High-Dimensional Entanglement in the Spatial Basis

Submitted by:

Donovan Slabbert 1668702

Supervised by: Prof. Andrew Forbes

School of Physics

University of the Witwatersrand

High-Dimensional Entanglement in the Spatial Basis

Submitted to the faculty of Science School of Physics
of the University of the Witwatersrand
in fulfillment of the requirements for the Degree of

Master of Science

in

Physics.

Internal Examiner

External Examiner

School of Physics

University of the Witwatersrand

Declaration

I, Donovan Michael Slabbert, declare that I am the sole author of this dissertation, written and submitted as requirement for the degree of Master of Science in Physics. All work contained within is my own, unless where explicitly referenced throughout the text. I certify and confirm that this written work has not been submitted to any other institution for a degree or diploma whatsoever. The duration of study, namely the theory, lab work and write up was just over 12 months.

Donovan Michael Slabbert

February 1 2022

Acknowledgments

I am deeply grateful to both the CSIR and DSI for their funding through the CSIR-DSI Interbursary program for postgraduate students. The massive burden of intuition costs, and more, was completely covered by their funding, which made the program exceedingly less stressful.

I would like to wholeheartedly thank my supervisor Prof. Andrew Forbes for the opportunity to complete my Master's as part of his research group and for facilitating all of the necessary equipment in order to do so. It is rare to find a supervisor who is completely committed and involved with their students and their projects.

The support from family cannot be understated. Without being able to vent about bad days or setbacks, wanting to give up would have been a constant temptation. A big thank you goes to my parents, Michael and Hanlie Slabbert, my sister Chané Slabbert, and my aunt Janie, whose support and motivation prompted me to keep going when the pressure became immense.

I would also like to thank the other students Chane, Isaac, Bereneice, Nick, and Keshaan, who guided and helped me whenever I got stuck on problems or struggled with experimental work.

Dedicated to 'Ouma Helena'

Contents

List of Figures

List of Tables

Abstract

Modern cryptography today is required to protect sensitive and important data from attackers. With the dawn of quantum computing, these classical cryptography methods are under threat, which implies that cryptography methods have to be adapted. Quantum cryptography is a promising solution to this problem, that makes use of the concept of quantum entanglement to encrypt information in various degrees of freedom of quantum systems, such as photons. The basics of quantum entanglement, applied to photons, is explored with the aim of extending it to quantum cryptography.

The fundamentals of structured light are investigated, discussed and applied in conjunction with the field of quantum entanglement. Quantum entanglement as a concept is used with the spatial basis of light, namely the theoretically infinite orbital angular momentum basis, to understand the change in entanglement properties as the transition is made from two-dimensional entanglement, using qubits, to higher-dimensional entanglement up to a dimension of four. The optical setup, along with some of the most important equipment and optics are discussed and explored to explain how theory translates to experiment. With the well-known concept of coincidence counting, numerous quantum experiments such as the spiral spectrum, quantum state tomography and Bell violation tests were performed. Finally, quantum key distribution as an application of spatial quantum entanglement is used to illustrate its capabilities and to make the understanding of the fundamentals of quantum entanglement application ready.

The overall observation made is that as the dimension of the quantum system under consideration was increased, by increasing the amount of elements in the chosen basis, the overall accuracy of measurements decreased. This included the spiral bandwidth, the Bell parameter used in Bell violation tests, the fidelity in quantum state tomography state reconstruction and the quantum bit error rate calculated for the well-known BB84 and E91 quantum key distribution algorithms. Another observation made was that precise alignment was really important, as quantum systems are extremely sensitive. Any loss of light effected results greatly. The noise usually associated with quantum systems was also observed, especially where quantum state tomography and quantum key distribution was concerned. This was measured through a decreased overall state fidelity.

Chapter 1

Introduction

Light has many interesting properties and strides have been made across the world to use these properties to its highest potential. Light is currently being used in some capacity in laser, medical, industrial, technological and even entertainment applications. Some of the most topical of these applications are optical metrology for accurate measurements of a physical nature [1], free-space optical communication [2, 3] and quantum applications.

The focus of this dissertation is placed primarily on quantum applications, specifically on quantum entanglement. Quantum entanglement has been used in many applications, some of which include: quantum imaging [4], quantum teleportation [5], and quantum cryptography [6]. There are efforts to use entanglement in quantum computing [7], entanglement swapping [8–10] and super dense coding applications [11].

These applications are possible by entangling what are called degrees of freedom of light. Degrees of freedom are independent values, meaning they do not interact or interact negligibly, that are intrinsic properties of light. Entanglement can be in the polarisation [12], orbital angular momentum [13], time-bin [14], and time-frequency [15] degrees of freedom. Pixel basis entanglement as entanglement in position-momentum space has also been studied [16]. Entanglement between quantum states can be two-, three- and multi-dimensional. The size of the dimension here refers to how many individual quantum states are actually entangled.

Many degrees of freedom can be combined in entangled states. Two of the most prominent types of these are hyper-entangled [17] and hybrid entangled [18] states. Hybrid entanglement is when the individual states making up the entangled state are each in a superposition of their own degree of freedom. Spin-orbit coupled

states [19, 20] and path-polarisation entangled states are two examples [21]. Hyper-entanglement is easily confused with hybrid-entanglement, but the key difference is that, for hyper-entanglement, individual states are in superposition of more than one degree of freedom. This means, for example, that the state is entangled in both of these degrees of freedom over both states, at the same time.

In order to exploit the quantum properties of light and gain the benefits from above, we have to start at the beginning: with the fundamentals of the spatial properties of light. The goal is to start from the beginning or at an introduction to structured light and spatial entanglement, to be application ready at the end. The application chosen to focus on was quantum key distribution.

Chapter 1 starts with the Helmholtz equation derivation and how solutions to this equation are the spatial modes that are widely used in optics. Three modes, Laguerre-Gaussian (LG), Hermite-Gaussian (HG), and Bessel-Gaussian (BG) modes, are described in more detail before linking a subclass of LG modes, called orbital angular momentum modes, as our bases of choice to use for quantum information applications.

The basics of quantum mechanics and how it can be used for quantum information theory is applied while consistently considering both polarisation and orbital angular momentum as the bases. This is expanded into a discussion about quantum entanglement and how to represent entangled states as vectors and density matrices.

Common quantum concepts such as mutually unbiased bases, fidelity, the No-Cloning theorem and the partial trace are discussed before going into multiple information measures in preparation for the final chapter on QKD.

1.1 Spatial Basis

1.1.1 Light

The word spatial represents everything that forms part of the transverse spatial profile of the wavefront of propagating light and its properties. Light consists of electric and magnetic fields that oscillate in orthogonal directions. The presence of electric and magnetic fields and the wave-like nature of light immediately imply the relevance of the four Maxwell equations [22]. The four laws are the divergence and curl of both the electric and magnetic field vectors and are given as:

$$\begin{aligned}
\nabla \cdot \vec{E} &= \frac{\rho}{\epsilon_0}, \\
\nabla \cdot \vec{B} &= 0, \\
\nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t}, \\
\nabla \times \vec{B} &= \mu_0 \left(\vec{J} + \epsilon_0 \frac{\partial \vec{E}}{\partial t} \right),
\end{aligned} \tag{1.1}$$

where $\vec{E}$ and $\vec{B}$ are the usual electric and magnetic field vectors, ρ and $\vec{J}$ are the charge and current densities and μ_0 and ϵ_0 are the permitivity and permeability constants of free space. To find the wave equations for electromagnetic waves we consider the case where there are no currents or charges present [22]. This sets both ρ and $\vec{J}$ to zero:

$$\begin{aligned}
\nabla \cdot \vec{E} &= 0, \\
\nabla \cdot \vec{B} &= 0, \\
\nabla \times \vec{E} &= -\frac{\partial \vec{B}}{\partial t}, \\
\nabla \times \vec{B} &= \epsilon_0 \mu_0 \frac{\partial \vec{E}}{\partial t}.
\end{aligned} \tag{1.2}$$

Taking the curl of the last two equations,

$$\begin{aligned}
\nabla(\nabla \cdot \vec{E}) - \nabla^2 E &= -\frac{\partial}{\partial t} \nabla \times \vec{B}, \\
\nabla(\nabla \cdot \vec{B}) - \nabla^2 B &= \epsilon_0 \mu_0 \frac{\partial}{\partial t} \nabla \times \vec{E},
\end{aligned} \tag{1.3}$$

and taking into consideration the two divergence equations above, the first terms in both equations are equal to zero. Using the curl equations and simplifying gives the wave equations [22]

$$\begin{aligned}
\left(\nabla^2 - \mu_0 \epsilon_0 \frac{\partial^2}{\partial t^2} \right) \vec{E} &= 0, \\
\left(\nabla^2 - \mu_0 \epsilon_0 \frac{\partial^2}{\partial t^2} \right) \vec{B} &= 0.
\end{aligned} \tag{1.4}$$

Both of these equations are known as the Maxwell wave equations and they are functions of position and time. Separation of variables allows us to isolate the position dependence. Let $U(\vec{r},t)$ represent the electric field of propagating light, and assume

$$U(\vec{r},t) = A(\vec{r})T(t). \tag{1.5}$$

When this is substituted into the wave equation, while using $c = \frac{1}{\sqrt{\mu_0\epsilon_0}}$ we get:

$$\begin{aligned} T(t)\nabla^2 A(\vec{r}) - \mu_0\epsilon_0 A(\vec{r})\frac{\partial^2}{\partial t^2}T(t) = 0, \\ \frac{c^2\nabla^2 A(\vec{r})}{A(\vec{r})} = \frac{\frac{\partial^2}{\partial t^2}T(t)}{T(t)}, \end{aligned} \tag{1.6}$$

where the equality statement between two partial derivatives, one in terms of position and one in terms of time, imply that they must be equal to some constant. Here the constant is the negative of the angular frequency squared, giving the position solution, which is the Helmholtz equation

$$\nabla^2 A(\vec{r}) = -k^2 A(\vec{r}), \tag{1.7}$$

where the constant $k = \frac{\omega}{c}$ is the wave number [23]. c is the speed of light and ω is the angular frequency. The last step is to use the paraxial approximation and to derive the paraxial Helmholtz equation, which is used to describe the behaviour of paraxial laser light [24]. The paraxial approximation restricts the variation of the field in the transverse direction as the light propagates in the z-direction [23]. For small angles, such that the angles almost point in the propagation direction, the spatial properties of laser light do not change noticeably, with distance.

We assume the wave from above is modulated by some complex envelope that changes with propagation direction as the light propagates:

$$U(\vec{r}) = U_0(\vec{r})\exp(-ikz). \tag{1.8}$$

If this complex envelope $U_0(\vec{r})$, by the paraxial approximation, is supposed to barely change then the paraxial approximation implies that this envelope must not change for at least a full wavelength [23], meaning

$$\delta U_0 = \frac{\partial U_0}{\partial z}\delta z \ll U_0. \tag{1.9}$$

This equation says that the change in the complex envelope is much less than the envelope itself multiplied by some propagation distance δ_z, which implies that there is almost no change over δz. If we let δz be of the order of one wavelenght λ and since the wave number k is related to the wavelength by $k = \frac{2\pi}{\lambda}$ we now get:

$$\frac{\partial U_0}{\partial z} \ll U_0/\lambda \sim kU_0. \tag{1.10}$$

Expanding $\nabla^2 U(\vec{r})$, which now has a transverse and longitudinal component, and applying the paraxial approximation by omitting terms that have negligible effect compared to the dominating terms [23], we finally arrive at the paraxial Helmholtz equation [23]. This is done by expanding the laplacian of the complex amplitude

$$\nabla^2 = \nabla_\perp^2 + \partial_z^2, \tag{1.11}$$

where the second order partial derivative of the complex amplitude $\partial_z^2 U(\vec{r})$ can be omitted, since the second order partial derivative is much smaller than the first order partial derivative as can be seen through

$$\frac{\partial^2}{\partial z^2}A \ll k\frac{\partial}{\partial z}A \ll kA^2, \tag{1.12}$$

which follows from equation 1.10 above. Simplifying leaves us with the final result of

$$\nabla^2 U(\vec{r}) - 2ik\partial_Z U(\vec{r}) = 0. \tag{1.13}$$

1.1.2 The Gaussian Beam

One solution to the paraxial Helmholtz equation is the gaussian beam. The intensity profile of such beams follows the statistical gaussian distribution where most of the photons are in the center of the beam and as you move radially away this amount decreases. The gaussian beam intensity profile can be written as:

$$I(r) = I_0 \exp\left(-\left(\frac{r}{\omega(z)}\right)^2\right), \tag{1.14}$$

where I_0 is the intensity amplitude, r is the radial distance from the propagation axis and $\omega(z)$ is the beam radius at a particular propagation distance z, which is expressed as

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z - z_0}{z_r}\right)^2}, \tag{1.15}$$

where z_0 is the position along the propagation direction where the beam radius is at a minimum, ω_0 is the minimum beam radius called the beam waist, and z_r is called the Rayleigh range and specifies the z-propagation distance at which the transverse area of the beam is double what it was at its smallest, namely where the beam radius was ω_0. The Rayleigh range is calculated using

$$z_R = \frac{\pi\omega^2}{\lambda}, \tag{1.16}$$

where λ is the wavelength. These quantities are important and used in the descriptions of the more exotic modes of light.

1.1.3 Laguerre-Gaussian Modes

LG modes, illustrated in Figure 1.1, are dependent on two indices: the topological charge ℓ, and a p number called the radial index. ℓ determines the amount of orbital angular momentum (OAM) intrinsic to the mode and p determines the number of radial rings. They are called the azimuthal and radial indices respectively. LG modes are modes of light, since they are solutions to the paraxial Helmholz equation, specifically solutions in cylindrical coordinates. LG modes are defined using the following function [25]:

$$LG_p^\ell(\rho, \phi, z) = \frac{\omega_0}{\omega(z)} \sqrt{\frac{2p!}{\pi(|\ell| + p))!}} \left(\frac{\sqrt{2}p}{\omega(z)}\right)^{|\ell|} L_p^\ell \left[2\left(\frac{\rho}{\omega(z)}\right)^2\right]$$
$$\times \exp[i(2p + |\ell| + 1)\zeta(z)] \exp\left[-\left(\frac{\rho}{\omega(z)}\right)^2\right] \exp\left[-\frac{ik\rho^2}{2R(z)}\right] \exp[-i\ell\phi] \exp[-ikz], \tag{1.17}$$

where ω_0 is the beam radius at the focus, $\omega(z)$ is the beam waist at propagated position z and $\zeta(z) = \arctan\left(\frac{z}{z_R}\right)$. $R(z)$ is the radius of curvature of the wavefront at propagation distance z, k is the magnitude of the wave vector and ρ, z and ϕ are the cylindrical coordinates. Lastly, L_p^ℓ is the generalized Laguerre polynomial

for indices p and ℓ.

Laguerre-Gaussian beams do not only carry an intensity distribution, but a phase as well. This is true for all propagating beams of light and implies that the LG mode function, which gives the field of the beam, can be divided into an amplitude and phase term. Taking the modulus squared of the beam field gives the intensity

$$I(\rho, \phi, z) = |LG_p^\ell(\rho, \phi, z)|^2. \tag{1.18}$$

The complex exponential factors carry the phase information of the beam and it is specifically the $\exp[i\ell\phi]$ factor that determines the amount of times the phase goes from 0 to 2π.

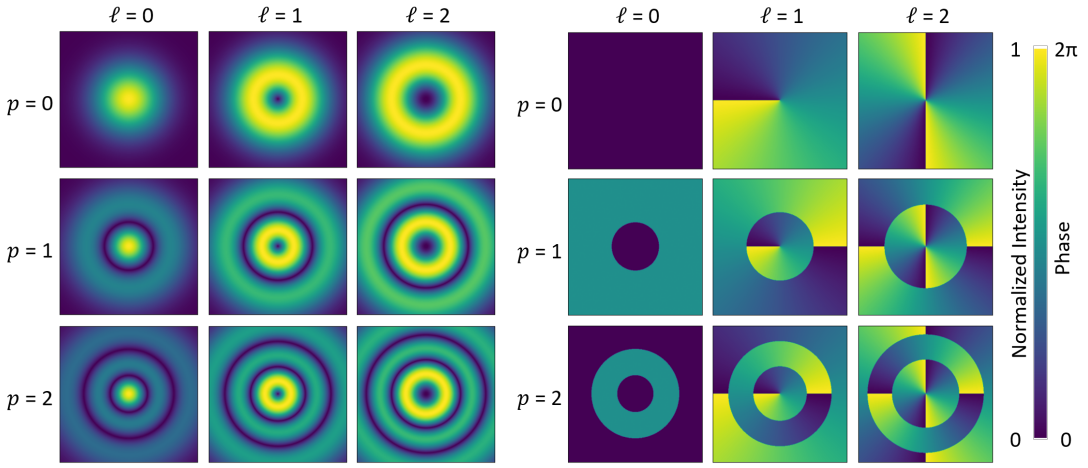

FIGURE 1.1: Laguerre-Gaussian modes at varying ℓ and p parameters. Left: Intensity. Right: Phase.

1.1.4 Hermite-Gaussian Modes

Another set of solutions to the paraxial wave equation, this time in cartesian coordinates x and y are called the Hermite-Gaussian modes [25]. Decomposing or factoring a paraxial beam into two separate factors, one a function of x and the other a function of y, is how these solutions or modes are found. HG modes can be expressed as

$$\begin{aligned} HG_{nm}(x, y, z) = \frac{1}{\omega(z)} \sqrt{\frac{2^{1-n-m}}{\pi n! m!}} H_n\left(\frac{\sqrt{x}}{\omega(z)}\right) H_m\left(\frac{\sqrt{y}}{\omega(z)}\right) \\ \times \exp[i(n+m+1)\zeta(z)] \exp\left[-\left(\frac{\rho}{\omega(z)}\right)^2\right] \exp\left[-\frac{ik\rho^2}{2R(z)}\right] \exp[-ikz]. \end{aligned} \tag{1.19}$$

Here the positive integers n and m spreads the modes out horizontally and vertically, in a grid-like pattern as in Figure 1.2, and are the mode orders in the x and y directions respectively. The H_n and H_m functions are the Hermite polynomials of order n and m, respectively.

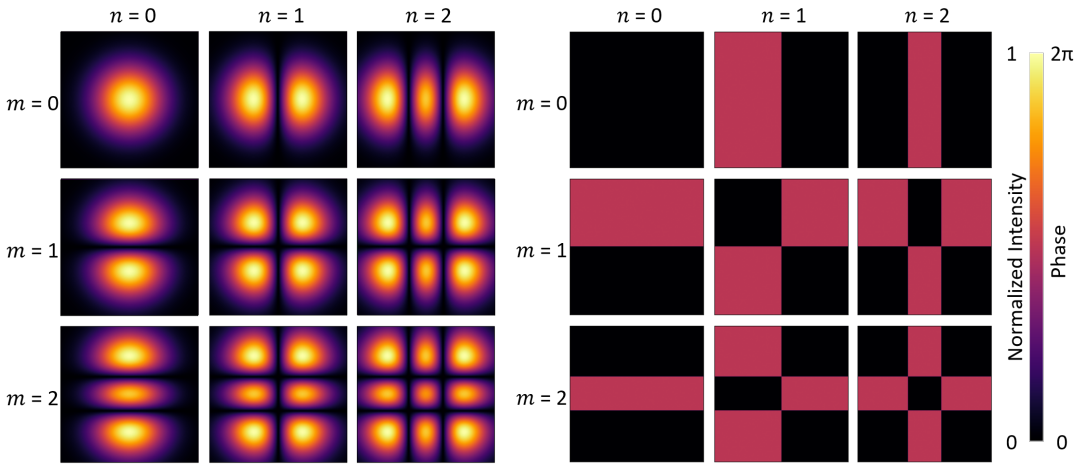

FIGURE 1.2: Hermite-Gaussian modes at varying n and m parameters. Left: Intensity. Right: Phase.

The Hermite-Gaussian modes are important as the superposition of two LG modes at $p = 0$ and equal, but opposite signs, of topological charge is a Hermite-Gaussian.

1.1.5 Bessel-Gaussian Modes

Bessel-Gassian modes, illustrated in Figure 1.3, are special solutions, insofar as they are exact solutions to the Helmholtz equation, and not the paraxial Helmholtz equation, in cyllindrical coordinates [25]. These modes are determined by two parameters as usual, but here the topological charge is used again. The other parameter is k_r, which is the transverse wave vector component that determines the overall size of the mode, by specifying the transverse momentum. Bessel-Gaussian beams are given by

$$BG(\rho, \phi, z) = BG_0 J_\ell(k_r \rho) \exp\left[-\left(\frac{\rho}{\omega_0}\right)^2\right] \exp[i\ell\phi], \tag{1.20}$$

where J_ℓ are the ℓ^{th} Bessel functions and BG_0 is the field amplitude. Bessel-Gaussian beams are interesting in that they are self-healing, even at long distances [26], and that entanglement is robust to loss of light, if the propagation direction is partially obstructed [27] and measurements take place in the Bessel basis. This has the consequence that Bessel-Gaussian beams are an interesting family of modes

to use in quantum applications, however, we will mostly care about the Laguerre-Gaussian and Hermite-Gaussian mode families from now on.

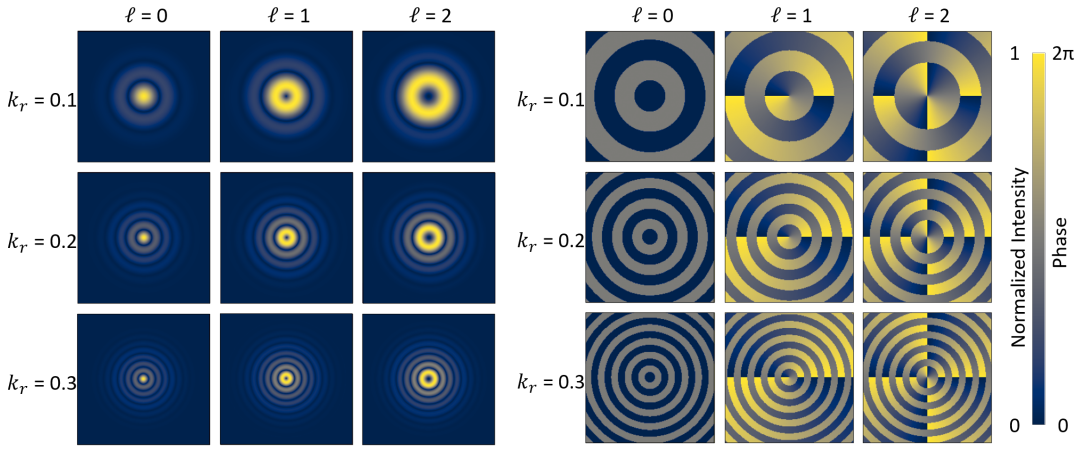

FIGURE 1.3: Bessel-Gaussian modes at varying ℓ and k_r parameters. Left: Intensity. Right: Phase.

1.2 Quantum Information

To harness the processing power made possible by quantum mechanics requires that we convert the usual on or off bits, that we use for example in binary computation, to two-level quantum states that are called qubits. Superconducting qubits, for example are used in superconducting quantum computers [28]. We can use the modes of light discussed in order to build up 2-dimensional and higher-dimensional bases that can be used to represent information, which is now called Quantum Information.

1.2.1 Qubits, Qutrits and Qudits

Qubits are superpositions of the usual on or off states, which are represented by 1's and 0's, that can be expressed using bra-ket notation as is standard for quantum mechanics:

$$|q\rangle = a|0\rangle + b|1\rangle. \tag{1.21}$$

Qubits form part of the foundation of everything quantum information has to offer. They are also fundamental to the operation of many applications such as quantum computing [29] and quantum key distribution [6].

The word superposition implies that the system is in both states $|1\rangle$ and $|0\rangle$ simultaneously. Measuring the quantum system will cause this superposition to collapse

probabilistically to one of the two possibilities in the qubit. These probabilities are calculated using the usual quantum mechanics projections, which are calculated directly from simply taking the square of the magnitude of inner products

$$P = |\langle 0|q\rangle|^2, \tag{1.22}$$

where here the probability that the qubit collapses to state $|0\rangle$ after measurement is given. It is important that all probabilities of all possibilities add up to unity. This condition is called the conservation of probability and can be expressed as $|a|^2 + |b|^2 = 1$.

1.2.2 Polarisation

All propagating electromagnetic radiation consists of oscillating electric and magnetic fields and the direction of oscillation of the electric field defines the polarisation direction. If the propagation direction is in the z-direction, then essentially all of the oscillation occurs in the xy-plane. This implies that polarisation can be in two orthogonal directions, which can be utilized as a 2-dimensional basis. A common way to use polarization as a 2-dimensional basis, is to use circularly polarised light. This is the polarisation state where the electric field vector rotates, at a constant rate, about the propagation direction, while oscillating. There are two directions for circularly polarised light, namely right circular $|R\rangle$ and left circular $|L\rangle$ polarised light as illustrated in Figure 1.4.

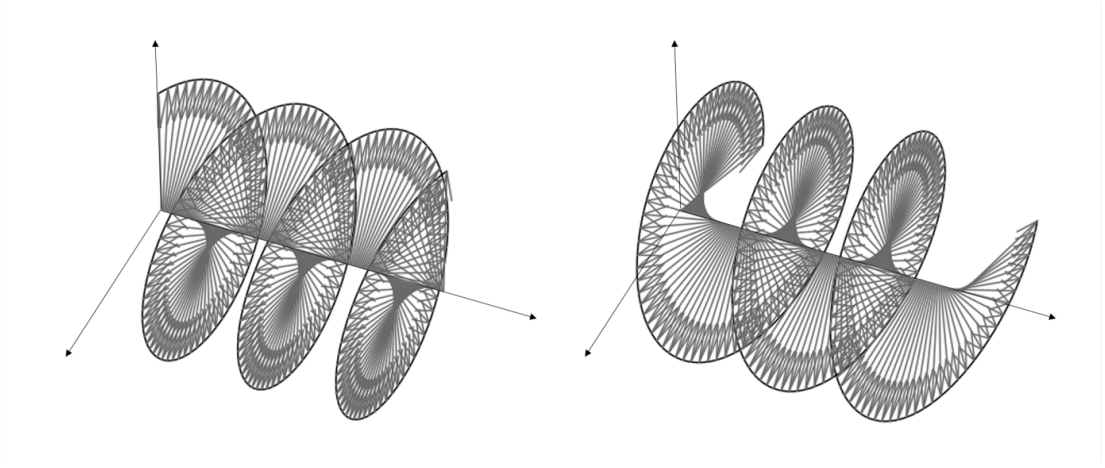

FIGURE 1.4: Left $|L\rangle$ and right $|R\rangle$ circularly polarized light. The electric field vector rotates as it oscillates because of the phase difference between the two linear polarizations that comprise it.

The other two options for a basis would be to combine horizontal $|H\rangle$ and vertical $|V\rangle$ polarisation or diagonal $|D\rangle$ and anti-diagonal $|A\rangle$ polarisation. Both choices constitute two-dimensional polarisation basis of linear polarisation states. Linear polarisation is when the electric field vector oscillates, without rotating, in the xy-plane of the propagating light. The horizontal and vertical polarisation basis is shown in Figure 1.5.

Any polarisation state can be written as linear combinations of the two basis elements from one of the three bases mentioned. For example, elliptical polarization can be written in terms of linear polarization and visa versa. Two linear polarization states that are added together, but with a phase difference between them, will be elliptical polarization. At specific angles, where the contributions of both linear polarization states are equal, circular polarization emerges. In fact any polarization state can be expressed as a linear combination of any two orthogonal polarizations.

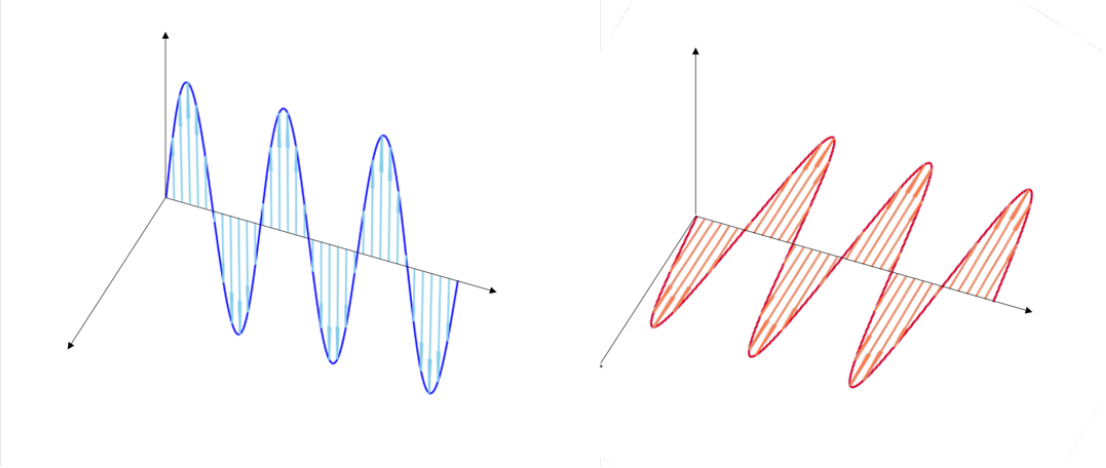

FIGURE 1.5: Vertical $|V\rangle$ and horizontal $|H\rangle$ polarization. The electric field vector oscillates only in the yz- or xz-planes.

The idea of qubits can be extended to the polarization degree of freedom of light, where polarization states are now described by superpositions of two orthogonal polarizations. We will choose our standard basis in this case to be the two orthogonal states right $|R\rangle$ and left $|L\rangle$ circularly polarized light. The standard basis is a basis of elements, in this case vectors, whose elements are all zero, except for one particular element so that all elements are orthogonal with respect to each other. Representing a qubit in another degree of freedom that is not the computational basis, the basis consisting of simple bit values as basis elements, is the most basic form of encoding information into physical properties, in this case the physical

properties of light like polarisation and orbital angular momentum. A photon in a superposition of right and left circularly polarised light is given by

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|R\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|L\rangle, \tag{1.23}$$

where the θ angle determines the weightings of the two basis states, which together should add up to 1, after calculating the usual probability values. The $e^{i\phi}$ is the phase factor that induces a relative phase difference between the two basis states. Depending on the values of these angles, any polarization state can be achieved. For example, if $\theta = 0$ and $\phi = 0$, then the superposition expression results in horizontal $|H\rangle$ polarization. All the combinations of the above quantum state can be visualised using Figure 1.6, which is the Poincaré sphere or the Bloch sphere used for polarisation, where the poles of the sphere are the two orthogonal basis states and all states pointing to the edge of the sphere are some linear combination of the two at some relative phase angle.

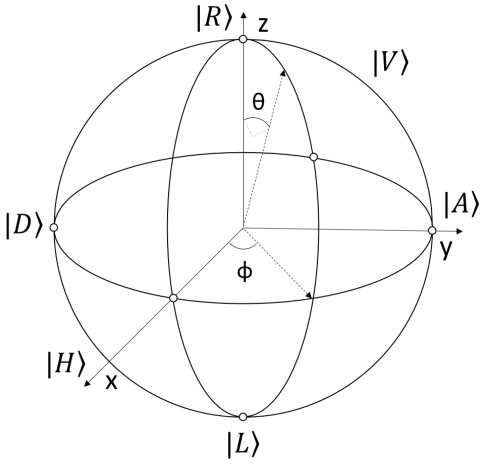

FIGURE 1.6: The Poincaré sphere - The standard basis states are at the poles of the sphere. Linear combinations that are equiprobable, but with different relative phase angles are on the equator, which is where the linear polarization states can be found. The points between the poles and the equator are elliptical polarization states.

1.2.3 Orbital Angular Momentum

Light can carry angular momentum that is intrinsic to the direction and rate of rotation of the electric field vector, which is called orbital angular momentum (OAM) and is indicated by the topological charge ℓ. The light field carrying OAM contains a phase factor $e^{i\ell\phi}$ that describes how light can "twist". OAM carrying

light has an angular momentum of $\ell\hbar$ per photon and undergoes a phase variation of exactly $\ell \times 2\pi$ times about the azimuth per wavelength λ. This is indicated in Figure 1.7.

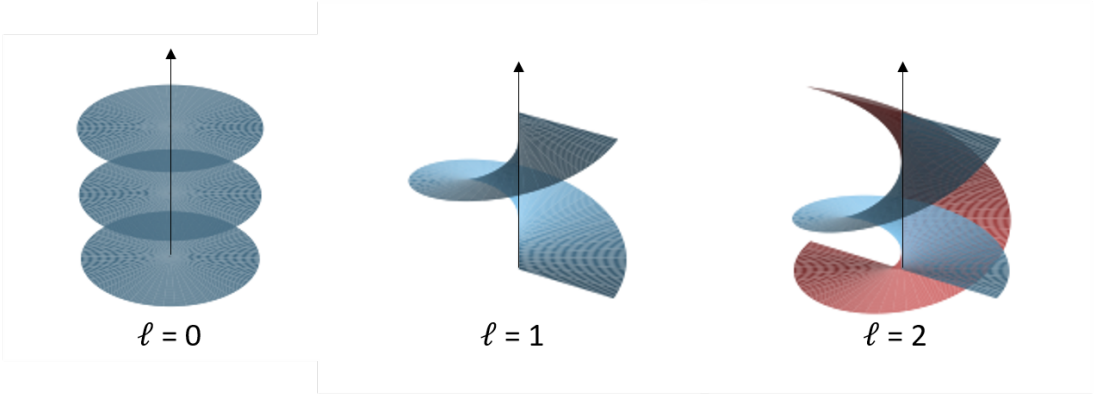

FIGURE 1.7: Illustration of how an increase of the topological charge means that more phase variations occur within one wavelength. The arrow points in the direction of propagation.

OAM supplies a theoretically infinite basis, since the topological charge can theoretically take any integer number.

It is a incorrect to think that for higher topological charges, the amount of twisted wavefronts over one full wavelength increases as in Figure 1.8.

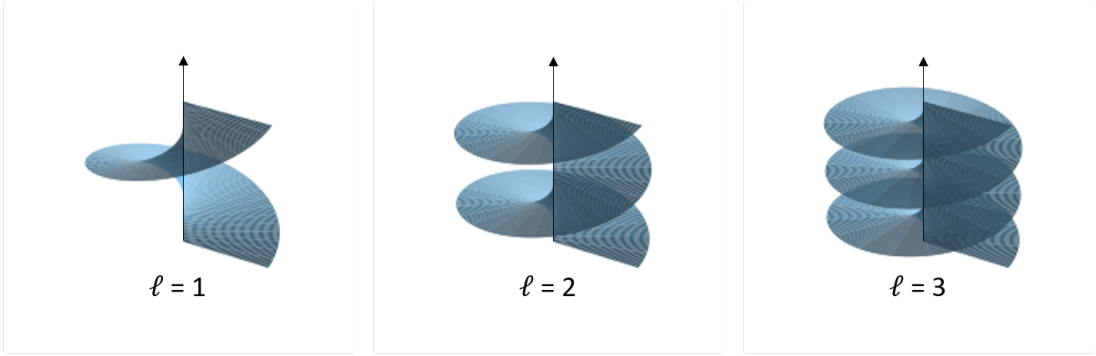

FIGURE 1.8: Misconception of how the number of twists or rotations the wavefront undergoes increases, as the topological charge is increased. The arrow points in the direction of propagation.

Despite the increase in the amount of "twists" or variations of phase per wavelength by an integer amount, the phase does not vary the $\ell \times 2\pi$ about the azimuth per wavelength. Instead what is now being considered is actually an integer amount of wavelengths, not an increase in OAM.

We could extend the idea of qubits to the spatial basis of light as well by considering a superposition between two OAM modes defined by their individual topological charges. Just like for polarization, we can write the general OAM state as a two-dimensional qubit state that also includes a phase term. These two-dimensional states can also be represented on the Bloch sphere (Figure 1.9) [30]. We consider LG modes where the radial index $p = 0$, which gives

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\ell_1\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|\ell_2\rangle. \tag{1.24}$$

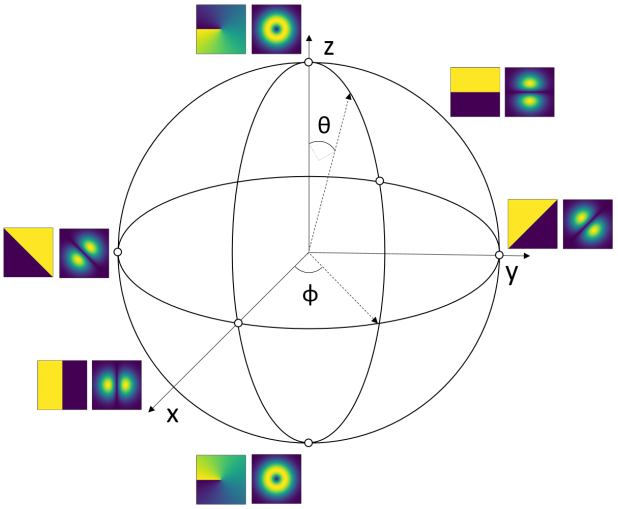

FIGURE 1.9: The OAM Bloch sphere - The standard basis states are at the poles of the sphere. Linear combinations of OAM charges on the equator implies that both standard basis states are equiprobable and are the Hermite-Gaussian modes from before.

The idea of qubits can be further extended to higher dimensions. If d is the number of basis states required to express the d-dimensional quantum state, then the state is called a qudit. A special case of a qudit is the qutrit, which is just a three-level quantum system

$$|q\rangle = a|-1\rangle + b|0\rangle + c|1\rangle, \tag{1.25}$$

where the basis states can be substituted with topological charge values or any other degree of freedom, except polarization of course. A qutrit has the general form:

$$|q\rangle = a|\ell_1\rangle + b|\ell_2\rangle + c|\ell_3\rangle. \tag{1.26}$$

It becomes difficult to visualise higher-dimensional qudits, since illustrating higher-dimensional states on a higher-dimensional equivalent of the Bloch sphere is impossible to visualise. Using higher-dimensional states, however, have multiple advantages. Including more possibilities in one qudit, increases the amount of information that can be encoded in a single qudit, since encoding is no longer limited to "on-off" or "yes-no" conditions.

1.2.4 Quantum Entanglement

Quantum entanglement is the concept that two or more quantum systems, such as atoms and photons, are intrinsically linked somehow to the extent that if one of the states' superposition was collapsed by measuring an observable, that the other's quantum state would also collapse, but to a predetermined state. This happens even when the two systems are spatially separated by millions of kilometres. This exact affect is what is described by the EPR-paradox [31] and is what Einstein referred to as "spooky action at a distance". For example: measuring system one as a $|1\rangle$ would immediately mean that system two is also measured as $|1\rangle$. We can represent this quantum entangled state as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{1.27}$$

The first number in both of the terms is for one of the two quantum systems, and by extension the second number indicates the second quantum system. Quantum entangled states cannot be written as a product of two constituent states. In other words, quantum entangled states are not factorisable. The most common example of two-dimensional entanglement are the four maximally entangled Bell states. All four Bell states together form the set

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).
\end{aligned} \tag{1.28}$$

All four of these states cannot be written as a product of its constituent parts, that is, they are not separable and therefore entangled. The separability condition for

separable states requires that the system state be written as the tensor product of two separate states

$$|\Psi\rangle = \psi_1 \otimes \psi_2. \tag{1.29}$$

This separability condition is for pure quantum states only. Mixed quantum systems also exist, but these will be expanded upon below.

The tensor product of two or more vector states is used to create a compound vector state of the two or more individual parts. The vectors are longer, containing all possible combinations of the constituent states as vector elements. For entangled quantum systems, it is impossible to separate the states representing each individual part, meaning we cannot write the entangled state as a tensor product of its constituents.

Since we can choose our standard basis to be anything, including the computational, polarization, or spatial basis of light, we can now write entangled quantum systems in any basis. Considering a pair of quantum entangled photons we can write entanglement using the polarization and spatial degrees of freedom in a similar way as before only now with the new basis elements substituted in:

$$\begin{aligned} |\Phi_P\rangle &= \frac{1}{\sqrt{2}} \left(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B \right), \\ |\Phi_S\rangle &= \frac{1}{\sqrt{2}} \left(|\ell_1\rangle_A |\ell_1\rangle_B + |\ell_2\rangle_A |\ell_2\rangle_B \right). \end{aligned} \tag{1.30}$$

Here the subscripts A and B indicate photon A and B in the entangled pair. If photon A were to be measured as a $|H\rangle$ ($|\ell_1\rangle$), then photon B would be measured as a $|H\rangle$ ($|\ell_1\rangle$) state as well, 100% of the time, regardless of the physical separation between the two photons. Entanglement does not have to be in only two dimensions. The OAM basis is theoretically infinite and two photons entangled in orbital angular momentum can be entangled for many OAM charges, which means we can write the entanglement state for two photons as follows

$$|\psi\rangle = \sum_{\ell} c_i |\ell_i\rangle | - \ell_i\rangle, \tag{1.31}$$

where as usual the conservation of probability requires that the sum of eigenvalue magnitudes equal 1: $|c_1|^2 + |c_2|^2 + ...|c_3|^2 = 1$.

Entanglement can also exist across many degrees of freedom. The best example to use is the case of spin-orbit coupled quantum systems where the entanglement is now between OAM charges and the spin polarization state. Entanglement states are written similarly, but now one photon is represented by only its polarization and the other by its topological charge as

$$|\psi\rangle = a|\ell\rangle_A|R\rangle_B + b|-\ell\rangle_A|L\rangle_B. \tag{1.32}$$

.

1.2.5 Density Matrices

A useful way in which to represent quantum entangled systems is to use the density matrix representation. If $|\psi\rangle$ is our quantum entangled state or system, then the density matrix ρ is found using the outer product

$$\rho = |\psi\rangle\langle\psi|. \tag{1.33}$$

When the state is described by only this outer product, the state is known as a pure state. If any terms were to be added to this expression that would alter its shape, then the density matrix would acquire noise and become mixed. Whenever a quantum state becomes maximally mixed, the entanglement is lost completely as the entangled systems now become a statistical mixture of separate quantum systems. The purity of a state density matrix p, ranging from 0 to 1, indicates how pure the quantum state is and is calculated using the trace

$$p = Tr(\rho^2), \tag{1.34}$$

which is the sum of all diagonal elements of the density matrix squared. A purity of 1 indicates a pure state.

An example of a pure state with some noise added to it, is the case of the isotropic density matrix. This class of density matrices can be used to represent bipartite quantum entangled systems [32] by way of

$$\rho = p|\psi\rangle\langle\psi| + \left(\frac{1-p}{d^2}\right) I_{d^2}. \tag{1.35}$$

The above expression is the expression for the isotropic density matrix, where p is the purity and d is the dimension of the system's individual parts, namely the

amount of elements in the chosen basis. I_{d^2} is the d^2 dimensional identity matrix. The word isotropic used to describe this density matrix, refers to the noise model. The noise is isotropic, constant, or is uniform in its contribution throughout the system.

Another example of mixed density matrices is the case of bipartite Werner states, that can also be used to describe bipartite entangled quantum states or to represent noisy quantum channels [33]. These states are inherently mixed, especially at higher dimensions. Werner states are made up of two contributing matrices, the symmetric and anti-symmetric parts, where the two individual parts are now weighted by a value called the symmetric weighting p_{sym}. The symmetric and anti-symmetric parts are similar to the triplet and singlet states from quantum mechanics or the four Bell states from entanglement in that under the permutation operator the symmetric parts do not undergo a sign change. This is not true for the anti-symmetric part. Werner states have the form

$$\rho = p_{sym}\frac{2}{d^2+d}P_{Sym} + (1-p_{sym})\frac{2}{d^2-d}P_{as}, \tag{1.36}$$

where d is still the dimension and P_{sym} and P_{as} are the symmetric and anti-symmetric matrix parts of the full density matrix, both of which depend on the permutation operator P [33]. The two matrices and permutation operator can be written as

$$\begin{aligned} P_{as} &= \frac{1}{2}(1-P), \\ P_{sym} &= \frac{1}{2}(1+P), \\ P &= \sum_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|. \end{aligned} \tag{1.37}$$

where the above definition is only valid, if the quantum state density matrix is invariant under the unitary operator $U \otimes U$, for some unitary operation U [33], namely

$$\rho = (U \otimes U)\,\rho\left(U^\dagger \otimes U^\dagger\right). \tag{1.38}$$

General mixed density matrices can be thought of as a set of many quantum systems, which can be entangled. Some mixed density matrices represent maximally mixed states and some are only partially mixed. As long as the state density

matrix is an ensemble of many pure states that are not necessarily related or entangled with each other, then the system is in a mixed state. Mixed states of many photon pairs, for example, would cause many detections, but where only a percentage of the pairs are actually entangled. Writing the general mixed density matrix of many systems is done by using a sum of pure state outer products, where each pure state can also have some noise added to it

$$\rho = \sum_{k=1}^{N} p_k |\psi_k\rangle\langle\psi_k|. \tag{1.39}$$

Density matrices can only truly represent bipartite quantum entangled states when they are positive semi-definite, are hermitian and have been normalized to have a trace of unity. To be positive semi-definite implies that all eigenvalues of all possible eigenmodes are non-negative and real. The trace of unity is related to the conservation of probability, since the trace, which is the sum of all diagonal elements, is the sum of all eigenvalues where eigenvalues are the probabilities in the case of density matrices. Hermitian matrices are matrices such that they are equal to their own complex conjugate transpose. When a density matrix adheres to all these requirements, then the matrix is considered to represent a bipartite quantum entangled quantum state. If a density matrix does not have a trace of unity, it can be normalized simply by dividing the entire matrix by its own trace.

Calculating the probability of observable measurements, which is still a projective measurement as for the vector representation, must now be done using matrix multiplication. This projective measurement is the mutual overlap between the observable matrix operator and the density matrix itself and is calculated similar to purity. Let A be the observable operator matrix, then:

$$P = Tr(\rho A). \tag{1.40}$$

A value of 1 indicates that the two states are identical and 0 indicates that the two state density matrices are completely orthogonal. The higher the overlap between the two matrices, the higher the probability of the observable measurement.

Linear entropy is another measure of the purity of a density matrix, the higher the value, the more mixed the state density matrix is [34] Linear entropy is calculated using

$$\begin{aligned} S &= 1 - Tr(\rho^2), \\ S &= 1 - p. \end{aligned} \tag{1.41}$$

Considering the case of quantum photon states, the operator matrices are called analysers and are usually encoded on the SLM screens, which is then used to modulate the spatial basis of light.

1.2.6 Partial Trace

The overwhelming majority of density matrices that are important to the experimental part will be bipartite entangled quantum systems. These density matrices can be represented by ρ_{AB}, where A and B indicate which of the two parts belonging to the joint quantum system we consider. ρ_A and ρ_B would be the density matrices describing the two smaller constituents of the larger entangled system. Taking the partial trace of the entangled state density matrix makes it possible to find either ρ_A or ρ_B, writing a quantum state that resides in d^2-dimensional subspace into a density matrix that resides in a d-dimensional subspace. This is referred to as "tracing out" the unwanted parts and is defined as [30, 35]:

$$\begin{aligned} \rho_A &= Tr_B(\rho_{AB}), \\ \rho_A &= \sum_{i,j} r_i r_j^* \langle i_A | j_A \rangle | j_B \rangle \langle i_B |, \end{aligned} \tag{1.42}$$

where i and j are summation indices that sum over the amount of columns and rows in the density matrix. $|i\rangle$ and $|j\rangle$ are basis elements, that could be substituted with the computational basis elements, and B acts as the part of the density matrix that is being traced over. This is simplified further to

$$\begin{aligned} \rho_A &= \sum_{i,j} r_i r_j^* \delta_{ij} | j_B \rangle \langle i_B |, \\ \rho_A &= \sum_{i} |r_i|^2 | i_B \rangle \langle i_B |, \end{aligned} \tag{1.43}$$

after imposing the orthogonality of the basis states and now only summing over one of the indices after removing all terms that go to zero.

Consider for example the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$ [35]. This is a bipartite

entangled system, where one of the two contributing states can be found by tracing out the other one. In density matrix notation this matrix is given by

$$\rho_{AB} = |\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}\left((|0_A 0_B\rangle + |1_A 1_B\rangle)(\langle 0_A 0_B| + \langle 1_A 1_B|)\right). \tag{1.44}$$

We can now trace out one of the contributing parts

$$\begin{aligned} \rho_A &= \frac{1}{2}\left(|1\rangle\langle 1|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |0\rangle\langle 0|\langle 1|1\rangle\right), \\ \rho_A &= \frac{1}{2}(|1\rangle\langle 1| + |0\rangle\langle 0|), \end{aligned} \tag{1.45}$$

where ρ_A is the reduced density matrix describing the quantum state only associated to A.

1.2.7 Mutually Unbiased Bases

Mutually unbiased bases or MUBs are bases with an equal amount of basis elements, but if a basis was used to measure a specific state expressed in a different mutually unbiased basis, the result would be equal to unity divided by the amount of basis elements in each mutually unbiased basis.

The most simple example of this happens when we consider the computational basis $|1\rangle$ and $|0\rangle$. A typical MUB would be the Hadamard basis, where the two states making up the basis are $|+\rangle$ and $|-\rangle$. These two states are given by

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \\ |-\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \end{aligned} \tag{1.46}$$

where it is easy to see that if the probability of either state in the computational basis was to be calculated by using the Hadamard basis for example, that both states would have a probability of 0.5 each. For example

$$\langle 0|+\rangle = \frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle), \tag{1.47}$$

and since $|1\rangle$ is orthogonal to $|0\rangle$, this becomes

$$\langle 0|+\rangle = \frac{1}{\sqrt{2}}(1) = \frac{1}{\sqrt{2}}, \tag{1.48}$$

which becomes 0.5 after taking the modulus sqaured for probability.

Since the probability is exactly equal and add up to unity, it is impossible to confidently conclude that the system is either one of the possible states.

For two bases to be considered mutually unbiased they have to satisfy the following condition: let two sets of states in two separate bases be $\{a_1|\rangle, |a_2\rangle, ..., |a_d\rangle\}$ and $\{b_1|\rangle, |b_2\rangle, ..., |b_d\rangle\}$, then for these two bases to be mutually unbiased the following must hold [36]:

$$|\langle a_i|b_j\rangle|^2 = \frac{1}{d}, \tag{1.49}$$

for all i and j up to the dimension of the two bases, which is just the amount of states comprising both.

Applying the idea of MUBs to spatial modes of light, starting with two-dimensional polarization, there are three mutually unbiased bases. These bases can be any two-dimensional bases, as long as they satisfy the MUB condition. The three bases are as mentioned earlier: $|R\rangle$ and $|L\rangle$, $|H\rangle$ and $|V\rangle$ and finally $|D\rangle$ and $|A\rangle$ constitute the choice of three mutually unbiased bases. The same can be applied to the OAM modes on the Bloch sphere.

If we go back to the general superposition state used for spatial modes, we can see that the four MUBs correspond to phase angles of 0, $\frac{\pi}{2}$, π and $\frac{3\pi}{2}$. These angles do not correspond to the polarization angles, since they are only the phase angles in the state expression.

As the dimension is increased from two-dimensional to high-dimensional quantum systems, the amount of MUBs increase. There is a way to find these bases that involves using either the Weyl or high-dimensional Hadamard matrices [37]. The concept of mutually unbiased bases will be important later.

1.2.8 Fidelity

A measure to calculate how similar two separate quantum states are, is to use the concept of Fidelity. Mutual overlap gives an indication of how similar two quantum density matrices are, but fidelity is a number that gives an indication of the probability that the one state can be considered to be the state under consideration. Experimentally, the higher the fidelity, the more likely it is for the

quantum state to be representative of the experimental quantum state. Fidelity is written either as a number between 0 and 1 or as a percentage and is calculated using [38]:

$$F(\rho,\sigma) = \left(Tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2, \tag{1.50}$$

where ρ and σ are the two states under consideration.

1.2.9 No-Cloning Theorem

Quantum information cannot be cloned without introducing noise into the quantum system [30]. When entanglement is considered, this implies that entanglement is lost when attempts are made to copy a quantum state. If we were to consider three parties Alice, Bob and Eve where Alice sends Bob a state density matrix and Eve tries to eavesdrop, then she would not be able to completely copy the state without alerting Bob to what she was attempting. The no-cloning theorem restricts the fidelity at which Bob measures his state and the cloning fidelity of Eve's state. The cloning fidelity here is the similarity between the original sent density matrix and the density matrix that Eve tries to reconstruct. This theorem is the entire reason quantum cryptography protocols are possible, which will be investigated later as an application of entanglement.

The proof of the no-cloning theorem is as follows [30]: assume that a linear copying operator exists that is able to copy the content of a quantum bit. If such an operator were to be applied to two qubit vector states, it must copy the state of the first vector state onto the second. This can be written as:

$$\begin{aligned} U|0\rangle_1|i\rangle_2 &= |0\rangle_1|0\rangle_2, \\ U|1\rangle_1|i\rangle_2 &= |1\rangle_1|1\rangle_2, \end{aligned} \tag{1.51}$$

where state $|i\rangle_2$ is the qubit, the first qubit will be copied to. Applying this operator to some unknown qubit state ψ, which has eigenvalues of α and β for states 0 and 1 we see:

$$\begin{aligned} U|\psi\rangle_1|i\rangle_2 &= \alpha U|0\rangle_1|i\rangle_2 + \beta U|1\rangle_1|i\rangle_2, \\ U|\psi\rangle_1|i\rangle_2 &= \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2 \neq |\psi\rangle_1|\psi\rangle_2. \end{aligned} \tag{1.52}$$

It is clear from the last line that the operator clearly has not copied the contents of qubit ψ onto state $|i\rangle_2$, as the state cannot be written as $|\psi\rangle_1|\psi\rangle_2$, since this would require factorizing an entangled state.

1.3 Information Measures

Knowing how to write entanglement and how to use quantum mechanics to the benefit of information theory is the first step, but it is as important to quantify the information contained within quantum and quantum entangled systems. The amount of information is generally measured in bits. Again, 1 bit of information is a yes or a no answer to a specific question or condition. This idea is now applied to quantum systems to compare how many bits of information we actually have available.

When it comes to information theory, a particular event that can occur at a certain probability can only supply information that is restricted by this probability. What this means is that, the less likely an event is to occur, the more information gained when it actually occurs. The simplest example would be a coin: if the coin was to land on heads many times in a row, where both events should happen with equal probability, the amount of information contained within the results of these events is large. It is immediately clear that the coin is weighted towards the one side.

There are a few measures of amount of information and they can all be visualised on a typical Venn-diagram (Figure 1.10). $H(X)$ and $H(Y)$ is the information entropy for the set of outcomes for events X and Y respectively. $I(X;Y)$ is the mutual or shared information contained in the intersection of the previous two entropies. $H(X,Y)$ is called the joint entropy and is simply the union of $H(X)$ and $H(Y)$. Finally the conditional entropies are the amount of information gained from event X or Y if event Y or X has either occurred or not.

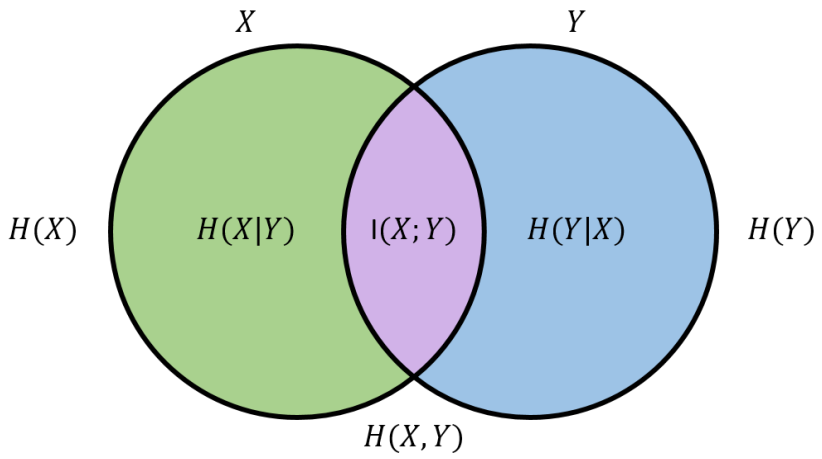

FIGURE 1.10: Information measure Venn-diagram - Illustrates the relationship between all the information entropy measures.

1.3.1 Entropy

Consider the scenario where some variable X can take many possibilities, each with their own probability of occurring. X can take $X = \{x_1, x_2, x_3, ...x_n\}$ where $P(x_i) = p_i$. Then the entropy of outcome $X = x_i$ is given by [30]:

$$H(X = x_i) = -\sum_{n}^{i=1} P(x_i) \log_2 P(x_i). \tag{1.53}$$

Entropy, in terms of quantum information, indicates the amount of memory a certain probable state requires to be stored. This means that the less likely the state is, the more memory it requires to be stored when it actually happens. This is why the equation depends on the probabilities $P(x_i)$. The above entropy equation is specifically called the Shannon entropy and is the classical form of entropy for information. The quantum version, called the Von Neumann entropy is where the probabilities are substituted for the eigenvalues of the state density matrix. Since the density matrix is normalized and positive semi-definite, the eigenvalues are just the diagonal elements, which causes these two entropies to be equivalent. λ_i is the i^{th} eigenvalue and the Von Neumann entropy is given by

$$H(\rho) = -Tr(\rho \log_2 \rho) = -\sum_{n}^{i=1} \lambda_i \log_2 \lambda_i, \tag{1.54}$$

where ρ is the state density matrix representing the system. The base of the log function determines the units of the entropy. If it is taken to the base of 2 it is

measured in bits and if it is calculated to the base of 10 the units are in Shannons.

1.3.2 Binary Entropy

Binary entropy is similar to entropy, however, the main difference comes from the amount of possible outcomes there are. The word binary refers to the fact that only two outcomes are possible. We will take these outcomes to be $X = 1$ and $X = 0$, where X simply indicates the unknown outcome. Consider the probability that X takes one of the two possibilities to be p. Thus, let $P(X = 1) = p$. The other possibility will have a probability of $1 - p$ by conservation of probability. Thus, this implies $P(X = 0) = 1 - p$. The binary entropy of such a scenario is given as:

$$h(X) = -p \log_2 p - (1 - p) \log_2 (1 - p). \tag{1.55}$$

Binary entropy is a number between 0 and 1, where a number of 1 indicates a scenario where both outcomes are equally possible. The relationship between binary entropy and probability is plotted in Figure 1.11.

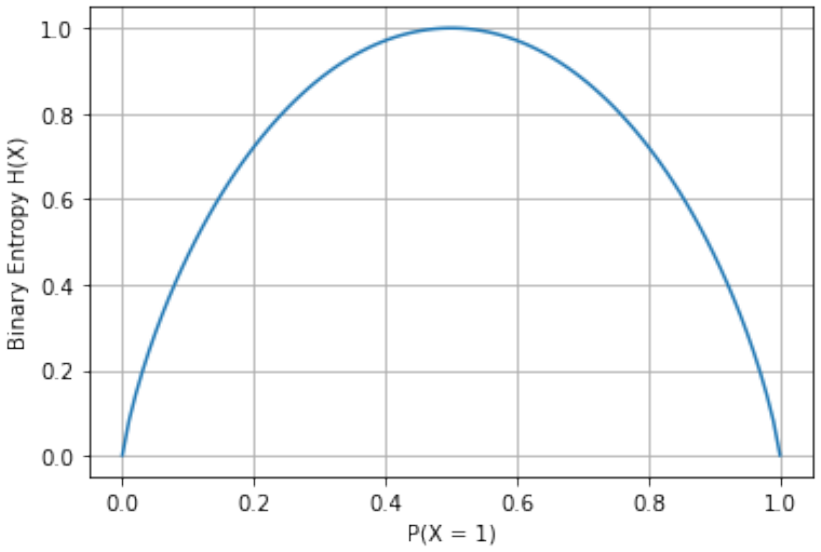

FIGURE 1.11: Binary entropy versus the probability that event X takes the result 1. Binary entropy maxes out when both outcomes are equally possible.

Binary entropy will be important later when we try and quantify the security of Quantum Key Distribution. These entropy measures are only usable for pure two-qubit quantum systems [30], which implies that we need to extend this concept to mixed states.

1.3.3 Concurrence

Concurrence is a number between 0 and 1 where a value of 0 indicates a maximally mixed statistical mixture and a value of 1 indicates maximally entangled states. Concurrence is defined as [30]:

$$C = \max\{\beta_1 - \beta_2 - \beta_3 - \beta_4, 0\}, \tag{1.56}$$

where the β values are the square root values of all the eigenvalues of the state density matrix $\rho_{AB}\tilde{\rho}_{AB}$ in decreasing order. State $\tilde{\rho}_{AB}$ is given by

$$\tilde{\rho}_{AB} = \sigma_{2_A} \otimes \sigma_{2_B} \rho^*_{AB} \sigma_{2_A} \otimes \sigma_{2_B}, \tag{1.57}$$

where the σ_{2_i} matrices are the Y Pauli operator matrices operating on part i. Once the concurrence has been calculated we can use it in the entanglement of formation [30] equation to get the mixed state equivalent of the von Neumann entropy used for pure qubits. The entanglement of formation is calculated using

$$E_F(\rho) = h\left(\frac{1 + \sqrt{(1 - C^2)}}{2}\right), \tag{1.58}$$

where the function $h(.)$ is just the binary entropy from before.

1.3.4 Conditional Entropy

Conditional entropy is calculated similarly to the usual individual entropies just like above, but now the probability is the conditional probability that is calculated using:

$$P(X|Y) = \frac{P(A:B)}{P(Y)}, \tag{1.59}$$

which is the probability of event X occurring based on knowledge of event Y occurring. The conditional entropy, by extension, is then the amount of information gained from event X after the information from event Y.

1.3.5 Joint Entropy

Joint entropy is calculated similarly to the usual entropy, but now the outcome probability depends on two or more outcomes. Event X and Y occur independently, but the probability that X or Y occur simultaneously is now denoted by

$P(X,Y)$ and it is this probability that must be used in the above entropy equation. The entropy for this is denoted similarly as $H(X,Y)$ and is the amount of information supplied when both events occur. It can be calculated by simply adding up the individual entropies

$$H(X,Y) = H(X) + H(Y). \tag{1.60}$$

1.3.6 Mutual Information

Using the entropy of two separate events and their joint entropy, the mutual information can now be defined. Mutual information is denoted by $I(X;Y)$ and is a measure of the shared information between the two systems. Mutual information also has an entropy associated with it that is called mutual entropy and is calculated as:

$$H(A:B) = H(A) + H(B) - H(A,B). \tag{1.61}$$

The amount of information two parties can share quantum mechanically is restricted, because of the inherent quantum uncertainty principles that apply. Consider the scenario where Alice prepares a state ρ_i at probability p_i and sends it to receiver Bob, then the probabilistic outcome of a measurement by Bob cannot supply more information than is allowed by this bound. This bound to the shared information is called the Holevo bound [30] and can be expressed as a typical upper bound in

$$I(A:B) \leq H(\rho) - \sum_{i=1}^{N} p_i H(\rho_i), \tag{1.62}$$

where $H(\rho)$ is just the von Neumann entropy of the density matrix and $H(\rho_i)$ is the von Neumann entropy of the density matrices that can be used to decompose the full state density matrix and are also the states that Alice sent to Bob, which form the linear combination of many entangled states. The p_i's are the probabilities that a specific ρ_i encoding a classical message is sent to Bob.

Chapter 2

Experimental Implementation

In order to make use of and exploit the quantum properties of quantum entanglement, a source of quantum entanglement is required. To entangle photons in the spatial basis, say in the orbital angular momentum degree of freedom, a non-linear crystal (NLC) can be used. This process is called spontaneous parametric down-conversion or SPDC and involves down-converting a pump beam into two signal and idler beams [39]. There are other sources of entangled photons, such as entangled photon sources (EPS) [40] (used here with QKD), but SPDC will be our generation method of choice. This process requires the use of non-linear crystals of which there are two common choices: periodically poled potassium titanyl phosphate (PPKTP) [41] and barium borate (BBO) [42] crystals.

Once the entangled photons have been generated, a method of spatial manipulation is required. There are multiple ways in which light can be spatially altered or shaped, that include SLMs which are used for any non-UV light for phase and complex amplitude modulation [43, 44], DMDs consisting of an array of tiny mirrors used mostly for classical light [45], Q-plates commonly used in spin-orbit coupling experiments [46] and spiral phase plates to add or subtract an integer amount of OAM to light that passes through [47].

There must also be a way to actually measure the entangled system. Quantum entangled photon states are measured using a concept called coincidence counting, where a coincidence counter and APDs are used in conjunction to turn photons into electric signals or voltages for detection. The counters are usually extremely precise, being able to distinguish individual photons arriving a few nanoseconds apart.

Chapter 2 includes a setup diagram with discussions of some of the most important components and concepts used to actually implement a quantum experiment.

Spontaneous parametric down-conversion as entangled state source is studied and elaborated on, before moving on to the measurements in the detection subsection. Overlap between modes in the two arms of the optical setup is discussed and linked to the spiral spectrum of the entangled state and is connected to coincidence counting as the method of choice to quantify this modal overlap. A brief investigation of the gating time, integration time and crystal temperature is included in order to get a good grasp of their affect on the coincidence measurements. Finally imaging using lenses in a 4F system and using SLMs to both shape light and do projective measurements is introduced as they both play a cardinal role in making optical quantum experiments possible.

2.1 Optical Setup

The optical setup can be divided into two main parts:

1 - Generation: This is where the pump laser is converted into entangled photons for exploitation later.

2 - Detection: This is where the photons are coupled into fibres and counted by a counter to quantify the entanglement. This is possible because of what is called projective measurements.

The lenses used for beam imaging and other optics will be discussed throughout this chapter. The optical setup as a schematic with most of the mirrors omitted is illustrated in Figure 2.1.

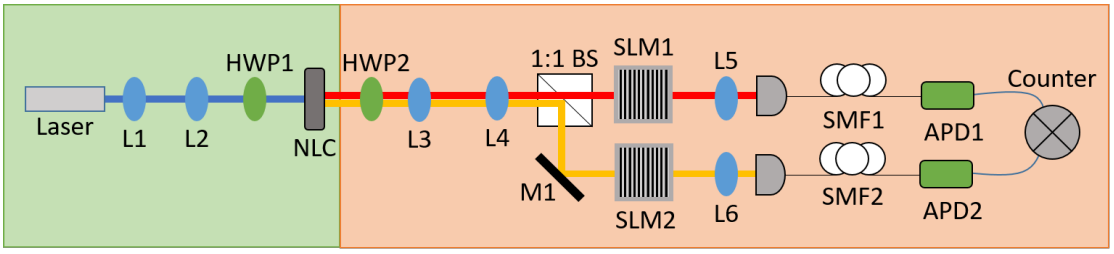

FIGURE 2.1: The setup used to take all measurements. Laser: 405nm, L: Lens, L1: 400mm, L2: 300mm, L3: 100mm, L4: 500mm, L5: 750mm, L6: 750mm, HWP: Half Wave Plate, NLC: Non-Linear Crystal, BS: 50:50 Beam Splitter, M: Mirror, SLM: Spatial Light Modulator, SMF: Single Mode Fibre, APD: Avalanche Photon Detector, Counter: Coincidence counting. Green: Generation. Red: Detection.

The laser used was a 405 nm UV laser at 130 mW and a liquid crystal UV Holoeye SLM was used to modulate the light. Mirrors of different coatings was used to direct the light throughout the setup: the mirror coatings before and after the

crystal were EO2 and EO3, respectively. A- and Uncoated lenses were used before the crystal, while B-coated lenses were used afterwards. A National Instruments coincidence counter, interfaced with Labview, was used to count correlated photons. The photons were directed towards the avalanche photon detectors using a single mode fibre suitable for down-converted 810 nm SPDC light.

An already built setup was used to perform many of the experimental runs that will follow, but a similar setup was also rebuilt for learning purposes. This rebuilt setup was used to take some additional experimental results and was built alongside another Masters student, Michael Lovemore. Both setups required a lot of optimization that included tipping and tilting mirrors, walking the beam into fibre couplers, calibrating the SLM, and translating the crystal.

2.2 State Generation

2.2.1 Spontaneous Parametric Down Conversion

SPDC is the process where higher energy photons, from a pump beam that enters the NLC, are down-converted into two lower energy photons called the signal and idler photons. SPDC using a NLC is illustrated in Figure 2.2. Throughout this process the energy and momentum must remain conserved. These conservation laws can be illustrated using energy level diagrams and momentum vectors, and are the cause of what are called the phase matching conditions. Controlling the indices of refraction of the ordinary and extra-ordinary axes of the birefringent NLC, enables many configurations of wave vectors that adhere to these conservation laws. Each individual case where the above applies, is called the phase matching conditions for that case. The control of the indices of refraction is done by altering the temperature of PPKTP crystals and changing the angle of incidence of the pump beam on the crystal for BBO crystals.

The conservation laws that follow from the phase matching conditions are represented through frequencies and momentum vectors. Recall that frequency and energy are closely related, which is why it is referred to as energy conservation. The two conservation laws are:

$$\begin{aligned} \omega_p &= \omega_i + \omega_s, \\ \vec{k_p} &= \vec{k_i} + \vec{k_s}, \end{aligned} \tag{2.1}$$

where the indices s, i, and p, refer to the signal, idler, and pump beams.

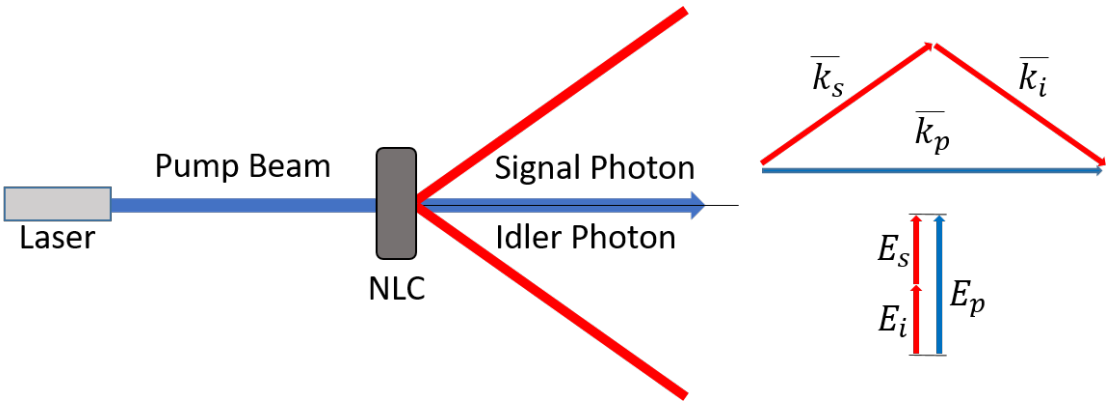

FIGURE 2.2: The pump beam from the laser is down converted into two lower energy beams: the signal and idler beams. The momentum and energy conservation laws are illustrated in the vector and energy level diagrams on the right.

There are three types of phase matching that can occur within non-linear crystals: Type 0, Type I and, Type II. Type 0 phase matching is where the down-converted beams have exactly the same polarisation as the pump beam. Type I is where the polarisation of the down-converted beams are the same, but orthogonal to the pump beam polarisation. Type II is where the polarisation of the two down-converted beams are orthogonal, but either the signal or idler beams have the same polarisation as the pump beam. The one that will be used, is Type I phase matching.

The process of SPDC can be collinear or non-collinear, which means that the two down-converted beams are either parallel or spatially separated. When the two beams are non-collinear they form a cone-shaped beam, where each opposing pair of points on the cone actually indicate the instantaneous position of two spatially separated, entangled photons in each of the signal and idler beams. In a PPKTP crystal, which was used, this collinearity is depended on the temperature of the crystal. At a specific optimum temperature the two down converted beams will be perfectly collinear, which will be spatially separated using a 1:1 beam splitter (BS) as can be seen in the setup diagram. As the temperature is increased the non-collinear signal and idler beams contract towards each other. The temperature is chosen to be 62°C so that the signal and idler beams are almost collinear, as pushing the crystal temperature higher can make the SPDC perfectly collinear. If the SPDC is perfectly collinear, it effects the bandwidth of the system, since the more contracted the SPDC beam is, the less modes there are available for encoding information and use in quantum systems [48]. The more collinear the SPDC, the smaller the area of the SPDC, which effects the spiral bandwidth. The goal is to

maximise the spiral bandwidth, while simultaneously making it easier to readily control the direction of propagation of both the signal and idler beams.

Finally, the down-conversion process can be degenerate or non-degenerate. The degenerate case is where the two down converted beams have exactly the same energy. In contrast, the non-degenerate case is where the two beams have different energies (and frequencies). The degenerate case was used for the experimental setup.

To describe the SPDC mathematically, its quantum state can be written using creation operators. SPDC photons are spontaneously created out of the vacuum state $|0,0\rangle$ when the higher energy laser impinges on the NLC. The SPDC state can be given by [49]

$$|\psi\rangle_{SPDC} = \int\int d\vec{k}_s d\vec{k}_i \Phi(\vec{k}_s, \vec{k}_i)\hat{a}_s^\dagger(\vec{k}_s)\hat{a}_i^\dagger(\vec{k}_i)|0,0\rangle, \tag{2.2}$$

where the integration is over the transverse spatial profile defined by the wave vectors of the signal and idler modes $\vec{k}_i$ and $\vec{k}_s$, the Φ function is the pump beam spatial profile or distribution that is converted into the signal and idler modes, and the state $|0,0\rangle$ is the vacuum state out of which the signal and idler modes are created by the creation operators $\hat{a}_s^\dagger(\vec{k}_s)$ and $\hat{a}_i^\dagger(\vec{k}_i)$.

The signal-idler photon pair can be entangled in many degrees of freedom namely OAM [50], time-energy [51] and polarisation [52], but here the focus is placed specifically on entanglement in the OAM degree of freedom. Since LG modes are eigenmodes of free space, they are solutions to the paraxial Helmholtz equation from before, we can use them here to describe the signal and idler modes, which carry OAM because of conservation of angular momentum. The integral over the entire transverse distribution now becomes a summation, where the summation is over the discreet radial and azimuthal indices of the LG modes, since summing all possible ℓ values implies summing the entire SPDC field. This implies that the SPDC state now becomes a linear combination of the signal and idler modes, that have oppositely signed orbital angular momenta, where the linear combination weightings, will be denoted by $C_{p_s,p_i}^{\ell_s,\ell_i}$ in

$$|\psi\rangle_{SPDC} = \sum_{\ell_i,p_i}\sum_{\ell_s,p_s} C_{p_s,p_i}^{\ell_s,\ell_i}|\ell_s,p_s;\ell_i,p_i\rangle. \tag{2.3}$$

It is important to note that the correlation coefficients and the probability of the SPDC state being in any one of its topological charge combinations are related.

This follows directly from quantum mechanics and how the projections are calculated. The probability of the SPDC state being in a particular combination is just the overlap or inner product of that combination with the entire SPDC state squared.

Since we only consider modes carrying OAM and no radial rings, the above p indices are actually zero and the coefficients only depend on the ℓ values. The combinations of all weighting values or coefficients for the above state is called the spectrum of the entangled state and for OAM entangled photon states like SPDC, this spectrum is referred to as the spiral spectrum. The coefficients are called the correlation coefficients because of the presence of entanglement in the state.

The SPDC state can be written more compactly if we ignore the radial part completely. Considering a SPDC state where entanglement is present, still in the OAM degree of freedom as before, but now only the topological charge values are referred to, we get the exact same entangled state as in Chapter 1:

$$|\psi\rangle_{SPDC} = \sum_i c_i |\ell_i\rangle |-\ell_i\rangle, \tag{2.4}$$

where now it is clear that only oppositely signed topological charged modes contribute to the entangled state.

2.3 Detection

2.3.1 Overlap

Measuring spatially entangled quantum states requires finding the correlation coefficients or weighting values $C^{\ell_s,\ell_i}_{p_s,p_i}$. This is done by projective measurements, similar to how quantum measurement probabilities are calculated, but now it is the overlap between the signal and idler modes at some combination of indices and the full SPDC state itself [53], which is written by the inner product

$$C^{\ell_s,\ell_i}_{p_s,p_i} = \langle \psi_i, \psi_s | \psi_{SPDC} \rangle. \tag{2.5}$$

Modelling the pump and the signal and idler modes as part of the LG OAM carrying mode family, this can be written as:

$$C^{\ell_s,\ell_i}_{p_s,p_i} = \int_0^{2\pi} \int_0^{\infty} \rho d\rho LG^{\ell_p}_{p_p}(\rho,\phi) \left[LG^{\ell_s}_{p_s}\right]^* \left[LG^{\ell_i}_{p_i}\right]^* d\phi. \tag{2.6}$$

Ignoring the radial integration for now and only considering the azimuthal integration, we see that part of the integral will only be integrated over the phase factors. The phase factors are the complex exponential terms carrying the phase information of the LG modes. The azimuthal integrations runs over an angle of 2π and is given by

$$\int_0^{2\pi} d\phi \exp\left[i(\ell_p - \ell_s - \ell_i)\right] = 2\pi\delta_{\ell_p,\ell_s+\ell_i}. \tag{2.7}$$

Since the integral of a complex exponential function is the dirac delta. In this setup, the pump is a simple gaussian beam, which means its indices are both taken as 0. This has the effect that the dirac delta function is non-zero only when the signal and idler modes have equal, but opposite signed topological charge values. This is the typical trend in SPDC OAM entangled photon pairs and is called the correlation, which in fact is actually an anti-correlation, since oppositely charged photons cause non-zero correlations.

Plotting all of the weighting values or correlation coefficients, gives us the overlap matrix of the SPDC state. The theoretical shape of the spiral spectrum should be completely flat, indicating a maximally entangled state. The reason they are maximally entangled is that all mode combinations, namely a combination of $+\ell$ and $-\ell$ in the two arms, are equally likely to occur. A clear anti-diagonal, indicating the anti-correlation is visible, which when isolated and plotted gives us a perfectly flat spiral spectrum plotted as a histogram in Figure 2.3.

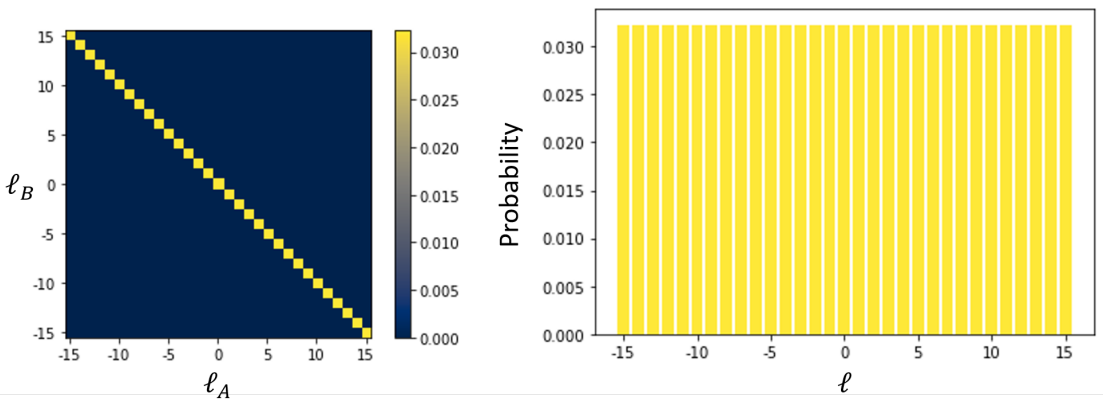

FIGURE 2.3: Left: The theoretical overlap matrix of the SPDC state showing the anti-correlations between oppositely charge topoligical charge values. Right: The anti-diagonal spiral spectrum indicating that the entangled modes all have the same probability.

The experimental overlap is never this ideal, because the equipment used will always introduce a deviation that affects the shape of the spiral spectrum. The true overlap for the spiral spectrum has to take into account the affect of the NLC and also the single mode fibres used to couple and direct the signal and idler beams into the detectors (APDs). The fibres are modelled as gaussians $g(r)$ with their own beam waist and the crystal can be modelled by a function that is a function of position $f(r)$. The true overlap integral then becomes

$$C^{\ell_s,\ell_i}_{p_s,p_i} = \int_0^{2\pi}\int_0^{\infty} f(r)g^2(r)\rho d\rho LG^{\ell_p}_{p_p}(\rho,\phi)\left[LG^{\ell_s}_{p_s}\right]^*\left[LG^{\ell_i}_{p_i}\right]^* d\phi, \tag{2.8}$$

where the new functions have been included in the overlap. If we ignore the affect of the crystal, since normally the crystal area is almost perfectly flat, does not change with position and much larger than the beam size that impinges on the crystal, only the fibres introduce the deviation from a flat spectrum. We do this by stating that $f(r) = 1$. The overlap now becomes

$$C^{\ell_s,\ell_i}_{p_s,p_i} = \int_0^{2\pi}\int_0^{\infty} g^2(r)\rho d\rho LG^{\ell_p}_{p_p}(\rho,\phi)\left[LG^{\ell_s}_{p_s}\right]^*\left[LG^{\ell_i}_{p_i}\right]^* d\phi. \tag{2.9}$$

Experimentally you would never be able to achieve a flat spectrum by just changing the fibre, pump and OAM beam waists, unless the pump beam sizes compared to the fibre and OAM beam sizes could be approximated using a plane wave. One way to output a flat spectrum would be to use the method of Procrustean filtering [54].

Higher topological charge modes are actually detected with lower probability. This happens because for larger topological charge values, the size of the "donut" or ring increases. This has the effect that when the LG mode is converted back into a gaussian mode for detection, which will be discussed later, that the overall intensity is distributed over a larger area and this causes the drop in detected intensity and eventually detected probability.

The SPDC distribution shape can change depending on a number of experimental factors and it is important to keep in mind that the detection overlap happens in the same plane. This plane could be anywhere, but is generally chosen to be on the SLM screen. This means the overlap will now depend on the beam radii of the various contributing beams, since the overlap is determined by the physical overlap of the beams. The ratios of the OAM signal and idler beam radii and the beam radius of the gaussian-modelled fibres or pump change the shape of the spiral spectrum, however, the most important requirement is that the forward

propagating SPDC must overfill the back propagating fibre gaussian in order to detect anything, as underfilling might cause some of the light to miss the fibres. If alignment is perfect this would not matter and only the beam radii will play a role in the overlap.

The shape of experimental spiral spectrums should follow a specific profile determined by the theoretical SPDC distribution. The theoretical SPDC distribution of spectral values is given by [48]

$$|C_{0,0}^{\ell_s,\ell_i}|^2 \propto \left(\frac{2\gamma^2}{1+2\gamma^2}\right)^{2|\ell|}, \tag{2.10}$$

where γ is determined by the experimental signal and idler mode beam radii. Here it is assumed that these radii are equal. γ is the ratio of pump radius ω_p to signal or idler beam radius $\omega_{i,s}$.

Simulating the overlap integral and plotting the spiral spectrum of the results using a gaussian pump with a 0.95 mm beam radius, fibre gaussian beam radii of 1.5 mm and OAM mode beam radius such that the ratio, which is indicated using γ, between pump beam radius to OAM mode beam radius changes, we get Figure 2.4.

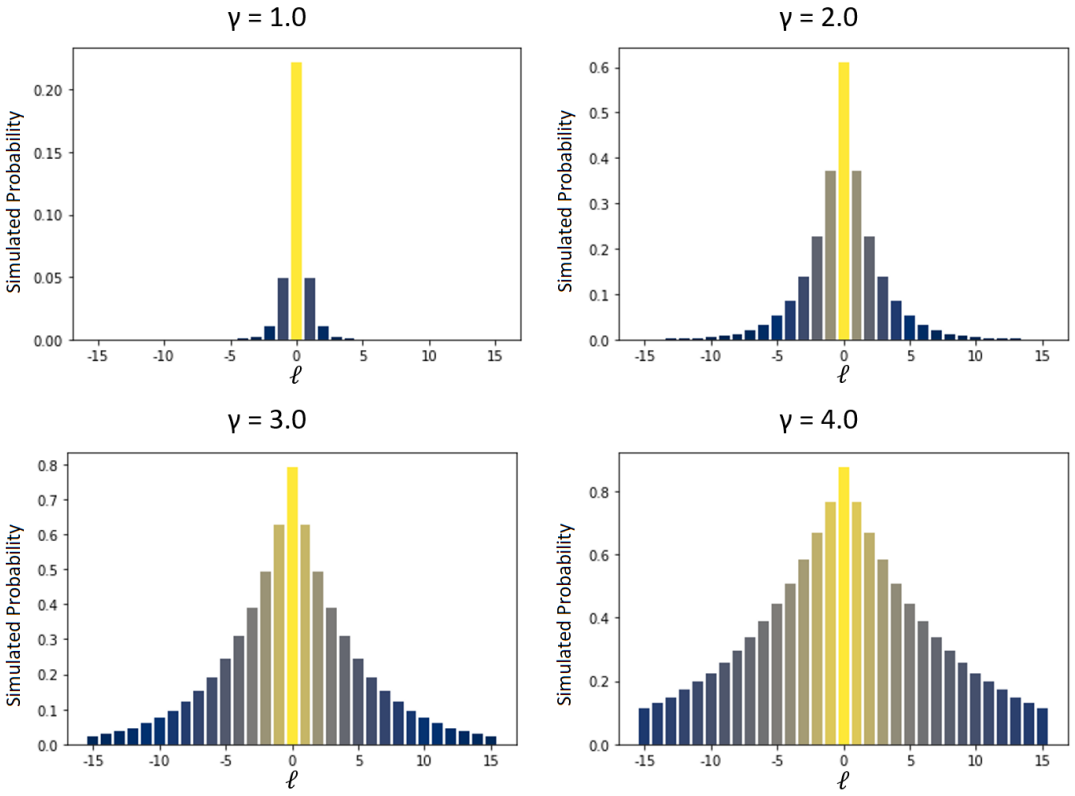

FIGURE 2.4: The shape of the spiral spectrum as the γ ratio changes.

It is obvious that the greater the ratio γ, the more flat or wide the spiral spectrum becomes. What this means is that if the gaussian pump beam radius is increased up until the point the pump becomes approximately a plane wave, we would approach the point where the spectrum becomes a flat spectrum. The only other restriction on the system would now be the fibres that are responsible for detection.

2.3.2 Coincidence Counting

The way we quantify and actually measure the overlap discussed, is through counting the coincidences or number of arrivals where the two photons in an entangled photon pair reach the detectors at the same time. This signifies that the two photons were likely spontaneously created at the same time in the non-linear process and hence are entangled. In optical setups, the signal and idler paths may have different distances, which is why this needs to be compensated for by what is called the gating time. The gating time is a time, of the order of a few nanoseconds, that tells the counter to count arrivals as simultaneous when the photons arrive at the two detectors within a set amount of time.

The relationship between coincidences and overlap is not apparent when considering only the amount of coincidences, but once they are normalized, they become probabilities. These probabilities are exactly the probabilities that the entangled photons are measured to be in whatever state the overlap is measured for. The connection, therefore, between coincidence counting and overlap probability values is that they are proportional. It is possible to count the coincidences for the entire array of possible OAM modes, which as before is called the overlap matrix.

Mathematically the overlap and coincidence counts can be linked by using an integral of the overlap over time, or in other words, summing over every instantaneous overlap value for a specific controlable time Δt, which is the gating time. Let T be the integration time, or the amount of time a single measurement integration is allowed to gather coincidences, then the integration time and gating time are related by $T = n\Delta t$, where n is now the amount of gating times in one integration time. The coincidences over one integration or many gating times is calculated using

$$C_{A,B}^{n\Delta t} = \int_0^{n\Delta t} \psi_A(x,t)\psi_B^*(x,t)dt, \tag{2.11}$$

where A and B denote the two photons and the integration naturally runs over the full integration time. The abstract functions $\psi_i(x,t)$ describe the distribution of photon arrivals at different positions and times in the two detectors and are used in a overlap equivalent calculation that calculates how many of the arrivals are actually coincidences.

Since the amount of coincidences can only be an integer value, this integral can be approximated by simply summing all of the coincidences per gating time for the entire integration time. If this number were to be divided by the integration time, the value would represent the coincidence rate with units coincidences per second. The total coincidences is now the sum of all gating time coincidences

$$C_{A,B}^{n\Delta t} = \sum_{i=1}^{n} C_i, \tag{2.12}$$

where n denotes the n^{th} gating time. As was said already, the amount of coincidences counted is proportional to the probability or weighting values in

$$C \propto C_{p_s,p_i}^{\ell_s,\ell_i}, \tag{2.13}$$

where C is now used for the total amount of coincidences.

It is possible for two stray photons to enter the two detectors at the same time and to register a coincidence or for a stray photon to be incorrectly paired with a photon from the SPDC source. These arrivals are part of the noise of the system an are called accidentals (A). The amount of accidentals can be calculated from coincidence count rate measurements by using [55, 56]

$$A_r = S_1 S_2 \Delta_t, \tag{2.14}$$

where S_1 and S_2 are the coincidence count rates in the two arms, Δ_t is the gating time and A_r is the accidental count rate. The count rate in both arms is determined by two parameters [55], called the quantum efficiency of the detectors, η_1 or η_2, and photon arrival rate, N_1 or N_2, in both arms. The count rates are usually measured by arrival counting and division by the integration time, but can be calculated using

$$S_i = \eta_i N_i. \tag{2.15}$$

To find accidentals the coincidence count rates are simply multiplied by the integration time (T) in

$$A = A_r T. \tag{2.16}$$

The signal to noise ratio, or the amount of coincidences divided by the number of accidentals, is called the quantum contrast (QC)

$$QC = \frac{C}{A}. \tag{2.17}$$

When the usual measurements are taken with an elevated number of photons external to the setup being detected, we expect the overall accidentals to go up slightly. The single photons in each arm should obviously go up, but it is the coincidences and quantum contrast that we are interested in. Coincidences that are not part of the true entangled photon pair amount should be removed in order to be more accurate. Using quantum contrast and coincidence measurements, the accidentals are calculated and simply removed from the coincidence counts before making any conclusions.

The amount of accidentals per second is called the classical rate and the amount of

coincidences per second the coincidence rate. Both the amount of coincidence and coincidence rate will be used going forward. The concept of coincidence counting can be visualised using Figure 2.5.

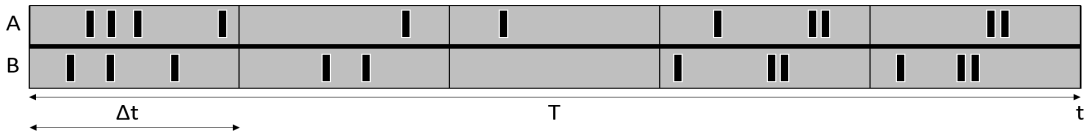

FIGURE 2.5: In this abstract diagram the grey rectangles indicate the bins or gating time, illustrated by Δt. T is the full integration time over which the counting is allowed to occur. The two rows indicate in which arm of the setup a photon is detected and the black lines indicate when a photon is detected by the APDs in both arms. When a photon count occurs in both arms within the same bin or gating time, this event is considered a coincidence.

The overlap here is not as general as the overlap before which included the pump beam and fibres, but the general idea should be clear: coincidences are the quantity that represent degree of overlap between modes.

Knowing what coincidences are and what they represent and knowing what the integration and gating time are, it is easy to study the affects when these factors are changed. Increasing the integration time would cause the total amount of time the counter "integrates" or counts over to be larger, which would simply increase the total coincidences counted. Increasing the gating time would make the criteria for arrivals to be considered a coincidence less stringent, which means that more coincidences are counted, but at the cost of losing accuracy in the form of a lower quantum contrast. Figures 2.6 and 2.7 below confirm this understanding.

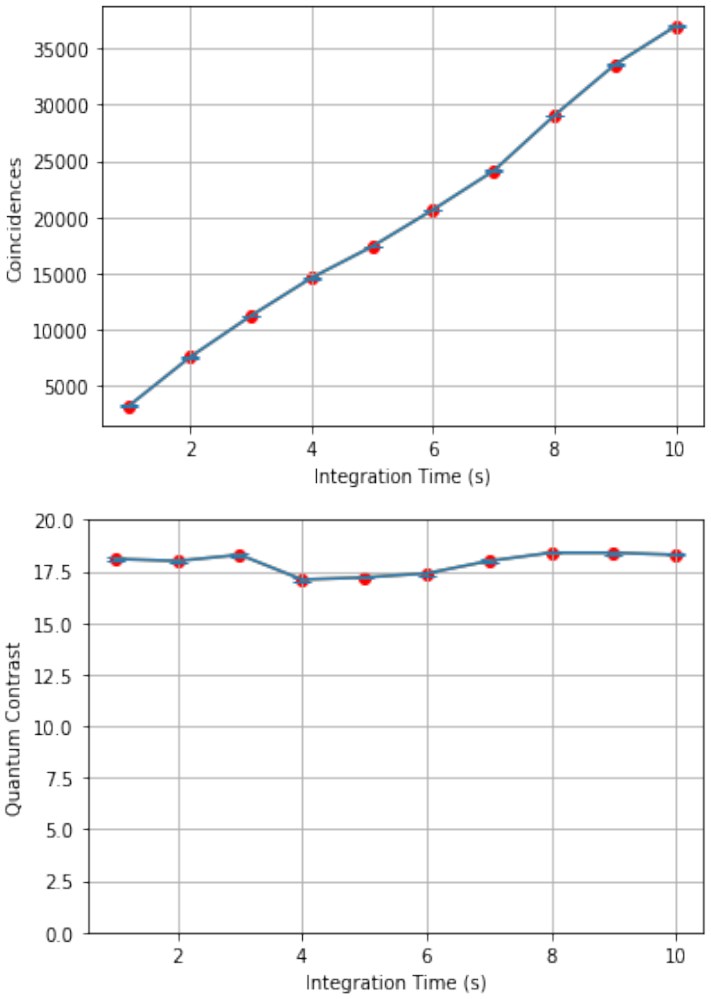

FIGURE 2.6: Two line plots showing the relationship between the coincidences (Top) and quantum contrast (Bottom), and integration time.

When the integration time is increased, more entangled photon pair arrivals are counted, because they are being counted for longer. Here the gating time remains the same. The amount of photon pairs that arrive increases as integration time increases, however the quantum contrast remains relatively constant. The reason is that the gating time is set in such a way to consider only the true coincidences as coincidences. This means that an increase in integration time not only increases coincidences, but accidentals as well. When both elements from the quantum contrast ratio increase at similar rates, we see a constant line.

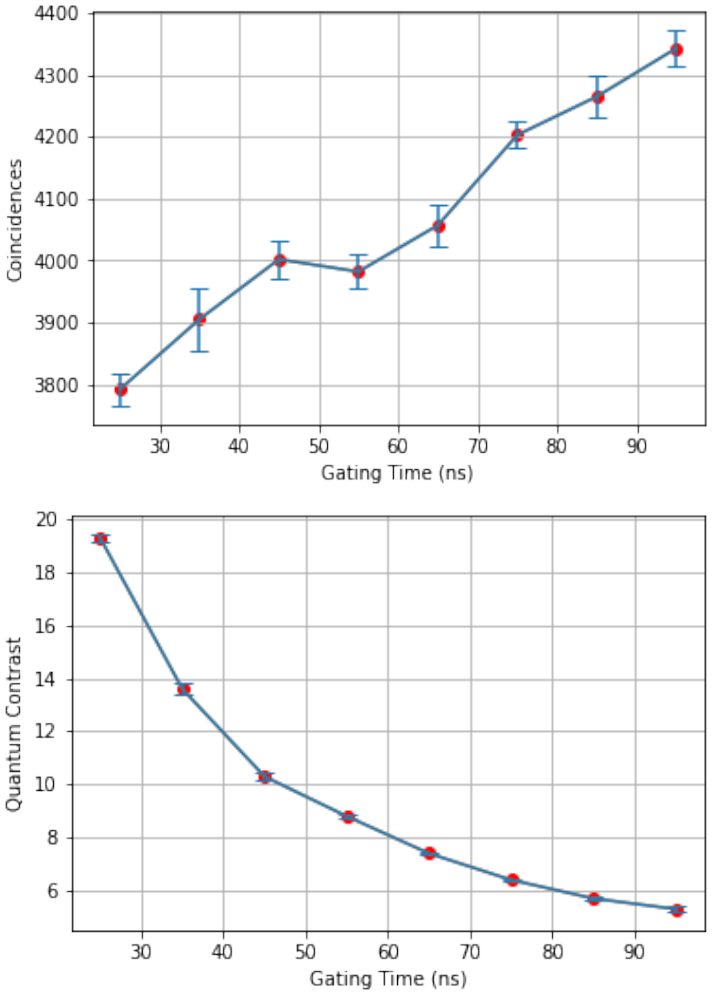

FIGURE 2.7: Two line plots showing the relationship between the coincidences (Top) and quantum contrast (Bottom), and gating time.

As the gating time is increased the number of photon arrivals that are considered as part of an entangled pair increases, which is why we see the increase in coincidences overall. The quantum contrast hyperbolically decreases, since only a certain amount of arrivals are actually part of entangled pairs. If the actual amount of entangled pairs are held constant, this would mean an inverse proportion between accidentals and quantum contrast. So as the amount of accidentals increases, brought forward by the increase in gating time, the quantum contrast has to decrease asymptotically to zero.

2.3.3 Crystal Temperature

This quick intermission backtracks to see the affect of changing the crystal temperature on both coincidences and the collinearity of the SPDC.

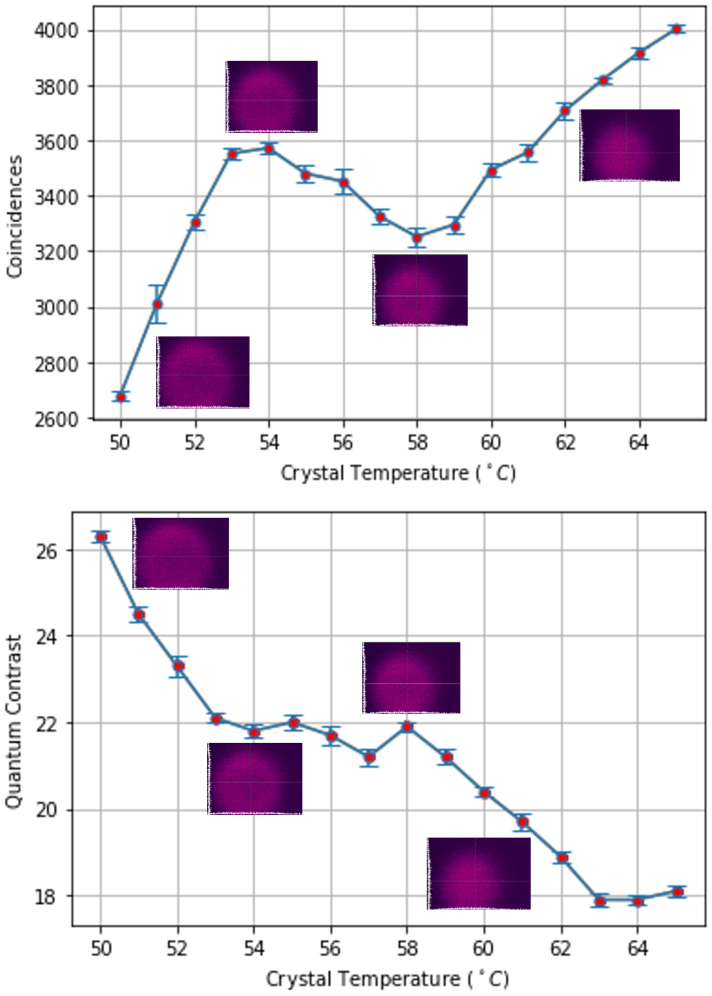

FIGURE 2.8: The affect of crystal temperature on the collinearity, coincidences and quantum contrast. Top: Coincidences against crystal temperature. Bottom: Quantum Contrast versus crystal temperature.

In Figure 2.8, the location or transverse spatial coordinates at which the coincidences and quantum contrast was measured never changed. This means that as the beam contracts from non-collinear to being almost completely collinear, the change in coincidences and quantum contrast is a reflection of the change in the propagation direction of the beams. This means that a dip in conicidences implies that the beams are being diverted away from the detectors and a drop in QC implies that the overall coincidences to accidentals is dropping. If the accidentals are assumed constant, since the light level external to the setup is held constant and all non-entangled photons are filtered out by a bandpass filter, this is just another indication that SPDC beams are moving away from the detectors.

The question becomes: Why do the coincidences start increasing again when the

crystal temperature is increased from 58 to 65°C? This is because as the collinearity is increased the intensity of the SPDC increases, causing the increase in coincidences. The amount of accidentals increase, causing a decrease in quantum contrast, since a higher intensity, or more photons overall, increases the probability of counting accidentals.

2.4 Imaging and Projective Measurements

The affect on light that interacts or passes through an optical element can be described by transformation matrices called Jones' matrices [57], that are matrices or operators that are applied to the electric field vectors. The same affect can be described by transmission functions of various optics, which are just factors that are multiplied to the field function similar to how matrices are applied to vectors. Every single optic has a distinct transmission function, but in this subsection the focus is placed on the transmission functions of lenses and SLMs, since they form the foundation of imaging the beam onto the SLM and into the fibres where the projective measurements are made. Generic transmission functions have the shape

$$t(x, y) = A(x, y) \exp\left[i\phi(x, y)\right], \tag{2.18}$$

where $t(x, y)$ is the transmission function and $A(x, y)$ and $\exp\left[i\phi(x, y)\right]$ alter the amplitude and phase of the field function.

2.4.1 Lenses

The lens is a refractive optical element that alters the path of light rays because of its index of refraction and shape. Laser light, which is a collection of many coherent, parallel rays of light is either diverged or focused to a point depending on the shape of the lens. The distance from the lens where the rays are focused is called the focal distance and it is at this point where the light will be the most intense, since it covers the smallest possible area. As the light propagates past the focal point, it will diverge again and the area it covers will increase until the intensity goes to zero. The point where the laser light covers an area that is twice that of at the focus is called the Rayleigh range as discussed before.

Lenses do not just bend rays of laser light, but apply the Fourier transform to the light field. This Fourier transform re-expresses the light field, that was originally written in terms of position, now in terms of momentum. The lens is thus the Fourier transform between the position and momentum spaces. If the point where the rays are focused is extended into a plane that is perpendicular to the

propagation direction, this plane would be called the focal plane. Once the field undergoes one Fourier transform from a lens, it is sometimes referred to as being in the Fourier plane. Transmitting the beam through a second lens would make it describable by position once again, since applying the Fourier transform a second time transforms the light field to be expressible in the position space. This is referred to as being in the image plane. The affect of using two lenses is an imaging system where the image plane is imaged onto or into optics. In other words, by using two lenses we can preserve in which plane we are working in, which is important when building optical setups.

The transmission function of a lens is simply multiplied by the field function of the light to model the affect of the lens on the field [58]. This transmission function is

$$t_l(x,y) = P(x,y)\exp\left[-i\frac{k}{2f}(x^2+y^2)\right], \tag{2.19}$$

where $t_l(x,y)$ is the lens transmission function and $P(x,y)$ is the complex pupil function that describes how the field amplitude is affected upon interacting with the lens. f is the focal distance, k is the wave number, x and y are the position coordinates and i is the imaginary number, that is also sometimes contained in $P(x,y)$.

Using this transmission function, and the method used in [58] where it is substituted into the Fresnel diffraction integral, we get the Fourier transform of a single lens and the expression of the light field at the focal plane of the lens. U_1 is the field that enters the lens and U_2 is the output field. U_2 is given in terms of U_1 in the Fourier transform:

$$\begin{aligned} U_2(x_2,y_2) &= \frac{\exp(ikf)}{i\lambda f}\exp\left[i\frac{k}{2f}(x^2+y^2)\right] \\ \times\int\int U_1(x_1,y_1)P(x_1,y_1)\exp&\left[-i\frac{2\pi}{\lambda f}(x_2x_1+y_2,y_1)\right]dx_1dy_1, \end{aligned} \tag{2.20}$$

where λ is the wavelength, x_1, y_1 are the coordinates of the field before the lens and x_2, y_2 are the coordinates of the field after the lens. For completeness the simple Fourier transform that converts position into momentum and visa versa is given as well:

$$
\begin{aligned}
U_2(k_x, k_y) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} U_1(x, y)\exp\left[-i2\pi(k_x x + k_y y)\right]dxdy, \\
U_1(x, y) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} U_2(k_x, k_y)\exp\left[i2\pi(k_x x + k_y y)\right]dk_x dk_y,
\end{aligned}
\tag{2.21}
$$

where k_x and k_y are the coordinates in momentum space and in Fourier analysis is called frequency variables that are associated to x and y [58].

Using two lenses is common practise and together this forms what is called a telescope or 4F system. 4F because of the four focal distances when two lenses are considered. A typical 4F system, like in Figure 2.9, requires that the two lenses be two focal distances away from each other in order to preserve the plane. The plane that is imaged by the 4F system must be one focal distance away from the lens combination's first lens and the position to where the plane is imaged to, must also be one focal distance away from the second lens. If the lenses have different focal lengths, they must be separated by the sum of their focal lengths.

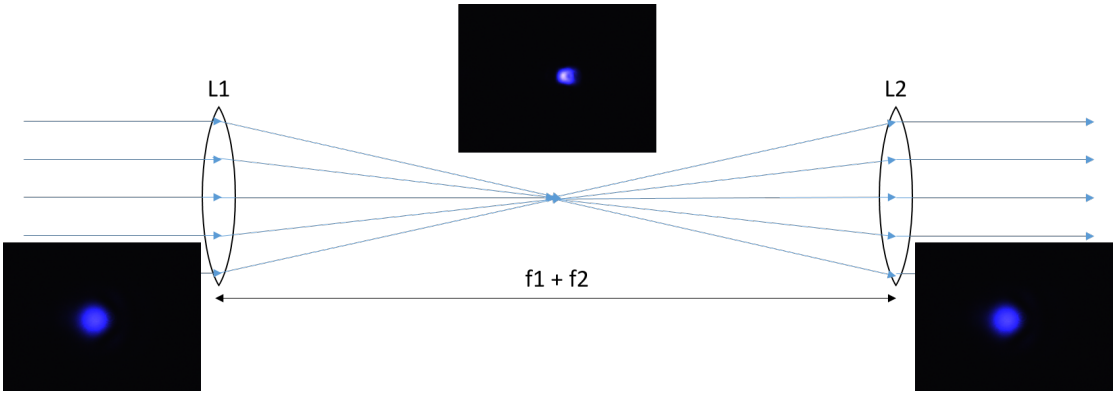

FIGURE 2.9: A basic illustration of how parallel light rays are focused to a point, which also has the affect of Fourier transforming the light field. Included are some beam images taken. A second lens applies the Fourier transform again.

The 4F telescope setup can be used to magnify or demagnify the beam itself and this magnification is calculated using the focal lengths. The reason the size of the beam would need to be changed depends on whether the system requires the beam to overfill or underfill various optics in the setup. The magnification of a 4F system is calculated using

$$
M = \frac{f_2}{f_1}, \tag{2.22}
$$

where M is the magnification of the 4F system and f_1 and f_2 are the focal lenghts of the two lenses.

2.4.2 Spatial Light Modulators

Projective measurements are probability measurements taken by overlapping the field with holograms on a spatial light modulator. This is part of using SLMs to shape light and is done by altering the transverse spatial properties, particularly of laser light. This can also be done by using digital micro-mirror devices, but focus will be placed on SLMs.

Spatial light modulators or SLMs are made up of a grid of small pixels containing many tiny liquid crystals where these pixels are of the order of a few microns. Figure 2.10 is an illustration of liquid crystal SLM pixels. The operation of an SLM depends on small voltages that are applied across the liquid crystals that change their orientation and effectively change the reflectivity or transmissivity of each pixel. The affect is that certain portions of the incident wavefront that impinges on the SLM grid of pixels will be variably reflected or transmitted and this is what alters the shape of light. This is all possible because of the birefringence of the liquid crystal array [59]. This is the concept where the crystals have a separate index of refraction along the ordinary and extraordinary axes, which when controlled allows the phase or complex amplitude of the beam to be altered in a controllable way [59].

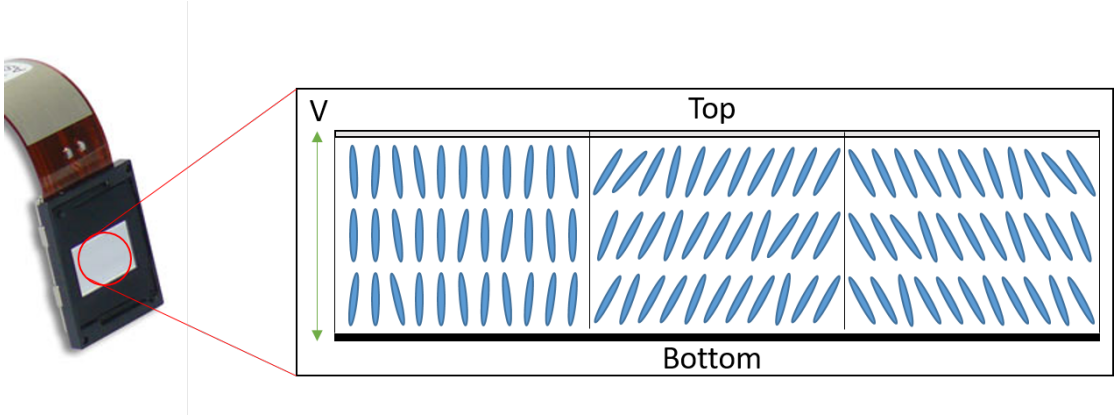

FIGURE 2.10: An illustration of some pixels on the SLM screen and how the voltages applied to the liquid crystals effect their orientation. Light is incident on the top, propagates through the liquid crystal array and reflects off the bottom face.

The two ways of modulating light are called phase-only [60] and complex amplitude modulation [61], which can be performed in conjunction, but is typically

used separately. In most of the experimental runs that will follow later, phase-only modulation was the method of choice. A third option is available: simple amplitude modulation where only the amount of light that is reflected/transmitted is altered, however, this restricts what is actually possible, since it only involves truncating the beam, but is often used to spatially filter out parts of the beam that are unwanted.

Representing the complex field of the laser beam as [62]

$$u(x, y) = a(x, y) \exp [i\phi(x, y)], \tag{2.23}$$

which includes the phase in the exponential term and the complex amplitude $a(x, y)$ that could have no complex components and would therefore be real. By modulating the light is implied that either one of these, or both, be changed in some way. This can be represented using a transfer function that is just an exponential factor and is a function of the original field's complex amplitude and phase. When this factor is multiplied by the field itself [62], it applies the modulation. An example of phase-only modulation would be

$$h(x, y) = \exp [i\psi(a, \phi)], \tag{2.24}$$

where the function $h(x, y)$ is the hologram that must be encoded on the SLM screen, Fourier expanded and used in an approximation. This is the Arrizon technique of encoding SLM holograms [62].

Amplitude modulation can be represented using a function $f(\rho, \phi)$ that is also simply multiplied by the beam field. One simple example would be a binary aperture that is modelled by a step function:

$$f(\rho, \phi) = \begin{cases} 1 & r > r_A \\ 0 & r \leq r_A \end{cases} \tag{2.25}$$

Any light at points where the distance to the propagation axis r is larger than r_A will be multiplied to zero applying the aperture to the beam.

Since birefringence is of interest here, polarisation becomes key, as the relative direction of the polarisation to the ordinary and extraordinary axes changes the index of refraction light interacts with. For the SLMs that we use only horizontal polarization will be modulated.

Understanding how to modulate the amplitude and phase of light is the first step,

but the entire reason SLMs are used in the first place is to do the necessary projective measurements to find, through measurement, the probability or eigenvalues of specific eigenmodes. These eigenmodes are typically the LG modes from before and the measurement is done by counting the coincidences. Since SPDC contains an entire distribution of OAM modes, which is clear from its state description, the SLM is used to choose which mode to measure. This procedure is called post selection and is usually done by encoding the opposite OAM charge on the SLM that the LG mode will interact with. This has the effect that the two OAM charges cancel, the mode becomes a gaussian beam and eventually couples into the SMF that can only couple gaussian beams that have no OAM.

Chapter 3

Controlled Experiments

Chapter 3 is the experimental results section and includes all of the basic quantum measurements that can be done in order to characterise the quantum system. This is done using the concept of state overlap and coincidence counting. These properties include: the spiral bandwidth, the density matrix and the presence of entanglement of the state. For completeness this chapter also includes some measurements that were not as successful or that completely failed.

3.1 Basic Quantum Measurements

The spiral bandwidth can be thought of as the total amount of modes available for use with respect to information encoding in any specified application, since these modes are the ones that, compared to the amount of noise in the system, are easily recognisable or in other words have a high enough signal to noise ratio that ensures the signal is not of the order of or dominated by the noise [63]. The spiral bandwidth is called the spiral bandwidth because orbital angular momentum implies spiralling wavefronts. The spiral bandwidth is closely tied to the spiral spectrum, which has a shape that can vary depending on how it is applied [48, 53, 63, 64].

The state density matrix is found from a procedure called quantum state tomography (QST) that uses overlap and minimization techniques to find the density matrix closest to the physical state, which implies finding the state and at the same time maximizing the reconstruction fidelity. Tomography has been applied to the spatial basis [34] as well as time-bin entangled states. [65]. The focus is placed on QST, but there is another new method of reconstructing the density matrices of bipartite quantum entangled systems, which uses an isotropic density matrix state model along with purity and dimensionality measurements to

accurately reconstruct the density matrix [66].

Finally, the presence of entanglement can be measured using the Bell parameter and whether the value of this parameter violates the CHSH-inequality or not, since this determines if entanglement is present in the state [67]. This is done by testing for local hidden variables [68]. Bell tests are tests of non-locality in the state and a Bell parameter equal to the Tsirelson bound of $2\sqrt{2}$ indicates a maximally entangled two-dimensional state. Bell tests can be done for polarisation [69] and OAM states using generic two-dimensional superposition states [70] as well as sector states [70]. Hyrbrid entangled states also violate the Bell inequality [71] and bell tests can be performed for higher-dimensional cases [72], such as for three dimensions [73]. Tests of separability through Bell tests have even been performed on classical light [74].

3.1.1 Spiral Bandwidth and Crosstalk

The spiral bandwidth is the amount of modes that contribute to the OAM entangled state generated by SPDC [48] and is calculated from the spiral spectrum. The spiral bandwidth is limited by experimental limitations, where the word "bandwidth" specifically refers to the amount of modes that can be detected by the experimental setup. It is in essence the amount of modes that can be used to encode information, as their spectral values or weighting coefficients are high enough to surpass the noise of the system. It is calculated by counting the amount of modes that have spectral values (coincidence counts or probabilities) higher than the full-width at half maximum (FWHM) [64]. The spectra from which the spiral bandwidths are calculated are plotted using the coincidence count rate, as coincidences and probability are proportional to each other:

$$C \propto P_{a,b}, \tag{3.1}$$

where C is the amount of coincidences and $P_{a,b}$ are the probabilities values that the state is in the specific combination denoted by the OAM charges of photon a and photon b. a and b are the OAM charges of the two photons.

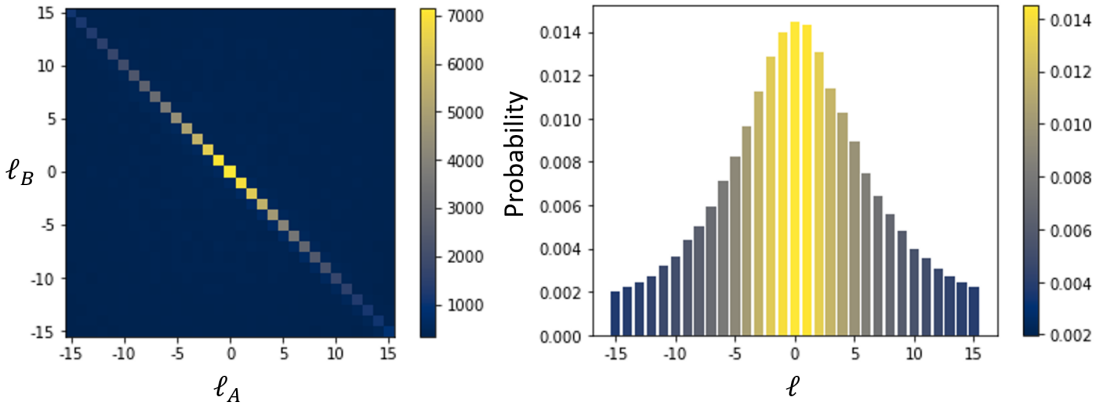

FIGURE 3.1: An example of a spiral bandwidth measurement. Left: Shows the entire overlap matrix of all the ℓ combinations as a grid of their coincidence counts in what is called the OAM spectrum. Right: Shows the spiral spectrum and is where the spiral bandwidth is calculated. The coincidence counts are now normalised by dividing every coincidence value by the sum of the entire spectrum. The spiral bandwidth is calculated using the FWHM and is 12 modes.

There exists another measure of the amount of modes that contribute to the entangled state. K or the Schmidt number can also be calculated and is a number indicating the number of effective modes that can be exploited for information encoding and is often referred to as the dimensionality of the state. The Schmidt number K is calculated using the spectrum probabilities or coincidence counts as before, but now in the equation

$$K = \frac{(\sum_i P_i)^2}{\sum_i P_i^4}, \tag{3.2}$$

where P_i denotes the probability values or normalized coincidences from the OAM spectrum. The P_i values can be substituted with the coincidences C_i measured or eigenvalues λ_i of the linear combination to give exactly the same answer. $P_{a,b}$ and P_i are different, as $P_{a,b}$ refers to the entire two-dimensional grid of overlap probability values, as in Figure 3.1 (Left), and P_i only to the one-dimensional diagonal of the spiral spectrum, as illustrated by Figure 3.1 (Right). The diagonal of the set of $P_{a,b}$ is the full set of P_i. K is almost always larger than the FWHM, since it is a more lenient measure of the amount of available modes with the respect to the noise levels.

Visually, from Figure 3.1, the spiral spectrum follows the general shape associated with the SPDC distribution from before. To confirm this, the SPDC distribution (Equation 2.10) has to be fitted to the spiral spectrum. This was done by using linear least squares fitting and calculating the residual sum of squares (RSS). An

RSS of 0 implies that the curve fits the data perfectly. The higher the RSS value the more the data deviates from the model. The RSS can be calculated by

$$\text{RSS} = \sum_k (f(\ell_k) - C_k)^2, \tag{3.3}$$

where the summation is over all of the measured ℓ values that form part of the spiral spectrum, C_k is the measured coincidence values, and $f(\ell_k)$ is the theoretical probability from the SPDC distribution.

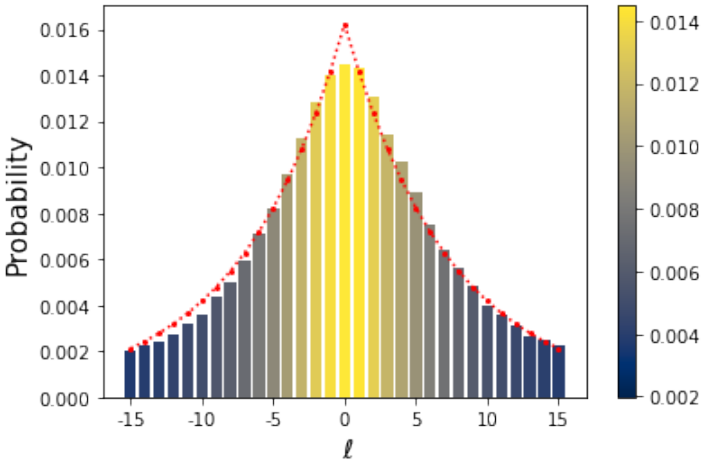

FIGURE 3.2: SPDC distribution curve fitted spiral spectrum with a calculated RSS value of 0.00000720.

The RSS value of 7.20×10^{-6} from Figure 3.2 is extremely close to 0, which means that the SPDC distribution is a near perfect model for the spiral spectrum plotted. This makes sense, since we are using an SPDC source for entangled photons.

It has been discussed, with regards to the overlap, that the size of the beam radii determine the shape, but here we are more concerned with small variations or deviations per OAM charge. Physical spectrums are generally effected by non-perfect alignment, optical aberrations or dirty optics, wavelength mismatched equipment, uncentered holograms etc. Whatever the reason for the deviation from the ideal shape, there must exist a way to quantify the deviation.

If signal is simply lost it becomes easy, since all that has to be done is to calculate how much is actually lost, but sometimes the overlap values in the spectrum scatter into adjacent mode combinations, which when combined into a total effect on the shape of the spectrum causes less modes to be detected than theoretically possible. This scattering of modes into adjacent mode combinations is known as crosstalk.

The total amount of crosstalk, measured as a deviation from the ideal case, can be calculated using the concept of fidelity. If the fidelity is not equal to unity, then it is clear that some deviation must have occurred. The problem with doing this is that calculating the fidelity of the entire spectrum includes all deviations, not just the ones caused from the spreading of OAM modes. It is important to focus down and calculate the fidelity around specific modes, instead of for the entire spectrum. More than pure crosstalk is still being included in such calculations, but at the very least we can get an idea of its affect close to specific mode combinations.

Instead of comparing the entire spectrum to the ideal spectrum, segments of the overlap matrix are isolated and compared to the same segments from the ideal overlap matrix. To illustrate this, rows and columns of 7 mode combinations were isolated from Figure 3.4 (Top Right) and plotted similarly to how the spiral spectrum was plotted. This was done for Figure 3.3. Figure 3.4 shows some of these segments.

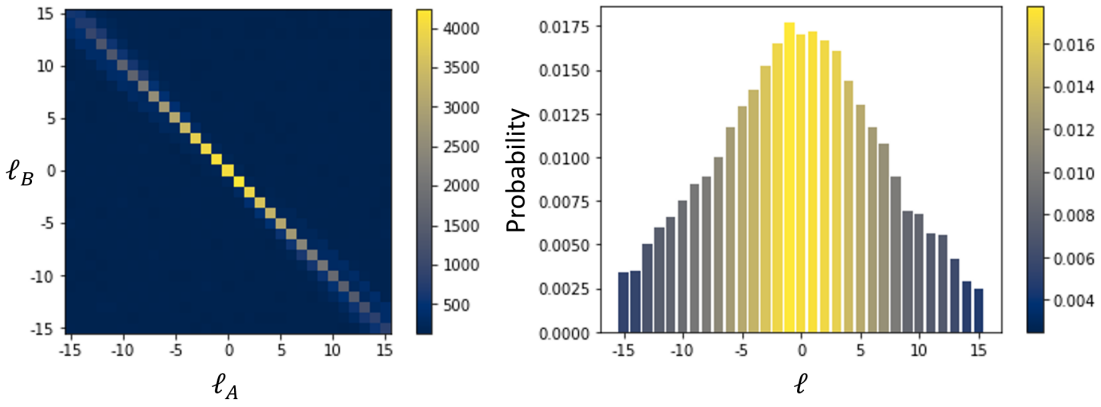

FIGURE 3.3: An example of a spiral bandwidth measurement with crosstalk. Left: Shows the entire grid of ℓ values and their coincidence counts. Right: Shows the diagonal. The spiral bandwidth is calculated to be 15 modes and $K = 25$ modes.

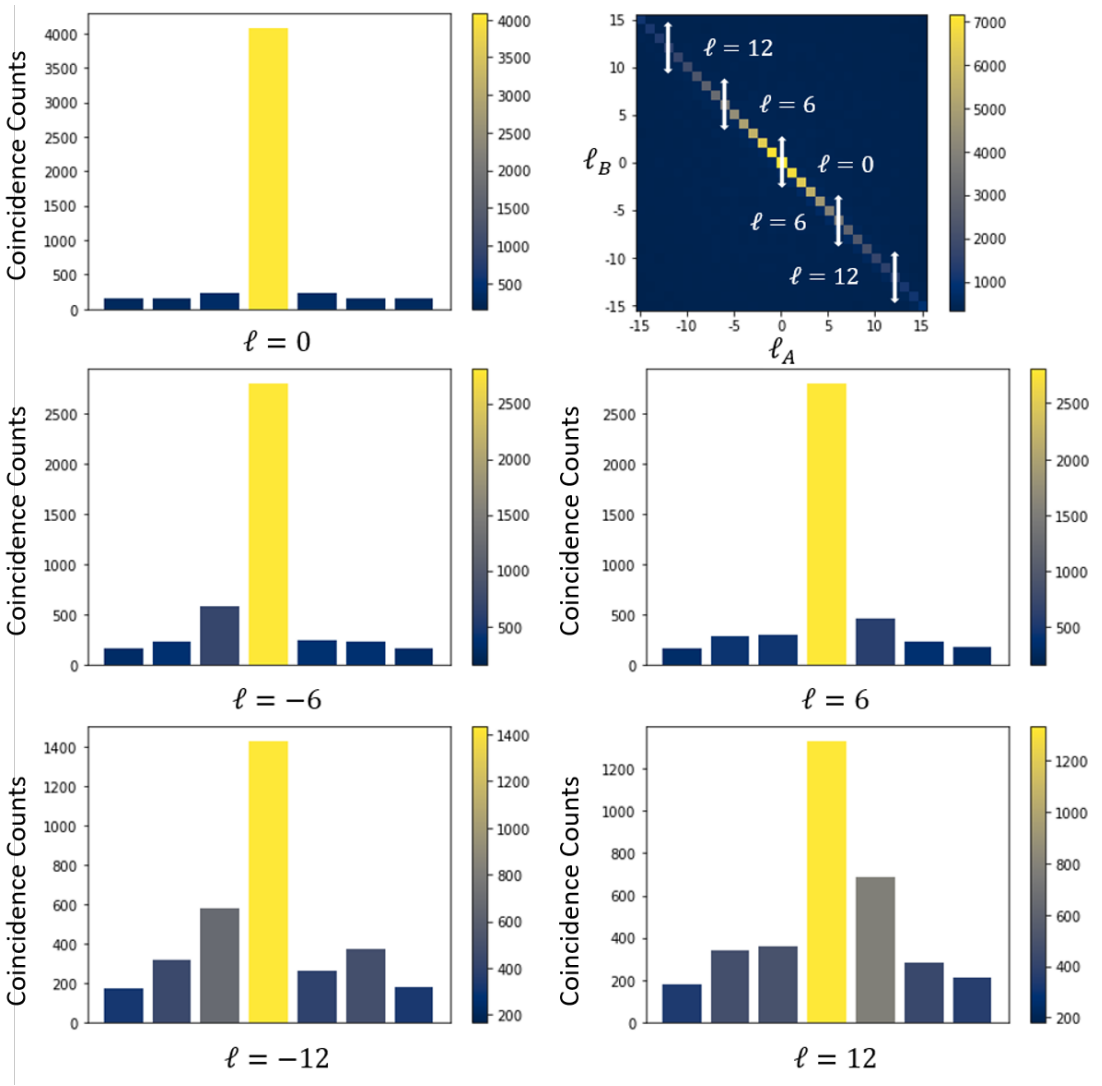

FIGURE 3.4: Column spectrum segments at various ℓ values plotted to illustrate the crosstalk around specific mode combinations. A generic spiral spectrum is included with double sided arrows to show which columns were selected.

The same can be done for row segments. Comparing the row and column segments to the ideal spectrum segment (which should most definitely only have measured values for the OAM value on the diagonal with zeros everywhere else), visually it should be immediately clear that we have mode dependent crosstalk. In other words, the crosstalk increases as the OAM charge increases. In the ideal case, each segment should look exactly the same, except for the change in the spectrum value itself. The ideal spectrum segment is shown in Figure 3.5.

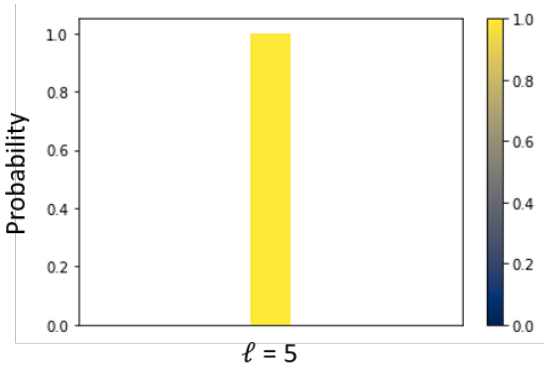

FIGURE 3.5: The ideal spectrum segment for any value of ℓ, which only has a non-zero value for the ℓ value on the diagonal. Any adjacent mode combinations should have a value of zero. The y-axis is still the amount of coincidences, now normalized to become probability.

To cement this, a plot of the fidelity values for each of the segments compared to this ideal segment can be plotted that shows how the fidelity decreases as we consider higher values of OAM. Such plots can be done for each spectrum measured and used to quantify the effect of crosstalk in the system.

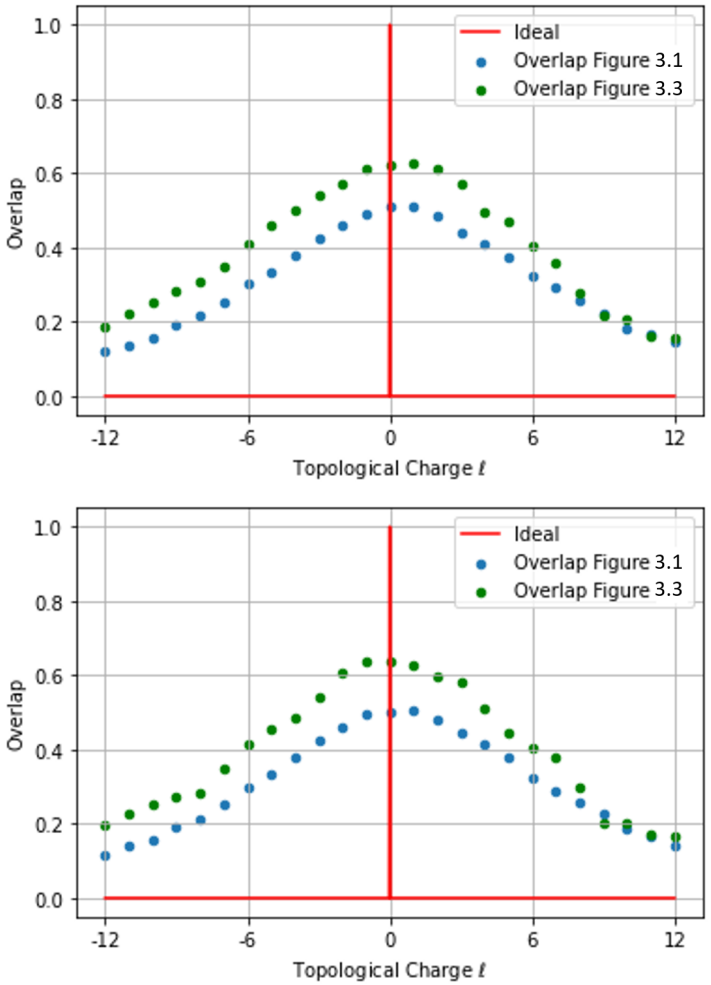

FIGURE 3.6: Fidelity plots illustrating the decrease in fidelity as the OAM charge is increased in magnitude. Top: Fidelity plot for column segments from Figures 3.1 and 3.3. Bottom: Fidelity plot for row segments from the same figures.

In both cases of Figure 3.6 we see that the fidelity decreases as the OAM charge is increased in magnitude. This illustrates what we could visually see already, that there is mode dependent crosstalk present. The lower the fidelity, the further the row- and column segments deviate from the ideal segment. The ideal straight line plot is included to show that the fidelity should be equal to one, since each segment should have matched perfectly with the ideal segment.

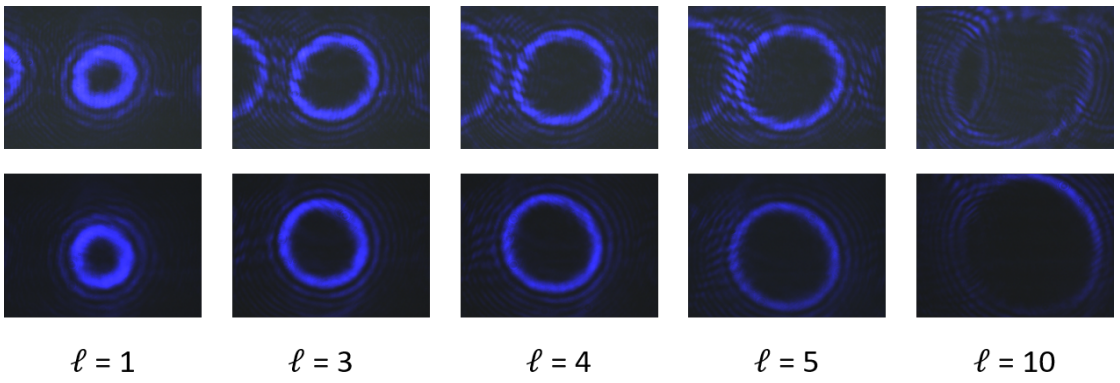

FIGURE 3.7: OAM modes in the two arms of the optical setup. Top: Arm A. Bottom: Arm B.

The OAM modes in the two arms, seen in Figure 3.7, increase in size as the topological charge increases. There is a slight deviation from the perfectly circularly shape of the mode as the aspect ratio also changes with increasing OAM. It is also clear that in arm A there are secondary mode orders that will influence the overlap measurements. This is a visual representation of where crosstalk can come from and the asymmetry of the modes in the two arms explains the asymmetry in the fidelity curves above.

It is unexpected that the fidelities corresponding to Figure 3.1 were always lower than for Figure 3.3. The values themselves are not important, but rather the profile of the fidelity distribution. In other words, increasing mode dependent crosstalk will tend to decrease the fidelity at a faster rate, which is clear from how Figure 3.3's fidelity curve decreases to coincide with Figure 3.1's fidelity curve. The higher fidelities for Figure 3.3 only state that, localised to specific row and column segments, Figure 3.3 matches the ideal segment better.

The uncertainty in the fidelities above can be taken to be a maximum of ± 0.08, which is found by fitting a gaussian distribution to the fidelity plots, finding the covariance, and then using the variance to calculate the standard deviation error. Crosstalk scatters a mode into adjacent modes, which follows a gaussian distribution.

Lastly, the SPDC distribution can also be fitted to this spiral spectrum and a corresponding RSS value can be calculated in order to determine how much the shape of the spiral spectrum deviates from the theoretical SPDC distribution. This calculation was done purely for completeness.

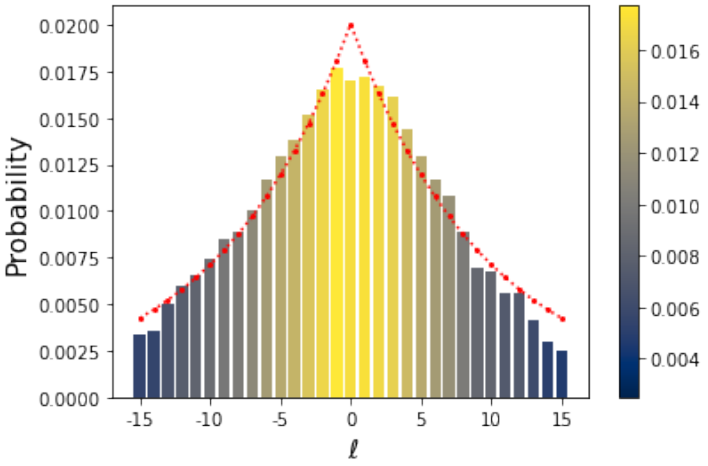

FIGURE 3.8: SPDC distribution curve fitted to the second spiral spectrum case with a calculated RSS value of 0.0000310.

The RSS value for the second spiral spectrum case, now in Figure 3.8, is 3.10×10^{-5}, which is still close to 0, meaning the model was still a good model for this spectrum. This makes sense, since SPDC was still the source of entangled photons, however, the spectrum shape deviated more from the theoretical distribution than the first considered spiral spectrum from figure 3.1. This is consistent than what can be observed visually.

Now that we know what crosstalk is, where the crosstalk in this scenario comes from, how to quantify it, how it effects the shape of the spiral spectrum and, how to quantify this deviation, we can now look at a spiral bandwidth attempt that did not deliver.

3.1.1.1 One-Sided Crosstalk

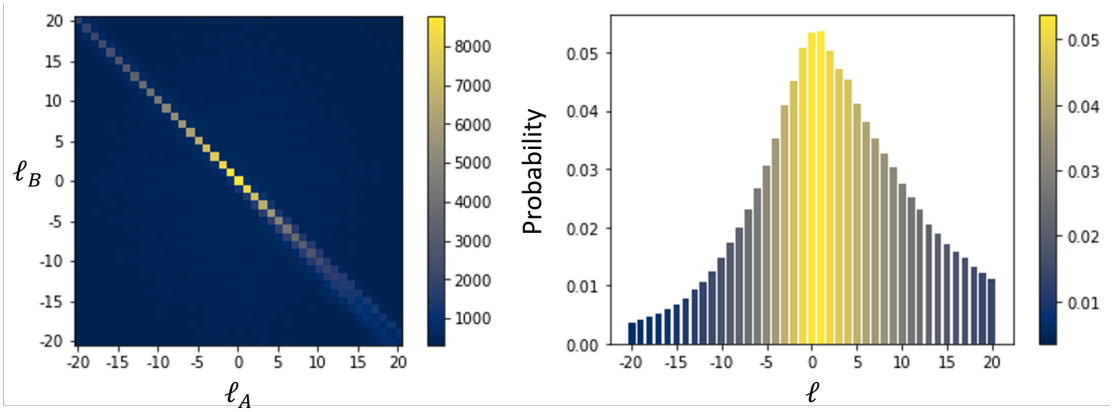

FIGURE 3.9: Spiral spectrum measurement that is skewed to one side.

Figure 3.9 is what happens when the beams used for detection are not coupled into both fibre couplers properly. If one of the couplers are slightly misaligned, loss will cause biasing of some ℓ combinations and eventually the spectrum becomes skewed to one side.

3.1.2 Quantum State Tomography

As discussed before, density matrices can be used to describe bipartite entangled systems consisting of pairs of photons, but when applied in an optical setup the exact density matrix is unknown. Models of the ideal state exist, but the same minor variations or deviations that can cause crosstalk in the spiral spectrum, can change the state in ways that make the state unknown.

In order to find the state density matrix we use the concept of quantum state tomography, which uses projective measurements on an ensemble of identical states to slowly build up the state density matrix [74]. In order to reconstruct the state density matrix, we need the overlap or probability values of all the pure states and some MUB states of all the two-dimensional ℓ combinations for the specific dimension under consideration. The pure states refer to the states where the signal and idler have a distinct OAM value assigned and the MUB states refer to the states where the two photons are each in a superposition at some phase angle, specifically the four MUB angles $0, \pi, \frac{\pi}{2}$, and $\frac{3\pi}{2}$. These angles are the phase angles from Equation 1.24. Not all MUB states are required to reconstruct the density matrix. Only the cases where $\ell_1 < \ell_2$ for all possible values of ℓ associated with the state, are required, specifically only for phase angles of 0 and $\frac{\pi}{2}$. More than the required amount of probabilities are usually calculated, which is called an over-complete measurement. This supplies more information than is required to actually reconstuct the density matrix. The modes being scanned over have the general equal superposition form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\ell_1\rangle + e^{i\theta}|\ell_2\rangle), \tag{3.4}$$

where θ is one of six possible phase angle.

QST scans through all combinations of two-level superpositions to reconstruct the density matrix, even for higher-dimensional QST. For example in a 3-dimensional QST, the state we want to reconstruct the density matrix for is in superposition of three possible states. The three states can be subdivided into six unique pairs, of which only three are ever necessary, namely the ones for which $\ell_1 < \ell_2$. This is done since each individual element in the density matrix is the outer product of

two states in the superposition.

The probability values calculated from the projective measurements (Figure 3.10) are compared to similar probabilities from many theoretical guessed density matrices and used to reconstruct the density matrix with a fidelity as high as possible. The guessed density matrix that minimizes the difference between the theoretical (guessed case) and experimental probabilities is taken as the density matrix of the system. An example of a over-complete two-dimensional QST, where the states $\ell = 1$ and $\ell = -1$ constitute the two-dimensional state, is shown in Figure 3.10. All 2D QST probability plots that follow will have the same arrangement as in this figure.

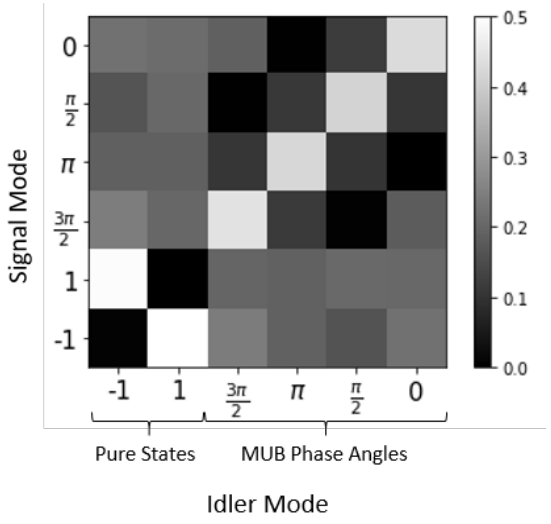

FIGURE 3.10: A grid of probability values that constitute a quantum state tomography measurement for a a two-dimensional state consisting of $\ell = 1$ and $\ell = -1$. These probability values will be compared to many other grids of probability values, each for a separate guessed density matrix.

In Figure 3.10 and in all QST measurements that follow, the whole grid is normalized by dividing every value by the sum of the pure state overlap or coincidence values to convert the values into probabilities [34]. The pure states are contained in the smaller two-dimensional array at the bottom left of the larger array.

The procedure in essence is to minimize the χ^2-squared distribution

$$\chi^2 = \sum_{i=1}^{N^2} \frac{(P_i^{\text{Experiment}} - P_i^{\text{Theory}})^2}{P_i^{\text{Theory}}}, \tag{3.5}$$

which aims to minimize the least square residuals between the theoretical and experimental probability values. P_i^{Theory} and $P_i^{\text{Experiment}}$ are the theoretical and experimental probabilities from the set of probabilities above.

The question is: how do these probabilities relate to the state itself? The density matrix of bipartite photon states can be written as

$$\rho = \sum_{m,n} b_{m,n} \tau_m \otimes \tau_n, \tag{3.6}$$

where the state is now a linear combination of the tensor product of the generalized Gell-Mann matrices of the dimension in question with coefficients $b_{m,n}$. These coefficients are exactly what is compared to the array of probabilities measured before.

Once a minimum has been found, the density matrix that corresponds to this minimum is taken as the final density matrix of the state. The final state density matrix should be positive semi-definite and hermitian implying that it has only non-negative eigenvalues and is equal to its own complex conjugate transpose. It must also have a unit trace to conserve probability. It is ensured that the guessed density matrices adheres to all these requirements by the following:

$$\rho_d = \frac{G^\dagger G}{Tr\left(G^\dagger G\right)}. \tag{3.7}$$

G is the final guess matrix that minimized the distribution, but did not adhere to all the requirements to actually be a physical state. ρ_d will be a physical state and is the final density matrix that is taken to be the density matrix of the system. The real and imaginary parts of the final density matrix are given in Figure 3.11.

The reconstructed state fidelity and linear entropy can now be calculated from the density matrix.

QST can also be done for higher dimensional systems, however, the amount of time the measurements take, scales with the amount of data points needed to do all superposition combinations. Since this increases rapidly with dimension, the higher the dimension, the longer it will take to finish the over-complete set of measurements.

QST was also done for a three-dimensional qutrit, that consisted of $\ell = -1, 0$, and 1 (Figures 3.12 and 3.13); and a four-dimensional state of $\ell = -2, -1, 1, 2$ (Figures 3.14 and 3.15).

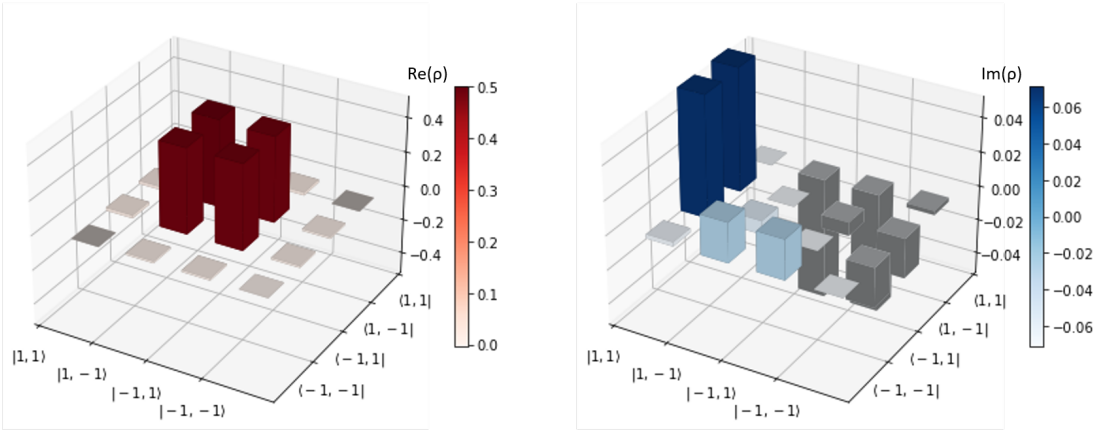

FIGURE 3.11: The final reconstructed density matrix as a result of the minimization above for the 2-dimensional entangled state $\ell = 1$ and $\ell = -1$. Each matrix element is the outer product of the labeled states on the x- and y-axis. Red: The real part of the density matrix. Blue: The imaginary part.

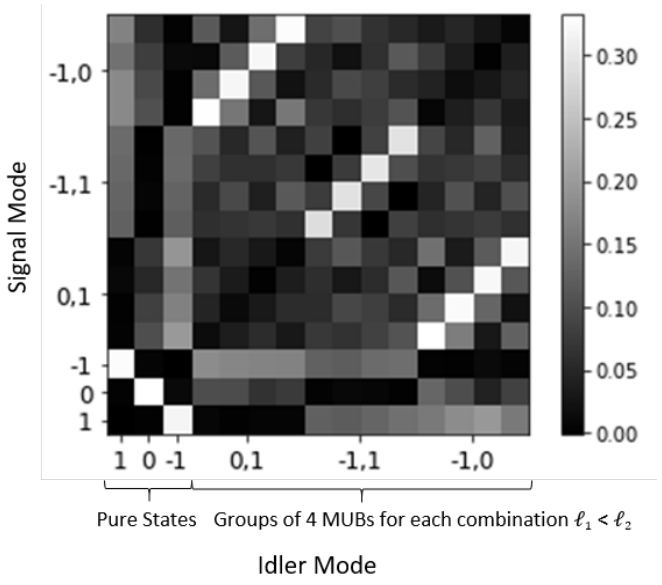

FIGURE 3.12: A grid of probability values that constitute a quantum state tomography measurement for a a three-dimensional state consisting of $\ell = 1$, $\ell = 0$, and $\ell = -1$. The MUB superposition states are subdivided into three sections of four states, where $\ell_1 < \ell_2$. The MUB angles remain fixed, but for new values of ℓ each time.

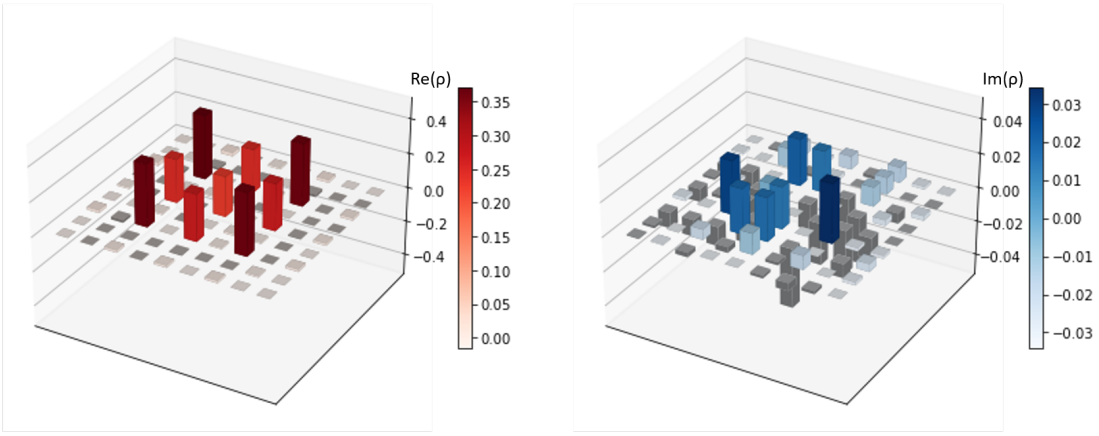

FIGURE 3.13: The final reconstructed density matrix for the 3-dimensional entangled state consisting of $\ell = 1$, $\ell = 0$, and $\ell = -1$. The x- and y-axes follow the same setup as before, where each element in the matrix is an outer product of state elements. Left: The real part of the density matrix. Right: The imaginary part of the density matrix.

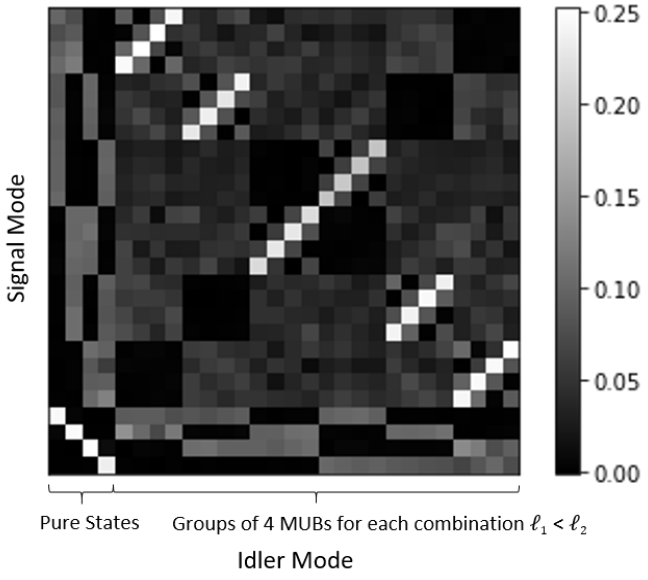

FIGURE 3.14: A grid of probability values that constitute a quantum state tomography measurement for a a four-dimensional state consisting of $\ell = -2$, $\ell = -1$, $\ell = 1$, and $\ell = 2$. The MUB superposition combinations follow the same pattern as before: they are separated into groups of four, where $\ell_1 < \ell_2$.

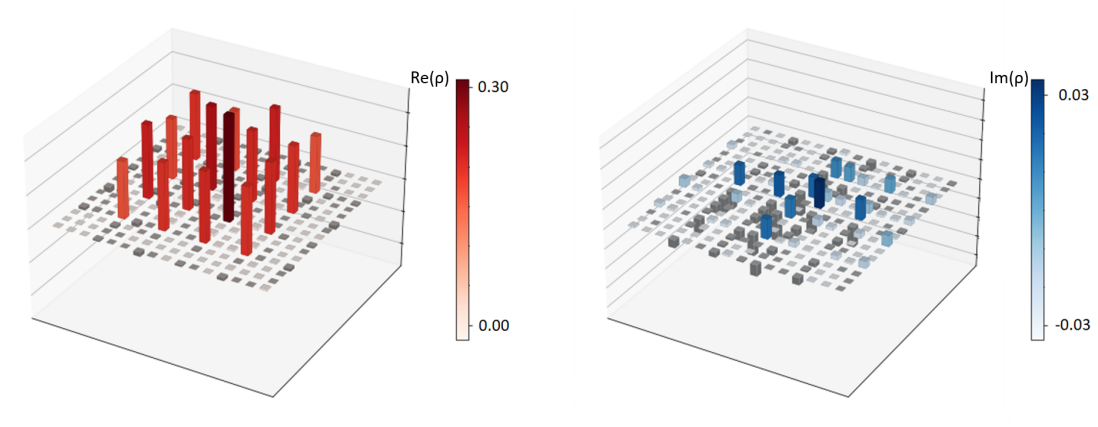

FIGURE 3.15: The final reconstructed density matrix for the 4-dimensional entangled state consisting of $\ell = 1$, $\ell = 2$, $\ell = -1$, and $\ell = -2$. The x- and y-axes follow the same setup as before.

The reconstructed state fidelities and linear entropies were calculated and are summarised in Table 3.1 below.

Dimension	Fidelity	Linear Entropy
2	0.984 ± 0.002	0.012 ± 0.006
3	0.913 ± 0.006	0.123 ± 0.016
4	0.839 ± 0.002	0.231 ± 0.026

TABLE 3.1: A table showing the relationship between the three states considered before and their reconstructed fidelities and linear entropies.

It is clear that the reconstructed state fidelity slowly decreased as the dimension increased, illustrating that is becomes increasingly difficult to reconstruct the density matrices accurately. The fidelity for the four-dimensional case is still above 80%, which is good enough to accept the reconstructed density matrix. The linear entropies increased, indicating that the states became more mixed as the dimension increased. In [34] both the fidelity and linear entropy were calculated up to a dimension of 8, where the fidelity and linear entropies approached values of 0.64 and 0.5, respectively.

The uncertainty values were calculated by using multiple QST runs. The increase in uncertainty in the linear entropy indicated that, as the dimension increased, more matrices were candidates to minimise the chi-squared distribution and to output a reconstructed density matrix. This was because a different mixed matrix minimised the chi-squared distribution in each individual run for a specific dimension. The higher the dimension, the more projective measurements required,

and the more readily the instantaneous quantum state can vary, changing the final density matrix and increasing the uncertainty measured in this way. The uncertainty in the fidelity remains relatively constant, which indicates that for each individual run, the reconstruction remains accurate, for that particular case, despite outputting a variety of dimension specific density matrices.

It is possible to perform QST for increasing dimensions, but one aspect that was ignored was the affect of the higher topological charge values on measured probabilities. We know that dimension decreases the accuracy of the reconstruction, but how does the spiral bandwidth tie together with QST? Figure 3.16 shows the QST grids for various ℓ values and Figure 3.17 shows the density matrix for the $\ell = 10$ case.

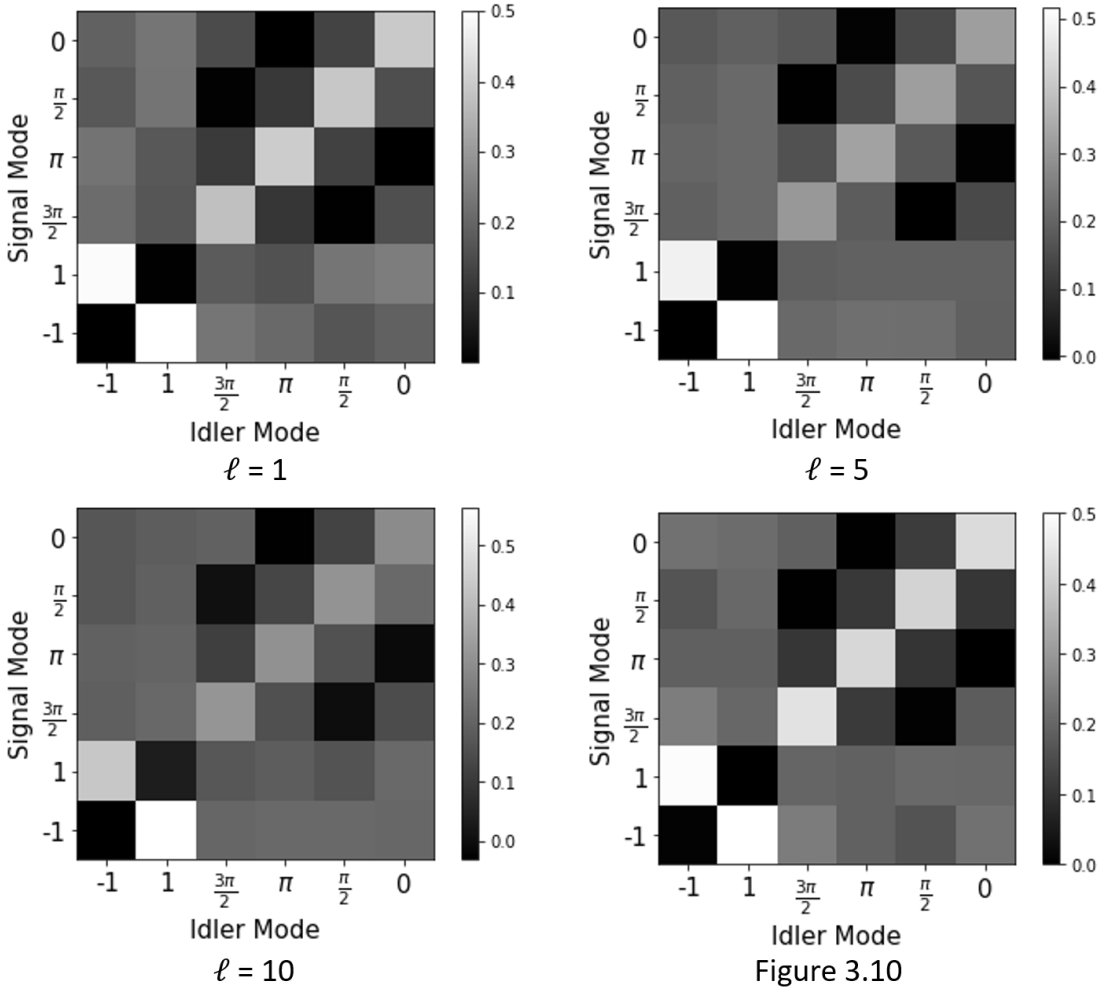

FIGURE 3.16: Overlap probability arrays for two-dimensional states consisting of $\ell = 1 - 1$, $\ell = 5, -5$, and $\ell = 10, -10$. The phase angles follow the same pattern as for the previous two-dimensional QST. The 2-dimensional QST run from figure 3.10 is included for visual comparison.

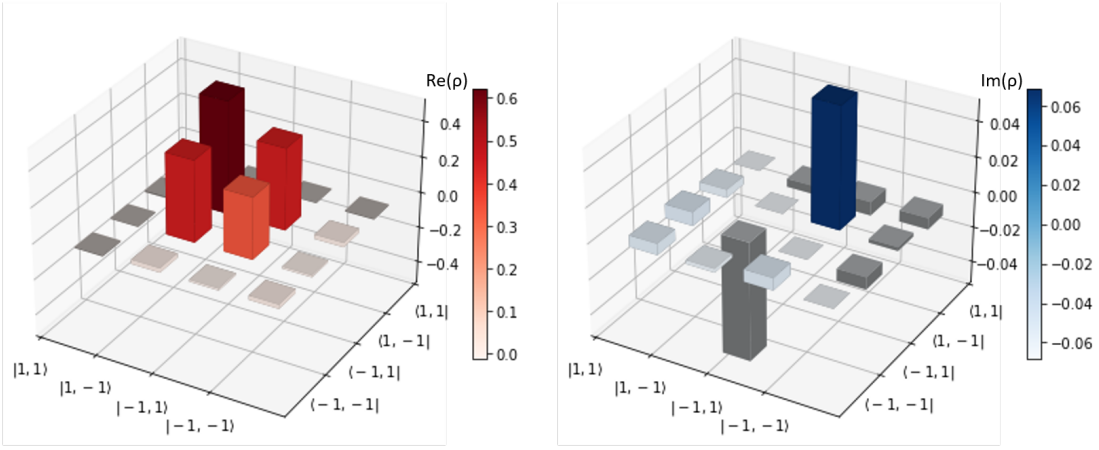

FIGURE 3.17: The reconstructed density matrix for $\ell = 10$.

ℓ	Fidelity	Linear Entropy	Concurrence
1	0.980 ± 0.001	0.019 ± 0.003	0.969 ± 0.002
5	0.982 ± 0.001	0.012 ± 0.003	0.966 ± 0.002
10	0.930 ± 0.001	0.082 ± 0.003	0.873 ± 0.002

TABLE 3.2: A table showing the relationship between two-dimensional states consisting of different OAM charges and their reconstructed fidelities, linear entropies, and concurrences.

The answer from Table 3.2 is that, as long as the setup is aligned, that the fidelity, linear entropy and even concurrence do not change markedly. There is a slight change when the OAM charge is increased to 10, which is most likely because of slight deviations in the shape of the OAM mode as seen before. If the shape deviates from a perfect ring, crosstalk is introduced, which will most definitely effect the QST measurements.

The uncertainty here was calculated using the $\ell = 1$ and $\ell = 5$ cases, because their values were almost equal and all three cases should be identical if it were not for the loss of coincidences with increasing ℓ. The $\ell = 10$ case was excluded, since it was clearly an outlier. Since all three runs are two-dimensional, and should be identical, it was assumed that the uncertainty was constant throughout each run.

3.1.2.1 The Importance of the First Order

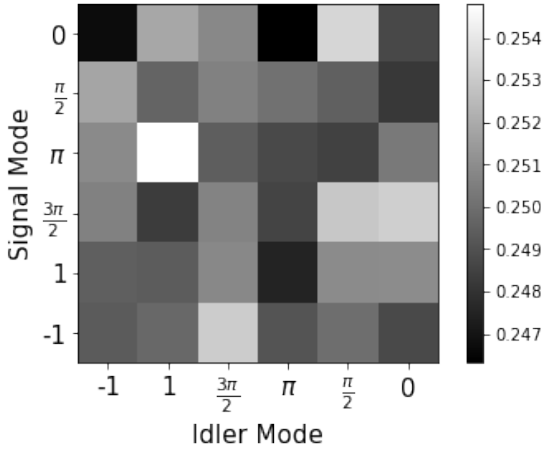

FIGURE 3.18: A failed attempt at taking a 2D QST for $\ell = 1$ and $\ell = -1$.

Figure 3.18 is what happens when a QST measurement is attempted without moving the setup from zero to first order. Since the zero order has no intrinsic OAM, there are no correlations or any patterns in the overlap between different mutually unbiased bases, which is why we see a nonsensical array of probability values. It is imperative that the setup be aligned to first order, before any measurement is made.

3.1.3 Bell Parameter

Entanglement witnesses are quantum measures used to identity whether or not quantum entanglement is present in a specific quantum state. One of the witnesses that is most commonly used and the one we will be focusing on, is whether the Bell parameter violates the CHSH-inequality [74]. In order to violate the CHSH-inequality and, by extension, for entanglement to be present, the Bell parameter must have a magnitude that is greater than 2. Therefore the CHSH-inequality is simply

$$S \leq |2|. \tag{3.8}$$

It is important to note that, for two-dimensional systems, there is still an upper bound to S called the Tsirelson bound, which is exactly $2\sqrt{2}$. For higher-dimensional states, the Bell test equivalent parameters can exceed this bound [72].

To calculate the Bell parameter S, four correlation coefficient (E) values are required, each of which are dependent on four separate coincidence count or coincidence count rate measurements. This implies that sixteen separate coincidence measurements are required to calculate the Bell parameter for one specific state.

The Bell parameter is calculated from the four correlation coefficients by:

$$S = E(\theta_A, \theta_B) - E(\theta_A, \theta'_B) + E(\theta'_A, \theta_B) + E(\theta'_A, \theta'_B), \tag{3.9}$$

where each individual correlation coefficient E is calculated using the coincidences at various hologram orientations (θ_A and θ_B) using

$$E(\theta_A, \theta_B) = \frac{C(\theta_A, \theta_B) + C(\theta_A + \frac{\pi}{2}, \theta_B + \frac{\pi}{2}) - C(\theta_A + \frac{\pi}{2}, \theta_B) - C(\theta_A, \theta_B + \frac{\pi}{2})}{C(\theta_A, \theta_B) + C(\theta_A + \frac{\pi}{2}, \theta_B + \frac{\pi}{2}) + C(\theta_A + \frac{\pi}{2}, \theta_B) + C(\theta_A, \theta_B + \frac{\pi}{2})}. \tag{3.10}$$

The angles $\theta_A = 0$, $\theta'_A = \frac{\pi}{4}$, $\theta_B = \frac{\pi}{8}$ and $\theta'_B = \frac{3\pi}{8}$ are the angles for which the Bell inequality violation is a maximum and are the angles required for the four correlation coefficients to be calculated.

Coincidences represent the degree of overlap between some chosen state and the greater SPDC state, which means that the state being used to calculate the Bell parameter through overlap measurements matters. In this case the state in both arms is simply the generic quantum superposition state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\ell_1\rangle + e^{i\phi}|\ell_2\rangle), \tag{3.11}$$

where the amplitude factors are replaced by the normalisation factor $\frac{1}{\sqrt{2}}$ to only consider states that are on the equator of the Bloch sphere, which has the effect of only considering states where both constituents are equally likely. Projection of the SPDC down to states on the equator can be simplified by writing states on the equator as [74]

$$|\theta_i\rangle = \frac{1}{\sqrt{2}}(|\ell_1\rangle + e^{2i\theta_i}|\ell_2\rangle), \tag{3.12}$$

where θ_i is now the hologram orientation. This means that the phase angle changes by half of the physical rotation of the hologram orientation angle. θ_A and θ_B are the angles θ_i in the two separate arms.

Superposition holograms of the above state are encoded on both SLMs for whatever choice of ℓ and varying hologram orientations θ_A and θ_B for the two SLMs. By hologram orientations it is meant that the holograms are physically being rotated through 180°. Rotating the holograms such that the relative angular separation changes, the superposition states used in the overlap between the two modes in the two arms, scans through all possibilities including the MUBs from before as well as the angles where maximal violation occurs.

The coincidence measurements used to calculate the four correlation coefficients are then extracted from the resulting so-called Bell curves. Each curve corresponds to a specific hologram orientation on one SLM and every point on these curves represent a coincidence measurement for a specific hologram orientation on the other SLM. A typical example of the curves from which these values are extracted, is illustrated below.

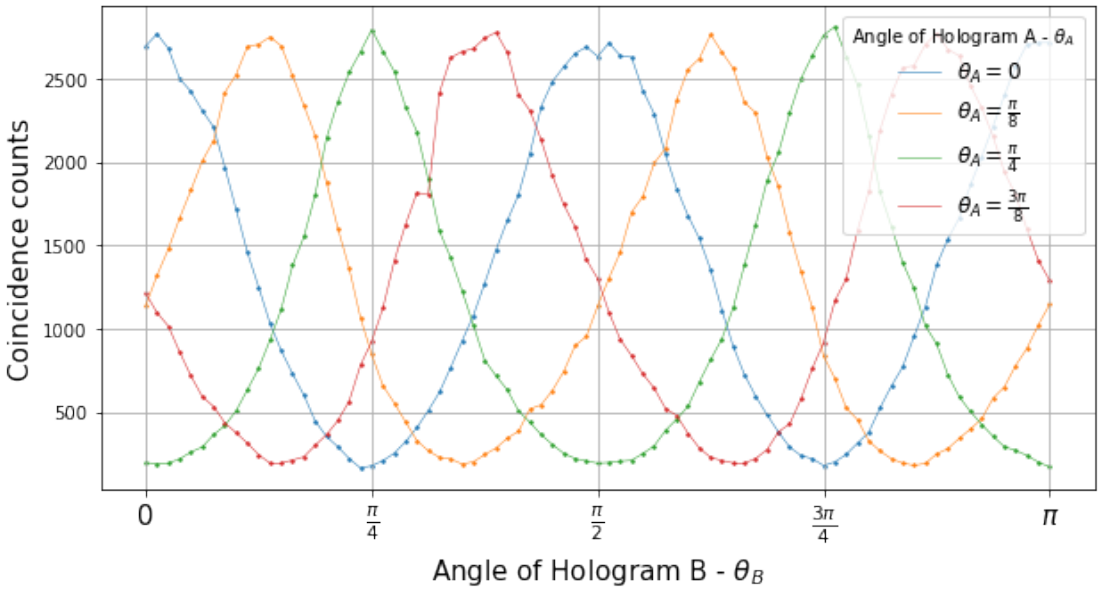

FIGURE 3.19: An example of the four required Bell or coincidences versus hologram angle θ_B curves for a Bell parameter calculation for $\ell = 1$ at hologram angles $\theta_A = 0$, $\frac{\pi}{8}$, $\frac{\pi}{4}$ and $\frac{3\pi}{8}$.

The Bell parameter S for Figure 3.19 or the $\ell = 1$ case is 2.73 ± 0.09.

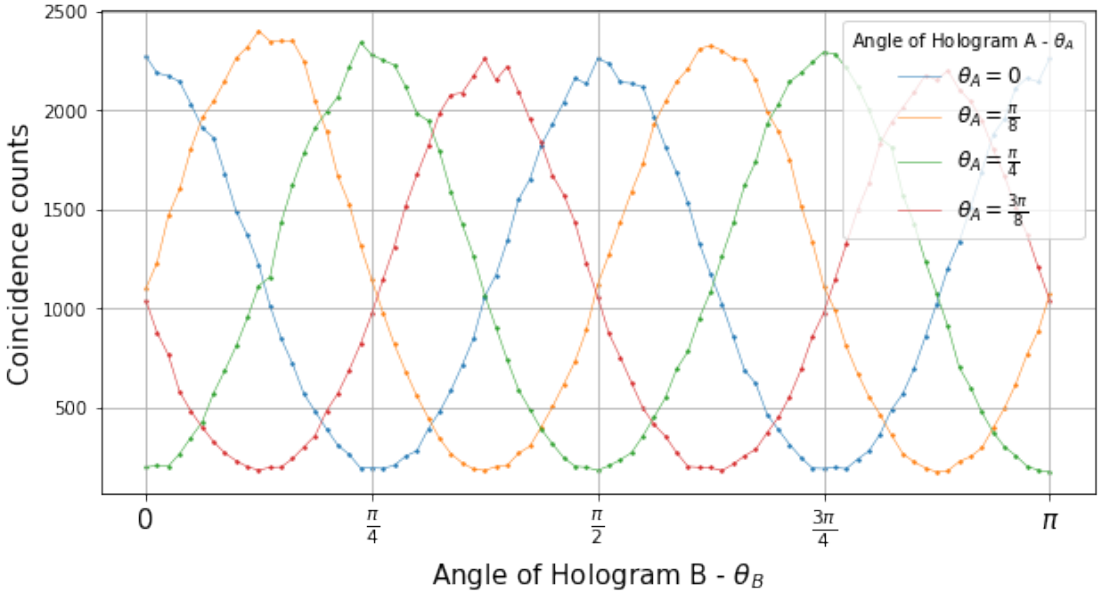

FIGURE 3.20: An example of the four required Bell or coincidences versus hologram angle θ_B curves for a Bell parameter calculation for $\ell = 2$ at hologram angles $\theta_A = 0$, $\frac{\pi}{8}$, $\frac{\pi}{4}$ and $\frac{3\pi}{8}$.

The Bell parameter S for Figure 3.20 or the $\ell = 2$ case is 2.66 ± 0.05.

The Bell parameters calculated from the above curves are both greater than 2 and thus indicate a Bell violation and the presence of entanglement. The curves follow the general sinusoidal form associated with Bell curves and their amplitudes. The period of these curves is 2, which is consistent with the 2 in the overlap of the SPDC and the phase factor in the equator states before.

The Bell curve periodicity can be found in overlap calculations. Let the shared entangled state and projection states be $|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|\ell\rangle_A|-\ell\rangle_B + |-\ell\rangle_A|\ell\rangle_B)$; and $|\theta_A\rangle$ and $|\theta_B\rangle$, respectively. This means that the overlap becomes

$$\begin{aligned} \text{Overlap}_{A,B} &= \langle\theta_B|\langle\theta_A|\psi_{AB}\rangle, \\ \text{Overlap}_{A,B} &= \frac{1}{2\sqrt{2}}(e^{2i\theta_B} + e^{2i\theta_A}), \end{aligned} \tag{3.13}$$

where in the last step the orthogonality of the OAM modes are used to remove some terms. Taking the modulus squared to get intensity, which is proportional to coincidences, the expression becomes

$$
\begin{aligned}
C(\theta_A, \theta_B) &= \frac{1}{8}(e^{2i\theta_B} + e^{2i\theta_A})(e^{2i\theta_B} + e^{2i\theta_A}), \\
C(\theta_A, \theta_B) &= \frac{1}{8}(2 + e^{-2i(\theta_B - \theta_A)} + e^{2i(\theta_B - \theta_A)}), \\
C(\theta_A, \theta_B) &= \frac{1}{4}(1 + \cos(2(\theta_B - \theta_A))), \\
C(\theta_A, \theta_B) &= \frac{1}{2}(\cos^2(2(\theta_B - \theta_A))),
\end{aligned}
\tag{3.14}
$$

where De Moivre's formula and trigonometric identities have been applied to reach the final expression showing the periodicity of 2 in the argument.

It is hard to tell from just two cases, but the Bell parameter S tends to decrease as we increase the topological charge. This is because as the OAM charge increases, the overall size of the mode does as well, which when increased far enough will cause the intensity of the mode to distribute over a larger area. When coupled into the fibres, some of the light will be excluded and it is this loss that is the cause of the decrease in Bell parameter with increasing ℓ.

This can be illustrated by calculating the visibility of the Bell curves. Visibility can be thought of as a measure of how easy it is to distinguish between the peaks and troughs of a sinusoidal signal and is calculated using

$$
V_\ell = \frac{C^\ell_{\max} - C^\ell_{\min}}{C^\ell_{\max} + C^\ell_{\min}}, \tag{3.15}
$$

where V_ℓ is the visibility for OAM charge ℓ and $C^\ell_{\min,\max}$ are the minimum and maximum coincidence values from the Bell curves.

ℓ	Visibility	Date
1	0.879 ± 0.004	09/14/2021
2	0.861 ± 0.005	09/14/2021
3	0.906 ± 0.002	09/15/2021
4	0.767 ± 0.003	09/14/2021

TABLE 3.3: Table showing the correspondence between the topological charge and the visibility of the Bell curves. (Dates are included, since the setup on the day changed because of complete realignment.)

Table 3.3 shows that the visibility of the Bell curves decrease with increasing ℓ, which causes the coincidence measurements required to calculate the Bell parameter to approach each other as the curves contract. Eventually the visibility will

be low enough to be dominated by noise and for the Bell parameter to no longer violate the CHSH-inequality and for entanglement to disappear.

3.1.3.1 A Failed Attempt

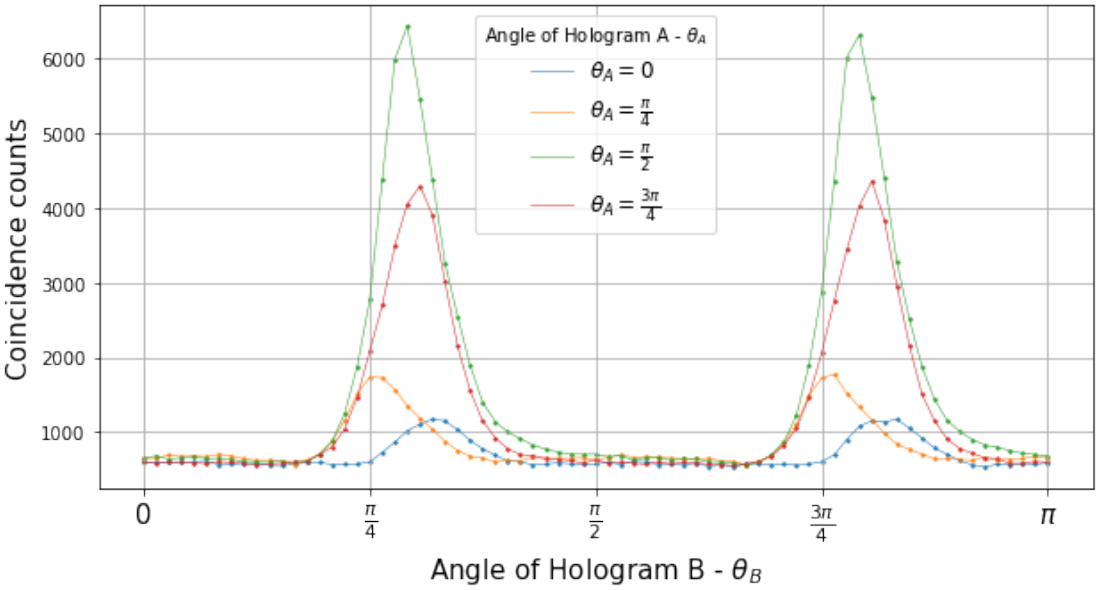

FIGURE 3.21: A failed attempt at taking a Bell measurement for $\ell = 1$ where there is no sinusoidal behavior.

Considering the failed Bell parameter experiment in Figure 3.21, where the holograms are still rotated the full 180 degrees, it is immediately observed that the Bell curves do not adhere to the sinusoidal behaviour normally expected.

It turns out that the reason for the lack of sinusoidal behavior is what happens when the SPDC signal and idler beams are not centered properly on the SLM screens. As both SLM holograms are rotated over the π radians, the beam is only ever incident on only a grating, which, depending on its orientation directs the first order away from the detectors. As it slowly rotates it brings the first order back into position, which is why we still see the peak periodically return. The periodicity is two, consistent with all Bell plots so far. The reason for the difference in width in the four Bell curves is because of the orientation of the SLM in arm A. Since only four angles are considered, some angles might have diverted the first order beam further away from the detector than other angles, which is why for those the peak width is smaller.

3.1.3.2 Sector States

In [70] they defined the states differently by introducing sector states. These states are defined by introducing a phase factor of $e^{i\ell\phi}$ and $e^{-i\ell\phi}$ for both ℓ states in the superposition

$$|\Theta\rangle = \frac{1}{\sqrt{2}}(e^{i\ell\theta}|\ell\rangle + e^{-i\ell\theta}|-\ell\rangle), \tag{3.16}$$

where the phase angle θ now represents a relative phase. The ℓ will ultimately determine the periodicity of the Bell curves, since it defines the periodicity of alternating phases over the entire transverse distribution. The correlation coefficients are now calculated using

$$E(\theta_A, \theta_B) = \frac{C(\theta_A, \theta_B) + C(\theta_A + \frac{\pi}{2\ell}, \theta_B + \frac{\pi}{2\ell}) - C(\theta_A + \frac{\pi}{2\ell}, \theta_B) - C(\theta_A, \theta_B + \frac{\pi}{2\ell})}{C(\theta_A, \theta_B) + C(\theta_A + \frac{\pi}{2\ell}, \theta_B + \frac{\pi}{2\ell}) + C(\theta_A + \frac{\pi}{2\ell}, \theta_B) + C(\theta_A, \theta_B + \frac{\pi}{2\ell})}. \tag{3.17}$$

The angles $\theta_A = 0$, $\theta'_A = \frac{\pi}{4\ell}$, $\theta_B = \frac{\pi}{8\ell}$ and $\theta'_B = \frac{3\pi}{8\ell}$ are the angles for which the Bell inequality violation is a maximum. Now the factor of ℓ has to be included, since the angles dynamically change based on the topological charge. The coincidence values as usual are measures of overlap and from the overlap calculation the theoretical curves can be modelled as

$$C(\theta_A, \theta_B) \propto cos^2[\ell(\theta_A - \theta B)]. \tag{3.18}$$

It is easy to simulate what the Bell curves would look like for sector states. For the $\ell = 2$ case they have a periodicity of two, just like before, with a constant amplitude throughout.

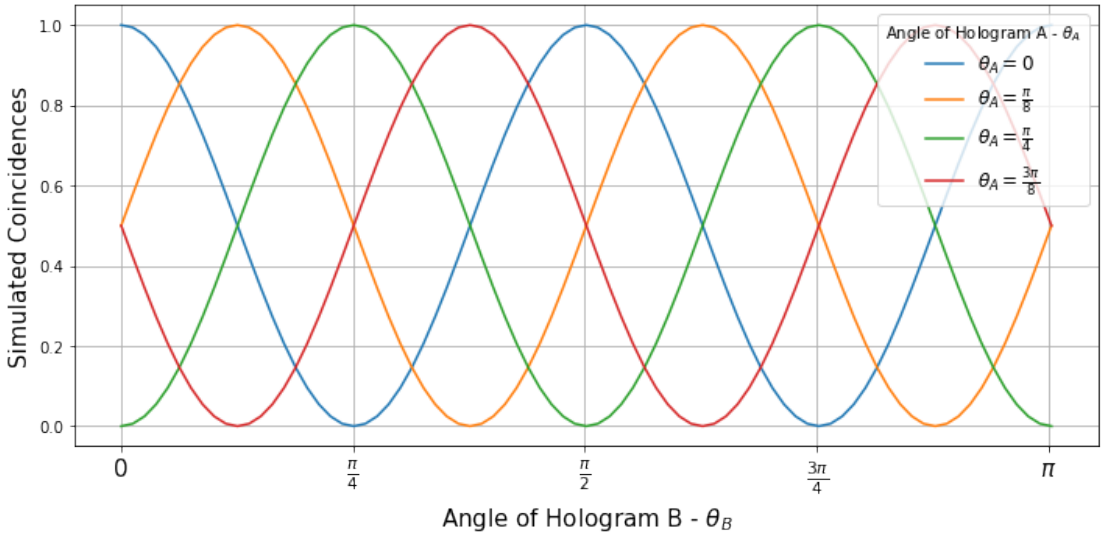

FIGURE 3.22: Simulation of the four required Bell or coincidences versus hologram angle θ_B curves for Bell parameter calculation for $\ell = 2$ at hologram angles $\theta_A = 0$, $\frac{\pi}{8}$, $\frac{\pi}{4}$ and $\frac{3\pi}{8}$.

For the simulated Bell curves of a two-dimensional case (Figure 3.22), defined using sector states, the Bell parameter is $2\sqrt{2}$ implying the state is maximally entangled.

Chapter 4

Quantum Key Distribution

With the quantum revolution well under way and the dawn of quantum computers becoming more and more of a reality, there is a genuine existential threat to current classical encryption methods, as the computational power of quantum computers makes it possible to completely decrypt common encryption methods. It is imperative to use the same quantum mechanical nature that quantum computers use to skyrocket their computational power, in quantum cryptographic encryption methods to guard against the impending quantum computers. One of the most well-known and studied quantum encryption methods is the subfield of quantum key distribution.

This chapter investigates the use of spatial entanglement in the application of quantum key distribution. The goal is to use various physical properties of physical systems, in this case of light, to encode information and be able to communicate it via a quantum communication channel that is considered secure. Quantum key distribution protocols, the procedures or algorithms used to securely communicate information, are protocols designed to introduce an inherently arbitrary measurement outcome of the encoded information, should an attacker try to listen in. It exploits the quantum mechanical behaviour in order to make it as difficult as possible for an attacker to decipher what is being communicated.

There are many quantum key distribution protocols, but the two protocols that the focus is placed on here, are the BB84 and E91 protocols. The BB84 protocol designed by Bennett and Bassard in 1994 [75, 76] is possible because of how the measurement bases are chosen. The BB84 protocol is such that many quantum systems, such as photons, are sent from a sender called Alice, to a receiver called Bob, where each randomly chooses between the measurement basis with the end goal of finding a secret key by sifting through all measurement outcomes. The

E91 protocol designed by Eckert [77] is practically identical to the BB84 protocol in operation, but the key difference is that instead of Alice sending Bob photons, they both receive one of an entangled pair of photons, apply their random choice of basis measurement independently and compare afterwards to create a secret key. There are more QKD protocols, which include: the Six-State [78] that uses three bases to encrypt information [79], BB92 [80] that only uses two states rather than four in its operation [79], SARG04 [81] which is less robust to noise and undergoes less erorr during attacks [79], COW [82] that also uses entanglement and is used for weak coherent pulses [79], DPS [83] that is simple to set up and is more robust to attacks [79], etc.

QKD has been performed many times over, only with slight changes or tweaks introduced to investigate the possible addition of new properties. QKD has been performed in the polarisation bases [84, 85], in the OAM basis [86], and even using spatial mode bases [85]. The affects of turbulence on QKD has been explored [87] in order to test whether QKD is robust to turbulence. Hybrid entangled states have been used in a multiplexing schemes to increase the dimensionality of E91, by using multiple 2-dimensional subspaces [88]. Other non-spatial degrees of freedom can be used, such as time-frequency entanglement, even targeting its use in free space optical channels [89]. It is clear that the amount of combinations are seemingly endless.

The ultimate goal of QKD is to make quantum communication channels robust to eavesdropping attacks. There exist many eavesdropping or attack strategies with the goal of extracting information from a supposedly secure quantum channel and they all are designed to optimise two separate factors. The one is to extract as much information as possible by intercepting the signal being sent, while at the same time minimising how detectable the attack is. Quantum key distribution as a field is thus the use of algorithms to make both of these goals as hard as possible for the attacker. There are two core eavesdropping strategies that will be considered: collective attacks and individual attacks [90].

The intercept-resend individual attack strategy involves measuring the quantum states before they reach their intended target and then sending the collapsed state on towards where it was originally intended [91]. Doing this has the most impact on the measurement outcomes of one of the communicating parties and is also the most readily detected strategy. When an attacker intercepts and measures every single quantum state in the string of states used for QKD in this way, all of the states that eventually reach the receiver, Bob, will have collapsed to a predetermined state, maximally influencing Bob's measurements and eventually

maximising the error in the measurement.

Collective attacks can be illustrated by considering a scenario where a string of N qubit states are encoded using any amount of bases and sent from Alice to Bob. If an eavesdropper, Eve, decides to attach a probe to a random substring of photons contained within the total sent string in order to simultaneously measure their states, then this eavesdropping strategy is called a coherent or collective attack [92, 93]. Eve can do this for any substring or any amount of substrings. She can even attack the entire string of states being sent.

According to [94], there are certain threshold values for the quantum bit error rate in both of these attacking strategies that are important to keep in mind. The quantum bit error rate quantifies the amount of influenced error in the measurement of the states and will be expanded upon later. If the eavesdropper applies a coherent attack, while simultaneously trying to remain discreet, the maximum quantum bit error rate that she can introduce is 11%. This happens when Eve chooses to coherently attack a substring that is much shorter than the total sent string. For individual attacks the quantum bit error rate must be 15% or lower in order for Alice and Bob to improve security through error correction and privacy amplification. These are techniques used to improve the security of the channel, where the details are ignored.

It is now possible to get into the two protocols investigated, while still remembering the threshold values to aim for.

Chapter 4 starts with the BB84 protocol, explaining the procedure on how security analysis is performed. Two-dimensional QKD results are included and discussed by way of secret key rate calculations and the channel transfer matrices. The BB84 protocol is then generalised to high-dimensions, which is for dimensions more than two. The E91 protocol is linked to the BB84 protocol as being its entanglement equivalent and the protocol itself with its security checks are included.

4.1 BB84 Protocol

The BB84 protocol is made possible because of the concept of mutually unbiased bases and is illustrated in Figure 4.1. Alice sends Bob bits of information after encoding the bits as photons carrying certain polarisation or orbital angular momentum. Encoding can be done in any chosen degree of freedom, but as usual the focus is placed on OAM. She uses two bases from which she randomly selects one to encode information for every single photon. Bob, after receiving the photons, must randomly select between the same two mutually unbiased basis to

measure the photons, without knowing Alice's encoding basis. One state from each basis corresponds to a 1 and the other state from each basis corresponds to a 0 in a bit string. This is decided beforehand and agreed upon before any bits of information are communicated. If the encoding and measuring bases match, the measurement result will collapse the photon superposition state to the correct bit value. If the bases are mismatched, the result will either be the correct bit value or the incorrect one. Both of these outcomes are equally probable, which means that the measurement was completely inconclusive, which is a direct consequence of the two bases being mutually unbiased. After a certain amount of photons have been encoded, sent, and measured, either in the correct or incorrect basis, the string of basis choices are compared and where the bases match, the bit values are saved as a bit string called the sifted key. This is the key generation part of the BB84 protocol. The other values are all simply discarded as they do not supply enough information for Bob to know what the state was that Alice encoded. In other words, Bob immediately knows that the basis was incorrect and can easily conclude that he should have chosen the other basis, but he cannot know whether the bit value should be a 1 or a 0. The two mutually unbiased bases to be used are denoted by ϕ and ψ.

Encoded Bit String	1	0	0	1	1	0	1	0	0	1	0	1	1
Alice	ψ	ψ	ϕ	ψ	ψ	ϕ	ϕ	ϕ	ψ	ϕ	ϕ	ψ	ϕ
Bob	ϕ	ψ	ϕ	ψ	ϕ	ϕ	ψ	ϕ	ϕ	ϕ	ϕ	ψ	ψ
Measured Bit String	0	0	0	1	1	0	0	0	0	1	0	1	1
Sifted Key	-	0	0	1	-	0	-	0	-	1	0	1	-

FIGURE 4.1: The BB84 protocol applied to a bit string of 13 bits. If the encoding and measuring bases match, then the measurement will supply the correct bit value. If the bases mismatch, the measurement outcome will be correct 50% of the time and incorrect 50% of the time, which is why they are discarded.

In the ideal case, where no systematic noise or eavesdropping is present, the sifted key will be 50% efficient, since Bob and Alice will randomly, correctly match their

chosen bases half of the time. In an experimental or practical implementation of the above protocol, the amount of correct bit values will decrease. Sometimes when the bases chosen by Alice and Bob match, the bit value that is measured will not be the correct bit value. The reason for the incorrect measured bit value, despite using the correct basis, has to do with an eavesdropper, Eve, trying to listen in on the channel or noise being introduced to the system in some way that may have altered the state of the photon. The integrity or security of the channel and protocol is dependent on its robustness to both an eavesdropper and noise, but circumventing an eavesdropper is more important. Eavesdropping is possible when a third party, Eve, tries to extract the information being sent by intercepting and measuring the photons being sent by Alice prematurely or before they reach Bob. She does this by choosing randomly between the same two bases that Alice and Bob have access to. This has the affect of collapsing the superposition of the photon, which will ultimately effect the accuracy of Bob's measurements. If Eve intercepted all of the photons sent then she would guess right half of the time, which means that when Bob measured the photons after they have been intercepted that he would only ever get the correct bit value 25% of the time.

The accuracy of Bob's measurements can be quantified using the quantum bit error rate. The amount of times the bases choices match, but the incorrect bit values are measured by Bob, are all counted and divided by the total amount of times the bases choices matched, which results in an error value Q called the quantum bit error rate. Q is, in other words, a measure of the probability that Bob measures the incorrect state or bit value, despite choosing the correct basis.

Instead of counting the amount of incorrect measurements, another way of calculating Q is to use overlap probabilities between modes [85] in an equation that subtracts the measuring fidelity from unity. The measuring fidelity is a measure of how accurately Bob measures the sent photons taking into consideration the communication channel. The communication channel is represented by matrix operator $\hat{U}$, where physical channels tend to alter the state by perturbations. This affect tends to become more pronounced as the state dimension is increased. Calculating Q using the measuring fidelity is done by using

$$\begin{aligned} Q_\psi &= 1 - \frac{1}{2}\sum_{i=1}^{2} |\langle \psi_i^{\text{Bob}} | \hat{U} | \psi_i^{\text{Alice}} \rangle|^2, \\ Q_\phi &= 1 - \frac{1}{2}\sum_{i=1}^{2} |\langle \phi_i^{\text{Bob}} | \hat{U} | \phi_i^{\text{Alice}} \rangle|^2, \end{aligned} \tag{4.1}$$

where the quantum bit error rate is defined as the mean of the above two values:

$$Q = \text{mean}(Q_\phi, Q_\phi). \tag{4.2}$$

Once the quantum bit error rate for the protocol has been calculated it can be used to calculate other important measures such as the key rate R and the eavesdropper Eve's cloning fidelity. The key rate is the amount of bits of information that Alice and Bob can share securely, and Eve's cloning fidelity F_{Eve} is a measure of how similar what she measures is to the state sent from Alice to Bob. The secret key rate is calculated using [85]

$$R(d, Q) = \log_2(d) + 2(1-Q)\log_2(1-Q) + 2Q\log_2\left(\frac{Q}{d-1}\right). \tag{4.3}$$

This can be plotted for various choices of dimension d and a whole range of quantum bit error rate Q, as in Figure 4.2. The y-axis is logarithmic for the profile of the key rate to be more readily recognised.

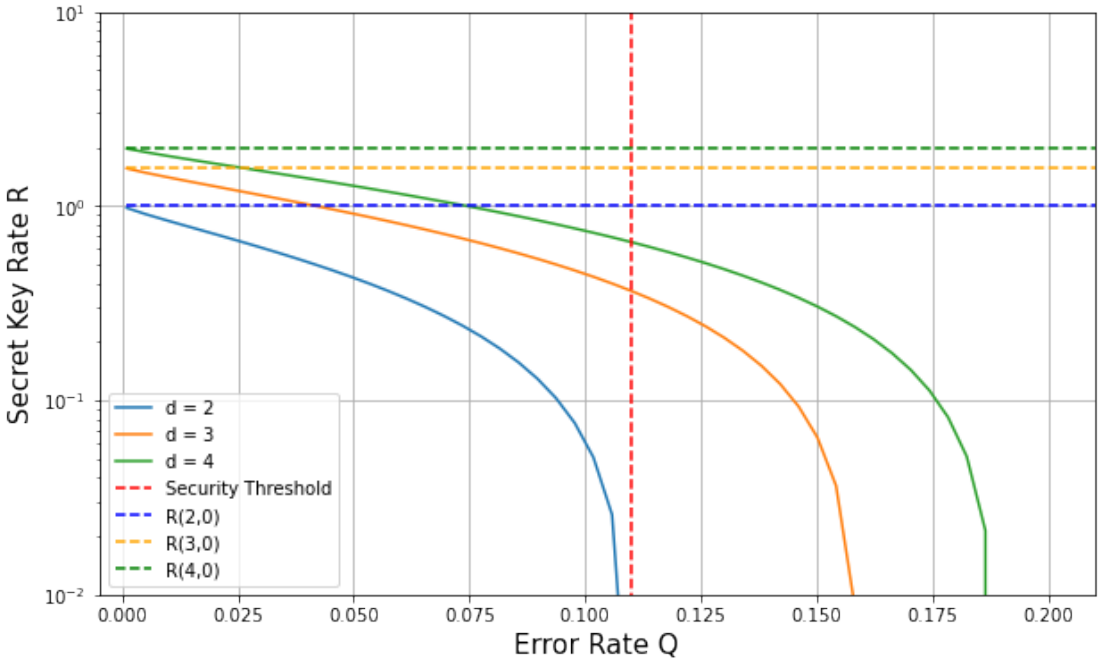

FIGURE 4.2: The generated key rate R versus the quantum bit error rate Q for dimensions 2, 3 and, 4. Also included are the maximum lines for the key rate for all three dimensions to illustrate how increasing the dimensions increase the secret key rate that can be generated. Finally the red dashed line represents the minimum Q that is aimed for, which is set because of eavesdropping strategies.

The two-dimensional line does not intersect the Q threshold value, which means that for two-dimensional BB84 QKD, an eavesdropper can never totally decrypt a message sent by Alice without having alerting both Bob and Alice immediately by letting the secret key rate go to zero. For higher dimensions there is a dedicated range where the protocol is considered completely secure, but eventually if the error becomes large enough, the secret key rate will still go to zero.

Eve's cloning fidelity can be calculated using

$$F_{\text{Eve}}(d,Q) = \frac{1}{d}\left(1 + (d-2)Q + 2\sqrt{(d-1)Q(1-Q)}\right). \tag{4.4}$$

Other measures that can also be used are the shared or mutual information between Bob and Alice $I_{\text{Alice,Bob}}$ and Alice and Eve $I_{\text{Alice,Eve}}$. The amount of information here is measured in bits, hence the base of 2 in the logarithmic functions. All four of these measures are functions of the dimension and Q of the channel [85]. The shared information between Bob and Alice and Alice and Eve are given by

$$\begin{aligned} I_{\text{Alice, Eve}}(d,Q) = \log_2(d) + (F_{\text{Eve}} - Q)\log_2\left(\frac{F_{\text{Eve}} - Q}{1-Q}\right) \\ +(1-F_{\text{Eve}})\log_2\left(\frac{1-F_{\text{Eve}}}{(d-1)(1-Q)}\right), \end{aligned} \tag{4.5}$$

$$\begin{aligned} I_{\text{Alice,Bob}}(d,Q) = \log_2(d) + (1-Q)\log_2(1-Q) \\ +Q\log_2\left(\frac{Q}{d-1}\right), \end{aligned} \tag{4.6}$$

where there are constraints placed on the amount of information shared between Bob and Alice and Alice and Eve. When Eve interrupts the channel by eavesdropping, changing the state of the sent photons, she can increase the shared information between her and Alice, but simultaneously decrease the amount of shared information between Bob and Alice. This is where the usefulness of this protocol lies: because of the probabilistic nature of quantum mechanics, Eve can never eavesdrop and gain all of the information she needs, without alerting Alice and Bob immediately that someone attacked their channel.

The channel through which the QKD transmission occurs can be characterized using the usual overlap of separate modes. These overlap values create arrays called the transfer matrices (Figure 4.3) and they can also be used to extract the

quantum bit error rate and the measuring fidelity.

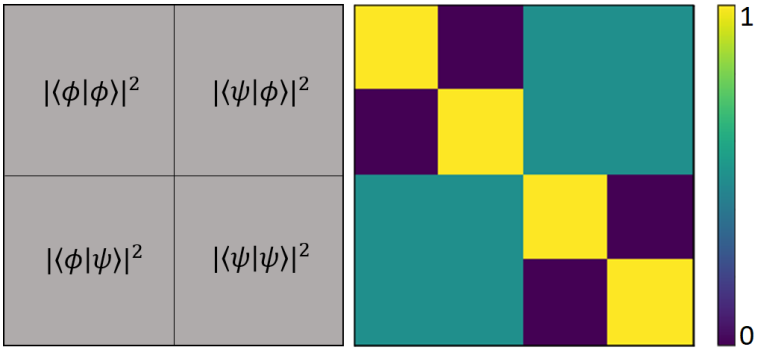

FIGURE 4.3: Simulated transfer matrices for the BB84 protocol plotted to show overlap probability. The basis choice mismatched overlap values are in the bottom left and top right 4x4 grids. The top left and bottom right 4v4 grids show what the overlap is when the basis choices match.

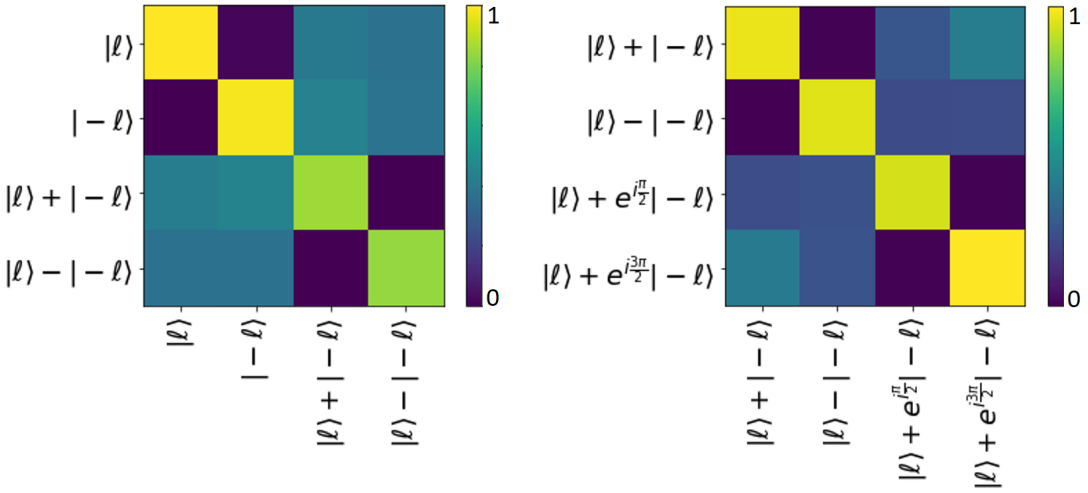

FIGURE 4.4: Two experimental transfer matrices for two separate sets of mutually unbiased bases for the $\ell = 1$ case. Left: $\psi = \{|\ell\rangle, |-\ell\rangle\}$ and $\phi = \{|\ell\rangle + |-\ell\rangle, |\ell\rangle + |-\ell\rangle\}$. Right: $\psi = \{|\ell\rangle + |-\ell\rangle, |\ell\rangle + |-\ell\rangle\}$ and $\phi = \{|\ell\rangle + e^{i\frac{\pi}{2}}|-\ell\rangle, |\ell\rangle + e^{i\frac{3\pi}{2}}|-\ell\rangle\}$.

For reference, let the transfer matrix on the left hand side of Figure 4.4 be "Run 1". The other transfer matrix will be "Run 2". The results for the three transfer matrices are summarised in Tables 4.1 and 4.2.

The simulated run shows that for a completely perfect QKD where $Q = 0$, Eve's cloning fidelity minimises to 50%. This cloning fidelity is not nearly high enough for Eve to be able to clone the state being sent and can be considered completely

Run	Q	F	F_{Eve}
1	0.0751 ± 0.0217	0.925 ± 0.021	0.764 ± 0.044
2	0.0318 ± 0.0217	0.968 ± 0.021	0.676 ± 0.044
Simulated	0	1	0.5

TABLE 4.1: First table showing the calculated measures discussed before for decreasing Q.

Run	R	$I_{\text{Eve,Alice}}$	$I_{\text{Alice,Bob}}$
1	0.230 ± 0.181	0.242 ± 0.066	0.701 ± 0.072
2	0.593 ± 0.181	0.109 ± 0.066	0.845 ± 0.072
Simulated	1	0	1

TABLE 4.2: Second table showing the calculated measures discussed before for decreasing Q.

inaccurate, since only half of the state has been reconstructed. This is consistent with the fact that the shared information between Eve and Alice is 0 bits. The key rate is 1, which is the maximal value for $d = 2$. Alice and Bob share 1 bit of information in the ideal case as the use of the photons are used to their maximum potential, while any noise is non-existent and no eavesdropping occurred.

In both run 1 and 2 it is clear that deviation from the simulated run has occurred. In both runs, eavesdropping was not introduced whatsoever, so any error being introduced is due to systematic or external noise sources. Both Q values, 7.51% and 3.18% are below the 11% mark, which is consistent with figure 4.2. The key rate drops tremendously as Q increases, which is also consistent with that plot.

If it is assumed that the error was caused by an eavesdropper instead, the cloning fidelity and shared information could be calculated. The more error introduced to the channel, the higher the cloning fidelity becomes, but the easier it will be to detect, since the measuring fidelity must conversely decrease. Another observation is that the shared information between Alice and Bob; and Eve and Alice do not add to unity. This means that there is always a loss of information because of both noise and eavesdropping.

The uncertainty in all measurements in the tables above were calculated as a standard error using only run 1 and 2. This means that the uncertainties are large compared to the actual experimental values, but since both runs are for exactly the same topological charge, only different bases, theoretically they should have been identical.

We can apply a two-dimensional QKD for higher charges of OAM in order to see

if the results are consistent with what we have seen so far. The transfer matrices for increasing ℓ is included in Figure 4.5.

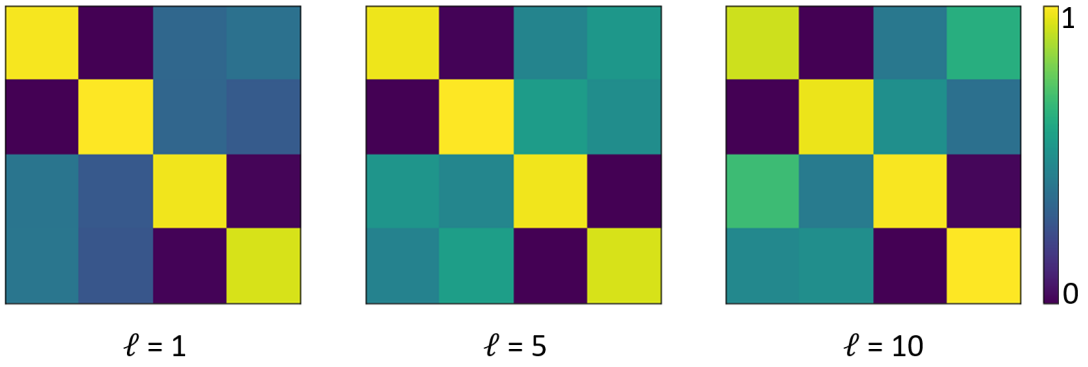

FIGURE 4.5: Three separate transfer matrices for the cases $\ell = 1$, $\ell = 5$, and $\ell = 10$. The matrix elements are all normalised so that the range remains from 0 to 1 throughout all three cases, where in reality for lower OAM, the coincidences measured were actually more.

Visually it is already clear that the results became more prone to error, but a table is required to summarise the results.

Run	Q	F	r
Simulated	0	1	1
$\ell = 1$	0.017 ± 0.01	0.983 ± 0.001	0.761 ± 0.012
$\ell = 5$	0.031 ± 0.01	0.969 ± 0.001	0.610 ± 0.012
$\ell = 10$	0.053 ± 0.01	0.947 ± 0.001	0.406 ± 0.011

TABLE 4.3: Table showing the relationship between the topological charge of the 2-dimensional state, the quantum bit error rate, and the secret key rate generated.

We see from Table 4.3 that the error rate increases, and consequently the secret key rate decreases, with OAM charge. This has been observed before in both QST and spiral bandwidth subsections where the increasing ℓ value implied a decrease in coincidences and the noise in the system to become more prominent.

The uncertainties in the fidelity followed from the QST runs where the topological charge was increased. The uncertainties were then propagated to Q and r.

The next step will be to do QKD for higher than two dimensions. The same rules apply: two mutually unbiased bases are required. The only difference is that now there are more basis states being used to encode information, which means the bit string does not have to be binary anymore. This increased alphabet

makes it possible to encode more information per photon. The transfer matrices (Figure 4.6) are similar to the two-dimensional case, only scaling according to the dimension.

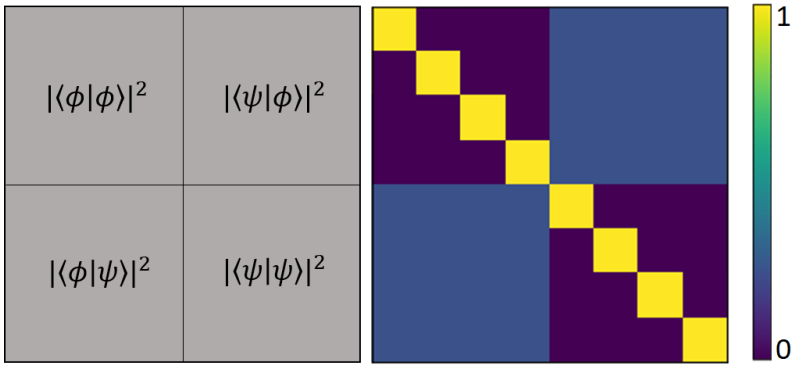

FIGURE 4.6: Simulated transfer matrix for the BB84 protocol for $d = 4$. All transfer matrices for the BB84 follow this general pattern. The main difference here is that the overlap between two mutually unbiased basis states are now 0.25 instead of 0.5.

Dimension	Q	F	F_{Eve}
2	0.014 ± 0.002	0.986 ± 0.002	0.617 ± 0.008
3	0.096 ± 0.006	0.904 ± 0.006	0.643 ± 0.010
4	0.160 ± 0.002	0.84 ± 0.002	0.647 ± 0.003

TABLE 4.4: First table showing the calculated measures discussed before for decreasing Q.

Dimension	R	$I_{\text{Eve,Alice}}$	$I_{\text{Alice,Bob}}$
2	0.787 ± 0.025	0.0500 ± 0.005	0.894 ± 0.012
3	0.481 ± 0.051	0.353 ± 0.017	1.033 ± 0.025
4	0.224 ± 0.016	0.617 ± 0.006	1.112 ± 0.010

TABLE 4.5: Second table showing the calculated measures discussed before for decreasing Q.

Tables 4.4 and 4.5 show that as the dimensions is increased, Q increased almost linearly. For $d = 4$, Q crosses the threshold of 11%, but this threshold was calculated for coherent attacks on QKD done with qubits, not four-dimensional qudits. Nevertheless, the quantum bit error rate does increase over dimension, implying that the channel become more and more susceptible to noise. If an eavesdropper were to attack the channel, these values would increase even more. The secret key rate that can be generated is supposed to increase by 0.5 bits per dimension. We

see that the experimental key rates deviate quite dramatically from what is theoretically possible. The higher the error rate, the more rapidly the secret key rate declines. Perhaps quantum error correction and privacy amplification can rectify this? As the dimensions increase both Alice and Bob; and Eve and Alice have greater shared information, but these two shared information values are restricted as before. Eve's cloning fidelity is kept relatively constant. This is because eavesdropping was never emulated and instead the eavesdropper in this case is just pure noise, systematic or otherwise.

The uncertainties in the above tables are directly from the QST runs for increasing dimension. The uncertainty was then propagated to the other measured values.

4.2 E91 Protocol

In the generic E91 protocol both Alice and Bob have two "measurement settings" or bases in which they can measure an entangled state. When Alice and Bob both choose setting ψ, then any measurement they take will give them perfect correlation determined by the SPDC state. The same happens for choice ϕ. These correlations are used for the secure key generation. If Alice and Bob were to choose any other combination of the two bases, ϕ and ψ, then they would be taking measurements that are used for the Bell inequality violation calculations from before.

The two basis choices are mutually unbiased bases as before, the main difference is that now instead of Alice sending Bob photons, they both receive an entangled photon pair to individually measure. The E91 security proof relies on the fact that the Bell parameter violates the CHSH-inequality to prove that entanglement is present and that the channel is secure [77]. Once again, systematic noise or an eavesdropper's influence will alter the state of photons before it reaches Bob, effecting the measurement outcome and ultimately effecting the Bell parameter calculation. This happens because measurements made by Eve, will destroy the entanglement in the system. If the Bell parameter does not violate the inequality, then the channel is considered insecure.

The quantum bit error rate (Q) is calculated in exactly the same way as with the BB84 protocol in that it is the probability of measuring the incorrect state when the correct basis was chosen during the key generation process. The key rate (r) is then calculated using the quantum bit error rate Q in the following [95], which is just the two-dimensional case of the previous key rate equation used for BB84 and is simply

$$r = 1 + 2(1 - Q)\log_2(1 - Q) + 2Q\log_2(Q). \tag{4.7}$$

It is possible to expand the E91 protocol to higher dimensions, using qudits of OAM for in principle any dimension d, but the main problem is that generalised Bell tests for dimensions larger than two are extremely difficult to implement [72]. Another limiting factor is the practicality of the optical setup.

It is possible to instead do higher-dimensional E91 QKD using many two-dimensional OAM subspaces. This combines two-dimensional E91 many times to achieve a larger alphabet, while simultaneously avoiding the more difficult Bell tests [88]. In this scenario the Bell parameters S_n must be calculated, where each parameter is calculated for the n^{th} OAM subspace. These subspaces are two-dimensional subspaces $\{\ell_n, -\ell_n\}$. The security of the channel then requires that each of the Bell parameters violate the Bell inequality. If even one of them do not meet this requirement, then it implies that the channel has been compromised, either by eavesdropping or systematical error. There is an upper bound to the secret key rate that can be generated using this approach and it is calculated using [88]

$$r \geq \sum_n 1 - h(Q_n) - h\left(\frac{1 + \sqrt{(S_n/2)^2 - 1}}{2}\right), \tag{4.8}$$

where the function h(X) is the binary entropy from Chapter 1. The reason the key rate is not allowed to go lower than a certain value is because of the restrictions placed on Q_n and S_n. Logarithmic functions are not defined for functional values equal to zero, hence $Q_n \neq 0$ and $Q_n \neq 1$. The same applies to the expression in the binary entropy in the third term. Here this leads to the strange restriction $S_n \neq 2\sqrt{2}$. This restriction implies that all of the OAM subspaces can never maxmimally violate the CHSH-inequality.

Chapter 5

Conclusion and Outlook

5.1 Conclusion

In this dissertation the spatial basis of light, namely the orbital angular momentum degree of freedom of light, and its use in quantum entanglement was investigated. All of the focus was placed on orbital angular momentum because, unlike the polarisation degree of freedom, it supplies a theoretically infinite basis. It was observed that despite this high-dimensional basis, that physical limitations are indeed imposed on what applications are actually possible. Nevertheless, the increased dimensionality of the orbital angular momentum basis allows for more information to be carried per quantum state; or per photon.

The entanglement itself was made possible because of the known process of spontaneous parametric down-conversion, where higher energy photons are converted into two lower energy photons called the signal and idler photons. This process depended on the phase matching conditions inside a PPKTP non-linear crystal.

The entanglement was quantified by measuring the overlap between modes in the two arms of the optical setup. This overlap was measured by performing projective measurements on the SPDC state by using liquid crystal spatial light modulators. What was measured was the amount of photon arrivals that arrived simultaneously at two spatially separated photon detectors, within some degree of accuracy. These measured values are called coincidence counts and are directly proportional to the degree of overlap or overlap probability between the two modes in the two arms of the setup.

Finally, quantum key distribution, specifically the BB84 and E91 protocols, were investigated as an application of the entanglement of orbital angular momentum of light. It was observed that the advantage of using a higher-dimensional basis

transfers itself unto this application as well, by showing that with an increased alphabet, it is more difficult for an eavesdropper to decypher any message sent without immediately alerting the other parties involved. It is also clear that as the dimension is increased, the entanglement becomes more robust to noise, in that noise applied to the system via an eavesdropper had less effect on the generated secret key rate with increasing dimension.

In Chapter 1 the basics of light and the solutions to the Helmholtz equation were discussed. These solutions are called modes of free space and signify the modes of light from which the OAM basis was selected. The modes considered were the LG, HG and BG modes, as well as the polarisation states that depend on the direction of oscillation of the electric field vector. Quantum information in its most fundamental level was discussed by investigating how common qubits can become multi-dimensional orbital angular momentum qudits. The Bloch sphere representation of these states was used, as is usual, to make visualising these states simpler, before the density matrix representation of entangled states was discussed. Multiple information measures were discussed, including the No-Cloning theorem, in preparation for the quantum state tomography and quantum key distribution sections that would eventually follow.

Chapter 2 explained the optical setup that was used to perform all experiments, as well as the physics behind all the important components. These components were specifically the detectors, SLMs, lenses and the non-linear crystal used. In this chapter the concept of coincidence counting was explored in more detail, by understanding what gating and integration time was. Coincidences and overlap probability were connected by way of SLM projective measurements.

Chapter 3 was the experimental results chapter of what has been discussed so far. Three main concepts were focused on here, namely the spiral bandwidth, quantum state tomography and Bell inequality violation tests. The spiral bandwidth can be considered as the amount of modes that are detectable within the supplied SPDC and is the amount of modes that are prominent enough to dominate the noise levels in the system. It was seen that physical limitations are what determined the shape of the spiral spectrum. Quantum state tomography, the method used to reconstruct the density matrix, was performed for increasing dimension, where as the dimension increased, it became more difficult to accurately determine the state and that the amount of measurements scaled extremely quickly. As entanglement witness the Bell parameter, and whether it violated the CHSH-inequality or not, was calculated for increasing topological charge, where the observation was that a loss of light would cause the entanglement to become undetectable.

Quantum key distribution was the focus of Chapter 4. Two protocols were studied: the BB84 and E91 protocols. The BB84 and E91 protocols use two mutually unbiased basis, regardless of dimension, and are used to securely encrypt information before it is sent between two communicating parties. Security analysis of these protocols was performed in order to determine if an eavesdropper, Eve, was able to intercept and decipher the secret key. It was seen that she could only achieve a limited reconstruction fidelity, before both the other parties would immediately be alerted to the attack.

5.2 Outlook

This dissertation could have gone into more detail regarding the specifics of the optical setup and the use of hybrid-entangled quantum states in similar applications, but at the risk of becoming too long, these considerations were only mentioned.

There are four main target areas that can be explored in more detail, all of which are related to quantum information. Quantum entanglement with hybrid entangled states for two- and many-dimensions and how they compare with the cases considered already. Quantum key distribution using the same hybrid entangled states as before in two- and many-dimensions. Expanding the study to more QKD protocols, especially ones that are considered to be practical or viable in real world applications. Investigating eavesdropping attacks in more detail and how QKD protocols must addapt depending on how these strategies are applied.

Combining the advantages of using different degrees of freedom in hybrid entangled states have become topical lately. Two- and multi-dimensional hybrid entanglement considering hybrid entangled states of two or more degrees of freedom would be the perfect launching point to expand on what was discussed in this dissertation. These degrees of freedom need not be the spatial properties of light.

The applications could be expanded more by considering hybrid entangled states in other quantum protocols and processes such as quantum imaging, quantum teleportation etc. Combining the advantages of multiple degrees of freedom in these well-known quantum applications could lead to both unexpected useful or completely trivial outcomes.

There exist more than just the BB84 and E91 quantum key distribution protocols. The field of quantum cryptography covers a wide range of such protocols where another of the most well-known protocols, the six-state protocol, is just one example. Spatial basis entangled states can be used in the application of other QKD protocols and one could even go as far as to apply it to completely different

quantum algorithms such as in quantum computation.

This dissertation tries to cover the basics of eavesdropping strategies. but in reality an eavesdropper can attack a channel whenever and wherever they like, depending on what they want to achieve. Depending on how the eavesdropper intends to attack the channel, the influence applied to the channel can vary dramatically. To understand all of the intrinsic affects of when and how attack strategies are applied to gain an edge over the already difficult to breach quantum probabilistic nature of quantum mechanics, is cardinal to the secure application of quantum cryptography going forward.

Bibliography

[1] Kjell J Gåsvik. *Optical metrology*. John Wiley & Sons, 2003.

[2] Hemani Kaushal, VK Jain, and Subrat Kar. *Free space optical communication*. Springer, 2017.

[3] Hennes Henniger and Otakar Wilfert. An introduction to free-space optical communications. *Radioengineering*, 19(2), 2010.

[4] Todd B Pittman, YH Shih, DV Strekalov, and Alexander V Sergienko. Optical imaging by means of two-photon quantum entanglement. *Physical Review A*, 52(5):R3429, 1995.

[5] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[6] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5 (1):3–28, 1992.

[7] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012.

[8] 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. *Physical Review Letters*, 70(13):1895, 1993.

[9] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical Review Letters*, 80(18):3891, 1998.

[10] Giovanni Guccione, Tom Darras, Hanna Le Jeannic, Varun B Verma, Sae Woo Nam, Adrien Cavaillès, and Julien Laurat. Connecting heterogeneous quantum networks by hybrid entanglement swapping. *Science Advances*, 6(22): eaba4508, 2020.

[11] XS Liu, GL Long, DM Tong, and Feng Li. General scheme for superdense coding between multiparties. *Physical Review A*, 65(2):022304, 2002.

[12] Sang Min Lee, Heonoh Kim, Myoungsik Cha, and Han Seb Moon. Polarization-entangled photon-pair source obtained via type-ii non-collinear SPDC process with PPKTP crystal. *Optics express*, 24(3):2941–2953, 2016.

[13] SP Walborn, AN De Oliveira, RS Thebaldi, and CH Monken. Entanglement and conservation of orbital angular momentum in spontaneous parametric down-conversion. *Physical Review A*, 69(2):023811, 2004.

[14] Ivan Marcikic, Hugues de Riedmatten, Wolfgang Tittel, Valerio Scarani, Hugo Zbinden, and Nicolas Gisin. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Physical Review A*, 66(6):062308, 2002.

[15] Alex OC Davis, Valérian Thiel, and Brian J Smith. Measuring the quantum state of a photon pair entangled in frequency and time. *Optica*, 7(10):1317–1322, 2020.

[16] Natalia Herrera Valencia, Vatshal Srivastav, Matej Pivoluska, Marcus Huber, Nicolai Friis, Will McCutcheon, and Mehul Malik. High-dimensional pixel entanglement: efficient generation and certification. *Quantum*, 4:376, 2020.

[17] Fu-Guo Deng, Bao-Cang Ren, and Xi-Han Li. Quantum hyperentanglement and its applications in quantum information processing. *Science Bulletin*, 62 (1):46–68, 2017.

[18] Hyunseok Jeong, Alessandro Zavatta, Minsu Kang, Seung-Woo Lee, Luca S Costanzo, Samuele Grandi, Timothy C Ralph, and Marco Bellini. Generation of hybrid entanglement of light. *Nature Photonics*, 8(7):564–569, 2014.

[19] Eleonora Nagali and Fabio Sciarrino. Generation of hybrid polarization-orbital angular momentum entangled states. *Optics Express*, 18(17):18243–18248, 2010.

[20] Ebrahim Karimi, Jonathan Leach, Sergei Slussarenko, Bruno Piccirillo, Lorenzo Marrucci, Lixiang Chen, Weilong She, Sonja Franke-Arnold, Miles J

Padgett, and Enrico Santamato. Spin-orbit hybrid entanglement of photons and quantum contextuality. *Physical review A*, 82(2):022115, 2010.

[21] SP Walborn, MO Terra Cunha, S Pádua, and CH Monken. Double-slit quantum eraser. *Physical Review A*, 65(3):033818, 2002.

[22] David J Griffiths. Introduction to electrodynamics, 2005.

[23] P. Piot. Helmholtz equation, 2008.

[24] Melvin Lax, William H Louisell, and William B McKnight. From maxwell to paraxial wave optics. *Physical Review A*, 11(4):1365, 1975.

[25] C Rosales-Guzmán and A Forbes. How to shape light with spatial light modulators,(2017).

[26] Christian Vetter, Ralf Steinkopf, Klaus Bergner, Marco Ornigotti, Stefan Nolte, Herbert Gross, and Alexander Szameit. Realization of free-space long-distance self-healing bessel beams. *Laser & Photonics Reviews*, 13(10): 1900103, 2019.

[27] Melanie McLaren, Thandeka Mhlanga, Miles J Padgett, Filippus S Roux, and Andrew Forbes. Self-healing of quantum entanglement after an obstruction. *Nature Communications*, 5(1):1–8, 2014.

[28] John Clarke and Frank K Wilhelm. Superconducting quantum bits. *Nature*, 453(7198):1031–1042, 2008.

[29] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[30] Pieter Kok and Brendon W Lovett. *Introduction to optical quantum information processing*. Cambridge University Press, 2010.

[31] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[32] Feng Zhu, Max Tyler, Natalia Herrera Valencia, Mehul Malik, and Jonathan Leach. Are high-dimensional entangled states robust to noise? *Preprint at https://arxiv. org/abs/1908.08943 v1*, 2019.

[33] Reinhard F Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277, 1989.

[34] Megan Agnew, Jonathan Leach, Melanie McLaren, F Stef Roux, and Robert W Boyd. Tomography of the quantum state of photons entangled in high dimensions. *Physical Review A*, 84(6):062101, 2011.

[35] Vlatko Vedral. *Introduction to quantum information science*. Oxford University Press on Demand, 2006.

[36] Stephen Brierley, Stefan Weigert, and Ingemar Bengtsson. All mutually unbiased bases in dimensions two to five. *arXiv preprint arXiv:0907.4097*, 2009.

[37] Ingemar Bengtsson. Three ways to look at mutually unbiased bases. In *AIP Conference Proceedings*, volume 889, pages 40–51. American Institute of Physics, 2007.

[38] Richard Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[39] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.

[40] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, 76(1):012307, 2007.

[41] Marco Fiorentino, Sean M Spillane, Raymond G Beausoleil, Tony D Roberts, Philip Battle, and Mark W Munro. Spontaneous parametric down-conversion in periodically poled KTP waveguides and bulk crystals. *Optics Express*, 15 (12):7479–7488, 2007.

[42] Suman Karan, Shaurya Aarav, Homanga Bharadhwaj, Lavanya Taneja, Arinjoy De, Girish Kulkarni, Nilakantha Meher, and Anand K Jha. Phase matching in β-barium borate crystals for spontaneous parametric down-conversion. *Journal of Optics*, 22(8):083501, 2020.

[43] Andrew Forbes, Angela Dudley, and Melanie McLaren. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics*, 8(2):200–227, 2016.

[44] Jonathan Pinnell, Isaac Nape, Bereneice Sephton, Mitchell A Cox, Valeria Rodríguez-Fajardo, and Andrew Forbes. Modal analysis of structured light with spatial light modulators: a practical tutorial. *JOSA A*, 37(11):C146–C160, 2020.

[45] Stirling Scholes, Ravin Kara, Jonathan Pinnell, Valeria Rodríguez-Fajardo, and Andrew Forbes. Structured light with digital micromirror devices: a guide to best practice. *Optical Engineering*, 59(4):041202, 2019.

[46] Bruno Piccirillo, Vincenzo D'Ambrosio, Sergei Slussarenko, Lorenzo Marrucci, and Enrico Santamato. Photon spin-to-orbital angular momentum conversion via an electrically tunable q-plate. *Applied Physics Letters*, 97 (24):241104, 2010.

[47] Peter Schemmel, Giampaolo Pisano, and Bruno Maffei. Modular spiral phase plate design for orbital angular momentum generation at millimetre wavelengths. *Optics Express*, 22(12):14712–14726, 2014.

[48] Filippo M Miatto, Alison M Yao, and Stephen M Barnett. Full characterization of the quantum spiral bandwidth of entangled biphotons. *Physical Review A*, 83(3):033816, 2011.

[49] Juan P Torres, Yana Deyanova, Lluis Torner, and Gabriel Molina-Terriza. Preparation of engineered two-photon entangled states for multidimensional quantum information. *Physical Review A*, 67(5):052313, 2003.

[50] Sonja Franke-Arnold, Stephen M Barnett, Miles J Padgett, and L Allen. Two-photon entanglement of orbital angular momentum states. *Physical Review A*, 65(3):033823, 2002.

[51] Irfan Ali Khan and John C Howell. Experimental demonstration of high two-photon time-energy entanglement. *Physical Review A*, 73(3):031801, 2006.

[52] TE Kiess, YH Shih, AV Sergienko, and CO Alley. Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by type-ii parametric down-conversion. *Physical Review Letters*, 71(24):3893, 1993.

[53] Alison M Yao. Angular momentum decomposition of entangled photons with an arbitrary pump. *New Journal of Physics*, 13(5):053048, 2011.

[54] Charles H Bennett, Herbert J Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046, 1996.

[55] David C Burnham and Donald L Weinberg. Observation of simultaneity in parametric production of optical photon pairs. *Physical Review Letters*, 25 (2):84, 1970.

[56] XY Zou, LJ Wang, and L Mandeļ. Violation of classical probability in parametric down-conversion. *Optics communications*, 84(5-6):351–354, 1991.

[57] Anthony Gerrard and James M Burch. *Introduction to matrix methods in optics*. Courier Corporation, 1994.

[58] David George Voelz. *Computational fourier optics: a MATLAB tutorial*. SPIE press Bellingham, WA, 2011.

[59] Uzi Efron. *Spatial light modulator technology: materials, devices, and applications*, volume 47. CRC Press, 1994.

[60] Yasunori Igasaki, Fanghong Li, Narihiro Yoshida, Haruyoshi Toyoda, Takashi Inoue, Naohisa Mukohzaka, Yuji Kobayashi, and Tsutomu Hara. High efficiency electrically-addressable phase-only spatial light modulator. *Optical Review*, 6(4):339–344, 1999.

[61] JL De Bougrenet De La Tocnaye and L Dupont. Complex amplitude modulation by use of liquid-crystal spatial light modulators. *Applied Optics*, 36(8): 1730–1741, 1997.

[62] Victor Arrizón, Ulises Ruiz, Rosibel Carrada, and Luis A González. Pixelated phase computer holograms for the accurate encoding of scalar complex fields. *JOSA A*, 24(11):3500–3507, 2007.

[63] JP Torres, A Alexandrescu, and Lluis Torner. Quantum spiral bandwidth of entangled two-photon states. *Physical Review A*, 68(5):050301, 2003.

[64] FM Miatto, D Giovannini, J Romero, S Franke-Arnold, SM Barnett, and MJ Padgett. Bounds and optimisation of orbital angular momentum bandwidths within parametric down-conversion systems. *The European Physical Journal D*, 66(7):1–6, 2012.

[65] Hiroki Takesue and Yuita Noguchi. Implementation of quantum state tomography for time-bin entangled photon pairs. *Optics Express*, 17(13):10976–10989, 2009.

[66] Isaac Nape, Valeria Rodríguez-Fajardo, Feng Zhu, Hsiao-Chih Huang, Jonathan Leach, and Andrew Forbes. Measuring dimensionality and purity of high-dimensional entangled states. *Nature Communications*, 12(1):1–8, 2021.

[67] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[68] John S Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38(3):447, 1966.

[69] Fabio A Bovino, Giuseppe Castagnoli, Adan Cabello, and Antia Lamas-Linares. Experimental noise-resistant Bell-inequality violations for polarization-entangled photons. *Physical Review A*, 73(6):062110, 2006.

[70] J Leach, B Jack, J Romero, M Ritsch-Marte, RW Boyd, AK Jha, SM Barnett, S Franke-Arnold, and MJ Padgett. Violation of a Bell inequality in two-dimensional orbital angular momentum state-spaces. *Optics Express*, 17(10): 8287–8293, 2009.

[71] Xiao-song Ma, Angie Qarry, Johannes Kofler, Thomas Jennewein, and Anton Zeilinger. Experimental violation of a Bell inequality with two different degrees of freedom of entangled particle pairs. *Physical Review A*, 79(4):042101, 2009.

[72] Adetunmise C Dada and Erika Andersson. On bell inequality violations with high-dimensional systems. *International Journal of Quantum Information*, 9 (07n08):1807–1823, 2011.

[73] Robert Thomas Thew, Antonio Acin, Hugo Zbinden, and Nicolas Gisin. Bell-type test of energy-time entangled qutrits. *Physical Review Letters*, 93(1): 010503, 2004.

[74] Ermes Toninelli, Bienvenu Ndagano, Adam Vallés, Bereneice Sephton, Isaac Nape, Antonio Ambrosio, Federico Capasso, Miles J Padgett, and Andrew Forbes. Concepts in quantum state tomography and classical implementation with intense light: a tutorial. *Advances in Optics and Photonics*, 11(1):67–134, 2019.

[75] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[76] Charles H Bennett and Gilles Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News*, 20(4):78–80, 1989.

[77] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661, 1991.

[78] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.

[79] Hitesh Singh, DL Gupta, and Ashish Kumar Singh. Quantum key distribution protocols: a review. *Journal of Computer Engineering*, 16(2):1–9, 2014.

[80] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[81] Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[82] Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, and Valerio Scarani. Towards practical and fast quantum cryptography. *arXiv preprint quant-ph/0411022*, 2004.

[83] K Inoue, E Waks, and Y Yamamoto. Differential-phase-shift quantum key distribution using coherent light. *Physical Review A*, 68(2):022317, 2003.

[84] T Ferreira Da Silva, D Vitoreti, GB Xavier, GC Do Amaral, GP Temporão, and JP Von Der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013.

[85] Eileen Otte, Isaac Nape, Carmelo Rosales-Guzmán, Cornelia Denz, Andrew Forbes, and Bienvenu Ndagano. High-dimensional cryptography with spatial modes of light: tutorial. *JOSA B*, 37(11):A309–A323, 2020.

[86] Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, and Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3):032305, 2013.

[87] Sandeep K Goyal, Filippus S Roux, Thomas Konrad, Andrew Forbes, et al. The effect of turbulence on entanglement-based free-space quantum key distribution with photonic orbital angular momentum. *Journal of Optics*, 18(6): 064002, 2016.

[88] Adetunmise C Dada. Multiplexing scheme for simplified entanglement-based large-alphabet quantum key distribution. *Physical Review A*, 91(5):052313, 2015.

[89] Jasper Rödiger, Nicolas Perlot, Oliver Benson, and Ronald Freund. Time-frequency quantum key distribution over a free-space optical link. *arXiv preprint arXiv:2112.04306*, 2021.

[90] Eleni Diamanti. *Security and implementation of differential phase shift quantum key distribution systems*. Stanford University, 2006.

[91] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000.

[92] Juan-Ignacio Cirac and Nicolas Gisin. Coherent eavesdropping strategies for the four state quantum cryptography protocol. *Physics Letters A*, 229(1):1–7, 1997.

[93] Eli Biham and Tal Mor. Security of quantum cryptography against collective attacks. *Physical Review Letters*, 78(11):2256, 1997.

[94] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002.

[95] Agnes Ferenczi and Norbert Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Physical Review A*, 85(5):052310, 2012.