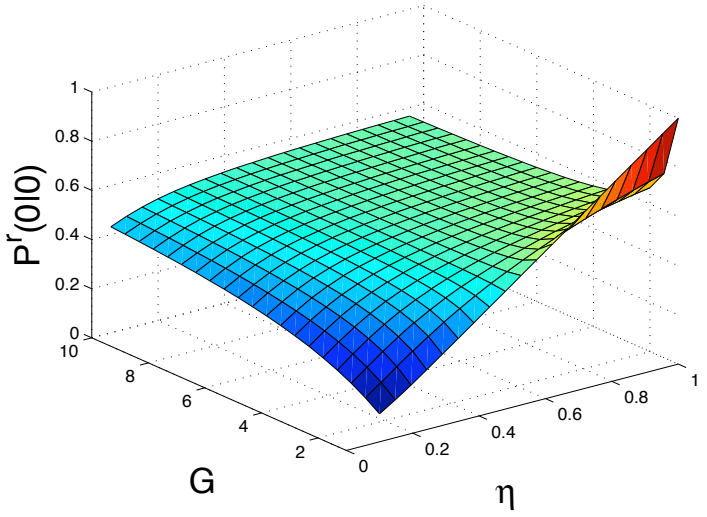


Figure 3.4: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$. The graph shows improvement in measurement confidence when $\eta < 1/2$ and a decrease in confidence when $\eta > 1/2$.

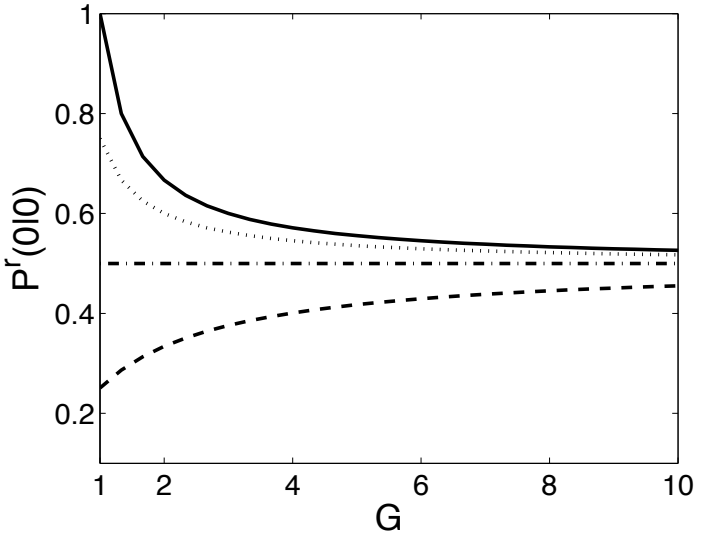


Figure 3.5: A two-dimensional slice of Figure (3.4) of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 2$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

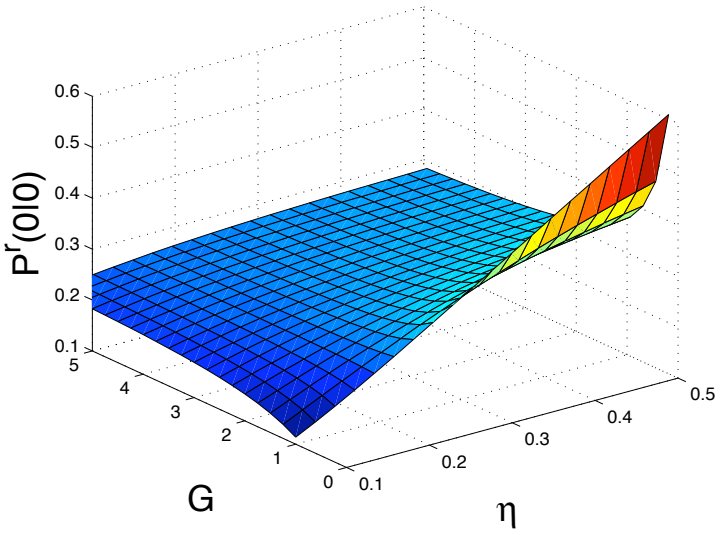


Figure 3.6: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 5$. The graph shows improvement in measurement confidence when $\eta < 1/5$ and a decrease in confidence when $\eta > 1/5$.

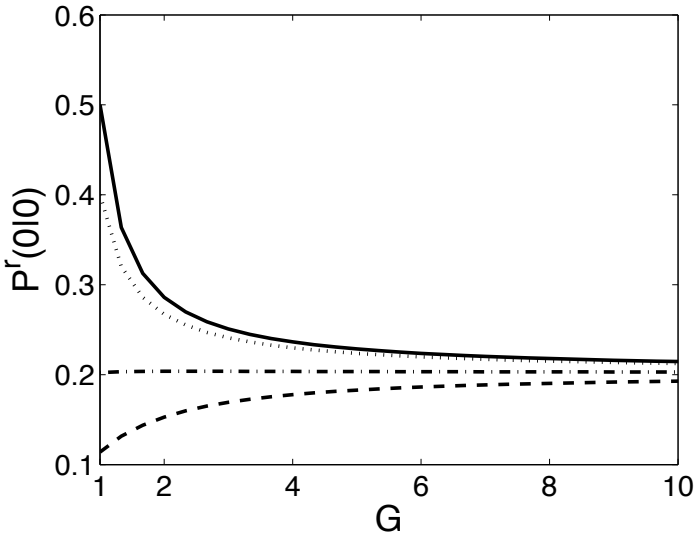


Figure 3.7: A two-dimensional slice of of $P^{\mathrm{r}}(0|0)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 5$ and the lines, from top to bottom, are η =0.5, 0.4, 0.2 and 0.1.

distribution. Our expression for $P^{\mathrm{r}}(0|0)$ at $G = 1$ is then,

$$P^{\mathrm{r}}(0|0)|_{G=1} = \frac{1}{\sum_n (1-\eta)^n} = \frac{1}{\frac{1}{1-(1-\eta)}} = \eta, \tag{3.33}$$

where we have used the sum of a geometric series. In the high gain limit ($G \to \infty$) we use the fact that all values of η tend to the same limit, and so choose $\eta = 1$ to use in equation 3.31, which gives,

$$\begin{aligned} P^{\mathrm{r}}(0|0) &= \frac{\sum_n \delta_{0n} \frac{n_{\mathrm{ex}}^n}{(n_{\mathrm{ex}}+1)^{n+1}}}{\sum_m \sum_n \delta_{0n} P^{\mathrm{p}}_{\mathrm{amp}}(n|m)} \\ = \frac{\frac{1}{n_{\mathrm{ex}}+1}}{\sum_m P^{\mathrm{p}}_{\mathrm{amp}}(0|m)} &= \frac{1}{\sum_m \left(1 - \frac{G}{n_{\mathrm{ex}}+1}\right)^m}, \end{aligned} \tag{3.34}$$

where the delta function comes from the term $(1-\eta)^n = 0^n = \delta_{0n}$. As $G \to \infty$, the summation in the denominator can be evaluated as,

$$\lim_{G\to\infty} \sum_m \left(1 - \frac{G}{n_{\mathrm{ex}}+1}\right)^m = \sum_m \left(1 - \frac{1}{N_{\mathrm{amp}}}\right)^m = N_{\mathrm{amp}}, \tag{3.35}$$

which is obtained using $n_{\mathrm{ex}} = N_{\mathrm{amp}}(G-1)$ and taking the sum of the geometric series. Thus,

$$\lim_{G\to\infty} P^{\mathrm{r}}(0|0) = N_{\mathrm{amp}}^{-1}. \tag{3.36}$$

It can be seen that if $P^{\mathrm{r}}(0|0)$ is greater in the high gain limit then at $G = 1$ i.e. when the condition,

$$\begin{aligned} \lim_{G\to\infty} P^{\mathrm{r}}(0|0) &> P^{\mathrm{r}}(0|0)|_{G=1} \\ N_{\mathrm{amp}}^{-1} &> \eta, \end{aligned}$$

is satisfied it is advantageous to use an amplifier. This comparison can be made due to $P^{\mathrm{r}}(0|0)$ being a monotonic function.

3.4 Pre-amplification based on recording zero photocounts with a Poisson photon distribution

In the previous section we described how the pre-amplification method will help to improve confidence in results when the *a priori* photon distribution was a uniform one. In this section we will describe similar results, but here we will be using a Poisson distribution,

$$P(n) = \frac{\lambda^n e^{-\lambda}}{n!}, \tag{3.37}$$

for the input photon number distribution. Coherent states, described in section 1.4.1, have photon number statistics with this distribution, where λ is the mean number of photons. The equation for $P^{\mathrm{r}}(0|0)$ is,

$$P^{\mathrm{r}}(0|0) = \frac{P^{\mathrm{p}}(0|0)P(0)}{\sum_n P^{\mathrm{p}}(0|n)P(n)} = \frac{P^{\mathrm{p}}(0|0)e^{-\lambda}}{\sum_n P^{\mathrm{p}}(0|n)\frac{e^{-\lambda}\lambda^n}{n!}}, \tag{3.38}$$

where $P^{\mathrm{p}}(0|n)$ is the same as given in equations 3.7, 3.21 and 3.25. Including these yields,

$$P^{\mathrm{r}}(0|0) = \frac{\sum_n (1-\eta)^n \frac{n_{\mathrm{ex}}^n}{(n_{\mathrm{ex}}+1)^{n+1}} e^{-\lambda}}{\sum_m \sum_n (1-\eta)^m P^{\mathrm{p}}_{\mathrm{amp}}(m|n)\frac{e^{-\lambda}\lambda^n}{n!}}. \tag{3.39}$$

Below we plot equation 3.39 in figs. 3.8 - 3.15 for $N_{\mathrm{amp}} = 1, 2$ and 5, the same values used in previous section, and for $\lambda = 0.1$ and 3. The first is a value of λ is one used for in various experimental cryptography schemes that require single photon sources to operate reasonably securely. The second value will be used as a comparison, as in this case the probability of zero photons is lower than higher numbers of photons, whereas in the first case $P(n)$ strictly decreases with photon number.

In fig. 3.8 $P^{\mathrm{r}}(0|0)$ from equation 3.39 is plotted against amplifier gain and

detector efficiency with $N_{\text{amp}} = 1$ and $\lambda = 0.1$. This is an ideal amplifier so we would expect to see improvement for all values of amplifier gain and all values of detector efficiency $\eta < 1$, as can be seen from the plot. We have a two-dimensional plot using the same parameter values in fig. 3.9.

Next, we plot $P^{\text{r}}(0|0)$ against amplifier gain and detector efficiency with $N_{\text{amp}} = 1$ and $\lambda = 3$. This is a distribution with zero photons less likely than any one of the higher photon numbers. These plots are shown in figs. 3.10 and 3.11. Finally we plot $P^{\text{r}}(0|0)$ with a $N_{\text{amp}} = 2$, for both values of $\lambda = 0.1,\ 3$ in figs. 3.14 and 3.15.

As can bee seen from the graphs, similar improvements in confidence are obtained for relatively good amplifiers (compared to the detectors) as were obtained for a uniform photon probability distribution.

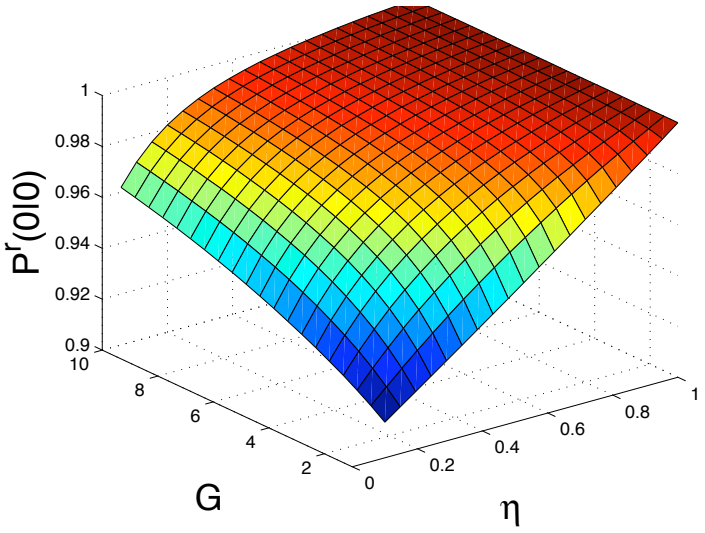


Figure 3.8: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 0.1$. This graph shows improvement for all lossy detectors and no change for a perfect detector.

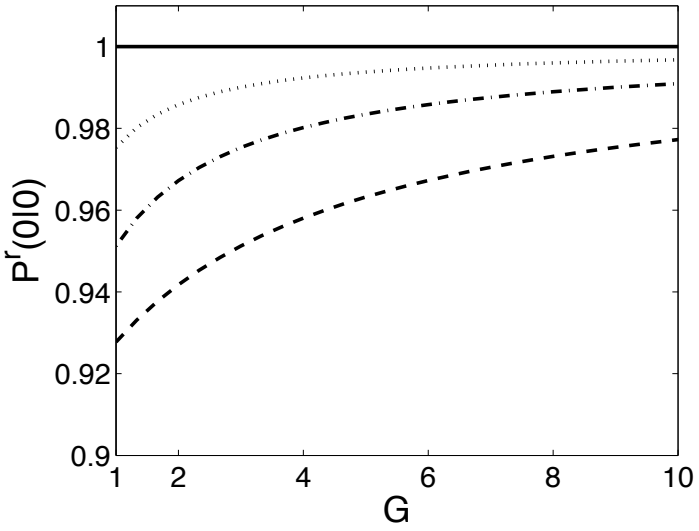


Figure 3.9: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 0.1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

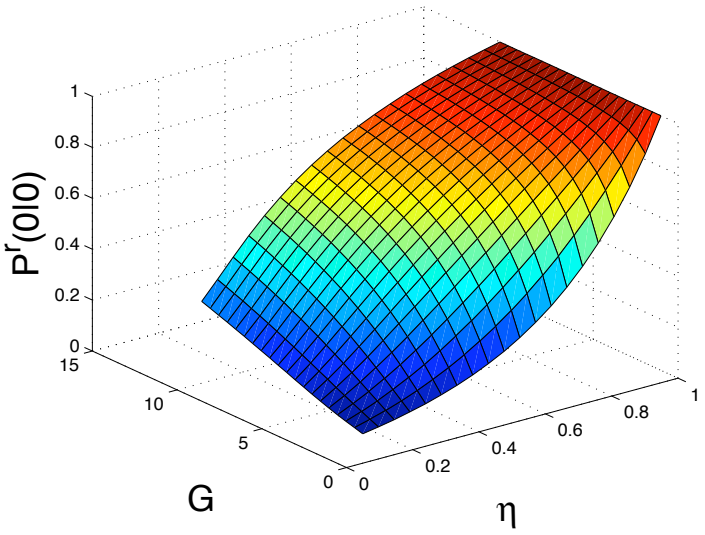


Figure 3.10: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 3$.

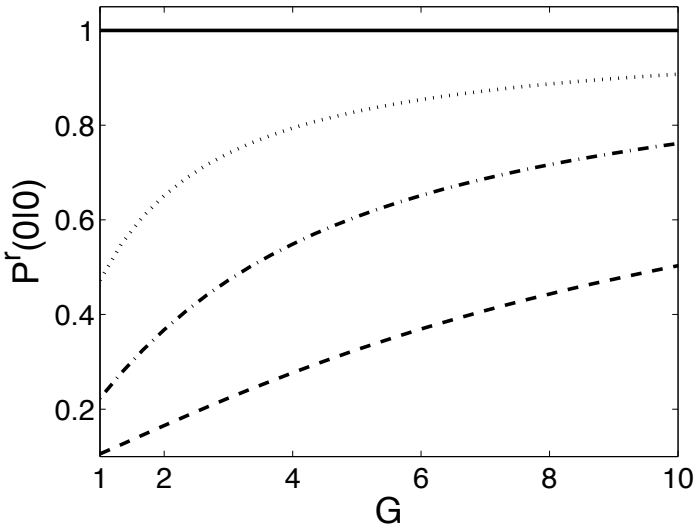


Figure 3.11: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ and $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

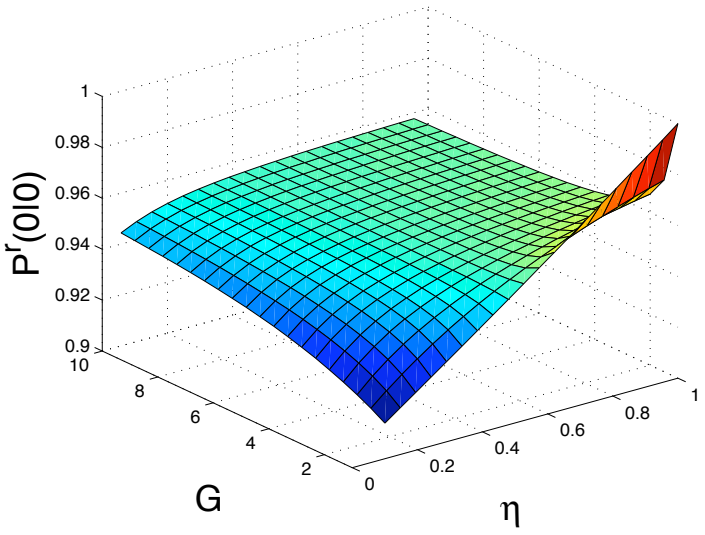


Figure 3.12: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ and $\lambda = 0.1$

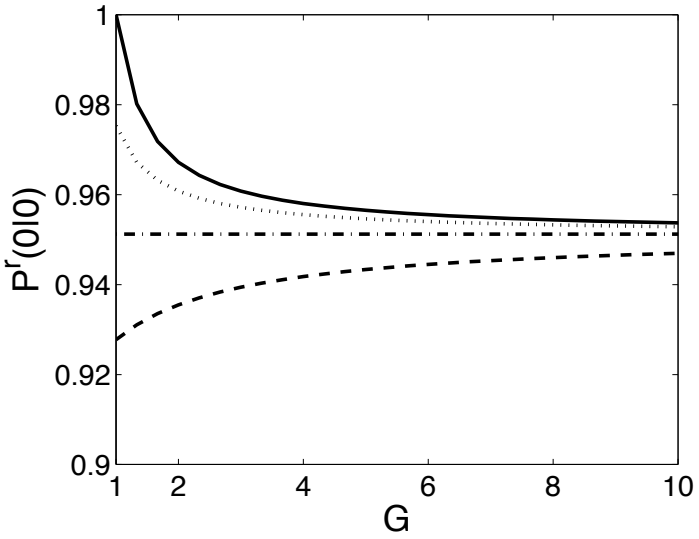


Figure 3.13: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$, $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

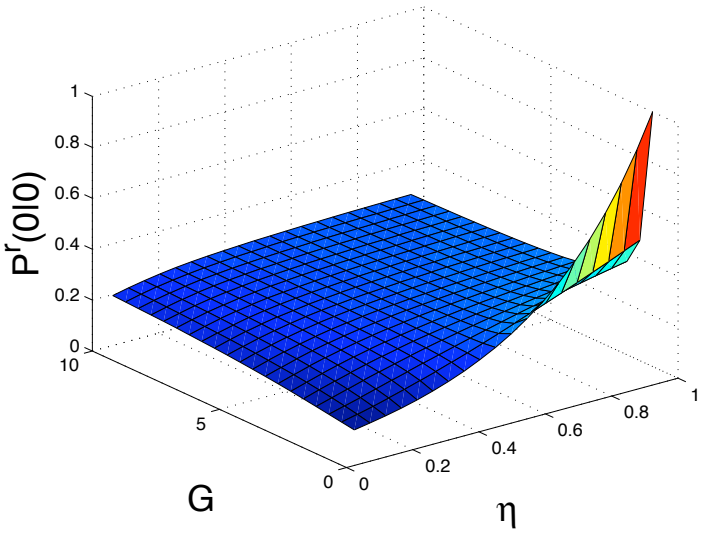


Figure 3.14: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ and $\lambda = 3$

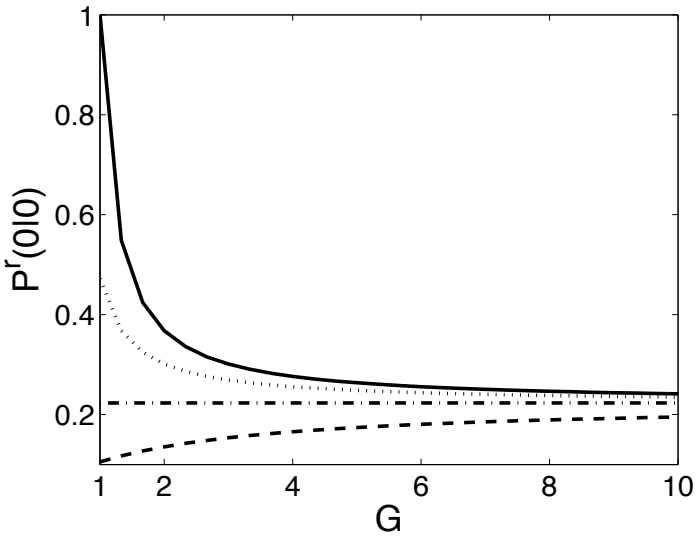


Figure 3.15: $P^{\mathrm{r}}(0|0)$ plotted against amplifier gain G with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$, $\lambda = 3$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

We again compare the the values of $P^{\mathrm{r}}(0|0)$ at $G = 1$ and as $G \to \infty$ with an *a priori* Poisson photon distribution to determine if we can derive suitable conditions under which we would use an amplifier. The value of $P^{\mathrm{r}}(0|0)$ at $G = 1$, no amplifier present, is given by,

$$\begin{aligned} P^{\mathrm{r}}(0|0)|_{G=1} &= \frac{e^{-\lambda}}{\sum_n (1-\eta)^n \frac{e^{-\lambda}\lambda^n}{n!}} = \frac{1}{\sum_n \frac{\lambda^n (1-\eta)^n}{n!}} \\ &= \exp[-\lambda(1-\eta)], \end{aligned} \tag{3.40}$$

where we have used equation 3.32. The value of $P^{\mathrm{r}}(0|0)$ as $G \to \infty$ can be obtained by setting $\eta = 1$ as before,

$$\begin{aligned} P^{\mathrm{r}}(0|0) &= \frac{\frac{1}{1+n_{\mathrm{ex}}} e^{-\lambda}}{\sum_m \frac{1}{n_{\mathrm{ex}}+1} \left(1 - \frac{G}{n_{\mathrm{ex}}+1}\right)^m \frac{e^{-\lambda}\lambda^m}{m!}} \\ &= \left(\sum_m \left(1 - \frac{G}{n_{\mathrm{ex}}+1}\right)^m \frac{\lambda^m}{m!} \right)^{-1} \end{aligned} \tag{3.41}$$

and then taking the limit,

$$\begin{aligned} \lim_{G\to\infty} P^{\mathrm{r}}(0|0) &= \left(\sum_m (1 - \frac{1}{N_{\mathrm{amp}}})^m \frac{\lambda^m}{m!} \right)^{-1} \\ &= \exp\left[-\lambda \left(1 - \frac{1}{N_{\mathrm{amp}}}\right) \right]. \end{aligned} \tag{3.42}$$

If we compare the two conditions 3.40 and 3.42 we arrive at the same conclusion as before for a flat distribution of input photons. For the amplifier to aid detection then the following condition must be satisfied,

$$N_{\mathrm{amp}} < \eta^{-1}. \tag{3.43}$$

3.5 Probability cost of pre-amplification

The downside to this method of aiding photo-detection is that the probability of detecting the correct event, zero photo-counts, decreases with increasing amplifier gain due to noise photons being added to this zero state component. This means that although we are more confident that we have the correct result when we obtain it, we will obtain it less often. This may not be a significant problem in secure communication schemes, where the key bit can always be re-sent but in quantum computation the waiting time for a correct event increasing may result in the destruction of the quantum coherence in the state.

The probability of detecting zero photo counts is given simply by,

$$P_{\text{out}}(0) = \sum_{m=0}^{\infty} P^{\text{p}}(0|m)P(m) \tag{3.44}$$

which is the denominator in $P^{\text{r}}(0|0)$. Below we plot it for various values of the parameters η and N_{amp}, and for a uniform *a priori* probability distribution and a Poisson distribution, with varying λ. We also rescale it by the probability of detecting zero photons in the ideal case, i.e. when we $\eta = 1$ and no amplifier, $G = 1$. In fig. 3.16 we have plotted $P(0)$ vs. amplifier gain for a uniform distribution with various values of N_{amp} and η. In fig. 3.17 we have plotted $P(0)$ vs. amplifier gain for a Poisson distribution, $\lambda = 0.1$, with various values of N_{amp} and η. In fig. 3.18 we have plotted $P(0)$ vs. amplifier gain for a Poisson distribution, $\lambda = 3$, with various values of N_{amp} and η.

We can see the costs of using this method to improve confidence in results and that they are similar for different values of N_{amp} when we have a flat distribution of photons but the costs vary when there is a Poissonian distribution of photons. We can compare these costs with another scheme which aims to improve confidence in photo-detection results. Branczyk *et. al.* [69] uses a homodyne detection scheme to test for a certain number of photons in a state. This has a higher cost, in terms of reduced probability of obtaining

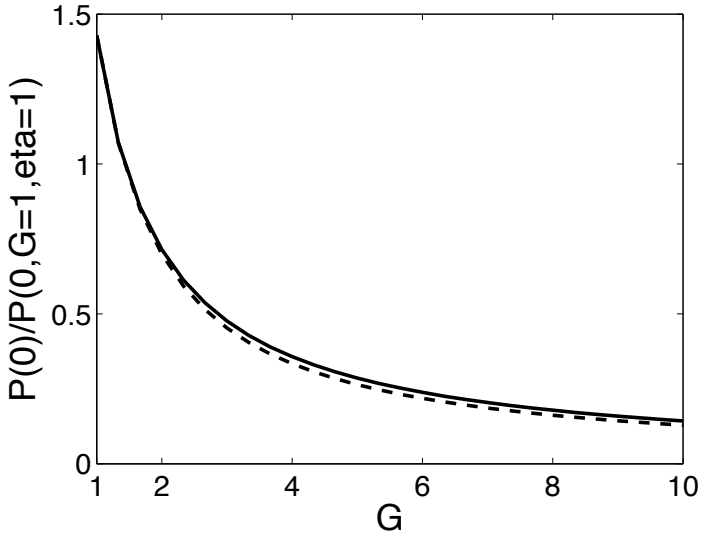


Figure 3.16: $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\text{amp}} = 1$ (full line) and $N_{\text{amp}} = 10$ (dashed line) with a uniform distribution of *a priori* input photons.

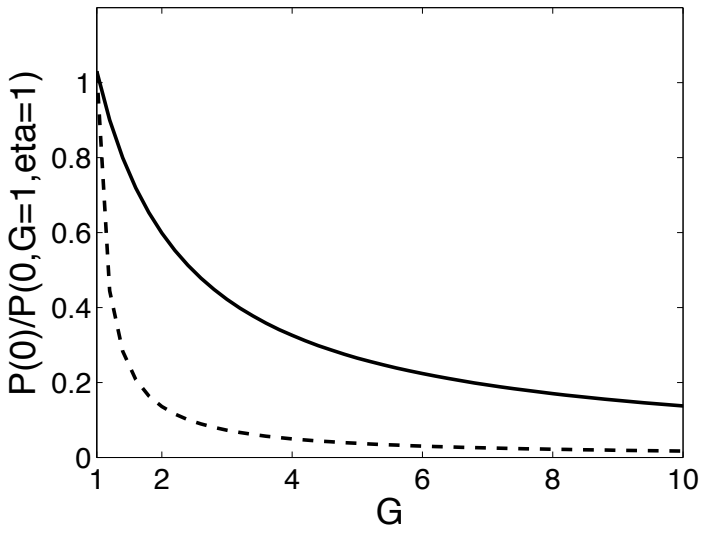


Figure 3.17: $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\text{amp}} = 1$ (full line) and $N_{\text{amp}} = 10$ (dashed line) with a Poisson distribution with $\lambda = 0.1$ of input photons.

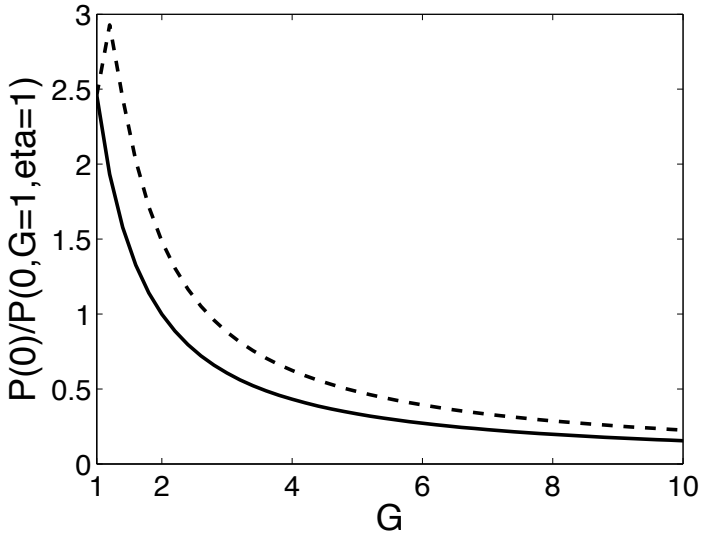


Figure 3.18: $P(0)/P(0, G = 1, \eta = 1)$ vs amplifier gain for $\eta = 0.7$ and $N_{\rm amp} = 1$ (full line) and $N_{\rm amp} = 10$ (dashed line) with a Poisson distribution with $\lambda = 3$ of input photons.

the 'trigger' state, than the scheme presented here but it can detect different photon number states.

3.6 Pre-amplification based on recording a single photocount

In the previous sections we examined the improved confidence in results of detecting zero photo-counts, and showed that in the presence of loss pre-amplification will improve results when $N_{\rm amp} < 1/\eta$. In this section we will analyse how results may be improved when a single photo-count is the trigger for our postselecting device when we have a flat distribution of photons.

Our measure of confidence is,

$$P^{\rm r}(1|1) = \frac{P^{\rm p}(1|1)P(1)}{\sum_n P^{\rm p}(1|n)P(n)} = \frac{P^{\rm p}(1|1)}{\sum_n P^{\rm p}(1|n)}. \tag{3.45}$$

Here, $P^{\rm p}(1|n)$ is given by,

$$P^{\rm p}(1|n) = \sum_{k=1} k\eta(1-\eta)^{k-1} P^{\rm p}_{\rm amp}(k|n), \tag{3.46}$$

and $P^{\rm p}_{\rm amp}(k|n)$ is given by equation 3.21. Results from this expression are plotted in figs. 3.19 - 3.22, using similar values of $N_{\rm amp}$ as was used in previous sections.

It can be seen from the graphs that improvements can be obtained for a flat probability distribution although the results are not as conclusive as before. The shape of the graph in figs. 3.19 and 3.20 is not as simple as before, and it is not easy to find a simple condition for how to improve confidence in results. We can however calculate the values of $P^{\rm r}(1|1)$ at $G = 1$ and as $G \to \infty$ and provide a rough guide for when to use a pre-amplifier. These two values of interest are,

$$\begin{aligned} P^{\rm r}(1|1)|_{G=1} &= \frac{\eta}{\sum_{n=1}^{\infty} n\,\eta\,(1-\eta)^{n-1}} \\ &= \left(\sum_{n=1}^{\infty} n(1-\eta)^{n-1}\right)^{-1} = \eta^2, \end{aligned} \tag{3.47}$$

where the final step is obtained by differentiating a geometric series and then summing. The second value is obtained by setting $\eta = 1$ in equation 3.45,

$$\begin{aligned} P^{\rm r}(1|1) &= \frac{\sum_{k=1} k0^{k-1} P^{\rm p}_{\rm amp}(k|1)}{\sum_n \sum_{k=1} k0^{k-1} P^{\rm p}_{\rm amp}(k|n)} \\ &= \frac{P^{\rm p}_{\rm amp}(1|1)}{\sum_n P^{\rm p}_{\rm amp}(1|n)} = \frac{P^{\rm p}_{\rm amp}(1|1)}{P^{\rm p}_{\rm amp}(1|0) + \sum_{n=1}^{\infty} P^{\rm p}_{\rm amp}(1|n)}, \end{aligned} \tag{3.48}$$

where,

$$\begin{aligned} P^{\rm p}_{\rm amp}(1|n) &= \sum_{s=0}^{min[n,1]} \left(\begin{array}{c} n \\ s \end{array} \right) \frac{n_{\rm ex}^{1-s}}{(n_{\rm ex}+1)^2} \\ &\times \left(\frac{G}{n_{\rm ex}+1}\right)^s \left(1 - \frac{G}{n_{\rm ex}+1}\right)^{n-s}. \end{aligned} \tag{3.49}$$

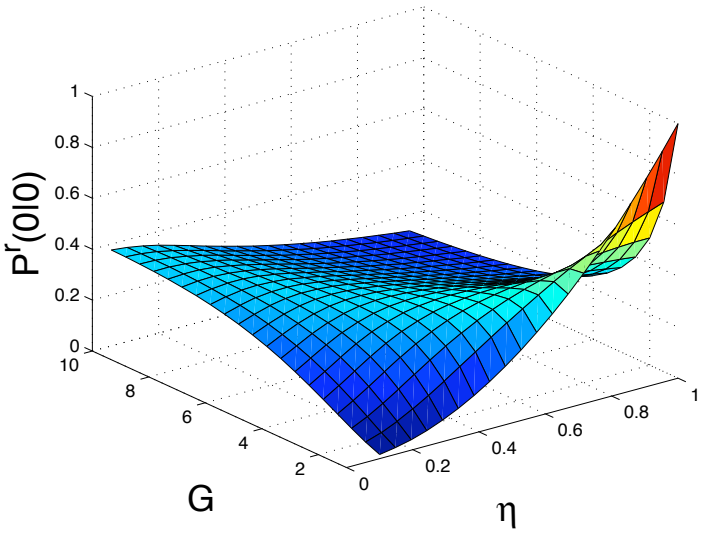


Figure 3.19: $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$.

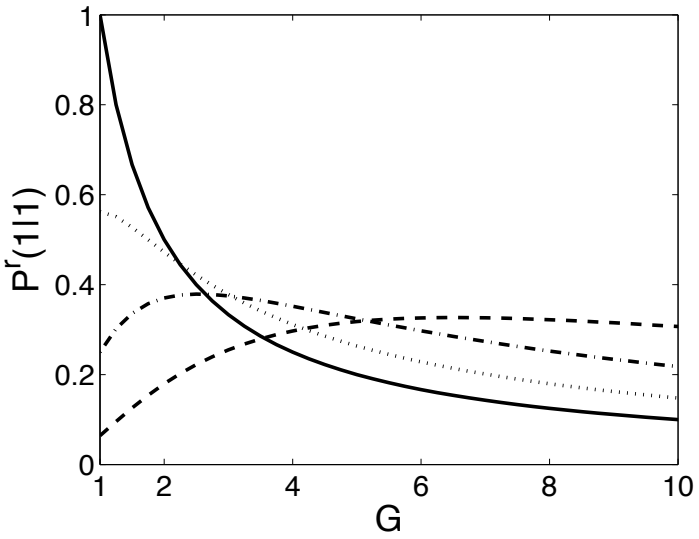


Figure 3.20: A two-dimensional slice of of $P^{\mathrm{r}}(1|1)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 1$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

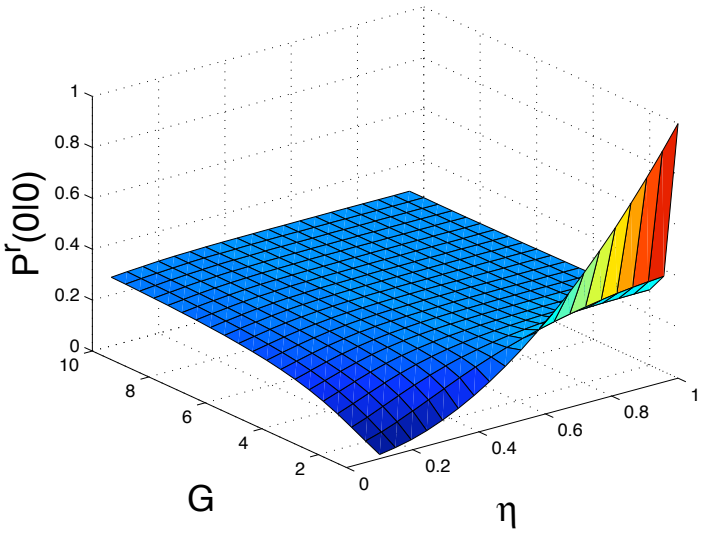


Figure 3.21: $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$.

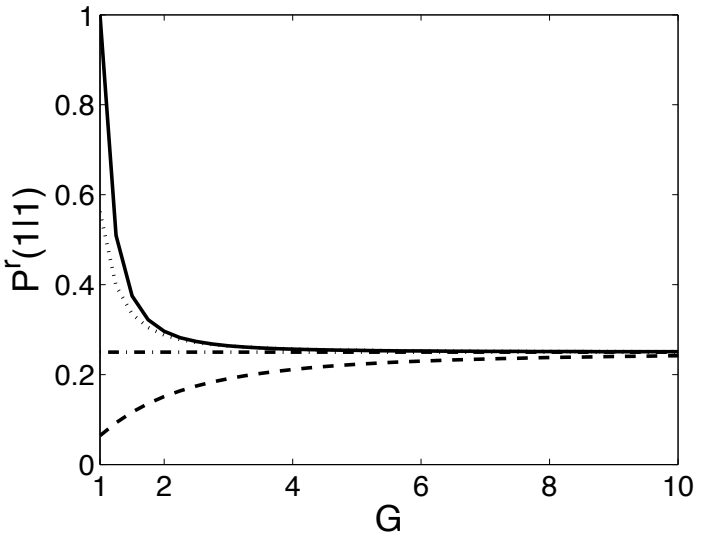


Figure 3.22: A two-dimensional slice of of $P^{\mathrm{r}}(1|1)$ vs. G, amplifier gain. The parameter values are $N_{\mathrm{amp}} = 2$ and the lines, from top to bottom, are η =1, 0.75, 0.5 and 0.25.

This gives,

$$P^{\mathrm{p}}_{\mathrm{amp}}(1|0) = \frac{n_{\mathrm{ex}}}{(n_{\mathrm{ex}}+1)^2}, \tag{3.50}$$

and for $n \geq 1$,

$$\begin{aligned} P^{\mathrm{p}}_{\mathrm{amp}}(1|n) &= \frac{n_{\mathrm{ex}}}{(n_{\mathrm{ex}}+1)^2}\left(1 - \frac{G}{n_{\mathrm{ex}}+1}\right) \\ &+ \frac{1}{(n_{\mathrm{ex}}+1)^2}\left(\frac{G}{n_{\mathrm{ex}}+1}\right). \end{aligned} \tag{3.51}$$

Using these terms 3.50 and 3.51 in equation 3.48 and then taking the limit $G \to \infty$ we find,

$$\lim_{g\to\infty} P^{\mathrm{r}}(1|1) = \frac{N_{\mathrm{amp}}-1}{N^2_{\mathrm{amp}}}. \tag{3.52}$$

Comparing 3.47 and 3.52 we find a the relation,

$$\eta < \frac{\sqrt{N_{\mathrm{amp}}-1}}{N_{\mathrm{amp}}} \tag{3.53}$$

for amplification to be better at high values of gain. However, as can be seen from fig. 3.19 and 3.20, amplification may not be useful for detecting single photocounts using intermediate values of amplifier gain.

3.7 Postselection based on recording a single photo-count when there is no vacuum component

An interesting addition to this method is when we want to detect a single photo-count and this is the lowest photon number present, i.e. $P(0) = 0$. This situation will arise in devices where photons may be created in down-conversion sources and have been heralded by the arrival of a another photon.

The expression for $P^{\mathrm{r}}(1|1)$ in this case is,

$$P^{\mathrm{r}}(1|1) = \frac{P^{\mathrm{p}}(1|1)P(1)}{\sum_{n=1} P^{\mathrm{p}}(1|n)P(n)}, \tag{3.54}$$

where,

$$P^{\mathrm{p}}(1|n) = \sum_{k=0}^{\infty} k\eta(1-\eta)^{k-1} P^{\mathrm{p}}_{\mathrm{amp}}(k|n), \tag{3.55}$$

and $P^{\mathrm{p}}_{\mathrm{amp}}(k|n)$ is given by equation 3.21.

Figs. 3.23 and 3.24 show $P^{\mathrm{r}}(1|1)$ vs amplifier gain for different values of N_{amp} and η. We can see that we get improvements similar to those in section 3.3 for the detection of no photocounts when the condition $N_{\mathrm{amp}} < \eta^{-1}$ is satisfied. This gives us an indication when the pre-amplification method helps improve photo-detection results.

3.8 Discussion

In this chapter we have shown that placing an amplifier before a lossy detector can improve confidence in measurement results. Here we try to shed some light on why this may occur.

In classical physics an amplifier is, ideally, a linear device that increases a signal by an amount proportional to the gain. Thus if we have two signals that we wish to distinguish, and some measure of distance D between them, then, in principle, a classical amplifier can increase this distance and can do so to infinity. Conversely, an attenuator would reduce that distance by a factor η whereas an amplifier would increase it by a factor G, thereby giving us an overall distance of $G\eta D$. In our quantum scheme we believe a similar effect occurs.

We start with a probability distribution of photons, which in the number basis will be perfectly distinguishable by a perfect detector. When we include the effects of attenuation we can view this in one of two ways, as suggested above. It can either be seen as mixing the measurement operators so they

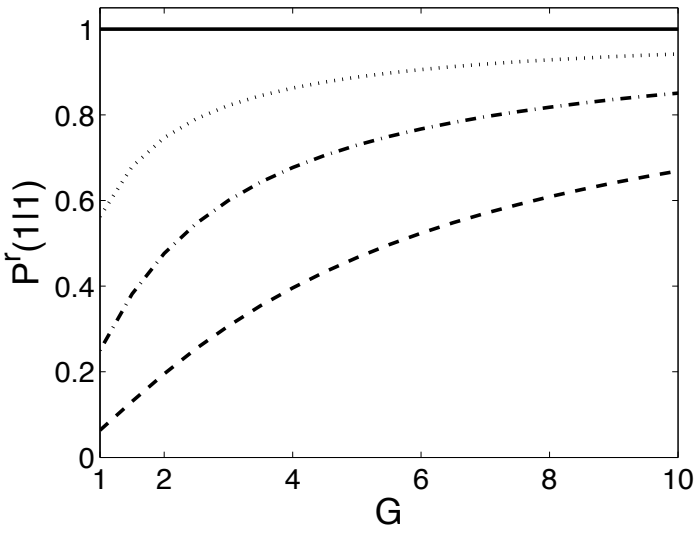


Figure 3.23: $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 1$ for a uniform distribution with no vacuum component. The lines are, from top to bottom, η=1, 0.75 0.5 and 0.25.

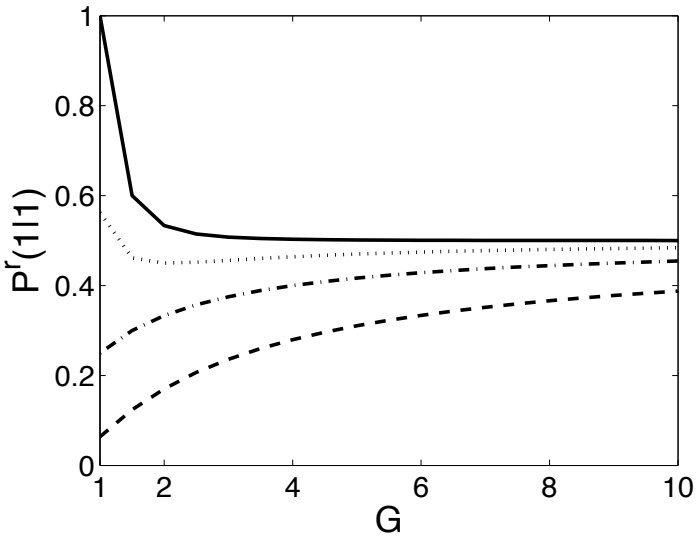


Figure 3.24: $P^{\mathrm{r}}(1|1)$ plotted against amplifier gain G and detector efficiency η with the amplifier noise parameter, $N_{\mathrm{amp}} = 2$ for a uniform distribution with no vacuum component. The lines are, from top to bottom, η=1, 0.75 0.5 and 0.25.

are no longer projection operators or as changing the density operator of the quantum state. We will use the latter explanation, as using an amplifier does not 'un-mix' the operators elements.

The attenuator causes some of the higher photon numbers to be projected into the lower photon number states i.e. it shifts the photon number distribution $P(n)$ closer to zero. We would therefore detect zero photo-counts more often and some of these would be wrong. By using an amplifier we amplify these higher photon states first, along with some of the zero photon state, so that when attenuated, the amplifier higher photon numbers of the initial distribution are less likely to give the lowest counts at the detector.

This works best when the desired number of photons to be detected is the lowest possible number present in the system, as has been shown in the previous sections. This is because for any intermediate photon number, as was demonstrated with a single photocount, we have additional ways of amplifying and then attenuating other photon numbers into that state, reducing our confidence in measurement results. Another reason for it working well for the lowest photon number is that the added noise photon will only cause us to reject the correct state. For intermediate photon numbers, noise photons can make us accept an incorrect state as correct.

Chapter 4

Analysis of quantum key distribution network

In this Chapter we will analyse how the coherent state comparison device introduced in section 2.6.2 can be used in a recently proposed Quantum Key Distribution (QKD) protocol. We can examine this as a postselecting device using the theory in Chapter 2 and we will examine imperfections in device components. We can also apply the theory of pre-amplification, from Chapter 3, to this device.

We start this chapter by giving some background to quantum cryptography then explaining the quantum key distribution network, which is based on linear optical elements and photodetectors. We then examine this network when there are imperfections in these device elements.

4.1 Quantum cryptography

Public key cryptography, the modern day approach to cryptography, relies on the difficulty of factoring large numbers for its security. The RSA protocol [31] uses public and private keys in order to send encoded messages between users. With the advent of quantum computation and Shor's algorithm for finding the factors of large primes this has lead to RSA public key systems

being vulnerable to attack.

The alternative to RSA is to use the one-time pad method (OTP), which is provably secure, although it has some difficulties in it's implementation. This is due to practical considerations in the secure creation, transmission and storage of the one-time pad's random key. Quantum communication could help with one of these concerns; classical communication would not allow for it to be securely transmitted but quantum communication, where states cannot be perfectly copied, could be used.

Quantum states are useful for cryptography and key distribution partly because quantum states cannot be copied [70, 71], unless the copier has very specific *a priori* information about the state that was sent. With classical communication an eavesdropper can intercept and read each bit in the key and then retransmit the original bit to the intended recipient. On the other hand, by using quantum states to transmit the key, measurements made by the eavesdropper may not tally with the sent state leading to an imperfect reproduction of the initial state. Furthermore the presence of an eavesdropper can be jointly detected by the sender and receiver; upon learning this both can then agree to start afresh with a new key.

In 1984 Bennett and Brassard [72] realized that by transmitting quantum states a secure key could be created between two parties. Their cryptographic scheme, known as BB84, uses non-orthogonal states to transmit a secure key between two parties by sending individual quantum states, which can represent the binary key bits 0 and 1, to another party, a secure key could be shared. This would then allow for a secure message to be sent using the one-time pad protocol. There have been various other protocols that use quantum states to transmit keys between parties [8, 73, 74, 59], with research showing them to be secure [75]. They have also been experimentally realised [76] and there are various multi-party key sharing protocols [77, 78].

In this chapter we examine the some of the experimental parameters of a scheme [57] for distribution of public keys using coherent states, introduced in section 1.4.1.

4.2 Quantum key distribution with coherent states

In a previous Chapter, section 2.6.2, we discussed a postselecting device that compares two coherent states to determine if they are identical or not. In this section we use this device in a QKD scheme suggested in [57]. In the scheme discussed here, there is one key sender and two key recipients, and the experimental setup is shown in fig. 4.1. The parts of the setup controlled by each recipient are enclosed by the dashed boxes. The protocol for sharing a key amongst three parties is as follows.

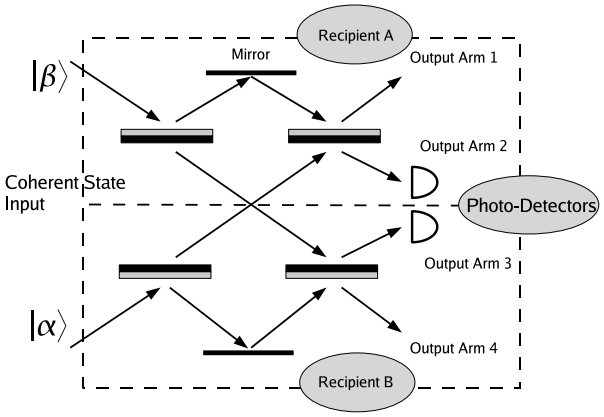


Figure 4.1: Quantum Key Distribution setup. If photons are detected in output arms 2 and/or 3 by the recipients, then the coherent states $|\alpha\rangle$ and $|\beta\rangle$ were necessarily different.

The experimental setup shown in fig. 4.1 achieves this. It consists of four 50/50 beam splitters, with a π phase change on reflection from the grey side. The π phase changes are a simple way to obtain the desired output state, although there are other ways to achieve this. For each recipient there is an output arm and a measurement arm with a photodetector. The output arms are labeled 1 to 4, with 1 and 2 belonging to recipient A and 3 and 4 belonging to recipient B.

The sender transmits two coherent key states, which should be identical, one to each recipient. The recipients direct their state onto a beamsplitter,

keeping one of the output modes for themselves and sending the other mode to the other recipient. Upon receiving this mode from their co-recipient, they then direct the two modes onto another beamsplitter. As the two modes should be coherent states, this part of the protocol is identical to the comparison test in the previous section. If the two initial coherent states transmitted by the sender were identical then the detector arm contains the vacuum state and if they were different then it contains a coherent state with finite amplitude.

4.2.1 Key states

The key states are selected from a predetermined finite set of coherent states. In the following analysis of the QKD protocol we will assume the the key states have equal amplitude and phases equally spaced around 2π. Fig. 4.2 shows two different sets of key states plotted in phase space where X and Y are the quadratures.

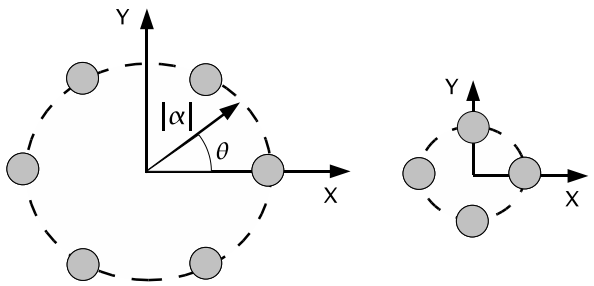


Figure 4.2: Quadrature plots of quantum key states. This figure shows two possible sets of key states.

In order to reduce the chance of a finite-amplitude coherent state being registered by the detector as vacuum, the amplitude of the state can be increased, as was mentioned in the previous section on coherent state comparison. However, by increasing the amplitude of the key states in this way means that the overlap between two states decreases i.e. they become more orthogonal and thus should be easier to distinguish. In turn however this

increases the accessible information of the states, I_{acc}, defined as,

$$I_{\text{acc}} \leq \chi(\hat{\rho}_{\text{key}}) = S(\hat{\rho}_{\text{key}}) - \sum_{j}^{N} p_j S(\hat{\rho}_j), \tag{4.1}$$

where $\hat{\rho}_j$ are the individual key states, p_j the probability of the jth state being sent,$\hat{\rho}_{\text{key}} = \sum_j^N p_j \hat{\rho}_n$ and $\chi(\hat{\rho})$ is the Holevo quantity [46]. For key states distributed as shown in fig. 4.2, i.e. $\hat{\rho}_j = \left||\alpha|e^{i\theta_j}\right\rangle$, as $|\alpha| \to \infty, \chi \to \log_2 N$, the classical limit, making it easier for eavesdroppers to gain information about the key state, as discussed in [57]. To combat this problem the number of key states in the set must be increased as this increases the overlap between the key states. Fig. 4.2 shows an example of two such sets of key states, with equal amplitude (within a set) and varying phases equally spaced around 2π.

4.2.2 Analysis of QKD scheme as a postselecting device

The scheme for quantum key distribution using coherent states will be analysed using the fidelity for correct output described in the previous section, as well as the pre-amplification method for improving detector results. We start by briefly explaining the scenario in distributing the quantum key between three parties [79].

The parties share knowledge of a set of two coherent states, $\{|\alpha\rangle, |-\alpha\rangle\}$, which they can use to form a secret key. The key sender sends one copy of the key state to each recipient who perform the splicing and re-sending of the key parts to the their co-recipient. If the initial state sent to each recipient is $|\alpha\rangle$ then the final output state across all four arms is,

$$\hat{\rho}_{1234} = |\alpha\rangle_1 \langle\alpha| \otimes |0\rangle_2 \langle 0| \otimes |0\rangle_3 \langle 0| \otimes |\alpha\rangle_4 \langle\alpha|. \tag{4.2}$$

As can be seen, when there are identical coherent states input into the device, the vacuum state is present in arms 2 and 3 and the state $|\alpha\rangle \langle\alpha|$ or $|-\alpha\rangle \langle -\alpha|$ is in arms 1 and 4. For a perfect system, the keys will be rejected for any

non-zero number of photocounts registered in either of the detectors. When the system is imperfect, whether or not results with photocounts in one or both of the detectors are accepted may depend on experimental parameters of the system and the level of security desired.

In the next section we examine the errors that could occur in the device and quantify their effect on the fidelity. Firstly we look at how losses in the device will affect the output state. In the subsequent section we describe an attempt to disrupt the key distribution by sending the incorrect key bits to each receiver and show how the detection element may ward against such activity.

4.3 Results

In this section we examine the operation of the postselector with imperfect components. Firstly the effects of photon loss and phase noise in the beam splitters will be included. Next, the effects of detector loss and the pre-amplification method to counteract it will be analyzed.

4.3.1 Lossy beamsplitters

Here we examine the effects of beamsplitter loss and phase noise in the model, assuming perfect detection. We also make the assumption in this section that the key sender transmits identical quantum key states to each recipient, modeling how these errors affect the operation of the device if all participants are honest. The state that is output at the beamsplitters will be a mixed state, which means that we are interested in calculating the Jozsa fidelity, equation 2.8, between the imperfect output state with the state created in an ideal case, equation 4.2.

When there are lossy beamsplitters in the setup then there is the chance that photons will be absorbed, along with the possibility of random phase noise in the system. This will lead to the device output state $\hat{\rho}_{1234}$ being corrupted, thereby reducing the fidelity. Each beam splitter has a loss factor

ϵ and the effective transformation for coherent states passing through a lossy beam splitter is obtained by making the substitutions $t \rightarrow \varepsilon t, r \rightarrow \varepsilon r$, $(|t|^2 + |r|^2 = |\varepsilon|^2, 0 < \varepsilon \leq 1)$, as shown in Ref. [80]. Assuming equal loss in all beam splitters, the new output state across all four arms is

$$\hat{\rho}_{1234} = \left|\varepsilon^2\alpha\right\rangle_1 \left\langle\varepsilon^2\alpha\right| \otimes \left|0\right\rangle_2 \left\langle 0\right| \otimes \left|0\right\rangle_3 \left\langle 0\right| \otimes \left|\varepsilon^2\alpha\right\rangle_4 \left\langle\varepsilon^2\alpha\right|$$

The fidelity, F_{J}, between this state and the ideal state in equation 4.2 is evaluated to be,

$$F_{\mathrm{J}} = \left(e^{-|\alpha|^2(1-\varepsilon^2)}\right)^2. \tag{4.3}$$

This is simply the overlap of two coherent states, then squared as we have two arms. This expression is plotted as a function of ε, as shown in fig. 4.3. We have plotted F_{J} for three different values of coherent state magnitude, $|\alpha|$=1, 2 and 5. It can be seen that the loss in the beam splitter affects a coherent state with a larger magnitude more than a state with a smaller magnitude.

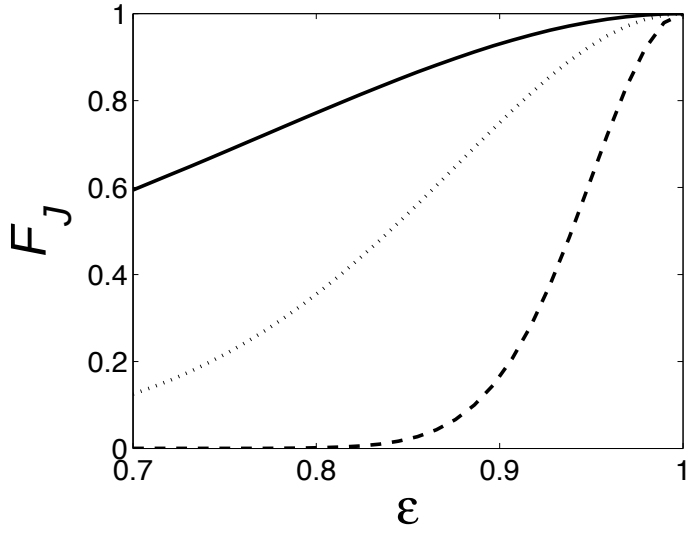


Figure 4.3: F_{J}, the fidelity between an ideal output state and the state in equation 4.3, for three different values of α. The solid line refers to $|\alpha| = 1$, the dotted line refers to $|\alpha| = 2$ and the dashed line refers to $|\alpha| = 5$.

As with any interferometer setup, the output state may be corrupted with phase noise. Here it is random phase noise that will be modelled, as experimentally constant phase shifts in the device can be accounted for. Phase noise in the internal arms will correspond to combined phase and amplitude noise in the output states. We consider two situations, the first in which the amplitude noise is minimal, and only phase noise is present in the output and the second in which both are included. We can include the effects of phase noise as a phase shift in the output coherent state, for example, the output in arm 1 will be,

$$\hat{\rho}_1 = \int d\theta_1 w_1(\theta_1) \left|\alpha e^{i\theta_1}\right\rangle_1 \left\langle \alpha e^{i\theta_1}\right| . \tag{4.4}$$

Here the phase shifts are modeled by rotating the ideal state, equation 4.2, by a random deviation θ_i and the $w(\theta_i)$ here are weighting functions that describe the probability of phase shifts in the device. We assume here that the phase noise is random and uncorrelated with noise in other arms for ease of calculation. For the w functions we choose a Gaussian distribution and a top-hat distribution. Both distributions will have a mean of zero and will be characterized by their width; the Gaussian will have a standard deviation of σ, $w(\theta, \sigma)$, and the top-hat will have a width B, $w(\theta, B)$. In fig. 4.4 is a plot of these two distributions for widths $B/2 = \sigma$.

For a Gaussian distribution of phase noise we have the following expression for the fidelity in arm 1,

$$\begin{aligned} F_{\mathrm{J}} &= \mathrm{Tr}\left[\int_{-\infty}^{\infty} d\theta_1 w_1(\theta_1, \sigma) \left|\alpha e^{i\theta_1}\right\rangle_1 \left\langle \alpha e^{i\theta_1}\right| \alpha\rangle\langle\alpha|\right] \\ &= \int_{-\infty}^{\infty} d\theta_1 \frac{e^{\frac{-\theta_1^2}{2\sigma^2}}}{\sqrt{2\pi\sigma^2}} e^{-|\alpha-\alpha e^{i\theta_1}|^2}, \end{aligned} \tag{4.5}$$

and when we have a top-hat distribution of phase noise our expression for

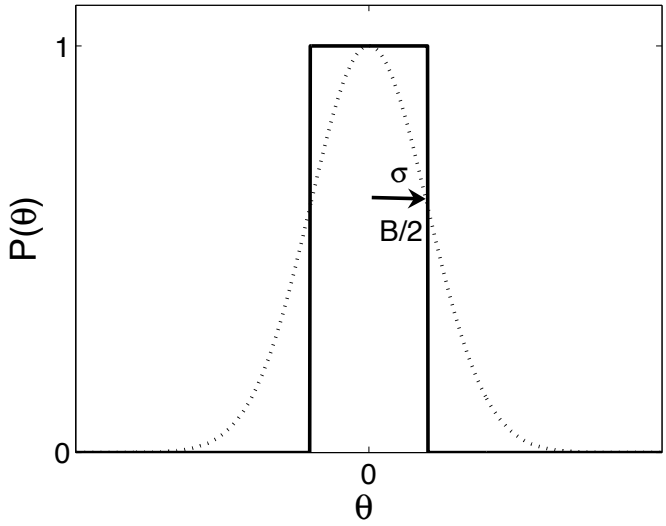


Figure 4.4: A plot of the Gaussian distribution (dotted line) and the top-hat distribution (full line), with $\sigma = B/2$.

fidelity is,

$$\begin{aligned} F_{\mathrm{J}} &= \mathrm{Tr}\left[\int_{-B/2}^{B/2} d\theta_1 w_1(\theta_1, B) \left|\alpha e^{i\theta_1}\right\rangle_1 \left\langle \alpha e^{i\theta_1}\right| \alpha\rangle\langle\alpha|\right] \\ &= \int_{-B/2}^{B/2} d\theta_1 \frac{1}{B} e^{-|\alpha-\alpha e^{i\theta_1}|^2}. \end{aligned} \tag{4.6}$$

We have plotted these fidelities in fig. 4.5, which shows that the Gaussian noise distribution has a much lower fidelity than the flat distribution. This is due to the Gaussian's large tails that contribute to lowering the fidelity further.

Next, we model the amplitude and phase noise together by adding a deviation term, δ_i, to the coherent state in each output arm. This gives the output state across all four arms as

$$\begin{aligned} \hat{\rho}_{1234} &= \int d^2\delta_1 w_1(\delta_1) \left|\alpha+\delta_1\right\rangle_1 \left\langle \alpha+\delta_1\right| \otimes \int d^2\delta_2 w_2(\delta_2) \left|0+\delta_2\right\rangle_2 \left\langle 0+\delta_2\right| \\ &\otimes \int d^2\delta_3 w_3(\delta_3) \left|0+\delta_3\right\rangle_3 \left\langle 0+\delta_3\right| \otimes \int d^2\delta_4 w_4(\delta_4) \left|\alpha+\delta_4\right\rangle_4 \left\langle \alpha+\delta_4\right|. \end{aligned} \tag{4.7}$$

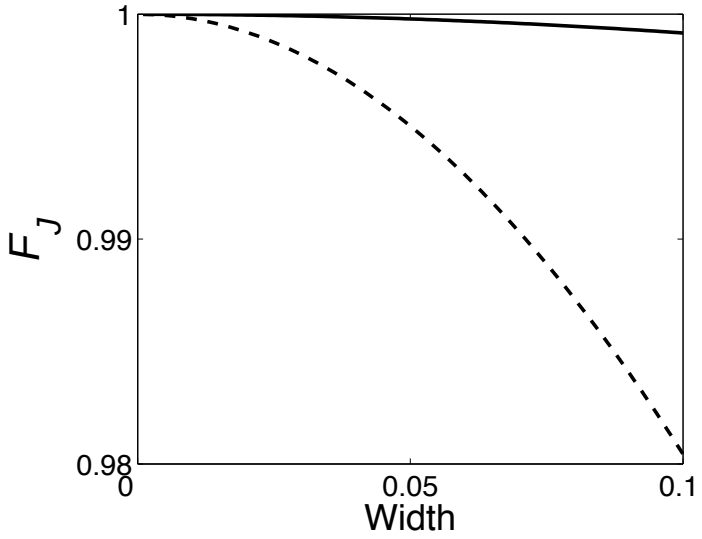


Figure 4.5: F_{J} with a Gaussian deviation equation 4.5, dashed line, and with a flat distribution equation 4.6, full line, plotted as a function of width. Here width corresponds to the Gaussian's standard deviation, σ, or the top-hat distribution's bandwidth halved, $B/2$.

Here we are integrating over the complex plane and for simplicity we chose the weighting functions, $w(\delta_i)$, to be complex Gaussian functions. The fidelity between the imperfect state in a single arm, i.e. arm 1, and the ideal state is

$$F_{\mathrm{J}} = \mathrm{Tr}\left[\int d^2\delta_1 w_1(\delta_1)\left|\alpha+\delta_1\right\rangle_1\left\langle\alpha+\delta_1\right|\left\langle\alpha\right\rangle\left\langle\alpha\right|\right] = \int d^2\delta_1 \frac{e^{\frac{-|\delta_1|^2}{\sigma^2}}}{\pi\sigma^2} e^{-|\delta_1|^2}, \tag{4.8}$$

which has a simple analytic expression,

$$F_{\mathrm{J}} = \frac{1}{\sigma^2+1}, \tag{4.9}$$

and is plotted in fig. 4.6 as a function of σ.

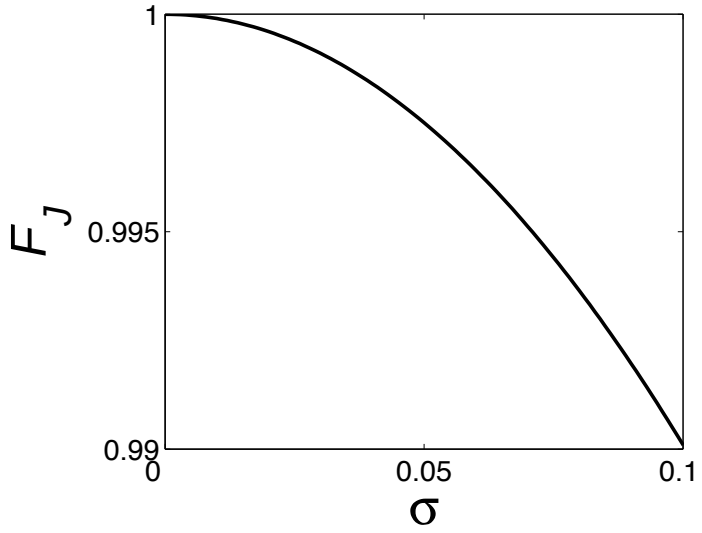


Figure 4.6: F, the fidelity given by Eq. (4.9), with both amplitude and phase noise present, plotted as a function of σ.

4.3.2 Imperfect detection: lossy detection and noisy amplification

Here we examine the effects of imperfect detection in the QKD protocol. The detection performed by the recipients provides some security against them receiving different key states, either corrupted from an eavesdropper or the initial sender of the states cheating by sending different states. If different key states are sent then there may be photons in the each recipients detector arms. If they have lossy photodetectors however, they will fail to measure these photocounts and accept incorrect key states as being correct. This lossy detection may be improved by the use of pre-amplification, as explained in Chapter 3, and here we apply it to the QKD protocol.

In our following analysis we assume that the sender may cheat by transmitting different key states to each recipient, where the set of key states is $\{|\alpha\rangle, |-\alpha\rangle\}$. She can decide to do this with some probability P_{cheat}, a number which is unknown to the recipients, but which will affect the *a priori* photon probability distribution in the detector arm. Unless the recipients

believe that P_{cheat} is zero or one, in which case they accept or discard what was sent to them, they need to make an assumption. In further analysis we assume that $P_{cheat} = 0.5$. When identical coherent states are sent to the recipients, then the state in both detector outputs is the vacuum state, $|0\rangle\langle 0|$, and when different coherent states are sent then the output state is a mixture of coherent states $|\pm\alpha\rangle\langle\pm\alpha|$. The *a priori* state in the detector arm is,

$$\begin{aligned}\hat{\rho} &= (1 - P_{cheat})\,|0\rangle\langle 0| + P_{cheat}\frac{1}{2}\left[|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle -\alpha|\right] \\ &= (1 - P_{cheat})\hat{\rho}_0 + P_{cheat}\hat{\rho}_i, \end{aligned} \tag{4.10}$$

where the second, cheating term, is obtaining by sending various combinations of the states $|\alpha\rangle$ and $-|\alpha\rangle$ to the two different recipients. To measure how well the recipients can determine the state in the detector arm we will use the retrodictive conditional probability that zero photons were present given we measured zero photocounts, $P^{\mathrm{r}}(0|0)$. We used this in the previous chapter, Chapter 3, where the amplifier/attenuator modified the photon number distribution. Here, we choose to use the alternative, though equivalent, method of letting the amplifier/attenuator modify the measurement operators, as discussed in section 2.5.1.

We first need the measurement operator that describes detecting zero photocounts from the amplifier-lossy detector setup, $\hat{\pi}'_0$. (Note that for a perfect detector setup $\pi_0 = |0\rangle\langle 0|$, a projective operator). Using the theory from Chapter 2, section 2.5.1, and Chapter 3, section 3.1, we find,

$$\hat{\pi}'_0 = \sum_{n}^{\infty}\sum_{s}^{\infty} P^{\mathrm{p}}_{\mathrm{att}}(0|s)P^{\mathrm{p}}_{\mathrm{amp}}(s|n)\hat{\pi}_n \tag{4.11}$$

Where $P^{\mathrm{p}}_{\mathrm{att}}(0|s)$ is the predictive conditional probability that 's' photons are attenuated to 0 photons and $P^{\mathrm{p}}_{\mathrm{amp}}(s|n)$ is the predictive conditional probability that 'n' photons are amplified to 's' photons. $\hat{\pi}_n$ is the photon number projector for 'n' photons and can be seen as a perfect measurement. $P^{\mathrm{p}}_{\mathrm{att}}(0|s)$ and $P^{\mathrm{p}}_{\mathrm{amp}}(s|n)$ can be combined to form $P^{\mathrm{p}}(0|n)$, which, if we write in the

explicit forms for the conditional probabilities from sections 3.1.1 and 3.1.3 is,

$$\begin{aligned} P^{\mathrm{p}}(0|n) &= \sum_{n=0}^{\infty}(1-\eta)^s \sum_{m=0}^{\min[n,s]} \left(\begin{array}{c} n \\ m \end{array} \right) \left(\begin{array}{c} s \\ m \end{array} \right) \\ &\times \frac{n_{ex}^{s-m}}{(1+n_{ex})^{s+1}} \left(\frac{G}{1+n_{ex}} \right)^m \left(1 - \frac{G}{1+n_{ex}} \right)^{n-m} \end{aligned} \tag{4.12}$$

where n_{ex} is the excess noise added by the amplifier, $n_{ex} = N_{amp}(G-1)$ and G is the amplifier gain. We assume that the state in the detector arm is given by equation (4.10). The expression for $P^{\mathrm{r}}(0|0)$ is then derived as,

$$P^{\mathrm{r}}(0|0) = \frac{\mathrm{Tr}[\hat{\rho}_0 \hat{\pi}_0']}{\mathrm{Tr}[\hat{\rho}\, \hat{\pi}_0']} = \frac{P^{\mathrm{p}}(0|0)P(0)}{\sum_n P^{\mathrm{p}}(0|n)P(n)}, \tag{4.13}$$

where $P(n)$ is the probability for n photons for the state given by equation (4.10), which is,

$$P(n) = (1-P_{cheat})\delta_{n0} + P_{cheat} e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} = \frac{1}{2}\left(\delta_{n0} + e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \right) \ . \tag{4.14}$$

Note that this is the same photon number distribution as in section 2.6.2. Using (4.12) and (4.14) we find an expression for $P^{\mathrm{r}}(0|0)$ as,

$$\begin{aligned} P^{\mathrm{r}}(0|0) &= \frac{P^{\mathrm{p}}(0|0)P(0)}{P^{\mathrm{p}}(0|0)p_0 + \sum_{n=1} P^{\mathrm{p}}(0|n)P(n)} \\ &= \frac{1+e^{-|\alpha|^2}}{1+e^{-|\alpha|^2} + (1+\eta\, n_{ex}) \sum_{n=1}^{\infty} P^{\mathrm{p}}(0|n) e^{-|\alpha|^2} \frac{|\alpha|^2}{n!}} , \end{aligned} \tag{4.15}$$

where we have evaluated $P^{\mathrm{p}}(0|0)$ to be,

$$\begin{aligned} P^{\mathrm{p}}(0|0) &= \sum_{n}^{\infty}(1-\eta)^n \frac{n_{ex}^n}{(1+n_{ex})^{n+1}} = \frac{1}{1+n_{\mathrm{ex}}} \sum_{n}^{\infty} \left(\frac{(1-\eta)n_{\mathrm{ex}}}{1+n_{\mathrm{ex}}} \right)^n \\ &= (1+\eta n_{\mathrm{ex}})^{-1}, \end{aligned} \tag{4.16}$$

using the fact that this geometric sum converges to a finite value.

We have plotted this expression in figs. 4.7 and 4.8 for various different values of variables $N_{\rm amp}$ and η. The graphs suggests that when our amplifier noise, $N_{\rm amp}$, is greater than the reciprocal of the detector loss, η^{-1}, then we do not increase our measurement confidence by including the noisy amplifier, as before. This is reinforced when $P^{\rm r}(0|0)$ with an amplifier gain equal to unity is compared to $P^{\rm r}(0|0)$ as amplifier gain tends to ∞. At $G = 1$,

$$P^{\rm r}(0|0) = \frac{1 + e^{-|\alpha|^2}}{1 + e^{-\eta|\alpha|^2}}, \tag{4.17}$$

and in the high gain limit,

$$\lim_{G\to\infty} P^{\rm r}(0|0) = \frac{1 + e^{-|\alpha|^2}}{1 + e^{-\frac{|\alpha|^2}{N_{amp}}}}. \tag{4.18}$$

It can be seen that if the denominator is greater in the case $G = 1$ than in the high gain limit then $P^{\rm r}(0|0)$ will be increased by using an amplifier, i.e. when the condition

$$\begin{aligned} 1 + e^{-\eta|\alpha|^2} &> 1 + e^{-\frac{|\alpha|^2}{N_{\rm amp}}} \\ \rightarrow \eta &> 1/N_{\rm amp} \end{aligned}$$

is satisfied it is advantageous to use an amplifier. The high gain limit of $P^{\rm r}(0|0)$ can be seen from fig. 4.7. The horizontal line is $P^{\rm r}(0|0)$ with $\eta = N_{\rm amp}^{-1}$. For values of $\eta < 1/3$, $P^{\rm r}(0|0)$ always increases with increasing G but for $\eta > 1/3$, $P^{\rm r}(0|0)$ decreases and an amplifier does not help. Note that in the QKD scheme there are two detectors, so the factor $P^{\rm r}(0|0)$ will appear twice in the overall device fidelity.

4.4 Conclusions

In this section we have analysed a quantum key distribution device that utilises coherent states as the key bits. The key states are shared between

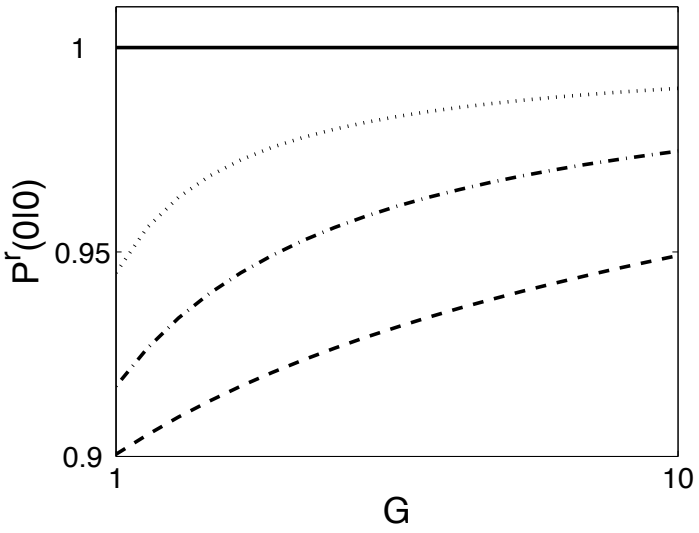


Figure 4.7: $P^{\mathrm{r}}(0|0)$ from equation 4.15 for different values of η, from top to bottom, 1, 0.5, 1/3 ($= N_{amp}^{-1}$), 0.25 and 0.1. Here $N_{amp} = 1$ and $|\alpha| = 0.5$.

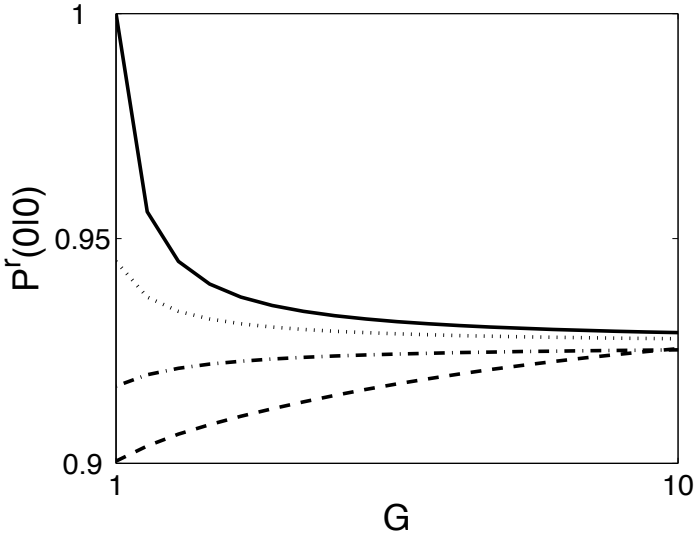


Figure 4.8: $P^{\mathrm{r}}(0|0)$ from equation 4.15 for different values of η, from top to bottom, 1, 0.5, 1/3 ($= N_{amp}^{-1}$), 0.25 and 0.1. Here $N_{amp} = 3$ and $|\alpha| = 0.5$.

two recipients, who, using beamsplitters, interfere these key states with one another in order to test for differences between them.

Using the theory laid out in Chapter 2, we calculate the two factors that comprise the fidelity of correct output derived in that chapter. The first factor only depends on the output state of the device and therefore on the properties of the components of the device. We examine the effects of lossy beamsplitters that also add in phase noise to the quantum states.

The second factor depends on the properties of the detector arm, such a quantum efficiency of the detector. Using the pre-amplification method described in Chapter 3, we show that using an amplifier before a lossy detector can improve confidence in detection results when the noise in the amplifier, N_{amp}, is less that the reciprocal of the detector loss, η^{-1}.

These two factors would give parties a means to improve the overall operation of the device.

Different values of $|\alpha|$ were not considered here. This is because by changing $|\alpha|$ we would also have to alter the number of key bits used in the protocol, which in turn would lead to a more complicated output state in our detector arms.

Chapter 5

Measurement master equation

In this Chapter we examine a quantum system that is monitored in time by measurements performed upon it, thus acquiring information about the quantum state. Such a system does not evolve unitarily and instead can be thought of as evolving under what has been called a measurement master equation. We first derive the measurement master equation used in the rest of the chapter. Next we analyse the equation using two different sets of measurement operators: a discrete, orthogonal set and then a continuous, non-orthogonal set of measurement operators. In both cases we solve the equation analytically and model the equation computationally to compare the results.

5.1 Measurement master equation

In this section we explain the derivation of the measurement master equation, as done in [81]. The physical premise for this evolution is that a quantum system is continually being measured, either by an observer or, in the case of quantum Brownian motion, by an environment. The latter case has been studied [82, 83] and provides a method to find the correct evolution of Brownian motion when compared to other methods which have un-physical effects, such as heating of the system and negative probabilities of states.

Master equations that describe the effect of measurements have been studied previously by Caves and Milburn [84] where they described measurements by coupling a probe to the system being measured through a Hamiltonian and then measuring the probe. Other equations of this type have been studied by Scott and Milburn [85].

In [81] the authors assume that the quantum state undergoes a series of measurements at a rate R, which are instantaneous in time, and between measurements the evolution is unitary under a Hamiltonian. The measurements are described by a set of Kraus operators $\{\hat{A}_i\}$ [10]. These form a Positive Operator Measure, $\hat{\pi}_i = \hat{A}_i^\dagger \hat{A}_i$, that satisfies the usual constraints of completeness and positivity (see section 1.2). Time is discretized into intervals of identical length Δt, which is short enough so that the only possible number of measurements that can occur are zero or one. The probability of a measurement occurring in an interval is then $R\Delta t$ and the probability of no measurement occurring is $1 - R\Delta t$. There are then two possible evolutions for the density operator within an interval. When no measurements occur within a time interval there is only unitary evolution and the state at the end will be,

$$\hat{\rho}(t + \Delta t) = \hat{\rho}(t) - \frac{i}{\hbar}[\hat{H}, \hat{\rho}(t)]\Delta t, \tag{5.1}$$

where it is assumed that the interval is short enough to neglect terms of higher order Δt. When a measurement occurs in an interval then the state at the end of the interval becomes the sum over all possible measurement outcomes weighted with their associated probability,

$$\hat{\rho}(t + \Delta t) = \sum_i \mathrm{Tr}[\hat{A}_i \hat{\rho}(t) \hat{A}_i^\dagger] \frac{\hat{A}_i \hat{\rho}(t) \hat{A}_i^\dagger}{\mathrm{Tr}[\hat{A}_i \hat{\rho}(t) \hat{A}_i^\dagger]} = \sum_i \hat{A}_i \hat{\rho}(t) \hat{A}_i^\dagger. \tag{5.2}$$

If these two outcomes, equations 5.1 and 5.2, are now combined with their associated probabilities we obtain,

$$\hat{\rho}(t + \Delta t) = (1 - R\Delta t)\hat{\rho}(t) - \frac{i}{\hbar}[\hat{H}, \hat{\rho}(t)] + R\Delta t \sum_i \hat{A}_i \hat{\rho} \hat{A}_i^\dagger, \tag{5.3}$$

which is correct to first order in Δt. Re-arranging the above expression and taking the limit $\Delta t \to 0$ the following is arrived at,

$$\dot{\hat{\rho}}(t) = \frac{-i}{\hbar}\left[\hat{H}, \hat{\rho(t)}\right] + R\left(\sum_i \hat{A}_i \hat{\rho}(t) \hat{A}_i^\dagger - \hat{\rho}(t)\right). \tag{5.4}$$

This is the measurement master equation and is clearly of Lindblad type (section 1.3.1) where our Lindblad operators have been replaced by the measurement operators and are now subject to the extra constraint that $\sum_i \hat{A}_i^\dagger \hat{A}_i = \hat{1}$, which is the source of the term $-R\hat{\rho}$.

The evolution of the state then depends on the rate of measurements, R, and the set of measurement operators $\{\hat{A}_i\}$. It is useful to quantify the measurement operators by a parameter that relates to their 'strength'. The strongest measurements would be projectors of the system's eigenstates while the weakest measurements would be proportional to the identity operator of the system because they will not change the state. For example, in [81] the system studied was a two-level atom under-going Rabi flopping evolution and the measurement operators were of the form,

$$\hat{A}_\pm = \frac{1}{\sqrt{2}}(\hat{1} \pm \epsilon\hat{\sigma}_z) = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pm \epsilon \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right], \tag{5.5}$$

where the parameter ϵ is the strength of the measurements, with $\epsilon = 1/2$ for strong measurements and $\epsilon = 0$ for the weakest measurements. The damping parameter, γ, in the Lindblad master equation, equation 1.46, depends upon both R and ϵ,

$$\gamma = \frac{R}{2}\left(\sqrt{1-\epsilon} - \sqrt{\epsilon}\right)^2. \tag{5.6}$$

It was found that when the γ is kept constant but ϵ and R are varied different evolutions are found for single quantum trajectories. When they had frequent, weak measurements they found quantum Zeno effect behaviour, which resulted in random "telegraph" type plots of the quantum trajectories, and for infrequent, strong measurements the Rabi-flopping evolution

was punctuated by state collapses into the eigen-states of the system.

In the following sections we use the general measurement master equation, equation 5.4, to evolve a quantum state in time and we analyse the differences between the two sets of measurement effect operators. In the next section the eigen-basis we use is photon-number states, $\{|n\rangle\langle n|\}$, where the operators are all orthogonal. In a following section the second eigenbasis we examine is the coherent states, $\{|\alpha\rangle\langle\alpha|\}$.

5.2 Measurement master equation with number states

In this section we examine a master equation where the eigen-basis used for the measurement operators will be the photon-number state basis, which is an orthogonal set of basis states and an infinite-dimensional space. The master equation can be solved be examining matrix elements of the density operator and how they evolve through time. We initially start with projective measurements and later in the section we introduce a 'strength' parameter.

Our measurement effect operators can be written as,

$$\hat{A}_n = |n\rangle\langle n|, \tag{5.7}$$

which are projective operators. Our master equation is then,

$$\begin{aligned} \dot{\hat{\rho}} &= R\sum_{n=0}^{\infty} \hat{A}_n\hat{\rho}\hat{A}_n^{\dagger} - R\hat{\rho} \\ &= R\sum_{n=0}^{\infty} \rho_{nn}|n\rangle\langle n| - R\hat{\rho}, \end{aligned} \tag{5.8}$$

where $\rho_{nn} = \langle n|\hat{\rho}|n\rangle$ and we will ignore the effects of any Hamiltonian evolution. We can solve this master equation quite simply using matrix elements as it has discrete elements. Using equation 5.8, the evolution for the diagonal

and off-diagonal elements are given by,

$$\langle m|\,\dot{\hat{\rho}}\,|m\rangle = \dot{\rho}_{mm} = R\sum_n \rho_{nn}\delta_{nm} - R\rho_{mm} = 0 \tag{5.9}$$

and

$$\langle m|\,\dot{\hat{\rho}}\,|k\rangle = \dot{\rho}_{mk} = R\sum_n \rho_{nn}\delta_{nm}\delta_{nk} - R\rho_{mk} = -R\rho_{mk},\ \ m \neq k. \tag{5.10}$$

It can be seen that the measurements do nothing to change the diagonal elements but decohere the off-diagonal elements exponentially. When we model this equation computationally the first measurement to occur collapses the system into a number state $|n\rangle\langle n|$ with probability $\langle n|\,\hat{\rho}\,|n\rangle$. It will remain in this state as subsequent measurements yield the same result unless any Hamiltonian evolution takes it out of this state.

5.2.1 Imperfect measurements in the number state basis

We now wish to include a parameter, σ, that reflects the strength of the measurement. As $\sigma \to \infty$ then $\hat{A} \to \hat{1}$, the identity operator of the system which means that there is no information gained from the measurement, and if $\sigma = 0$ then $\hat{A}_n = |n\rangle\langle n|$, projective measurements with no error and maximum information transfer from the system to the observer. We model our imperfect measurement operators as,

$$\hat{A}_n = \frac{1}{\sqrt{N_{n,\sigma}}}\sum_{m=0}^{\infty} e^{\frac{-(n-m)^2}{2\sigma}}\,|m\rangle\langle m|\,, \tag{5.11}$$

where σ is finite and $N_{n,\sigma}$ is the normalisation constant. The POM element corresponding to this effect is,

$$\begin{aligned}\hat{\pi}_n &= \frac{1}{\sqrt{N_{n,\sigma}}}\sum_{m=0}^{\infty} e^{\frac{-(n-m)^2}{2\sigma}} |m\rangle\langle m| \frac{1}{\sqrt{N_n}}\sum_{j=0}^{\infty} e^{\frac{-(n-j)^2}{2\sigma}} |j\rangle\langle j| \\ &= \sum_{m=0}^{\infty} \frac{e^{\frac{-(n-m)^2}{\sigma}}}{N_{n,\sigma}} |m\rangle\langle m| . \end{aligned} \tag{5.12}$$

Using the condition $\sum_n \hat{\pi}_n = \hat{1}$ we find that,

$$\sum_{n=0}^{\infty} \frac{e^{\frac{-(n-m)^2}{2\sigma}}}{N_{n,\sigma}} = 1. \tag{5.13}$$

It can be seen that if we set $\sigma = 0$ we obtain the projective measurement operators from the previous equations.

Our master equation with imperfect measurements becomes,

$$\begin{aligned}\dot{\hat{\rho}} &= \sum_{n,m,j} \hat{A}_n\hat{\rho}\hat{A}_n^{\dagger} - R\hat{\rho} \\ &= \left[\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} |m\rangle\langle m|\hat{\rho}|j\rangle\langle j|\right] - R\hat{\rho} \\ &= \left[\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} \rho_{mj} |m\rangle\langle j|\right] - R\hat{\rho}. \end{aligned} \tag{5.14}$$

The evolution for the diagonal elements is,

$$\begin{aligned}\langle k|\dot{\hat{\rho}}|k\rangle &= \dot{\rho}_{kk} = R\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} \rho_{mj}\langle k|m\rangle\langle j|k\rangle - R\rho_{kk} \\ &= R\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} \rho_{mj}\delta_{mk}\delta_{jk} - R\rho_{kk} \\ &= R\sum_{n} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-k)^2}{\sigma}} \rho_{kk} - R\rho_{kk} = 0, \end{aligned} \tag{5.15}$$

as,

$$\sum_n \frac{1}{N_{n,\sigma}} e^{\frac{-(n-k)^2}{\sigma}} = 1, \tag{5.16}$$

by definition. We can see that imperfect measurements do not change the average evolution of the diagonal elements of the density matrix, as before. For the off-diagonal elements,

$$\begin{aligned}
\langle k|\,\dot{\hat{\rho}}\,|k'\rangle &= \dot{\rho}_{kk'} = R\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} \rho_{mj} \langle k\,|m\rangle\,\langle j\,|\,k'\rangle - R\rho_{kk'} \\
&= R\sum_{n,m,j} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-m)^2}{2\sigma}} e^{\frac{-(n-j)^2}{2\sigma}} \rho_{mj}\delta_{mk}\delta_{jk'} - R\rho_{kk'} \\
&= R\sum_{n} \frac{1}{N_{n,\sigma}} e^{\frac{-(n-k)^2}{2\sigma}} e^{\frac{-(n-k')^2}{2\sigma}} \rho_{kk'} - R\rho_{kk'}.
\end{aligned} \tag{5.17}$$

This decoheres the state at a lower rate than projective measurements if $\sigma \neq \infty$. Otherwise the first term evaluates to $R\rho_{kk'}$ and thus $\dot{\rho}_{kk'} = 0$. This means in the limit of weak measurements we do not alter our state.

If we compare the evolution of weaker measurements to that of projective measurements we can see that the diagonal density matrix elements evolve as before (on average), and that the state decoheres at a lower rate. However, in a single measurement there will be a difference as the weak measurement yield less information about the state and cause less collapse in the state. We examine this computationally in the next section.

5.2.2 Computational modelling

Modelling this equation with weak measurement operators computationally yields different evolutions from the projective operators which collapse the state immediately. Our initial state is the coherent state $|\alpha\rangle$ which we evolve by making a certain number of measurements on. This is plotted in fig. 5.1, that shows the diagonal elements for the state, the photon-number probability, after a certain number of measurements. It can be seen that the state eventually collapses into a single number state, as after each measurement the

photon number distribution becomes more peaked. Note that the evolution to this final state is stochastic, and the system could evolve to any final state, albeit with a given probability. Although this figure shows a continuous line, this is for clarity. The state is only defined at the integers, corresponding to the diagonal elements of the density matrix.

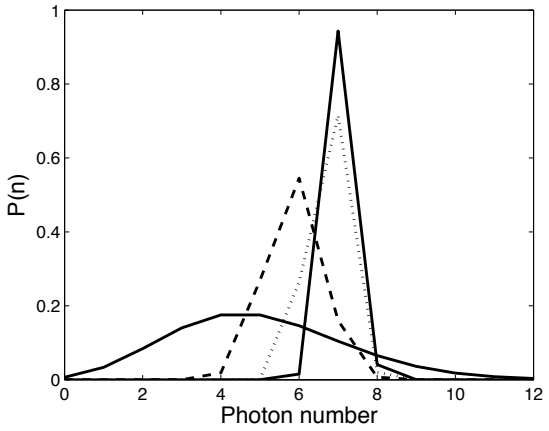


Figure 5.1: The photon-number distribution after a certain number of measurements. The solid line is the initial distribution, whereas the next distributions are after 3, 6 and 9 measurements each. The distribution becomes more peaked after each measurement.

In fig. 5.2, we show the photon-number distribution after a single measurement with varying σ. It can be seen that the projective measurement instantly collapses the state into a single number state after measurement whereas this collapse is slower for higher values of σ, as these measurement operators are closer to the identity operator for the system. Again, this evolution is stochastic and the density matrix elements are only defined at the integer values of n.

In this next section we will choose our measurement operators to be taken from the coherent state basis, a different basis of states. In contrast to the system studied below, and also studied in [81], these measurement operators are continuous and non-orthogonal. To solve the master equation in a coherent state basis we will have to use phase-space methods. We will

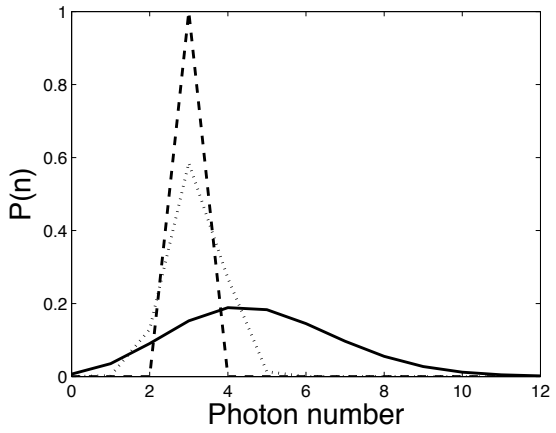


Figure 5.2: The photon-number distribution after a single measurement with varying values of σ. A lower σ induces more collapse onto a single number state.

next describe these methods used in the next section.

5.3 Measurement master equation with coherent states

In this section we provide an example of a measurement master equation where the measurement operators used will be based upon coherent states. These are continuous operators and therefore we cannot solve it using a discrete system of equations as done in [81] and in the previous section.

In order to solve our measurement master equation analytically we must use phase space methods to transform the density matrix and master equation into a quasi-probability function and partial-differential equation respectively. We will explain these methods in the next section and then use them to solve our master equation. Finally we computationally model our system and plot trajectories of our state evolution.

5.3.1 Phase space methods in quantum optics

In the next section we will derive a master equation for our system undergoing measurements, which gives us a Fokker-Planck Equation (FPE) for the density matrix. In general, for infinite-dimensional systems, this will be difficult to solve. However there are methods we can employ to change the FPE into a partial differential equation for a quasi-probability density and then use this to calculate moments of this density function. There are various ways to transform a quantum state in a Hilbert space to a complex-valued function in phase space. The first case was discovered by Wigner [86] in 1932 and others by Glauber [87], Sudarshan [26] and Husimi. This work has been extended to generalized quasi-probability functions of density operators [88].

In the following sections we will make use of the normally-ordered quantum characteristic function, defined as,

$$\chi(\lambda, \lambda^*) = \mathrm{Tr}\left[e^{\lambda \hat{a}^\dagger} e^{-\lambda^* \hat{a}} \hat{\rho}\right], \tag{5.18}$$

which, upon differentiation with respect to λ, λ^*, gives us normally-ordered expectation values of the density matrix,

$$\langle (\hat{a}^\dagger)^m \hat{a}^n \rangle = (-1)^n \left(\frac{\partial^{(m+n)}}{\partial \lambda^m \partial^n \lambda^*} \chi(\lambda, \lambda^*) \right) \Big|_{\lambda, \lambda^* = 0}. \tag{5.19}$$

To transform combinations of operators $\hat{a}^\dagger, \hat{a}$ and the density matrix $\hat{\rho}$ to operations on χ, we use the following rules [18, 27],

$$\begin{aligned}
\hat{a}\,\hat{\rho} &\rightarrow -\frac{\partial}{\partial \lambda^*}\chi \\
\hat{a}^\dagger \hat{\rho} &\rightarrow \left(-\lambda^* + \frac{\partial}{\partial \lambda}\right)\chi \\
\hat{\rho}\,\hat{a} &\rightarrow \left(\lambda - \frac{\partial}{\partial \lambda^*}\right)\chi \\
\hat{\rho}\,\hat{a}^\dagger &\rightarrow \frac{\partial}{\partial \lambda}\chi.
\end{aligned}$$

As well as the quantum characteristic function, we also use the Q-function for the density matrix,

$$Q(\alpha, \alpha^*) = \frac{1}{\pi} \langle \alpha | \hat{\rho} | \alpha \rangle , \tag{5.20}$$

which is a positive function and is related to the quantum characteristic function by a Fourier transform,

$$\chi(\lambda, \lambda^*) = e^{|\lambda|^2} \int d^2\alpha e^{\lambda\alpha^* - \alpha\lambda^*} Q(\alpha, \alpha^*). \tag{5.21}$$

5.3.2 Derivation of the measurement master equation solution

Here we describe a measurement master equation and then solve this to obtain expectation values of operators as the state evolves in time. Our equation will be of the form of equation 5.4. We start by choosing a simple Hamiltonian for the system,

$$\hat{H} = \hbar\omega \left[\hat{a}^\dagger \hat{a} + \frac{1}{2} \right], \tag{5.22}$$

and we choose coherent state projectors as our measurement operators,

$$\hat{A}(\beta) = \frac{1}{\sqrt{\pi}} |\beta\rangle \langle\beta| . \tag{5.23}$$

This choice of measurement operators satisfies the two criteria we need, completeness and positivity,

$$\int d^2\beta \hat{A}^\dagger(\beta)\hat{A}(\beta) = \int d^2\beta \frac{1}{\pi} |\beta\rangle \langle\beta| = \hat{1}, \tag{5.24}$$

$$\mathrm{Tr}[\hat{\rho}\hat{A}^\dagger(\beta)\hat{A}(\beta)] \geq 0 \; \forall \, \hat{\rho}, \; \hat{A}(\beta). \tag{5.25}$$

The integral is performed over all phase space and $d^2\beta = d\mathrm{Re}(\beta)\, d\mathrm{Im}(\beta) = dx\, dy$, where x and y are the quadrature axes.

Including the Hamiltonian and measurement operators into the master equation, equation 5.4, we have,

$$\dot{\hat{\rho}} = -i\,\omega\left[\hat{a}^\dagger\hat{a},\hat{\rho}\right] + R\left(\frac{1}{\pi}\int_\beta |\beta\rangle\langle\beta|\,\hat{\rho}\,|\beta\rangle\langle\beta|\;d^2\beta - \hat{\rho}\right) \tag{5.26}$$

and we note that inside the integral, the factor $\frac{1}{\pi}\langle\beta|\,\hat{\rho}\,|\beta\rangle$ is the Q-function of $\hat{\rho}$,

$$\dot{\hat{\rho}} = -i\,\omega\left[\hat{a}^\dagger\hat{a},\hat{\rho}\right] + R\left(\int_\beta Q(\beta,\beta^*)\,|\beta\rangle\langle\beta|\;d^2\beta - \hat{\rho}\right). \tag{5.27}$$

We can now solve this equation analytically using the phase-space methods outlined above. We choose to convert our equation for the evolution of the density operator into one that evolves the quantum characteristic function of the state, defined in equation 5.18. The terms involving the Hamiltonian evolution and $R\hat{\rho}$ are simple to transform. We use the rules for transforming operators, equations 5.20, to obtain,

$$-i\,\omega\left[\hat{a}^\dagger\hat{a},\hat{\rho}\right] = -i\omega(\hat{a}^\dagger\hat{a}\hat{\rho} - \hat{\rho}\hat{a}^\dagger\hat{a}) \rightarrow -i\omega\left(\lambda^*\frac{\partial}{\partial\lambda^*} - \lambda\frac{\partial}{\partial\lambda}\right)\chi, \tag{5.28}$$

and the term,

$$R\hat{\rho} \rightarrow R\chi. \tag{5.29}$$

The term involving measurement operators,

$$R\int d^2\beta\hat{A}(\beta)\hat{\rho}\hat{A}^\dagger(\beta) = R\int_\beta Q(\beta,\beta^*)\,|\beta\rangle\langle\beta|\;d^2\beta, \tag{5.30}$$

is more involved. We start at the definition of the characteristic function, equation 5.18, and insert the term 5.30 to obtain the expression,

$$\mathrm{Tr}\left[e^{\lambda\hat{a}^\dagger}e^{-\lambda^*\hat{a}}R\int_\beta d^2\beta\,Q(\beta,\beta^*)\,|\beta\rangle\langle\beta|\right], \tag{5.31}$$

and using the cyclical property of the trace operation we have,

$$\mathrm{Tr}\left[R\int_{\beta}d^{2}\beta e^{-\lambda^{*}\hat{a}}\ |\beta\rangle\, Q(\beta,\beta^{*})\,\langle\beta|\ e^{\lambda\hat{a}^{\dagger}}\right]. \tag{5.32}$$

Next, we use the theory described in section 1.4.1 to evaluate the operators acting upon the coherent states,

$$\mathrm{Tr}\left[R\int_{\beta}d^{2}\beta\, e^{-\lambda^{*}\beta}\ |\beta\rangle\, Q(\beta,\beta^{*})\,\langle\beta|\ e^{\lambda\beta^{*}}\right]. \tag{5.33}$$

If we take the trace operation (in any basis, we choose the number state basis) this leads to,

$$\begin{aligned}&\sum_{n}\langle n|\,R\int_{\beta}d^{2}\beta\, e^{-\lambda^{*}\beta+\lambda\beta^{*}}Q(\beta,\beta^{*})\,|\beta\rangle\,\langle\beta|\,n\rangle\\ &=\sum_{n}R\int_{\beta}d^{2}\beta\, e^{-\lambda^{*}\beta+\lambda\beta^{*}}Q(\beta,\beta^{*})\langle n\,|\beta\rangle\,\langle\beta|\,n\rangle,\end{aligned} \tag{5.34}$$

and we re-arrange the operators to form the identity $\sum_{n}|n\rangle\,\langle n|$ (which can be removed) to get,

$$R\int_{\beta}d^{2}\beta\, e^{-\lambda^{*}\beta+\lambda\beta^{*}}Q(\beta,\beta^{*}). \tag{5.35}$$

If we use the fact that the characteristic function is the Fourier transform of the Q-function, equation 5.21, we replace 5.35 with,

$$R\int_{\beta}d^{2}\beta e^{-\lambda^{*}\beta+\lambda\beta^{*}}Q(\beta,\beta^{*})=R\, e^{-|\lambda|^{2}}\chi(\lambda,\lambda^{*}). \tag{5.36}$$

Combining the three terms, 5.28, 5.29 and 5.36, we have an expression for the time-evolution of the quantum characteristic function,

$$\dot{\chi}=-i\omega\left(\lambda^{*}\frac{\partial}{\partial\lambda^{*}}-\lambda\frac{\partial}{\partial\lambda}\right)\chi+R\left(e^{-|\lambda|^{2}}-1\right)\chi. \tag{5.37}$$

We can solve this by using the method of characteristics for partial differential

equations [89]. First we re-write 5.37 as,

$$\partial_t \chi - i\omega\lambda\partial_\lambda \chi + i\omega\lambda^*\partial_{\lambda^*}\chi = R_c\chi, \tag{5.38}$$

where $R_c = R(e^{-|\lambda|^2} - 1)$ and ∂_j is partial differentiation with respect to variable j. Solving this we obtain,

$$\chi(\lambda, \lambda^*, t) = \chi(\lambda_0 e^{-i\omega t}, \lambda_0^* e^{i\omega t}) e^{R_c t}, \tag{5.39}$$

where λ_0, λ_0^* are the initial conditions of the state, which can be obtained from equation 5.18 using the initial density operator. The first factor is our state rotating under the Hamiltonian evolution while the second factor is due to the presence of the measurements. In the next section we calculate expectation values of operators using this expression.

5.3.3 Calculating observable values using the characteristic function

We can calculate expectation values of normally-ordered observables using the expression for χ, derived in the last section, by taking derivatives of it with respect to λ, λ^*. The formula for doing so is,

$$\langle (\hat{a}^\dagger)^m \hat{a}^n \rangle = (-1)^n \left(\frac{\partial^{(m+n)}}{\partial\lambda^m \partial\lambda^{*n}} \chi(\lambda, \lambda^*) \right) \Bigg|_{\lambda,\lambda^*=0}. \tag{5.40}$$

Our function for χ is given by equation 5.39 and we choose the initial state to be $|\alpha\rangle\langle\alpha|$, which has the characteristic function,

$$\chi(\lambda, \lambda^*) = \exp(\alpha^*\lambda - \alpha\lambda^*), \tag{5.41}$$

so that our function for $\chi(\lambda, \lambda^*, t)$ is,

$$\chi(\lambda, \lambda^*, t) = \exp(\alpha^*\lambda_0 e^{-i\omega t} - \alpha\lambda_0^* e^{i\omega t}) e^{R_c t}, \tag{5.42}$$

where $R_c = R(e^{-|\lambda|^2} - 1)$. Some operator values of interest are,

$$\langle \hat{a}^\dagger(t) \rangle = \left. \frac{\partial \chi(\lambda, \lambda^*)}{\partial \lambda} \right|_{\lambda,\lambda^*=0} = \alpha^* e^{-i\omega t} \tag{5.43}$$

$$\langle \hat{a}(t) \rangle = -\left. \frac{\partial \chi(\lambda, \lambda^*)}{\partial \lambda^*} \right|_{\lambda,\lambda^*=0} = \alpha e^{i\omega t} \tag{5.44}$$

$$\langle \hat{a}^\dagger(t)\hat{a}(t) \rangle = \langle \hat{n}(t) \rangle = -\left. \frac{\partial^2 \chi(\lambda, \lambda^*)}{\partial \lambda \partial \lambda^*} \right|_{\lambda,\lambda^*=0} = |\alpha|^2 + Rt, \tag{5.45}$$

where the last operator is the number operator. The presence of measurements does not affect the first two expectation values from their Hamiltonian-only behaviour. However, the presence of measurements causes the photon-number operator to grow linearly in time.

For time-derivatives of these observables, i.e. $\langle \dot{\hat{a}} \rangle$, we need an expression for the time-derivative of the characteristic function,

$$\dot{\chi}(\lambda, \lambda^*, t) = -i\omega[\alpha^* \lambda_0 e^{-i\omega t} + \alpha \lambda_0^* e^{i\omega t}]\chi(\lambda, \lambda^*, t) + R_c\, \chi(\lambda, \lambda^*, t) \tag{5.46}$$

and then use this in the above expression for calculating expectation values. The time-derivative values of the above operators are,

$$\langle \dot{\hat{a}}^\dagger \rangle = \left. \frac{\partial \dot{\chi}(\lambda, \lambda^*)}{\partial \lambda} \right|_{\lambda,\lambda^*=0} = -i\omega\alpha^* e^{-i\omega t} \tag{5.47}$$

$$\langle \dot{\hat{a}} \rangle = -\left. \frac{\partial \dot{\chi}(\lambda, \lambda^*)}{\partial \lambda^*} \right|_{\lambda,\lambda^*=0} = i\omega\alpha e^{i\omega t} \tag{5.48}$$

$$\langle \dot{\hat{n}} \rangle = -\left. \frac{\partial^2 \dot{\chi}(\lambda, \lambda^*)}{\partial \lambda \partial \lambda^*} \right|_{\lambda,\lambda^*=0} = R. \tag{5.49}$$

It can be seen that these expectation values of time-derivatives agree with the previous ones.

In the next section we will compare the analytical results with computational results when we use computer modelling to plot the systems trajectory in phase space. We will see that for a single trajectory the quantum system have motion similar to Brownian motion.

5.3.4 Computational modelling of the measurement master equation

In this section we describe how we simulated the measurement master equation, equation 5.26, stochastically using Monte-Carlo methods to obtain a phase space trajectory of our quantum system as it evolves in time. The method that we use to evolve our state computationally is the same procedure that the master equation was derived from, section 5.1, which we will now describe.

We first discretize time into intervals Δt and choose a probability that a measurement will occur in that interval. This probability gives us a rate R for measurements, with higher probabilities corresponding to higher rates. At the start of each interval we randomly decide, according to the rate R, if a measurement occurs or not. If a measurement occurs the density matrix changes according to,

$$\hat{\rho} \rightarrow \frac{\hat{A}(\beta)\hat{\rho}\hat{A}^{\dagger}(\beta)}{\mathrm{Tr}[\hat{A}(\beta)\hat{\rho}\hat{A}^{\dagger}(\beta)]} \tag{5.50}$$

because we know the result of the measurement. As our measurement operators are projectors, when we obtain result β our state after measurement is $|\beta\rangle\langle\beta|$, a pure state. If our initial state before measurement is $|\alpha\rangle\langle\alpha|$ then we measure β with probability $e^{-|\alpha-\beta|^2}/\pi$. If no measurement occurs then the state remains unchanged. After the measurement decision we then evolve our state according to the Hamiltonian, which, in our case, rotates our state at a frequency ω.

Following a measurement the new state is randomly chosen, and the probability distribution for moving to the state β given the current state α is,

$$P(\beta|\alpha) = \frac{1}{\pi}e^{-|\alpha-\beta|^2}. \tag{5.51}$$

We can write this complex Gaussian as two separable one-dimensional Gaussian functions for the real-valued components of α and β ($\alpha_x, \alpha_y, \beta_x$ and β_y)

as,

$$P(\beta|\alpha) = \frac{1}{2\pi\sigma^2} e^{\frac{-(\alpha_x-\beta_x)^2}{2\sigma^2}} e^{\frac{-(\alpha_y-\beta_y)^2}{2\sigma^2}}, \tag{5.52}$$

with $\sigma = 1/\sqrt{2}$. To model the change in the density operator when a measurement occurs we select a random variable from each of the two distributions of real numbers above, x and y, and then the new state after measurement will be the coherent state $|x + iy\rangle$. We then repeat this for a certain number of iterations to obtain a trajectory. We then repeat the algorithm from the same initial conditions and average the individual trajectories.

We now plot the average evolution for 1, 10, 100 and 2000 trajectories of the evolution in figs. 5.3-5.5, with the same initial state $|\alpha\rangle \langle\alpha|$ and same rate of measurements, R. From fig. 5.3, we have typical single trajectory. We can see periods of Hamiltonian evolution, which is simple rotation in phase space tracing out a circle, punctuated by random deviations induced by measurement. As we increase the number of trajectories over which we have averaged, we being to see evolution approaching a smooth, circular shape in phase space, as can be seen in fig. 5.5. This agrees with our analytical analysis in the previous section.

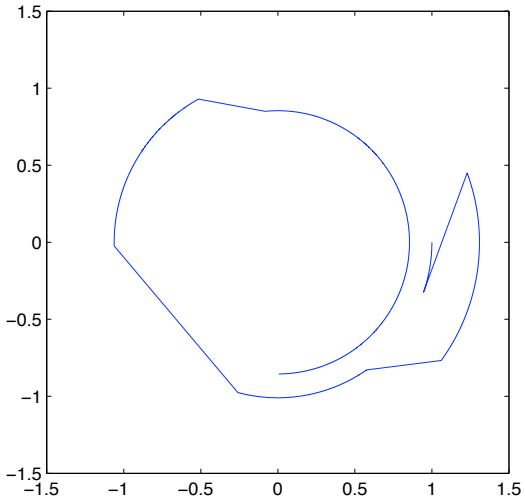


Figure 5.3: A single evolution of the trajectory in phase space.

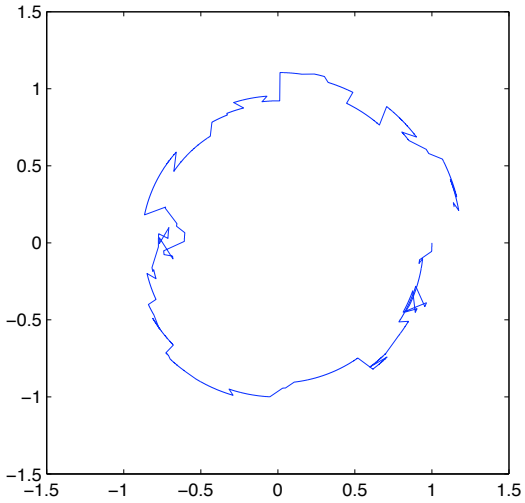


Figure 5.4: The average of 10 trajectories in phase space

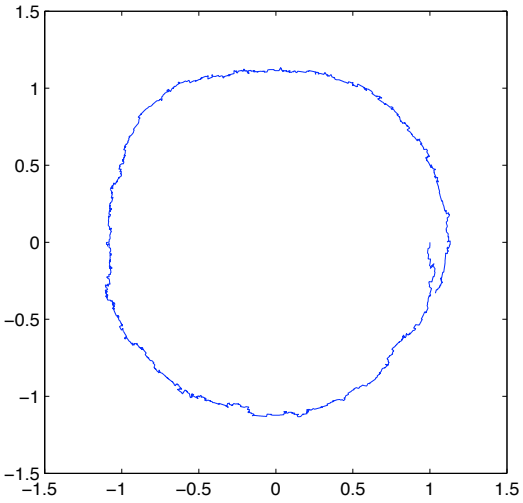


Figure 5.5: The average of 100 trajectories in phase space

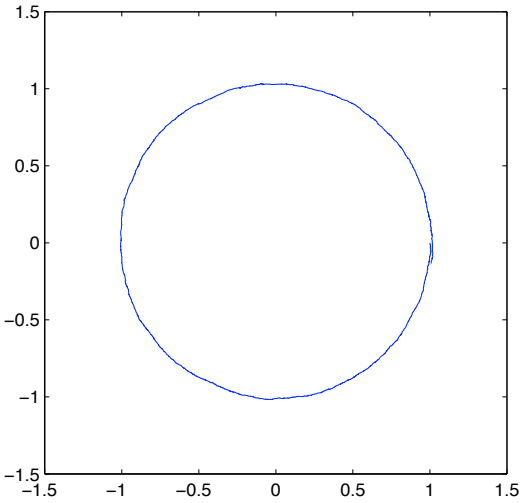


Figure 5.6: The average of 2000 trajectories in phase space

5.3.5 Imperfect Measurements in the coherent state basis

As before with the number state basis, we will now examine imperfect measurements made in the coherent state basis. These measurement operators will have the form,

$$\hat{A}(\alpha) = \sqrt{\frac{2\sigma^2+1}{\pi}} \int d^2\delta \frac{e^{-|\alpha-\delta|^2/\sigma^2}}{\pi\sigma^2} |\delta\rangle \langle\delta| , \tag{5.53}$$

where δ is a random deviation from the result of the measurement and it follows a complex Gaussian distribution. The POM elements are,

$$\begin{aligned} \hat{\pi}(\alpha) = \hat{A}^\dagger(\alpha)\hat{A}(\alpha) &= \frac{2\sigma^2+1}{\pi} \int d^2\delta \int d^2\delta' \frac{e^{-|\alpha-\delta|^2/\sigma^2}}{\pi\sigma^2} \frac{e^{-|\alpha-\delta'|^2/\sigma^2}}{\pi\sigma^2} \\ &\times \; e^{-\frac{1}{2}(|\delta|^2+|\delta'|^2-2\delta'^*\delta)} |\delta'\rangle \langle\delta| , \end{aligned} \tag{5.54}$$

such that,

$$\int d^2\alpha \; \hat{\pi}(\alpha) = \hat{1}. \tag{5.55}$$

Again the strength of the measurements is parameterized by σ, which is the spread of the deviation. For $\sigma = 0$ we have projective measurements and as $\sigma \to \infty$, $\hat{\pi} \to \hat{1}$.

The master equation with this form of measurement operators becomes more difficult to solve. The term involving the measurement operators is,

$$\begin{aligned} R \int d^2\alpha \, \hat{A}(\alpha)\hat{\rho}\hat{A}^\dagger &= R \, \frac{2\sigma^2+1}{\pi} \int d^2\alpha \int d^2\delta \int d^2\delta' \\ &\quad \times \frac{e^{-|\alpha-\delta|^2/\sigma^2}}{\pi\sigma^2} \frac{e^{-|\alpha-\delta'|^2/\sigma^2}}{\pi\sigma^2} |\delta\rangle \langle\delta| \, \hat{\rho} \, |\delta'\rangle \langle\delta'| \\ &= R \, \frac{2\sigma^2+1}{\pi} \int d^2\delta \int d^2\delta' \frac{e^{-|\delta-\delta'|^2/2\sigma^2}}{2\pi\sigma^2} |\delta\rangle \langle\delta| \, \hat{\rho} \, |\delta'\rangle \langle\delta'| . \end{aligned} \tag{5.56}$$

This term is difficult to evaluate in general as it has no corresponding quasi-probability distribution.

5.4 Conclusions

In this chapter we have analysed a master equation that describes a system undergoing measurements in times. These measurements are described most generally by Kraus effect operators, and the subsequent evolution of the system satisfies the conditions of a Lindblad master equation. We have looked at two different sets of measurement operators, the photon-number states and the coherent states.

The first example of measurement operators, the photon-number states, are an orthogonal set of states. We found that the analytical evolution under these measurements caused decoherence but that they did not affect the diagonal entries of the density matrix on average. When we modelled these equations computationally we found that in a single evolution we would see the state collapse into a photon-number state, and that the analytical solution only represents the average behaviour of the system under evolution. We examined weaker measurements that yield less information about the state and disturb the state less.

The second example of measurement operators were the coherent states, a non-orthogonal set of basis states. To solve the master equation we employed phase space methods in order to turn this equation for density operators into a Fokker-Planck equation for a complex function. For projective measurement operators this was possible we obtained an analytical expression that allowed us to calculate expectation values of the quantum state. We found that some of these expectation values did not depend upon the measurements being present. When we modelled these measurements computationally we observed a diffusion-like evolution of the quantum state, as it jumps in phase-space after each measurement. We again only obtain the analytical results after we average over many such evolutions. Imperfect measurements in the coherent state basis were more difficult to deal with due to the master equation having no corresponding Fokker-Planck expression. This could be an area of future work.

Chapter 6

Conclusions

6.1 Summary of thesis

In this thesis we have addressed some issues of measurements in postselecting devices and open quantum systems.

We first explained, in Chapter 2, a method to quantify how well a postselecting device operates i.e. how well it produces the state that it is intended to produce. We termed this the fidelity of correct output. This figure of merit is based on the general mixed state fidelity, though we have removed terms from the final output density matrix of the device that do not contribute to the correct operation of the device. It was shown that this measure depended on two factors: one that depends on the properties of the postselecting device itself and another that depends upon the properties of the detector used. At the end of the chapter we demonstrated this measure by providing two examples of postselecting device, a two-photon state generator and a coherent-state comparison device, and calculating the measure for both devices.

This second factor in this measure of fidelity, the one that depends upon the properties of the detection element, leads us onto the theory in Chapter 3. Here we describe the theory of pre-amplification assisting photo-detection in the presence of a lossy photo-detector. By placing a photo-amplifier in front

of a lossy detector we can sometimes improve the discrimination of states with different photon numbers. To illustrate this method working we used several examples of situations were we wish to distinguish between photon numbers. We looked at two separate case where we the 'trigger' result is either zero photons or a single photon. We found two conditions that we can use to determine if pre-amplification will be useful. Firstly, it appears that the amplifier noise, N_{amp}, must be less than the reciprocal of the detector efficiency to be effective $N_{\text{amp}} < \eta^{-1}$. Secondly, we must aim to distinguish between the lowest photon number present i.e. zero photons or a single photon in a heralded input, for the scheme to be helpful.

In Chapter 4 we combined the theory from the previous two chapters in order to quantify the operation of a network for quantum key distribution (QKD). In this protocol the quantum key bits were coherent states, $|\alpha\rangle$. The 'alphabet' of different key bits that could be sent all had equal magnitude, $|\alpha|$, but varying phase about 2π. We analysed the effect of lossy beamsplitters and phase noise in the transmission of key bits, as well as the theory of pre-amplification assisting state discrimination.

Finally in Chapter 5 we analysed the dynamics of a quantum system undergoing repeated measurements in time. This evolution in time was described by a master equation and so our quantum state, which initially was pure, decohered into a mixed state. This decoherence depended on the rate of measurements and the strength of measurements, where a strong measurement is close to a projective, Von Neumann measurement and a weak measurement would be close to the identity operator of the system. We considered measurements in two different sets of basis state: coherent state basis and the photon-number state basis. The photon-number state showed eventual collapse into a single state of the system, whereas the coherent state basis showed diffusion throughout all of phase space.

Bibliography

[1] P. Dirac. *The Principles of Quantum Mechanics*. OUP, Oxford, 2003.

[2] J. Von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, 1996.

[3] M. Schlosshauer. *Decoherence and the Quantum-to-Classical Transition*. Springer, Berlin, 2007.

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

[5] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(195), 1964.

[6] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49(2):91–94, Jul 1982.

[7] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, 49(25):1804–1807, Dec 1982.

[8] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6), 1991.

[9] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[10] K. Kraus. *States, Effects and Operations*. Springer-Verlag, Berlin, 1983.

[11] S.M. Barnett and S. Croke. Quantum state discrimination. *Adv. Opt. Photon.*, 1, 2009.

[12] C. W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.

[13] S. Croke et. al. Maximum confidence quantum measurements. *Phys. Rev. Lett.*, 96(7), 2006.

[14] D. T. Pegg, S. Barnett, and J. Jeffers. Quantum theory of preparation and measurement. *Journal of Modern Optics*, 49(913), 2002.

[15] G. M. Clarke and D. Cooke. *A Basic Course in Statistics*. Arnold, London, 1998.

[16] S. M. Barnett and D. Pegg. Bayes' theorem and quantum retrodiction. *J. Mod. Opt.*, 47(11), 2000.

[17] H. Carmichael. *An Open Systems Approach to Quantum Optics*. Springer-Verlag, Berlin, 1993.

[18] C. W. Gardiner and P. Zoller. *Quantum Noise: A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics*. Springer, Berlin, 2004.

[19] H.P. Breuer and F. Petruccione. *The Theory of Open Quantum Systems*. OUP, Oxford, 2007.

[20] M. D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and Its Applications*, 10(285), 1975.

[21] G. Landblad. On the generators of quantum dynamical semigroups. *Commum. Math. Phys.*, 48(119), 1976.

[22] R. Loudon. *The Quantum Theory of Light*. OUP, New York, 2000.

[23] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, Cambridge, 1995.

[24] R. Glauber. Coherent and incoherent states of the radiation field. *Phys. Rev.*, 131, 1963.

[25] Roy J. Glauber. The quantum theory of optical coherence. *Phys. Rev.*, 130(6):2529–2539, Jun 1963.

[26] E. C. G. Sudarshan. Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Phys. Rev. Lett.*, 10(7):277–279, Apr 1963.

[27] S. M. Barnett and P. M. Radmore. *Methods in Theorectical Quantum Optics*. OUP, Oxford, 1997.

[28] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. In *Proc. R. Soc. Lond. A*, 1985.

[29] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In *Proc. R. Soc. Lond. A*, 1992.

[30] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceeding, 35th Annual Symposium on Foundations of Computer Science*, 1994.

[31] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(120), 1978.

[32] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, Jul 1997.

[33] Lov K. Grover. Quantum computers can search rapidly by using almost any transformation. *Phys. Rev. Lett.*, 80(19):4329–4332, May 1998.

[34] David P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51(2):1015–1022, Feb 1995.

[35] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, May 2001.

[36] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(2):022312, Aug 2003.

[37] Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86(5):910–913, Jan 2001.

[38] Steane A. The ion trap quantum information processor. *Appl. Phys. B*, 64(623), 1997.

[39] Gavin K. Brennen, Carlton M. Caves, Poul S. Jessen, and Ivan H. Deutsch. Quantum logic gates in optical lattices. *Phys. Rev. Lett.*, 82(5):1060–1063, Feb 1999.

[40] Daniel Loss and David P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A*, 57(1):120–126, Jan 1998.

[41] P. Kok et al. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79(135), 2007.

[42] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(46), 2001.

[43] D. Gottemans and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature*, 402(390), 1999.

[44] N. Yoran and B. Reznik. Deterministic linear optics quantum computation with single photon qubits. *Phys. Rev. Lett.*, 91(3):037903, Jul 2003.

[45] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Phys. Rev. A*, 59(5):3295–3300, May 1999.

[46] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. OUP, New York, 2000.

[47] C. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of New Mexico, 1996.

[48] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41, 1994.

[49] A. Uhlmann. The transition probability in the state space of a *-algebra. *Rep. Math. Phys.*, 9(273), 1976.

[50] J. Jeffers. Retrodictive fidelities for pure state postselectors. *New J. Phys.*, 8, 2006.

[51] C. S. Hamilton and J. Jeffers. Fidelity for imperfect postselection. *Phys. Rev. A*, 76, 2007.

[52] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59(18):2044–2046, Nov 1987.

[53] R. Loudon. Fermion and boson beam-splitter statistics. *Phys. Rev. A*, 58(6):4904–4909, Dec 1998.

[54] S. M. Barnett, L. S. Phillips, and D. T. Pegg. Imperfect photodetection as projection onto mixed states. *Op. Comms.*, 15(45), 1998.

[55] P. L. Kelley and W. H. Kleiner. Theory of electromagnetic field measurement and photoelectron counting. *Phys. Rev.*, 136(2), 1964.

[56] J. Jeffers. Interference and the lossless lossy beam splitter. *J. Mod. Opt.*, 47(1819), 2000.

[57] E. Andersson, M.Curty, and I. Jex. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A*, 74, 2006.

[58] M. Sedlák *et. al.* Unambiguous identification of coherent states: Searching a quantum database. *Phys. Rev. A*, 76, 2008.

[59] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin. Unambiguous quantum measurement of nonorthogonal states. *Phys. Rev. A*, 54(5):3783–3789, Nov 1996.

[60] J. Jeffers. Preamplified photodectors for high-fidelity postselectors optical devices. *Phys. Rev. A*, 75, 2007.

[61] C. S. Hamilton and J. Jeffers. Noisy preamplified photodetection for high-fidelity postselection. *J. Phys. B: At. Mol. Opt. Phys.*, 42, 2009.

[62] J. R. Jeffers *et. al.* Quantum optics of travelling-wave attenuators and amplifiers. *Phys. Rev. A*, 47(4), 1993.

[63] C. M. Caves. Quantum limits on noise in linear amplifiers. *Phys. Rev. D*, 26(1817), 1982.

[64] R. Loudon and T. J. Sheperd. Properties of the optical amplifier. *Journal of Modern Optics*, 31(1243), 1984.

[65] R. J. Glauber. Amplifiers, attenuators and the quantum theory of measurement. In *Frontiers in Quantum Optics*, 1986.

[66] S. Tarzi. The inverted harmonic oscillator: some statistical properties. *J. Phys. A: Math. Gen.*, 21(3105), 1988.

[67] O. Jedrkiewicz, R. Loudon, and J. Jeffers. Retrodiction for optical attenuators, amplifiers and detectors. *Phys. Rev. A*, 70, 2004.

[68] N. Herbert. Flash- a superluminal communicator based uopn a new kind of quantum measurement. *Found. Phys.*, 12(12), 1982.

[69] A. M. Brańczyk, Tobias J. Osborne, Alexei Gilchrist, and T. C. Ralph. Photon-added detection. *Phys. Rev. A*, 68(4):043821, Oct 2003.

[70] W. K. Wooters and W. H. Zurek. A single quanta cannot be cloned. *Nature*, 299, 1982.

[71] Howard Barnum, Carlton M. Caves, Christopher A. Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76(15):2818–2821, Apr 1996.

[72] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 1984.

[73] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(3121), 1992.

[74] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61(5):052304, Apr 2000.

[75] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2), 2000.

[76] T. Jennewien *et. al.* Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84(20), 2000.

[77] M. Hillery *et. al.* Quantum secret sharing. *Phys. Rev. Lett.*, 59(3), 1999.

[78] Igor Jex *et. al.* Antisymmetric multi-partite quantum states and their applications. *Fortschr. Phys.*, 51(2), 2002.

[79] C. S. Hamilton, H. Lavička, E. Andersson, J. Jeffers, and I. Jex. Quantum public key distribution with imperfect device components. *Phys. Rev. A*, 79, 2009.

[80] S. M. Barnett, J. Jeffers, A. Gatti, and R. Loudon. Quantum optics of lossy beamsplitters. *Phys. Rev. A*, 57(3), 1998.

[81] J. D. Cresser, S. M. Barnett, J. Jeffers, and D. T. Pegg. Measurement master equation. *Op. Comm.*, 264(352), 2006.

[82] Stephen M. Barnett and James D. Cresser. Quantum theory of friction. *Phys. Rev. A*, 72(2):022107, Aug 2005.

[83] Stephen M Barnett, John Jeffers, and James D Cresser. From measurements to quantum friction. *Journal of Physics: Condensed Matter*, 18(16):S401–S410, 2006.

[84] Carlton M. Caves and G. J. Milburn. Quantum-mechanical model for continuous position measurements. *Phys. Rev. A*, 36(12):5543–5555, Dec 1987.

[85] A. J. Scott and G. J. Milburn. Quantum nonlinear dynamics of continuously measured systems. *Phys. Rev. A*, 63(4):042101, Mar 2001.

[86] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40(5):749–759, Jun 1932.

[87] K. E. Cahill and R. J. Glauber. Density operators and quasiprobability distributions. *Phys. Rev.*, 177(5):1882–1902, Jan 1969.

[88] P D Drummond and C W Gardiner. Generalised p-representations in quantum optics. *Journal of Physics A: Mathematical and General*, 13(7):2353–2368, 1980.

[89] C. Constanda. *Solution Techniques for Elementary Partial Differential Equations*. Chapman and Hall/CRC, London, 2000.