Communicating with Transverse Modes of Light

by

Brandon Rodenburg

Submitted in Partial Fulfillment of the

Requirements for the Degree

Doctor of Philosophy

Supervised by Professor Robert W. Boyd

The Institute of Optics
Arts, Sciences and Engineering
Edmund A. Hajim School of Engineering and Applied Sciences

University of Rochester
Rochester, New York

2015

To my wonderful wife Liz:

Achievement unlocked!

Biographical Sketch

Brandon V. Rodenburg was born in Omaha, Nebraska in 1984. He attended Creighton University (Omaha, Nebraska) from which he graduated cum laude with both a bachelor of science in physics, and a bachelor of science major in mathematics in 2007. During his undergraduate program he performed research studying the dynamics of glass-forming liquids using photon correlation spectroscopy which led to publications in Physical Review Band The Journal of Chemical Physics, and for which he was awarded the Thomas Zepf Award for excellence in research, scholarship and service. In addition he won the 2006 – 2007 Alumni Award for best modern physics score on the Graduate Comprehensive Exam. He began his doctoral studies in optics at the University of Rochester in 2007, where he worked under the direction of Professor Robert W. Boyd.

List of Graduate Publications

[1] R. W. Boyd, A. Jha, M. Malik, C. O'Sullivan, B. Rodenburg, and D. J. Gauthier. Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon. Proceedings of SPIE**7948**, 79480L–6. doi:10.1117/12.873491 (2011).

[2] P. B. Dixon, G. Howland, K. Chan, C. O'Sullivan-Hale, B. Rodenburg, N. Hardy, J. H. Shapiro, D. S. Simon, A. V. Sergienko, R. W. Boyd, and J. Howell. Quantum ghost imaging through turbulence. Physical Review A**83**. doi: 10.1103/PhysRevA.83.051803 (2011).

[3] R. W. Boyd, B. Rodenburg, M. Mirhosseini, and S. M. Barnett. Influence of atmospheric turbulence on the propagation of quantum states of light using plane-wave encoding. Optics Express**19**, 18310. doi:10.1364/OE.19.018310 (2011).

[4] K. Chan, D. S. Simon, A. V. Sergienko, N. Hardy, J. H. Shapiro, P. B. Dixon, G. Howland, J. Howell, J. Eberly, M. N. O'Sullivan, B. Rodenburg, and R. W. Boyd. Theoretical analysis of quantum ghost imaging through turbulence. Physical Review A**84**. doi:10.1103/PhysRevA.84.043807 (2011).

[5] M. P. J. Lavery, D. Robertson, M. Malik, B. Robenburg, J. Courtial, R. W. Boyd, and M. J. Padgett. The efficient sorting of light's orbital angular momentum for optical communications. Proceedings of SPIE**8542**, 85421R. doi:10.1117/12.979934 (2012).

[6] M. Malik, M. N. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. J. Lavery, M. J. Padgett, and R. W. Boyd. Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding. Optics Express**20**, 13195. doi:10.1364/OE.20.013195 (2012).

[7] B. Rodenburg, M. P. J. Lavery, M. Malik, M. N. O'Sullivan, M. Mirhosseini, D. J. Robertson, M. J. Padgett, and R. W. Boyd. Influence of atmospheric

turbulence on states of light carrying orbital angular momentum. Optics Letters **37**, 3735. doi:10.1364/OL.37.003735 (2012).

[8] M. Mirhosseini, O. S. Magaña Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd. Rapid generation of light beams carrying orbital angular momentum. Optics Express **21**, 30196. doi:10.1364/OE.21.030196 (2013).

[9] M. Mirhosseini, B. Rodenburg, M. Malik, and R. W. Boyd. Free-space communication through turbulence: a comparison of plane-wave and orbital-angular-momentum encodings. Journal of Modern Optics **61**, 43–48. doi:10.1080/09500340.2013.834084 (2014).

[10] B. Rodenburg, M. Mirhosseini, M. Malik, O. S. Magaña Loaiza, M. Yanakas, L. Maher, N. K. Steinhoff, G. A. Tyler, and R. W. Boyd. Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication. New Journal of Physics **16**, 033020. doi:10.1088/1367-2630/16/3/033020 (2014).

[11] B. Rodenburg, M. Mirhosseini, O. S. Magaña Loaiza, and R. W. Boyd. Experimental generation of an optical field with arbitrary spatial coherence properties. Journal of the Optical Society of America B **31**, A51. doi:10.1364/JOSAB.31.000A51 (2014).

[12] O. S. Magaña Loaiza, M. Mirhosseini, B. Rodenburg, and R. W. Boyd. Amplification of Angular Rotations Using Weak Measurements. Physical Review Letters **112**, 200401. doi:10.1103/PhysRevLett.112.200401 (2014).

[13] M. Mirhosseini, O. S. Magaña Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, D. J. Gauthier, and R. W. Boyd. High-dimensional quantum cryptography with twisted light. arXiv:1402.7113 (2014).

Acknowledgments

English poet John Donne stated, "No man is an island." This is true in life, and the road leading to this thesis has been no exception to this maxim. I am indebted to Prof. Robert W. Boyd for giving me the opportunity to work with him during my time in graduate school. I have learned so much about how to do good research and what it means to be a scientist under his mentorship. I'd also like to thank Prof. James R. Fienup, Prof. John Howell, and Prof. Carlos Stroud, for agreeing to serve on my committee and for providing valuable insight and discussions that helped hone and improve the quality of this work.

I'd also like to thank the fellow members of Prof. Boyd's research group for creating such an excellent environment to work and grow, as well as for the many friendships that have developed from working together. I thank past members Dr. Aaron Schweinsberg, Dr. Petros Zerom, Dr. Heedeuk Shin, Prof. Zhimin Shi, Dr. Alex Radunsky, Dr. Mehul Malik, Prof. George Gehring, and Prof. Anand Jha. I especially want to thank Colin Malcolm O'Sullivan for taking me under his wing when I joined the group. Thank you for your wisdom from which I learned so much, and for your eternal patience with me

as I followed you around constantly questioning you and trying to help in the lab even when I lacked the experience to be of much use. And to Dr. Joe Vornehm, who had the misfortune to share an office with me and didn't have the heart to ever turn me away from the many hours of discussions that we had that distracted from his own work. To Dr. Andreas Liapis, one of the few people I've met whose love of film may be as great as my own, thanks for the many interesting discussions on science and culture. I also would like to thank the current members Mahmud Siddiqui, Boshen Gao, Robert Cross, and Mohammad Hashemi, and a special thanks to Mohammad Mirhosseini and Omar Magaña-Loaiza, with whom I've had the privilege of working for the last few years on numerous projects, we made one hell of a team.

Many of the projects I worked on were in close collaboration with others. I'd like to acknowledge Prof. Miles Padgett and his group, especially Dr. Martin Lavery, as well as Prof. Howell and his group, especially Dr. Ben Dixon and Dr. Gregory Howland. I'd also like to thank Dr. Glenn Tyler and Dr. Nicholas Steinhoff of the Optical Sciences Company. Thanks to Prof. Clifford Chan, Prof. Alexander V. Sergienko, Prof. Jeffrey H. Shapiro, Prof. Joeseph Eberly, and Prof. Stephen M. Barnett.

I'd also like to acknowledge all those here at the Institute of Optics that make this such a wonderful institution. Thanks to all the faculty who taught me so much, and to the many friends that I've made, and to the hard working staff who I've worked with including Gina Kern, Lissa Cotter, Lori Russel, Maria Schnitzler, Gayle Thompson,

Betsy Benedict, Per Adamson, Noelene Votens, Kari Brick, and everyone else who works to keep thinks running so smoothly.

I am grateful to my family, especially my parents, Ed and Lynda Rodenburg; my brother Matthew Rodenburg and his family; my Grandparents, Jean and Gene Rodenburg and Doris and Joe Breglia; and my aunt and uncle, Karen and John Priebe, who for years put up with my constant questioning of everything. Thanks for not only putting up with me, but encouraging and supporting me all these years. Thanks to my parents-in-law, David and Paula Sowl, my brother-in-law Sam Sowl, and sister-in-law Chelae Williams and her family for accepting me into your family and treating me as your own.

Lastly I thank my wife, Liz, to whom this thesis is dedicated. You are the love of my life, you give meaning to all that I do, you are my strength when life is hard and my joy when it is easy. This has been a long journey and we finally made it. Thank you.

Abstract

Shannon's theory of communication created a set of tools for studying complex systems in an abstract and powerful way, providing the core foundations for the field of information theory. This thesis uses these ideas to provide a framework for studying the transverse degree of freedom of an optical field, appropriate for both classical and quantum states of light. This degree of freedom is in principle an unbounded space, providing a complex resource for encoding a large amount of information. This work focuses on studying the physical limits to the information of this space, both in terms of fundamental theoretical limitations as well as practical limitations due to experimental implementation and error.

This thesis will pay particular interest to the design and implementation of a quantum key distribution system encoded using a particular set of transverse modes for encoding known as orbital angular momentum states, which represent normal modes of a typical free-space optical system. This specific technological implementation provides a motivation that acts to unify many of the themes in this work including quantum state preparation, state detection or discrimination, and state evolution

or propagation. Additionally, such a setup gives a specific physical meaning to the abstract tools we will be utilizing as the information that we will be quantifying can be thought of as a measure of the possible complexity or information content of a single photon.

Chapter 1 provides a brief introduction to information theory and the basic concepts and tools that are used throughout this work, as well as a basic introduction to quantum key distribution. Chapter 2 theoretically explores the fundamental limits of the information capacity of a channel due to diffraction, as well as computes the communication modes of a channel using a normal mode approach to propagation. Chapter 3 concerns the experimental implementation of a free-space quantum key distribution system including quantum state preparation and detection, as well as demonstration of a working system. Finally, in chapter 4 we consider the effects of a noisy channel on our analysis, especially decoherence due to the presence of atmospheric turbulence.

Contributors and Funding Sources

This work was supervised by a dissertation committee consisting of Professors Robert W. Boyd (advisor), James R. Fienup, and Carlos Stroud of the Institute of Optics (Edmund A. Hajim School of Engineering and Applied Sciences), as well as by Professor John Howell of the Department of Physics (School of Arts and Sciences). Prof. Boyd also holds an appointment at the University of Ottawa, Ottawa, Canada.

Chapter 1 contains no origional research and simply provides necessary background material used for this thesis. Chapter 2 consists of review information with the relevant citations containted within the text, as well as origional material and numerical analysis that I have done for the purpose of this thesis. Many of the general ideas discussed are known and properly cited, however their exact use and the results given within the context of the information theoretical framework developed in this thesis are new.

Chapter 3 consists of work done both in our group, as well as work done in collaboration with the group of Professor Miles Padgett from the University of Glasgow. Section 3.1 contains work that comes from two separate papers [1, 2]. Reference [1] describes a method of rapidly generating spatial modes of light and was a project that

was led by Mohammad Mirhosseini and involved the efforts of Omar S. Magaña-Loaiza, Changchen Chen, Mehul Malik, Prof. Boyd and myself. Reference [2] describes a procedure that I developed to generate any arbitrary spatially partially coherent beam and involved Mohammad Mirhosseini, Omar S. Magaña-Loaiza, and Prof. Boyd. Section 3.2 describes an optical orbital angular momentum mode sorting device developed by our collaborators in the Padgett group which was lent to us and used in a number of our experiments. Section 3.3 describes the implementation of a quantum key distribution system as described in [3]. This work was led by Mohammad Mirhosseini and involved the efforts of Omar S. Magaña-Loaiza, Malcolm N. O'Sullivan, Mehul Malik, Prof. Daniel J. Gauthier of Duke University, Robert W. Boyd, and myself.

Chapter 4 involved studying the effects of atmospheric turbulence on spatial modes within the context of communication and is based on five papers [4–8]. I was the main researcher in charge of this project which involved both theoretical and experimental studies. This effort involved Mohammad Mirhosseini and Mehul Malik who were involved in many of the projects and authored Ref. [7] and [6] respectively. In addition experimental support was also provied by Malcolm N. O'Sullivan, Jonathan Leach, Omar S. Magaña-Loaiza, Michael Yanakas, and Laura Maher from the the Boyd group, as well as Martin P. J. Lavery, David J. Robertson, and Prof. Padgett who were collaborators from the Padgett group in Glasgow. Professor Stephen M. Barnett from the University of Strathclyde was involved with the theoretical study in Ref. [4]. Finally, Nicholas K. Steinhoff and Glenn A. Tyler from the Optical Sciences Company

provided the design for the system and some of the numerical simulations for the work done in [8].

My graduate study was supported by Defense Advanced Research Projects Agency's information in a photon project (DARPA InPho).

Table of Contents

Biographical Sketch **iii**

List of Graduate Publications **iv**

Acknowledgments **vi**

Abstract **ix**

Contributors and Funding Sources **xi**

List of Tables **xvii**

List of Figures **xviii**

1 Introduction **1**

1.1 Shannon Information Theory 2

1.2 Quantum Cryptography 10

1.2.1 Communication with quantum states 11

1.2.2 Quantum key distribution 14

2 Theory of spatial mode communication 18

2.1 Diffraction limited communication 19

2.2 Communication modes 20

2.3 Channel capacity with communication mode encoding 22

2.4 Communication modes of a free-space channel 26

2.5 One dimensional apertures (square geometry) 28

2.5.1 Gaussian apodized apertures 30

2.5.2 Hard rectangular apertures 41

2.6 Cylindrical apertures 49

2.6.1 Gaussian apodized apertures 53

2.6.2 Hard circular apertures 58

2.7 Orbital angular momentum of light 65

2.7.1 Rotational eigenmodes 66

2.7.2 Angular momentum of an optical field 68

3 Implementing spatial mode communication 73

3.1 Spatial mode generation 74

3.1.1 Phase only spatial light modulation 78

3.1.2 Binary spatial light modulation 82

3.1.3 Rapid generation of spatial modes 86

3.1.4 Generation of modes with arbitrary spatial coherence 90

3.2 Spatial mode detection and discrimination 100

3.2.1 Projection measurements of spatial modes 101

3.2.2 Mode sorting of spatial modes 102

3.3 OAM QKD 107

4 Communication with a noisy channel **114**

4.1 Atmospheric turbulence 114

4.2 Thin-phase turbulence 118

4.2.1 OAM encoding with thin-phase turbulence 120

4.2.2 Plane-wave encoding with thin-phase turbulence 128

4.3 Thick turbulence 132

4.3.1 Simulating thick turbulence 133

4.3.2 OAM encoding with thick-phase turbulence 140

5 Conclusions and Future Work **145**

References **149**

List of Tables

1.1 Encoding in the BB84 scheme 15

1.2 Intercept-resend errors in the BB84 scheme 16

List of Figures

1.1 Schematic of Shannon's general communication system 3

1.2 Mutual Information 8

2.1 Communication with diffraction limited spots. 20

2.2 Hermite-Gaussian functions 33

2.3 Hermite-Gaussian 2D wavefunctions 35

2.4 Single photon channel capacity using Hermite-Gaussian communication modes 38

2.5 Configuration space for the Hermite-Gaussian communication modes 39

2.6 Classical channel capacity using Hermite-Gaussian communication modes 40

2.7 Transmission efficiencies of the prolate spheroidal communication modes 44

2.8 Abbe's model of diffraction 45

2.9 Channel capacity using prolate spheroidal communication modes . . . 47

2.10 Prolate spheroidal wavefunctions 48

2.11 Laguerre-Gaussian wavefunctions 57

2.12 Circular prolate spheroidal wavefunctions 62

2.13 Configuration space for the circular prolate spheroidal communication modes 63

2.14 Transmission efficiencies of the circular prolate spheroidal communication modes 64

2.15 Orbital angular momentum states 66

3.1 Detour phase of a shifted diffraction grating 76

3.2 Spatial mode generation setup 77

3.3 Phase only diffraction grating 79

3.4 Spatial light modulation using phase only holograms 82

3.5 Binary diffraction grating 83

3.6 Spatial light modulation using binary holograms 85

3.7 Setup for rapidly generating spatial modes 87

3.8 Images and interferograms of rapidly generated spatial modes 88

3.9 Setup for temporally resolving rapidly generated spatial modes 89

3.10 Time trace of the power in a set of rapidly switched spatial modes . . 89

3.11 Interference of coherent plane waves 94

3.12 Interference of plane waves with spatially varying coherence 98

3.13 Fringe visibility plot of partially coherent generated field 99

3.14 Setup for the projection measurement of spatial modes 101

3.15 Scaling inefficiency using traditional projection measurements 103

3.16 Ideal sorting of optical modes 104

3.17 Image of an optical log-polar transformation device used for mode sorting 105

3.18 Setup for a free-space, spatially encoded quantum key distribution system 108

3.19 Mutually unbiased bases of the spatial modes used for a spatially encoded QKD system 109

3.20 Measured conditional probabilities of detection in our QKD system . 111

3.21 Error-bounds for unconditional security 112

4.1 Thin phase turbulence model 120

4.2 Experimental setup for simulating a channel with thin-phase turbulence 123

4.3 Measurement of OAM spectrum by spatial binning 124

4.4 OAM scattering due to thin-phase turbulence 125

4.5 OAM input mode invariance of thin-phase turbulence 126

4.6 Decrease in channel capacity of an OAM channel due to turbulence . 127

4.7 Setup for simulating the effects of thin-phase turbulence on plane-wave encoding 130

4.8 Plane-wave mode scattering due to thin-phase turbulence 131

4.9 Decrease in channel capacity due to turbulence using plane-wave encoding 132

4.10 Procedure to find paramters of two phase screen that emulate thick turbulence 136

4.11 Comparison of Strehl ratio statistics of a thick turbulent path and its equivalent two-screen path 137

4.12 Fresnel propagation 139

4.13 Experimental setup for simulating a one kilometer channel with continuous turbulence 141

4.14 Crosstalk of OAM communication in a one kilometer channel due to turbulence 142

4.15 Decrease in channel capacity of a one kilometer OAM channel due to turbulence 144

Chapter 1

Introduction

As conscious living beings we all have our own subjective experiences that we live with. One of the amazing features of the human race is the ability to abstract these feelings and experiences and represent these thoughts and ideas. The appearance of language within our species has sharpened and extended this ability tremendously, as well as has given us the ability to transmit meaning to others. This ability to communicate with other people is one of the fundamental elements of what makes us human.

The tools we use to transmit information have grown and evolved through history enabling ever more complex communication. The creation of spoken language encoded ideas or meanings into distinct sounds. The invention of writing put the information into a form that gave the ideas a permanence that allowed ideas to spread further and be remembered longer. The modern era gave birth to electronic means of encoding and transmitting information that now allows the flow of ideas to occur virtually instantly and between nearly any two points on the earth.

This chapter will introduce the basics of information theory from the perspective of communication. These tools will provide the basic context for describing the transverse degree of freedom of light within the framework of communication or information. This provides a universal framework for thinking about such topics as spatial mode modulation, optical beam propagation, and measurement theory that will be explored in later chapters. In addition, section 1.2 will give a brief introduction to the field of quantum communication and cryptography which provides a specific technological implementation that integrates many of the topics that will be discussed throughout this thesis and thus provides a motivation for many of the ideas that will be presented.

1.1 Shannon Information Theory

The complexity of modern communication has given rise to a number of fields that try to model and thus better understand this phenomena. One of the major areas that has arisen in this context is the field of information theory. Information theory tries to analyze information qua information, and is seen as having been formally established in the seminal paper by Claude Shannon, "A mathematical theory of communication" [9]. Shannon gave a generalized picture of communication which is shown schematically in Fig. 1.1 and consists of three stages; a sender and receiver (traditionally named Alice and Bob), and a physical medium or channel over which the intended information is transmitted between Alice and Bob.

Figure 1.1: Schematic of Shannon's general communication system

Alice must encode the intended information onto some physical medium that can be transmitted to Bob. This stage is the fundamental stage of abstracting or symbolically representing meaning. Language is a natural example of this. In speech a specific idea is represented by a specific sound or grouping of sounds, while in written language the representation of the idea is in the form of visual characters or symbols. In general, ideas are represented in some physical form that can be transmitted and ultimately experienced or sensed by another person. Each physical symbol is chosen from a set of distinct possible symbols with pre-agreed upon meanings.

So in the general communication scheme of Fig. 1.1, Alice translates the intended message into a series of abstract symbols. Each symbol is encoded onto the state of the physical medium in one of a number of different possible configurations. The list of possible configurations or symbols $x \in X$ is called the alphabet, in analogy with written communication. The information $I(X)$ of a random symbol X with N equally likely possible values $x \in X$ is defined to be

$$I(X) = \log_b(N): \tag{1.1}$$

The logarithmic measure of information is chosen because the number of distinct possible messages generally grows exponentially with resources. For example if a message contains n independent random symbols X, each chosen from an alphabet of size N, then the total number of possible combinations of sequences is N^n, and the amount of information contained in this sequence is

$$I(X^n) = \log_b(N^n) = n \log_b(N) = nI(X): \tag{1.2}$$

It should be noted that information as defined by Eq. (1.1) is only defined to within a constant, which is equivalent to the freedom to choose the base b of the logarithm which defines the units of information. If the natural logarithm is chosen then information is given by nats, and if base two is chosen then the information is in bits.

Although Eq. (1.1) specifies the information for a message with equally likely outcomes, this is not always the case. A more general method of quantifying the information of an unknown process or message is to consider a set of possibilities $x \in X$ that are not equally likely. In this case each outcome will have an associated probability

$$p(x) \quad p(X = x); \tag{1.3}$$

that represents the relative likelihood that the event X will be represented by the particular possibility x. The more probable an event x is to occur, the less weight or information is conveyed when x occurs. For instance if $p(x) = 1$, then there is no

difference in knowledge before and after the event occurs and thus $I(x) = 0$. Whereas, if $p(x) \quad 0$, then if x occurs this is very surprising, i.e. a lot of information is gained and thus $I(x)$ should be large. The information gained from measuring $x \ 2 \ X$ is therefore given by

$$I(x) \quad I(X = x) = \log \left(\frac{1}{p(x)} \right) = \quad \log(p(x)): \tag{1.4}$$

The average information per event X is given by

$$H(X) = E[I(x)] = \sum_x p(x) I(x) = \sum_x p(x) \log(p(x)); \tag{1.5}$$

where E is the expected value operator. $H(X)$ is known as the Shannon information or entropy by analogy between Eq. (1.5) and the thermodynamic formula for entropy S given by

$$S = k_B H_B = k_B \sum_x p(x) \log(p(x)); \tag{1.6}$$

where k_B is Boltzman's constant, $p(x)$ represents probabilities of a system existing in microstate x, and H_B is the function used in Boltzman's H-theorem. Note that if all outcomes of an event X are equally likely, i.e. if the probabilities are given by

$$p(x) = 1 = N \quad 8x \ 2 \ X; \tag{1.7}$$

then the information is

$$I(x) = \log(1/N) = \log(N); \tag{1.8}$$

and we recover the expression given by Eq. (1.1).

The Shannon information given by Eq. (1.5) can describe equally well the amount of information that Alice can encode in a message as well as the amount of information that Bob learns upon receiving that message. If we say that the channel transmits from $A \to B$, i.e. Alice sends some symbol $A = a \in A$ and Bob measures some possible state $B = b \in B$, then the expectation value of the amount of information that Bob obtains upon measurement of his received symbol is given by $H(B)$, where the probabilities $p(x)$ in Eq. (1.5) are replaced by the probability of Bob detecting mode $b \in B$ given by $p(b)$. If the channel is ideal, than Bob receives the exact encoded message Alice transmitted and thus Bob has the same amount of information as was sent and $H(B) = H(A)$. However for a general channel there will be errors and some of the information necessary to describe Bob's detection will be caused by these errors. Assuming that Alice sent a, the amount of the information that Bob gains from his measurement $B = b$ that are due to these errors alone can be quantified by considering the entropy of B conditioned on $A = a$ given by

$$H(B|A = a) = \sum_b p(b|a) \log(p(b|a)). \tag{1.9}$$

The average or expected error is given by the conditional entropy $H(B|A)$ given by

$$H(B|A) = E[H(B|A = a)] = \sum_{a,b} p(a)p(b|a)\log(p(b|a)). \quad (1.10)$$

The average amount of information that Alice transmits to Bob in a noisy or imperfect channel is thus given by the mutual information which is simply the information Bob measures minus the information that is not due to Alice quantified by the conditional entropy, i.e.

$$I(A;B) \equiv H(B) - H(B|A). \quad (1.11)$$

The relationships between the Shannon entropies, the conditional entropy, and the mutual information is shown schematically in Fig. 1.2.

Generally one does not know the probabilities $p(b)$ a priori, as this depends both on the encoding scheme as well as the channel itself. Therefore it is often convenient to use the identity

$$p(b) = \sum_{a} p(b|a)p(a); \quad (1.12)$$

to make the dependence on $p(a)$ and $p(b|a)$ explicit. This way information due to the encoding and to the channel are separated as $p(a)$ is based on the encoding used and the conditional probabilities $p(b|a)$ are a property of the channel which can be

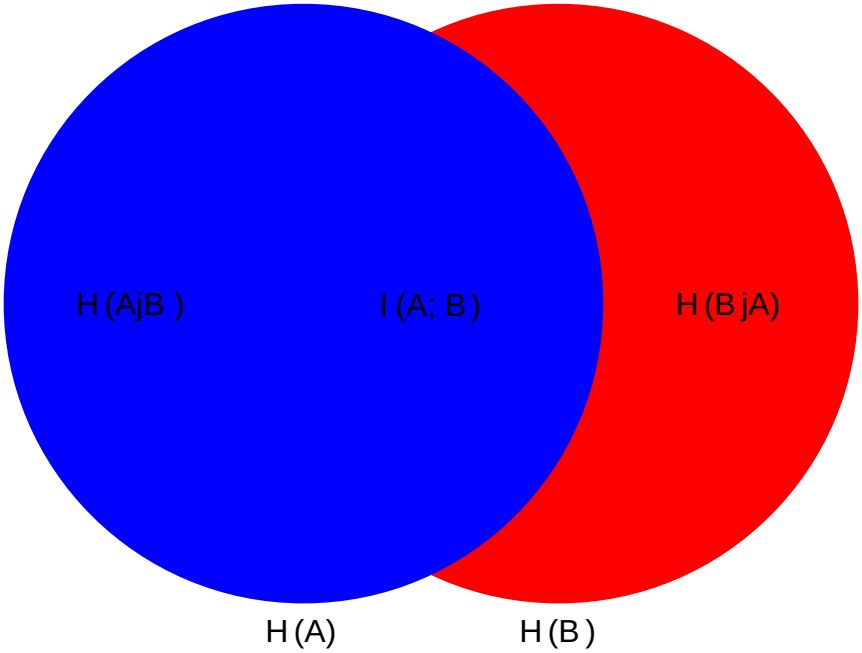

Figure 1.2: The marginal entropies representing the information that Alice encodes $H(A)$ and Bob measures $H(B)$ is represented by the blue and red circles respectively. The areas that do not overlap are the conditional entropies and the overlapping region represents the mutual information $I(A;B)$.

experimentally tested. Using this identity Eq. 1.11 can be written as

$$\begin{aligned} I(A;B) &= \sum_{b} p(b)\log(p(b)) + \sum_{a;b} p(bja)p(a)\log(p(bja)) \\ &= \sum_{a;b} p(bja)p(a)\log\Big(\sum_{a'} p(bja')p(a')\Big) + \sum_{a;b} p(bja)p(a)\log(p(bja)) \\ &= \sum_{a;b} p(bja)p(a)\log\left(\frac{p(bja)}{\sum_{a'} p(bja')p(a')}\right); \end{aligned} \tag{1.13}$$

where the last line is given in terms of quantities that are directly available to the experimenter.

The final stage of communication shown in Fig. 1.1 is decoding of the received message by Bob. However, a noisy channel (i.e. a channel with a non-zero value of $H(B|A)$) means that Bob's message will contain errors, and the average amount of information contained in the received message that correlates with the message Alice sent is $I(A;B)$. Alternatively, if Alice and Bob know in advance that the channel is imperfect, then Alice can encode redundant information in the sent message in a predetermined way which Bob can than use to correct for possible errors in his received message. In what is now known as Shannon's noisy-channel coding theorem [10], Shannon showed that in principle an intended message could be recovered using error correction with negligible probability of error. However, this is true only if the average amount of information that is extracted per symbol is less than the channel capacity C given by mutual information maximized over all input weightings $p(a)$, i.e.

$$C = \sup_{p(a)} I(A;B): \tag{1.14}$$

The maximum information rate transmitted into the channel is simply the symbol rate times $I(A;B)$. In order to maximize communication there are three primary methods available. The first method is to maximize the rate at which symbols are generated and sent. The second method is to maximize the information of each symbol, represented by either $H(A)$ or $H(B)$, which is done primarily by using the largest alphabet possible. Finally one wants to find a means of communication that minimizes

the errors of transmission $H(B|A)$, which may come from the channel or imperfect transmitters or receivers.

Much of this work focuses on communication with optical fields that exploit the large configuration space afforded by the transverse spatial degree of freedom of the field to maximize the symbol alphabet and the limitations of such a scheme.

1.2 Quantum Cryptography

Maximization of the information capacity of a channel is not the only parameter that is generally cared about in communication. If the channel is a public channel, or there is a fear of an eavesdropper listening in on the channel, then it may be desirable to find a way for Alice and Bob to communicate in a secure fashion. One standard method used is to encrypt the message with a cryptographic key. This is an algorithm that takes the message plus a random key to generate a new message that (ideally) contains only random information if one does not know how to decrypt the message (such as by knowing the key). Standard methods generally rely on computational complexity for encryption, but an exciting alternative is quantum cryptographic methods such as quantum key distribution (QKD), which relies on using quantum resources to securely distribute a random key for use in encrypting an intended message [11].

1.2.1 Communication with quantum states

Section 1.1 gave an introduction to some of the theoretical foundations of information and communication. Expanding this theory to include tools that require quantum resources leads to the fields of quantum communication and quantum information. One of the fundamental features of a quantum system that becomes one of the basic tools in quantum information is the phenomena of superposition. Consider a system that can be measured in one of two mutually exclusive states which we can write in the standard Dirac notation as $|0\rangle$ or $|1\rangle$. If this were simply a classical system then we would have each symbol or bit $x = 0$ or 1 encoded using the states $|0\rangle$ or $|1\rangle$. However as a quantum system the most general possible state $|\ \rangle$ of this system is represented as the (normalized) linear combination

$$|\ \rangle = a|0\rangle + b|1\rangle ; \tag{1.15}$$

where $a; b \in C$, and

$$|a|^2 + |b|^2 = 1: \tag{1.16}$$

The state in Eq. (1.15) is a general representation of what is called a quantum bit or qbit with the states $|0\rangle$ and $|1\rangle$ acting as a basis for this representation.

If Alice prepares a qbit in the state given by Eq. (1.15) and Bob checks to see if the state was in the $|0\rangle$ or $|1\rangle$ state, he will get a definite answer of one or the other

with probabilities given by

$$p(x = 0) = |a|^2; \text{ and } p(x = 1) = |b|^2: \tag{1.17}$$

Thus at most Bob only gets one bit of information per measurement. This type of measurement is known as projection measurement. In general a projection measurement is described by a Hermitian operator $\hat{M}$ which can be expanded in terms of it's spectral decomposition

$$\hat{M} = \sum_n {}_n\hat{P}_n = \sum_n {}_n|\,{}_n\rangle\langle\,{}_n|; \tag{1.18}$$

where $\hat{P}_n = |\,{}_n\rangle\langle\,{}_n|$ are projectors of the N orthogonal eigenstates $|\,{}_n\rangle$ spanning the N-dimensional space, and ${}_n$ are corresponding eigenvalues of $\hat{M}$. A projection style measurement of $\hat{M}$ will result in one of the N outcomes ${}_n$ with the probability of measuring the nth state given by

$$p_n = \langle\,|\hat{P}_n|\,\rangle = |\langle\,|\,{}_n\rangle|^2: \tag{1.19}$$

Therefore the case of Bob testing if the state is $|0\rangle$ or $|1\rangle$ corresponds to projectors

$$\hat{P}_0 = |0\rangle\langle 0| \text{ and } \hat{P}_1 = |1\rangle\langle 1|: \tag{1.20}$$

A special feature of measurements of quantum systems is the ability to choose a different measurement scheme $\hat{M}'$ for the same system with projectors over states $|\phi'_n\rangle$ that are superpositions of the eigenstates $|\phi_n\rangle$ of $\hat{M}$. $\hat{M}$ and $\hat{M}'$ are said to represent incompatible observables and will introduce uncertainty into Bob's measurement, i.e. the entropy of Bob's measurement conditioned on Alice's preparation will not be zero. For instance if Alice prepares the system in the state $|0\rangle$ and Bob measures the state using the projectors given by Eq. (1.20), he will decide the symbol was zero with 100% certainty. However if instead Bob makes a measurement by projecting over the states

$$|\phi\rangle = \frac{1}{2}\left(|0\rangle - |1\rangle\right) ; \tag{1.21}$$

he will find the state in either $|\phi_+\rangle$ or $|\phi_-\rangle$ each with 50% probability. Therefore, even in the absence of noise the conditional entropy is one bit and the mutual information between Alice and Bob is exactly zero. After the measurement either the particle itself will have been destroyed, such as when a photon is detected, or the quantum state will have been collapsed into the detected state and any subsequent measurement will yield the same result and so there is nothing more Bob can do to recover the lost information.

1.2.2 Quantum key distribution

One of the first papers on QKD was given by Bennett and Brassard in 1984 and is aptly known as the BB84 protocol [12]. In a BB84 scheme Alice sends a random key to Bob using at least two distinct sets of modes from incompatible observables $\hat{M}$ and $\hat{M}^0$ for encoding. For each symbol that is transmitted, Alice randomly chooses which alphabet or basis of states to choose her symbol from, and Bob randomly chooses which basis to measure in. An important constraint on these modes is the requirement that both sets of modes span the same Hilbert (sub)space and each basis of states must represent a mutually unbiased basis (MUB) with respect to any other basis used in the scheme. This means that if a state in one basis is measured by projecting in another, then the probability of detection is equal among all states and thus the mutual information between the prepared state and measured state is identically zero. This can alternately be written as

$$|\langle a_j | b_i \rangle|^2 = 1/N; \tag{1.22}$$

where $|a_i\rangle$ and $|b_i\rangle$ are any two states from different MUBs and N is the dimensionality of the Hilbert space. Security comes from the fact that any eavesdropper (conventionally referred to as Eve) who may have access to the transmitted state will be ignorant of which basis each state was prepared and as a result, will introduce errors into the

stream of symbols due to this ignorance and the inherent quantum uncertainty in measuring such general unknown states.

	H=V basis		D=A basis	
Symbol	0	1	0	1
State	$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|A\rangle$

Table 1.1: Encoding of binary symbols in the original BB84 scheme of Ref. [12] demonstrating the use of two incompatible polarization bases.

The original example in Ref. [12] used the polarization of photons to encode the key. Each symbol consisted of a single linearly polarized photon whose orientation determines whether the state is a binary zero or one. In the first basis the photon polarization is either horizontally or vertically oriented i.e.

$$|0\rangle_1 = |H\rangle \text{ and } |1\rangle_1 = |V\rangle : \tag{1.23}$$

A second basis was chosen such that the polarization is linear and orientated along the diagonal and anti-diagonal directions, which can be represented in terms of the original basis as

$$|0\rangle_2 = |D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \text{ and } |1\rangle_2 = |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{1.24}$$

respectively. Alice randomly sends in either the H=V or D=A basis and Bob chooses which basis to make a measurement in. After sending a sufficiently long message Alice

and Bob will sift the key by announcing which basis was used for each symbol and keep only the part of the message in which both choose the same basis.

Alice and Bob then announce part of their key to test for errors to check for the presence of Eve, as her presence will necessarily introduce errors. For instance if Eve measures and then resends in a randomly chosen basis, she will measure in the wrong basis half of the time and thus Bob, measuring in the correct basis, will get an incorrect bit half of these times. For instance if Alice prepares the symbol x = 0 in the H=V basis she will send state jH i. There is a 50% chance Eve will choose the correct H=V basis in which case she will measure and send the same state to Bob introducing no errors. However, if Eve choses to measure in the D=A basis then she will measure and resend either jD i or jAi to Bob. In both of these cases a measurement by Bob in the correct H=V measurement will be completely random with a measurement of jH i and jV i both occurring with a probability of 50%. A list of possible combinations is given in Table 1.2. If Eve is using an intercept-resend strategy she will induce an error rate of at least 25%. Therefore if Alice and Bob measure an error rate of less than 25%, then they can be certain there was no eavesdropper making such an attack.

Alice/Bob's Basis	Eve's Basis	Frequency	Error	Contribution to total error
H=V	H=V	1/4	0%	0%
H=V	D=A	1/4	50%	25%
D=A	H=V	1/4	50%	25%
D=A	D=A	1/4	0%	0%

Table 1.2: Introduction of errors into the sifted key in a BB84 QKD scheme due to an eavesdropper (Eve) intercepting and measuring each symbol in a random basis and then resending the measured symbol to Bob.

The error rate caused by Eve in an intercept-resend strategy can be generalized to using more than two MUBs and using a state space dimensionality greater than two. If the number of MUBs used is N, then Eve will choose the wrong basis with probability $(N-1)/N$. If the dimensionality of the Hilbert space is d, and Eve measures in the incorrect basis, Bob will get an error with probability $(d-1)/d$. Therefore the intercept-resend strategy will in general create an error with probability $(N-1)(d-1)/Nd$. Thus the security of the protocol can be improved by increasing the state space or the number or MUBs and it can be shown that this holds true even for more sophisticated eavesdropping strategies [13, 14]. Although security is improved by increasing either N or d, increasing the number of MUBs has the disadvantage of not only increasing the probability that Eve will choose the wrong basis, but also that Bob will choose incorrectly as well, thus decreasing the sifted key rate by a factor of N. For this reason our work focuses entirely on an increase in the number of symbols used for encoding, rather than on finding a large number of MUBs.

Chapter 2

Theory of spatial mode communication

As was demonstrated in chapter 1, using large alphabets or state spaces to encode information in a communication channel can allow for significant increases to channel communication rates as well as improvements in security in QKD. A particularly attractive physical resource that allows for many distinct states is the transverse or spatial degree of freedom of light, as the number of modes needed to describe an arbitrary field in a plane are unbounded. Optical means of communication are a natural and common means of communication, although exploiting spatial modes of light have only recently begun to be explored in this context. This interest includes both increasing transmission rates in classical channels [15] as well as for use in QKD systems [3, 14, 16, 17]

2.1 Diffraction limited communication

As previously seen, the benefit of using a resource for communication depends largely on the number of distinct possible states N for that resource. Although the spatial degree of freedom of an optical field appears unbounded, in practice N will always be limited. The primary physical mechanism limiting N will be diffraction and loss due to the sender and receiver having finite apertures. N can be estimated by imagining Alice communicates to Bob by focusing a beam to a spot in Bob's receiver as shown in Fig. 2.1. Two spots will be barely resolvable if they are separated by the Rayleigh criterion given by

$$x / \quad z = D_T ; \tag{2.1}$$

where is the wavelength, z is the separation between apertures and D_T is the transmitter diameter. The area of each spot therefore takes up roughly

$$(x)^2 / \ (z)^2 = A_T ; \tag{2.2}$$

where A_T is the area of the transmitting aperture.

The total number of spots distinguishable in the receiver aperture is therefore equal to the number of spots that fit within an area of the receiver A_R which gives

$$N \quad A_R = (x)^2 \quad \frac{A_R A_T}{(z)^2} = D_F ; \tag{2.3}$$

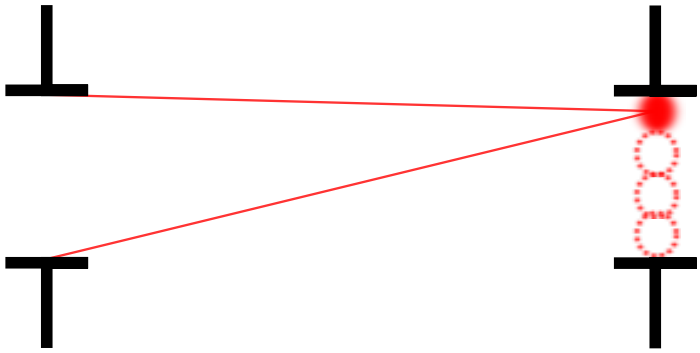

Figure 2.1: Communication scheme where various symbols are encoded by the location of distinct spots focused within the receiver's aperture. The number of distinct spots is given by the Fresnel number product D_F of the sender and receiver.

where D_F is known as the Fresnel number product of the sender and receiver. Therefore the amount of information that can be transmitted by a diffraction limited communication channel is expected to be approximately

$$I(A;B) \quad \log(D_F): \tag{2.4}$$

2.2 Communication modes

The more rigorous method of counting the number of available modes is to consider the Green's function operator $\hat{G}$ that maps functions in Alice's aperture A to Bob's aperture B, i.e.

$$\hat{G}: A ! B \quad : \tag{2.5}$$

The Green's function operator $\hat{G}$ includes loss from both apertures as well as the propagation in the channel, and is therefore generally not a unitary or information

preserving map. For all physically realistic situations $\hat{G}$ will be represented as a Hilbert-Schmidt operator, meaning an operator that is a linear operator with a norm of finite measure and therefore by Mercer's theorem [18] there will be a normal mode decomposition of $\hat{G}$. Thus we can write the propagator as

$$\hat{G} = \sum_n g_n |b_n\rangle\langle a_n| ; \tag{2.6}$$

where $|a_n\rangle \in A$ and $|b_n\rangle \in B$ are orthonormal sets of modes within their respective apertures. Equation (2.6) can be rewritten as the set of eigenequations

$$\hat{G}^\dagger \hat{G} |a_n\rangle = |g_n|^2 |a_n\rangle \qquad \hat{G}\hat{G}^\dagger |b_n\rangle = |g_n|^2 |b_n\rangle : \tag{2.7}$$

The modes in Eqs. (2.6) – (2.7) are known as the communication modes [19], and Eq. (2.6) can be interpreted as a one-to-one map of the set of modes $|a_n\rangle$ onto the set $|b_n\rangle$ with coupling constant g_n (i.e. power efficiency $\eta_n = |g_n|^2$). Such a decomposition discretizes the problem and allows us to apply the discrete tools developed in section 1.1 that allow us to quantify a physical process in terms of information theoretical concepts. In addition, the communication modes abstract the problem of propagation from all further analysis, allowing a full characterization of the problem in terms of a single special set of modes. Therefore a careful examination of the problem of diffraction using this perspective is both desirable and advantageous.

2.3 Channel capacity with communication mode encoding

Since Eqn. (2.6) specifies a one-to-one map of modes, this means we can write the conditional probability of Bob detecting mode $|b_n\rangle$ given that Alice sends mode $|a_n\rangle$ as

$$p(b_n|a_m) = \delta_{m,n}\, p_s(\eta_n); \tag{2.8}$$

where $p_s(\eta_n)$ is the probability that Bob measures a signal. For communication using single photons (such as in QKD) then η_n is the probability of Bob receiving a photon or not and thus for ideal detection

$$p_s^{QKD}(\eta_n) = \eta_n. \tag{2.9}$$

For classical communication communication, Bob will still receive a signal, even in the presence of loss. If the original signal was some power P_0, then Bob will receive a signal with power ηP_0. If the noise equivalent power (NEP) is significantly less than ηP_0, then Bob will register the correct symbol with very high probability. Therefore, a simple model for p_s is to treat it as a threshold or step function, i.e.

$$p_s^{classical}(\eta_n) = \begin{cases} 1 & \text{if } \eta_n > \eta_{min} \\ 0 & \text{otherwise} \end{cases}. \tag{2.10}$$

The value of $_{min}$ must be chosen high enough that errors are not introduced from noise, but low enough that the capacity of the channel isn't artificially restricted. The ideal value will depend on optimising these effects which depend on the exact nature of the noise of the system. This is a major area of study within the fields of signal processing and estimation theory, the details of which is beyond the scope of this thesis.

Using the conditional probability defined in Eq. (2.8), the marginal probability of Bob measuring mode $jb_n i$ therefore takes on the simple form

$$p(b_n) = \sum_m p(b_n|a_m)p(a_m) = \sum_m {}_{m;n}\, p_s(\ _n)p(a_m) = p_s(\ _n)p(a_n): \tag{2.11}$$

Using these two equations allows us to write the mutual information in a form that only depends on the values of $p(a_n)$ and $p_s(\ _n)$,

$$\begin{aligned} I(A;B) &= \sum_{m;n} p(a_m)p(b_n|a_m) \log \left[\frac{p(b_n|a_m)}{p(b_n)} \right] \\ &= \sum_{m;n} p(a_m)\ {}_{m;n}\, p_s(\ _n) \log \left[\frac{{}_{m;n}\, p_s(\ _n)}{p_s(\ _n)p(a_n)} \right] \\ &= \sum_n p(a_n)p_s(\ _n) \log \left[\frac{1}{p(a_n)} \right] \\ &= \sum_n p(a_n)p_s(\ _n) \log\ p(a_n)\ : \end{aligned} \tag{2.12}$$

An expression for the channel capacity can be found by finding the supremum of Eq. (2.12) subject to the constraint

$$\sum_n p(a_n) = 1 : \tag{2.13}$$

Using the method of Lagrange multipliers this requires extremizing the function

$$\begin{aligned} L &= I(A;B) + \left(\sum_n p(a_n) \right) - 1 \\ &= \sum_n p(a_n) p_s(\ _n) \log\ p(a_n) + \left(\sum_n p(a_n) \right) - 1 \ ; \end{aligned} \tag{2.14}$$

where is a constant chosen to satisfy the constraint in Eq. (2.13). The function L in Eq. (2.14) will be maximized at points of stationarity with respect to the probabilities $p(a_n)$, i.e.

$$\frac{@L}{@p(a_n)} = 0 = - p_s(\ _n) \log(p(a_n)) - p_s(\ _n) + \ : \tag{2.15}$$

Solving this equation for $p(a_n)$ gives

$$p(a_n) = \exp\left(\frac{}{p_s(\ _n)} - 1 \right) : \tag{2.16}$$

Since this equation yields non-negative values for $p(a_n)$, and the sum of probabilities is equal to one, we can see that Eq. (2.16) gives the correct range of values

$$0 \quad p(a_n) \quad 1 \quad 8n: \tag{2.17}$$

For the quantum case where we use the signal probability $p_s^{QKD}(\ _n) = \ _n$ from Eq. (2.9) the channel capacity is

$$C^{QKD} = \sum_n p^{QKD}(a_n)\ _n \log(p^{QKD}(a_n)) \tag{2.18}$$

with

$$p^{QKD}(a_n) = \exp\left[-\frac{1}{\ _n}\right]: \tag{2.19}$$

For the classical case we assume there are N total states with efficiencies greater than the threshold $\ _{min}$ given by Eq. (2.10), i.e.

$$p_s^{classical}(\ _n) = \begin{cases} 1 & \text{if } n \quad N \\ 0 & \text{otherwise} \end{cases}: \tag{2.20}$$

In this case

$$p^{classical}(a_n) = \begin{cases} \exp(\quad 1) & \text{if } n \quad N \\ 0 & \text{otherwise} \end{cases}; \tag{2.21}$$

which solving for the constraint specified in Eq. (2.13) gives

$$p^{classical}(a_n) = \begin{cases} 1=N & \text{if } n \quad N \\ 0 & \text{otherwise} \end{cases}: \tag{2.22}$$

Therefore by Eq. (2.12) the channel capacity of a classical channel is given as

$$C^{classical} = \sum_{n=1}^{N} \frac{1}{N} \log(N) = \log(\ N): \tag{2.23}$$

2.4 Communication modes of a free-space channel

An important metric that will be shown to correspond roughly to the total number of modes is the Hilbert-Schmidt inner product of $\hat{G}$ defined as

$$\left\|\hat{G}\right\|^2 \quad \mathrm{Tr}\left[\hat{G}^{\dagger}\hat{G}\right] = \sum_n |g_n|^2 = \sum_n \lambda_n^2. \tag{2.24}$$

Assuming propagation over a distance z within a free-space optical channel assumed to be within the paraxial regime, then the Green's function can be written as [20]

$$\left\langle r\left|\hat{G}\right|r'\right\rangle \quad G(r;r') = \frac{P_R(r)P_T(r')}{i\lambda z}\exp\left[ikz + ik\frac{|r-r'|^2}{2z}\right]; \tag{2.25}$$

where λ is the wavelength, $k = 2\pi/\lambda$ is the wavenumber, and $P_T(r)$ and $P_R(r)$ are the pupil transmission functions for Alice and Bob. For such a propagator

$$\left\|\hat{G}\right\|^2 = \int\int |G(r;r')|^2 dr'dr = A_R A_T/(\lambda z)^2 = D_F \tag{2.26}$$

where

$$A = \int |P(r)|^2 dr \tag{2.27}$$

is the area of the aperture. Therefore by combining the above expressions with Eq. (2.24), we see that the sum of the mode coupling efficiencies equals the Fresnel

number product D_F, i.e.

$$\sum_n |g_n|^2 = D_F. \tag{2.28}$$

In order to gain any more information about the communication modes or their coupling strengths g_n, we need to solve the eigenequations in Eq. (2.7). The spatial representation of these eigenequations is

$$\begin{aligned} \int\int \left\langle r_T \left| \hat{G}^\dagger \hat{G} \right| r_T' \right\rangle \psi_n(r_T')\, dr_T' &= \int\int K(r_T; r_T')\, \psi_n(r_T')\, dr_T' = |g_n|^2 \psi_n(r_T) \\ \int\int \left\langle r_R \left| \hat{G} \hat{G}^\dagger \right| r_R' \right\rangle \psi_n(r_T')\, dr_T' &= \int\int K'(r_R; r_R')\, \psi_n(r_R')\, dr_R' = |g_n|^2 \psi_n(r_R); \end{aligned} \tag{2.29}$$

where

$$\psi_n(r) \equiv \langle r | a_n \rangle \quad \text{and} \quad \phi_n(r) \equiv \langle r | b_n \rangle \tag{2.30}$$

are the spatial representations of the communication modes in Alice and Bob's apertures respectively. The integral kernels K and K' of Eq. (2.29) can be found using Eq. (2.25). This is given by

$$\begin{aligned} K(r_T; r_T') &= \left\langle r_T \left| \hat{G}^\dagger \hat{G} \right| r_T' \right\rangle \\ &= \int\int \left\langle r_T \left| \hat{G}^\dagger \right| r_R \right\rangle \left\langle r_R \left| \hat{G} \right| r_T' \right\rangle dr_R \\ &= \frac{P_T(r_T) P_T(r_T')}{(z)^2} \int\int |P_R(r_R)|^2 e^{i\frac{k}{2z}|r_T - r_R|^2} e^{-i\frac{k}{2z}|r_T' - r_R|^2} dr_R; \end{aligned} \tag{2.31}$$

and similarly

$$K'(r_R; r_R') = \frac{P_R(r_R) P_R(r_R')}{(z)^2} \int\int |P_T(r_T)|^2 e^{-i\frac{k}{2z}|r_R - r_T|^2} e^{i\frac{k}{2z}|r_R' - r_T|^2} dr_T. \tag{2.32}$$

Note that if the channel is symmetric, i.e. if

$$P_T(r) = P_R(r); \tag{2.33}$$

then $K' = K$ and thus the eigenequations in Eq. (2.29) are complex conjugates of each other. In this situation the eigenstates are simply related as

$$_n(r) = \quad _n(r): \tag{2.34}$$

The solutions to Eq. (2.29) depend on the form of the pupil functions P_T and P_R. Two typical cases are are given in sec. 2.5 – 2.6. Section 2.5 looks at the case of rectangular apertures, which gives solutions in separable Cartesian coordinates. Section 2.6 gives solutions for the more typical round apertures which leads to a natural decomposition in cylindrical coordinates.

2.5 One dimensional apertures (square geometry)

The first and simplest geometry we consider is one in which the pupil functions are separable in Cartesian coordinates, i.e.

$$P_R(x;y) = P_{R;x}(x) \quad P_{R;y}(y) \quad \text{and} \quad P_T(x;y) = P_{T;x}(x) \quad P_{T;y}(y): \tag{2.35}$$

In this case Eq. (2.31) can be written as

$$\begin{aligned} K(r_T; r_T^0) &= \frac{P_T(r_T)P_T(r_T^0)}{(z)^2} \iint P_R(r_R)^2 e^{i\frac{k}{2z}|r_T - r_R|^2} e^{-i\frac{k}{2z}|r_T^0 - r_R|^2} dr_R \\ &= \frac{P_{T;x}(x_T)P_{T;x}(x_T^0)}{z} \int P_{R;x}(x_R)^2 e^{i\frac{k}{2z}|x_T - x_R|^2} e^{-i\frac{k}{2z}|x_T^0 - x_R|^2} dx_R \\ &\quad \frac{P_{T;y}(y_T)P_{T;y}(y_T^0)}{z} \int P_{R;y}(y_R)^2 e^{i\frac{k}{2z}|y_T - y_R|^2} e^{-i\frac{k}{2z}|y_T^0 - y_R|^2} dy_R \\ &= K_{1D}(x_T; x_T^0) \quad K_{1D}(y_T; y_T^0): \end{aligned} \tag{2.36}$$

Therefore we can write the eigenequation for $(x; y)$ from Eq. (2.29) as

$$\begin{aligned} &\int K_{1D}(x_T; x_T^0) \, _{m;x}(x_T^0) \, dx_T^0 \int K_{1D}(y_T; y_T^0) \, _{n;y}(y_T^0) \, dy_T^0 \\ &\qquad = \, _{m;x} \, _{m;x}(x_T) \quad _{n;y} \, _{n;y}(y_T); \end{aligned} \tag{2.37}$$

where $_{m;n}(x; y) = \, _{m;x}(x) \quad _{n;y}(y)$ and $_n = \, _{m;x} \quad _{n;y}$. This means that for a square geometry we only need to solve the one dimensional eigenequations

$$\begin{aligned} \int K_{1D}(x; x^0) \, _{m;x}(x^0) \, dx^0 &= \, _{m;x} \, _{m;x}(x) \\ \int K_{1D}(y; y^0) \, _{n;y}(y^0) \, dy^0 &= \, _{n;y} \, _{n;y}(y): \end{aligned} \tag{2.38}$$

It is convenient to define the one dimensional version of the norm, $\hat{G}^2$, given in Eq. (2.26). This can be written as

$$\hat{G}_{1D}^2 = \iint G_{1D}(x; x^0)^2 \, dx \, dx^0 \int K_{1D}(x; x)^2 \, dx = \frac{L_R L_T}{z} = D_{F;1D}; \tag{2.39}$$

where $D_{F;1D}$ is the 1D Fresnel number product and

$$L = \int^{Z} P(x)^{2} dx \tag{2.40}$$

is the generalized pupil length, which acts as the 1D analog to the area defined in Eq. (2.27).

2.5.1 Gaussian apodized apertures

In order to solve for the eigenequations in Eq. (2.38), we need to know K_{1D} and thus have a specific form for the apertures. We first consider apertures that are Gaussian apodized as these results are known to have analytic solutions [21]. Such apertures will be specified by the (one dimensional) pupil functions

$$P_T(x) = \exp\left[\frac{x^2}{2\sigma_T^2}\right] \quad \text{and} \quad P_R(x) = \exp\left[\frac{x^2}{2\sigma_R^2}\right]; \tag{2.41}$$

which have characteristic lengths based on Eq. (2.40) of

$$L_{R=T} = \int^{Z} P_{R=T}(x)^{2} dx = \int^{Z} e^{x^2/\sigma_{R=T}^2} dx = \sigma_{R=T}\sqrt{\pi}. \tag{2.42}$$

This system has a (one dimensional) Fresnel number product of

$$D_F = \frac{L_R L_T}{z} = \frac{\sigma_R \sigma_T}{z} = \frac{k \sigma_R \sigma_T}{2z}. \tag{2.43}$$

Now we can compute the kernel K_{1D} by plugging the pupil expressions into Eq. (2.36). This gives

$$\begin{aligned} K_{1D}(x;x') &= \frac{P_{T;x}(x)P_{T;x}(x')}{z} \int P_{R;x}(x_R)^2 e^{i\frac{k}{2z}(x-x_R)^2} e^{j\frac{k}{2z}(x'-x_R)^2}\,dx_R \\ &= \frac{e^{(x^2+x'^2)/2\sigma_T^2}}{z} e^{j\frac{k}{2z}(x'^2-x^2)} \int e^{-x_R^2/\sigma_R^2} e^{j\frac{k}{z}(x-x')x_R}\,dx_R \\ &= \frac{e^{(x^2+x'^2)/2\sigma_T^2}}{z} e^{j\frac{k}{2z}(x'^2-x^2)} L_R e^{-k^2\sigma_R^2(x-x')^2/4z^2} \\ &= \frac{e^{(x^2+x'^2)/2\sigma_T^2}}{z} e^{j\frac{k}{2z}(x'^2-x^2)} L_R e^{-2D\frac{\sigma_R^2}{\sigma_F^2}(x-x')^2/2\sigma_T^2}. \end{aligned} \tag{2.44}$$

Our eigenequation now becomes

$$\begin{aligned} \lambda_m \psi_m(x) &= \int K(x;x')\psi_m(x')\,dx' \\ &= \frac{L_R}{z} \int e^{(x^2+x'^2)/2\sigma_T^2} e^{j\frac{k}{2z}(x'^2-x^2)} e^{-2D\frac{\sigma_R^2}{\sigma_F^2}(x-x')^2/2\sigma_T^2} \psi_m(x')\,dx'. \end{aligned} \tag{2.45}$$

If we make the substitution

$$\psi(x) = \psi_0(x)\exp\left(-j\frac{k}{2z}x^2\right); \tag{2.46}$$

then this becomes the real-valued eigenequation

$$\begin{aligned} \lambda_m \psi_m^0(x) &= e^{j\frac{k}{2z}x^2} \int K_{1D}(x;x')\psi_m(x')\,dx' \\ &= \frac{L_R}{z} \int e^{(x^2+x'^2)/2\sigma_T^2} e^{-2D\frac{\sigma_R^2}{\sigma_F^2}(x-x')^2/2\sigma_T^2} \psi_m^0(x')\,dx' \\ &= \frac{L_R}{z} \int e^{-(1+2D\frac{\sigma_R^2}{\sigma_F^2})(x^2+x'^2)/2\sigma_T^2} e^{4D\frac{\sigma_R^2}{\sigma_F^2}xx'/2\sigma_T^2} \psi_m^0(x')\,dx'. \end{aligned} \tag{2.47}$$

Using a substitution of variables we can write the exponential function as

$$\exp\left[\frac{(1+2D_F^2)(x^2+x'^2)+4D_F^2xx'}{2\sigma_T^2}\right] = \exp\left[\frac{(1+t^2)(y^2+z^2)+4tyz}{2(1-t^2)}\right] = \sqrt{\frac{1}{(1-t^2)}}\sum_n HG_n(y)HG_n(z)t^n; \tag{2.48}$$

where we have used Mehler's formula [22] to express the exponential function in terms of a bilinear expansion using the complete and orthogonal Hermite-Gaussian functions. These functions are given by

$$HG_n(z) = \sqrt{\frac{1}{2^n n!\sqrt{\pi}}}e^{z^2/2}H_n(z); \tag{2.49}$$

where $H_n(z)$ are the Hermite polynomials which can be written as

$$H_n(z) = (-1)^n e^{x^2}\frac{d^n}{dx^n}e^{-x^2}: \tag{2.50}$$

The first few Hermite-Gaussian functions are plotted in Fig. 2.2. The value of n corresponds to the degree of the Hermite polynomial $H_n(z)$ that makes up $HG_n(z)$. As a result of this the HG_n mode will have $n-1$ nodes and thus a larger mode number can be seen as corresponding to higher spatial frequencies of the mode. In addition the width (or variance) of the function itself will also grow with n as can be seen in the figure.

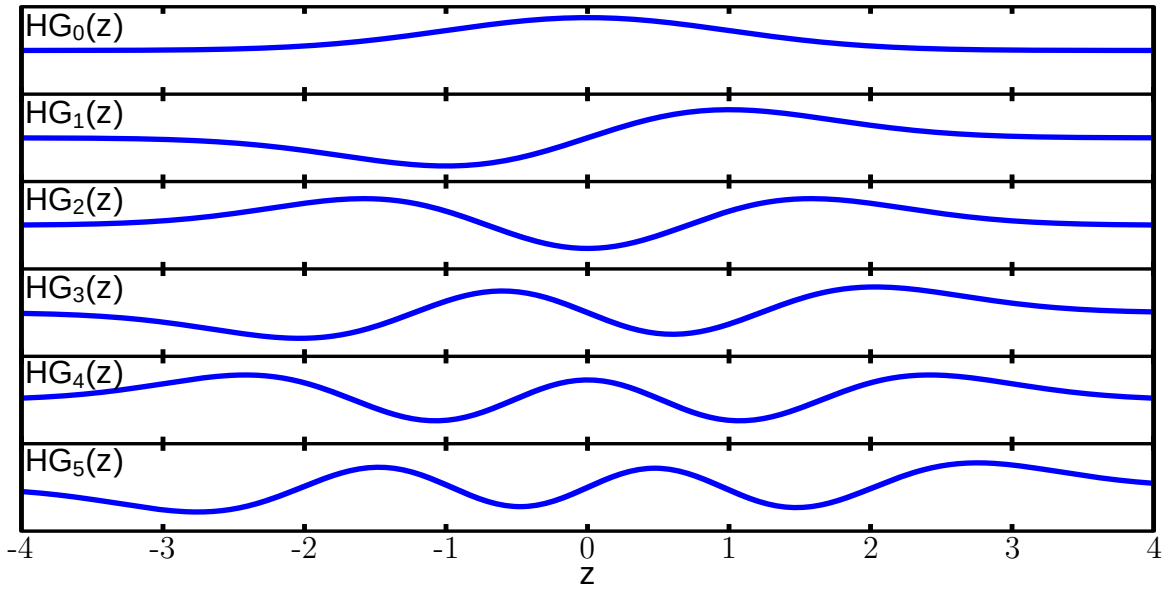

Figure 2.2: Plots of the six lowest order Hermite-Gaussian functions $HG_n(z)$ given by the expression in Eq. (2.49).

The substitution in Eq. (2.48) is true if we have

$$y = \sqrt{\frac{1-t^2}{1+t^2}}\sqrt{\frac{1+2D_F^2}{\tau}}x; \quad z = \sqrt{\frac{1-t^2}{1+t^2}}\sqrt{\frac{1+2D_F^2}{\tau}}x', \tag{2.51}$$
$$\text{and} \quad \frac{t}{1+t^2} = \frac{D_F^2}{1+2D_F^2}:$$

Solving for t gives

$$t = \frac{1+2D_F^2 \quad \sqrt{1+4D^2}}{2D_F^2} \tag{2.52}$$

and

$$y = \frac{(1+4D_F^2)^{1=4}}{\tau}x; \quad z = \frac{(1+4D_F^2)^{1=4}}{\tau}x'. \tag{2.53}$$

With this substitution our eigenequation becomes

$$\begin{aligned} {}_m\,{}^0_m(y) &= \frac{L_R}{z}\int e^{(1+2D_F^2)(x^2+x'^2)/2w_T^2} e^{4D_F^2 xx'/2w_T^2}\,{}^0_m(x')\,dx' \\ &= \sqrt{\frac{D_F}{1+2D_F^2}}\sqrt{1+t^2}\sum_n t^n\,HG_n(y)\int HG_n(z)\,{}^0_m(z)\,dz \\ &= \sqrt{t}\sum_n t^n\,HG_n(y)\int HG_n(z)\,{}^0_m(z)\,dz \\ &= \sqrt{t}\,t^m\,{}^0_m(y); \end{aligned} \tag{2.54}$$

where the integration is performed by assuming that ${}^0_m(z) \propto HG_m(z)$. We have therefore found the communication modes which are given by the normalized functions

$${}_m(x) = \sqrt{\frac{1}{(1+4D_F^2)^{1/4}w_T}}\,HG_m\!\left(\frac{x}{(1+4D_F^2)^{1/4}w_T}\right)e^{i\frac{k}{2z}x^2} \tag{2.55}$$

in Alice's aperture, and similarly by

$${}_m(x) = \sqrt{\frac{1}{(1+4D_F^2)^{1/4}w_R}}\,HG_m\!\left(\frac{x}{(1+4D_F^2)^{1/4}w_R}\right)e^{i\frac{k}{2z}x^2} \tag{2.56}$$

at Bob's aperture. These modes have a power coupling efficiency given by the eigenvalues

$${}_m = \sqrt{t}\,t^m = \left(\frac{\sqrt{1+2D_F^2}}{\sqrt{1+4D_F^2}}\right)^{\frac{1}{2}+m}: \tag{2.57}$$

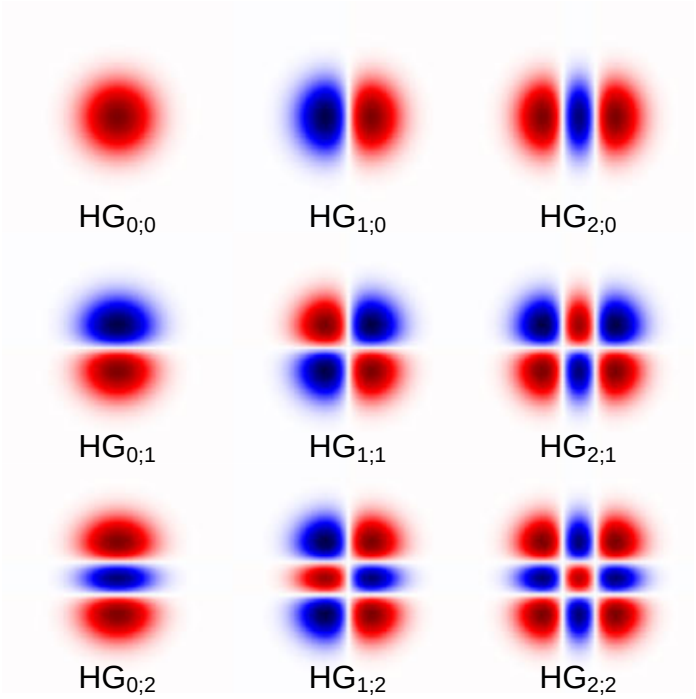

Figure 2.3: Plots of the nine lowest order 2D Hermite-Gaussian wavefunctions $HG_{m;n}(x;y)$ given by the expression in Eq. (2.61). The magnitude of the amplitude is represented by the color brightness, while phase (e.g. sign) is represented by the color hue with red representing a real and positive value and blue representing a real and negative value.

The full two dimensional solutions are just given as the product of the one dimensional solution, i.e.

$$ _{m;n}(x;y) = \quad _m(x) \quad _n(y); \quad _{m;n}(x;y) = \quad _m(x) \quad _n(y); $$
$$ \text{and} \quad _{m;n} = \quad _m \quad _n: \tag{2.58} $$

In particular, if $_{R;x} = _{R;y} = _{R}$ and $_{T;x} = _{T;y} = _{T}$ then the communication modes are given by

$$_{m;n}(x;y) = \frac{(1+4D^{2})^{1=4}}{_{T}} \exp\left[i\frac{k}{2z}\left(x^{2}+y^{2}\right)\right] \\ HG_{m;n}\left[\frac{(1+4D^{2})^{1=4}}{_{T}}x;\frac{(1+4D^{2})^{1=4}}{_{T}}y\right] \tag{2.59}$$

in Alice's aperture, and similarly by

$$_{m;n}(x;y) = \frac{(1+4D^{2})^{1=4}}{_{R}} \exp\left[i\frac{k}{2z}\left(x^{2}+y^{2}\right)\right] \\ HG_{m;n}\left[\frac{(1+4D^{2})^{1=4}}{_{R}}x;\frac{(1+4D^{2})^{1=4}}{_{R}}y\right] \tag{2.60}$$

at Bob's aperture, where we have defined the two dimensional Hermite-Gaussian functions

$$HG_{m;n}(x;y) \quad HG_{m}(x) \quad HG_{n}(y): \tag{2.61}$$

These modes have a power coupling efficiency given by the eigenvalues

$$_{m;n} = _{m} \quad _{n} = t^{1+m+n} = \left[\frac{\sqrt{1+2D_{F;2D}}}{\sqrt{1+4D_{F;2D}}}\right]^{1+m+n}; \tag{2.62}$$

where

$$D_{F;2D} = D_{F;x} \quad D_{F;y} = D_{F}^{2} \tag{2.63}$$

is the usual (two dimensional) Fresnel number product.

We can use the expression for the power efficiencies $_{m;n}$ given by Eq. (2.62) to compute the informational capacity of the channel. For communication using single photons the capacity as given by Eq. (2.18) is

$$\begin{aligned} C^{QKD} &= \sum_{m;n} p^{QKD}(a_n)\ _{m;n} \log(p^{QKD}(a_n)) \\ &= \sum_{m;n} \exp\left(\frac{}{m;n}\right)\left(1\ _{m;n} \log\left[\exp\left(\frac{}{m;n}\right)\left(1\right)\right]\right) \\ &= \sum_{m;n} \exp\left(\frac{}{t^{1+m+n}}\right)\left(1\ t^{1+m+n} \log\left[\exp\left(\frac{}{t^{1+m+n}}\right)\left(1\right)\right]\right); \end{aligned} \tag{2.64}$$

where is the Lagrange multiplier that must be chosen such that the probabilities are properly normalized.

There is no simple analytic formula for in Eq. (2.64), so one must resort to using numerical methods such as by minimizing the error function

$$\left(\ \right) \quad \left[1 \sum_{m;n} p_{m;n}(\ )\right]^2 = \left[1 \sum_{m;n} \exp\left(\frac{}{t^{1+m+n}}\right)\left(1\right)\right]^2 : \tag{2.65}$$

The results of numerically computing the channel capacity from Eq. (2.18) for a range of values for the Fresnel number product $N_{F;2D}$ are plotted in Fig. 2.4. As is shown in the figure the capacity can be expressed as

$$C^{QKD} \quad \frac{1}{2}\log(D_{F;2D}): \tag{2.66}$$

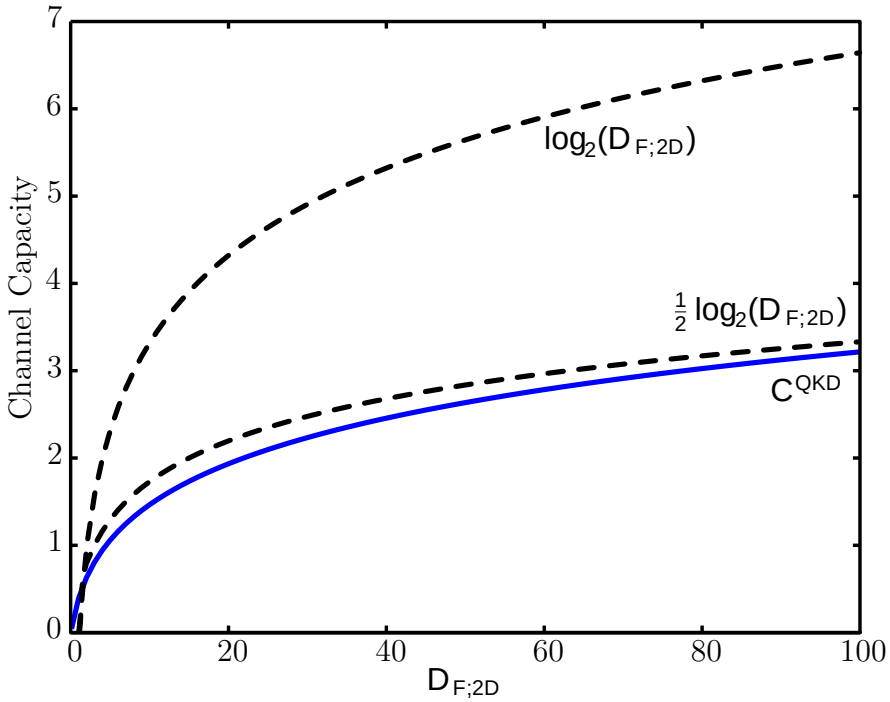

Figure 2.4: Plot of the single photon channel capacity for a free-space channel with apodized apertures encoded using the Hermite-Gaussian communication modes of the channel as given by Eq. (2.64). Also plotted (dashed lines) for comparison are the plots for $\log(D_{F;2D})$ and $\frac{1}{2}\log(D_{F;2D})$.

The classical channel capacity given by Eq. (2.23) is simply $\log N$, where N is the number of modes with efficiencies greater than $_{min}$. This means we are only considering modes $HG_{m;n}$ such that

$$_{m;n} = t^{1+m+n} > _{min}: \tag{2.67}$$

The maximum value of N_{max} such that $m + n < N_{max}$ is given by

$$_{min} = t^{1+N_{max}} \; ! \quad N_{max} = \frac{\log(_{min})}{\log(t)} \quad 1: \tag{2.68}$$

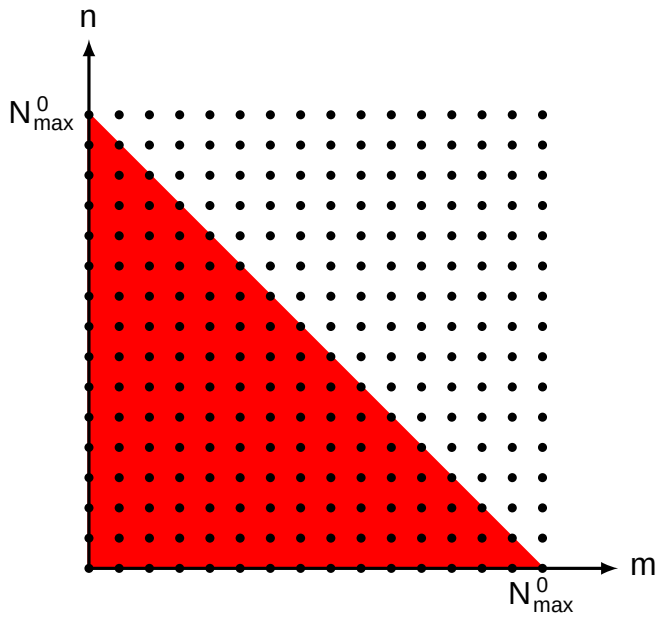

Figure 2.5: A configuration space diagram of Hermite-Gaussian communication modes $HG_{m;n}$. The red area indicates those states for which $m + n \quad N^0_{max}$.

The total number of modes N is given by counting all the modes $HG_{m;n}$ such that $m + n < N_{max}$ which is shown diagramatically as the modes in the red region in Fig. 2.5. This is equivalent to

$$\begin{aligned} N &= \sum_{m+n<N_{max}} 1 \\ &= \sum_{m=0}^{N^0_{max}} \left(\sum_{n=0}^{N^0_{max} - m} 1 \right) \\ &= \sum_{m=0}^{N^0_{max}} N^0_{max} \quad m + 1 \\ &= \frac{1}{2}(N^0_{max} + 2)(N^0_{max} + 1); \end{aligned} \tag{2.69}$$

where $N^{0}_{max} = \lfloor N_{max} \rfloor$ is the largest interger less than N_{max}. Therefore the channel capacity is

$$C^{classical} = \log\left[\frac{1}{2}(N^{0}_{max}+2)(N^{0}_{max}+1)\right] \log\left[\frac{1}{2}\frac{\log(\epsilon_{min})}{\log(t)}+1\right]^{\frac{\log(\epsilon_{min})}{\log(t)}}. \quad (2.70)$$

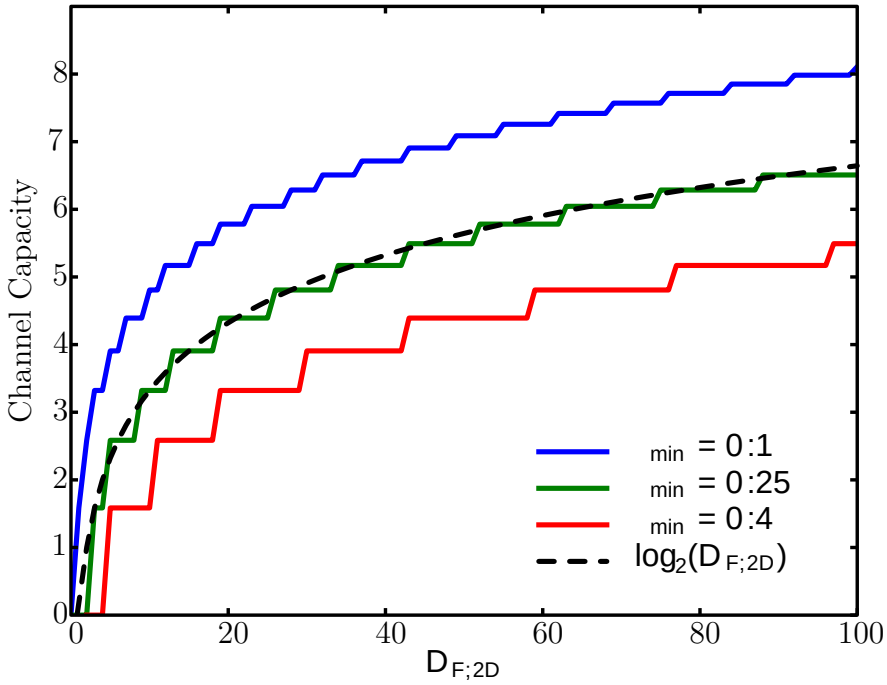

Figure 2.6: Plots of the classical channel capacity for a free-space channel with apodized apertures encoded using the Hermite-Gaussian communication modes of the channel for various threshold values ϵ_{min}. Also plotted (dashed lines) for comparison is the plot for $\log(D_{F;2D})$.

The classical channel capacity was computed and the results are plotted in Fig. 2.6. The capacity was plotted for a range of values for ϵ_{min} from 0.1 to 0.4. In addition a dashed curve representing $\log(D_{F;2D})$ is also shown. As can be seen a threshold value

of $_{min} = 0:25$ gives a capacity that is close to $\log(D_{F;2D})$, while smaller values of $_{min}$ give larger capacities and vice versa.

2.5.2 Hard rectangular apertures

Although the Gaussian apodized pupils given in Eq. (2.41) allowed us to analytically solve the one dimensional eigenequations of Eq. (2.38), a more realistic situation is to have hard apertures. For hard apertures with Cartesian or rectangular symmetry the (one dimensional) pupil functions are given by

$$P_T(x) = \text{rect}\left(\frac{x}{L_T}\right) \quad \text{and} \quad P_R(x) = \text{rect}\left(\frac{x}{L_R}\right); \tag{2.71}$$

where $\text{rect}(x)$ is the rectangle function defined as

$$\text{rect}(x) = \begin{cases} 1 & \text{for } |x| < \frac{1}{2} \\ 0 & \text{otherwise} \end{cases}: \tag{2.72}$$

We can see immediately that L_T and L_R are the characteristic lengths based on Eq. (2.40) as

$$\int P(x)^2\,dx = \int P(x)\,dx = \int \text{rect}\left(\frac{x}{L}\right) dx = L: \tag{2.73}$$

This system also has the simple (one dimensional) Fresnel number product as given in Eq. (2.39) of

$$D_F = \frac{L_R L_T}{z}: \tag{2.74}$$

Now again we must compute the kernel K_{1D} by plugging the pupil expressions into Eq. (2.36). Doing this gives

$$\begin{aligned} K_{1D}(x;x') &= \frac{P_T(x)P_T(x')}{z} \int P_R(x_R)^2 e^{i\frac{k}{2z}(x-x_R)^2} e^{-i\frac{k}{2z}(x'-x_R)^2}\,dx_R \\ &= \frac{\mathrm{rect}\left(\frac{x}{L_T}\right)\mathrm{rect}\left(\frac{x'}{L_T}\right)}{z} e^{-i\frac{k}{2z}(x'^2-x^2)} \int \mathrm{rect}\left(\frac{x_R}{L_R}\right) e^{-i\frac{k}{z}(x-x')x_R}\,dx_R \\ &= \frac{\mathrm{rect}\left(\frac{x}{L_T}\right)\mathrm{rect}\left(\frac{x'}{L_T}\right)}{z} e^{-i\frac{k}{2z}(x'^2-x^2)} L_R\,\mathrm{sinc}\left(\frac{L_R}{z}(x-x')\right) \\ &= \frac{\mathrm{rect}\left(\frac{x}{L_T}\right)\mathrm{rect}\left(\frac{x'}{L_T}\right)}{z} e^{-i\frac{k}{2z}(x'^2-x^2)} L_R\,\mathrm{sinc}\left(D_F\frac{x-x'}{L_T}\right); \end{aligned} \tag{2.75}$$

where the function $\mathrm{sinc}(x)$ is defined to be

$$\mathrm{sinc}(x) \quad \frac{\sin(\pi x)}{\pi x}. \tag{2.76}$$

As we did before, we make the substitution

$$\psi(x) = \phi(x)\exp\left(-i\frac{k}{2z}x^2\right); \tag{2.77}$$

which gives us the real-valued eigenequation

$$\begin{aligned} \lambda_m \phi_m(x) &= e^{-i\frac{k}{2z}x^2} \int K_{1D}(x;x')\,\psi_m(x') \\ &= \frac{D_F}{L_T}\mathrm{rect}\left(\frac{x}{L_T}\right) \int \mathrm{rect}\left(\frac{x'}{L_T}\right)\mathrm{sinc}\left(D_F\frac{x-x'}{L_T}\right)\phi_m(x')\,dx'. \end{aligned} \tag{2.78}$$

The solutions to Eq. (2.78) are known as the prolate spheroidal wavefunctions (PSWs) [23]. Writing Eq. (2.78) in standard form [24] gives

$$2R^2_{0;m}(c;1)S_{0;m}(c;t) = \int_{-1}^{1} \operatorname{sinc}\left[c(t-s)\right] S_{0;m}(c;s)\,ds; \tag{2.79}$$

which is equivalent to Eq. (2.78) with the substitutions

$$\begin{gathered} s = \frac{2x'}{L_T}; \quad t = \frac{2x}{L_T}; \quad c = \frac{D_F}{2}; \\ R^2_{0;m}(c;1) = \frac{\lambda_m}{D_F}; \quad \text{and} \quad \psi_m(t) = S_{0;m}(c;t): \end{gathered} \tag{2.80}$$

The functions $S_{m;n}(c;t)$ and $R_{m;n}(c;t)$ are known as the angular prolate spheroidal and radial prolate spheroidal functions respectively. These functions are solutions of the differential eigenequation [24]

$$(t^2-1)\frac{d^2u}{dt^2} + 2t\frac{du}{dt} + \left[c^2t^2 - \frac{m^2}{t^2-1}\right]u = -\lambda_{m;n}u; \tag{2.81}$$

where

$$u_{m;n}(c;t) = \begin{cases} S_{m;n}(c;t) & \text{for } |t| \le 1 \\ R_{m;n}(c;t) & \text{for } |t| \ge 1 \end{cases}. \tag{2.82}$$

Our eigenvalues, which are related to the radial prolate spheroidal functions, are given by

$$\lambda_m = D_F R^2_{0;m}(c;1) = D_F R^2_{0;m}\left[\frac{D_F}{2};1\right]: \tag{2.83}$$

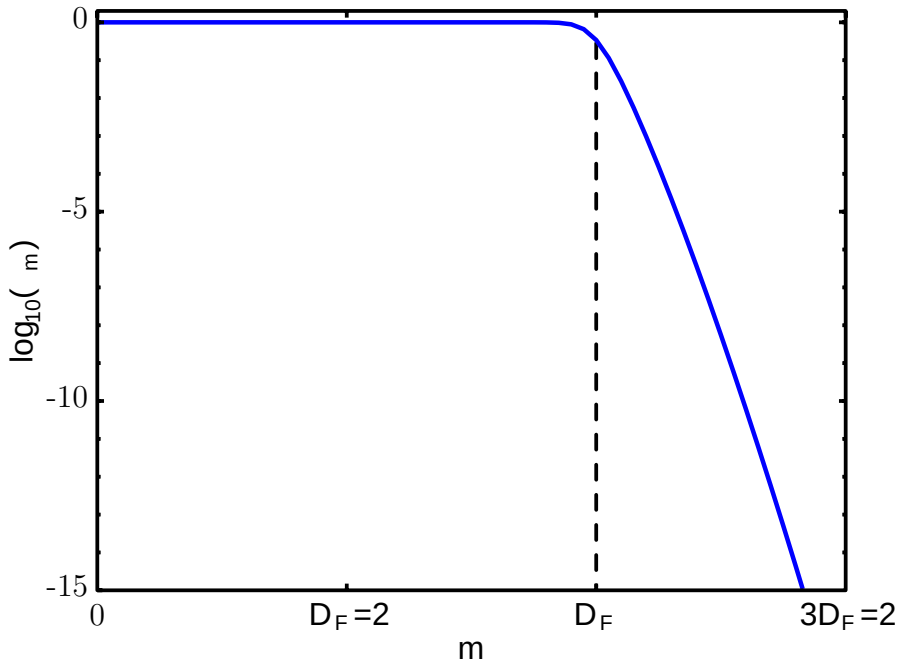

Figure 2.7: Plot of the transmission efficiencies $_m$ for a free-space channel with hard apertures encoded using the prolate spheroidal communication modes of the channel. The efficiencies display a sharp cutoff for $m > D_F$.

A plot of $_m$ is given in Fig. 2.7. Generally, $_m$ falls off very rapidly for m D_F. Therefore, for systems with $D_F > 1$, the eigenvalues are well approximated by the step functions

$$_m = \begin{cases} 1 & \text{for } m < D_F \\ 0 & \text{otherwise} \end{cases} : \tag{2.84}$$

For D_F 1 we only have approximately one mode which is transmitted with an efficiency

$$D_F : \tag{2.85}$$

It is a general feature of systems with hard apertures to have an abrupt cutoff in the transmission of spatial modes as one goes to larger spatial frequencies [25]. This can

be simply understood using Abbe's model of diffraction in which optical propagation between pupils is understood in terms of geometrical optical rays [20]. Each ray leaves the aperture at a different angle with larger angles being associated with larger spatial frequencies. The light that can be collected after the second pupil is simply the sum of all spatial frequencies that are within the solid angle of the pupil. Since the aperture has a hard edge, there is a hard cutoff in the angle of the rays that make it into the aperture. This is represented diagrammatically in Fig. 2.8.

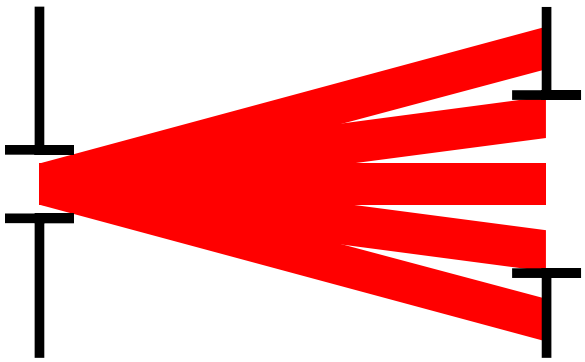

Figure 2.8: Schematic representing Abbe's model of diffraction in which a field at a pupil can be represented by a set of geometrical rays representing the different spatial frequency components of that field within the first aperture. The second aperture blocks the rays representing the high order spatial frequencies while leaving untouched the moderate and low order frequencies.

The sharp cutoff in the spectrum of $_m$, as well as the fact that $^P = D_F$, means that we essentially have D_F good modes to communicate with nearly lossless transmission. For a classical channel this gives a capacity of

$$C^{\text{classical}} = \log(D_F): \tag{2.86}$$

We expect this also to be the case for communication with single photons. Again we use the expression in Eq. (2.18) for communication using single photons given as

$$\begin{aligned} C^{QKD} &= \sum_m p^{QKD}(a_m)\ {}_m \log(p^{QKD}(a_m)) \\ &= \sum_m \exp\left(-\frac{1}{m}\right)\ {}_m \log\left[\exp\left(-\frac{1}{m}\right)\right]; \end{aligned} \tag{2.87}$$

and solve for the value of that properly normalizes the probabilities. The results are plotted in Fig. 2.9 along with $\log(D_F)$ (as the dashed line). As can clearly be seen, the two are nearly identical and thus to a very good approximation we can claim that

$$C^{QKD} = \log(D_F): \tag{2.88}$$

We have also uptained the eigenfunctions to Eq. (2.78) which are given by

$${}_m(x) = S_{o;m}\left(\frac{D_F}{2}; \frac{2x}{L_T}\right) \exp\left(i\frac{k}{2z}x^2\right) \tag{2.89}$$

at Alice. Repeating the procedure to find the modes at Bob gives us the kernel K^0_{1D} in the eigenequation for ${}_m$ that is identical to the complex conjugate of K_{1D} if we make the substitution

$$L_T \to L_R: \tag{2.90}$$

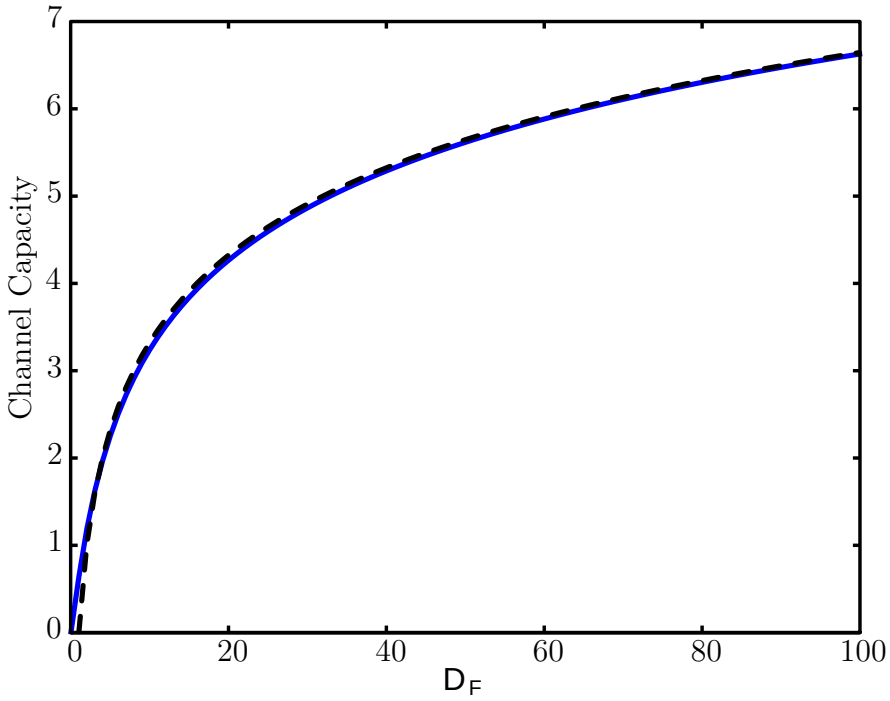

Figure 2.9: Plot of the single photon channel capacity for a free-space channel with hard apertures encoded using the prolate spheroidal communication modes of the channel (Eq. (2.87)). Also plotted (dashed lines) for comparison is the plot for $\log(D_F)$.

Therefore the communication modes at Bob are simply

$$_m(x) = S_{o;m}\left(\frac{D_F}{2}; \frac{2x}{L_R}\right) \exp\left(i\frac{k}{2z}x^2\right) : \tag{2.91}$$

The functions $S_{o;m}(D_F=2;2x=L)$ are real and continuous and have exactly m zeros within the aperture (i.e. for $x \in (-L/2; L/2)$) [24]. These eigenfunctions are very similar to the eigenmodes that were derived in section 2.5.1 (Eqs. (2.55) – (2.56)), and for mode numbers $m \ll D_F$, the two sets of modes are nearly indistinguishable [26]. Plots of the communication modes for a system with a (one dimensional) Fresnel number product of $D_F = 5$ are shown in Fig. 2.10 for the modes with non-negligible

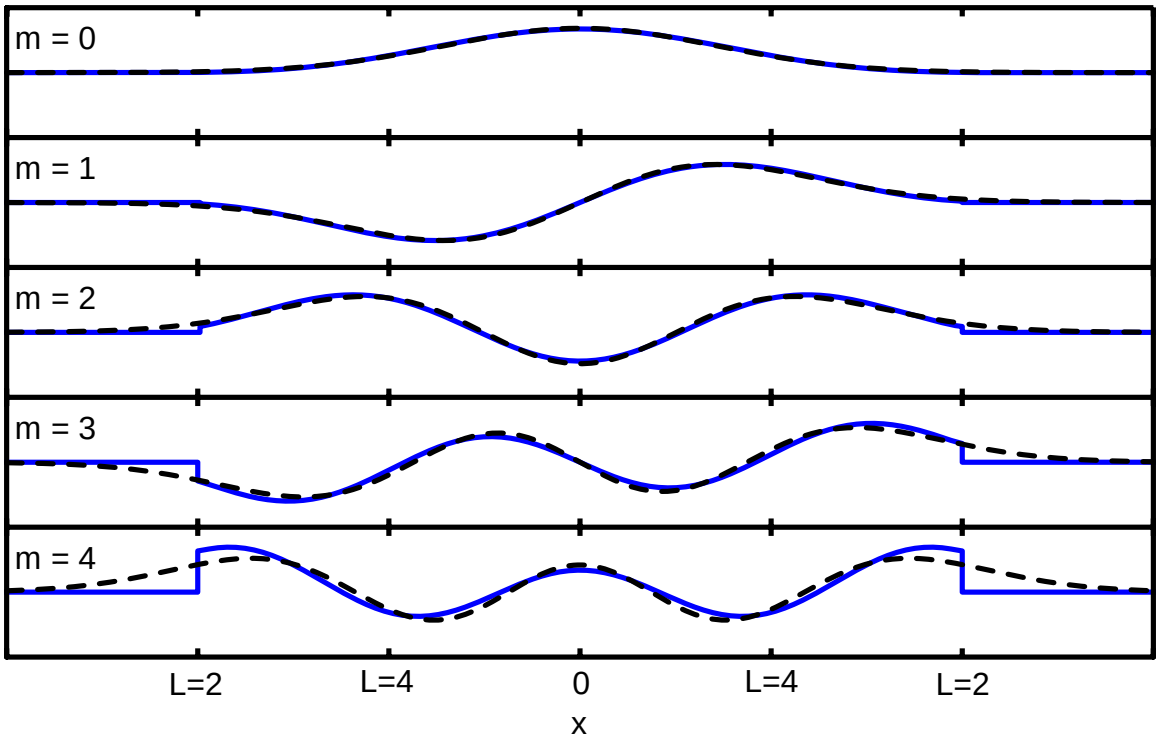

Figure 2.10: Plots of the prolate spheroidal wavefunctions that act as the communication modes for a system with hard apertures and a Fresnel number product of $D_F = 5$. In addition the Hermite-Gaussian communication modes of an analogous channel with Gaussian apodized apertures are plotted (dashed lines) in order to show the close similarities between the two sets of modes.

transmission efficiencies $_m$. In addition the Hermite-Gaussian modes for a system with identical Fresnel number product and aperture size $L = \sqrt{p}$ – are superimposed as the dashed line demonstrating the similarities between the two sets of modes.

2.6 Cylindrical apertures

The second type of geometry we consider is one in which the pupil functions are cylindrically symmetric, i.e.

$$P_T(\mathbf{r}) = P_T(r) \quad \text{and} \quad P_R(\mathbf{r}) = P_R(r); \tag{2.92}$$

where $r = |\mathbf{r}|$. The area of such pupils can be given by the one dimensional integral over r as

$$A = \iint |P(r)|^2 \, d\mathbf{r} = 2\pi \int |P(r)|^2 \, r \, dr. \tag{2.93}$$

Such a geometry represents round pupils which is a more typical case relative to the geometry discussed in section 2.5. Assuming such a geometry, Eq. (2.31) can be written as

$$\begin{aligned} K(r_T, r_T') &= \frac{P_T(r_T)P_T(r_T')}{(\lambda z)^2} \iint |P_R(r_R)|^2 e^{i\frac{k}{2z}|r_T - r_R|^2} e^{-i\frac{k}{2z}|r_T' - r_R|^2} \, dr_R \\ &= \frac{P_T(r_T)P_T(r_T')}{(\lambda z)^2} \exp\left[\frac{ik}{2z}\left(r_T'^2 - r_T^2\right)\right] \int_0^{2\pi} |P_R(r_R)|^2 \\ &\quad \exp\left[-i\frac{kr_R}{z}\left(r_T\cos(\theta_R - \theta_T) - r_T'\cos(\theta_R - \theta_T')\right)\right] dr_R. \end{aligned} \tag{2.94}$$

We can expand the exponential terms in the integral in terms of Bessel functions using the identity

$$e^{iz\cos(\theta)} = \sum_{n=-\infty}^{\infty} i^n e^{in\theta} J_n(z); \tag{2.95}$$

where the functions $J_n(z)$ are the Bessel functions which can be defined by the generating sequence [27]

$$e^{\frac{1}{2}(t\ 1=t)z} = \sum_{n=\ 1}^{1} t^n J_n(z): \tag{2.96}$$

Equation (2.95) is known as the Jacobi-Anger expansion and is derived by the substitution $t = i\exp(i\ )$ in Eq. (2.96). Therefore our kernel becomes

$$\begin{aligned} K(r_T; r_T^0) &= \frac{P_T(r_T)P_T(r_T^0)}{(\ z\ )^2} e^{\frac{ik}{2z}(r_T^{02} r\ _T^2)} (\ 1)^{\ n} i^{m+n} \int_0^Z P_R(r_R)^{\ 2} r_R\, dr_R \\ &\quad \sum_{m;n} e^{in\ _T^0} e^{im\ \ _T} J_m\left(\frac{kr_R r_T}{z}\right)^{!} J_n\left(\frac{kr_R r_T^0}{z}\right)^{!} \int_0^{2} e^{j(m\ n)\ \ _R} d\ _R \\ &= \frac{P_T(r_T)P_T(r_T^0)}{(\ z\ )^2} e^{\frac{ik}{2z}(r_T^{02} r\ _T^2)} \sum_m e^{im(\ _T^0\ \ _T)} \\ &\quad 2 \int_0^Z P_R(r_R)^{\ 2} J_m\left(\frac{kr_R r_T}{z}\right)^{!} J_m\left(\frac{kr_R r_T^0}{z}\right)^{!} r_R\, dr_R: \end{aligned} \tag{2.97}$$

Now if we make the substitution

$$\ _{`;p}(r;\ ) = \ _{`;p}(r) e^{i\ \frac{k}{2z} r^2} e^{j`\ }\ ; \tag{2.98}$$

where we have used the ansatz that all of the azimuthal dependence is due to $e^{i\ell}$, where ℓ is an integer, then our eigenequation (Eq. (2.29)) becomes

$$\begin{aligned}
\gamma_{\ell,p}\,\psi_{\ell,p}(r) &= \int\!\!\int e^{\frac{ik}{2z}(r'^2 - r^2)} e^{i\ell} e^{i\ell\theta'} K(r; r')\,\psi_{\ell,p}(r')\,dr' \\
&= \frac{P_T(r)P_T(r')}{(\lambda z)^2} \sum_m e^{i(\ell-m)\theta} e^{i(\ell-m)\theta'} d\theta' \int_0^\infty \psi_{\ell,p}(r')r'dr' \\
&\quad 2\pi \int_0^\infty P_R(r_R)^2 J_m\left(\frac{kr_R r}{z}\right) J_m\left(\frac{kr_R r'}{z}\right) r_R\,dr_R \\
&= \left(\frac{k}{z}\right)^2 P_T(r) \int_0^\infty P_R(r_R)^2 J_\ell\left(\frac{kr_R r}{z}\right) r_R\,dr_R \\
&\quad \int_0^\infty P_T(r')\,\psi_{\ell,p}(r') J_\ell\left(\frac{kr_R r'}{z}\right) r'dr'.
\end{aligned} \tag{2.99}$$

We can simplify Eq. (2.99) if we assume that the pupil functions P_T and P_R are simply scaled versions with the same functional form. Therefore, we assume we can write our pupil functions as

$$P_T(\rho L_T) = P_R(\rho L_R) = P(\rho); \tag{2.100}$$

where L_T and L_R are characteristic lengths for the transmitter and receiver pupils respectively, and ρ is a dimensionless radial coordinate. Now if we rewrite Eq. (2.99) with the coordinate change

$$\rho = r/L_T; \quad \rho' = r'/L_T; \quad \text{and} \quad \rho_R = r_R/L_R; \tag{2.101}$$

then we get

$$\lambda_{\ell,p}\,\psi_{\ell,p}(\theta) = c^2 P(\theta) \int_0^{\pi} P(\theta_R)\sin\theta_R J_\ell(c\cos\theta_R)\,\sin\theta_R\,d\theta_R \int_0^{\pi} P(\theta')\,\psi_{\ell,p}(\theta') J_\ell\left(c\cos\theta'\right)\sin\theta'\,d\theta', \tag{2.102}$$

where

$$c = kL_T L_R/z. \tag{2.103}$$

Eigenfunctions of the above equation are also eigenfunctions of the simpler equation

$$\lambda_{\ell,p}\,\psi_{\ell,p}(\theta) = P(\theta) \int_0^{\pi} P(\theta')\,\psi_{\ell,p}(\theta') J_\ell(c\cos\theta')\sin\theta'\,d\theta'. \tag{2.104}$$

This can be shown by applying the integral operator

$$\hat{O} = P(\theta) \int_0^{\pi} P(\theta') J_\ell(c\cos\theta')\sin\theta'\,d\theta' \tag{2.105}$$

to Eq. (2.104), i.e.

$$\begin{aligned}\lambda_{\ell,p}\hat{O}\,\psi_{\ell,p}(\theta) &= \lambda_{\ell,p}^2\,\psi_{\ell,p}(\theta) \\ &= P(\theta) \int_0^{\pi} P(\theta') J_\ell(c\cos\theta')\sin\theta'\,d\theta' \\ &\quad \int_0^{\pi} P(\theta')\,\psi_{\ell,p}(\theta') J_\ell\left(c\cos\theta'\right)\sin\theta'\,d\theta',\end{aligned} \tag{2.106}$$

which is identical to Eq. (2.102) with

$$\lambda_{;p} = \frac{p\,\overline{\lambda_{;p}}}{c}. \tag{2.107}$$

Therefore we only need to solve Eq. (2.104) to find the communication modes.

2.6.1 Gaussian apodized apertures

In order to go any further in solving Eq. (2.104), we need to specify the form of the apertures. As we did in section 2.5.1, we first consider Gaussian apodized apertures in order to obtain analytic solutions [21] to gain physical insight and intuition to the problem. Such apertures are specified by the radial pupil functions

$$P_T(r) = \exp\left[-\frac{r^2}{2\sigma_T^2}\right] \quad \text{and} \quad P_R(r) = \exp\left[-\frac{r^2}{2\sigma_R^2}\right]. \tag{2.108}$$

Such apertures have areas based on Eq. (2.93) of

$$A_{R=T} = 2\pi \int_0^\infty P_{R=T}(r)^2\, r\, dr = 2\pi \int_0^\infty \exp\left[-\frac{r^2}{\sigma_{R=T}^2}\right] r\, dr = \pi\sigma_{R=T}^2, \tag{2.109}$$

and therefore the Fresnel number product of this system is

$$D_F = \frac{A_R A_T}{(\lambda z)^2} = \left(\frac{\sigma_R \sigma_T}{\lambda z}\right)^2 = \left(\frac{k\,\sigma_R \sigma_T}{2\pi z}\right)^2. \tag{2.110}$$

The Gaussian widths $_T$ and $_R$ provide natural lengths for the transmitter and pupil receiver, and so we use

$$L_T = \ _T \quad \text{and} \quad L_R = \ _R \tag{2.111}$$

for our normalized coordinates as defined by Eq. (2.101). In this case our general pupil function is simply

$$P( ) = \exp(\quad ^2=2); \tag{2.112}$$

and Eq. (2.104) becomes

$$\begin{aligned} `;p \ `;p( ) = \ P( ) \quad & P(\ ^0) \ `;p( \ ^0)J`(c \ ^0) \ ^0d \ ^0 \\ = e \ ^{2=2} & \int e \ ^{02=2} \ `;p( \ ^0)J`(c \ ^0) \ ^0d \ ^0: \end{aligned} \tag{2.113}$$

In addition we have that the scaling parameter c is given by

$$c = \frac{k \ _T \ _R}{z} = 2^q \overline{D_F}: \tag{2.114}$$

Using a substitution of variables we can write

$$\begin{aligned} e \ ^{\frac{1}{2}(\ ^2+ \ ^{02})}J`(c \ ^0) = \ & e \ ^{\frac{1}{2}(x+y \ )(\frac{1 \ t}{1+t})}J` \ \frac{2^p \overline{xyt}}{1+t}! \\ = (1+ \ t)t^{j`j=2} & \sum_n \ t^n \ `_n(x) \ `_n(y); \end{aligned} \tag{2.115}$$

where we have used the Hill-Hardy theorem [28] to express the function in terms of a bilinear expansion using the complete and orthogonal Laguerre functions. These functions are given by

$$\grave{}_n(z) = \sqrt{\frac{n!}{(n+j\grave{}j)!}}\, e^{z=2} z^{j\grave{}j=2} L_n^{j\grave{}j}(z); \tag{2.116}$$

where $L_n^{j\grave{}j}(z)$ are the generalized Laguerre polynomials which can be written as

$$L_n^{j\grave{}j}(z) = \frac{e^z z^{j\grave{}j}}{n!} \frac{d^n}{dz^n} \left(e^z \, z^{n+j\grave{}j} \right) : \tag{2.117}$$

The substitution in Eq. (2.115) is true if we have

$$\begin{aligned} {}^2 &= \frac{1 \quad t}{1+t} x; \qquad {}^{02} = \frac{1 \quad t}{1+t} y; \\ \text{and} \quad \frac{2\sqrt{xyt}}{1+t} &= c \quad {}^0 = 2 \sqrt{D_F} \quad {}^0. \end{aligned} \tag{2.118}$$

Solving for t gives

$$t = \frac{1 + 2D_F \quad \sqrt{1+4D_F}}{2D_F} \tag{2.119}$$

and

$$x = \sqrt{1+4D_F} \quad {}^2; \quad y = \sqrt{1+4D_F} \quad {}^{02}. \tag{2.120}$$

With this substitution our eigenequation becomes

$$\begin{aligned}\lambda_{\ell p}\,\psi_{\ell p}(y) &= \int e^{\frac{1}{2}(x+y)\left(\frac{1-t}{1+t}\right)} J_\ell\!\left(\frac{2\sqrt{xyt}}{1+t}\right)\psi_{\ell p}(x)\,\frac{\sqrt{t}}{c(1+t)}\,dx \\ &= \frac{t^{(|\ell|+1)/2}}{c}\sum_n t^n\,\phi_n^{|\ell|}(y)\int \phi_n^{|\ell|}(x)\,\psi_{\ell p}(x)\,dx \\ &= \frac{t^{(2p+|\ell|+1)/2}}{c}\,\phi_p^{|\ell|}(y);\end{aligned} \tag{2.121}$$

where the integration is performed by assuming that $\psi_{\ell p}(x) \propto \phi_p^{|\ell|}(x)$. We have therefore found the communication modes which are given by the normalized functions

$$\begin{aligned}\psi_{\ell p}(r,\theta) &= \psi_{\ell p}(r,\theta)e^{-i\ell\theta}e^{i\frac{k}{2z}r^2} \\ &= \frac{(1+4D_F)^{1/4}}{\sqrt{\pi}}\,\phi_p^{|\ell|}\left(\frac{\sqrt{1+4D_F}}{T}r\right)^{|\ell|}\exp\left(-\frac{1+4D_F}{2T^2}r^2\right)e^{i\ell\theta}e^{i\frac{k}{2z}r^2} \\ &= \frac{(1+4D_F)^{1/4}}{\sqrt{\pi}}\,LG_p^{\ell}\left(\frac{(1+4D_F)^{1/4}}{T}r,\theta\right)e^{i\frac{k}{2z}r^2}\end{aligned} \tag{2.122}$$

at Alice, where LG_p^{ℓ} are the Laguerre-Gaussian functions defined as

$$LG_p^{\ell}(r,\theta) = \phi_p^{|\ell|}\left(r^2\right)e^{i\ell\theta}. \tag{2.123}$$

By symmetry we know that the communication modes at Bob's aperture are given by

$$\psi_{\ell p}(r,\theta) = \frac{(1+4D_F)^{1/4}}{\sqrt{\pi}R}\,LG_p^{\ell}\left(\frac{(1+4D_F)^{1/4}}{R}r,\theta\right)e^{-i\frac{k}{2z}r^2}; \tag{2.124}$$

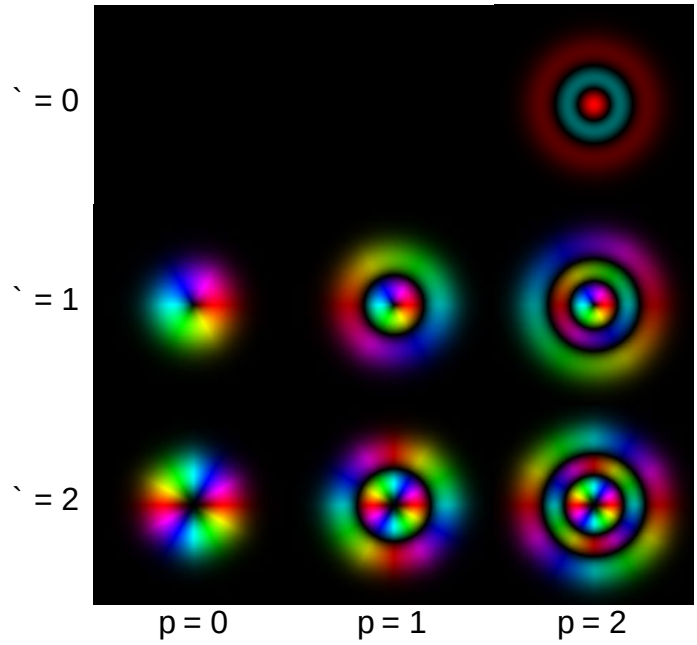

Figure 2.11: Plots of nine of the lowest order Laguerre-Gaussian wavefunctions $LG_p^{\ell}(\ ;\ )$ given by the expression in Eq. (2.123). The complex phase information is represented by the hue of the color in the plots, while the amplitude is represented by the color's brightness.

The LG_p^{ℓ} communication modes have a power coupling efficiency given by the eigenvalues

$$\ell;p = c^2\ {}^2_{\ell;p} = t^{2p+|\ell|+1} = \left(\frac{1+2D_F}{2D_F}\right)^0 \left(\frac{p}{1+4D_F}\right)^{1\ 2p+|\ell|+1} : \qquad (2.125)$$

This expression is identical to the expression found in section 2.5.1 for the efficiencies of the Hermite-Gaussian modes of a square Gaussian apodized aperture given in Eq. (2.62) if we replace $2p+|\ell|$ by $m+n$. This is not a coincidence, however as a

square Gaussian function also has cylindrical symmetry, i.e.

$$\exp\left[\frac{x^2}{2\sigma^2}\right]\exp\left[\frac{y^2}{2\sigma^2}\right] = \exp\left[\frac{x^2+y^2}{2\sigma^2}\right] = \exp\left[\frac{r^2}{2\sigma^2}\right]: \tag{2.126}$$

This additional symmetry is also the reason for the degenerate eigenvalues in either the HG or LG spectrum. In addition, the LG_p^{ℓ} modes can be expressed as a linear combination of $HG_{m;n}$ modes (and vice versa) within this degenerate subspace [29] spanned by

$$2p+|\ell| = m+n = \text{constant}; \tag{2.127}$$

i.e.

$$LG_p^{\ell}(r;\theta) = \sum_{m+n=2p+|\ell|} c_{m;n}\, HG_{m;n}(x;y): \tag{2.128}$$

Therefore we know that all the results concerning the channel capacity for a Gaussian apodized channel encoded with LG modes is identical to the results found in section 2.5.1.

2.6.2 Hard circular apertures

As was done in section 2.5, Gaussian apodized apertures allowed for the analytic computation of the communication modes but hard apertures provide a more realistic geometry. For the case of hard apertures, a communication system with cylindrical

symmetry means we have circular apertures with (radial) pupil functionals given by

$$P_T(r) = \mathrm{circ}\left(\frac{r}{R_T}\right) \quad \text{and} \quad P_R(r) = \mathrm{circ}\left(\frac{r}{R_R}\right); \tag{2.129}$$

where $\mathrm{circ}(\,)$ is the circle function defined as

$$\mathrm{circ}(\,) = \begin{cases} 1 & \text{for } \; < \; 1 \\ 0 & \text{otherwise} \end{cases}: \tag{2.130}$$

These pupils have the obvious areas of

$$A_{R=T} = \; R^{\,2}_{R=T}; \tag{2.131}$$

and therefore such a channel has a Fresnel number product of

$$D_F = \frac{A_R A_T}{(\,z\,)^2} = \left(\frac{R_{\,R} R_T}{z}\right)^2 = \left(\frac{k R_R R_T}{2z}\right)^2: \tag{2.132}$$

The circular widths R_T and R_R provide natural lengths for the transmitter and pupil receiver, and so we use

$$L_T = R_T \quad \text{and} \quad L_R = R_R \tag{2.133}$$

for our normalized coordinates as defined by Eq. (2.101). In this case our general pupil function is simply

$$P(\rho) = \mathrm{circ}(\rho) \tag{2.134}$$

and Eq. (2.104) becomes

$$\begin{aligned} \int_{\ell,p} \Psi_{\ell,p}(\rho) &= P(\rho) \int_0^\infty P(\rho') \Psi_{\ell,p}(\rho') J_\ell(c\rho\rho') \rho' d\rho' \\ &= \mathrm{circ}(\rho) \int_0^1 \Psi_{\ell,p}(\rho') J_\ell(c\rho\rho') \rho' d\rho', \end{aligned} \tag{2.135}$$

where our scaling parameter c is given by

$$c = \frac{kR_T R_R}{z} = 2\pi \sqrt{D_F}. \tag{2.136}$$

The solutions to Eq. (2.135) are known as the circular prolate spheroidal wavefunctions (CPSW), and are the cylindrical analog of the PSWs found in section 2.5.2 [26]. Writing Eq. (2.135) in standard form [30] gives

$$\int_{\ell,p} \Psi'_{\ell,p}(\rho) = \int_0^1 \sqrt{c\rho'}\, \Psi_{\ell,p}(\rho') J_\ell(c\rho\rho') d\rho', \tag{2.137}$$

which is equivalent to Eq. 2.135 with the substitutions

$$\Psi'_{\ell,p}(\rho) = \Psi_{\ell,p}(\rho) \sqrt{\rho}, \quad \text{and} \quad \int_{\ell,p} = \sqrt{c}\, \Psi_{\ell,p} = \sqrt{\frac{\chi_{\ell,p}}{c}}. \tag{2.138}$$

The functions $'_{`;p}(\ ;\ )$ are known as the generalized prolate spheroidal functions and are also solutions of the differential eigenequation

$$(\ ^2\ \ 1)\frac{d^2'}{d\ ^2} + 2\ \ \frac{d'}{d} + \ \ c^2\ ^2\ \ \frac{1=4\ \ `^2}{^2}\ '\ =\ '; \tag{2.139}$$

which is identical to the differential equation for the prolate spheroidal functions given in Eq. (2.81) except for the $(1=4\ \ `^2)=\ ^2$ term. Finding numerical expressions for $'_{`;p}(\ ;\ )$ is computationally intensive, although there exist approximations that make the problem more tractable [31].

We have therefore found the communication modes which are given by the functions

$$\begin{aligned}
_{`;p}(r;\ ) &= \ \ _{`;p}(r;\ )e^{\ i`}\ \ e^{i\ \frac{k}{2z}r^2} \\
&= \frac{'_{`;p}(r=R_T;\ \ )}{q\ \overline{\ \ \ \

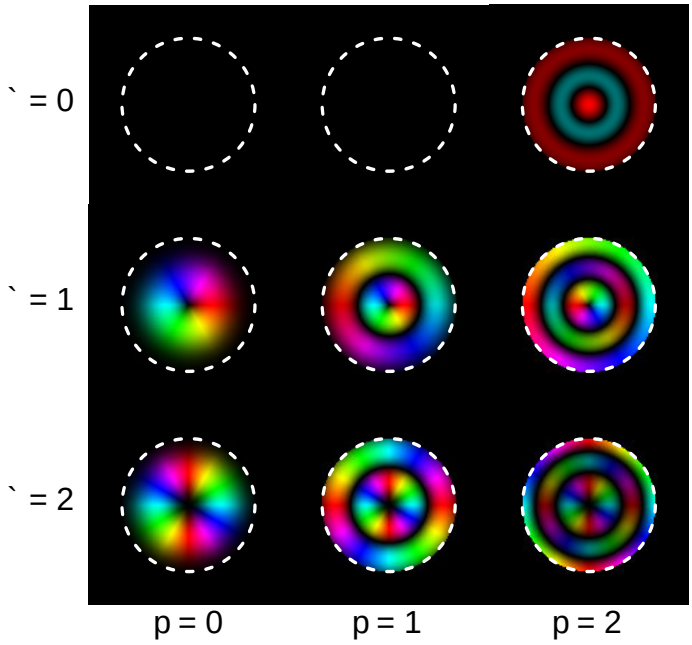

Figure 2.12: Plots of nine of the lowest order CPSWs given by the expression in Eq. (2.142) for a system with hard apertures and a Fresnel number product of $D_F = 25$. The dotted white lines represent the edge of the aperture. The complex phase information is represented by the hue of the color in the plots, while the amplitude is represented by the color's brightness. These modes have the same scaling as the LG modes plotted in Fig. 2.11 in order to show the close similarities between the two sets of modes.

Plots of the communication modes for a system with hard circular apertures and a Fresnel number product of $D_F = 25$ are shown in Fig. 2.12. It was demonstrated in section 2.5.2 that the PSWs communication modes of a system with hard square apertures are very similar to the HG modes of the analogous system with Gaussian apodized apertures. In the same way a comparison of Fig. 2.12 with Fig. 2.11 shows that the CPSWs can be closely approximated by the LG modes of an analogous apodized system.

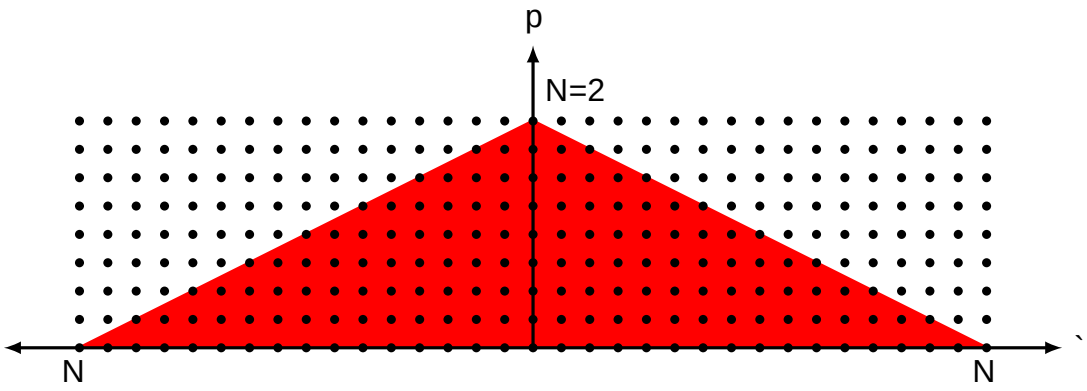

Figure 2.13: A configuration space diagram of CPSW communication modes. The red area indicates those states for which $2p + |\ell| \leq N$.

As was discussed in section 2.5.2, we expect the transmission efficiencies $\eta_{\ell;p}$ to be approximately equal to unity up to some sharp cutoff in the modal indices $(\ell; p)$ due to Abbe's model of diffraction between apertures. We know from section 2.5.1 that the maximum spatial frequencies of mode $(\ell; p)$ is related to the quantity $2p + |\ell|$, therefore we expect

$$\eta_{\ell;p} \begin{cases} 1 & \text{for } 2p + |\ell| \leq N \\ 0 & \text{otherwise} \end{cases}; \tag{2.143}$$

where N is some number related to the total number of modes the communication system supports.

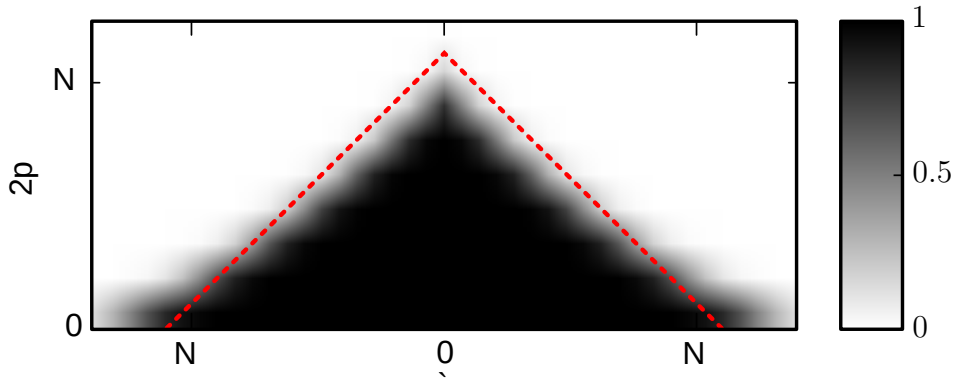

Figure 2.14: Plot of the transmission efficiencies $\eta_{\ell,p}$ for a free-space channel with hard apertures encoded using the circular prolate spheroidal communication modes of the channel. The efficiencies display a sharp cutoff for $2p + |\ell| > N$ which is represented by the dashed line.

The total number of modes such that Eq. (2.143) holds true is approximately D_F and thus

$$\begin{aligned} D_F &\approx \sum_{2p+|\ell| \le N} 1 \\ &= \sum_{p=0}^{N/2} \Bigg(\sum_{\ell=-(N-2p)}^{N-2p} 1 \Bigg) \\ &= \sum_{p=0}^{N/2} 2(N-2p)+1 \\ &= \frac{1}{2}(N+1)(N+2); \end{aligned} \tag{2.144}$$

which is represented diagrammatically as the red region in Fig. 2.13. Inverting this equation gives

$$N = \frac{1}{2}\sqrt{1+8D_F} - 3 \approx \sqrt{2D_F}. \tag{2.145}$$

A two dimensional plot of $_{`;p}$ is shown in Fig. 2.14 showing the accuracy of Eq. (2.143) (represented by the dashed line) compared with the actual numerically computed values.

2.7 Orbital angular momentum of light

The communication modes derived in section 2.6 are orbital angular momentum (OAM) eigenstates of light as will be demonstrated in this section. This is due to azimuthal dependence of the beam being described by the $e^{i`}$ phase term. Such beams are sometimes known as vortex beams with topological charge equal to ` due to the fact that the phase is singular at $r = 0$ with a topological winding number of ` about the optical axis [32].

As the "vortex" name suggests, there is a rotation of the field that is responsible for the existence of angular momentum in the beam. This can be seen if one considers the wavefronts of the beam. The phase of a vortex beam has the form

$$\text{phase} \quad kz + `; \tag{2.146}$$

which for surfaces of constant phase, will rotate about the optical axis with period $=`$. A plot of the wavefronts of the states $` 2 [3; 3]$ are shown in Fig. 2.15 which clearly show the rotational nature of the wavefront of these beams.

Figure 2.15: Plots of the seven lowest order Orbital angular momentum states of light. The top row shows states with negative topological OAM charge while the bottom row shows plots of states with negative charge. Two dimensional slices are presented at $z = 0$ and $z =$, while only the surface with phase equal to zero is shown between these two planes. Phase of the beams is represented by the color hue, while amplitude is represented by the color's brightness.

2.7.1 Rotational eigenmodes

In section 2.6 we made the ansatz that the azimuthal dependence of the communication modes of a system with circular apertures was completely described by the term $e^{i\ell}$. This is due to the fact that the system has cylindrical symmetry about the optical z