Bidirectional adaptive optics architectures for optical communication through atmospheric turbulence

by
Nivedita Chandrasekaran

S.B. Electrical Engineering, Massachusetts Institute of Technology (2008)
S.B. Physics, Massachusetts Institute of Technology (2009)
M.Eng Electrical Engineering and Computer Science, Massachusetts Institute of Technology (2009)

Submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering and Computer Science at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2016

© Massachusetts Institute of Technology 2016. All rights reserved.

Signature redacted

Author ................................................

Department of Electrical Engineering and Computer Science

Certified by ...........................................
Jeffrey H. Shapiro
Julius A. Stratton Professor of Electrical Engineering
Thesis Supervisor

Accepted by ...........................................
Wlad A. Kolodziejski
Chairman, Department Committee on Graduate Theses
Bidirectional adaptive optics architectures for optical communication through atmospheric turbulence

by

Nivedita Chandrasekaran

Submitted to the Department of Electrical Engineering and Computer Science
on August 31, 2016, in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering and Computer Science

Abstract

Free-space optical (FSO) classical communication links can provide high data rates vital for successfully serving the world’s exponentially growing demand for bandwidth, while FSO quantum key distribution (QKD) links allow information-theoretic rather than computational secure communication between two parties. Unlike fiber-optic classical communication and QKD links, FSO links can do so with minimal up-front investments in infrastructure. Setting aside absorption and scattering losses along the propagation path, optical links with a terrestrial terminal will still experience the deleterious effects of clear-weather turbulence, namely beam spread, beam wander, angle-of-arrival spread, and scintillation, which leads to low end-to-end power transfer from the transmitter to receiver. Decreases in the power transfer result in lower communication rates and may result in no secure-key rate for the loss-sensitive QKD communication protocols. Adaptive optics holds the best promise for mitigating, if not completely compensating for, these turbulence-induced degradations.

Nevertheless, despite adaptive optics being a richly developed field, theoretical studies of adaptive optics systems have not fully exploited the reciprocal nature of propagation through atmospheric turbulence. It is known that applying ideal, full-wave adaptive optics at both the transmitter and receiver of a free-space optical link can guarantee scintillation-free power transmission when operation is deep in the near-field power transfer regime. Buoyed by the advent of enabling technologies like scalable Mach-Zehnder interferometer arrays and coherent receiver arrays, this thesis: (1) introduces both a full-wave and phase-only bidirectional adaptive optics (BDAO) protocol; (2) assesses the ergodic performances of FSO classical and QKD communication links utilizing these BDAO systems using both theoretical performance bounds as well as turbulence simulation results; and (3) provides an initial study of the noise and time-dynamics the BDAO protocol can tolerate while still achieving near-optimal classical communication or QKD rates.

Thesis Supervisor: Jeffrey H. Shapiro
Title: Julius A. Stratton Professor of Electrical Engineering
Acknowledgments

My time as a graduate student at MIT and the completion of this thesis would not have been nearly as enjoyable (or possible!) without the support of many people.

First and foremost, I would like to thank my advisor, Professor Jeffrey H. Shapiro, for his invaluable guidance during his time as my supervisor. I have known him since 2005 when he became my EECS advisor after I chose to major in electrical engineering as an undergraduate at MIT. As my undergraduate advisor, Jeff provided valuable advice on course selection with an eye towards gaining a wider breadth of technical knowledge so that I would get the most out of my time as an undergraduate in EECS at MIT. As my on-campus supervisor during my time as a VI-A M.Eng. thesis student, Jeff spent a truly amazing amount of time with me ensuring that I fully understood the historical background and physics behind my project, and also spent an unbelievable amount of time editing both my M.Eng. thesis proposal and M.Eng. thesis. So, when I returned to MIT as a graduate student, I was very honored that Jeff offered to take me on as a student in his group. I am very grateful to have had him as my advisor for four reasons: (1) his breadth of knowledge of both the theory and physical implementations of quantum communications; (2) his ability and willingness to patiently explain technical concepts from first principles; (3) his clear communication of the standards to which his students should adhere; and (4) his concern for the well-being and success of his students. All of these qualities have ensured that I have had a wonderful time as one of his students, and that he will be one of the people on whom I will pattern my research and management style in the future.

Next, I would also like to thank my thesis committee, Professor Vincent Chan and Dr. Tim Yarnall of Group 67 at MIT Lincoln Laboratory, for their time and advice on my thesis work. Professor Chan provided excellent historical context for my research and suggested relevant papers to read, and his courses on optical communication networks, while not directly relevant to my thesis, will be something that will serve me well in my career in industry. Dr. Yarnall provided useful reminders to consider experimental implementations of my thesis work, adding valuable perspective to my
This thesis would not have been possible without the support of Group 67 at MIT Lincoln Laboratory (MITLL). First, I must thank Dr. Scott Hamilton for hiring me as a summer intern in 2013 and then continuing to advocate for my thesis research via the Integrated Quantum Initiative (IQI) at MITLL. His willingness to make time for me to talk about the future of my thesis research and his sage advice on my career path after completing my Ph.D. made me feel very supported as I performed my thesis work at MITLL. I am also very thankful to Dr. Roy Bondurant for his support of my thesis work at MITLL and his clearing of bureaucratic hurdles. Without Dr. Hamilton and Dr. Bondurant’s support, I would not have been able to complete the simulation work in this thesis.

Working at Group 67 has been a great privilege — it is very easy, especially during a theory-focused Ph.D. thesis, to become fairly isolated and lose perspective on the utility of the work and the ways in which it could be immediately useful. At Group 67, however, I was able to constantly converse with a wide range of colleagues whose diversity of experience and expertise kept me constantly aware of applications for my thesis work. I am especially grateful to Dr. Andrew Puryear, Dr. Venkat Chandar, Dr. P. Ben Dixon, and Dr. Andrew Fletcher for all the time they have spent with me and advice they have given me. I am also thankful to Dr. Matt Grein and Ryan Murphy for being fantastic MITLL officemates and always being willing to answer my questions about their work. Thanks to Mark Besch for his invaluable IT help and his fascinating stories. Finally, many thanks to Gary Hackett — having known him since 2006 when I first started as an undergraduate summer intern at MITLL, his peppy presence and cheerful conversations have been a consistent source of happiness at MITLL.

A running theme throughout these acknowledgments has been my reliance on colleagues with a wide array of research backgrounds and interests at MITLL. I have had the joy of being a member of not one, but two, similarly interdisciplinary communities on campus. I am grateful to the Interdisciplinary Quantum Information Science and Engineering (iQuISE) program for funding the first three years of my research.
thesis work at MIT and providing a supportive community and course framework with which to jumpstart the initially daunting process of gaining a foothold in quantum communication and computation. Similarly, I am very happy to have been a member of the IQI, a collaboration between MITLL and MIT to foster collaboration in quantum research between the two institutions. Without the framework and community provided by these interdisciplinary communities, I would not have been able to properly appreciate the wide breadth of applications of quantum computation and communication, and would not have gained nearly as much as I did from my time as a graduate student at MIT.

Having thanked the abstract entities, I would like to thank the following people for being fantastic colleagues and MITLL shuttle buddies: thanks to Catherine Lee, Hannah Clevenson, and Greg Steinbrecher for making every day at Lincoln fun. Thanks to Catherine for QKD/security discussions and poster session support, thanks to Hannah for fantastically useful presentation feedback, and thanks to Greg for super-useful optics discussions and abetting my crossword obsession. Being a member of the Optical and Quantum Communications Group has been a joy, with my special thanks to Chris Chudzicki, Dr. Nick Hardy, Justin Dove, and Quntao Zhuang for their friendship and collaboration. Thanks to Dr. Tom Baran and Dr. David B. Cole for their friendship and advice over the years.

Thanks to Professor Anantha Chandrakasan for giving me a warm welcome on my return to MIT, and for giving me the opportunity to TA during the second year of SuperUROP. Thanks to Patsy Sampson for lovely pictures and lovelier conversation. Many thanks to Janet Fischer and Alicia Duarte for all of the assistance they’ve given me and red tape they’ve cut through — I really don’t know what EECS graduate students would do without them.

Thanks to my fellow students in my Harvard Tamil class, and my great gratitude and thanks to our teacher Jonathan Ripley, whose classes are one of the great highlights of my time as a graduate student. His fantastic curriculum, hilarious classes, and determination to make Tamil accessible to his students have opened up a whole new world for me.
Thank you to the fantastic friends, old and new, I have made and kept up with during my fairly long time at MIT (some of whom have already been thanked!). I have not yet mentioned the Quantum Girls, especially Veronika Stelmakh, Sara Mouradian, and Dr. Clarice Aiello for all the support and seriously fun times they provided throughout these six years. A further thanks to Catherine and Hannah for socially conscious and supportive conversations about being women in science. Thanks to Veronika, Dr. Mitali Thakor and Sebastian Schmidt for pushing along with me in these last few months of thesis-writing — I’m looking forward to all the dance parties we’re going to have all over the country as we all get done with our theses!

I have been very lucky to keep old friends that I made at MIT in my time there as an undergraduate — thanks to: (1) Lauren White for being a constant source of support and soothing time with kitties Link and Zelda; (2) Clinton Blackburn and Michelle Lessly for their wellness checks and their understanding of my migraine and/or thesis-induced flakiness; and (3) Wendi Li and Helen Liang, for cross-country sanity checks and reminders to just finish already. Thanks to Dexter Liu for having been an awesome friend since high school and starting the StarParty email thread.

Finally, this thesis would not have been possible without the support of my parents, Dr. Hema Chandrasekaran and Chandrasekaran (Chandra) Kalyanaraman. It is difficult for me to express how grateful I am to have such an empathetic and constant source of support. To my mother, Hema, thank you for all of the technical advice, editing of papers, emotional and mental support, and reminders of the great things waiting for me after I complete my Ph.D. To my father, Chandra, thank you for being a soothing and steady presence in my life, for being my source of home-roasted, high-grade coffee, for being willing to drop everything and come spend time with me when I needed it the most, and for all the 3AM wakeup calls during the last month of this thesis. I love you both very much, cannot believe how lucky I am to have you two as parents, and look forward to being closer to you both and spending more time with you.
Contents

1 Introduction 25
   1.1 Atmospheric propagation and its common consequences 26
   1.2 Previous approaches to communication through turbulence 28
   1.3 Towards scintillation-free communication 31

2 Single-Spatial-Mode Power Transfer through Atmospheric Turbulence 35
   2.1 A mathematical model of the free-space optical propagation channel 36
       2.1.1 Normal-mode decomposition of the free-space propagation kernel 38
       2.1.2 Mutual coherence function of the free-space propagation Green's
            function 40
   2.2 Channel transmissivity bounds in single-spatial mode operation 41
   2.3 Power transfers of FSO links operating with bidirectional adaptive optics (BDAO) 45
       2.3.1 Full-wave bidirectional compensation 45
       2.3.2 Phase-only bidirectional compensation 50
       2.3.3 Simulating turbulence with Parallel Optical Propagation Software (POPS) 51
   2.4 Full-wave and phase-only BDAO power transfer statistics 56
       2.4.1 Probability distributions and convergence behavior of the extinction-loss
            neglected BDAO power transfers 56
       2.4.2 Steady-state BDAO power transfers in FSO links with extinction 63
3 Single-Spatial-Mode Classical Communication through Atmospheric Turbulence

3.1 Classical communication over a free-space link .................................. 70
3.2 Rate bounds for FSO classical communication links ............................. 72
3.3 Classical capacities of FSO links operating with BDAO ...................... 76
3.4 Challenges in achieving optimal communication rates in a free-space link 80

4 Single-Spatial-Mode Quantum Key Distribution through Atmospheric Turbulence

4.1 Overview of QKD protocols ................................................................. 84
4.2 Secret-key rate bounds for FSO decoy-state BB84 QKD links .............. 87
  4.2.1 Decoy-state BB84 ............................................................... 88
  4.2.2 Performance bounds for decoy-state BB84 ......................... 92
4.3 Decoy-state BB84 QKD secret-key rates of FSO links operating with BDAO .......................... 95

5 Single-Spatial-Mode Floodlight Quantum Key Distribution through Atmospheric Turbulence

5.1 Overview of the floodlight quantum key distribution protocol .......... 105
  5.1.1 Alice and Eve's deterministic-channel receiver performance ...... 110
  5.1.2 Performance bounds of FL-QKD ......................................... 117
5.2 Floodlight QKD secret-key rates of FSO links operating with BDAO 120

6 Communication with multiple spatial modes in atmospheric turbulence

6.1 M-spatial-mode links with and without adaptive optics ..................... 128
6.2 Power transmissivity and crosstalk statistics of an M-spatial mode link 132
6.3 Rate bounds for M-spatial mode FSO classical communication links 133
6.4 Secret-key rate bounds for multi-spatial-mode ds-BB84 QKD in turbulence ............... 141
6.5 Secret-key rate bounds for multi-spatial-mode FL-QKD in turbulence 146
7 Communication with FSO links operating with non-ideal BDAO systems

7.1 FSO links operating with BDAO with Gaussian noise .............. 154
  7.1.1 Full-wave bidirectional compensation with AWGN ......... 154
  7.1.2 Phase-only bidirectional compensation with AWGN ..... 156
  7.1.3 Power transfers of full-wave and phase-only BDAO with AWGN 157
  7.1.4 Communication over FSO links with extinction .......... 165

7.2 FSO links operating with non-instantaneous BDAO in wind ...... 173
  7.2.1 Full-wave and phase-only bidirectional compensation with wind 173
  7.2.2 Power transfer statistics of full-wave and phase-only BDAO with wind .......... 175
  7.2.3 Communication over FSO links with extinction .......... 179

8 Conclusions and Future Work ........................................... 189

A Scaling property of the turbulent channel's mutual coherence function 195

B Verification and validation procedures for POPS .................. 199

C Probability distribution fits for $\tilde{\eta}_1^{\text{full}}$ and $\tilde{\eta}_1^{\text{phase}}$ 205

D Secret-key rate of BB84 QKD with decoy states .................. 209

E Secret-key rate of floodlight QKD ................................. 217
List of Figures

2-1 Atmospheric-channel propagation geometry. .......................... 38
2-2 A model for ideal bidirectional full-wave compensation through atmospheric turbulence on its $k^{th}$ iteration. .......................... 47
2-3 A model for phase-only bidirectional full-wave compensation through atmospheric turbulence on its $k^{th}$ iteration. .......................... 50
2-4 An example of full-wave field propagation performed by POPS from transmitter aperture $A_T$ at $z = 0$ to receiver aperture $A_R$ at $z = L$ with the assumption of moderate turbulence and wind along the path. 52
2-5 Histograms for $\hat{n}_1^{\text{full}}(k)$ (plotted with filled green bars) and $\hat{n}_1^{\text{phase}}(k)$ (plotted with open green bars) and their corresponding beta-distribution fits for $D_f = 4$ in mild, moderate, strong, and very strong turbulence for an FSO link with no extinction loss and parameters given in Table 2.3. 58
2-6 Convergence behavior of the power transmissivity distributions $\hat{n}_1^{\text{full}}(k)$ and $\hat{n}_1^{\text{phase}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3. 60
2-7 Surface plots of $\beta$-distribution parameters $a$ and $b$ as functions of the Fresnel-number product $D_f$ and Rytov-logamplitude variance $\sigma^2_\chi$ for the $\beta$-distribution fits made to $\hat{n}_1^{\text{full}}$ and $\hat{n}_1^{\text{phase}}$ for an FSO link with no extinction loss and with parameters given in Table 2.3. 62
2-8 Moderate turbulence, $\sigma^2_\chi = 0.137$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3. 64
2-9 Strong turbulence, $\sigma_\chi^2 = 1.37$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3.

2-10 Very strong turbulence, $\sigma_\chi^2 = 13.7$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3.

3-1 Upper and lower bounds on heterodyne, homodyne, and Holevo capacities for free-space optical communication for varying turbulence strengths over a link for fixed signal photon number $N_s = 1$ for the notional case set in Table 2.3.

3-2 Moderate turbulence, $\sigma_\chi^2 = 0.137$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta_1) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$.

3-3 Strong turbulence, $\sigma_\chi^2 = 1.37$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta_1) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$.

3-4 Very strong turbulence, $\sigma_\chi^2 = 13.7$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta_1) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$.

4-1 The secret key rate of a ds-BB84 QKD channel, $R_{\text{ds-BB84}}(\eta, n_b)$, versus a deterministic power transmissivity $\eta$ for a fixed background $n_b = 10^{-4}$ photons/use and a modulation rate $R_{\text{mod}} = 10$ Gbps.

4-2 Moderate turbulence, $\sigma_\chi^2 = 0.137$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10$ Gbps.
4-3 Strong turbulence, $\sigma^2_\chi = 1.37$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{\text{mod}} = 10$ Gbps. ........................................ 98

4-4 Very strong turbulence, $\sigma^2_\chi = 13.7$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{\text{mod}} = 10$ Gbps. ........................................ 100

5-1 A model of FL-QKD between two parties Alice and Bob in the presence of an eavesdropper Eve making an optimal frequency-domain collective attack by using her own SPDC source and a beam splitter. For simplicity, only the $m^{th}$ modes are shown, but modes $1 \leq m \leq M = TW \gg 1$ are employed in the protocol. ........................................ 107

5-2 The secret key rate of a FL-QKD channel, $R_{\text{FL}}(\eta_{\text{atm}})$, versus a deterministic power transmissivity $\eta_{\text{atm}}$ for the FL-QKD parameters set in Table 5.1. ........................................ 116

5-3 Moderate turbulence, $\sigma^2_\chi = 0.137$: Lower bounds on $\langle R_{\text{FL}}(\eta_1) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. . . . 121

5-4 Strong turbulence, $\sigma^2_\chi = 1.37$: Lower bounds on $\langle R_{\text{FL}}(\eta_1) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. . . . 123

5-5 Very strong turbulence, $\sigma^2_\chi = 13.7$: Lower bounds on $\langle R_{\text{FL}}(\eta_1) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. . . . 125

6-1 Power transmissivity statistics for $M = 169$ spatial mode system operating with a Fresnel-number product $D_f = 250$, realized by square transmitter and receiver apertures with sides of length $d = 49.5$ cm and with other operational parameters described in Table 2.3. . . . . . . . 138
Upper and lower bounds on photon information efficiency (plotted as bits/transmitted photon) as functions of spectral efficiency of the ergodic Holevo capacities for a $M = 169$ FB-mode system with a Fresnel-number product $D_f = 250$, realized by square transmitter and receiver apertures with sides of length $d = 49.5$ cm and with other operational parameters described in Table 2.3. 

The top 20 average mode couplings $\langle |h_{m0}^{\text{non}}|^2 \rangle$ for FB mode $\Phi_{0,0}^{(0)}(\rho)$ for an $M = 169$ FB-mode system with a Fresnel-number product $D_f = 250$, realized by square transmitter and receiver apertures with sides of length $d = 49.5$ cm and with other operational parameters described in Table 2.3.

Upper and lower bounds on the 9-spatial mode ds-BB84 secret-key rate $R_{ds-BB84,M}$ in no turbulence, mild, moderate, strong, and very strong turbulence vs. the Fresnel number product $D_f$ for a link with parameters given in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{\text{mod}} = 10$ Gbps.

Upper and lower bounds on the 169-spatial mode ds-BB84 secret-key rate $R_{ds-BB84,M}$ in no turbulence, mild, moderate, strong, and very strong turbulence vs. the Fresnel number product $D_f$ for a link with parameters given in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{\text{mod}} = 10$ Gbps.

Upper and lower bounds at $D_f = 1$ on the multiple-spatial mode ergodic decoy-state BB84 QKD secure rate $\langle R_{ds-BB84,M} \rangle$ in vacuum, mild, moderate, strong, and very strong turbulence vs. a varying number $M$ of spatial modes with all other link parameters given in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{\text{mod}} = 10$ Gbps.

Lower bounds on the 9-spatial mode ergodic FL-QKD secure rate $\langle R_{FL,M} \rangle$ in no, mild, moderate, strong, and very strong turbulence vs. the Fresnel number product $D_f$ for a link with parameters given in Tables 2.3 and 5.1.
6-8 Lower bounds on the 169-spatial mode ergodic FL-QKD secure rate $(R_{FL,M})$ in no, mild, moderate, strong, and very strong turbulence vs. the Fresnel number product $D_f$ for a link with parameters given in Tables 2.3 and 5.1. 149

6-9 Upper and lower bounds on the multiple-spatial mode ergodic FL-QKD secure rate $(R_{FL,M})$ in no, mild, moderate, strong, and very strong turbulence vs. a varying number $M$ of spatial modes for a link with fixed Fresnel number product $D_f = 1$ and parameters given in Tables 2.3 and 5.1. 151

7-1 A model for bidirectional full-wave compensation with AWGN through frozen atmospheric turbulence on its $k^{th}$ iteration. 155

7-2 A model for ideal bidirectional phase-only compensation with AWGN through atmospheric turbulence on its $k^{th}$ iteration. 157

7-3 Convergence behavior of the power transmissivity distributions $\hat{\eta}_1^{\text{full-noise}}(k)$ and $\hat{\eta}_1^{\text{phase-noise}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate, strong, and very strong turbulence operating with AWGN with $\text{SNR}_0 = 6 \text{ dB}$. 159

7-4 Convergence behavior of the power transmissivity distributions $\hat{\eta}_1^{\text{full-noise}}(k)$ and $\hat{\eta}_1^{\text{phase-noise}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate, strong, and very strong turbulence operating with AWGN with $\text{SNR}_0 = 3 \text{ dB}$. 160

7-5 Moderate turbulence, $\sigma_x^2 = 0.137$: Histograms for $\hat{\eta}_1^{\text{full}}$ and $\hat{\eta}_1^{\text{phase}}$ and their corresponding beta-distribution fits vs. histograms for $\hat{\eta}_1^{\text{full-noise}}$ and $\hat{\eta}_1^{\text{phase-noise}}$ and their beta-distribution fits. An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with $\text{SNR}_0 = 6 \text{ dB}$ or $3 \text{ dB}$ for the cases with AWGN. 162
7-6 Strong turbulence, $\sigma^2_\chi = 1.37$: Histograms for $\hat{\eta}_1^{\text{full}}$ and $\hat{\eta}_1^{\text{phase}}$ and their corresponding beta-distribution fits vs. histograms for $\hat{\eta}_1^{\text{full-noise}}$ and $\hat{\eta}_1^{\text{phase-noise}}$ and their beta-distribution fits. An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with SNR$_0$ = 6 dB or 3 dB for the cases with AWGN. .......................... 163

7-7 Very strong turbulence, $\sigma^2_\chi = 13.67$: Histograms for $\hat{\eta}_1^{\text{full}}$ and $\hat{\eta}_1^{\text{phase}}$ and their corresponding beta-distribution fits vs. histograms for $\hat{\eta}_1^{\text{full-noise}}$ and $\hat{\eta}_1^{\text{phase-noise}}$ and their beta-distribution fits. An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with SNR$_0$ = 6 dB or 3 dB for the cases with AWGN. .......................... 164

7-8 Moderate turbulence, $\sigma^2_\chi = 0.137$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for SNR$_0$ = 6 dB and 3 dB vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. .......................... 166

7-9 Strong turbulence, $\sigma^2_\chi = 1.37$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for SNR$_0$ = 6 dB and 3 dB vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. .......................... 168

7-10 Very strong turbulence, $\sigma^2_\chi = 13.67$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for SNR$_0$ = 6 dB and 3 dB vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. .......................... 169

7-11 Moderate turbulence, $\sigma^2_\chi = 0.137$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10$ Gbps. .......................... 170
7-12 Strong turbulence, $\sigma^2 = 1.37$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $R_{\text{ds-BB84}}(\eta_1)$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10 \text{ Gbps}$.

7-13 Very strong turbulence, $\sigma^2 = 13.67$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $R_{\text{ds-BB84}}(\eta_1)$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10 \text{ Gbps}$.

7-14 A model for $k^{th}$ iteration bidirectional full-wave compensation with time-delayed compensation through atmospheric turbulence that is time varying because of a transverse wind with speed $v_w$.

7-15 A model for $k^{th}$-iteration bidirectional phase-only compensation with time-delayed compensation through atmospheric turbulence that is time varying because of a transverse wind with speed $v_w$.

7-16 Convergence behavior of the power transmissivity distributions $\tilde{\eta}^{\text{full-wind}}_1(k)$ and $\tilde{\eta}^{\text{phase-wind}}_1(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate, strong, and very strong turbulence operating with $v_w = 12 \text{ m/s}$ and $t_\Delta = 0.5 \text{ ms}$.

7-17 Histograms for $\tilde{\eta}^{\text{full}}_1$ (plotted with filled green bars) and $\tilde{\eta}^{\text{phase}}_1$ and their corresponding beta-distribution fits plus histograms for $\tilde{\eta}^{\text{full-noise}}_1$ and $\tilde{\eta}^{\text{phase-noise}}_1$ operating with wind speed $v_w = 12 \text{ m/s}$ and time delay $t_\Delta = 0.5 \text{ ms}$ for an FSO link with $D_f = 0.05$, no extinction loss, and parameters given in Table 2.3.
7-18 Moderate turbulence, $\sigma_x^2 = 0.137$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay $t_\Delta = 0.5\text{ ms}$.

7-19 Strong turbulence, $\sigma_x^2 = 1.37$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay $t_\Delta = 0.5\text{ ms}$.

7-20 Very strong turbulence, $\sigma_x^2 = 13.67$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay $t_\Delta = 0.5\text{ ms}$.

7-21 Moderate turbulence, $\sigma_x^2 = 0.137$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10\text{ Gbps}$.

7-22 Strong turbulence, $\sigma_x^2 = 1.37$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10\text{ Gbps}$.

7-23 Very strong turbulence, $\sigma_x^2 = 13.67$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10\text{ Gbps}$. 
B-1 Earth-to-space channel geometry. ............................ 200
B-2 Intensity plot of a POPS-propagated field displaying grid-like spatial artifacts as a result of its propagation with a too-large rVaryCos filter radius. .................................................... 201
B-3 POPS propagation of a field at $z = 0$ through a phase screen at $z = L_1$
    to a final transverse plane at $z = L_2$. ........................ 201
B-4 Field intensities at $z = L$ received when the focused, flat-intensity beam $U_0(\rho)$ is transmitted for an FSO link with $D_f = 4$ and parameters listed in Table 2.3 in strong and very strong turbulence. .......... 203

21
List of Tables

2.1 Spherical-wave coherence length ($\rho_0$) and weak-perturbation spherical-wave logamplitude variance ($\sigma_\chi^2$) versus turbulence strength ($C_n^2$) for a 10-km-long path at 1.55 $\mu$m wavelength. ........................................ 54

2.2 Square aperture side $d$ versus the Fresnel-number product $D_f$ for a 10-km-long path at 1.55 $\mu$m wavelength with identical square transmitter and receiver apertures of the same size. Turbulence strengths in units of both $C_n^2$ and $\sigma_\chi^2$ for which apertures of area $d^2$ would lie inside an atmospheric coherence area $\rho_0$ are also given. ......................... 55

2.3 Parameter values for the notional case of link geometry and turbulence values selected for a use case in this thesis. .......................... 55

3.1 First and second derivatives of the heterodyne, homodyne, and Holevo capacities of a non-fading, pure-loss channel. ....................... 73

3.2 Taylor expansions of the heterodyne, homodyne, and Holevo capacities of a non-fading, pure-loss channel for small $\eta N_s$ and values of $\eta C(N_s)$. 73

5.1 Parameter values for the notional case of an FL-QKD link selected as a use case for the rest of this thesis. .............................. 115
7.1 POPS-simulated SNR values at the conjugate transmitter at \( z = L \) conjugate transmitter for \( k = 4 \) iterations of full-wave BDAO with AWGN assuming SNR\( _0 = 6 \text{ dB} \) with \( D_f = 4 \), no extinction loss, and parameters given in Table 2.3 for moderate \( (\sigma^2_X = 0.137) \), strong \( (\sigma^2_X = 1.367) \), and very strong turbulence \( (\sigma^2_X = 13.67) \) averaged over 1,000 POPS turbulence simulations.

C.1 Parameters with 95% confidence intervals for the polynomial fit function given in (2.39) for the parameters \( a(D_f, \sigma^2_X) \) and \( b(D_f, \sigma^2_X) \) of the \( \beta \) distribution \( \beta_{\hat{n}_{\text{full}}} (\eta; a, b) \) of the steady-state power transmissivity \( \hat{n}_{\text{full}} \) for full-wave BDAO operation in an FSO link with no extinction loss and with parameters given in Table 2.3.

C.2 Parameters with 95% confidence intervals for the polynomial fit function given in (2.39) for the parameters \( a(D_f, \sigma^2_X) \) and \( b(D_f, \sigma^2_X) \) of the \( \beta \) distribution \( \beta_{\hat{n}_{\text{phase}}} (\eta; a, b) \) of the steady-state power transmissivity \( \hat{n}_{\text{phase}} \) for full-wave BDAO operation in an FSO link with no extinction loss and with parameters given in Table 2.3.
Chapter 1

Introduction

Information transfer in an electromagnetic-wave communication link is accomplished by generating the wave, encoding data by applying a modulation scheme to the wave, and then allowing the wave to propagate through some medium to a receiver where it is demodulated and decoded. Communicating at optical wavelengths, instead of the longer wavelengths of the radio-frequency regime, yields a larger available modulation bandwidth, permits the communication system to achieve a higher power density in a narrower beam, and allows for the construction of smaller transmitters and receivers because of the small sizes of optical components [1]. Generally, optical communication links are either guided or unguided, i.e. they use optical fiber or propagate through free space.

Fiber-optic communications are the backbone of the Internet, providing high-rate, reliable communication links. However, the construction of an optical fiber network capable of providing full connectivity to end-users requires a serious infrastructure investment since the network’s optical fibers must either be laid underground or strung above ground [2]. If additional capacity is needed such that a new fiber must be added to the network in either a densely populated region or a remote and previously unserved location, the required investment in time and capital can be prohibitive. In contrast, free-space optical (FSO) links only require a line of sight between a transmitter and receiver in order to provide the same Gbps data rates that would be achieved by analogous fiber-optic links. They are also the only option for
long-haul communication links between ground stations and satellites or unmanned aerial vehicles. Furthermore, they are also an interesting option for purely terrestrial short-haul communication links [3, 4] operating in densely populated metropolitan areas (i.e. between office buildings [5]) or providing high-bandwidth connections from end-users to fiber backbones of optical networks. In both cases, atmospheric paths are involved. Because improving optical communication performance for atmospheric optical paths is the subject of this thesis, it is germane to begin with a discussion of the atmosphere's effects on FSO links.

1.1 Atmospheric propagation and its common consequences

In bad weather, the presence of clouds or fog along the line-of-sight\(^1\) path prevents high-rate Gbps free-space optical communications [6]. Since we are interested in high data-rate communications, we assume clear-weather propagation, and discuss the atmosphere's effects in this regime. Even in clear weather, absorption and scattering arise from the atmosphere's molecular constituents and the presence of aerosols and particulates along the propagation path. The power lost to these effects can be assessed using software packages like MODTRAN [7] that provide wavelength-dependent transmittance curves for various profiles of particulate, molecular, and aerosol matter along an atmospheric link, which, in turn, are functions of the geographic location and altitude of the link. Typically, wavelengths in the low-loss atmospheric windows in the near-infrared (0.7-1.7 \(\mu m\)) and mid-infrared (3-5 \(\mu m\)) regime [8] yield the best power transfer. Further narrowing of the wavelength selection requires the knowledge of the bandwidth and noise characteristics of the optical

\(^1\)Intermittent physical obstructions, such as birds flying across the path, will temporarily degrade if not destroy information transmission along a free-space path. Pointing or tracking errors on transmitter or receiver platforms that may arise from building sway or platform motion may do the same. These impediments are typically treated as outages whose effects can be alleviated by applying interleaved coding (where the interleaving time is longer than a typical outage period). Bad weather, however, can cause outages whose durations far exceed any reasonable interleaving time.
components (e.g., detectors and spectral filters) with which the optical link's transmitter and receiver will be implemented. Judicious selection of the operating wavelength can minimize absorption and scattering losses. However, the link will still be affected by atmospheric turbulence.

Atmospheric turbulence is the name given to the parts-per-million refractive-index fluctuations along the propagation path that are due to the turbulent mixing of air parcels with temperature variations on the order of 1K. As a result, the wavefront of the propagating beam will experience the following principal detrimental effects [9]:

- **Beam wander and beam spread**: Beam wander is defined as the random motion of the beam's centroid [10]. Beam spread is the increased spatial extent of the beam's time-averaged power density in the receiver's entrance aperture beyond the transmitter's diffraction limit [11]. Beam spread includes the time-averaged wander of an otherwise undistributed beam plus the time-averaged effect of the beam breakup that occurs when the receiver's aperture contains many atmospheric coherence areas. Beam wander and beam spread can severely reduce the power coupled into the receiver.

- **Angle-of-arrival spread**: Angle-of-arrival spread is the increased extent of the time-averaged power density in the receiver's focal plane beyond the diffraction limit of its objective lens [12].

- **Scintillation**: Scintillation is the random power density fluctuations of the beam across the receiver's entrance aperture due to the constructive and destructive interference of the wave's distorted phasefront [13].

In contrast to the effects just described, the other characteristics of propagation through turbulence are rather benign. Turbulence does not depolarize the propagating electromagnetic wave [14]. Neither does it induce appreciable dispersion or multipath spreading of the propagating beam, because it has a coherence bandwidth in excess of 1 THz [15]. Furthermore, turbulence has a coherence time on the order of milliseconds. Thus, Gbps communication systems can assume that the state of
turbulence is frozen over the transmission of millions of bits, and can attempt to compensate for its listed effects accordingly.

Beam-spread and angle-of-arrival spread are typically 10's of μrad. If the entire transmitter and receiver apertures lie within single atmospheric coherence areas, then these variations can be almost completely eliminated with tilt-tracking systems. Scintillation effects, however, are by far the most catastrophic in an FSO link. They can cause deep fades with millisecond [13] durations whose mitigation at Gbps communication rates requires interleaving and error correction codes that greatly increase the complexity and latency of a communication system. Thus, the design, implementation, and integration of scintillation-limiting physical layer architectures into free-space optical links is imperative for establishing high-rate free-space optical communication links. Next, we discuss the work that has been done towards this goal.

1.2 Previous approaches to communication through turbulence

There is a large and well-developed body of work that seeks to construct architectures for free-space optical links that compensate for turbulence-induced beam spread, beam wander, and scintillation [16–24]. The initial burst of work on the theory of optical communications through the atmosphere began almost immediately after the invention of the laser [12, 14, 25, 26]. Activity in the field waned, however, as it became clear that short-haul free-space links (unlike fiber links) would experience outages due to bad weather, rendering them unacceptable for telecommunication applications. FSO connections to satellites were considered, but the combination of immature optical technologies and relatively low data rate requirements made radio-frequency communication links a far more attractive option. Finally, in 1995, the first two-way optical link between a satellite and the ground was established with the Ground-to-Orbit Lasercom Demonstration [27]. It was followed by further successful demonstrations of bidirectional long-haul optical communication links in 2001 with
the Geosynchronous Lightweight Technology Experiment and the Semiconductor-
laser Intersatellite Link Experiment [28]. Research in optical communication through
atmospheric turbulence thus saw a resurgence, as any successful free-space optical
link required to communicate with a terrestrial terminal would have to deal with
atmospheric turbulence in some manner.

Due to the focus on constructing uplinks and downlinks between ground stations
and satellites, for which all successful implementations had used some form of pulse-
position modulation encoding, initial work focused on improving the performance of
free-space optical links employing intensity modulation schemes and direct detection.
Assuming weak turbulence, so that the statistics of the phase and log-amplitude fluctu-
tuations of a turbulence-distorted beam could be taken to be jointly Gaussian, was
common in this early work. In particular, Zhu et al. [16–18] sought to limit the im-
pact of turbulence-induced fading on intensity-modulated symbols by applying digital
communication theory to construct maximum-likelihood estimators and error-control
codes for spatial-diversity reception. They assumed that the individual receivers knew
the overall fading statistics of the atmosphere but had no knowledge of the turbulent
channel’s instantaneous state, and simply experienced additive Gaussian noise. Fur-
ther work by Razavi and Shapiro [19] improved the performance characterization of
direct-detection spatial-diversity receivers in atmospheric turbulence by considering
the physical optical components that would perform the incoherent detection. Bit-
error-rate (BER) and signal-to-noise ratio (SNR) analyses were modified to take the
shot and thermal noise models of photon-counting detectors into account, and the
effects of introducing optical preamplifiers were considered. It was found that optical
preamplification suppressed receiver thermal noise, greatly aiding the performance of
diversity detection techniques like aperture averaging and receiver adaptive optics.

Focus on the performance of actual optical receivers in turbulence (rather than
the generic receivers with simple Gaussian noise) with the use of spatial diversity
techniques led to analysis of coherent rather than direct-detection reception. Lee and
Chan [20, 21, 29] found that utilizing the more sensitive techniques of heterodyne
or homodyne reception in conjunction with diversity detection greatly improved the
performance of an FSO link while, thus decreasing the link's outage probability. It was found that recklessly increasing the spatial diversity of a receiver employing direct detection invariably decreased the performance of the FSO communication link, due to the additional background noise introduced with each additional photon-counting detector. In contrast, the diversity of a coherent detection system could be increased without penalty, due to the ability of coherent detection techniques to reject background noise and interference [21]. This work made it clear that coherent diversity reception was the best strategy for improving the performance of terrestrial FSO links in turbulence.

After the development of receiver architectures for weak atmospheric turbulence, research turned to further performance improvements that could be achieved if an FSO link had a transmitter capable of adaptively modifying outgoing beams in an effort to construct near-optimal spatial wavefronts for atmospheric propagation after being fed some information about the state of turbulence along the link. Puryear and Chan considered the performance of FSO links with a multi-aperture diversity transmitter in conjunction with a sparse-aperture receiver employing diversity coherent detection. Initial work [22] assumed that the transmitter received complete, instantaneous information about the channel state information of frozen turbulence. In an effort to relax these optimistic assumptions regarding the quality and relevance of available channel-state information in an FSO link and assess the performance of more realistic feedback system, Puryear et al. [23, 24] developed theoretical models for the time dynamics of the atmosphere in weak turbulence. Achievable classical communication capacities and bit-error rates (BERs) of an FSO link with channel-state feedback were analyzed as functions of the latency of the channel-state information and feedback, number of transmit and receive apertures, turbulence strength, and link length. It was found that an optimal BER could be achieved with low-rate feedback on the order of hundreds of bits per second, provided that the feedback latency was less than the coherence time of the atmosphere and that a very large number of transmitters and receivers comprised the diversity transmitter and receiver.

Up to this point, we have only discussed receiver architectures designed to boost
the data rates of FSO classical communication links. Quantum key distribution (QKD) protocols are a class of protocols that facilitate perfectly secure information exchange between two parties by allowing them to share a perfectly random one-time pad. The proof of security of QKD relies solely on the laws of physics, unlike the security proofs of classical cryptography algorithms, which rely on upper bounds on an eavesdropper’s computational power. Recently, disclosures of mass-surveillance programs [30], have highlighted the ease of tapping traffic from fiber-optic cables, thus boosting the interest in implementing secure optical communication over commercial networks. In fact, QKD protocols have been successfully implemented in fiber networks [31]. The interest in FSO QKD communication is a natural outgrowth of the need for perfectly-secure communication links that have minimal infrastructure requirements, high-directionality, and operate in an unregulated region of the electromagnetic spectrum. Shapiro analyzed the effects of turbulence on FSO links employing the canonical QKD protocol Bennett-Brassard 1984 (BB84) [32, 33]. He found that while the error probabilities of BB84 QKD were not greatly affected by scintillation, they did increase as the power transfer from transmitter to receiver decreased, thus motivating the use of adaptive optics. Erven et al. [34] implemented a free-space BB84 QKD link and found that incorporating adaptive optics at the receiver alone, even if non-ideal, greatly improved the accessible secret-key rates of the link.

1.3 Towards scintillation-free communication

The research in FSO communication links we have reviewed thus far leads us to the conclusion that transmitting limited channel state information between diversity receivers and transmitters employing adaptive optics improves the power transmissivity and thus the achievable communication rates. Is it possible to construct a system that minimizes losses due to scintillation for any turbulence strength and distribution? Due to the reciprocal nature of atmospheric turbulence, the answer is yes.

When research into the implementation and performance of free-space laser com-
munication links began, Shapiro [35, 36] addressed the issue of what spatial modulation of electromagnetic signals would yield optimal power transmission through atmospheric turbulence for all strengths of turbulence. After proving that the channel impulse response of a frozen atmospheric turbulence state was reciprocal [37], Shapiro showed that optimal power transfer could be achieved by applying adaptive optics at both transmitter and receiver in order to achieve the maximum possible energy transfer between transmitter and receiver in a process we will call “full-wave compensation with bidirectional adaptive optics (BDAO).”

Recent research by Shapiro, Puryear, and Parenti [38, 39] analyzed communication system designs by applying the principles of reciprocity. BDAO were used to overcome scintillation in far-field links, but these systems did not consider the exact full-wave algorithm mentioned above. Puryear et al. did, however, prove that taking advantage of reciprocity with bidirectional adaptive optics achieved the ergodic capacity of a far-field link in the presence of scintillation for any turbulence strength without requiring sophisticated, latency-inducing error-correcting codes with interleaving.

Given the preceding appraisal of FSO communication through turbulence, the goal of this doctoral work is to analyze the performance of FSO classical communication and quantum-key distribution links with ideal, full-wave BDAO systems as well as other, suboptimal BDAO systems that are constrained to phase-only operations or are noisy. Thus, we seek BDAO systems that will ensure that FSO links employing these architectures will be able to operate in a regime where scintillation loss is minimized, thus enabling high-rate optical classical communication and secure communication links, regardless of the strength of atmospheric turbulence along the propagation path.

The structure of this thesis will be as follows. In Chapter 2, we will derive theoretical bounds on the ultimate single-mode power transfer from transmitter to receiver of an FSO link achievable in turbulence and introduce the BDAO algorithm that will allow us to achieve this optimal power transfer. Due to the lack of higher-order turbulence statistics valid for all strengths of turbulence, we introduce results from an atmospheric turbulence simulation program known as the Parallel Optical Propaga-
tion Software (POPS) that will allow us to simulate power transfers in links without BDAO, with an ideal, noiseless version of BDAO, and with sub-optimal implementations of BDAO. In Chapter 3, we derive theoretical bounds on single-spatial mode FSO classical communication links operating in turbulence, and assess their performance when ideal and non-ideal versions of BDAO are implemented. In Chapter 4, we review the canonical quantum communication protocol known as decoy-state Bennett-Brassard 1984 quantum key distribution (ds-BB84 QKD), bound the ergodic secret key rate for an FSO ds-BB84 QKD link operating in turbulence, and assess how its secret key rate can be improved by implementing ideal and non-ideal versions of BDAO. In Chapter 5, we review a new protocol for secret key distribution known as floodlight QKD (FL-QKD), derive bounds on its ergodic secret-key rate for FSO operation, and assess how its FSO secret-key rate increases when BDAO is implemented. In Chapter 6, we extend our power transfer analysis to a multi-spatial mode link. Using the mutual coherence function of the atmospheric turbulence, we derive multi-spatial-mode power-transfer statistics, which are then used to derive bounds on multi-spatial-mode classical communication rates, ds-BB84 QKD secret-key, and FL-QKD secret-key rates. In Chapter 7, we present POPS-simulated power-transfer statistics for FSO links operating with BDAO algorithms that either introduce Gaussian noise into the power-transfer tracking system or function in the presence of time-evolving atmospheric turbulence. In Chapter 8, we will discuss candidate optical systems that could implement BDAO, summarize the contributions of this thesis to the field of FSO classical and quantum communication, and will suggest future avenues for continued work on characterizing and building BDAO FSO architectures.
Chapter 2

Single-Spatial-Mode Power Transfer through Atmospheric Turbulence

In Chapter 1, we noted that atmospheric turbulence degrades the achievable rates of FSO classical and quantum communication systems by decreasing the average power transfer, viz the fraction of power exiting the transmitter that is detected by the receiver, due to scintillation and other clear-weather turbulence-induced effects. In this chapter, we characterize the gap between the power transmissivities achieved by FSO links using standard methods to compensate for atmospheric turbulence and the power transmissivities achieved by FSO links employing both ideal and non-ideal versions of BDAO.

We begin by using the extended Huygens-Fresnel principle in combination with the technique of normal-mode decomposition to derive the explicit behavior of free-space channel transmissivities as functions of link parameters like the communication wavelength, path length, and transmitter and receiver aperture sizes. Noting that normal-mode decomposition guarantees that there is, in fact, an optimal power transfer for a given instantiation of clear-weather turbulence, we derive two lower bounds on the optimal power transmissivity applicable for all turbulence strengths corresponding to systems employing either no adaptive optics or receiver-only adap-
tive optics. Then, we will compare these bounds to the ultimate single-spatial mode power transmissivity of a vacuum propagation channel. Following these derivations, we will discuss and define the explicit operation of a link employing ideal BDAO that takes advantage of the reciprocity of clear-weather turbulence such that it achieves the optimal single-spatial mode power transmissivity. Noting the lack of statistics available for this ultimate power transmissivity, we will introduce simulation results from the turbulence simulation software POPS and discuss the boost in power transmissivity achievable by systems employing BDAO. Finally, we will introduce non-ideal variants of BDAO and assess what power transmissivity penalties, if any, are induced by the non-ideal BDAO architectures.

2.1 A mathematical model of the free-space optical propagation channel

To assess the impact of atmospheric turbulence on a free-space link, we begin by considering the propagation of linearly-polarized, quasimonochromatic light with center wavelength $\lambda$ from a $d_T \times d_T$ transmitter pupil $\mathcal{A}_T$ in the $z = 0$ plane to a $d_R \times d_R$ receiver pupil $\mathcal{A}_R$ in the $z = L$ plane, as shown in Fig. 2-1. We assume that the temporal behavior is just the line-of-sight propagation delay $L/c$ by exploiting the facts that turbulence-induced multipath spread is sub-ps and that Gbps communication can be accomplished with ns-duration pulses that are much shorter than the ~ms atmospheric coherence time.

From the extended Huygens-Fresnel principle [40] we have that the complex envelope, $E_L(\rho', t)$, in the receiver's entrance pupil is related to the complex envelope in the transmitter's exit pupil, $E_0(\rho, t)$, by the superposition integral$^1$.

$$E_L(\rho', t) = \int_{\mathcal{A}_T} d\rho E_0(\rho, t - L/c)h(\rho', \rho, t), \text{ for } \rho' \in \mathcal{A}_R, \quad (2.1)$$

$^1$No loss of generality is incurred by employing a scalar-wave theory because turbulence does not cause depolarization [14].
where \( h(p', p, t) \) is the atmospheric Green's function at time \( t \) and \( E_0(p, t) \) and \( E_L(p', t) \) have units of \( \sqrt{\text{W/m}^2} \). Furthermore, because the coherence time of the turbulence is on the order of milliseconds, we can safely limit our attention to a single atmospheric state and suppress the Green’s function’s time argument, resulting in a propagation kernel of the form \( h(p', p) \).

The usual formulation of the extended Huygens-Fresnel principle takes the Green’s function for a single atmospheric state to be

\[
h(p', p) = e^{-\frac{\alpha}{2} L} h^0_L(p' - p) \exp[\chi(p', p) + i\phi(p', p)].
\] (2.2)

\( e^{-\alpha L} \) represents the extinction, viz., the loss due to absorption and scattering, when the extinction loss is uniformly distributed along the path \( z = 0 \) to \( z = L \) with an extinction coefficient \( \alpha. \) \( h^0_L(p' - p) \) is the Fresnel diffraction (vacuum propagation) Green’s function

\[
h^0_L(p' - p) = \frac{\exp[ik(L + |p' - p|^2/2L)]}{i\lambda L},
\] (2.3)

where \( k = 2\pi/\lambda \) is the wave number at the operating wavelength. \( \chi(p', p) \) and \( \phi(p', p) \) are real-valued random processes that represent the random logamplitude and phase fluctuations imposed by atmospheric turbulence on the field received at \( p' \) in the \( z = L \) plane from a point source located at \( p \) in the \( z = 0 \) plane. Physically, \( \chi(p', p) \) gives rise to scintillation, while \( \phi(p', p) \) is responsible for the beam spread and angle-of-arrival spread produced by the turbulence. Thus, propagation through clear turbulent air from \( z = 0 \) to \( z = L \), or propagation in the absence of extinction, has the Green’s function

\[
h_L(p', p) = \frac{\exp[ik(L + |p' - p|^2/2L)]}{i\lambda L} \exp[\chi(p', p) + i\phi(p', p)],
\] (2.4)

\(^2\) A nonuniform extinction distribution is easily accommodated by simply replacing \( e^{-\alpha L/2} \) with \( e^\int_0^L dz \alpha(z)^2 / 2 \), where \( \alpha(z) \) is the z-dependent extinction coefficient along the path from the transmitter to receiver.
2.1.1 Normal-mode decomposition of the free-space propagation kernel

The normal-mode decomposition of $h(p', p)$ consists of: (1) a complete, orthonormal (CON) set of input transverse modes $\{ \Phi_m(p) : 1 \leq m < \infty, p \in A_T \}$; (2) a CON set of transverse output modes $\{ \phi_m(p') : 1 \leq m < \infty, p' \in A_R \}$; and (3) a set of power-transfer eigenvalues $\{ \eta_m : 1 \leq m < \infty \}$, such that

$$\int_{A_T} dp \, h(p', p) \Phi_m(p) = \sqrt{\eta_m} \, \phi_m(p'),$$

for $p' \in A_R$ and $1 \leq m < \infty$. \hspace{1cm} (2.5)

Physically, Eq. (2.5) states that transmission of $\Phi_m(p)$ from $A_T$ results in reception of $\sqrt{\eta_m} \, \phi_m(p')$ in $A_R$. Because the input and output modes are normalized to have unit power when integrated over the transmitter and receiver apertures, respectively, it follows that $\eta_m$ is the fractional power-transfer from $A_T$ to $A_R$ that is achieved when $\Phi_m(p)$ is transmitted. Without loss of generality we will assume that the modes are ordered so that the modal transmissivities are nonincreasing, i.e., $e^{-\alpha L} \geq \eta_1 \geq \eta_2 \geq \cdots \eta_m \geq \cdots \geq 0$, where the upper limit follows from the passive nature of propagation through either vacuum or atmospheric turbulence and effect of extinction loss along the link. For the clear-weather turbulence kernel (2.4), this upper bound would be 1.

In the simplest scenario of an FSO link encoding information along a single spatial mode and assuming $\eta_1 > \eta_2$, the system can attain the optimal channel transmissivity $\eta_1$ if and only if the input eigenmode mode $\Phi_1(p)$ is generated by the transmitter at $A_T$ and the corresponding $\phi_1(p')$ received at $A_R$ is coupled with unity efficiency into the
receiver’s detector. If there are $M$ spatial mode input-output pairs $\{\Phi_m(\rho), \phi_m(\rho') : 1 \leq m \leq M\}$ with $\{\eta_1 = \eta_m : 1 \leq m \leq M\}$, then the transmitter must track the $M$ $\Phi_m(\rho)$ modes and encode its transmissions in the spatial mode basis spanned by the $\{\Phi_m(\rho) : 1 \leq m \leq M\}$ while the receiver must decompose the received modes over the spatial basis spanned by the $\{\phi_m(\rho') : 1 \leq m \leq M\}$ at the receiver aperture in order to achieve the maximum power transfer along the free-space optical link.

When $h(\rho', \rho)$ is known, the input modes, output modes, and eigenvalues can be found by first solving the Fredholm equation \[41, 42\]

$$\int_{A_T} d\rho_2 K(\rho_1, \rho_2) \Phi_m(\rho_2) = \eta_m \Phi_m(\rho_1), \text{ for } \rho_1 \in A_T,$$  \hspace{1cm} (2.6)

where

$$K(\rho_1, \rho_2) = \int_{A_R} d\rho' h^*(\rho', \rho_1) h(\rho', \rho_2),$$  \hspace{1cm} (2.7)

to obtain the input modes and the eigenvalues, and then using Eq. (2.5) to get the output modes.

For vacuum propagation, the normal-mode decomposition for the square-pupil geometries is known exactly—the input modes $\{\Phi_m(\rho)\}$ and output modes $\{\phi_m(\rho)\}$ are prolate spheroidal wavefunctions. Expressions for their eigenvalues $\{\eta_m\}$ are known as well \[43, 44\], although they are quite complicated. Closed-form asymptotic expressions in terms of the Fig. 2-1 geometry’s Fresnel-number product $D_f = \left(\frac{d_T d_R}{\lambda L}\right)^2$ are available for the largest eigenvalue $\eta_1^{\text{vac}}$.

$$\eta_1^{\text{vac}}(D_f) \simeq \left\{ \begin{array}{ll} D_f \left(1 - \frac{\pi^2 D_L}{36}\right)^2 \frac{\pi D_f^{1/2}}{2} \ll 1 & \\
\left(1 - \pi \sqrt{8} D_f^{1/4} e^{-\sqrt{D_f}} \left(1 - \frac{3}{16\pi \sqrt{D_f}}\right)\right)^2 \frac{\pi D_f^{1/2}}{2} \gg 1. & \end{array} \right.$$  \hspace{1cm} (2.8)

It is known that regardless of the aperture geometry, the sum of the vacuum-propagation eigenvalues $\sum_{m=1}^{\infty} \eta_m$ is equal to the link’s Fresnel-number product viz., $D_f = \frac{A_T A_R}{(\lambda L)^2}$, where $A_T$ and $A_R$ are the areas of $A_T$ and $A_R$. It is also known that the value of $D_f$ delineates two power transfer regimes for vacuum-propagation. In the far-field regime $D_f \ll 1$, there is only one spatial mode per polarization that transfers appreciable
power from transmitter to receiver and thus $\eta_1 = D_f$. Conversely, in the near-field regime with $D_f \gg 1$, there are approximately $D_f$ orthonormal spatial modes per polarization in the transmitter pupil that couple nearly all of their power into the receiver pupil.

For propagation through turbulence, however, the $\{\Phi_m(\rho)\}$, $\{\phi_m(\rho)\}$, and $\{\eta_m\}$ are, in general, random. Nevertheless, these random eigenvalues satisfy

$$\sum_{m=1}^{\infty} \eta_m = \int_{A_T}^{} d\rho' \int_{A_T}^{} d\rho |h(\rho', \rho)|^2.$$  \hspace{1cm} (2.9)

Shapiro proved [45] that the ensemble average of (2.9) for the extinction-loss-neglecting Green's function $h_L(\rho', \rho)$ equals the vacuum-propagation $D_f$ and that the same $D_f$-parameterized results for the power transfers derived for vacuum propagation hold for propagation through clear-weather turbulence, i.e. $D_f \ll 1$ and $D_f \gg 1$ identify far-field and near-field power-transfer regimes for the turbulent channel. When extinction loss is incorporated, the $D_f$-parameterized power transfer results still hold and are simply scaled by the extinction loss $e^{-\alpha L}$. With this general knowledge of the way that an optical communication link’s geometry affects single-spatial-mode channel transmissivity, we now turn our attention to the statistics of the stochastic turbulence kernel.

2.1.2 Mutual coherence function of the free-space propagation Green’s function

The principal Green’s function turbulence statistic that has been proven to be valid well into the saturation regime of turbulence [40, 46] (in other words, the region of strong turbulence) is the mutual coherence function, which satisfies

$$\langle h^*(\rho_1, \rho_1) h(\rho_2, \rho_2) \rangle = e^{-\alpha L} h^*_L(\rho_1, \rho_1) h_L(\rho_2, \rho_2) \times \exp[-D(\rho_2 - \rho_1, \rho_2 - \rho_1)/2],$$  \hspace{1cm} (2.10)
where

\[ D(\Delta \rho', \Delta \rho) = 2.91k^2 \int_0^L dz \frac{C_n^2(z)}{\frac{\Delta \rho'}{2}} \left| \Delta \rho' z/L + \Delta \rho (1 - z/L) \right|^{5/3}, \quad (2.11) \]

is the two-source, spherical-wave, wave structure function for Kolmogorov-spectrum turbulence with inner scale \( l_0 = 0 \), outer scale \( L_0 = \infty \), and \( C_n^2(z) \) being the turbulence strength profile along the path from the transmitter \((z = 0)\) to the receiver \((z = L)\). The initial derivation of this mutual coherence function employed the Rytov approximation, so its validity was thought to be limited to the weak-perturbation regime before the onset of saturated scintillation. Subsequent work—employing the small-angle approximation to the transport equation or the local method of smooth perturbations applied to the parabolic equation—has shown that (2.10) and (2.11) are valid in the saturation regime as well.

### 2.2 Channel transmissivity bounds in single-spatial mode operation

We present results for the average of single-mode power transmissivities for two different free-space optical communication links, one without and one with adaptive optics. For all following derivations, we assume that the transmitter communicates by imposing temporal modulation on a fixed spatial-mode pattern. We will also show that these results are lower bounds on the average of the maximum single-mode spatial transmissivity \( \langle \eta \rangle \), and will also provide a simple upper bound on \( \langle \eta \rangle \).

For our first lower bound, we will assume that the transmitter encodes information on a fixed, unity-power spatial-mode pattern \( U_0(\rho) \). The resulting spatial pattern at \( \mathcal{A}_R \) is then

\[ U_L(\rho') = \int_{\mathcal{A}_R} d\rho \ h(\rho', \rho) U_0(\rho) \quad (2.12) \]

We assume coherent detection and that adaptive optics are not employed at the receiver. Thus, the local oscillator of a coherent receiver will have a fixed, unity-power
spatial pattern $U_0(\rho')$. As a result, the coherent receiver will, in general, suffer an additional spatial-coupling loss on top of the $A_T$-to-$A_R$ attenuation. The free-space optical channel transmissivity of a coherent receiver with no adaptive optics $\eta_{\text{noAO}}$ is [1]

$$\eta_{\text{noAO}} = \left| \int_{A_R} d\rho' U^*_{0}(\rho')U_L(\rho') \right|^2. \quad (2.13)$$

Because $U_0(\rho)$ and $U_0(\rho')$ may not be equal to $\Phi_1(\rho)$ and $\phi_1(\rho')$, respectively, $\eta_{\text{noAO}}$ is a lower bound on $\eta_1$, i.e. $\eta_{\text{noAO}} \leq \eta_1$. In the case of a receiver that couples the received $U_L(\rho')$ from the transmitter to a single-mode fiber with transmission mode $U_0(\rho')$, the expression for the power-in-fiber is also given by $\eta_{\text{noAO}}$.

Averaging $\eta_{\text{noAO}}$ over all turbulence states yields

$$\langle \eta_{\text{noAO}} \rangle = \left\langle \left| \int_{A_R} d\rho' U^*_{0}(\rho')U_L(\rho') \right|^2 \right\rangle$$

$$= \int_{A_R} d\rho_1 U^*_{0}(\rho_1) \int_{A_R} d\rho_2 U_0(\rho_2) \int_{A_T} d\rho_2 U^*_0(\rho_2) \int_{A_T} d\rho_1 U_0(\rho_1)$$

$$\times \langle h^*(\rho_2', \rho_2)h(\rho_1', \rho_1) \rangle. \quad (2.14)$$

For ease of computation, let us take the transmitted spatial pattern to be a uniform-intensity focused beam

$$U_0(\rho) = \frac{e^{-\frac{4\pi\rho^2}{d_T^2}}}{d_T}, \quad \rho \in A_T. \quad (2.15)$$

Additionally, we take the local oscillator's spatial pattern to be the Gaussian with $e^{-1/2}$ intensity radius $\sigma = d_R/2$ that is normalized to have unit power over the receiver aperture $A_R$,

$$U_0(\rho') = \frac{e^{\left(i\frac{\pi}{4} - \frac{1}{2}\frac{i\rho^2}{d_R^2}\right)}}{d_R \sqrt{\frac{\pi}{2}} \text{erf} \left( \frac{1}{\sqrt{2}} \right)} \rho \in A_R. \quad (2.16)$$

where $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x dt e^{-t^2}$. 

42
Appendix A proves that turbulence power-transfer integrals of a specific form are parameterized solely by the turbulence strength in the form of the Rytov logamplitude variance \( \sigma_x^2 = 0.56k^{7/6} \int_0^L dz C_n^2(z)(\frac{z}{L})^{\frac{5}{6}}(L-z)^{\frac{1}{6}} \), the Fresnel number product \( D_f \), and the ratio between the lengths of the sides of the transmitter and receiver apertures \( R = d_T/d_R \). Since (2.14) is of this form, the preceding parameterization holds. Throughout the rest of this thesis, we assume a constant turbulence strength \( C_n^2(z) = C_n^2 \) along the path and make the square-law approximation for \( D(\Delta \rho', \Delta \rho) \), i.e.,

\[
D(\Delta \rho', \Delta \rho) = \frac{|\Delta \rho'|^2 + \Delta \rho' \cdot \Delta \rho + |\Delta \rho|^2}{\rho_0^2},
\]

where

\[
\rho_0 = (1.09k^2C_n^2L)^{-3/5} = (85.3\sigma_x^{12/5}\lambda L)^{-1/2}
\]

is the atmosphere’s uniform-\( C_n^2 \) spherical-wave coherence length, and

\[
\sigma_x^2 = 0.124k^{7/6}C_n^2L^{11/6}
\]

is the uniform-\( C_n^2 \) Rytov-theory logamplitude variance. The square-law approximation reduces the computational burden of evaluating \( \langle \eta_{\text{noAO}} \rangle \), allowing us to arrive at the following lower bound for \( \langle \eta \rangle \):

\[
\langle \eta \rangle \geq \langle \eta_{\text{noAO}} \rangle = \frac{e^{-\alpha L D_f}}{2\sqrt{\pi}} \left( \int_{-1/2}^{1/2} \frac{dx_2}{\sqrt{2}} \int_{-1/2}^{1/2} \frac{dx_1}{\sqrt{2}} e^{-(x_1^2+x_2^2)} \right)
\times \int_{-1/2}^{1/2} \frac{dx_2}{\sqrt{2}} \int_{-1/2}^{1/2} \frac{dx_1}{\sqrt{2}} \cos \left( 2\pi \sqrt{D_f(x_1^2 x_1 - x_2^2 x_2)} \right)
\times e^{-42.85\sigma_x^{12/5}\sqrt{D_f}\left( \frac{(x_2^2-x_1^2)^2}{R^2} + (x_2-x_1)^2 + R(x_2-x_1)^2 \right)}
\]

(2.20)

For our second bound, we assume the receiver has adaptive optics capable of tracking and measuring the spatial pattern \( U_L(\rho') \) at \( \mathcal{A}_R \) and setting \( U_{\text{io}}(\rho') \propto U_L(\rho') \), thus eliminating the spatial-mode coupling loss at the receiver. The free-space optical channel transmissivity \( \eta_{\text{recAO}} \) of a coherent receiver with this adaptive optics capability
\[ \eta_{\text{recAO}} = \frac{\int_{A_R} d\rho' |U_L(\rho')|^2}{\int_{A_T} d\rho_1 \int_{A_T} d\rho_2 U_0(\rho_1)U_0^*(\rho_2) h(\rho', \rho_1)h^*(\rho', \rho_2)}. \] (2.21)

Equation (2.21) is also equal to the power-in-aperture at the receiver plane. We know that \( \eta_{\text{recAO}} \) is larger than \( \eta_{\text{noAO}} \) because the former suffers no spatial-mode coupling loss while the latter, in general, does. Because \( U_0(\rho) \) may not be equal to \( \Phi_1(\rho) \), \( \eta_{\text{recAO}} \) is a lower bound on \( \eta_1 \). Hence we have \( \eta_{\text{noAO}} \leq \eta_{\text{recAO}} \leq \eta_1 \).

Taking the average of \( \eta_{\text{recAO}} \) over all possible instances of atmospheric turbulence, assuming that \( C_n^2 \) is constant along the path, and making the square-law approximation for \( D(\Delta \rho', \Delta \rho) \), we arrive at

\[ \langle \eta_{\text{recAO}} \rangle = \int_{A_R} d\rho' \int_{A_T} d\rho_1 \int_{A_T} d\rho_2 U_0(\rho_1)U_0^*(\rho_2) \langle h(\rho', \rho_1)h^*(\rho', \rho_2) \rangle \]
\[ = e^{-\alpha L} D_f \left( \int_{-1/2}^{1/2} dx_1 \int_{-1/2}^{1/2} dx_2 \text{sinc} \left( \pi \sqrt{D_f} (x_2 - x_1) \right) \right) \]
\[ = e^{-42.65 \sigma_1^{12/5} \sqrt{D_f} R(x_2-x_1)^2}. \] (2.22)

We now have two lower bounds on the average maximum channel transmissivity \( \langle \eta_1 \rangle \) for the free-space propagation geometry shown in Fig. 2-1. We also state the following upper bound on \( \eta_1 \),

\[ \langle \eta_1 \rangle \leq \langle \eta_1 \rangle^{\text{UB}} = e^{-\alpha L} \min(D_f, 1), \] (2.23)

which follows from \( \sum_{m=1}^\infty \langle \eta_m \rangle = D_f \), the passive nature of atmospheric turbulence, and the link’s extinction loss. Our conjecture is that a full-wave adaptive optics system at both the transmitter and receiver capable of tracking, generating, and receiving the \( \Phi_1(\rho) \) and \( \phi_1(\rho') \) would achieve an \( \langle \eta_1 \rangle \) significantly greater than \( \langle \eta_{\text{recAO}} \rangle \), if not \( \langle \eta_1 \rangle \simeq e^{-\alpha L} \eta_1^{\text{vac}} \), for all link geometries and for all strengths of turbulence. Furthermore, in the near-field power-transfer regime, \( \langle \eta_1 \rangle \simeq e^{-\alpha L} \) would imply that the
link was essentially scintillation-free. To test this hypothesis, we introduce a system that tracks, transmits, and receives the modes $\Phi_1(\rho)$ and $\phi_1(\rho')$ and achieves the optimal $\eta_1$ power transfer between the transmitter and receiver apertures of the FSO link.

### 2.3 Power transfers of FSO links operating with bidirectional adaptive optics (BDAO)

Up to this point, we have derived lower bounds on power transmissivities over the link for two scenarios. In the first scenario, neither the transmitter nor the receiver have knowledge of the turbulence kernel, and neither apply adaptive optics. In the second scenario, the receiver has full-wave adaptive optics, which it uses to minimize any spatial coupling loss as the received mode is either detected by a coherent system or coupled into fiber. In order for FSO transmitter and receiver terminals to establish a link with instantaneous, optimal power transfer $\eta_1$, the terminals must perfectly transmit $\Phi_1(\rho)$ at the $z=0$ aperture and detect $\phi_1(\rho')$ at the $z=L$ aperture. We will discuss the main property of the Green’s function of the atmosphere, reciprocity, that enables this spatial mode tracking as well as the adaptive optics required at both the transmitter and receiver to establish the optimal power transfer $\eta_1$ across the single-spatial mode FSO link.

#### 2.3.1 Full-wave bidirectional compensation

We begin with the normal-mode decomposition of the atmospheric Green’s function for $z=0$ to $z=L$ propagation in frozen turbulence. It can be written in terms of the CON set of input modes $\{\Phi_m(\rho) : 1 \leq m < \infty, \rho \in \mathcal{A}_T\}$, the CON set of output modes $\{\phi_m(\rho') : 1 \leq m < \infty, \rho' \in \mathcal{A}_R\}$, and their associated power transfers $\{\eta_m : 1 \leq m < \infty\}$, as follows

$$h_{atm}^{0\rightarrow L}(\rho', \rho) = \sum_{m=1}^{\infty} \sqrt{\eta_m} \phi_m(\rho') \Phi_m^*(\rho),$$  \hspace{1cm} (2.24)

45
where we have added the $0 \to L$ to emphasize the propagation direction. The point-reciprocity of the atmosphere has long been known [11, 37], which means that the Green’s function that maps a point source at $\rho'$ the $z = L$ plane to a complex amplitude at $\rho$ the $z = 0$ plane is

$$h_{atm}^{0 \to L}(\rho, \rho') = h_{atm}^{0 \to L}(\rho', \rho)$$

$$= \sum_{m=1}^{\infty} \sqrt{\eta_m} \phi_m(\rho') \Phi_m^*(\rho).$$

(2.25)

(2.26)

Thus, the conjugates of the input and output spatial eigenfunctions of the forward-propagation Green’s functions are, respectively, the output and input spatial eigenfunctions of the reverse-propagation Green’s function, and the associated modal power transfers are the same for both propagation directions. As a result, if an FSO link has established a power transfer $\eta_1$ in the $0 \to L$ direction by transmitting $\Phi_1(\rho)$ at $z = 0$ and receiving $\phi_1(\rho')$ at $z = L$, it can also establish a link with optimal power transfer $\eta_1$ in the $L \to 0$ direction by transmitting $\phi_1^*(\rho')$ at $z = L$ and receiving $\Phi_1^*(\rho)$ at $z = 0$. This tracking requires full-wave bidirectional adaptive optics, that is, adaptive optics capable of measuring the magnitude and phase of an incoming wavefront at the transmitter and receiver.

We suggest the following algorithm for bidirectional, full-wave adaptive optics compensation for optical propagation through turbulence using a single spatial mode when a BDAO tracking system operates in a frozen atmosphere and makes noiseless, full-wave measurements on electromagnetic fields. The full-wave assumption will be relaxed in Section 2.3.2, while BDAO incorporating measurement noise and atmospheric evolution in time will be discussed in Chapter 7. A cartoon of an FSO system implementing full-wave, bidirectional compensation for turbulence is shown in Fig. 2-2. Suppose a system has access to an ideal conjugate transmitter that perfectly measures an incoming wavefront and generates its conjugate. By applying conjugate transmission at both of its terminals, it can implement the following protocol to asymptotically obtain the spatial modes that will yield an optimal power transfer $\eta_1$ between the $z = 0$ and $z = L$ apertures.
1. A beacon signal with normalized transverse spatial pattern \( v_0(\rho) \) is sent from the transmitter to the receiver through the atmosphere, where

\[
v_0(\rho) = \sum_{m=1}^{\infty} c_m \Phi_m(\rho) \quad \text{with} \quad \sum_{m=1}^{\infty} |c_m|^2 = 1
\]

and \( c_1 \neq 0 \) assumed.

2. Transmission of the beacon signal results in reception of the unnormalized spatial pattern

\[
\tilde{v}_0(\rho') = \int_{A_T} h^{0\rightarrow L}_{\text{atm}}(\rho', \rho) v_0(\rho) = \sum_{m=1}^{\infty} c_m \sqrt{\eta_m} \Phi_m(\rho')
\]

at the receiver aperture \( A_R \).

We set \( v_0(\rho) = U_0(\rho) \) as defined in (2.15) so that the spatial pattern at the receiver aperture is \( \tilde{v}_0(\rho') = U_L(\rho') \) from (2.12). Thus, the BDAO power transfer from the transmitter to a coherent receiver with no adaptive optics at this step of the algorithm is \( \tilde{\eta}_{\text{noAO}} = \eta_{\text{noAO}} \) from (2.13). For a coherent receiver with full-wave adaptive optics, the power transfer is \( \tilde{\eta}_{\text{recAO}} = \eta_{\text{recAO}} \) as defined in (2.21).

3. The receiver perfectly measures the received wave and generates a conjugated...
version with a spatial pattern

\[ u_0(\rho') = \frac{\sum_{m=1}^{\infty} c_m^* \sqrt{\eta_m} \phi_m^*(\rho')} {\sqrt{\sum_{m=1}^{\infty} \eta_m |c_m|^2}}. \] (2.29)

normalized to have unit power over the aperture.

4. The wave received at the transmitter aperture \( A_T \) at \( z = 0 \) has unnormalized spatial pattern

\[ \tilde{u}_0(\rho) = \frac{\sum_{m=1}^{\infty} c_m^* \eta_m \Phi_m(\rho)} {\sqrt{\sum_{m=1}^{\infty} \eta_m^2 |c_m|^2}}. \] (2.30)

5. The transmitter perfectly measures the received wave and generates a conjugated version with normalized spatial pattern. It begins the next iteration by transmitting the normalized spatial pattern

\[ v_1(\rho) = \frac{\sum_{m=1}^{\infty} c_m \eta_m \Phi_m(\rho)} {\sqrt{\sum_{m=1}^{\infty} \eta_m^2 |c_m|^2}}. \] (2.31)

In the \( k^{th} \) iteration of this algorithm, the beacon sent from the transmitter at the \( z = 0 \) plane may be written as

\[ v_k(\rho) = \frac{c_1 \eta_1^k}{\sqrt{\sum_{m=1}^{\infty} \eta_m^{2k} |c_m|^2}} \left( \Phi_1(\rho) + \sum_{m=2}^{\infty} \left( \frac{c_m}{c_1} \right) \left( \frac{\eta_m}{\eta_1} \right)^k \Phi_m(\rho) \right). \] (2.32)

while the beacon transmitted in the backward direction from the \( z = L \) plane is

\[ u_k(\rho') = \frac{c_1 \eta_1^{k+\frac{1}{2}}}{\sqrt{\sum_{m=1}^{\infty} \eta_m^{2k+1} |c_m|^2}} \left( \phi_1^*(\rho') + \sum_{m=2}^{\infty} \left( \frac{c_m}{c_1} \right)^* \left( \frac{\eta_m}{\eta_1} \right)^{k+\frac{1}{2}} \phi_m^*(\rho') \right). \] (2.33)

The power transfer achieved when transmitting \( v_k(\rho) \) on the \( k^{th} \) pass of the full-wave BDAO algorithm, \( \eta_1^{\text{full}}(k) \), is

\[ \eta_1^{\text{full}}(k) = \left| \int_{A_T} d\rho \, h(\rho', \rho) \, v_k(\rho) \right|^2 \]
The steady state power transfer of the full-wave BDAO algorithm, \( \eta_1^{\text{full}}(k \to \infty) \), will be denoted as \( \eta_1^{\text{full}} \).

This algorithm is a physical realization of the common numerical power method [47] used to find the dominant eigenvalue and corresponding eigenfunction of a matrix applied, in this case, to the Green's function of atmospheric turbulence. However, (2.32) is instructive in that it yields the rate of convergence, \( \eta_2/\eta_1 \), for the algorithm and emphasizes that the initial \( z = 0 \) beacon \( v_0(\rho) \) must have a nonzero component in the direction of \( \Phi_1(\rho) \) for the algorithm to converge to the highest-transmissivity spatial mode.

As discussed in Section 2.1.1, in the extreme far-field regime \( D_f \ll 1 \) there is only a single mode with non-negligible power transmissivity \( e^{-\alpha L} D_f \), while in extreme near-field regime \( D_f \gg 1 \) there are approximately \( D_f \) modes with power transmissivities near \( e^{-\alpha L} \) while all other spatial modes have essentially no power transmissivity. Thus, in either of these regimes, it is clear that a single iteration of the ideal full-wave adaptive optics algorithm will be sufficient to arrive at the optimal spatial modes for both transmitter and receiver\(^3\).

The statistics of \( \eta_1 \) for the near-unity Fresnel-number product, which we define as \( D_f \approx 1 \), are not easily obtained from the Green’s function’s mutual coherence function, \( i.e. \) the bounds we reported earlier are unlikely to be tight in that Fresnel-number product-regime [45]. Additionally, regardless of the link’s \( D_f \), second-moment statistics of the \( \{ \eta_m \} \) are required to bound the power transmissivities of the one-pass beacon signals \( v_2(\rho) \) and \( u_2(\rho') \) over multiple instances of turbulence. These power transmissivities, however, require information about the fourth-order moments of \( h_{\text{atm}}^{\alpha L}(\rho, \rho') \), which are quite difficult to obtain outside of the weak-perturbation propagation regime. As a result, we must employ computer simulation to fill this

\[ \left\{ \begin{array}{ll} \hat{\eta}_{\text{recAO}} & \text{for } k = 0, \\ \eta_1 \left( \frac{1 + \sum_{m=2}^{\infty} \frac{|c_m|^2}{|c_1|^2} \left( \frac{\eta_m}{\eta_1} \right)^{2k+1}}{1 + \sum_{m=2}^{\infty} \frac{|c_m|^2}{|c_1|^2} \left( \frac{\eta_m}{\eta_1} \right)^{2k}} \right) & \text{for } k \geq 1 \end{array} \right. \] (2.34)
gap in our knowledge of the $D_f \approx 1$ propagation statistics. Before introducing the simulation results, however, we will introduce a non-ideal version of BDAO that does not make full-wave measurements at its conjugate transmitter terminals.

### 2.3.2 Phase-only bidirectional compensation

Noting that an optical component capable of measuring the magnitude and phase-front of an incoming electromagnetic wave and generating the conjugate of that wave is quite difficult to implement, we introduce a modification of the full-wave BDAO algorithm as shown in Fig. 2-3. In this modification, the conjugate transmitter, rather than making a full magnitude and phase measurement, simply measures the phase-front of the incoming wave, generates the conjugate of the phase screen, and applies this new phase screen to the focused, flat-intensity beam $U_0(\rho)$ given by (2.15) at the beginning of each iteration.

This phase-only BDAO algorithm can be easily implemented via a Shack-Hartmann wavefront sensor performing the phase-only measurement, and a deformable mirror generating the conjugate phase-screen and applying it to the focused output of a laser.

$$h_{\text{atm}}^{0-L}(\rho, \rho') = \sum_{m=1}^{\infty} \sqrt{\eta_m} \phi^*(m) \phi(m)(\rho)$$

$$h_{\text{atm}}^{0-L}(\rho, \rho') = \sum_{m=1}^{\infty} \sqrt{\eta_m} \Phi^*(m) \phi(m)(\rho')$$

Figure 2-3: A model for phase-only bidirectional full-wave compensation through atmospheric turbulence on its $k^{th}$ iteration.

The power transfer on the $k^{th}$ pass of the phase-only BDAO algorithm achieved when transmitting $v_k(\rho)$ will be denoted as $\eta_{\text{phase}}(k)$, where $\eta_{\text{phase}}(0) = \eta_{\text{recAO}}$ since $U_0(\rho)$ will be used as the initial beacon signal. Its steady state power transfer (if it
converges), \( \hat{\eta}_1^{\text{full}}(k \to \infty) \), will be denoted as \( \hat{\eta}_1^{\text{phase}} \). Due to the lack of closed-form power transfer statistics and spatial mode statistics of the CON input and output spatial mode sets, we cannot derive the statistics of the accessible single-spatial-mode power transfer \( \hat{\eta}_1^{\text{phase}} \) of the phase-only BDAO link. Thus, we must turn to the computer simulation of turbulence along an optical path to assess whether or not phase-only BDAO compensation will afford an FSO link the same increases in power transfer as full-wave BDAO compensation does.

2.3.3 Simulating turbulence with Parallel Optical Propagation Software (POPS)

A full-wave optical propagation software application known as Parallel Optical Propagation Software (POPS) enables us to simulate the full probability distribution of \( \eta_1 \) for a terrestrial link with an optical signal propagating through turbulence. POPS has a software application programming interface (API) composed of various software blocks modeling both perfect and imperfect versions of common optical components found in free-space optical communication systems, like deformable mirrors, phase-conjugators, and single-mode fibers. As input, POPS requires that a path from \( z = 0 \) to \( z = L \) be defined and that objects like transmitter and receiver apertures, wave-conjugators, amplifiers, and any other required optical components be placed along the path. Next, POPS populates the free-space portion of the path with phase screens randomly generated from stochastic processes parametrized by values like the \( C_n^2 \) strength, wind speed, and desired energy spectrum of the turbulence. Then, POPS propagates an input field defined by the user from the start of the path to the end of the path by applying the appropriate two-dimensional Fourier transforms or magnitude and phase operations, depending on whether the object it encounters is vacuum, a phase-screen, or some user-defined optical object. Statistics of propagation through turbulence can be obtained by repeatedly running POPS with different instantiations of turbulence-simulating phase screens.

Figure 2-4 is an example of the full-wave field propagation POPS performs when
simulating turbulence as a series of phase screens placed along an otherwise vacuum-propagation path. POPS does not simulate extinction loss; the extinction coefficient must be simulated from a software like MODTRAN [7] and used to scale the clear-weather power transfers that POPS simulates in order to accurately assess the FSO channel transmissivity of a link with extinction loss.

Figure 2-4: An example of full-wave field propagation performed by POPS from transmitter aperture \( A_T \) at \( z = 0 \) to receiver aperture \( A_R \) at \( z = L \) with the assumption of moderate turbulence and wind along the path. In this scenario, POPS simulates the desired turbulence by placing randomly generated phase screens at \( z = L_1 \) and \( z = L_2 \) (whose phases are plotted in pseudocolor in the landscape-orientation rectangles). The intensity of the propagated EM wave in the transverse plane after each aperture or phase screen object is plotted in the blue squares.

At this point, we note that POPS is a simulation tool and is therefore only as good as the model on which its operation is based. Details of the modifications made to POPS to ensure the consistency of its results with weak-propagation turbulence statistics, the power transfer bounds derived in Section 2.2, and additional verification and validation procedures are discussed in Appendix B.

We seek to compare the ultimate single-spatial mode power transfer \( \tilde{\eta}_1^{\text{full}} \) \( (\tilde{\eta}_1^{\text{phase}}) \) achievable when employing noiseless, bidirectional full-wave (phase-only) adaptive optics system to the power transfer bounds \( \langle \eta_{\text{recAO}} \rangle \) for the receiver-only adaptive optics case (2.22) and \( \langle \eta_{\text{noAO}} \rangle \) for the no-adaptive optics case (2.20). The bounds, at least, are parametrized solely by the Rytov log-amplitude variance \( \sigma_x^2 \), the Fresnel-number product \( D_f \), and the ratio between the lengths of the sides of the transmitter and receiver apertures \( R = d_T/d_R \).
We select a set of notional FSO link parameters with an operating wavelength \( \lambda = 1550 \text{ nm} \) and a path length of \( L = 10 \text{ km} \). \( L = 10 \text{ km} \) is a fairly standard path length for a point-to-point terrestrial link that could span a city or underserved rural area, and \( \lambda = 1550 \text{ nm} \) is a standard telecommunication fiber wavelength that also has high good-weather transmissivity, despite the absorption and scattering losses that are inevitable in a free-space link. We also set \( R = \frac{d_T}{d_R} = 1 \), noting that the mutual coherence function suggests that the effects of turbulence will be the same at both the \( z = 0 \) and \( z = L \) apertures for \( R = 1 \). Using the square-pupil setup in Fig. 2-1, our \( z = 0 \) and \( z = L \) apertures are squares with sides of length \( d_T = d_R = d \), yielding a Fresnel number product \( D_f = d^4/(\lambda L)^2 \). In an effort to clarify the behaviors of \( \tilde{\eta}_1^{\text{full}} \) and \( \tilde{\varphi}_1^{\text{phase}} \) in near-unity Fresnel-number products, we will present power transfer results versus varying values of \( D_f \) and turbulence strength \( \sigma_x^2 \). Holding the operating wavelength \( \lambda \) and path length \( L \) constant while modifying the Fresnel number product \( D_f \) of the link is equivalent to choosing \( d = \sqrt{D_f^{1/2} \lambda L} \).

Holding the path length constant also means that the extinction loss of the link caused by absorption and scattering along the path will remain constant. In our case, we will assume that \( 10 \text{ km} \) link operates in fairly clear weather with good visibility along the link with an extinction length \( \alpha = 0.2 \text{ dB/km} \), and thus has an initial power transmissivity \( e^{-\alpha L} = 0.631 \).

To match the two-source spherical-wave structure function \( D(\Delta \rho', \Delta \rho) \) given in (2.11) that was used to derive \( \langle \eta_{\text{noAO}} \rangle \) and \( \langle \eta_{\text{recAO}} \rangle \), we simulated the POPS turbulence screens for a Kolmogorov-spectrum turbulence with inner scale \( l_0 = 0 \) and outer scale \( L_o = \infty \) with uniform turbulence \( C^2_\text{n} \) along the path\(^4\). Four turbulence strengths with constant \( C^2_\text{n} \) values are considered: \( 10^{-16} \text{ m}^{-2/3} \) (mild turbulence), \( 10^{-15} \text{ m}^{-2/3} \) (moderate turbulence), \( 10^{-14} \text{ m}^{-2/3} \) (strong turbulence), and \( 10^{-13} \text{ m}^{-2/3} \) (very strong turbulence). Table 2.1 lists the values for the spherical-wave coherence length \( \rho_0 \) from (2.18) and the weak-perturbation (Rytov-theory) spherical-wave log-amplitude variance \( \sigma_x^2 \) from (2.19).

\(^4\)As a result, our simulated values of \( \tilde{\eta}_{\text{noAO}}, \tilde{\eta}_{\text{recAO}}, \tilde{\eta}_1^{\text{full}}, \) and \( \tilde{\varphi}_1^{\text{phase}} \) will all follow the 5/3-law expression for \( D(\Delta \rho', \Delta \rho) \) given in (2.11) rather than the simplified square-law approximation given in (2.17).
The bulk of the body of work characterizing optimal power transfers and the corresponding enabling spatial modes for FSO links has been performed solely for far-field links, in which either the transmitter or receiver apertures lie within a single atmospheric coherence area of size $\rho_0^2$. A receiver lying within a single coherence area of the atmosphere will always observe a spatial mode with a nearly flat phasefront with minimal angle of arrival spread or beam spread, allowing simpler models of atmospheric turbulence to be applied. With these simpler statistical models for the effects of atmospheric turbulence, closed-form probability distributions are available for the power transfer as a function of turbulence strength and the geometry of the FSO link.

In this thesis, however, we are concerned with the power transfer behavior for varying strengths of turbulence of FSO links with near-unity or near-field Fresnel-number products where the transmitter and receiver apertures will span multiple atmospheric coherence areas. For our notional case, we consider a range of Fresnel-number products spanning $D_f = 10^{-2}$ to $D_f = 250$. Table 2.2 lists the aperture size $d$ for some selected values of $D_f$ at our chosen $\lambda$ and $L$, as well as the maximum turbulence strengths for which the transmit and receive apertures lie within an atmospheric coherence area. For very strong turbulence, $D_f \geq 10^{-2}$ results in links with $d^2 > \rho_0^2$, ensuring that there will be many coherence areas at the receiver aperture. Thus, beam wander, beam spread, and scintillation will severely affect the power transfer of a link with no BDAO for our selected range of $D_f$ values, ensuring that BDAO will be required to couple any appreciable amount of power into a detector. It is this stressful test that will allow us to assess at what turbulence strengths BDAO
has significant utility in far-field, near-unity, or near-field links.

For the rest of this thesis, we will present our results in terms of the Rytov-theory logamplitude variance $\sigma^2$, with $\sigma^2 > 1$ indicating operation in the saturation regime. This $\sigma^2$ does not represent the actual logamplitude variance that would be measured along the link; rather, it is just a simple dimensionless measure of the turbulence strength by which our power transfer bounds are parameterized. All values of the notional case are listed in Table 2.3.

<table>
<thead>
<tr>
<th>$D_f$</th>
<th>$d$ (cm)</th>
<th>$C_n^2$ (m$^{-2/3}$) for $\rho_0^2 = d^2$</th>
<th>$\sigma^2$ for $\rho_0^2 = d^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.01</td>
<td>3.9</td>
<td>$1.25 \times 10^{-15}$</td>
<td>1.14</td>
</tr>
<tr>
<td>1</td>
<td>12.4</td>
<td>$2.00 \times 10^{-16}$</td>
<td>0.17</td>
</tr>
<tr>
<td>10</td>
<td>22.1</td>
<td>$6.31 \times 10^{-17}$</td>
<td>0.02</td>
</tr>
<tr>
<td>100</td>
<td>39.4</td>
<td>$2.51 \times 10^{-17}$</td>
<td>0.004</td>
</tr>
<tr>
<td>250</td>
<td>50.0</td>
<td>$2.00 \times 10^{-17}$</td>
<td>0.002</td>
</tr>
</tbody>
</table>

Table 2.2: Square aperture side $d$ versus the Fresnel-number product $D_f$ for a 10-km-long path at 1.55 $\mu$m wavelength with identical square transmitter and receiver apertures of the same size. Turbulence strengths in units of both $C_n^2$ and $\sigma^2$ for which apertures of area $d^2$ would lie inside an atmospheric coherence area $\rho_0$ are also given.

<table>
<thead>
<tr>
<th>parameters</th>
<th>values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda$</td>
<td>1550 nm</td>
</tr>
<tr>
<td>$L$</td>
<td>10 km</td>
</tr>
<tr>
<td>$R = d_T/d_R$</td>
<td>1</td>
</tr>
<tr>
<td>$D_f$</td>
<td>$10^{-2}$ to 250</td>
</tr>
<tr>
<td>$d = d_T = d_R$</td>
<td>3.9 cm to 50 cm</td>
</tr>
<tr>
<td>$C_n^2$</td>
<td>$10^{-16}$ m$^{-2/3}$ to $10^{-13}$ m$^{-2/3}$</td>
</tr>
<tr>
<td>$\sigma^2$</td>
<td>0.0137 to 13.67</td>
</tr>
<tr>
<td>$\sigma^2_{\chi_{\alpha L}}$</td>
<td>0.631</td>
</tr>
</tbody>
</table>

Table 2.3: Parameter values for the notional case of link geometry and turbulence values selected for a use case in this thesis.
2.4 Full-wave and phase-only BDAO power transfer statistics

We have set up a notional case of an FSO link with fixed values of $\lambda$, $L$, and $R$ and have chosen ranges of values for turbulence strength $\sigma_x^2$ and $D_f$ so that this thesis will address the characterization of the power transfer behavior of FSO links with near-unity and near-field Fresnel number products. In this section, we present POPS-simulated results on the statistics of the $\eta_1^{\text{full}}(k)$ and $\eta_1^{\text{phase}}(k)$ values accessible after four passes through the atmosphere as well as comparisons between the square-law-derived power transfer bounds $\langle \eta_{\text{recAO}} \rangle$ and $\langle \eta_{\text{hoAO}} \rangle$ and the POPS-simulated ergodic power transfers $\langle \eta_{\text{recAO}} \rangle$ and $\langle \eta_{\text{recAO}} \rangle$ for the FSO link with parameters given in Table 2.3. We begin by considering the probability distributions and convergence behavior of the clear-weather turbulence, extinction-loss neglecting power transfers simulated by POPS.

2.4.1 Probability distributions and convergence behavior of the extinction-loss neglected BDAO power transfers

In this subsection, we will assume that $e^{-\alpha L} = 1$ in order to analyze the results of the raw, clear-weather turbulence POPS simulations of power transfers $\eta_1^{\text{full}}(k)$ and $\eta_1^{\text{phase}}(k)$. To give a sense of how the probability distributions of the extinction-loss neglected $\eta_1^{\text{full}}(k)$ and $\eta_1^{\text{phase}}(k)$ evolve for each iteration $k$ of either full-wave or phase-only BDAO, we present Fig. 2-5. In Fig. 2-5, we have plotted the histograms of $\eta_1^{\text{full}}(k)$ and $\eta_1^{\text{phase}}(k)$ that are derived from 10,000 POPS instantiations of full-wave and phase-only BDAO applied to an FSO link with near-unity Fresnel-number product $D_f = 4$ operating in mild, moderate, strong, or very strong turbulence. Each row of plots corresponds to BDAO operating in a specific turbulence strength given by $\sigma_x^2$, while each column of plots corresponds to a BDAO iteration value $k$ ranging from 0 to 4. For a given $k$ and $\sigma_x^2$, the histogram of the 10,000 $\eta_1^{\text{full}}(k)$ values is represented by with solid green bars, while the histogram of the 10,000 $\eta_1^{\text{phase}}(k)$
values is represented by unfilled green bars. In the first column of plots, $k = 0$ - thus, the power transfer for the $k = 0$ pass is simply $\tilde{\eta}_{\text{recAO}}$, and the histograms for full-wave and phase-only BDAO are the same. Finally, the best beta-distribution fits\(^5\) to the histogrammed $\hat{\eta}^\text{full}_1(k)$ and $\hat{\eta}^\text{phase}_1(k)$ are plotted as black curves, where the probability density function (PDF) of the beta distribution is

$$
\beta(\eta; a, b) = \begin{cases} 
\frac{1}{B(a, b)} \eta^{a-1} (1 - \eta)^{b-1} & \text{for } 0 \leq \eta \leq 1 \\
0 & \text{otherwise}
\end{cases}
$$

(2.35)

for $a, b > 0$, with $B(x, y)$ being the beta function.

Reading across a specific row in the matrix of plots in Fig. 2-5 is equivalent to observing the evolution of the probability distributions of $\tilde{\eta}^\text{full}_1(k)$ and $\tilde{\eta}^\text{phase}_1(k)$ through $k = 4$ BDAO iterations for a specific turbulence strength. For $D_f = 4$ and all selected strengths of turbulence, it appears that the distributions of $\tilde{\eta}^\text{full}_1(k)$ and $\tilde{\eta}^\text{phase}_1(k)$ converge by the third iteration of BDAO. The closed form equation of the full-wave BDAO power transfer $\tilde{\eta}^\text{full}_1(k)$ given in (2.34) made its convergence to $\tilde{\eta}^\text{full}_1 = \eta_1$ a forgone conclusion. However, given that we were unable to write a closed-form equation for the phase-only BDAO power transfer $\tilde{\eta}^\text{phase}_1(k)$, its convergence to some steady state $\tilde{\eta}^\text{phase}_1$ is a pleasant surprise. In Fig. 2-5, it is clear that for all strengths of turbulence, $\langle \tilde{\eta}^\text{full}_1(k) \rangle \geq \langle \tilde{\eta}^\text{phase}_1(k) \rangle$, although the variances of the $\tilde{\eta}^\text{phase}_1$ are lower than the variances of $\tilde{\eta}^\text{full}_1$ for moderate, strong, and very strong turbulence. In the following chapters of this thesis, we will use these distributions to assess how the use of phase-only BDAO vs. full-wave BDAO affects the performance of communication protocols discussed in the later chapters.

We now address whether or not the $\tilde{\eta}^\text{full}_1(k)$ and $\tilde{\eta}^\text{phase}_1(k)$ for all Fresnel-number products $D_f$ listed in our notional case in Table 2.3 converge within the $k = 4$ iterations of full-wave and phase-only BDAO simulated with POPS. Beta distributions were fit to each $\tilde{\eta}^\text{full}_1(k)$ and $\tilde{\eta}^\text{phase}_1(k)$ for the Fresnel-number products $D_f$ and the Rytov-theory logamplitude variances $\sigma^2_X$ listed in Table 2.3, resulting in proba-

\(^5\)The beta-distribution was chosen because its support is $[0, 1]$ and its parameters can be adjusted so that the distribution is skewed.
Figure 2-5: Histograms for $\tilde{n}_1^{\text{full}}(k)$ (plotted with filled green bars) and $\tilde{n}_1^{\text{phase}}(k)$ (plotted with open green bars) and their corresponding beta-distribution fits for $D_f = 4$ in mild, moderate, strong, and very strong turbulence for an FSO link with no extinction loss and parameters given in Table 2.3.
bility distributions \( \beta_{\eta_1}^{\text{null}}(k) (\eta; a(D_f, \sigma^2_X), b(D_f, \sigma^2_X)) \) and \( \beta_{\eta_1}^{\text{full}}(k) (\eta; a(D_f, \sigma^2_X), b(D_f, \sigma^2_X)) \) (which we abbreviate as \( \beta_{\eta_1}^{\text{null}}(k) \) and \( \beta_{\eta_1}^{\text{full}}(k) \)).

In order to check the convergence of the \( \beta_{\eta_1}^{\text{full}}(k) \) and \( \beta_{\eta_1}^{\text{phase}}(k) \) with increasing \( k \) for a given \( D_f \) and \( \sigma^2_X \), we use the Kullback-Liebler (KL) divergence test. The KL divergence \( D(p||q) \) is a measure of the difference between two probability distributions \( p \) and \( q \). For distributions \( p(x) \) and \( q(x) \) of a continuous random variable, it is defined as

\[
D(p||q) = \int_{-\infty}^{\infty} p(x) \log \left( \frac{p(x)}{q(x)} \right) \, dx. \tag{2.36}
\]

The KL divergence between two beta distributions with parameters \((a_1, b_1)\) and \((a_2, b_2)\), \( D(\beta(x; a_1, b_1)||\beta(x; a_2, b_2)) \), is

\[
D(\beta(x; a_1, b_1)||\beta(x; a_2, b_2)) = \ln \left( \frac{B(a_2, b_2)}{B(a_1, b_1)} \right) + \psi(a_1)(a_1 - a_2) + \psi(b_1)(b_1 - b_2). \tag{2.37}
\]

where \( \psi(x) \) is the digamma function [48]. Two beta distributions are considered to be close to one another if \( D(\beta(x; a_1, b_1)||\beta(x; a_2, b_2)) \leq 1 \).

\( D(p||q) \) is not a proper distance metric: it is neither symmetric (\( D(p||q) \neq D(q||p) \)) nor does it satisfy the triangle inequality. It does, however, provide a valid convergence test. If there is a sequence \( p_1, p_2, \ldots \) of distributions such that

\[
\lim_{k \to \infty} D(p_k||q) = 0 \tag{2.38}
\]

then it is said that \( p_k \xrightarrow{D} q \), or that the \( p_k \) converge to a steady state distribution \( q \) in divergence. In our case, we will assume that our steady state distribution \( q \) is \( \beta_{\eta_1}^{\text{null}}(4) \left( \beta_{\eta_1}^{\text{phase}}(4) \right) \) for full-wave BDAO (phase-only BDAO), and that our series of \( p_k \) distributions are the \( \beta_{\eta_1}^{\text{full}}(k) \left( \beta_{\eta_1}^{\text{phase}}(k) \right) \) for \( k = 0, 1, 2, 3 \).

In Fig. 2-6, the \( D\left( \beta_{\eta_1}^{\text{full}}(k)||\beta_{\eta_1}^{\text{null}}(4) \right) \) and \( D\left( \beta_{\eta_1}^{\text{phase}}(k)||\beta_{\eta_1}^{\text{phase}}(4) \right) \) vs. the Fresnel number product for moderate \( (\sigma^2_X = 0.137) \), strong \( (\sigma^2_X = 1.367) \), and very strong
Figure 2-6: Convergence behavior of the power transmissivity distributions $\tilde{\eta}_1^{\text{full}}(k)$ and $\tilde{\eta}_1^{\text{phase}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate ($\sigma_X^2 = 0.137$), strong ($\sigma_X^2 = 1.367$), and very strong turbulence ($\sigma_X^2 = 13.67$). KL divergences $D\left(\beta_{\tilde{\eta}_1^{\text{full}}} (k) \parallel \beta_{\tilde{\eta}_1^{\text{full}}} (4)\right)$ for full-wave BDAO and $D\left(\beta_{\tilde{\eta}_1^{\text{phase}}} (k) \parallel \beta_{\tilde{\eta}_1^{\text{phase}}} (4)\right)$ and phase-only BDAO are plotted for $k = 0, 1, 2, \text{and } 3$. 

(a) $\sigma_X^2 = 0.137$

(b) $\sigma_X^2 = 1.37$

(c) $\sigma_X^2 = 13.7$
turbulence \( \sigma^2 = 13.67 \) are plotted for \( k = 0, 1, 2, \) and 3. We omit the KL divergence for the mild \( \sigma^2 = 0.014 \) case because (1) the steady-state distributions \( \beta_{\eta_1}^{\text{full}} \) and \( \beta_{\eta_1}^{\text{phase}} \) converge almost immediately at \( k \geq 1 \) and are nearly Dirac-delta functions (or beta distributions with very small variance) in mild turbulence; and (2) fitting the beta distribution parameters to the Dirac-delta-like distributions is quite difficult due to how large the beta parameters \( a \) and \( b \) must be in order to achieve a beta distribution with a near-zero variance. Thus, knowing that \( \beta_{\eta_1}^{\text{full}}(4) \) and \( \beta_{\eta_1}^{\text{phase}}(4) \) are fairly good approximations to the steady-state distributions of \( \beta_{\eta_1}^{\text{full}} \) and \( \beta_{\eta_1}^{\text{phase}} \) for mild turbulence, we analyze Fig. 2-6 to show that this is true for stronger strengths of turbulence as well.

For each of the full-wave plots in Fig. 2-6, moving from the curve \( D \left( \beta_{\eta_1}^{\text{full}}(k) || \beta_{\eta_1}^{\text{full}}(4) \right) \) to \( D \left( \beta_{\eta_1}^{\text{full}}(k+1) || \beta_{\eta_1}^{\text{full}}(4) \right) \) results in nearly an order-of-magnitude drop in the KL-divergence for a given Fresnel-number product \( D_f \) and turbulence strength \( \sigma^2 \). What is surprising is that this fact holds for the KL divergence curves shown in the phase-only BDAO plots in strong and very strong turbulence. \( D \left( \beta_{\eta_1}^{\text{phase}}(k) || \beta_{\eta_1}^{\text{phase}}(4) \right) \) to \( D \left( \beta_{\eta_1}^{\text{phase}}(k+1) || \beta_{\eta_1}^{\text{phase}}(4) \right) \) for mild turbulence also results in an overall drop multi-order of magnitude decreases in divergence, although this is not true for all values of \( D_f \). For all Fresnel-number products \( D_f \) and turbulence strengths \( \sigma^2 \), however, it is the case that \( D \left( \beta_{\eta_1}^{\text{full}}(k) || \beta_{\eta_1}^{\text{full}}(4) \right) \) and \( D \left( \beta_{\eta_1}^{\text{phase}}(k) || \beta_{\eta_1}^{\text{phase}}(4) \right) \) for \( k = 3 \) are much closer to 0 than for any \( k < 3 \), showing that the beta distributions \( \tilde{\eta}_{\eta_1}^{\text{full}}(4) \) and \( \tilde{\eta}_{\eta_1}^{\text{phase}}(4) \) that we have fitted are fairly good approximations to the steady state single-spatial-mode power transfers \( \tilde{\eta}_{\eta_1}^{\text{full}} \) and \( \tilde{\eta}_{\eta_1}^{\text{phase}} \). Thus, for the rest of this thesis, we will take \( \tilde{\eta}_{\eta_1}^{\text{full}}(4) \) and \( \tilde{\eta}_{\eta_1}^{\text{phase}}(4) \) to be our steady-state power transfers \( \tilde{\eta}_{\eta_1}^{\text{full}} \) and \( \tilde{\eta}_{\eta_1}^{\text{phase}} \).

From our POPS simulations, we acquired a grid of beta distribution parameter values \( a(D_f, \sigma^2_X) \) and \( b(D_f, \sigma^2_X) \) derived from the fits applied to the \( \tilde{\eta}_{\eta_1}^{\text{full}} \) and the \( \tilde{\eta}_{\eta_1}^{\text{phase}} \) histograms for a given Fresnel-number product \( D_f \) and Rytov-theory logamplitude variance \( \sigma^2_X \). The natural logarithms of \( a(D_f, \sigma^2_X) \) and \( b(D_f, \sigma^2_X) \) vs. \( \ln(D_f) \) and \( \ln(\sigma^2_X) \) are pink circles\(^6\) in Fig. 2-7. We then fit polynomials that are fifth-order in \( \ln(D_f) \) and

---

\(^6\) For very mild \( \sigma^2_X = 0.001 \) and mild \( \sigma^2_X = 0.014 \) turbulence, the distributions of \( \tilde{\eta}_{\eta_1}^{\text{full}} \) and the \( \tilde{\eta}_{\eta_1}^{\text{phase}} \) had extremely small variances, thus requiring large values of \( a \) and \( b \) on the order of \( 10^6 \) that were quite difficult to fit with small confidence intervals. As a result, for small values of \( \sigma^2_X \), the
Figure 2-7: Surface plots of $\beta$-distribution parameters $a$ and $b$ as functions of the Fresnel-number product $D_f$ and Rytov-logamplitude variance $\sigma^2_r$ for the $\beta$-distribution fits made to $\bar{\eta}^\text{full}$ and $\bar{\eta}^\text{phase}$, where $\bar{\eta}^\text{full}$ and $\bar{\eta}^\text{phase}$ are simulated for an FSO link with no extinction loss and with parameters given in Table 2.3. The POPS-simulation fitted points of $\ln(a)$ and $\ln(b)$ are shown as pink circles, while the polynomial fits to $\ln(a)$ and $\ln(b)$ are plotted as three-dimensional surfaces.
fourth-order in \( \ln(\sigma_X^2) \) to the pink circles represented in Fig. 2-7; these polynomials are plotted as three-dimensional surfaces.

\[
f(D_f, \sigma_X^2) = \exp \left( p_{00} + p_{10}x + p_{01}y + p_{20}x^2 + p_{11}xy + p_{02}y^2 
+ p_{30}x^3 + p_{21}x^2y + p_{12}xy^2 + p_{03}y^3 
+ p_{40}x^4 + p_{31}x^3y + p_{22}x^2y^2 + p_{13}xy^3 + p_{04}y^4 
+ p_{50}x^5 + p_{41}x^4y + p_{32}x^3y^2 + p_{23}x^2y^3 + p_{14}xy^4 \right)
\]
where \( x = \ln(D_f), \ y = \ln(\sigma_X^2), \ f = a \) or \( b \) \hspace{1cm} (2.39)

The general equation of the polynomial is given in (2.39). Tables C.1 and C.2 in Appendix B contain the values of the fitted coefficients \( p_{ij} \) and their 95% confidence intervals for integers \( 0 \leq i \leq 5 \) and \( 0 \leq j \leq 5 \) for the beta distribution parameters \( a \) and \( b \) applied to \( \bar{\eta}_{\text{full}} \) for full-wave BDAO and \( \bar{\eta}_{\text{phase}} \) for phase-only BDAO, respectively.

### 2.4.2 Steady-state BDAO power transfers in FSO links with extinction

In this subsection, we will assume that extinction loss is present along the link so that \( e^{-\alpha L} = 0.631 \) as in the notional case set in Table 2.3. In Figs. 2-8 through 2-10, we compare the ergodic averages of the steady-state full-wave and phase-only BDAO power transfers \( \langle \bar{\eta}_{\text{full}} \rangle \) and \( \langle \bar{\eta}_{\text{phase}} \rangle \), as well as the ergodic no-pass power-in fiber and power-in-aperture power transfer \( \langle \bar{\eta}_{\text{noAO}} \rangle \) and \( \langle \bar{\eta}_{\text{recAO}} \rangle \), to the upper bound \( \langle \eta_{\text{1}} \rangle^{UB} \), the no-turbulence power transmissivity \( e^{-\alpha L} \eta_{\text{1}}^{\text{rec}} \), and square-law derived lower bounds \( \langle \eta_{\text{noAO}} \rangle \) and \( \langle \eta_{\text{recAO}} \rangle \). Figures 2-8 through 2-10 present these ergodic power transfer results for moderate, strong, and very strong turbulence, respectively. \( \langle \eta_{\text{1}} \rangle^{UB} \) and \( e^{-\alpha L} \eta_{\text{1}}^{\text{rec}} \) are plotted as solid and dashed blue lines, respectively, while \( \langle \eta_{\text{noAO}} \rangle \) and \( \langle \eta_{\text{recAO}} \rangle \) are plotted as solid and dashed red lines, respectively. \( \langle \bar{\eta}_{\text{noAO}} \rangle \) and \( \langle \bar{\eta}_{\text{recAO}} \rangle \)

polynomial surfaces are not particularly well-fitted to these pink points, many of which are outliers. This poor characterization does not matter because the \( a \) and \( b \) values of the polynomial fit are so high that they fit the histogrammed, low-variance distributions fairly well.
Average Power Transfers vs. $D_f$

Figure 2-8: Moderate turbulence, $\sigma^2 = 0.137$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3. Circles represent the average power-in-fiber $\langle \tilde{\eta}_{\text{noAO}} \rangle$, crosses are the average power-in-aperture $\langle \tilde{\eta}_{\text{recAO}} \rangle$. Their bounds $\langle \tilde{\eta}_{\text{noAO}} \rangle$ and $\langle \tilde{\eta}_{\text{recAO}} \rangle$ are plotted as dashed and solid red lines, while $\langle \eta_1 \rangle^{\text{UB}}$ and $e^{-\alpha L} \tilde{\eta}_{\text{vac}}$ are plotted as solid and dashed blue lines. The steady state full-wave and phase-only BDAO power transfers $\langle \tilde{\eta}_1^{\text{full}} \rangle$ and $\langle \tilde{\eta}_1^{\text{phase}} \rangle$ are plotted as stars and squares, respectively.

In Fig. 2-8, the lower bound $\langle \tilde{\eta}_{\text{recAO}} \rangle$ is very tight to the ultimate power transfer $e^{-\alpha L} \tilde{\eta}_{\text{vac}}$ and $\langle \eta_1 \rangle^{\text{UB}}$ for moderate turbulence — $\langle \tilde{\eta}_{\text{recAO}} \rangle$ lies almost directly underneath $\langle \eta_1 \rangle^{\text{UB}}$ in mild turbulence. Thus, we omit the ergodic power transfer results for mild turbulence ($\sigma^2 = 0.014$) because there is no significant difference between $\langle \tilde{\eta}_{\text{recAO}} \rangle$ and $\langle \tilde{\eta}_1^{\text{full}} \rangle$ as expected.

We now discuss the tightness of the bounds $\langle \tilde{\eta}_{\text{noAO}} \rangle$ and $\langle \tilde{\eta}_{\text{recAO}} \rangle$ compared to their respective POPS averages $\langle \tilde{\eta}_{\text{noAO}} \rangle$ and $\langle \tilde{\eta}_{\text{recAO}} \rangle$. First, we note that in moderate turbulence in Fig. 2-8, the lower bounds $\langle \tilde{\eta}_{\text{noAO}} \rangle$ and $\langle \tilde{\eta}_{\text{recAO}} \rangle$ are fairly tight to one another in the far-field, but grow apart rapidly in the near-field. The far-field tightness is not surprising given that, as discussed, the receiver aperture captures a single, flat-phase coherence area of the received beam, which is an ideal shape to be coupled into...
This bound loosens significantly as \( D_f \), and thus, the aperture sizes increase to the near-unity and near-field Fresnel number range, thus ensuring that the receiver aperture contains multiple coherence areas. In the near-field, a power-in-fiber receiver or coherent receiver with a fixed local oscillator simply will not be able to extract all of the power in the received spatial pattern. As the turbulence strength increases, the separation between \( \langle \eta_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{rec AO}} \rangle \) grows for the given Fresnel-number product range, as expected.

In moderate turbulence, \( \langle \tilde{\eta}_{\text{no AO}} \rangle \) and \( \langle \tilde{\eta}_{\text{rec AO}} \rangle \) are fairly tight to \( \langle \eta_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{rec AO}} \rangle \) and follow the behavior of the bounds well, although there is a slight mismatch between \( \langle \tilde{\eta}_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{no AO}} \rangle \) in the near-unity Fresnel-number product region. For the stronger turbulence strengths in Fig. 2-9 and Fig. 2-10, \( \langle \tilde{\eta}_{\text{rec AO}} \rangle \) is sits almost directly on top of \( \langle \eta_{\text{rec AO}} \rangle \). \( \langle \tilde{\eta}_{\text{no AO}} \rangle \), however, does not follow the \( \langle \eta_{\text{no AO}} \rangle \) bound well, especially in strong turbulence as seen in Fig. 2-9. The shapes of the curves of \( \langle \tilde{\eta}_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{no AO}} \rangle \) are different, with \( \langle \tilde{\eta}_{\text{no AO}} \rangle \geq \langle \eta_{\text{no AO}} \rangle \) and hewing tight to \( \langle \eta_{\text{rec AO}} \rangle \) in the far-field for \( D_f \leq 10^{-1} \), but greatly diverging from the \( \langle \eta_{\text{rec AO}} \rangle \) bound such that \( \langle \eta_{\text{no AO}} \rangle \leq \langle \eta_{\text{no AO}} \rangle \) for \( D_f \geq 12.6 \). A similar mismatch occurs in Fig. 2-10. We attribute this difference between \( \langle \tilde{\eta}_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{no AO}} \rangle \) to the square-law approximation to the two-source spherical-wave structure function (which was made to ease the numerical burden of calculating \( \langle \eta_{\text{no AO}} \rangle \)) used to evaluate \( \langle \eta_{\text{no AO}} \rangle \) in (2.20) rather than the actual 5/3-law given in (2.11). POPS, on the other hand, generates power-transmissivity statistics using the 5/3-law structure function, causing the mismatch between \( \langle \tilde{\eta}_{\text{no AO}} \rangle \) and \( \langle \eta_{\text{no AO}} \rangle \).

It is more interesting to compare \( \langle \tilde{\eta}_1^{\text{full}} \rangle \) to \( \langle \tilde{\eta}_{\text{rec AO}} \rangle \) in the near-unity and near-field \( D_f \) range, because the former should be close to \( \langle \eta \rangle \) whereas we have conjectured that the latter may be well below \( \langle \eta \rangle \). We also note that \( \langle \tilde{\eta}_1^{\text{phase}} \rangle \) lies almost directly underneath \( \langle \tilde{\eta}_1^{\text{full}} \rangle \) in moderate, strong, and very strong turbulence. In moderate turbulence, applying BDAO (be it full-wave or phase-only) does not yield a significant improvement over receiver-only adaptive optics, which again, is unsurprising when the tightness of theoretical bounds \( \langle \eta_{\text{rec AO}} \rangle \) and \( \langle \eta \rangle^{\text{UB}} \) in moderate turbulence is considered. BDAO offers a slight improvement, however, in the near-unity to near-
Figure 2-9: Strong turbulence, $\sigma_n^2 = 1.37$: Upper and lower bounds on $\langle \eta_t \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3. Circles represent $\langle \eta_{\text{HOAO}} \rangle$, crosses are $\langle \eta_{\text{REC AO}} \rangle$. Bounds $\langle \eta_{\text{HOAO}} \rangle$ and $\langle \eta_{\text{REC AO}} \rangle$ are plotted as dashed and solid red lines, while $\langle \eta_{\text{UB}} \rangle$ and $\langle \eta_{\text{UB}} \rangle \times e^{-\alpha L} \eta_{\text{UB}}^{\text{AC}}$ are plotted as solid and dashed blue lines. $\langle \eta_{\text{UB}}^{\text{full}} \rangle$ and $\langle \eta_{\text{UB}}^{\text{phase}} \rangle$ are plotted as stars and squares, respectively.

Field region of $D_f$ where $0.32 \leq D_f \leq 31.6$.

In strong and very strong turbulence in Figs. 2-9 and 2-10, the results are much more interesting. For strong turbulence, the power transfer in the far field is not increased by the application of full-wave BDAO. For near-unity $D_f$ where $0.32 \leq D_f \leq 10$, both full-wave and phase-only BDAO increase the power transmissivity of a link by nearly an order of magnitude as compared to a link only using receiver adaptive optics. Most interestingly, $\langle \eta_{\text{UB}}^{\text{full}} \rangle \approx e^{-\alpha L}$, which means that scintillation in the near-field can be almost completely eliminated. Finally, for very strong turbulence, there is almost a 10 dB gain in power transmissivity from $\langle \eta_{\text{REC AO}} \rangle$ to $\langle \eta_{\text{UB}}^{\text{full}} \rangle$ and $\langle \eta_{\text{UB}}^{\text{phase}} \rangle$, although it is clear that the degree to which the power transfer improves decreases as $D_f$ decreases into the far-field regime. Moreover, scintillation in strong turbulence is not, apparently, removed completely by full-wave BDAO.

Thus, we conclude that while full-wave BDAO has minimal utility in a far-field
Figure 2-10: Very strong turbulence, $\sigma^2_x = 13.7$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3. Circles represent $\langle \eta_{\text{noAO}} \rangle$, crosses are $\langle \eta_{\text{recAO}} \rangle$. Bounds $\langle \eta_{\text{noAO}} \rangle$ and $\langle \eta_{\text{recAO}} \rangle$ are plotted as dashed and solid red lines, while $\langle \eta_1 \rangle^{\text{UB}}$ and $e^{-\alpha L} \eta_{\text{vac}}^{\text{rec}}$ are plotted as solid and dashed blue lines. $\langle \eta_{\text{full}} \rangle$ and $\langle \eta_{\text{phase}} \rangle$ are plotted as stars and squares, respectively.
link operating in mild or moderate turbulence, it offers a marked increase in the power transmissivity if implemented in near-unity or near-field FSO links operating in moderate or stronger turbulence. Moreover, both Fig. 2-9 and Fig. 2-10 highlight that despite phase-only BDAO yielding $\eta^\text{phase}_1$ values slightly worse than the $\eta^\text{full}_1$ of full-wave BDAO, the difference in average power transfer is quite small. Thus, we tentatively conclude that incorporating phase-only BDAO rather than full-wave BDAO into an FSO link may be extremely preferable due to (1) the low implementation complexity of phase-only BDAO; and (2) the almost-negligible decrease in the average power transfer achievable by the phase-only BDAO system vs. the full-wave BDAO system.

In order to assess how much this degradation matters, however, we must derive bounds on the classical and quantum communication rates of FSO links using full-wave and phase-only BDAO systems and then incorporate both the theoretical upper bound $\langle \eta_1 \rangle^{\text{UB}}$ and lower bounds $\langle \eta_{\text{noAO}} \rangle$ and $\langle \eta_{\text{recAO}} \rangle$ derived in this chapter, as well as the POPS results on power transfers $\langle \eta^\text{full}_1 \rangle$ and $\langle \eta^\text{phase}_1 \rangle$ in phase-only and full-wave BDAO links. So, we turn our attention to deriving these bounds for classical communication links and secure-key rate quantum communication links.
In this chapter, the performance gap that lies between single-spatial-mode free-space optical communication systems using current methods to mitigate atmospheric turbulence and the performance these FSO systems would achieve were full-wave adaptive optics applied will be quantified. We begin by reviewing the ultimate information transmission rates of free-space optical channels utilizing one of three receivers - namely, Holevo, heterodyne, or homodyne receivers. We discuss their dependence on the power transfer of the free-space optical link and derive upper and lower bounds on the ergodic classical communication rates in terms of the upper and lower bounds on the average FSO power transfer through atmospheric turbulence derived in Chapter 2. Finally, we will quantify the BDAO-enabled ergodic classical communication rate increases more accurately by incorporating the probability distribution functions for the steady-state BDAO power transfers $\tilde{\eta}_1^{\text{full}}$ and $\tilde{\eta}_1^{\text{phase}}$ discussed in Chapter 2.
3.1 Classical communication over a free-space link

Optical propagation along a line-of-sight link between finite transmitter and receiver pupils is a lossy bosonic channel. For vacuum propagation, the bosonic channel's loss is due solely to diffraction. When an optical signal propagates through the atmosphere, additional loss factors accrue owing to absorption, scattering, and clear-weather turbulence. Given our interest in high-rate, clear-weather communication, and assuming an operating wavelength that minimizes atmospheric absorption and scattering losses, we will assume that the changes in channel transmissivity from vacuum-propagation values are due to clear-weather turbulence and an extinction loss characterized by a known extinction coefficient and the length of the propagation path. The worst-case value of the average background rate due to daylight and blackbody radiation for a narrowband optical communication link operating at fiber-compatible wavelengths is on the order of $10^{-6}$ photons per mode [49], which negligibly affects ultimate optical communication rates [50]. Thus, we may assume that the environmental noise injected on a single-mode basis into the lossy bosonic channel modeling free-space optical propagation is the minimum vacuum-state noise that preserves the Heisenberg uncertainty principle\(^1\).

The trace-preserving completely-positive map of the pure-loss channel with a single-mode input electromagnetic field with annihilation operator $\hat{a}$ and output electromagnetic field with annihilation operator $\hat{a}'$ is written as the commutator-preserving beam splitter relation

$$\hat{a}' = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{b}$$

where $\hat{b}$ is in its vacuum state and $\eta$ is the channel transmissivity.

Due to the quantum nature of light, the ultimate limit on the rate of reliable information transfer over an optical communication link is a function not only of the bosonic channel transmissivity $\eta$, but of the receiver's detection method. Coherent re-

\(^1\)Of course, a conventional direct-detection receiver will collect many spatiotemporal modes simultaneously, and hence can incur nontrivial background-light shot noise.
receivers employing either heterodyne or homodyne detection yield Gaussian statistics, resulting in easily-derived capacity formulas from the well-known Shannon theory for the additive white Gaussian noise channel. In particular, heterodyne and homodyne channel capacities for an optical communication link transmitting \( N_s \) signal photons per mode on average over a pure loss bosonic channel with channel transmissivity \( \eta \) are

\[
C_{\text{het}} = \log_2 (1 + \eta N_s) \text{ bits/channel use} \tag{3.2}
\]

\[
C_{\text{hom}} = \frac{1}{2} \log_2 (1 + 4\eta N_s) \text{ bits/channel use}. \tag{3.3}
\]

These capacities correspond to single-channel-use quantum measurements, rather than optimal joint measurements made over a long sequence of channel uses. The ultimate (Holevo) capacity of the pure-loss bosonic channel when such joint measurements are employed is [51]

\[
C_{\text{hol}} = g(\eta N_s) \tag{3.4}
\]

where

\[
g(x) \equiv (x + 1) \log_2(x + 1) - x \log_2(x) \tag{3.5}
\]

is the Shannon entropy of the Bose-Einstein probability distribution with mean \( x \). The Holevo capacity is achieved when the transmitter performs single-channel use random encoding over coherent states with a zero-mean isotropic Gaussian prior distribution whose variance satisfies the transmitter’s average photon-number constraint. Regardless of the reception technique, the ultimate rate of a free-space optical communication channel will be determined by the channel transmissivity \( \eta \). Thus, we now turn our attention to employing results from Chapter 2 to: (1) obtain bounds on the ergodic capacities of single-spatial-mode FSO links employing Holevo, heterodyne, and homodyne detection with or without adaptive optics; and (2) evaluate the ergodic capacities of the listed FSO links using the single-spatial-mode power transfer
PDFs derived from turbulence simulation.

### 3.2 Rate bounds for FSO classical communication links

We now use the upper bound (2.23) and lower bounds (2.20) and (2.22) on $\langle \eta \rangle$ to develop analogous upper and lower bounds on the classical capacities of free-space optical systems transmitting information along a single spatial mode. Because we would like to assess the average capacities of the channels for varying states of atmospheric turbulence, the *ergodic channel capacity* is the relevant metric of interest.

Consider a non-fading pure-loss channel whose capacity function is $C(\eta N_s)$ bits/use, where $\eta$ is the transmissivity and $N_s$ is the constraint on the transmitter’s average photon number per channel use. Now suppose that the transmissivity is random because of turbulence-induced fading — the ergodic capacity $\langle C \rangle$ of that fading channel is defined to be

\[
\langle C \rangle = \int_0^1 d\eta p(\eta) C(\eta N_s) \geq \int_0^1 d\eta p(\eta)\eta C(N_s) = \langle \eta \rangle C(N_s),
\]

where $p(\eta)$ is the probability density function for the channel transmissivity and (3.7) holds by Jensen’s inequality if $C(\eta N_s)$ is concave in $\eta$ for fixed $N_s$ because $C(0) = 0$. Additionally, if $C(\eta N_s)$ is concave in $\eta$ for fixed $N_s$, we may also derive the upper bound

\[
\langle C(\eta N_s) \rangle \leq C(\langle \eta \rangle N_s)
\]

using Jensen’s inequality. Proving that $C(\eta N_s)$ is concave is simple. Table 3.1 lists the first and second derivatives of the heterodyne, homodyne, and Holevo capacities for classical communication over a non-fading, pure-loss channel with transmissivity $\eta$ and average transmitted photon number $N_s$. 

72
\[
\begin{align*}
C(0) & = \ln(2) \ln(2) / 2, \\
\ln(2) & = 1.44, \\
\ln(2) & = 2.88. 
\end{align*}
\]

Table 3.1: First and second derivatives of the heterodyne, homodyne, and Holevo capacities of a non-fading, pure-loss channel.

<table>
<thead>
<tr>
<th>( C(\eta N_s) ) for ( \eta N_s \ll 0 )</th>
<th>( \eta C(N_s) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_{\text{het}}(\eta N_s) = \log_2(1 + \eta N_s) )</td>
<td>( \eta N_s / \ln(2) = 1.44 \eta N_s )</td>
</tr>
<tr>
<td>( C_{\text{hom}}(\eta N_s) = \log_2(1 + 4\eta N_s) / 2 )</td>
<td>( 2\eta N_s / \ln(2) = 2.88 \eta N_s )</td>
</tr>
<tr>
<td>( C_{\text{hol}}(\eta N_s) = g(\eta N_s) )</td>
<td>( \eta N_s (1 - \ln \eta N_s) / \ln(2) )</td>
</tr>
</tbody>
</table>

Table 3.2: Taylor expansions of the heterodyne, homodyne, and Holevo capacities of a non-fading, pure-loss channel for small \( \eta N_s \) and values of \( \eta C(N_s) \).

All of the Table 3.1 capacities equal zero at \( \eta = 0 \), all are increasing functions of \( x = \eta N_s \), and all are concave in \( \eta \) at fixed \( N_s \). Thus, the listed ergodic capacities obey\( \langle C(\eta_1 N_s) \rangle \geq \langle \eta_1 \rangle C(N_s) \geq \langle \eta_1 \rangle^{\text{LB}} C(N_s) \) for any lower bound \( \langle \eta_1 \rangle^{\text{LB}} \) on \( \langle \eta_1 \rangle \), and obey\( \langle C(\eta_1 N_s) \rangle \leq C(\langle \eta_1 \rangle N_s) \leq C(\langle \eta_1 \rangle^{\text{UB}} N_s) \) for any upper bound \( \langle \eta_1 \rangle^{\text{UB}} \) on \( \langle \eta_1 \rangle \). Before linking these bounds to physical realizations of FSO links, we note that the upper and lower bounds for the discussed capacities \( C(\eta N_s) \) do not converge as \( \eta N_s \to 0 \).

Table 3.2 lists the Taylor-series approximation for \( C(\eta N_s) \) around \( \eta N_s = 0 \), which corresponds to the upper bound on communication capacity, as well as \( \eta C(N_s) \), which is the form of the lower bound on communication capacity. It is clear that as \( \eta N_s \) becomes small, the upper and lower bounds on \( C(\eta N_s) \) will not converge to the same value.

The \( \langle \eta_{\text{noAO}} \rangle C(N_s) \) lower bound on the channel capacity derives from a focused-beam, uniform-intensity transmitter and a receiver that poorly couples to the resulting spatial pattern at receiver \( A_R \). The \( \langle \eta_{\text{recAO}} \rangle C(N_s) \) bound is derived from the same transmitter paired with a receiver that couples all power from the received spatial pattern at \( A_R \). \( C(\langle \eta_1 \rangle^{\text{UB}} N_s) \) is an upper bound on the ergodic capacity that can be achieved over a free-space propagation link with Fresnel-number product \( D_f \) and extinction loss \( e^{-\alpha L} \). A system with a transmitter tracking the optimal input \( \Phi_1(\rho) \)
Bounds on $(C_{\text{het}}), N_s = 1$

(a) Bounds on heterodyne classical capacity.

Bounds on $(C_{\text{hom}}), N_s = 1$

(b) Bounds on homodyne classical capacity.

and $\phi_1(\rho')$ may approach this bound, and will certainly perform better than a system that only applies adaptive optics at the receiver. These capacity bounds are plotted in Fig. 3-1 for heterodyne, homodyne, and Holevo capacities and for fixed $N_s = 1$. 

74
Figure 3-1: Upper and lower bounds on heterodyne, homodyne, and Holevo capacities for free-space optical communication for varying turbulence strengths over a link for fixed signal photon number \( N_s = 1 \) for the notional case set in Table 2.3. Lower bounds on the single-mode channel capacity using \( \langle \eta_{\text{HOAO}} \rangle C(N_s) \) are shown as dotted lines; lower bounds using \( \langle \eta_{\text{freeAO}} \rangle C(N_s) \) are plotted as solid lines. The upper bound on the ultimate channel capacity of a link with Fresnel-number product \( D_f, C(\langle \eta \rangle^{UB} N_s) \), is shown as a solid blue line, while the lower bound on this channel’s no-turbulence capacity, \( e^{-\alpha L \eta_{\text{vac}}^{UB}} C(N_s) \), is shown as a dashed line.

From Fig. 3-1, it is apparent that for links with Fresnel-number product \( D_f < 0.016 \) operating in mild and moderate turbulence, sending out a constant-intensity focused beam allows a classical communication to nearly achieve the lower bound on the channel’s no-turbulence capacity \( e^{-\alpha L \eta_{\text{vac}}^{UB}} C(N_s) \). Had we extended the plots further into the far field, we would see the same result for the capacity curves corresponding to strong and very strong turbulence for \( D_f < 10^{-6} \). Thus, we state that for links with Fresnel number product \( D_f \ll 1 \), the constant-intensity focused beam is the optimal input spatial mode to the channel. This is hardly surprising; it has long been known that a plane wave achieves near-optimal channel transmissivity \( \langle \eta_{\text{freeAO}} \rangle \) approaches \( D_f \) for long-haul links well into the far field where a receiver aperture will necessarily lie within a single coherence area of the atmosphere [37]. For \( d_T/d_R = 1 \) and \( D_f \ll 1 \), the quadratic phase factor in (2.15) becomes irrelevant. For links with Fresnel-number products \( D_f \sim 1 \) or \( D_f \gg 1 \), however, this is most certainly not the
case. Fig. 3-1 identifies the non-far-field regime as one in which we might make significant improvements in the classical capacity by applying BDAO. Thus, we introduce our POPS simulation results and evaluate the true ergodic capacities of the link when adaptive optics are applied.

3.3 Classical capacities of FSO links operating with BDAO

We now present POPS-simulated results for the ergodic Holevo classical capacities achieved after a BDAO system tracking the power-transfer optimizing spatial mode has reached a steady state. To evaluate the tightness of our previous bounds (3.7) and (3.8), we also present the ergodic capacities for links operating with no BDAO and employing either no adaptive optics or receiver-only adaptive optics with fixed photon number $N_s = 1$.

Figures 3-2 through 3-4 present both the theoretical upper and lower bounds on the Holevo capacity of an FSO link with parameters given in Table 2.3, as well as the ergodic capacities for systems operating with: (1) no adaptive optics and coupling into fiber, $\langle C_{\text{hol}}(\tilde{\eta}_{\text{noAO}}) \rangle$; (2) receiver-only adaptive optics, $\langle C_{\text{hol}}(\tilde{\eta}_{\text{recAO}}) \rangle$; (3) steady-state full-wave BDAO, $\langle C_{\text{hol}}(\tilde{\eta}_{\text{full}}) \rangle$; and (4) steady-state phase-only BDAO, $\langle C_{\text{hol}}(\tilde{\eta}_{\text{phase}}) \rangle$.

As we did in Chapter 2, results for the mild-turbulence case are omitted because the lower and upper bounds are so tight that they assure minimal capacity increases from the receiver-only adaptive optics case to the phase-only BDAO and full-wave BDAO cases.

Figures 3-2 through 3-4 highlight the looseness of the lower bounds on the ultimate FSO Holevo capacity $\langle \tilde{\eta}_{\text{recAO}} \rangle C(1)$ and $\langle \tilde{\eta}_{\text{noAO}} \rangle C(1)$ with respect to the true

---

2 The results for FSO ergodic heterodyne and homodyne classical capacities are omitted because the showed the same features and behavior as the ergodic communication rates featured in the following Holevo capacity plots.

3 By POPS ergodic capacities, we mean that given a Fresnel-number product $D_f$ and Rytov-logamplitude variance $\sigma_Y^2$, power transfers $\tilde{\eta}_{\text{noAO}}$, $\tilde{\eta}_{\text{recAO}}$, $\tilde{\eta}_{\text{full}}$, and $\tilde{\eta}_{\text{phase}}$ were simulated for $n_{\text{iter}}$ instantiations of the turbulence screens along the FSO link. We calculate the ergodic value of a function $f(\eta)$ along a link by taking its mean over the $n_{\text{iter}}$ power transfer values.

---
Figure 3-2: Moderate turbulence, $\sigma_x^2 = 0.137$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$. Circles represent the ergodic Holevo capacity with power-in-fiber reception $\langle C_{\text{hol}}(\eta_{\text{noAO}}) \rangle$, crosses are the average power-in-aperture Holevo capacity $\langle C_{\text{hol}}(\eta_{\text{recAO}}) \rangle$. Their corresponding lower bounds $\langle \eta_{\text{noAO}} \rangle C_{\text{hol}}(1)$ and $\langle \eta_{\text{recAO}} \rangle C_{\text{hol}}(1)$ are plotted as dashed and solid red lines, while the upper bound $\langle C_{\text{hol}}(\eta_{\text{UB}}) \rangle$ and no-turbulence rate lower bound $e^{-\alpha L} \eta_{\text{recAO}}^{\text{rec}} C_{\text{hol}}(1)$ are plotted as solid and dashed blue lines. The steady state full-wave and phase-only BDAO ergodic Holevo capacities $\langle C_{\text{hol}}(\eta_f^{\text{full}}) \rangle$ and $\langle C_{\text{hol}}(\eta_f^{\text{phase}}) \rangle$ are plotted as stars and squares, respectively.
Figure 3-3: Strong turbulence, $\sigma^2 = 1.37$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta_1) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$. Circles are $\langle C_{\text{hol}}(\eta_{\text{noAO}}) \rangle$, crosses are $\langle C_{\text{hol}}(\eta_{\text{recAO}}) \rangle$. Bounds $\langle \eta_{\text{noAO}} \rangle C_{\text{hol}}(1)$ and $\langle \eta_{\text{recAO}} \rangle C_{\text{hol}}(1)$ are dashed and solid red lines, while $C_{\text{hol}}(\langle \eta_1 \rangle_{\text{UB}})$ and $e^{-\alpha L} \eta_{\text{vac}} C_{\text{hol}}(1)$ are solid and dashed blue lines. $\langle C_{\text{hol}}(\eta_{\text{full}}) \rangle$ and $\langle C_{\text{hol}}(\eta_{\text{phase}}) \rangle$ are squares and stars, respectively.
Figure 3-4: Very strong turbulence, $\sigma^2 = 13.7$: Upper and lower bounds on $\langle C_{\text{hol}}(\eta_1) \rangle$ and ergodic Holevo capacities vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and $N_s = 1$. Circles are $\langle C_{\text{hol}}(\eta_{\text{hoAO}}) \rangle$, crosses are $\langle C_{\text{hol}}(\eta_{\text{recAO}}) \rangle$. Bounds $\langle \eta_{\text{hoAO}} \rangle C_{\text{hol}}(1)$ and $\langle \eta_{\text{recAO}} \rangle C_{\text{hol}}(1)$ are dashed and solid red lines, while $C_{\text{hol}}(\langle \eta_1 \rangle_{\text{UB}})$ and $e^{-\alpha L} \eta_1 \text{var} C_{\text{hol}}(1)$ are solid and dashed blue lines. $\langle C_{\text{hol}}(\hat{\eta}_1^{\text{full}}) \rangle$ and $\langle C_{\text{hol}}(\hat{\eta}_1^{\text{phase}}) \rangle$ are squares and stars, respectively.
ergodic capacities $C_{\text{hol}}(\bar{\eta}_{\text{noAO}})$ and $C_{\text{hol}}(\bar{\eta}_{\text{recAO}})$. From Figs. 3-2 and 3-3 it is clear that BDAO, whether implemented with full-wave measurements or phase-only measurements, does not significantly increase the Holevo capacity of a link in the far field for $D_f \leq 10^{-1}$ in the presence of strong, moderate, or mild turbulence. Moreover, in the far field for these turbulence cases, even receiver-only adaptive optics does not greatly increase the capacity of the link. In the near-field, for $D_f \geq 10^2$ in moderate or strong turbulence, incorporating receiver-only adaptive optics provides the bulk of the increase in Holevo capacity, while adding BDAO does not greatly increase the ergodic capacity of the link.

Figure 3-3 shows that adding receiver-only adaptive optics is sufficient to achieve close-to-optimal performance in the near and far-field regimes. In the near-unity $D_f$ range, however, there does appear to be some utility to adding either full-wave or phase-only BDAO to the link. In very strong turbulence, as seen in Fig. 3-4, we see that there are significant rate increases achieved with the addition of receiver-only adaptive optics, and again with the incorporation of BDAO, be it full-wave or phase-only, into the link. Moreover, Figs. 3-2 through 3-4 all demonstrate that there is only a minimal difference between the ergodic rates achieved by links operating with full-wave BDAO compared to links operating with the less-ideal, more easily-implemented phase-only BDAO.

3.4 Challenges in achieving optimal communication rates in a free-space link

Achieving near-optimal channel transmissivity for far-field links is simple: the constant-intensity input given in (2.15) is near optimal. For $d_T/d_R \ll 1$ and $d_T < \rho_0$, $\Phi_1(\rho)$ is no longer random and may be generated exactly as discussed in [45].

This is not the case for near-field free-space communication links with $d_T = d_R$. In this scenario, the only way for a system with a coherent receiver to achieve the optimal channel transmissivity $\eta_1$ is for: (1) the transmitter to track and generate the
random spatial input eigenmode $\Phi_1(\rho)$ of the free-space propagation kernel $h(\rho', \rho)$; and (2) for the receiver to track and extract the random spatial output eigenmode $\phi_1(\rho')$. A system employing direct detection could avoid the spatial coupling loss by use a photon bucket detector to capture all power at $A_R$, but would experience higher background-light shot noise as a result. Moreover, if an FSO communication link was required to have a fiber-coupled detector, it would need to employ adaptive optics to efficiently couple the received spatial mode $U_L(\rho')$ into that fiber.

Thus, we were motivated to design a free-space optical link that achieves optimal performance in the near-unity and near-field $D_f$-regimes by implementing full-wave adaptive optics at both the transmitter and receiver. Bounding the performance of a system that tracks these input-output mode pairs is difficult due to the lack of closed-form higher-order statistics for the power transfer eigenvalues. Thus, we introduced POPS simulation results to resolve the Fresnel-number product $D_f$ regimes in which the addition of BDAO would enable large improvements in rate. We found that BDAO offers almost no improvement over systems operating with receiver-only adaptive optics in moderate or weaker turbulence. In strong turbulence, full-wave and phase-only BDAO only offer a significant rate improvement for near-unity Fresnel-number products. In very strong turbulence, however, both full-wave and phase-only BDAO yield almost an order of magnitude of improvement in the communication rate. The following question then arises. Is the utility of BDAO limited to near-unity Fresnel-number product scenarios or links that may experience very strong turbulence for all communication protocols? Classical capacity rates behave in a fairly smooth fashion with respect to their power transfers, unlike quantum communication protocols, which generally require a minimal amount of received power to guarantee a nonzero secret-key rate. We seek to answer this question in Chapters 4 and 5, where we consider the secure key rate increases available to FSO links implementing two selected quantum key distribution protocols.
Chapter 4

Single-Spatial-Mode Quantum Key Distribution through Atmospheric Turbulence

Having discussed the rate increases realized when classical communication protocols use full-wave adaptive optics for turbulence compensation, we now turn our attention to the realizable rate increases in quantum communication protocols operating over FSO links. We consider a class of protocols known as quantum key distribution (QKD) [52], which allow two parties (traditionally called Alice and Bob) connected by a quantum channel and an authenticated classical channel to exchange a perfectly secret key in the presence of an eavesdropper (Eve) whose computing power and signal manipulation techniques are restricted only by the fundamental laws of physics. First, we will provide a general overview of quantum key distribution protocols. Then, we will discuss the operation of the most successfully implemented QKD protocol, decoy-state Bennett-Brassard 1984 (ds-BB84) quantum key distribution, and present its secure-key rate for an FSO link as a function of the power transmissivity of the link and other system parameters. We will then present theoretical upper and lower bounds on the ergodic secure key rate of a ds-BB84 QKD FSO link operating in atmospheric turbulence in terms of the power transfer bounds derived in Chapter 2, and use the POPS-derived PDFs for steady-state BDAO power transfers $\tilde{\eta}_1^{\text{full}}$ and
\( \hat{\eta}_1 \) to calculate the ergodic secure key rate increases furnished by the addition of BDAO to the FSO link.

### 4.1 Overview of QKD protocols

QKD is particularly attractive because it can distribute a one-time-pad — also referred to as a random secret key — needed for information-theoretic security, as compared to the security guarantees of classical cryptographic protocols, which are based on assumptions of the computational resources available to Alice, Bob, and Eve. QKD guarantees that at the end of the protocol, Alice and Bob will share a random bit string about which Eve has no information. This security guarantee holds even when all non-ideal behavior of the quantum channel is attributed to Eve. Eve is assumed to collect all lost signal photons, insert all background light, and can perform any operation allowed by the laws of quantum mechanics. In the public classical channel, however, she can only listen to the classical information exchanged between Alice and Bob. The figure of merit for QKD is the rate at which Alice and Bob can distill a perfectly secure key.

Quantum key distribution protocols can either be prepare and measure (P&M) or entanglement-based (EB) protocols. In a P&M protocol, Alice shares information with Bob by encoding data in a quantum state and transmitting it to Bob. Bob generates a raw key by measuring the state. In an EB protocol, Alice and Bob initially share an entangled state and measure it together, resulting in Bob having a raw key correlated with Alice’s raw key. The steps for P&M and EB protocols are identical after this stage. In order to distill a shared secret key from their raw key, Alice and Bob use the public classical channel to implement the following procedures [53].

1. **Channel estimation**: Alice and Bob publish a subset of their measurements and results and compare them to derive the quantum error rate of the channel, which in turn allows them to assess the possible actions that were taken by their adversary, Eve.
2. **Error correction.** Alice and Bob apply classical error-correcting codes to their raw bit strings, sharing information like checksums across the public channel as needed.

3. **Privacy amplification.** Realizing that they have shared information with Eve about their error-corrected strings in the form of checksums and measurement results, Alice and Bob use their estimate of the channel’s error rate to apply hashing functions that randomize and distill their raw key into a shorter secret key about which Eve has virtually no information [54, 55].

The ultimate secret key rate of a QKD protocol implemented on a noisy channel between Alice and Bob in the presence of an eavesdropper Eve is given by the Csiszár-Körner bound [56]. It states that the secret-key rate, in bits per channel use, is bounded above by the difference between (1) the mutual information between Alice and Bob’s lists of correlated measurement results, \( I(A : B) \), and (2) the information \( f(A/B : E) \) that Eve extracts by eavesdropping on the quantum channel and observing the information exchanged over the public classical channel. The upper bound on the secret-key rate \( R \) neglecting finite-key effects and sub-unity reconciliation efficiency [53] is

\[
R \leq I(A : B) - f(A/B : E). \tag{4.1}
\]

Bob and Alice can share a key of \( I(A : B) \) bits that is error free with high probability by having Bob (Alice) apply an error correction protocol to his (her) bit string and sending the error-correction information to Alice (Bob) in a process known as reverse (direct) reconciliation. In an effort to minimize the information acquired by Eve, the party receiving the checksum information simply makes the necessary corrections and sends no information back to the other party. Thus, this error-correction process is known as one-way reverse (direct) reconciliation.

If reverse (direct) reconciliation is applied, Eve’s accessible information is written as the mutual information between Bob (Alice) and Eve \( f(B : E) \) \( f(A : E) \). The function \( f(X : E) \) of the information about the key accessible to Eve is determined by which of the three possible types of attacks – individual, collective, or coherent –
Eve is assumed to implement.

1. Suppose Eve is restricted to an *individual* attack; i.e. she is only able to attack single quantum symbols flying from Alice to Bob and is restricted to making the same measurement on each quantum symbol. In this case, the information she gains is the Shannon mutual information $I(X : E)$.

2. If Eve mounts a *collective* attack, she interacts individually with each quantum symbol flying from Alice to Bob, stores her results in a quantum memory, and performs an optimal, joint measurement on all stored quantum symbols at the end of the QKD session. The information she gains is the Holevo information $\chi(X : E)$ where

$$\chi(X : E) = S(\hat{\rho}_E) - \sum_x p(x)S(\hat{\rho}_{E|x}). \quad (4.2)$$

Here: $\hat{\rho}_E$ is the density operator of Eve’s individual stored quantum symbols; $S(\hat{\rho}_E)$ is the von Neumann entropy of the $\hat{\rho}_E$; $X$ is the classical message with alphabet $\{x\}$ and probability distribution $p_X(x)$; and $\hat{\rho}_{E|x}$ is the density operator of Eve’s stored quantum state conditioned on $X = x$.

3. When Eve stages a *coherent* attack, she performs a joint operation with all quantum symbols flying from Alice to Bob, stores her results in a quantum memory, and performs an optimal joint measurement on those stored quantum symbols at the end of the QKD session. While this has not been proven to hold in all cases, it is known for several important QKD protocols, including BB84, that coherent attacks are no better than collective attacks [53, 57].

A great many quantum key distribution protocols have been proposed. Discrete-variable protocols encode information in polarization [58], spatial mode [59], or discretized time-frequency bases [60]. Continuous-variable protocols generally encode information in the quadrature of a Gaussian quantum state [61]. Each such protocol has had a wealth of analysis deriving security bounds for various attacks. For this thesis, we will focus on the ds-BB84 protocol, which is the latest version of one of the
oldest QKD protocols and has many successful implementations in both fiber [62, 63] and free space [64–66].

4.2 Secret-key rate bounds for FSO decoy-state BB84 QKD links

In ideal prepare-and-measure BB84 [67], Alice transmits each bit by preparing a single photon in one of four randomly selected polarizations: horizontal \( (H) \), vertical \( (V) \), diagonal \( (+45^\circ) \), or antidiagonal \( (-45^\circ) \). Bob randomly selects either the \( H/V \) or the \( +45^\circ/-45^\circ \) basis for his polarization measurement. If Eve is not present and Bob detects a single-photon state in the same basis Alice used, then Bob’s measurement provides a shared random bit. In order to arrive at the shared random key after the quantum transmission, Alice and Bob perform a procedure called sifting. Alice sends Bob a list of the bases she used via their public channel, after which Bob uses that public channel to tell Alice the transmissions on which he detected a photon using the same basis that she employed. Alice and Bob then discard results from all other time slots. With no Eve and Alice and Bob having perfect equipment, sifting alone would yield a shared secret key. However, Eve’s presence cannot be dismissed, and Alice and Bob will not have ideal equipment. Thus, Alice and Bob must complete the protocol by performing error correction and privacy amplification to distill their shared secret key.

The Shor-Preskill security proof for BB84 [68], based on entanglement distillation, certified the prepare-and-measure protocol as one that generated shared one-time pads at a high rate provided that optimal conditions, namely perfectly prepared single-photon polarization states, lossless but noisy propagation, and 100%-efficient photodetectors, were met. Further work by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [69] modified the key generation rate derived in [68] to account for inevitable imperfections, like detectors whose behavior might differ from polarization basis to polarization basis or basis misalignments in either the transmitted state or in Bob’s
receiver. They proved that the BB84 protocol was secure against collective attacks. GLLP also included the deleterious effect of “tagging” errors on BB84, in which an imperfect source could add additional information to transmitted photon states that could be exploited by Eve without being detected by Bob. Renner et al. [57] later proved that the BB84 secure key rate derived by Gottesman et al. was agnostic as to whether Eve mounted a coherent attack or a collective attack.

The effect of basis misalignments and detector errors can be eliminated by careful calibration of the polarization encoding and polarization analysis at Alice’s transmitter and Bob’s receiver, respectively. Mitigating the effect of tagging errors in a security analysis, however, was much more difficult. The security of BB84 lies in the fact that Eve cannot interfere with a single photon state without introducing a detectable error in Bob’s bit string. Unfortunately, high-rate, high-fidelity sources that generate single photons on demand [70] are not yet available. Thus, BB84 QKD systems are typically implemented with sources that generate weak coherent states, which have a non-zero probability of multiple-photon pulses. In a photon-number splitting (PNS) attack, Eve can perform a quantum non-demolition measurement and split off a single photon from Alice’s transmitted multiple-photon state, thus gaining information about the one-time pad without introducing errors in Bob’s bit string. Without modifying the BB84 protocol, the only solution available to Alice and Bob is to use an extremely weak coherent source so that the probability of a multi-photon state is reduced [71], which, naturally, results in low key-generation rates.

4.2.1 Decoy-state BB84

In order to Eve’s PNS attack, Lo and Ma introduced and proved the security of decoy-state BB84 against PNS attacks [72, 73]. The secure-key rate derived in [69] for the unmodified BB84 protocol presumed that all multi-photon transmissions reach Bob, despite the presence of absorption in the channel. Thus, in order to preserve the BB84’s security, Alice and Bob must use extremely pessimistic estimates of the fraction of and quantum bit error rate (QBER) for the single-photon transmissions contributing to Bob’s bit string.
Decoy-state BB84 neatly solves this problem by requiring Alice to poll the channel with quantum states of varying photon number. Consider a toy case [74] in which Alice can send either single-photon or two-photon states on demand through a channel with no absorption and Bob has 100% efficient detectors that generate no dark counts. During a PNS attack, Alice’s single-photon states will never result in a detection at Bob’s receiver due to their interception by Eve. Alice’s two-photon states will always result in a detection at Bob’s receiver. Thus, it is clear that the likelihood of Bob logging a detection event when Alice sends a two-photon state will be artificially high compared to the likelihood of a detection event when Alice transmits a single photon state. Because it is not practical for Alice to poll the channel with photon-number states, the decoy state protocol requires Alice to poll the channel with coherent states (with randomized phase) \( \{ \sqrt{n_d e^{i\theta}} \} \) for several values of the average photon number \( n_d \), and to use the state \( \sqrt{n_s e^{i\theta}} \) with randomized phase as the designated signal state. At the end of the QKD session, Alice tells Bob which transmitted symbols had \( n_s \) photons on average and he replies with the probability \( P^B_{n_s} \), that he detected such a symbol:

\[
P^B_{n_s} = \sum_{k=0}^{\infty} p^B_k e^{-n_s} n_s^k \frac{k!}{k^k} = \sum_{k=0}^{\infty} P^B_{k;n_s},
\]

After channel estimation, Alice will also know the QBER for her \( \sqrt{n_s e^{i\theta}} \) transmission:

\[
E_{n_s} = \frac{1}{P^B_{n_s}} \sum_{k=0}^{\infty} p^B_k e_k e^{-n_s} n_s^k \frac{k!}{k^k}.
\]

Here, \( p^B_k \) is Bob’s conditional probability of making a detection given that Alice’s \( \sqrt{n_s e^{i\theta}} \) transmission contained \( k \) photons and \( e_k \) is the QBER for a \( k \)-photon state. For a deterministic channel with end-to-end power transmissivity (including detector
quantum efficiency) $\eta$ and average background-light plus dark count rate $n_b$, we have

$$p^B_k = 1 - (1 - \eta)^k e^{-n_b}. \quad (4.6)$$

By polling the channel with multiple decoy states $\{|\sqrt{n_d} e^{i\theta}\}$, Alice and Bob can develop a system of equations from which the $\{p^B_k\}$ (and thus the $\{P^B_{k;n_s}\}$) and the $\{e_k\}$ can be determined. A detailed explanation of the protocol and full expressions for $P^B_{n_s}$, $E_{n_s}$, $P^B_{1;n_s}$, and $e_1$ are given in Appendix D. From the GLLP security proof [69, 73], it has been shown that Alice and Bob achieve a secret key rate $\Delta I$ in bits/channel use given by

$$\Delta I(\eta, n_s, n_b) = \max[0, P^B_{1;n_s}(\eta, n_s, n_b)(1 - H_2(e_1(\eta, n_s, n_b)))$$

$$- P^B_{n_s}(\eta, n_s, n_b)H_2(E_{n_s}(\eta, n_s, n_b))]. \quad (4.7)$$

when Eve mounts a collective or coherent attack [57], where $H_2(p)$ is the binary entropy function $-p \log_2(p) - (1 - p) \log_2(1 - p)$.

Equation (4.7) assumes that Alice polls the channel with an infinite number of decoy states, which allows exact determination of $P^B_{1;n_s}$, Bob’s probability of detection when Alice’s $|\sqrt{n_d} e^{i\theta}\rangle$ transmission contains a single photon, and $e_1$, the resulting QBER. Ma et al. [75] were the first to discuss a modified, more realistic version of ds-BB84 QKD in which Alice and Bob are constrained to a finite number of decoy states. This constraint yields a lower bound on $P^B_{1;n_s}$ and an upper bound on $e_1$, thus resulting in a lower key-generation rate. We will assume that Alice and Bob poll the channel with an infinite number of decoy states and operate at the key-generation rate given in (4.7), but we note that the rate of the practical two-decoy state method is extremely close to that of the infinite-decoy state method [75].

Monitoring the channel by sounding it with decoy states allows Alice and Bob to reach significantly higher rates in the presence of background light and dark counts, detector misalignments, and multi-photon signal states than would be possible without decoy states. Most QKD implementations tune the signal state’s average pho-
Decoy-State BB84 Rate vs. $\eta$, $n_b = 10^{-4}$ photons/use

Figure 4-1: The secret key rate of a ds-BB84 QKD channel, $R_{\text{ds-BB84}}(\eta, n_b)$, versus a deterministic power transmissivity $\eta$ for a fixed background $n_b = 10^{-4}$ photons/use and a modulation rate $R_{\text{mod}} = 10$ Gbps.

For classical communication, power constraints at the transmitter limited the maximum signal state photon number. For ds-BB84, however, the optimal secret-key rate will, at most, require $n_s = 1$. Thus, we omit a power constraint on $n_s$ in (4.8).

Figure 4-1 plots $R_{\text{ds-BB84}}(\eta, n_b)$ for a ds-BB84 QKD link operating over a channel with deterministic power transmissivity $\eta$ for a fixed background plus dark count rate $n_b = 10^{-4}$ photons/channel use and modulation rate $R_{\text{mod}} = 10$ Gbps. The most interesting feature of this figure is its showing that the secure-key rate vanishes below $\eta \approx 10^{-3}$ for $n_b = 10^{-4}$ photons/use. This disappearance is because Eve is
able to capture too much of the signal power along the link for $\eta$ values below that threshold. Such thresholding behavior is not found in classical capacities, and leads us to conjecture that it will lead to regimes in which adaptive optics or even BDAO are required to guarantee a non-zero secure-key rate for all turbulence strengths.

4.2.2 Performance bounds for decoy-state BB84

There have been numerous successful free-space implementations of QKD, and those that have most closely approached the secret key rates predicted by theory have implemented BB84 QKD with decoy states [34, 64–66]. In free space, polarization states are an excellent basis on which to encode information because clear weather turbulence is not depolarizing. To minimize losses due to absorption and scattering along a free-space path, QKD links generally transmit at wavelengths of 800 nm or 1064 nm. Thus far, the adaptive optics implemented for these free-space QKD demonstrations have been simplistic. Air-to-ground QKD demonstrations have used tilt-tracking mirrors to sustain a line of sight between the two terminals, forgoing higher secure key rates for the sake of simple transmitter and receiver designs [65, 66], and shorter-haul ground-to-ground QKD demonstrations operating over path lengths on the order of kilometers have generally utilized the same strategy [34, 76].

Despite these attempts to mitigate atmospheric turbulence-induced rate losses, clear-weather turbulence still causes sharp attenuations in the overall power transmissivity $\eta$ of the channel. For example, Erven et al. [34] implemented a ds-BB84 QKD link operating wavelength of $\lambda = 808$ nm over a 1.3 km path between two buildings. They attributed nearly 5 dB of their overall 15 dB loss to beam spreading and breakup despite using 7.5 cm-diameter transmit and receive apertures yielding a Fresnel-number product $D_f \approx 18$. Erven et al. achieved an average secure key rate of 75 kbps, which they were able to increase to 98 kbps by deliberately excluding time frames in which the FSO link experienced deep fades.

Our own theoretical calculations suggest that with full-wave adaptive optics this 5 dB loss could be reduced to 1 dB, which in turn would result in a doubling of the secure key-generation rate to 200 kbps. A 200 kbps rate, unlike a 98 kbps rate, is
above the threshold required to support secure videoconferencing at 128 kbps. Thus, we now turn our attention to developing upper and lower bounds on the ergodic secret key rates of free-space decoy-state BB84 links encoding bits on a single spatial mode in the presence of turbulence for systems that employ: (1) no adaptive optics; (2) receiver-only adaptive optics; (3) full-wave BDAO; and (4) phase-only BDAO. For all that follows, we assume that detectors have unity quantum efficiency, and that the measurements for each polarization basis are perfectly aligned.

We first develop upper and lower bounds on the ergodic secret key rate of a decoy-state BB84 link in single-spatial mode operation \( R_{ds-BB84} \) that can be instantiated from Chapter 2’s \( (\eta_1)^{UB}, (\eta_{hoAO}), \) and \( (\eta_{recAO}) \). For those bounds we need the following lemmas, which are proved in Appendix D.

**Lemma D.1:** For fixed average background plus dark counts \( n_b \), where \( n_b \ll 1 \), and fixed average photon number \( n_s \), the function

\[
\Delta I = \max \left[ 0, \frac{B_{I,n_s}(\eta, n_s, n_b)}{1 - H_2(e_1(\eta, n_s, n_b))} - \frac{B_{I,n_s}(\eta, n_s, n_b)}{H_2(E_{n_s}(\eta, n_s, n_b))} \right] 
\]

is increasing in the overall power transmissivity \( \eta \).

**Lemma D.2:** For fixed average background plus dark counts \( n_b \), where \( n_b \ll 1 \), and fixed average photon number \( n_s \),

\[
S_1(\eta, n_s, n_b) = \frac{B_{I,n_s}(\eta, n_s, n_b)}{1 - H_2(e_1(\eta, n_s, n_b))} 
\]

is convex in \( \eta \).

**Lemma D.3:** For fixed average background plus dark counts \( n_b \), where \( n_b \ll 1 \), fixed average photon number \( n_s \), and \( B_{I,n_s}(\eta, n_s, n_b) \) and \( E_{n_s}(\eta, n_s, n_b) \) defined as in (D.6) and (D.9), the function

\[
S_2(\eta, n_s, n_b) = \frac{B_{I,n_s}(\eta, n_s, n_b)}{H_2(E_{n_s}(\eta, n_s, n_b))} 
\]

is concave in \( \eta \).
Lemma D.4: For a fixed $n_s, n_b > 0$, the unoptimized instantaneous secret key rate $\Delta I(\eta, n_s, n_b)$ in bits per channel use is convex in $\eta$, the power transmissivity of the Alice-to-Bob channel.

With these lemmas in hand, we may state that

$$\Delta I(\eta, n_s, n_b) \leq \eta \Delta I(1, n_s, n_b)$$

(4.12)

since $\Delta I(\eta, n_s, n_b)$ is convex in $\eta$ and $\Delta I(0, n_s, n_b) = 0$. From this result, we have that

$$\max_\eta \Delta I(\eta, x, n_b) \leq \eta \Delta I(1, x, n_b)$$

(4.13)

$$\leq \eta \Delta I(1, x^*_\eta, n_b)$$

(4.14)

where $x^*_\eta$ maximizes $\Delta I(\eta, x, n_b)$ and $x^*_1$ maximizes $\Delta I(1, x, n_b)$. By averaging (4.14) over $\eta$ and multiplying by $R_{\text{mod}}$, we arrive at the following upper bound on $\langle R_{\text{ds-BB84}} \rangle$, the ergodic secure key rate in bits/second when the link operates with modulation rate $R_{\text{mod}}$.

$$\langle R_{\text{ds-BB84}}(\eta, n_b) \rangle \leq \langle \eta \rangle R_{\text{mod}} \Delta I(1, x^*_1, n_b)$$

(4.15)

$$\leq \langle \eta \rangle \UB R_{\text{mod}} \Delta I(1, x^*_1, n_b)$$

(4.16)

$$= \langle \eta \rangle \UB R_{\text{ds-BB84}}(1, n_b)$$

(4.17)

where (4.16) is the further upper bound derived when an $\UB \geq \langle \eta \rangle$ is inserted in (4.15). Now, we derive a lower bound on $\langle R_{\text{ds-BB84}} \rangle$:

$$\langle R_{\text{ds-BB84}}(\eta, n_b) \rangle = \langle R_{\text{mod}} \max_\eta \Delta I(\eta, x, n_b) \rangle$$

(4.18)

$$\geq R_{\text{mod}} \max_\eta \langle \Delta I(\eta, x, n_b) \rangle$$

(4.19)

$$\geq R_{\text{mod}} \max_\eta \Delta I(\eta^L_B, x, n_b)$$

(4.20)
where (4.18) follows from the average of a maximum equaling or exceeding the maximum of an average, and (4.19) follows from Jensen’s inequality. Inequality (4.20) is the further lower bound introduced when a lower bound on $\langle \eta \rangle$, $\langle \eta \rangle^{LB}$, is inserted into (4.19).

Now, we may use $\langle \eta \rangle^{UB}$ in (4.17) and $\langle \eta_{noAO} \rangle$ and $\langle \eta_{recAO} \rangle$ in (4.21) to bound the secret-key rates of an FSO ds-BB84 link from above and below.

### 4.3 Decoy-state BB84 QKD secret-key rates of FSO links operating with BDAO

We now present POPS-simulated results for the ergodic decoy-state BB84 QKD secret-key rate achieved after a BDAO system tracking the power-transfer optimizing spatial mode has reached a steady state for an FSO link with parameters listed in Table 2.3 operating with modulation rate $R_{mod} = 10$ Gbps. We assume that Bob has four identical detectors with average background plus dark count rate $n_b = 10^{-4}$ counts/channel use, which corresponds to detectors experiencing a total background and dark count rate of 1000 kilocounts/second. To evaluate the tightness of our secret-key rate bounds (4.21) and (4.17), we also present the ergodic secret-key rates for links operating with no BDAO and employing either no adaptive optics or receiver-only adaptive optics with these system parameters. Having fixed the parameter $n_b$, we will drop it from the list of arguments in (4.8) so that the secret-key rate equation is simply $R_{ds-BB84}(\eta)$.

Figures 4-2 through 4-4 present both the theoretical upper and lower bounds on the ergodic secret-key rate of a ds-BB84 QKD FSO link with parameters given in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{mod} = 10$ Gbps as well as the ergodic secret-key rates for systems operating with: (1) no adaptive optics and coupling into fiber, $\langle R_{ds-BB84}(\tilde{\eta}_{noAO}) \rangle$; (2) receiver-only adaptive optics, $\langle R_{ds-BB84}(\tilde{\eta}_{recAO}) \rangle$; (3) steady-state full-wave BDAO, $\langle R_{ds-BB84}(\tilde{\eta}_{full}) \rangle$; and (4) steady-state phase-only
Figure 4-2: Moderate turbulence, $\sigma_\chi^2 = 0.137$: Upper and lower bounds on $\langle R_{ds-BB84}(\eta_1) \rangle$ and ergodic ds-BB84 secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{mod} = 10$ Gbps. Circles represent the ergodic secret-key rate with power-in-fiber reception $\langle R_{ds-BB84}(\eta_{noAO}) \rangle$, crosses are the average power-in-aperture secret-key rate $\langle R_{ds-BB84}(\eta_{recAO}) \rangle$. Their corresponding lower bounds $R_{ds-BB84}(\eta_{noAO})$ and $R_{ds-BB84}(\eta_{recAO})$ are plotted as dashed and solid red lines, while the upper bound $\langle R_{ds-BB84}(\eta_{noAO}) \rangle$ and no-turbulence rate lower bound $R_{ds-BB84}(e^{-\alpha L}\eta_{nac})$ are plotted as solid and dashed blue lines. The steady state full-wave and phase-only BDAO ergodic secret-key rates $\langle R_{ds-BB84}(\eta_{full}^{phase}) \rangle$ and $\langle R_{ds-BB84}(\eta_{full}^{phase}) \rangle$ are plotted as stars and squares, respectively.

BDAO, $\langle R_{ds-BB84}(\eta_{full}^{phase}) \rangle$. As we did in Chapters 2 and 3, results for the mild-turbulence case are omitted because the lower and upper bounds are so tight that they assure negligible increases in the secret-key rate from the receiver-only adaptive optics case to the phase-only and full-wave BDAO cases.

Figure 4-2 shows that our lower bound on the secret-key rate for a power-in-fiber receiver is quite tight in moderate turbulence, especially in the near-field Fresnel-number product regime, where $\langle R_{ds-BB84}(\eta_{noAO}) \rangle$, plotted with circles, lies almost directly on top of $R_{ds-BB84}(\eta_{noAO})$, which is plotted as a dashed red line. Assessing the performance of a power-in-fiber receiver for decoy-state BB84-QKD is
valid because commonly-used high-quantum efficiency detectors like superconducting nanowire single-photon detectors (SNSPDs) are typically fiber-coupled rather than free-space coupled [77]. This is because they operate at cryogenic temperatures, thus requiring housing in a cryostat, for which fiber-coupling is preferable. We may assess the degree to which this loss can be eliminated by observing the increase in rate shown by \( \langle R_{ds-BB84}(\eta_{recAO}) \rangle \), which is the ergodic secret-key rate of a ds-BB84 QKD link with a receiver that applies perfect adaptive optics to couple all received power in the aperture leading to the high quantum-efficiency detectors.

For moderate turbulence, \( R_{ds-BB84}(\langle \eta_{recAO} \rangle) \), plotted as a solid red line, is an extremely tight lower bound on \( \langle R_{ds-BB84}(\eta_{recAO}) \rangle \), which is plotted with crosses. \( \langle R_{ds-BB84}(\eta_{recAO}) \rangle \), however, lies almost directly underneath both the ergodic secret-key rates of systems operating with full-wave BDAO, \( \langle R_{ds-BB84}(\eta_{full}) \rangle \), and with phase-only BDAO, \( \langle R_{ds-BB84}(\eta_{phase}) \rangle \). Both of these curves, in turn, lie directly under the ultimate upper bound \( \langle \eta_1 \rangle^UB R_{ds-BB84}(1) \) as well as the lower bound of the no-turbulence ergodic secret-key rate \( R_{ds-BB84}(e^{-\alpha L \eta_1^{vac}}) \). Thus, for moderate turbulence, the bounds provide a very good indication of the actual average secret-key rates. In the far-field and near-unity Fresnel-number product regimes, a power-in-fiber receiver alone is sufficient to achieve a near-optimal average secret-key rate. In the near-field, receiver adaptive optics yields a near-optimal key rate and neither full-wave nor phase-only BDAO systems are necessary.

Figure 4-3 displays the ergodic secret-key rates and secret-key rate bounds in strong turbulence. There is a much greater gap between \( R_{ds-BB84}(\langle \eta_{hoAO} \rangle) \) and \( \langle R_{ds-BB84}(\eta_{hoAO}) \rangle \), which is due to the mismatch between the square-law approximation of the mutual coherence function used to evaluate \( \langle \eta_{hoAO} \rangle \) and the 5/3-law mutual coherence statistics exhibited by the POPS-generated \( \eta_{hoAO} \). For the receiver-only adaptive optics scenario, however, the ergodic secret-key rate \( \langle R_{ds-BB84}(\eta_{recAO}) \rangle \) and its corresponding lower bound \( R_{ds-BB84}(\langle \eta_{recAO} \rangle) \) are still quite close. There is a greater gap between the lower bound \( R_{ds-BB84}(\langle \eta_{recAO} \rangle) \) and the upper bound on secret-key rate \( \langle \eta_1 \rangle^UB R_{ds-BB84}(1) \) than was observed in operation with moderate turbulence. Thus, it is unsurprising that in strong turbulence full-wave and phase-only
Decoy-State BB84 Secret-Key Rates vs. $D_f$

Figure 4-3: Strong turbulence, $\sigma^2 = 1.37$: Upper and lower bounds on $\langle R_{ds-BB84}(\eta_1) \rangle$ and ergodic ds-BB84 secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{mod} = 10$ Gbps. Circles are $\langle R_{ds-BB84}(\hat{\eta}_{noAO}) \rangle$, crosses are $\langle R_{ds-BB84}(\hat{\eta}_{recAO}) \rangle$. Bounds $R_{ds-BB84}(\eta_{recAO})$ and $R_{ds-BB84}(\eta_{noAO})$ are dashed and solid red lines, while $\langle \eta_1 \rangle^{UB} R_{ds-BB84}(1)$ and $R_{ds-BB84}(e^{-\alpha L_{bac}})$ are solid and dashed blue lines. $\langle R_{ds-BB84}(\eta_{full}) \rangle$ and $\langle R_{ds-BB84}(\eta_{phase}) \rangle$ are squares and stars, respectively.
BDAO can provide significant rate improvements for some Fresnel-number product regimes; however, BDAO cannot eliminate scintillation completely and yield ergodic rates that lie very close to $\langle \eta_1 \rangle \text{UB} R_{ds, BB84}(1)$ or $R_{ds, BB84}(e^{-\alpha L \eta_1^{\text{vac}}})$ for all Fresnel-number products. In the far-field, for example, power-in-fiber and power-in-aperture receivers yield almost exactly the same QKD rate, while full-wave and phase-only BDAO offer minimal increases in the ergodic secret-key rate. In the near-field, power in fiber yields very low rates; receiver adaptive-optics pushes the secret-key rate nearly to the upper bound, while incorporating BDAO yields a complete cancellation of scintillation. For near-unity Fresnel-number products, incorporating receiver-only adaptive optics produces nearly an order-of-magnitude increase in secret-key rate from a no-adaptive optics scenario, while the addition of full-wave or phase-only BDAO to the link provides another 5 dB increase in the rate, although it does not approach the upper bound or even the no-turbulence lower bound on the secret-key rate. Thus, in the near-unity $D_f$ regime, BDAO cannot completely mitigate turbulence-induced scintillation.

Figure 4-4 displays the ergodic secret-key rates and secret-key rate bounds in very strong turbulence. The lower bound $R_{ds, BB84}(\langle \eta_{\text{noAO}} \rangle)$ on the ergodic secret-key rate with a power-in-fiber receiver vanishes in strong turbulence because $\langle \eta_{\text{noAO}} \rangle \leq 10^{-3}$; the transmissivity threshold shown in Fig. 4-1 and so cannot be shown in Fig. 4-4. Interestingly, $\langle R_{ds, BB84}(\hat{\eta}_{\text{noAO}}) \rangle$ is nonzero for some $D_f$ because in some iterations, $\hat{\eta}_{\text{noAO}} > 10^{-3}$, thus yielding a small nonzero ergodic secret-key rate. It is clear from the severely diminished $\langle R_{ds, BB84}(\hat{\eta}_{\text{noAO}}) \rangle$ that a FSO link operating in very strong turbulence with no adaptive optics will experience extremely low key rates. While receiver-only adaptive optics greatly increases the achievable ds-BB84 rate, $\langle R_{ds, BB84}(\hat{\eta}_{\text{recAO}}) \rangle$ yields significantly higher secret-key rates at near-field and near-unity Fresnel-number products, but even it diminishes sharply in the far-field. The introduction of full-wave or phase-only BDAO, however, provides a massive, order-of-magnitude increase in the secret-key-rate for all Fresnel-number product regimes, although the introduction of BDAO does not completely eliminate the effects of scintillation.
Decoy-State BB84 Secret-Key Rates vs. $D_f$

Figure 4-4: Very strong turbulence, $\sigma^2 = 13.7$: Upper and lower bounds on $\langle R_{dBs-BB84}(\eta) \rangle$ and ergodic dBs-BB84 secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{mod} = 10$ Gbps. Circles are $\langle R_{dBs-BB84}(\eta\text{hoAO}) \rangle$, crosses are $\langle R_{dBs-BB84}(\eta\text{recAO}) \rangle$. Bounds $R_{dBs-BB84}(\eta\text{hoAO})$ and $R_{dBs-BB84}(\eta\text{recAO})$ are dashed and solid red lines, while $\langle \eta \rangle^{UB} R_{dBs-BB84}(1)$ and $R_{dBs-BB84}(e^{-\alpha L}\eta_{\text{vac}})$ are solid and dashed blue lines. $\langle R_{dBs-BB84}(\eta^\text{full}) \rangle$ and $\langle R_{dBs-BB84}(\eta^\text{phase}) \rangle$ are squares and stars, respectively.
Thus, it is clear that a ds-BB84 QKD link that is required to reliably provide high-secret key rates across all strengths of turbulence must employ either full-wave or phase-only BDAO. Phase-only BDAO may be preferable because of its lower implementation complexity and its providing secret-key rates very close to that of a full-wave BDAO system.

Having addressed the Fresnel-number product regimes and turbulence strengths in which BDAO provides a significant rate increase for ds-BB84 QKD links, we turn our attention to a novel quantum key distribution protocol known as floodlight quantum key distribution (FL-QKD) that can provide much higher secret-key rates in fiber as compared to state-of-the-art QKD systems. In the next chapter, we will see if FL-QKD can provide similar secret-key rate increases in free-space.
Chapter 5

Single-Spatial-Mode Floodlight Quantum Key Distribution through Atmospheric Turbulence

Decoy-state quantum key distribution is not the only way two parties can share information in a secure manner — secure communication can also be implemented via a protocol known as floodlight quantum key distribution (FL-QKD), which was derived from the technique of quantum illumination. Quantum illumination (QI) was originally conceived as a means to improve target-detection performance [78]. In the current version [79] of that protocol, the presence or absence of a target is determined by illuminating the target with a signal field derived from spontaneous parametric down-conversion (SPDC). The receiver then determines whether or not the target is present by performing a joint measurement between the idler retained from the SPDC source and the background plus target (if present) light returned from the region interrogated by the signal. Although the signal and idler produced by SPDC have maximally-entangled quadratures, this entanglement is destroyed by loss and noise along the propagation path between the target region and the receiver, i.e. the return light and the idler are in a joint state that is classical. Nevertheless, the error-probability exponent is better when entangled light is used to illuminate the target instead of classical light of the same average photon number.
Noting this performance increase, Shapiro [80] constructed a two-way protocol for secure communication based on quantum illumination that is immune to passive eavesdropping, in which Eve can only measure light that leaks out of the Alice-to-Bob and Bob-to-Alice channels. This protocol was been successfully implemented in a proof-of-principle experiment over a fiber link [81]. Its secure communication rate against a collective attack by Eve exceeded 300 kbps for a 500 kbps modulation rate despite the presence of an eavesdropper who siphoned off as much as 50% of the power sent from Alice to Bob and 90% of the power sent from Bob to Alice.

Shapiro’s QI secure communication protocol has two significant drawbacks: (1) its performance degrades if idler storage is lossy; and (2) it is vulnerable to active eavesdropping, in which Eve can inject her own light into Bob. Floodlight quantum key distribution (FL-QKD) is a descendant of Shapiro’s QI protocol that solves both of these problems. FL-QKD has been shown to be secure against Eve’s optimum frequency-domain collective attack — which includes both passive and active attacks — and capable of a 2 Gbps secret-key rate over a 50-km-long fiber link [82] when operated with a 10Gbps modulation rate. A preliminary proof-of-principle experiment has demonstrated a 55 Mbps secret-key rate using a 100 Mbps modulation rate over a channel with 10 dB of attenuation, which is equivalent to 50 km of 0.2 dB/km loss fiber [83].

Because of its unprecedented, extraordinarily high secret-key rate over metropolitan-area distance fiber links, as well as its not requiring any multiplexing or technology development to realize that performance, FL-QKD is an extremely attractive candidate for enabling one-time pad encryption of large data files. Our interest is in translating FL-QKD to FSO links, where similar capability would be highly desirable. Thus, our goal is to understand the degree to which BDAO can enable FL-QKD to cope with the ill effects of propagation through atmospheric turbulence. We will begin with an overview of the FL-QKD protocol [82, 83] in the presence of an eavesdropper who mounts the optimum frequency-domain collective attack.
5.1 Overview of the floodlight quantum key distribution protocol

A simple two-way communication protocol in which information is transferred between Alice and Bob may be defined as follows: Alice sends light over a propagation medium to Bob, who then modulates the light with an information-carrying signal and returns it to Alice. A passive eavesdropper Eve can, of course, capture some part of the signals sent between Alice to Bob. An active eavesdropper, in contrast, can inject her own light into Bob’s modulator and make her own measurements in order to spy on the data transferred between Alice and Bob. In this chapter, we will consider an Eve who makes both passive and active attacks as well as the measures that Zhuang et al. [82] require Alice and Bob to implement so that they can thwart Eve’s attack. Modifying these results, we will present secure communication rate bounds on a free-space, single-spatial mode FL-QKD link in the presence of an Eve mounting an optimum frequency-domain collective attack that she realizes as a combined passive plus active attack.

When implementing FL-QKD, Alice uses both a high-brightness, single-spatial mode beam of amplified spontaneous emission (ASE) noise with a $W$ Hz flat bandwidth generated by an optical amplifier, as well as a continuous-wave SPDC source with maximally entangled signal and idler beams and a $W$ Hz phase-matching bandwidth whose signal beam has the same center frequency as her ASE source. In order to monitor the integrity of the channel between herself and Bob, Alice monitors two portions of her light with single-photon detectors (SPDs) that serve as her channel monitors. She sends the idler beam of her SPDC source to the first SPD, uses a beam combiner to merge a very small portion of her ASE source with her SPDC signal light, and sends a small fraction of the combined ASE-SPDC light to another SPD. She then sends the rest of her ASE-SPDC light to Bob. She stores the remainder of her ASE light, which has very high brightness, in a fiber that is delay-matched to the time-of-flight of an Alice-to-Bob-to-Alice round trip and an optical amplifier to mitigate any loss of brightness caused by the fiber. Bob, in turn, sends a small fraction
of his received light to his own single-photon detector, which serves as his channel monitor, and applies binary phase-shift keying (BPSK) modulation and amplification to the remaining light before sending it back to Alice. Alice performs broadband homodyne detection on the light she receives from Bob, using her stored and delayed bright ASE light as her local oscillator (LO).

FL-QKD provides secure communication when Eve makes her optimal frequency-domain collective attack, which is defined as follows. In each duration-\(T\) modulation time bin, Eve performs a general unitary operation on all \(M\) modes traveling from Alice to Bob along with \(K\) of Eve’s own vacuum ancilla states. Eve’s unitary operation is associated with an intrusion parameter \(f_E\), which we define as the perturbation of the phase-sensitive cross-correlation between Alice’s idler and Bob’s received light from what they would experience if Eve had only made a passive attack. After performing the general unitary operation, Eve stores her \(K\) ancilla modes and later makes a collective measurement on the ancillas plus the light she captures from the Bob-to-Alice channel. Eve’s optimum frequency-domain collective attack maximizes her Holevo information for a given photon flux and intrusion parameter \(f_E\). The photon flux and intrusion parameter constraints arise from the statistics Alice and Bob derive from their channel monitors. In particular, their channel monitors afford them a calibration-free measurement of \(f_E\), which determines the secret-key rate they can achieve.

For the SPDC-injection realization of Eve’s optimum frequency-domain collective attack [82], in which Eve injects her own SPDC signal light into the Alice-to-Bob channel while retaining her own idler beam, \(f_E\) equals the fraction of light entering Bob’s terminal that is due to Eve. Alice and Bob’s secret-key rate decreases with increasing \(f_E\). If \(f_E\) is too high, this rate vanishes and they abort the protocol, i.e. they recognize Eve as having mounted a denial-of-service attack. Throughout what follows, we will assume that Eve makes the SPDC-injection attack for ease of discussion, but emphasize that the secret-key rate analysis summarized in this section and originally presented by Zhuang et al. [82] applies to the optimum frequency-domain collective attack performed by Eve.
Our performance metric of interest is Alice’s information advantage over Eve. This information advantage, which converts easily to FL-QKD’s secret-key rate, can be derived from Alice’s probability of error and an upper bound on Eve’s Holevo information. In order to either explicitly calculate or bound these quantities, we require the density operators for the modes collected by Alice and Eve’s receivers when the quantum communication is carried out over an FSO channel.

Alice’s transmitter produces $M$ independent, identically distributed temporal-mode pairs per bit interval. Propagation over the extended Huygens-Fresnel principle model for turbulence from (2.1) will not mix the temporal modes. Thus, we have that Alice and Bob’s conditional density operators given Bob’s message can be found by propagating the initial transmitter annihilation operators for the mode pairs $\{\hat{a}_S, \hat{a}_I\}$, where $1 \leq m \leq M$ through the FL-QKD setup shown in Fig. 5-1. The

![Figure 5-1: A model of FL-QKD between two parties Alice and Bob in the presence of an eavesdropper Eve making an optimal frequency-domain collective attack by using her own SPDC source and a beam splitter. For simplicity, only the $m^{th}$ modes are shown, but modes $1 \leq m \leq M = TW \gg 1$ are employed in the protocol.](image)

protocol as implemented in Figure 5-1 has the following explicit steps.
1. Alice uses an SPDC source to generate entangled signal and idler mode pairs \( \{a_{SM}^{SPDC}, a_{IM}^{SPDC}\} \), each with brightness \( N_{SPDC} \ll 1 \). She uses an ASE source to generate signal-reference mode pairs \( \{a_{SM}^{ASE}, a_{RM}^{ASE}\} \) with average photon numbers \( N_{ASE} = 1 \) and \( N_{LO} \gg 1 \), respectively.

2. Alice sends her SPDC idler modes \( \{a_{IM}^{SPDC}\} \) to an SPD that measures the singles rate \( S_I \) for her idler beam. She combines her SPDC signal modes \( \{a_{SM}^{SPDC}\} \) and ASE signal modes \( \{a_{SM}^{ASE}\} \) with a beam splitter of transmissivity \( \kappa_C \), which results in modes \( \{a_{Am}\} \). Because Alice wants each of these modes to have a signal power \( N_A = \langle a_{Am}^\dagger a_{Am}\rangle \ll 1 \), she sets \( \kappa_C = 1 - nN_A/(n + 1) \) with \( n \gg 1 \) and sets her SPDC brightness \( N_{SPDC} = N_A/(n(1 - N_A) + 1) \).

3. Using a beam splitter with transmissivity \( \kappa_A \), Alice taps off a small fraction \( \kappa_A \) of her combined ASE-SPDC light and sends it to her second SPD that measures singles rate \( S_A \). We denote the vacuum-noise inputs of the beam splitter with annihilation operators \( \{\hat{a}_{Am}\} \). Alice sends the rest of the combined ASE-SPDC light \( \{a_{Sm}\} \) to Bob.

4. As Alice’s transmission travels through the free-space channel with transmissivity \( \eta_{atm} \), Eve captures all photons not received by Bob. Eve also injects the signal light of her own SPDC source with brightness \( N_E = f_E\eta_{atm}N_s/(1 - (1 - f_E\eta_{atm})) \) into the Alice-to-Bob channel via a beam splitter with Alice-to-Bob transmissivity \( \sqrt{1 - f_E}\eta_{atm} \). The light exiting this operation has the annihilation operators \( \{\hat{a}_{Sm}'\} \).

5. Bob receives modes with annihilation operators \( \{\hat{a}_{Sm}'\} \) and uses a beam splitter (with vacuoiseum noise input annihilation operators \( \{\hat{v}_{Bm}\} \)) to direct a small fraction \( \kappa_B \) of the received light to his SPD and measures singles rate \( S_B \). He then applies BPSK modulation at rate \( R_{mod} = 1/T \) to the remainder of the received light \( \{\hat{a}_{Sm}''\} \).

6. The \( \{\hat{a}_{Sm}''\} \) mode are then passed through a phase-insensitive optical amplifier, shown in Fig. 5-1 as an erbium-doped fiber amplifier (EDFA), with gain \( G_B \).
and auxiliary noise modes with operators \( \{\hat{n}_{B_m}\} \). Each of the noise modes results in an amplified spontaneous emission at the amplifier’s output that is in a thermal state with average photon number 
\[
N_B = (G_B - 1)(\langle \hat{n}^\dagger_{B_m} \hat{n}_{B_m} \rangle + 1)
\]
in the resulting output mode \( \hat{a}_{B_m} \).

7. Bob sends the \( \{\hat{a}_{B_m}\} \) back to Alice through the free-space channel with transmissivity \( \eta_{atm} \).

8. Eve performs a collective measurement on (1) all light not received by Bob in the Alice-to-Bob channel, (2) her retained idler light \( \{\hat{a}^{E_{\text{Eve}}}_{B_m}\} \), and (3) all light not received by Alice in the Bob-to-Alice channel (which contains the modulated, amplified version of the SPDC signal light \( \{\hat{a}^{E_{\text{Eve}}}_{S_m}\} \) Eve injected into the Alice-to-Bob channel).

9. Alice receives modes with annihilation operators \( \{\hat{a}'_{B_m}\} \) and measures them via balanced homodyne detection with efficiency \( \eta_{\text{hom}} \) using her reference modes \( \{\hat{a}'_{R_m}\} \) as the LO modes. She also experiences vacuum-noise operators \( \{v_{\pm m}\} \) with the homodyne measurement.

The \( \{\hat{a}'_{R_m}\} \) are the annihilation operators of the original ASE reference mode \( \{\hat{a}^{\text{ASE}}_{R_m}\} \) after Alice applies an optical amplifier with gain \( G_R \) and output ASE \( N_R = G_R \) before delaying the light with a fiber spool of transmissivity \( \kappa_I \) (whose length yields delay equal to that of the round-trip time between the Alice and Bob terminals).

After detecting the \( M \) output modes \( \{\hat{a}'_{B_m}\} \) using the operator \( \hat{N}_{\text{hom}} \) defined below, she performs a hypothesis test on the outcome to decode Bob’s transmitted bit.

10. Alice and Bob also use their channel monitors to measure the \( C_{IA} \) and \( \tilde{C}_{IA} \) (\( C_{IB} \) and \( \tilde{C}_{IB} \)), the time-aligned and time-shifted coincidence rates between Alice’s idler and Alice’s (Bob’s) tap on the transmitted (received) beam, accounting for all necessary propagation delays. Alice and Bob then compute the intrusion
parameter $f_E$ from

$$f_E = 1 - \frac{[C_{IB} - \tilde{C}_{IB}]}{S_B} \bigg/ \frac{[C_{IA} - \tilde{C}_{IA}]}{S_A}.$$  \hspace{1cm} (5.1)

If the intrusion parameter is too high, Alice and Bob abort the protocol.

The operator-valued input-output relations for the annihilation operators in Fig. 5-1 are listed as follows. Also included is Alice’s homodyne-measurement operator.

- $\hat{a}_{Am} = \sqrt{\kappa_C} \hat{a}_{Sm} + \sqrt{1 - \kappa_C} \hat{a}_{Sm}^{ASE}$
- $\hat{a}_{Sm} = \sqrt{1 - \kappa_A} \hat{a}_{Am} + \sqrt{\kappa_A} \hat{v}_{Am}$
- $\hat{a}_{Sm}' = \sqrt{(1 - f_e)\eta_{atm}} \hat{a}_{Sm} + \sqrt{f_E \eta_{atm}} \hat{a}_{E}^{Eve}$
- $\hat{a}_{Sm}'' = \sqrt{1 - \kappa_B} \hat{a}_{Sm}' + \sqrt{\kappa_B} \hat{v}_{Bm}$
- $\hat{a}_{Bm} = (-1)^b \sqrt{G_B} \hat{a}_{Sm}'' + \sqrt{G_B - 1} \hat{n}_{Bm}^\dagger$ for $b \in \{0, 1\}$, where $b$ is Bob’s bit value
- $\hat{a}_{Rm}' = \sqrt{\kappa_I} \left( \sqrt{G_R} \hat{a}_{Rm} + \sqrt{G_R - 1} \hat{n}_{Rm}^\dagger \right) + \sqrt{1 - \kappa_I} \hat{v}_{Rm}$
- $\hat{a}_{\pm m}' = \sqrt{\eta_{hom}} \left( \frac{\hat{a}_{pm} \pm \hat{a}_{Rm}'}{\sqrt{2}} \right) + \sqrt{1 - \eta_{hom}} \hat{v}_{\pm m}$
- $\hat{N}_{hom} = \sum_{m=1}^{M} \left( \hat{a}_{+ m} \hat{a}_{- m} + \hat{a}_{- m} \hat{a}_{+ m} \right)$

### 5.1.1 Alice and Eve’s deterministic-channel receiver performance

We shall now provide a quick review of the derivations of Alice’s error probability and her information advantage over Eve as given by Zhang et al. and Shapiro [80–82] for the communication protocol displayed in Fig. 5-1, where we will take $\eta_{atm}$ to be deterministic.

Alice’s operations on her transmitted signal modes $\{\hat{a}_{Sm}\}$, her SPDC idler modes $\{\hat{a}_{Sm}^{SPDC}\}$, and her ASE reference modes $\{\hat{a}_{Sm}^{ASE}\}$ form $M$ independent, identically distributed mode-triplets that are in zero-mean Gaussian states with Wigner covariance
matrix $A_{SIR}$

$$A_{SIR} = \frac{1}{4} \begin{bmatrix} A_S & C'_{SPDC} & C'_{ASE} \\ C'_{SPDC} & A_{SPDC} & 0 \\ C'_{ASE} & 0 & A_{LO} \end{bmatrix},$$

(5.2)

where $A_S = (2N_s + 1)I_2$, $N_s = (1 - \kappa_A)N_A$, $C'_{SPDC} = \sqrt{(1 - \kappa_A)\kappa_C} C_{SPDC}$,

$$C_{SPDC} = \begin{bmatrix} C_{SPDC} & 0 \\ 0 & -C_{SPDC} \end{bmatrix},$$

(5.3)

$C_{SPDC} = 2\sqrt{N_{SPDC}(N_{SPDC} + 1)}$, $C'_{ASE} = \sqrt{(1 - \kappa_A)(1 - \kappa_C)} C_{ASE}$, $C_{ASE} = 2\sqrt{N_{ASE}N_{LO}}I_2$, and $I_2$ is the $2 \times 2$ identity matrix.

In order to find Alice's error probability and information rate, we require the conditional means and standard deviations associated with Alice's $\hat{N}_{hom}$ measurement given Bob's bit value. The input-output transformations previously listed are linear operations, all of whose inputs, given Bob's bit value, are in zero-mean Gaussian states. By the central limit theorem, Alice's aggregate conditional homodyne measurement statistics over all $M$ modes (where $M \gg 1$) will be Gaussian. Assuming that Bob is equally likely to encode either $b = 1$ or $b = 0$ and that Alice knows the value of $\eta_{atm}$ to implement the optimal hypothesis test when decoding Bob's transmitted bit [81], we get the following expression for Alice's error probability.

$$P_{err}^{Alice} = Q \left( \frac{\mu_b - \mu_0}{\sigma_b + \sigma_0} \right),$$

(5.4)

where $\mu_b$ and $\sigma_b^2$ are the conditional mean and variance, respectively, of Alice's homodyne measurement if Bob transmits bit $b$, and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty du e^{-\frac{u^2}{2}}$ is the tail probability of the standard normal distribution. We can easily calculate $\mu_b$ and $\sigma_b$ by propagating the statistics of Alice's transmitted state through the system detailed in Fig. 5-1. We omit the calculation and state $\mu_b$ and the asymptotic form of $\sigma_b$ assuming $N_{LO} \gg 1$ and $N_B \gg 1$, since these are the conditions under which the
high-rate FL-QKD system will operate.

\[
\begin{align*}
\mu_b &= 2(-1)^b M \eta_{\text{hom}} \eta_{\text{atm}} \sqrt{G_B (1 - \kappa_B)(1 - f_E)(1 - \kappa_A)(1 - \kappa_C) N_{\text{ASE}} N_{\text{LO}}} \\
\sigma_b &\approx \sqrt{2 M \eta_{\text{hom}}^2 \eta_{\text{atm}} N_B N_{\text{LO}}}. 
\end{align*}
\] (5.5)

Alice's Shannon information in bits/channel use is

\[
I_A = (1 - H_2(P_{\text{err}}^{\text{Alice}})),
\] (5.7)

where \( H_2(p) \) is the binary entropy function.

In order to lower bound Alice and Bob's secret-key rate, we require an upper bound on the Holevo information Eve can extract during the optimal collective attack she makes on the \( 3M \) modes accessible to her when Bob transmits a single bit of information. These \( 3M \) modes are composed of the \( M \) modes from Eve's SPDC idler and the \( 2M \) modes she collects from the Alice-to-Bob and Bob-to-Alice channels. Defining \( \hat{\rho}_E^{(b)} \) as Eve's joint density operator for her \( 3M \) modes conditioned on Bob's bit \( b \), Eve's optimal collective attack will result in a Holevo information in bits/channel use

\[
\chi_E = \left[ S(\hat{\rho}_E) - \frac{S(\hat{\rho}^{(0)}_E) + S(\hat{\rho}^{(1)}_E)}{2} \right]
\] (5.8)

where \( \hat{\rho}_E = \frac{1}{2} (\hat{\rho}_E^{(0)} + \hat{\rho}_E^{(1)}) \) is Eve's unconditional joint density operator.

Although \( \hat{\rho}_E \) is zero-mean, it is not Gaussian; thus its von Neumann entropy is difficult to evaluate. Its Wigner covariance matrix, however, is easy to find. Because \( S(\hat{\rho}_E) \leq S(\hat{\rho}_E^{\text{Gauss}}) \), where \( \hat{\rho}_E^{\text{Gauss}} \) is a zero-mean Gaussian state with the same Wigner covariance matrix as \( \hat{\rho}_E \), we can bound (5.8) above by

\[
\chi_E \leq \min \left[ S(\hat{\rho}_E^{\text{Gauss}}) - \frac{S(\hat{\rho}^{(0)}_E) + S(\hat{\rho}^{(1)}_E)}{2}, 1 \right].
\] (5.9)

where the minimization follows is because Bob is using binary modulation.
Zhuang et al. [82] reduced (5.9) to

$$\chi_E \leq \chi_E^{UB} = \min \left[ M(S_G(A_B) + S_G(A_{IS'}) - S_G(A_{IB'}^{(0)})), 1 \right],$$

(5.10)

where $S_G(A)$ is the von Neumann entropy of a Gaussian state with Wigner covariance matrix $A$, $A_B$ is the Wigner covariance matrix of the $\{\hat{a}_{B_m}\}$ modes, $A_{IS'}$ is the joint Wigner covariance matrix of the $\{\hat{a}_{lm}\}$ and $\{\hat{a}_{s_m}'\}$ modes, and $A_{IB'}^{(0)}$ is the joint Wigner covariance matrix of the $\{\hat{a}_{lm}\}$ and $\{\hat{n}_{B_m}'\}$ modes given $b = 0$, with the latter modes being

$$\hat{n}_{B_m}' = \sqrt{G_B - 1} \hat{a}_{s_m}' - \sqrt{G_B} \hat{n}_{B_m}.$$  \hfill (5.11)

The von Neumann entropies of Gaussian quantum states depend solely on the symplectic eigenvalues of their Wigner covariance matrices. The derivation of these symplectic eigenvalues is complicated but is discussed in great detail in the works of Shapiro [80] and Pirandola et al. [84]. Single-mode Gaussian states have a single symplectic eigenvalue, while two-mode Gaussian states have two symplectic eigenvalues. In the case of Eve mounting an optimal collective attack via a beam splitter and injected SPDC light, the symplectic eigenvalues of $A_B$, $A_{IS'}$, and $A_{IB'}^{(0)}$ are

$$\nu_B = (1/4)(2G_B(\eta_{atm}N_s + 1) - 1)$$  \hfill (5.12)

$$\nu_{IS'}^\pm = (1/2) \left( (1 + \eta_{atm})N_s \pm \sqrt{4(1 - f_E)\eta_{atm}N_s(N_s + 1) + (1 - \eta_{atm})^2N_s^2} \right)$$  \hfill (5.13)

$$\nu_{IB'}^{\pm} = (1/2) \left( (1 + (G_B - 1)\eta_{atm})N_s + (G_B - 1) \right.$$
$$\left. \pm \sqrt{4(1 - f_E)\eta_{atm}(G_B - 1)N_s(N_s + 1) + ((G_B - 1)\eta_{atm} - 1)^2N_s^2} \right).$$  \hfill (5.14)

To upper bound $\chi_E$ by $\chi_E^{UB}$, Zhuang et al. assumed that Bob’s amplifier has a quantum-limited ASE noise $N_B = G_B - 1$ in a best-case scenario for Eve. Thus, (5.12) and (5.14) do not have an explicit dependence on $N_B$. In terms of (5.12)-(5.14), the
upper bound in (5.10) becomes
\[
\chi_E^{UB} = \min \left[ M \left( g \left( \frac{4\nu_B - 1}{2} \right) + g \left( \frac{4\nu_{IS'} - 1}{2} \right) + g \left( \frac{4\nu_{IB'} - 1}{2} \right) \right) 
- g \left( \frac{4\nu_{IB'} - 1}{2} \right) - g \left( \frac{4\nu_{IS'} - 1}{2} \right) \right), 1 \right],
\]
(5.15)

Redefining scaled versions of the symplectic eigenvalues \( \tilde{\nu} = \frac{4\nu - 1}{2} \), we rewrite \( \chi_E^{UB} \) as
\[
\chi_E^{UB} = \min (MY_E, 1) \quad (5.16)
\]
\[
Y_E = g(\tilde{\nu}_B) + g(\tilde{\nu}_{IS'}^+) + g(\tilde{\nu}_{IS'}^-) - g(\tilde{\nu}_{IB'}^+) - g(\tilde{\nu}_{IB'}^-) \quad (5.17)
\]

Combining (5.7) and (5.16), we obtain a lower bound on Alice’s information advantage in bits/channel use for FL-QKD operating in a deterministic channel with transmissivity \( \eta_{atm} \).
\[
\Delta I \geq I_A - \chi_E^{UB} \quad (5.18)
\]
\[
= 1 - H_2(P_{err}^{Alice}) - \min (MY_E, 1) \quad (5.19)
\]

Writing an equation for Alice’s information advantage in bits/second in an FLQKD link where Bob’s BPSK modulation rate is \( R_{mod} \) is not as simple as multiplying (5.19) by \( R_{mod} \) as we did in Chapter 4 for the ds-BB84 QKD secret-key rate. For a fixed signal bandwidth \( W \), the number of time-frequency modes \( M = W/R_{mod} \). Thus, the lower bound on Alice’s FL-QKD secret-key rate in a link operating at a modulation rate \( R_{mod} \) with power transmissivity \( \eta_{atm} \) is
\[
R_{mod} \left( 1 - H_2(P_{err}^{Alice}) - \min \left( \frac{W}{R_{mod}Y_E}, 1 \right) \right) \quad (5.20)
\]

The lower bound on Alice and Bob’s secret-key rate is a function of Alice’s signal strength \( N_s \), Bob’s modulation rate \( R_{mod} \), the power transmissivity of the link \( \eta_{atm} \), the transmissivities of Alice’s beam splitters \( \kappa_A \) and \( \kappa_C \), the transmissivity of Bob’s beam splitter \( \kappa_B \), Bob’s EDFA gain \( G_B \), Bob’s EDFA noise \( N_B \), Alice’s signal
bandwidth $W$, Alice’s homodyne measurement efficiency $\eta_{\text{hom}}$, and Eve’s injection fraction $f_E$. We will maximize Alice’s information-advantage lower bound over her source brightness $N_s$ and Bob’s modulation rate $R_{\text{mod}}$, where $R_{\text{mod}}$ is constrained to be no more than a fixed maximum $R_{\text{max}}$ with all other parameters being constant. The resulting optimized secret-key rate lower bound for a deterministic power transmissivity-$\eta_{\text{atm}}$ link is

$$R_{FL}(\eta_{\text{atm}}) = \max_{R_{\text{mod}}; R_{\text{mod}} \leq R_{\text{max}}, N_s} R_{\text{mod}} \left( 1 - H_2(P_{\text{err}}^{\text{Alice}}) - \min \left( \frac{W}{R_{\text{mod}}} \frac{1}{F_{E}}, 1 \right) \right).$$

(5.21)

In order to compare the behavior of FL-QKD’s secret-key rate versus power transmissivity $\eta_{\text{atm}}$ to the secret-key rate behavior of the ds-BB84 QKD protocol, we begin by considering the notional case for FL-QKD operation whose parameters are given in Table 5.1. Fig. 5-2 is a plot of the secret-key rate of an FL-QKD link implemented with these system parameters over a channel with deterministic power transmissivity $\eta_{\text{atm}}$. Interestingly, we do observe the same precipitous drop in rate in the FL-QKD link when the power transmissivity falls under a below a threshold value — in this case, $\eta_{\text{atm}} \approx 6.3 \times 10^{-5}$. What is very interesting about the behavior of FL-QKD’s secret-key rate lower bound versus the rate of the ds-BB84 QKD link shown in Fig. 4-1 is that the FL-QKD secret-key rate is much less sensitive to transmissivity decreases until transmissivity approaches its threshold for a nonzero secret-key rate. More-

<table>
<thead>
<tr>
<th>parameters</th>
<th>values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$W$</td>
<td>2 THz</td>
</tr>
<tr>
<td>$R_{\text{max}}$</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>$G_B = N_B + 1$</td>
<td>$10^4$</td>
</tr>
<tr>
<td>$f_E$</td>
<td>0.01</td>
</tr>
<tr>
<td>$\eta_{\text{hom}}$</td>
<td>0.9</td>
</tr>
<tr>
<td>$\kappa_A$</td>
<td>0.0345</td>
</tr>
<tr>
<td>$\kappa_B$</td>
<td>0.0345</td>
</tr>
<tr>
<td>$\kappa_C$</td>
<td>0.0345</td>
</tr>
</tbody>
</table>

Table 5.1: Parameter values for the notional case of an FL-QKD link selected as a use case for the rest of this thesis.
Figure 5-2: The secret key rate of a FL-QKD channel, $R_{FL}(\eta_{atm})$, versus a deterministic power transmissivity $\eta_{atm}$ for the FL-QKD parameters set in Table 5.1. The kink in the graph at $\eta_{atm} \approx 0.1$ is due to the modulation rate $R_{mod}$ saturating at $R_{max}$ for $\eta_{atm} \geq 0.01$, with $R_{mod} < R_{max}$ otherwise.
over, FL-QKD’s nonzero rate threshold permits an order of magnitude lower power transmissivity than ds-BB84’s nonzero rate threshold, which was $\eta_{\text{atm}} \approx 10^{-3}$. This disparity is not surprising given that BB84’s security hinges on low numbers of signal photons being transmitted across the link, thus rendering the link vulnerable to low transmissivities. The FL-QKD protocol, in contrast, can transmit many more photons per bit interval. Its security depends on Alice transmitting $N_s \ll 1$ photons for each frequency mode, but there are $M \gg 1$ total modes transmitted for each bit interval, making it less susceptible to channel loss in comparison to ds-BB84 QKD.

5.1.2 Performance bounds of FL-QKD

We now turn our attention to deriving lower bounds on FL-QKD’s ergodic secret-key rate for a channel with nondeterministic power transmissivity $\eta_{\text{atm}}$ so that we may bound the secret-key rates of FSO links operating either without adaptive optics or with receiver-only adaptive optics. For assessing the performance of floodlight quantum key distribution through the atmosphere, the quantities we are concerned with are Alice’s turbulence-averaged error probability $\langle P_{\text{err}}^{\text{Alice}} \rangle$ and Alice’s turbulence-averaged information advantage over Eve, $\Delta I = \langle I_A \rangle - \langle \chi_E \rangle$. These averages are taken over the probability distributions of Alice and Eve’s power transmissivities and capture the effect of turbulence-induced fading on the secret-key rate.

We start by considering Alice’s Shannon information in a deterministic channel with transmissivity $\eta_{\text{atm}}$. Assuming $N_B = G_B - 1 \gg 1$, Alice’s error probability is

$$P_{\text{err}}^{\text{Alice}} = Q \left( \sqrt{2M(1 - \kappa_B)(1 - f_E)(1 - \kappa_A)(1 - \kappa_C)N_s\eta_{\text{atm}}} \right). \quad (5.22)$$

The following lemma is proved in Appendix E.

Lemma E.1: Alice's mutual information, $I_A$, is concave in $\eta_{\text{atm}}$ for fixed EDFA gain $G_B$, EDFA noise $N_B$, time-frequency mode number $M = TW$, signal strength per mode $N_s \ll 1$, Bob's tap value $\kappa_B$, and Eve's intrusion parameter $f_E$. 

117
From Lemma E.1 and the fact that \( I_A|_{\eta_{\text{atm}}=0} = 0 \), we have that

\[
I_A \geq \eta_{\text{atm}}(1 - H_2(P_{\text{err}}|_{\eta_{\text{atm}}=1}))
\]

(5.23)

\[
= \eta_{\text{atm}}^2 \left( 1 - H_2 \left( Q \left( \sqrt{2M(1 - \kappa_B)(1 - f_E)(1 - \kappa_A)(1 - \kappa_C)N_s} \right) \right) \right)
\]

(5.24)

\[
= I_A^{LB}(\eta_{\text{atm}})
\]

(5.25)

As a result, the following lower bound on Alice’s ergodic Shannon information holds.

\[
\langle I_A \rangle \geq \langle \eta_{\text{atm}}^2 \rangle (1 - H_2(P_{\text{err}}|_{\eta_{\text{atm}}=1}))
\]

(5.26)

\[
= I_A^{LB}(\langle \eta_{\text{atm}} \rangle)
\]

(5.27)

Turning our attention to deriving an upper bound on Eve’s ergodic Holevo information \( \chi_E^{UB} \), we begin by using the Taylor series approximations valid for \( N_s \ll 1 \) and \( G_B \gg 1 \) of the \( \nu_B, \nu_{IS'}^+, \text{ and } \nu_{IB'}^+ \) defined in (5.12)-(5.14). Then, we define the scaled versions of the Taylor approximations of the symplectic eigenvalues \( \tilde{\nu} = \frac{4\nu - 1}{2} \).

\[
\tilde{\nu}_B = G_B(\eta_{\text{atm}}N_s + 1) - 1
\]

(5.28)

\[
\tilde{\nu}_{IS'}^+ = (N_s\eta_{\text{atm}})^2 (f_E(1 - f_E)) + N_s(1 - (1 - f_E)\eta_{\text{atm}})
\]

(5.29)

\[
\tilde{\nu}_{IS'}^- = (N_s\eta_{\text{atm}})^2 (f_E(1 - f_E)) + N_s(f_E\eta_{\text{atm}})
\]

(5.30)

\[
\tilde{\nu}_{IB'}^+ = N_s(1 - (1 - f_E)\eta_{\text{atm}}) + N_s(1 + \eta_{\text{atm}})
\]

(5.31)

\[
\tilde{\nu}_{IB'}^- = G_B(\eta_{\text{atm}}N_s + 1) - 1 - N_s(1 - (1 + 2f_E)\eta_{\text{atm}})
\]

(5.32)

For these definitions of the symplectic eigenvalues, \( \Upsilon_E \) is a function of \( N_s, G_B, f_E, \) and \( \eta_{\text{atm}} \). Assuming that \( G_B \) and \( f_E \) are fixed system parameters, we will write the function with its two key parameters \( \Upsilon_E(\eta_{\text{atm}}, N_s) \) for the rest of the chapter in order to highlight \( \Upsilon_E \)'s dependence on \( \eta_{\text{atm}} \) and \( N_s \). The following lemma on the behavior of \( \Upsilon_E(\eta_{\text{atm}}, N_s) \), when \( \Upsilon_E(\eta_{\text{atm}}, N_s) \) is evaluated using the Taylor-approximated symplectic eigenvalues defined above, is proved in Appendix D.

**Lemma E.2:** For fixed \( G_B \gg 1, N_s \ll 1, \) and \( 0 \leq f_E \leq 1 \), \( \Upsilon_E(\eta_{\text{atm}}, N_s) \) is concave in \( \eta_{\text{atm}} \).
Using Lemma E.2, we may write an upper bound on \( \langle \chi^U_E \rangle \) as follows.

\[
\langle \chi^U_E \rangle = \min \left( MT_E(\eta_{atm}, N_s), 1 \right)
\]
(5.33)

\[
= \min \left( M \langle T_E(\eta_{atm}, N_s) \rangle, 1 \right)
\]
(5.34)

\[
\leq \min \left( M T_E(\langle \eta_{atm} \rangle, N_s), 1 \right)
\]
(5.35)

\[
= \chi^U_E(\langle \eta_{atm} \rangle)
\]
(5.36)

where inequality (5.35) follows from the concavity of \( T_E \) in \( \eta_{atm} \) and Jensen’s inequality. Combining (5.27) and (5.35), we obtain a lower bound on Alice’s ergodic information advantage over Eve, \( \langle \Delta I \rangle \), in bits/channel use.

\[
\langle \Delta I \rangle = \langle I_A \rangle - \langle \chi_E \rangle
\]
(5.37)

\[
\geq \langle I^L_A \rangle - \langle \chi^U_E \rangle
\]
(5.38)

\[
\geq \langle \eta_{atm} \rangle \left( 1 - H_2(P^\text{Alice}_{\eta_{atm}=1}) \right) - \min \left( M T_E(\langle \eta_{atm} \rangle, N_s), 1 \right)
\]
(5.39)

\[
= I_A^L(\langle \eta_{atm} \rangle) - \chi_E^U(\langle \eta_{atm} \rangle)
\]
(5.40)

Having developed (5.39), we now turn our attention to deriving a lower bound for Alice and Bob’s secret-key-rate \( \langle R_{FL} \rangle \) in bits/second when Alice optimizes her signal brightness \( N_s \) and Bob optimizes his modulation rate \( R_{mod} \) subject to some maximum modulation rate \( R_{max} \), where

\[
\langle R_{FL} \rangle = \max_{R_{mod}:R_{mod} \leq R_{max}, N_s} \left\{ \frac{R_{mod}}{ \frac{W}{R_{mod}} T_E(\eta_{atm}, N_s), 1} \left( 1 - H_2(P^\text{Alice}_{\eta_{atm}=1}) \right) - \min \left( M T_E(\langle \eta_{atm} \rangle, N_s), 1 \right) \right\}
\]
(5.41)

\[
\geq \max_{R_{mod}:R_{mod} \leq R_{max}, N_s} \left\{ \frac{R_{mod}}{ \frac{W}{R_{mod}} T_E(\eta_{atm}, N_s), 1} \left( 1 - H_2(P^\text{Alice}_{\eta_{atm}=1}) \right) - \min \left( M T_E(\langle \eta_{atm} \rangle, N_s), 1 \right) \right\}
\]
(5.42)

\[
\geq \max_{R_{mod}:R_{mod} \leq R_{max}, N_s} \left\{ \frac{R_{mod}}{ \frac{W}{R_{mod}} T_E(\eta_{atm}, N_s), 1} \left( \langle \eta_{atm} \rangle \left( 1 - H_2(P^\text{Alice}_{\eta_{atm}=1}) \right) - \min \left( M T_E(\langle \eta_{atm} \rangle, N_s), 1 \right) \right) \right\}
\]
(5.43)
\[
\max_{R_{\text{mod}}: R_{\text{mod}} \leq R_{\text{max}}, N_s} R_{\text{mod}}(I_A^{\text{LB}}(\eta_{\text{atm}})) - \chi_E^{\text{UB}}(\eta_{\text{atm}}))
\]
\[
= R_{\text{FL}}^{\text{LB}}(\eta_{\text{atm}})
\]

Equation (5.41) follows from the lower bound on the FL-QKD secret-key rate (5.21) for a channel with deterministic \( \eta_{\text{atm}} \). Inequality (5.42) follows from the maximum of an average never exceeding the average of a maximum. Inequality (5.43) employs (5.39) and is the lower bound on the ergodic FL-QKD secret key rate.

## 5.2 Floodlight QKD secret-key rates of FSO links operating with BDAO

We now present POPS-simulated results for the ergodic FL-QKD secret-key rate lower bound achieved after a BDAO system tracking the power-transfer optimizing spatial mode has reached a steady state for an FSO link with parameters listed in Tables 2.3 and 5.1. To evaluate the tightness of our lower bound on the ergodic secret-key rate (5.44), we also present the ergodic secret-key rate lower bounds for links operating with no BDAO and operating either without adaptive optics or with receiver-only adaptive optics.

Figures 5-3 through 5-5 present both the theoretical lower bounds on the ergodic secret-key rate capacity of an FL-QKD FSO link with parameters given in Tables 2.3 and 5.1 as well as the ergodic secret-key rates for systems operating with: (1) no adaptive optics and coupling into fiber, \( R_{\text{FL}}(\hat{n}_{\text{noAO}}) \); (2) receiver-only adaptive optics, \( R_{\text{FL}}(\hat{n}_{\text{recAO}}) \); (3) steady-state full-wave BDAO, \( R_{\text{FL}}(\hat{n}_{\text{full}}) \); and (4) steady-state phase-only BDAO, \( R_{\text{FL}}(\hat{n}_{\text{phase}}) \). As we did in Chapters 2-4, results for the mild-turbulence case are omitted because the lower bounds are so tight to the performance of turbulence-free FL-QKD that they assure minimal secret-key rate increases from the receiver-only adaptive optics case to the phase-only BDAO and full-wave BDAO cases.

In Fig. 5-3, we observe many of the same results we saw in Fig. 4-2, which plotted...
Figure 5-3: Moderate turbulence, $\sigma^2 = 0.137$: Lower bounds on $\langle R_{\text{FL}}(\eta) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. Circles represent the ergodic secret-key rate with power-in-fiber reception $\langle R_{\text{FL}}(\eta_{\text{noAO}}) \rangle$, crosses are the average power-in-aperture secret-key rate $\langle R_{\text{FL}}(\eta_{\text{recAO}}) \rangle$. Their corresponding lower bounds $R_{\text{FL}}^{\text{LB}}(\langle \eta_{\text{noAO}} \rangle)$ and $R_{\text{FL}}^{\text{LB}}(\langle \eta_{\text{recAO}} \rangle)$ are plotted as dashed and solid red lines, while the lower bound $R_{\text{FL}}^{\text{LB}}(\langle \eta \rangle^{\text{UB}})$ in the case of the ultimate power transmissivity and the no-turbulence rate lower bound $R_{\text{FL}}^{\text{LB}}(e^{-\alpha L} \eta_{\text{vac}})$ are plotted as solid and dashed blue lines. The steady state full-wave and phase-only BDAO ergodic secret-key rates $\langle R_{\text{FL}}(\eta_{\text{full}}) \rangle$ and $\langle R_{\text{FL}}(\eta_{\text{phase}}) \rangle$ are plotted as stars and squares, respectively.
the ds-BB84 ergodic secret key rates in moderate turbulence. The primary difference between the two plots is that FL-QKD clearly provides secret-key rates nearly an order of magnitude higher than ds-BB84 QKD can. Figure 5-3 shows that our lower bound on the secret-key rate for a power-in-fiber receiver is quite tight, especially in the near-field Fresnel-number product regime, where $R_{\text{FL}}(\hat{\eta}_{\text{noAO}})$, plotted with circles, lies almost directly on top of $R_{\text{FL}}^{\text{LB}}(\hat{\eta}_{\text{noAO}})$, which is plotted as a dashed red line. For moderate turbulence, $R_{\text{FL}}^{\text{LB}}(\hat{\eta}_{\text{recAO}})$, plotted as a solid red line, is an extremely tight bound to $R_{\text{FL}}(\hat{\eta}_{\text{recAO}})$, which is plotted with crosses. $R_{\text{FL}}(\hat{\eta}_{\text{recAO}})$, however, lies almost directly underneath both the ergodic secret-key rates of systems operating with full-wave BDAO, $R_{\text{FL}}(\hat{\eta}_{\text{full}})$, and with phase-only BDAO, $R_{\text{FL}}(\hat{\eta}_{\text{phase}})$. Both of these curves, in turn, lie directly under the lower bound $R_{\text{FL}}^{\text{LB}}(\hat{\eta}_{1}^{\text{UB}})$ as well as the lower bound of the no-turbulence ergodic secret-key rate $R_{\text{FL}}^{\text{LB}}(\exp(-\alpha_{1}^{\text{vac}}))$. In the far-field and near-unity Fresnel-number product regimes, a power-in-fiber receiver alone is sufficient to achieve the average secret-key rate that could be achieved with full-wave BDAO. In the near-field, receiver adaptive optics yields an average key rate very close to that of full-wave BDAO; thus neither full-wave nor phase-only BDAO systems are required to achieve near-optimal performance in moderate turbulence in the near-field regime.

Figure 5-4 displays the ergodic secret-key rates and secret-key rate bounds in strong turbulence, and shows that in strong turbulence our selected FL-QKD system guarantees secret-key rates nearly two orders of magnitude greater than the secret-key rates guaranteed by employing ds-BB84 QKD. The mismatch between our square-law mutual coherence function used to evaluate $\langle \eta_{\text{noAO}} \rangle$ and the 5/3-law mutual coherence statistics exhibited by the POPS-generated $\hat{\eta}_{\text{noAO}}$ manifests itself as the mismatch in curve shapes between $R_{\text{FL}}^{\text{LB}}(\hat{\eta}_{\text{noAO}})$ and $R_{\text{FL}}(\hat{\eta}_{\text{noAO}})$, as well as $R_{\text{FL}}^{\text{LB}}(\langle \eta_{\text{noAO}} \rangle)$$^{*}$'s drastic underestimation of the FL-QKD rates that can be achieved in the far-field by employing a power-in-fiber receiver. For the receiver-only adaptive optics scenario, however, the ergodic secret-key rate $R_{\text{FL}}(\hat{\eta}_{\text{recAO}})$ and its corresponding lower bound $R_{\text{FL}}^{\text{LB}}(\langle \hat{\eta}_{\text{recAO}} \rangle)$ are still quite close.

There is a greater gap between the lower bound $R_{\text{FL}}^{\text{LB}}(\langle \hat{\eta}_{\text{recAO}} \rangle)$ and the lower bound
Figure 5-4: Strong turbulence, $\sigma^2 = 1.37$: Lower bounds on $\langle R_{FL}(\eta) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. Circles are $\langle R_{FL}(\eta_{hoAO}) \rangle$, crosses are $\langle R_{FL}(\eta_{recAO}) \rangle$. Bounds $R_{FL}^{UB}(\langle \eta_{hoAO} \rangle)$ and $R_{FL}^{UB}(\langle \eta_{recAO} \rangle)$ are dashed and solid red lines, while $R_{FL}^{LB}(\langle \eta \rangle^{UB})$ and $R_{FL}^{LB}(e^{-\alpha L} \eta_{nc})$ are solid and dashed blue lines. $\langle R_{FL}(\eta_{full})^{UB} \rangle$ and $\langle R_{FL}(\eta_{phase})^{UB} \rangle$ are squares and stars, respectively.
on secret-key rate $R_{FL}^{LB}(\langle \eta \rangle_{UB})$. Thus, it is unsurprising that in strong turbulence full-wave and phase-only BDAO can provide significant rate improvements for some Fresnel-number product regimes; however, BDAO cannot eliminate scintillation completely and yield ergodic rates that lie very close to $R_{FL}^{LB}(\langle \eta \rangle_{UB})$ and $R_{FL}^{LB}(e^{-\alpha L}n_{vac})$ for all Fresnel-number products. In the far-field, for example, power-in-fiber and power-in-aperture receivers yield almost exactly the same secret-key rate, while full-wave and phase-only BDAO offer minimal increases in the ergodic secret-key rate. In the near-field, power in fiber yields very low rates; receiver adaptive-optics pushes the secret-key rate nearly to the key rate of a channel without turbulence, while incorporating BDAO yields a complete elimination of scintillation. In the near-unity Fresnel-number product regime, incorporating receiver-only adaptive optics produces a one to two order of magnitude increase in secret-key rate from a no-adaptive optics scenario, while the addition of full-wave or phase-only BDAO to the link provides another 4 dB increase in the rate, although it does not approach the no-turbulence lower bound on the secret-key rate.

Figure 5-5 displays the ergodic secret-key rates and secret-key rate bounds in very strong turbulence. The lower bound $R_{FL}^{LB}(\langle \eta_{noAO} \rangle)$ on the ergodic secret-key rate with a power-in-fiber receiver vanishes in strong turbulence because $\langle \eta_{noAO} \rangle \leq 6.3 \times 10^{-5}$, the nonzero-rate transmissivity threshold shown in Fig. 5-2. $\langle R_{FL}(\hat{\eta}_{noAO}) \rangle$, however, does yield a nonzero secret-key rate due to small fraction of realizations of $\hat{\eta}_{noAO} \geq 6.3 \times 10^{-5}$, the nonzero-rate threshold. Moreover, $\langle R_{FL}(\hat{\eta}_{noAO}) \rangle$ is nearly an order of magnitude greater than $\langle R_{ds-BB84}(\hat{\eta}_{noAO}) \rangle$ displayed in Fig. 4-4. As was the case in the analysis of ergodic ds-BB84 QKD secret-key rates, incorporating full-wave receiver adaptive optics greatly increases the accessible secret-key rate of the FSO FL-QKD link operating in very strong turbulence. Moreover, unlike the ds-BB84 QKD curves in Fig. 4-4, Fig. 5-5 makes it clear that $R_{FL}^{LB}(\langle \hat{\eta}_{recAO} \rangle)$ is a very good lower bound on $\langle R_{FL}(\hat{\eta}_{recAO}) \rangle$. Finally, we see that the lower bounds on achievable secret-key rates of FSO FL-QKD operating with full-wave BDAO, $\langle R_{FL}(\hat{\eta}_{full}) \rangle$, are nearly an order of magnitude higher than $\langle R_{FL}(\hat{\eta}_{recAO}) \rangle$ and that the rate lower bound of an FL-QKD link employing phase-only BDAO, $\langle R_{FL}(\hat{\eta}_{phase}) \rangle$, lies almost directly underneath it.
Figure 5-5: Very strong turbulence, $\sigma^2 = 13.7$: Lower bounds on $\langle R_{FL}(\eta_1) \rangle$ and ergodic FL-QKD secret-key rates vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 and Table 5.1. Circles are $\langle R_{FL}(\tilde{\eta}_{noAO}) \rangle$, crosses are $\langle R_{FL}(\tilde{\eta}_{recAO}) \rangle$. Bounds $R_{FL}^{LB}(\tilde{\eta}_{noAO})$ and $R_{FL}^{LB}(\tilde{\eta}_{recAO})$ are dashed and solid red lines, while $R_{FL}(\eta_1)^{UB}$ and $R_{FL}(e^{-\alpha L} \eta_1^{vac})$ are solid and dashed blue lines. $\langle R_{FL}(\tilde{\eta}_1^{full}) \rangle$ and $\langle R_{FL}(\tilde{\eta}_1^{phase}) \rangle$ are squares and stars, respectively.
\( \langle R_{FL}(\hat{\eta}_I^{\text{full}}) \rangle \) and \( \langle R_{FL}(\hat{\eta}_I^{\text{phase}}) \rangle \) begin to approach the lower bound of an FL-QKD link without turbulence, \( R_{FL}^{LB}(e^{-\alpha L \eta_{\text{vac}}} \rangle \), in the near-field Fresnel-number product regime. Thus, BDAO achieves near-elimination of scintillation in the near-field in very strong turbulence. Outside of the near-field, BDAO still affords order-of-magnitude increases in secret-key rate from a system operating with receiver-only adaptive optics.

We have shown that the FL-QKD protocol offers multiple-order of magnitude rate increases over ds-BB84 QKD in a free-space link over a wide range of turbulence strengths and Fresnel-number products. Moreover, we have shown that the addition of receiver-only adaptive optics yields large increases in rate for strong or weaker turbulence. In the near-unity and near-field regime in strong turbulence, full-wave or phase-only BDAO is required to reach scintillation-free performance. In very strong turbulence, BDAO is required to retain very high key rates that are at least a hundredth of the modulation rate. Applying phase-only BDAO, with its lower implementation complexity, yields nearly the same results as full-wave BDAO. Thus, we state that an FSO link employing FL-QKD with phase-only BDAO optics will provide highly reliable high-secret key rates for all strengths of turbulence.

In Chapters 3–5 we have only addressed single-spatial-mode systems. Recent work on FSO communications — both classical and quantum — has turned to spatial-division-multiplexing, i.e., multi-spatial-mode systems, in the quest for higher-rate capabilities [85–87]. So, in the next chapter, we provide the mathematical framework for determining whether classical and quantum FSO communications would benefit from BDAO multi-spatial mode operation.
Chapter 6

Communication with multiple spatial modes in atmospheric turbulence

So far, we have only considered single-spatial-mode free-space optical links. We have shown, however, that $D_f$ orthogonal spatial input-output eigenmode pairs per polarization with transmissivities near the $e^{-\alpha L}$ extinction limit exist for $D_f \gg 1$. It follows that there are $D_f$ orthogonal channels along which to transmit information in the near-field regime, making it a particularly attractive region for extremely high-rate communication. In this chapter, we summarize results from Chandrasekaran et al. [88, 89] that bound the ultimate rates of classical communication in the near-field regime, and we add new multi-spatial-mode results for ds-BB84 and FL-QKD systems.

Very little was known about the near-field instantaneous power transfers $\{\eta_m\}$ discussed in Chapter 2 until [88, 89], which provided system designs for multiple spatial-mode transmission and reception with and without the use of adaptive optics. These papers developed bounds on average power transmissivities from which we obtained bounds on the ergodic capacities for multiple-spatial-mode classical communications using specific transmitter mode sets with or without adaptive optics. In the sections that follow, we will first reprise these results and then present
the ergodic secret-key rate bounds for multiple-spatial-mode ds-BB84 and FL-QKD with and without adaptive optics.

6.1 \( M \)-spatial-mode links with and without adaptive optics

The best high-photon information efficiency (PIE = bits/photon), high-spectral efficiency (SE = bits/sec-Hz) communication performance through atmospheric turbulence in an \( M \)-spatial-mode link results from near-field operation with a transmitter that tracks and employs the \( M \) input spatial modes, \( \Phi_1(\rho), \ldots, \Phi_M(\rho) \), whose power-transfer eigenvalues are the highest. Implementing such a system, however, would be quite demanding when \( M \gg 1 \). So we shall consider a simpler transmitter that uses a fixed set of \( M \) orthonormal input modes

\[
\Phi^{(0)}(\rho) = \begin{bmatrix}
\Phi^{(0)}_1(\rho) & \Phi^{(0)}_2(\rho) & \cdots & \Phi^{(0)}_M(\rho)
\end{bmatrix}^T,
\]

for \( \rho \in \mathcal{A}_T \),

where \( ^T \) denotes transpose, and the superscripts are meant to distinguish this fixed mode set from the atmosphere’s input spatial eigenmodes \( \{\Phi_m(\rho)\} \). Moreover, we will take this mode set to approximate the vacuum-propagation input modes that have the highest associated power transfers, arranged in nonincreasing power-transfer order. The transmitter encodes and sends information to the receiver via the \( z = 0 \) plane complex envelope

\[
E_0(\rho, t) = E^T_{\text{in}}(t) \left( U\Phi^{(0)}(\rho) \right) \\
= E^T_{\text{in}}(t)\Psi^{(0)}(\rho) \\
= \sum_{m=1}^M E_{\text{in}_m}(t)\Psi^{(0)}_m(\rho)
\]
where

\[ E_{\text{in}}(t) = \begin{bmatrix} E_{\text{in}1}(t) & E_{\text{in}2}(t) & \cdots & E_{\text{in}M}(t) \end{bmatrix}^T, \]

(6.5)
is the set of temporal waveforms applied to the \( M \) spatial modes \( \{\Psi_m^{(0)}(\rho)\} \), and \( U \) is the \( M \times M \) unitary transform that generates \( \{\Psi_m^{(0)}(\rho)\} \) so that they are the linear combinations of the \( \{\phi_m^{(0)}(\rho)\} \) chosen such that the corresponding received spatial patterns, \( \{\psi_m(\rho') : 1 \leq m \leq M\} \), have minimal crosstalk at the receiver, as described below. The selection of \( U \) will depend on the way in which the receiver extracts the spatially-multiplexed information from the received field \( E_L(\rho', t) \). So, we introduce two candidate receivers — one which employs full-wave adaptive optics, and one which does not.

Transmission of the spatial mode \( \Phi_m^{(0)}(\rho) \) from the transmitter pupil \( A_T \) gives rise to reception of the spatial pattern

\[ \zeta_m(\rho') = \int_{A_T} d\rho \, h(\rho', \rho) \Phi_m^{(0)}(\rho), \]

(6.6)

for \( \rho' \) in the receiver pupil \( A_R \). The collection of these \( M \) spatial patterns is, in general, random, owing to the random nature of the turbulent channel’s Green’s function. The two candidate receivers must extract the information embedded in the received field,

\[ E_L(\rho', t) = E_{\text{in}}^T(t - L/c) U \zeta(\rho'), \]

(6.7)

where

\[ \zeta(\rho') = \begin{bmatrix} \zeta_1(\rho') & \zeta_2(\rho') & \cdots & \zeta_M(\rho') \end{bmatrix}^T. \]

(6.8)
The first uses ideal (full-wave) adaptive optics to extract \( M \) orthonormal modes from the vector space of spatial patterns spanned by \( \{\zeta_m(\rho') : 1 \leq m \leq M, \rho' \in A_R,\} \). The second extracts a fixed set of orthonormal modes

\[ \phi^{(0)}(\rho') = \begin{bmatrix} \phi_1^{(0)}(\rho') & \phi_2^{(0)}(\rho') & \cdots & \phi_M^{(0)}(\rho') \end{bmatrix}^T, \]

(6.9)

for \( \rho' \in A_R \).
where the superscripts are meant to distinguish this fixed mode set from the atmosphere's instantaneous output modes, \( \{ \phi_m(\rho') \} \). For both of the preceding receivers we shall assume that the receiver and the transmitter know the resulting power-transfer behavior and that they use this information to eliminate crosstalk by appropriate choice of the unitary matrix \( U \). This elimination will allow each system to realize a set of \( M \) independent parallel channels and achieve their ergodic capacities.

Power transmissivities for the chosen transmitter modes and receiver mode-extraction approach are obtained as follows. For the adaptive optics receiver, we define a channel function

\[
H_{ad}(\rho') = \zeta^T(\rho'),
\]

(6.10)

so that the received field is given by

\[
E_L(\rho', t) = H_{ad}(\rho') U^T E_{in}(t - L/c).
\]

(6.11)

The power-transfer eigenvalues, \( \{ \mu_m^{ad} : 1 \leq m \leq M \} \), that determine the ergodic capacities for the adaptive optics system are therefore those of the \( M \times M \) Hermitian matrix

\[
K_{ad} = \int_{A_R} d\rho' H_{ad}^T(\rho') H_{ad}(\rho'),
\]

(6.12)

where \( \dagger \) denotes conjugate transpose. Moreover, the transmitter should use the unitary matrix \( U_{ad} \), satisfying

\[
U_{ad}^T = \sum_{m=1}^M \theta_m^{ad} 1_m^T
\]

(6.13)

where \( 1_m^T \) is the \( 1 \times M \)-dimensional vector with 1 in its \( m^{th} \) place and zeros elsewhere, and the \( \{ \theta_m^{ad} : 1 \leq m \leq M \} \) are the normalized eigenvectors of \( K_{ad} \) with the \( M \) highest eigenvalues \( \mu_1^{ad} \geq \mu_2^{ad} \geq \cdots \geq \mu_M^{ad} \).

Turning now to the receiver that extracts the fixed mode set \( \phi^{(0)}(\rho') \), we have that this receiver obtains

\[
E_{out}(t) = H_{non} U^T E_{in}(t - L/c),
\]

(6.14)
after mode extraction, where the channel matrix $H_{\text{non}}$ is

$$H_{\text{non}} = \int A \right(0^* (p')H_{\text{ad}}(p') \right)$$

(6.15)

We will refer to the $mn^{th}$ element of $H_{\text{non}}$ as $h_{mn}^{\text{non}}$. The power-transfer eigenvalues, $\{ \mu_{\text{non}}^m : 1 \leq m \leq M \}$, that determine the ergodic capacities for the system without adaptive optics are therefore those of the $M \times M$ Hermitian matrix

$$K_{\text{non}} = H_{\text{non}}^* H_{\text{non}}.$$  

(6.16)

In this case, the transmitter should use the unitary matrix $U_{\text{non}}$ satisfying

$$U_{\text{non}}^T = \sum_{m=1}^{M} \theta_{m}^{\text{non}} 1_m^T$$

(6.17)

where the $\{ \theta_{m}^{\text{non}} : 1 \leq m \leq M \}$ are the normalized eigenvectors of $K_{\text{non}}$ with the $M$ highest eigenvalues $\mu_1^{\text{non}} \geq \mu_2^{\text{non}} \geq \cdots \geq \mu_M^{\text{non}}$. If the transmitter and receiver with no adaptive optics did not compensate for turbulence-induced crosstalk to achieve the optimal ergodic capacity, the strength of the instantaneous intermodal crosstalk between the $n^{th}$ transmitted mode and $m^{th}$ element of $\phi^{(0)}(p')$ would be $|h_{mn}^{\text{non}}|^2$.

In general, the eigenvalues for the adaptive and non-adaptive mode extraction cases will be random, just like the $\{ \eta_m : 1 \leq m < \infty \}$ discussed in Chapter 2. Before attempting to characterize the statistics of the $\{ \mu_{m}^{\text{ad}} \}$ and the $\{ \mu_{m}^{\text{non}} \}$, which we will undertake in the next section, it is worth noting the following majorization results,

$$\sum_{m=1}^{K} \eta_m \geq \sum_{m=1}^{K} \mu_{m}^{\text{ad}} \geq \sum_{m=1}^{K} \mu_{m}^{\text{non}}, \text{ for } 1 \leq K \leq M,$$

(6.18)

where each set of eigenvalues has been arranged in nonincreasing order. These results are immediate consequences of the increasing constraints on the input and output mode sets as one goes from the $\{ \eta_m \}$ to the $\{ \mu_{m}^{\text{ad}} \}$ to the $\{ \mu_{m}^{\text{non}} \}$.
6.2 Power transmissivity and crosstalk statistics of an $M$-spatial mode link

We need bounds on the power transmissivities of the $M$-spatial mode systems in order to evaluate the prospects of optical communication with high photon and spectral efficiency over an $L$-m long line-of-sight path through turbulence. For single-spatial mode operation, (3.7) was used to bound the ergodic capacities of free-space optical communication links with different degrees of adaptive optics from bounds on the ensemble average of the single-mode power transmissivity $\langle \eta_1 \rangle$. It follows that bounds on the multiple-spatial mode ergodic channel capacities with and without adaptive optics should be obtainable from bounds on the ensemble averages of the power transmissivities $\{\mu^{\text{ad}}_m\}$ and $\{\mu^{\text{non}}_m\}$.

The power-transfer bounds we will need are obtainable from the ensemble-averaged matrices $\langle K_{\text{ad}} \rangle$ and $\langle K_{\text{non}} \rangle$, as is a bound on the average intermodal crosstalks $\{\langle |h_{mn}^{\text{non}}|^2 \rangle \}$ of a system without adaptive optics. The $mn^{\text{th}}$ elements of $\langle K_{\text{ad}} \rangle$ and $\langle K_{\text{non}} \rangle$ are

$$\langle K_{\text{ad}} \rangle_{mn} = \int_{\mathcal{A}_R} d\rho' \int_{\mathcal{A}_T} d\rho_1 \int_{\mathcal{A}_T} d\rho_2 \Phi_m^{(0)}(\rho_1) \times \langle h^*(\rho', \rho_1) h(\rho', \rho_2) \rangle \Phi_n^{(0)}(\rho_2),$$

and

$$\langle K_{\text{non}} \rangle_{mn} = \sum_{k=1}^M \int_{\mathcal{A}_R} d\rho'_1 \int_{\mathcal{A}_R} d\rho'_2 \int_{\mathcal{A}_T} d\rho_1 \int_{\mathcal{A}_T} d\rho_2 \times \phi_k^{(0)}(\rho'_1) \phi_k^{(0)*}(\rho'_2) \langle h^*(\rho'_1, \rho_1) h(\rho'_2, \rho_2) \rangle \times \Phi_m^{(0)*}(\rho_1) \Phi_n^{(0)}(\rho_2),$$

while the average strength of the $mn^{\text{th}}$ element of $H_{\text{non}}$ is

$$\langle |h_{mn}^{\text{non}}|^2 \rangle = \int_{\mathcal{A}_R} d\rho'_1 \int_{\mathcal{A}_R} d\rho'_2 \int_{\mathcal{A}_T} d\rho_1 \int_{\mathcal{A}_T} d\rho_2$$
\[
\times \phi_m^{(0)}(\rho_1)\phi_m^{(0)*}(\rho_2)\langle h^*(\rho_1', \rho_1)h(\rho_2', \rho_2) \rangle \\
\times \Phi_n^{(0)*}(\rho_1)\Phi_n^{(0)}(\rho_2).
\] (6.21)

The only turbulence statistic needed to evaluate the ensemble-averaged matrices \( \langle K_{ad} \rangle \) and \( \langle K_{non} \rangle \) is the mutual coherence function of the Green’s function. By evaluating \( \langle K_{ad} \rangle \) and \( \langle K_{non} \rangle \), we can diagonalize them to obtain their respective eigenvalues, \( \{ \gamma_{m}^{ad} : 1 \leq m \leq M \} \) and \( \{ \gamma_{m}^{non} : 1 \leq m \leq M \} \), which we arrange in nonincreasing order. Because the ensemble-averaged eigenvalues of a random \( M \times M \) Hermitian matrix majorize the deterministic eigenvalues of the ensemble average of that matrix [90], we have that

\[
\sum_{m=1}^{K} \langle \mu_m^{ad} \rangle \geq \sum_{m=1}^{K} \gamma_{m}^{ad}, \text{ for } 1 \leq K \leq M,
\] (6.22)

and

\[
\sum_{m=1}^{K} \langle \mu_m^{non} \rangle \geq \sum_{m=1}^{K} \gamma_{m}^{non}, \text{ for } 1 \leq K \leq M.
\] (6.23)

### 6.3 Rate bounds for \( M \)-spatial mode FSO classical communication links

We now sketch the proof (given in detail in [89]) that the power-transmissivity majorization relations allow us to bound the ergodic Holevo capacities of an \( M \)-spatial mode link operating with or without adaptive optics. The Holevo capacity, in bits per channel use, of a deterministic, pure-loss, \( M \) spatial-mode optical channel whose transmitter constrained to at most \( N_T \) photons on average is [91]

\[
C_{\text{hol}, M}(\mu, N_T) = \max_{N: \sum_{m=1}^{M} N_m = N_T} \sum_{m=1}^{M} g(\mu_m N_m),
\] (6.24)

where \( N = [N_1, N_2, \ldots, N_M] \) is the vector of average photon numbers used for the \( M \) modes, the \( \{\mu_m\} \) are the modal transmissivities (arranged in nonincreasing
order), and \(g(\mu N)\) from (3.4) is the Holevo capacity of a single mode channel with transmissivity \(\mu\) and average photon-number \(N\).

The ergodic capacity of an \(M\) spatial-mode system operating through the turbulent channel is then

\[
(C_{\text{hol},M}(\mu, N_T)) = \left\langle \max_{N: \sum_{m=1}^{M} N_m = N_T} \sum_{m=1}^{M} g(\mu_m N_m) \right\rangle,
\]

(6.25)

where \(\mu\) denotes the \(\{\mu_m\}\) and throughout this section \(\mu_m = \mu_m^{\text{ad}} (\mu_m^{\text{non}})\) for the system that does (does not) employ adaptive optics.

An upper bound on the ergodic Holevo capacities is easily obtained. Because \(g(\mu N)\) is monotonically increasing with increasing argument as seen in Table 3.1, setting all \(M\) power-transfer eigenvalues to the extinction-loss limited upper bound given in (2.23) immediately yields the bound

\[
(C_{\text{hol},M}(\mu, N_T)) \leq Mg(e^{-\alpha L}N_T/M),
\]

(6.26)

which applies to adaptive and non-adaptive receivers.

We now derive a lower bound on the ergodic Holevo capacity for adaptive and non-adaptive operation. The maximum of an average cannot exceed the average of a maximum. So, we have

\[
(C_{\text{hol},M}(\mu, N_T)) \geq \max_{N: \sum_{m=1}^{M} N_m = N_T} \sum_{m=1}^{M} \left\langle g(\mu_m N_m) \right\rangle.
\]

(6.27)

We claim that

\[
(C_{\text{hol},M}(\mu, N_T)) \geq \max_{N: \sum_{m=1}^{M} N_m = N_T} \sum_{m=1}^{M} \langle \mu_m \rangle g(N_m),
\]

(6.28)

i.e., these capacities can be bounded from below using knowledge of the \(\{\langle \mu_m \rangle\}\). We prove this by noting that the single-mode Holevo capacity \(g(\mu N)\) is concave in \(\mu\) for fixed \(N\) and that \(g(0) = 0\). It follows that \(\langle g(\mu N) \rangle \geq \langle \mu \rangle g(N)\), which allows us to arrive at (6.28) for \(C_{\text{hol},M}(\mu, N_T)\). To obtain a bound that we can evaluate, we will
use majorization to show that (6.28) implies

\[ C_{\text{hol},M}(\mu, N_T) \geq \max_{N: \sum_{m=1}^{M} N_m = N_T} \sum_{m=1}^{M} \gamma_m g(N_m) \]

\[ = C_{\text{hol},M}^{\text{LB}}(\gamma, N_T), \quad (6.29) \]

where \( \gamma \) denotes the \( \{\gamma_m : 1 \leq m \leq M\} \). To prove this result, it suffices to demonstrate that, for \( N \) achieving the maximum in (6.29),

\[ \sum_{m=1}^{M} ((\mu_m) - \gamma_m) g(N_m) \geq 0. \quad (6.30) \]

Rearranging terms in (6.30) we can write

\[
\begin{align*}
\sum_{m=1}^{M} ((\mu_m) - \gamma_m) g(N_m) & = \left[ \sum_{m=1}^{M} ((\mu_m) - \gamma_m) \right] g(N_M) \\
& + \left[ \sum_{m=1}^{M-1} ((\mu_m) - \gamma_m) \right] [g(N_{M-1}) - g(N_M)] \\
& + \cdots \\
& + \left[ \sum_{m=1}^{M-k} ((\mu_m) - \gamma_m) \right] [g(N_{M-k}) - g(N_{M-k+1})] + \cdots \\
& + \left[ (\mu_1) - \gamma_1 \right] [g(N_1) - g(N_2)]. \quad (6.31)
\end{align*}
\]

We know that \( g(\cdot) \) is a monotonically increasing, non-negative function of its argument. Lagrange-multiplier optimization yields the choice of \( N \), which we shall call \( N^* \), that achieves the lower bound \( C_{\text{hol},M}^{\text{LB}}(\gamma, N_T) \) given in (6.29) for \( C_{\text{hol},M}(\mu, N_T) \). The \( \{N^*_m\} \) are

\[ N^*_m = \frac{1}{\exp(\beta/\gamma_m) - 1}, \quad (6.32) \]

where \( \beta \) is chosen so that \( \sum_{m=1}^{M} N^*_m = N_T \), and \( \gamma_m = \gamma_m^{\text{ad}} (\gamma_m^{\text{non}}) \) when the receiver uses (does not use) adaptive optics. Because the \( \{\gamma_m\} \) are nonincreasing with increasing \( m \), the elements of \( N^* \) also have this property. Therefore, in (6.31), we have \( g(N_M) \geq 0 \) and \( g(N_{M-k}) - g(N_{M-k+1}) \geq 0 \) for \( 1 \leq k \leq M - 1 \). The inequality in (6.30)
then follows immediately from the \( \{ \gamma_m \} \) being majorized by the \( \{ (\mu_m) \} \), and so we obtain the desired lower bounds on the ergodic Holevo capacities for adaptive and non-adaptive operation.

To exhibit the potential performance of \( M \)-spatial-mode communication through turbulence, we will evaluate our bounds for the square-pupil setup shown in Fig. 2-1 with \( d_T = d_R = d = 49.5 \text{ cm} \) and parameters given in Table 2.3 (yielding a Fresnel-number product \( D_f \approx 250 \)). Table 2.1 lists the turbulence strengths considered as well as their corresponding spherical-wave coherence lengths \( \rho_0 \) and the weak-perturbation (Rytov-theory) spherical-wave logamplitude variance \( \sigma^2_\chi \) from (2.19).

Because the transmit and receive pupils are appreciably larger than the turbulence coherence length for the case of moderate or stronger turbulence, we can expect that significant beam spread and angle-of-arrival spread will occur. Likewise, the spherical-wave logamplitude variance for those turbulence strengths implies that there will be considerable scintillation. Thus, to ward off some of the ill effects of these turbulence-induced deteriorations, we shall only employ \( M = 169 \) transmitter modes in our calculations, choosing those that achieve the best power transfers under vacuum-propagation conditions.

We consider the focused-beam modes

\[
\phi_{n_x,n_y}^{(0)FB}(\rho) = \frac{\exp[-ik(x^2 + y^2)/2L + i2\pi(n_xx + n_yy)/d]}{d}
\]

for \( -\frac{\sqrt{M-1}}{2} \leq n_x, n_y \leq \frac{\sqrt{M-1}}{2} \).

for \( \rho \in \mathcal{A}_T \), where \( \rho = (x, y) \) in Cartesian coordinates. These modes are orthonormal on \( \mathcal{A}_T \) in the \( z = 0 \) plane, focused on the \( z = L \) plane, and have phase tilts — indexed by \( n_x \) and \( n_y \) — such that their orthogonality is very nearly preserved in vacuum propagation because \( D_f = 250 \). It is these vacuum-propagation \( z = L \) patterns that

---

1. We note that indexing the modes in this way does imply a constraint on the chosen \( M \) - in order to ensure that \( \frac{\sqrt{M-1}}{2} \) will be an integer, we stipulate that the number of spatial modes \( M = (2k+1)^2 \), where \( k > 0 \) and is an integer. For \( M = 169 \), this requirement is satisfied and \( \frac{\sqrt{M-1}}{2} = 6 \).

2. For the \( M = 169 \) FB mode set, the maximum power of a given mode \( m \) extracted to incorrect modes \( n \neq m \), \( \sum_{n=1}^{169} |h_{mn}|^2 \), is 0.0995 out of unity in vacuum.
our non-adaptive receiver will extract,

\[
\phi_{n_x n_y}^{(0),FB}(\rho') = \frac{\sqrt{D_f}}{d} e^{i k (x'^2 + y'^2) / 2L} \frac{\sin[\pi (\sqrt{D_f x' / d - n_x})]}{\pi (\sqrt{D_f x' / d - n_x})} \\
\times \frac{\sin[\pi (\sqrt{D_f y' / d - n_y})]}{\pi (\sqrt{D_f y' / d - n_y})}, \text{ for } -\frac{\sqrt{M-1}}{2} \leq n_x, n_y \leq \frac{\sqrt{M-1}}{2},
\]

for \( \rho' \in \mathcal{A}_R \), where \( \rho' = (x', y') \) in Cartesian coordinates.

In Fig. 6-1 we have plotted the \( \{\gamma_m^{ad}\} \) and the \( \{\gamma_m^{non}\} \) versus \( m \) under no, mild, moderate, strong, and very strong turbulence for our FB mode set, and in Fig. 6-2 we show the resulting ergodic Holevo capacity bounds. The no-turbulence \( \{\gamma_m^{ad}\} \) lie almost directly under the mild turbulence \( \{\gamma_m^{ad}\} \), and the same is true for their associated capacity bounds. The step-like behavior of the \( \{\gamma_m^{ad}\} \) and the \( \{\gamma_m^{non}\} \) in no turbulence and mild turbulence is caused by the degeneracy of the crosstalk geometry caused by the symmetric square apertures and rectangular symmetry of the focused-beam modes. The degeneracy, and thus the step-like behavior, is blurred out with increasing turbulence-induced beam spread, resulting in the smoother \( \{\gamma_m^{ad}\} \) and \( \{\gamma_m^{non}\} \) curves for strong and very strong turbulence.

Figures 6-1 and 6-2 show that the non-adaptive system's power transfers and ergodic capacities may degrade much more rapidly as turbulence increases as compared to the corresponding adaptive optics system. However, under moderate turbulence, we have \( \sum_{i=1}^{M} \gamma_{m_i}^{non} \approx 120 \). Therefore, it is not surprising that even under moderate turbulence, high photon information efficiency and high spectral efficiency can be obtained without adaptive optics as shown in Fig. 6-2.

We see from Fig. 6-2 that the capacity lower bounds and upper bounds of FB systems that use adaptive optics in mild or moderate turbulence are nearly coincident with each other and with the no-turbulence-propagation curve. Evidently, perfect full-wave adaptive optics enables near-field multi-spatial-mode classical communication with considerable protection against the ill-effects of atmospheric turbulence, as we found in Chapter 3 for single-spatial-mode operation. Indeed, these systems can deliver nearly 5 bits/detected-photon at 5 bits/sec-Hz performance with 169 spatial
Figure 6-1: Power transmissivity statistics for \( M = 169 \) spatial mode system operating with a Fresnel-number product \( D_f = 250 \), realized by square transmitter and receiver apertures with sides of length \( d = 49.5 \) cm and with other operational parameters described in Table 2.3. Solid lines represent systems with perfect receiver adaptive optics, while dashed lines represent systems without adaptive optics.

modes at the ergodic Holevo limit with aperture efficiency \( M/D_f \approx 0.7 \). We must note, however, that the curves in Figures 6-1 and 6-2 do not account for the photons needed by the adaptive-optics system’s wavefront sensor.

A receiver extracting fixed mode patterns \( \{ \phi_m(\rho') \} \) will have to compensate for the appreciable crosstalk between the spatial patterns generated in the receiver pupil \( A_R \) in order to achieve the ergodic capacities that yield high PIE and high SE. As an example of the challenge that crosstalk presents, Fig. 6-3 shows the top 20 crosstalk couplings to the \( \phi(\rho') \) given in (6.34) from fundamental mode FB mode \( \Phi_{00}(\rho) \). The orthogonality of the FB modes in vacuum is apparent from this figure, as is the fact that even mild turbulence induces a significant amount of crosstalk for the non-adaptive FB-mode system. Under moderate or stronger turbulence, the problem
of crosstalk is further compounded by the drastic decrease in the amount of power the receiver extracting the fixed mode pattern $\phi_{0,0}(\rho')$ collects when $\Phi_{0,0}(\rho)$ is transmitted. A saving grace, however is that under moderate and stronger turbulence, the crosstalk couplings $|h_{m0}^{(0)}|^2$ for $m \neq 0$ are still less than $|h_{00}^{(0)}|^2$. Although a multiple-spatial mode link without adaptive optics can achieve extremely high data rates with extremely efficient use of its transmitted photons, its receiver architecture may be prohibitively complicated in order to track and compensate for turbulence-induced crosstalk. In fact, its implementation may be even more complex than a receiver that uses adaptive optics, given the fact that an array of heterodyne receivers could certainly track and separate spatial modes.
The overarching conclusion to be drawn from the use case just evaluated is that multiple-spatial mode free-space optical communication enables both high photon-information efficiency and high spectral efficiency for classical communication through moderate turbulence. Chandrasekaran et al. [89] showed similar results for the Holevo private capacities. These private capacity results, like those just presented, are for systems employing suboptimal, fixed-mode set encoding. We now consider what secure key rate improvements can be observed when decoy-state BB84 QKD is implemented with multi-spatial-mode multiplexing.
6.4 Secret-key rate bounds for multi-spatial-mode
ds-BB84 QKD in turbulence

We are interested in generalizing the Chapter 4 results for ds-BB84 to apply to operation in which the transmitter employs a fixed set of \( M \) orthonormal spatial modes \( \Phi(0)(\rho) \) as given in (6.1) and the receiver uses either full-wave adaptive optics to extract \( M \) orthonormal spatial modes spanning the vector space defined in (6.6) or just extracts a fixed set of \( M \) orthonormal spatial modes \( \Phi(0)(\rho') \) as shown in (6.9).

The secret key rate in bps of a \( M \) spatial-mode optical channel with deterministic transmissivities \( \{\mu_m\} \) experiencing a fixed background plus dark count rate \( n_b \) across each channel is

\[
R_{\text{ds-BB84},M}(\mu, n_b) = \sum_{m=1}^{M} R_{\text{ds-BB84}}(\mu_m, n_b)
\]

(6.35)

where the \( \{\mu_m\} \) are the modal transmissivities (arranged in nonincreasing order) and \( R_{\text{ds-BB84}}(\mu_m, n_b) \) from (4.7) is the signal-strength optimized ds-BB84 secret key rate of a single mode channel with transmissivity \( \mu_m \) and average background plus dark counts \( n_b \). Throughout this section we use \( \mu_m = \mu_m^{\text{ad}} (\mu_m^{\text{non}}) \) for the system that does (does not) employ adaptive optics. As we noted in Chapter 4, the ds-BB84 rate will, at most, require an optimal signal photon strength \( n_s^* = 1 \). Thus, even when encoding along thousands of spatial modes at modulation rates on the order of \( \sim \text{Gbps} \), the total power required to run the multi-spatial mode ds-BB84 link is on the order of microwatts. Thus, we will omit a power constraint in (6.35). The ergodic multi-mode decoy-state BB84 secret key rate is

\[
\langle R_{\text{ds-BB84},M}(\mu, n_b) \rangle = \left\langle \sum_{m=1}^{M} R_{\text{ds-BB84}}(\mu_m, n_b) \right\rangle.
\]

(6.36)

Using the upper bound (4.17) on the single-mode decoy-state BB84 rate, the ergodic
multi-mode decoy-state BB84 key rate can be bounded above by

$$\langle R_{\text{ds-BB84,}M(\mu, n_b)} \rangle \leq \left( \sum_{m=1}^{M} \langle \mu_m \rangle \right) R_{\text{ds-BB84}} (1, n_b) \tag{6.37}$$

$$= \text{tr}(\langle K \rangle) R_{\text{ds-BB84}} (1, n_b) \tag{6.38}$$

$$\leq e^{-\alpha L} \min(M, D_f) R_{\text{ds-BB84}} (1, n_b), \tag{6.39}$$

where (6.38) follows because $\sum_{m=1}^{M} \mu_m$ equals the trace of the channel matrix $K$. (6.39) follows from $\text{tr}(\langle K \rangle) \leq e^{-\alpha L} D_f$ and $\text{tr}(\langle K \rangle) \leq e^{-\alpha L} M$, where the second upper bound is derived from the single-spatial-mode power transfer constraint $0 \leq \mu_m \leq e^{-\alpha L}$.

A lower bound in terms of the $\{\gamma_m\}$ on the ergodic secret-key rate of an $M$ spatial-mode decoy-state BB84 link operating through the turbulent channel may be found by using the following lemma, which is proved in Appendix D.

**Lemma D.5:** For a fixed $n_b > 0$, the multi-mode decoy-state BB84 secret key rate $R_{\text{ds-BB84,}M(\mu, n_b)}$ is both convex and Schur-convex in $\mu$, the vector of the Alice-to-Bob channel’s modal power transmissivities.

The $\mu$ majorize the $\gamma$, so combining this fact with Lemma D.5, we obtain

$$R_{\text{ds-BB84,}M(\mu, n_b)} \geq \sum_{m=1}^{M} R_{\text{ds-BB84}} (\gamma_m, n_b). \tag{6.40}$$

Figures 6-4 and 6-5 show lower bounds on $\langle R_{\text{ds-BB84,}M} \rangle$ with parameters given by Table 2.3 operating with and without adaptive optics at either $M = 9$ or $M = 169$ spatial modes. We assume that each individual spatial mode is operated at a 10 Gbps modulation rate and has identical detectors that experience the same background plus dark count rate $n_b = 10^{-4}$ photons/channel use. The upper bound (6.39) on the secret-key rate of ds-BB84 QKD is plotted as a dotted blue curve. Unlike the lower bounds on the rate of single-spatial-mode ds-BB84 without adaptive optics displayed in Figs. 4-2–4-4, the multi-spatial-mode QKD lower bounds for operation without adaptive optics do not decrease with increasing $D_f$ values. This difference is
because in the single-mode case, beam spreading and breakup at large Fresnel-number products made it nearly impossible to couple appreciable amounts of power into the single mode given by (2.16). In the multi-spatial mode case, however, despite the lack of mode-tracking at the receiver without adaptive optics, the received spatial modes are decomposed over the \( \{ \phi^{(0), FB}_{n_x} (\rho') \} \) given in (6.34), thus ensuring that a far larger fraction of the power in aperture is coupled into the multi-spatial mode receiver.

Also, there are kinks in the lower bound curves as \( D_f \) increases for systems with adaptive optics operating at low \( D_f \) (shown in the solid green, orange, and red curves) as well as systems without adaptive optics operating in high \( D_f \) and very strong turbulence (shown in the dashed pink curve). These kinks occur because in both of
these cases the \( \{\gamma_m\} \) are all very small. With the increase of \( D_f \), some \( \gamma_m \) values are pushed above the \( \eta = 0.001 \) power-transfer threshold for ds-BB84 to have nonzero key rate, resulting in slope changes in the total secret-key rate vs. \( D_f \) of the multi-spatial-mode FSO link.

We see from Figs. 6-4 and 6-5 that the QKD rate lower and upper bounds for FB systems that use adaptive optics in mild or moderate turbulence are nearly coincident with the no-turbulence bound, and, in fact, the upper bound on QKD rates for \( D_f \geq 10^{-2} \). However, in very strong turbulence the lower bound on the ds-BB84 key rate for a system with adaptive optics can be orders of magnitude lower than the upper bound on the multi-spatial-mode ds-BB84 QKD rate. For a particular receiver
Figure 6-6: Upper and lower bounds at $D_f = 1$ on the multiple-spatial mode ergodic decoy-state BB84 QKD secure rate $\langle R_{ds-BB84,M} \rangle$ in vacuum, mild, moderate, strong, and very strong turbulence vs. a varying number $M$ of spatial modes with all other link parameters given in Table 2.3, $n_b = 10^{-4}$ photons/channel use, and $R_{mod} = 10$ Gbps. Lower bounds on $\langle R_{ds-BB84,M} \rangle$ of a link with no adaptive optics are plotted with crosses while lower bounds on the $\langle R_{ds-BB84,M} \rangle$ of a link with adaptive optics are plotted with diamonds. An upper bound corresponding to the $\langle R_{ds-BB84,M} \rangle$ of a system operating with $e^{-\alpha L} \min(D_f, M)R_{ds-BB84}(1, n_b)$ is plotted as a dashed blue curve.

For systems with no adaptive optics (the dashed lines plotted in Figs. 6-4 and 6-5), only operation in mild and moderate turbulence with $D_f > 5$ approaches the upper bound on the multi-spatial-mode ds-BB84 key rate. Operation in strong or very strong turbulence yields lower bounds on the secret-key rate that are orders of
magnitude lower than the ultimate upper bound. Increasing the number of spatial modes from $M = 9$ to $M = 169$, however, decreases the degree to which lower bounds on the secret-key rate drop in strong and very strong turbulence.

From Figs. 6-4 and 6-5, we observe that increasing the number of spatial modes $M$ does not broaden the Fresnel-number product regions that yield non-zero secret-key rates at a given turbulence strength. Increasing $M$ does increase the non-zero rates, especially for near-unity and near-field Fresnel-number products. Figure 6-6 plots the lower and upper bounds on ds-BB84 secret-key rates for 10 Gbps/mode systems operating either with or without adaptive optics at $D_f = 1$. Increasing the number of modes $M$ from $M = 1$ to $M = 9$, which is larger than the Fresnel-number product $D_f = 1$, increases the system’s secret-key rate by an order of magnitude in strong or very strong turbulence whether or not the system uses adaptive optics. Thus, it is clear that there is significant secret-key rate to be gained by going to multi-spatial-mode operation, even with a smaller, near-unity Fresnel-number product like $D_f \sim 1$.

### 6.5 Secret-key rate bounds for multi-spatial-mode FL-QKD in turbulence

Paralleling our development for a multi-spatial-mode FSO decoy-state BB84 link, we now bound the performance of a multi-spatial-mode FL-QKD system. We will use Schur-convexity and majorization arguments to derive lower bounds on FL-QKD secret-key rates from the power-transfer eigenvalues $\{ \gamma^\text{ad}_m : 1 \leq m \leq M \}$ and $\{ \gamma^\text{non}_m : 1 \leq m \leq M \}$ of the average channel kernels $\langle K_\text{ad} \rangle$ and $\langle K_\text{non} \rangle$.

The FL-QKD secret key rate in bps of a deterministic, pure-loss $M$ spatial-mode optical channel is

$$R_{FL,M}(\mu) = \sum_{m=1}^{M} R_{FL}(\mu_m)$$  

(6.41)

where $\{\mu_m\}$ are the modal transmissivities of the $M$ spatial modes (arranged in
nonincreasing order), and \( R_{\text{FL}}(\mu_m) \) from (5.21) is the FL-QKD secret-key rate of a single mode channel with transmissivity \( \mu_m \). As was true in the case of the multi-spatial-mode ds-BB84 QKD link, there is no need for a power constraint at the transmitter - the FL-QKD rate equation requires an optimal signal photon brightness \( N_s \ll 1 \), thus ensuring that, even when encoding along thousands of spatial modes at modulation rates on the order of \( \sim \)Gbps, the total power required to run the multi-spatial mode FL-QKD link is on the order of microwatts.

The ergodic multi-spatial-mode FL-QKD secret-key rate is

\[
\langle R_{\text{FL},M}(\mu) \rangle = \sum_{m=1}^{M} \langle R_{\text{FL}}(\mu_m) \rangle
\]

(6.42)

\[\geq \sum_{m=1}^{M} R_{\text{FL}}^{\text{LB}}(\mu_m) \]

(6.43)

\[= R_{\text{FL},M}^{\text{LB}}(\mu), \]

(6.44)

where (6.43) follows from (5.44).

A lower bound in terms of the \( \{\gamma_m\} \) on the ergodic secret-key rate of an \( M \) spatial-mode FL-QKD link operating through the turbulent channel may be found by using the following lemma, which is proved in Appendix E.

**Lemma E.3:** For \( N_s \ll 1, G_B \gg 1, \) and \( N_B \gg 1 \), the lower bound on the multi-spatial mode FL-QKD secret key rate \( R_{\text{FL},M}^{\text{LB}}(\mu) \) is both convex and Schur-convex in \( \mu \).

Because the \( \mu \) majorize the \( \gamma \), Lemma E.3 allows us to arrive at the following lower bound on the ergodic secret key rate of an \( M \)-spatial-mode FL-QKD link.

\[
\langle R_{\text{FL},M}(\mu) \rangle \geq R_{\text{FL},M}^{\text{LB}}(\gamma).
\]

(6.45)

We now illustrate this lower bound’s behavior for an \( M \)-spatial-mode FL-QKD FSO link whose parameters are given in Tables 2.3 and 5.1 with \( M = 9 \) and \( M = 169 \). These lower bounds are plotted in Figs. 6-7 and 6-8, where rates of systems operating with (without) adaptive optics are plotted as solid (dashed) lines. We
assume that each single-mode channel is coupled into a fiber that leads to a single
detector, allowing us to assume that each such channel experiences the same $G_B$ and
$N_B$ values.

![9-Spatial Mode FL-QKD Rate Bounds vs. $D_f$](image)

Figure 6-7: Lower bounds on the 9-spatial mode ergodic FL-QKD secure rate $\langle R_{FL,M} \rangle$ in no, mild, moderate, strong, and very strong turbulence vs. the Fresnel number product $D_f$ for a link with parameters given in Tables 2.3 and 5.1. Lower bounds on $\langle R_{FL,M} \rangle$ of a link without adaptive optics are plotted as dashed curves while lower bounds on $\langle R_{FL,M} \rangle$ of a link with adaptive optics are plotted as solid lines.

We see from Figs. 6-7 and 6-8 that the secret-key rates of systems that use adaptive optics in mild, moderate, or strong turbulence lie within a half-an-order of magnitude of one another across the range of $D_f$ shown. For a system with adaptive optics operating in very strong turbulence with $M = 9$ spatial modes, the lower bound on the secret-key rate is an order of magnitude lower than the rates of adaptive-optics system operating in no, mild, moderate, or strong turbulence for $D_f > 10^{-2}$ and disappears for $D_f < 0.00126$. For an adaptive-optics system with $M = 169$, the lower bound on the key-rate in very strong turbulence is only a half an order of magnitude
lower for $D_f > 10^{-1}$, although it too disappears for $D_f < 0.00126$. As we saw in our study of multi-spatial-mode ds-BB84, for a particular receiver type (either with or without adaptive optics) and for a given strength of turbulence, the lower bounds on FL-QKD rates all fall to zero at the same $D_f$ whether $M = 9$ or $M = 169$. However, the lower bounds of the FL-QKD key rate of the system using $M = 169$ spatial modes are much higher than the lower bounds on the key rate of a system using $M = 9$ spatial modes above the nonzero rate $D_f$ threshold.

For systems with no adaptive optics, the rate decreases are much more severe. Systems without adaptive optics operating in mild or moderate turbulence will be able to achieve rates near the lower bounds of key rates of systems operating in no turbulence. In strong turbulence, having no adaptive optics causes the rate the
decrease by a half an order of magnitude. Having no adaptive optics when operating in strong turbulence could be catastrophic - a nonzero lower bound on the FL-QKD rate is only available for $D_f > 1.23$, and in operation with either $M = 9$ or $M = 169$, the rate lower bounds are at least an order of magnitude lower than the lower bounds on rate in no turbulence. Thus, we hypothesize that adaptive optics will be absolutely necessary in order to preserve high secure key rates for all strengths of turbulence in optical links with near-unity Fresnel-number products.

As was the case for multi-spatial-mode ds-BB84 QKD, there are two kinks in the FL-QKD secret-key rate lower bounds for a system without adaptive optics in very strong turbulence (plotted as dashed red lines in Figs. 6-7 and 6-8). These kinks occur because the $\gamma_m$ are all very small in very strong turbulence without adaptive optics. With the increase of $D_f$, two of the $\gamma_m$ values are pushed above the $\eta = 6.3 \times 10^{-5}$ power-transfer threshold for FL-QKD to have a nonzero key rate, resulting in the slope changes in the total secret-key rate vs. $D_f$ of multi-spatial-mode FL-QKD.

The most fascinating phenomenon shown in Figs. 6-7 and 6-8 is that increasing the turbulence strength can sometimes increase the lower bounds on the link’s secret-key rates. This seemingly anomalous increase is caused by the behavior of the single-mode deterministic-channel FL-QKD rate shown in Fig. 5-2, which increases much faster with $\eta_{atm}$ for low values of $\eta_{atm}$ than it does for high values of $\eta_{atm}$. Thus, turbulence, which has a tendency to displace power from a dominant mode into a less dominant mode, can actually increase the overall secure key rate of a multi-spatial mode link. For very strong turbulence, however, this redistribution cannot compensate for the overall drastic drop across all power transmissivities, resulting in rate curves for adaptive (non-adaptive) operation that lie under all other rate curves in adaptive (non-adaptive) operation. A good example of this crossover occurs in Fig. 6-8, where the lower bound of the FL-QKD rate for a system with adaptive optics in strong turbulence lies above the FL-QKD rate lower bound for adaptive optics systems operating in moderate, mild, or no turbulence for $0.126 \leq D_f \leq 200$.

As we saw for ds-BB84, increasing the number of spatial modes of an FL-QKD system does not extend the range of Fresnel-number products that yield non-zero
secret-key rates, although it can greatly increase the achievable rates in the near-unity and near-field Fresnel-number products. In Fig. 6-9, we plot the $D_f = 1$ secret-key rates for an FL-QKD system using the parameters given in Tables 2.3 and 5.1 operating either with or without adaptive optics as $M$ is increased. As we saw in the ds-BB84 link, increasing the number of spatial modes from 1 to 9, which is larger than the Fresnel-number product $D_f = 1$, provides an order-of-magnitude improvement in the rate for operation in very strong or strong turbulence. While increasing $M$ does cause the rate to saturate at some point, it is clear that for a near-unity $D_f$, operating at $M > D_f$ can have great benefits.

Having addressed the possible rate increases achievable in both classical and quantum communication links when multiple-spatial modes are used, we now turn our at-
attention back to BDAO in order to assess its efficacy in the single-spatial-mode regime when measurement noise or the time-varying nature of turbulence are accounted for.
Chapter 7

Communication with FSO links operating with non-ideal BDAO systems

In Section 2.3.1, we introduced an algorithm for bidirectional, full-wave adaptive optics compensation for single-spatial mode optical propagation through atmospheric turbulence. Due to the complexity of implementing a full-wave conjugate transmitter, we relaxed the full-wave adaptive optics requirement in Section 2.3.2, where we introduced an algorithm for bidirectional, phase-only adaptive optics compensation, and compared the steady-state power transfers, $\hat{\eta}_1^{\text{full}}$ and $\hat{\eta}_1^{\text{phase}}$, achieved by the two protocols. As shown in Figs. 2-2 and 2-3, our POPS simulations of these protocols assumed that the conjugate transmitters made noiseless measurements on the received wavefronts. So, we were able to: (1) characterize the ultimate power transfer of a single-spatial mode FSO link operating in frozen atmospheric turbulence; and (2) compare its average power transfers to upper and lower bounds derived from the mutual coherence function of frozen atmospheric turbulence.

However, these ultimate power transfers may not be achievable by realistic BDAO systems. It is impossible to build a noiseless conjugate transmitter, since optical measurements of the magnitude or phase of a wavefront will always be affected by noise. Moreover, there will certainly be wind along the propagation path from $z = 0$ to
\[ z = L \] on an FSO link, thus ensuring that the turbulence varies in time. To assess the
degree to which these non-idealities may affect the single-spatial-mode power transfer
of an FSO link operating with either full-wave or phase-only BDAO, we present
POPS simulation results of the power transfers achieved by: (1) BDAO systems
operating with noisy conjugate transmitters; and (2) BDAO systems operating with
noiseless conjugate transmitters generating time-delayed wavefronts in time-varying
atmospheric turbulence.

\section{7.1 FSO links operating with BDAO with Gaussian noise}

Conjugate transmitters in either full-wave or phase-only BDAO systems may use an
array of optical heterodyne receivers to measure wavefronts and generate either the
conjugate wave fronts or conjugate phase screens, respectively, needed for our two
BDAO protocols. Heterodyne receivers operate by mixing the received wavefront
with a strong local oscillator (LO) and detecting the combined optical signal. For
the classical-state signals considered in this thesis, the receivers can be described
semiclassically and experience local-oscillator (LO) shot noise, which may be ap-
proximated as additive white Gaussian noise (AWGN) in the strong local-oscillator
limit \[92, 93\]. Thus, in this section we will study how the power transfers achieved by
single-spatial-mode FSO systems employing either full-wave or phase-only BDAO de-
cline when conjugate transmitters make measurements with varying levels of AWGN.

\subsection{7.1.1 Full-wave bidirectional compensation with AWGN}

A cartoon of an FSO system implementing full-wave, bidirectional compensation for
turbulence with AWGN is shown in Fig. 7-1. Rather than being able to make a
noiseless, full-wave, and spatially-continuous measurement of an incoming wavefront
and generate its conjugate, this conjugate transmitter now makes a discretized mea-
surement of the incoming wavefront using an array of heterodyne receivers. Thus,
complex envelope measurements at each detector experience zero-mean, circularly
complex AWGN, $N_C(0, \sigma_t^2)$, with variance $\sigma_t^2$ such that total average noise power over
the array of heterodyne receivers is $N_e \sigma_t^2$, where $N_e$ is the number of elements in the
array. For the purposes of this thesis, we will simply fix the value of signal-to-noise
ratio on the 0th iteration of full-wave BDAO with AWGN, SNR$_0$, and then use the relationship

$$\text{SNR}_0 = \frac{\langle \eta \rangle_{\text{recAO}}}{N_e \sigma_t^2},$$

where $\langle \eta \rangle_{\text{recAO}}$ is the lower bound on $\langle \eta \rangle_{\text{full}}$ given in (2.22), to set the value of the variance per pixel, $\sigma_t^2$. We assume that $N_e$ is large relative to the number of atmospheric coherence areas in the receivers at $z = 0$ and $z = L$ so that the noisy conjugate transmitter operates in the continuum regime on the incoming wavefronts. Finally, after
the wavefront is measured noisily, a normalized, conjugated version of the wavefront
is generated and sent back through the atmosphere, as shown in Figure 7-1.

![Figure 7-1: A model for bidirectional full-wave compensation with AWGN through frozen atmospheric turbulence on its kth iteration.](image_url)

While we fix the average value SNR$_0$, we note that the SNR at the conjugate transmitter
will, on average, increase with each iteration of BDAO due to the fact that each pass
of BDAO will increase the power transfer from $z = 0$ to $z = L$ (and vice versa), thus
increasing the ratio of the signal power at the conjugate transmitter to the added

\[ h_{\text{atm}}^{0 \rightarrow L}(\rho, \rho') = \sum_{m=1}^{\infty} \sqrt{\eta_m} \phi_m(\rho') \phi_m^*(\rho) \]

\[ h_{\text{atm}}^{0 \rightarrow L}(\rho, \rho') = \sum_{m=1}^{\infty} \sqrt{\eta_m} \phi_m^*(\rho) \phi_m(\rho') \]
noise power. Average SNR increases over multiple iterations of POPS for a particular
$D_f$ and set of turbulence strengths are given in Table 7.1.

Because the second-moment statistics of the $\{\eta_m\}$ required to bound the power
transmissivities are not available in closed form, we again employ POPS to assess how
the power transfers $\hat{\eta}_1^{\text{full-noise}}(k)$ for full-wave BDAO operating at a particular SNR
value differ from their $\hat{\eta}_1^{\text{full}}(k)$ counterparts for noiseless full-wave BDAO. The steady
state power transfer of full-wave BDAO in noise (if it converges), $\hat{\eta}_1^{\text{full-noise}}(k \to \infty)$,
will be denoted as $\hat{\eta}_1^{\text{full-noise}}$.

### 7.1.2 Phase-only bidirectional compensation with AWGN

Figure 7-2 depicts the phase-only BDAO protocol operating in the presence of AWGN.
To make a proper comparison between full-wave and phase-only BDAO with AWGN,
we model the conjugate transmitter at $z = L$ on the $k^{\text{th}}$ iteration of BDAO as simply
taking the phase measurement from the array of $N_e$ heterodyne receivers experienc-
ing a per-pixel, complex circular AWGN with variance $\sigma_0^2$ as described in the previous
section for full-wave BDAO with noise. Rather than generating the normalized con-
jugate of the measured wavefront, however, the conjugate transmitter simply applies
the conjugates of their noisy phasefront measurements to a focused, uniform-intensity
beam with unit power over the aperture at either $z = 0$ or $z = L$.

The power transfer on the $k^{\text{th}}$ pass of the phase-only BDAO algorithm achieved
when transmitting will be denoted as $\hat{\eta}_1^{\text{phase-noise}}(k)$, where $\hat{\eta}_1^{\text{phase-noise}}(0) = \hat{\eta}_{\text{recAO}}$
since $U_0(\rho)$ will be used as the initial beacon signal. Its steady state power transfer
(if it converges), $\hat{\eta}_1^{\text{phase-noise}}(k \to \infty)$, will be denoted as $\hat{\eta}_1^{\text{phase-noise}}$. Due to the lack
of closed-form power transfer statistics and spatial mode statistics of the CON input
and output spatial mode sets, we cannot derive the statistics of the single-spatial-
mode power transfer $\hat{\eta}_1^{\text{phase-noise}}$ of the phase-only, noisy BDAO link. Thus, we must
turn to POPS simulation of phase-only BDAO with AWGN to assess (1) whether
the steady-state power transfer $\hat{\eta}_1^{\text{phase-noise}}$ exists, and, if so, if it differs greatly from
$\hat{\eta}_1^{\text{phase}}$; and (2) whether it will afford an FSO link the same increases in power transfer
as full-wave BDAO compensation with AWGN.
7.1.3 Power transfers of full-wave and phase-only BDAO with AWGN

In this section, we present the POPS-simulated clear-weather turbulence, extinction-loss neglecting \( e^{-\alpha L} = 1 \) results for the statistics of the \( \tilde{h}_i^{\text{full-noise}}(k) \) and \( \tilde{h}_i^{\text{phase-noise}}(k) \) values after four passes through the atmosphere. Also included are comparisons between the square-law-derived power transfer bound \( \langle \eta_{\text{recAO}} \rangle \) and the POPS-simulated mean power transfers \( \langle \tilde{\eta}_{\text{recAO}} \rangle \) and \( \langle \tilde{\eta}_{\text{recAO}} \rangle \) for the FSO link. The assumed parameters are given in Table 2.3, and results will be presented for the systems with initial SNR\(_0\) = 6 dB and 3 dB. Simulations were performed for SNR\(_0\) values from 43 dB to 3 dB, but appreciable deviations from the infinite-SNR case only occurred for SNR\(_0\) ≤ 6 dB for all considered turbulence strengths. This bodes well for the eventual implementation and integration of BDAO systems into communication links because the conjugate transmitters will not require large amounts of signal power to track optimal spatial modes and improve the power transfer of the link.

First, it should be noted that the SNR values at each iteration of both phase-only and full-wave BDAO do, on average, increase at each iteration of BDAO. An example of this iteration-to-iteration SNR increase averaged over multiple POPS simulations for varying strengths of turbulence is given in Table 7.1 for full-wave BDAO operating
with \( \text{SNR}_0 = 6 \, \text{dB} \) and \( D_f = 4 \) through 4 iterations of the protocol.

<table>
<thead>
<tr>
<th>iteration ( k )</th>
<th>( \text{SNR}<em>k ) (dB), ( \sigma^2</em>\chi = 0.137 )</th>
<th>( \text{SNR}<em>k ) (dB), ( \sigma^2</em>\chi = 1.37 )</th>
<th>( \text{SNR}<em>k ) (dB), ( \sigma^2</em>\chi = 13.67 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6.0</td>
<td>6.0</td>
<td>6.0</td>
</tr>
<tr>
<td>1</td>
<td>6.2</td>
<td>11.9</td>
<td>15.4</td>
</tr>
<tr>
<td>2</td>
<td>6.5</td>
<td>12.6</td>
<td>16.6</td>
</tr>
<tr>
<td>3</td>
<td>6.5</td>
<td>12.8</td>
<td>17.0</td>
</tr>
<tr>
<td>4</td>
<td>6.6</td>
<td>12.9</td>
<td>17.2</td>
</tr>
</tbody>
</table>

Table 7.1: POPS-simulated SNR values at the conjugate transmitter at \( z = L \) conjugate transmitter for \( k = 4 \) iterations of full-wave BDAO with AWGN assuming \( \text{SNR}_0 = 6 \, \text{dB} \) with \( D_f = 4 \), no extinction loss, and parameters given in Table 2.3 for moderate \( (\sigma^2_\chi = 0.137) \), strong \( (\sigma^2_\chi = 1.367) \), and very strong turbulence \( (\sigma^2_\chi = 13.67) \) averaged over 1,000 POPS turbulence simulations.

Because Table 7.1 suggests that effects of the added noise may be canceled by the operation of BDAO — especially in very strong turbulence — we consider the convergence behavior of \( \tilde{\eta}^\text{full-noise}_1(k) \) and \( \tilde{\eta}^\text{phase-noise}_1(k) \) for all Fresnel-number products \( D_f \) and turbulence strengths listed in our notional case in Table 2.3. As was done in Chapter 2, beta distributions were fit to each \( \tilde{\eta}^\text{full-noise}_1(k) \) and \( \tilde{\eta}^\text{phase-noise}_1(k) \), resulting in probability distributions \( \beta^\text{full-noise}_1(k)(\eta; a(D_f, \sigma^2_\chi), b(D_f, \sigma^2_\chi)) \) and \( \beta^\text{phase-noise}_1(k)(\eta; a(D_f, \sigma^2_\chi), b(D_f, \sigma^2_\chi)) \) (which we abbreviate as \( \beta^\text{full-noise}_1(k) \) and \( \beta^\text{phase-noise}_1(k) \)).

To check the convergence in \( k \) of the \( \beta^\text{full-noise}_1(k) \) and \( \beta^\text{phase-noise}_1(k) \), we checked if the KL-divergence \( \beta^\text{full-noise}_1(k) \) \( (\beta^\text{phase-noise}_1(k)) \) for \( k = 0, 1, 2, 3 \) converged to the steady state distribution, which we took to be \( \beta^\text{full-noise}_1(0) \) \( (\beta^\text{phase-noise}_1(0)) \) for full-wave BDAO (phase-only BDAO) operating with AWGN with a given SNR.

In Figs. 7-3 and 7-4, the \( D(\beta^\text{full-noise}_1(k)||\beta^\text{full-noise}_1(4)) \) and \( D(\beta^\text{phase-noise}_1(k)||\beta^\text{phase-noise}_1(4)) \) are plotted vs. the Fresnel number product for moderate \( (\sigma^2_\chi = 0.137) \), strong \( (\sigma^2_\chi = 1.367) \), and very strong turbulence \( (\sigma^2_\chi = 13.67) \) for \( k = 0, 1, 2, \) and 3. We omit the KL divergence for the mild \( (\sigma^2_\chi = 0.014) \) case because the steady-state distributions \( \beta^\text{full-noise}_1 \) and \( \beta^\text{phase-noise}_1 \) converge by \( k = 2 \) and are nearly Dirac-delta functions (or beta distributions with very small variance) in mild turbulence. Thus, knowing that \( \beta^\text{full-noise}_1(4) \) and \( \beta^\text{full-noise}_1(4) \) are fairly good approximations to the steady-state distributions of \( \beta^\text{full-noise}_1 \) and \( \beta^\text{phase-noise}_1 \) for mild turbulence, we analyze Figs. 7-3 and 7-4 to show that this is true for stronger strengths of turbulence as well.
Figure 7-3: Convergence behavior of the power transmissivity distributions $\tilde{\eta}_{\text{full-noise}}^{\text{full}}(k)$ and $\tilde{\eta}_{\text{phase-noise}}^{\text{full}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate ($\sigma_{\chi}^2 = 0.137$), strong ($\sigma_{\chi}^2 = 1.367$), and very strong turbulence ($\sigma_{\chi}^2 = 13.67$) operating with AWGN with SNR$_0 = 6$ dB. KL divergences $D\left(\tilde{\eta}_{\text{full-noise}}^{\text{full}}(k)\|\tilde{\eta}_{\text{full-noise}}^{\text{full}}(4)\right)$ for full-wave BDAO and $D\left(\tilde{\eta}_{\text{phase-noise}}^{\text{full}}(k)\|\tilde{\eta}_{\text{phase-noise}}^{\text{full}}(4)\right)$ for phase-only BDAO are plotted for $k = 0, 1, 2, 3$. 
Figure 7-4: Convergence behavior of the power transmissivity distributions $\beta_{\eta_1}^{\text{full-noise}}(k)$ and $\beta_{\eta_1}^{\text{phase-noise}}(k)$ for full-wave and phase-only BDAO with AWGN with $\text{SNR}_0 = 3$ dB for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate ($\sigma_\chi^2 = 0.137$), strong ($\sigma_\chi^2 = 1.367$), and very strong turbulence ($\sigma_\chi^2 = 13.67$). KL divergences $D\left(\beta_{\eta_1}^{\text{full-noise}}(k) \parallel \beta_{\eta_1}^{\text{full-noise}}(4)\right)$ for full-wave BDAO and $D\left(\beta_{\eta_1}^{\text{phase-noise}}(k) \parallel \beta_{\eta_1}^{\text{phase-noise}}(4)\right)$ for phase-only BDAO are plotted for $k = 0, 1, 2, 3$. 

(a) $\sigma_\chi^2 = 0.137$

(b) $\sigma_\chi^2 = 1.37$

(c) $\sigma_\chi^2 = 13.7$
In both Figs. 7-3 and 7-4, there is a large change in the shape of the divergence curves from \( k = 0 \) to \( k = 1 \) — in fact, the divergence sometimes increases. Given that AWGN noise is only introduced into the BDAO power transfers during the \( k = 1 \) iteration, the convergence at \( k = 2 \) is not surprising. The divergences 

\[
D \left( \beta_{\eta_1^{\text{full-noise}}(k)} \| \beta_{\eta_1^{\text{full-noise}}(4)} \right) \text{ and } D \left( \beta_{\eta_1^{\text{phase-noise}}(k)} \| \beta_{\eta_1^{\text{phase-noise}}(4)} \right)
\]

do decrease monotonically in \( k \) for \( k > 1 \) with nearly an order of magnitude decrease in divergence from iteration \( k \) to \( k+1 \) in strong and very strong turbulence. In moderate turbulence, this monotonic decrease in the divergence as \( k \) increases only begins for \( k \geq 2 \). This is due to the fact that it takes the system one complete pass through the atmosphere and the AWGN added by both conjugate transmitters before the system begins to approach a steady state power transmissivity. Because the monotonic decrease in divergence holds from the \( k = 2 \) to \( k = 3 \) divergence curves and the final KL-divergences are less than 1, we state \( \eta_1^{\text{full-noise}}(4) \) and \( \eta_1^{\text{phase-noise}}(4) \) are fairly good approximations to the steady state single-spatial-mode power transfers \( \eta_1^{\text{full-noise}} \) and \( \eta_1^{\text{phase-noise}} \) for both \( \text{SNR}_0 = 6 \) dB and \( \text{SNR}_0 = 3 \) dB. Thus, we will take \( \eta_1^{\text{full-noise}}(4) \) and \( \eta_1^{\text{phase-noise}}(4) \) to be our steady-state power transfers \( \eta_1^{\text{full-noise}} \) and \( \eta_1^{\text{phase-noise}} \) for the rest of this chapter.

To get some idea how the steady state distributions of \( \eta_1^{\text{full}} \) and \( \eta_1^{\text{phase}} \) achieved in the case of ideal, noiseless BDAO differ from the \( \eta_1^{\text{full-noise}} \) and \( \eta_1^{\text{phase-noise}} \) for different initial \( \text{SNR}_0 \) values, we have plotted their histograms and corresponding beta-distribution fits for a \( D_f = 4 \) link operating in moderate, strong, or very strong turbulence in Figs. 7-5 through 7-7.

Figures 7-5 through 7-7 plot the histograms of \( \eta_1^{\text{full}} \) (plotted with solid green bars) and \( \eta_1^{\text{phase}} \) (plotted with open green bars) and their corresponding beta-distribution fits vs. histograms for \( \eta_1^{\text{full-noise}} \) (plotted with solid bars) and \( \eta_1^{\text{phase-noise}} \) (plotted with open bars) operating with AWGN at two different \( \text{SNR}_0 \) values for a \( D_f = 4 \) FSO link with no extinction loss and parameters given in Table 2.3. The beta-distribution fits for histograms without or with noise are plotted with solid or dashed lines, respectively. For a BDAO system operating with an SNR as low as 3 dB in strong or very strong turbulence, the distribution of \( \eta_1^{\text{full-noise}} \) (plotted with solid purple
Figure 7-5: Moderate turbulence, $\sigma_X^2 = 0.137$: Histograms for $\eta_1^{\text{full}}$ (plotted with filled green bars) and $\eta_1^{\text{phase}}$ (plotted with open green bars) and their corresponding beta-distribution fits (plotted with solid black lines) vs. histograms for $\eta_1^{\text{full-noise}}$ (plotted with solid bars) and $\eta_1^{\text{phase-noise}}$ (plotted with open bars) and their beta-distribution fits (plotted with dashed black lines). An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with SNR$_0 = 6$ dB or 3 dB for the cases with AWGN.
Figure 7-6: Strong turbulence, $\sigma_x^2 = 1.37$: Histograms for $\hat{\eta}_{\text{full}}$ (filled green bars) and $\hat{\eta}_{\text{phase}}$ (open green bars) and their corresponding beta-distribution fits (solid black lines) vs. histograms for $\hat{\eta}_{\text{full-noise}}$ (solid bars) and $\hat{\eta}_{\text{phase-noise}}$ (open bars) and their beta-distribution fits (dashed black lines). An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with $\text{SNR}_0 = 6$ dB or $3$ dB for the cases with AWGN.
Very strong turbulence, $\sigma^2 = 13.67$: Histograms for $\hat{\eta}_1^{\text{full}}$ (filled green bars) and $\hat{\eta}_1^{\text{phase}}$ (open green bars) and their corresponding beta-distribution fits (solid black lines) vs. histograms for $\hat{\eta}_1^{\text{full-noise}}$ (solid bars) and $\hat{\eta}_1^{\text{phase-noise}}$ (open bars) and their beta-distribution fits (dashed black lines). An FSO link with $D_f = 4$, no extinction loss, and parameters given in Table 2.3 is assumed with $\text{SNR}_0 = 6$ dB or 3 dB for the cases with AWGN.
bars) is not drastically different from the distribution of $\hat{\eta}^{\text{full}}_1$, nor is the distribution of $\hat{\eta}^{\text{phase-noise}}_1$ drastically different from the distribution of $\hat{\eta}^{\text{phase}}_1$ (plotted with open green bars), suggesting that the effects of added noise are minimal in very strong strengths of turbulence. Such is not the case in moderate turbulence, where significant differences exist between the distributions with and without noise.

We surmise that the better behavior of $\hat{\eta}^{\text{full-noise}}_1$ and $\hat{\eta}^{\text{phase-noise}}_1$ in strong and very strong turbulence comes about because the added noise on the initial iterations makes the conjugate transmissions couple better to the dominant spatial mode. This could occur because the spatial coherences lengths — 1.1 cm and 0.3 cm, respectively — for strong and very strong turbulence are so much smaller than the $d = 17$ cm aperture length needed for $D_f = 4$. Consequently, as seen in Table 7.1, the presence of noise leads to greater increases in SNR$_k$ when the turbulence is strong or very strong than it does for moderate turbulence. In the next section, we will use our $\hat{\eta}^{\text{full-noise}}_1$ and $\hat{\eta}^{\text{phase-noise}}_1$ statistics to assess the effects of noisy wavefront measurements on BDAO FSO communications.

7.1.4 Communication over FSO links with extinction

Before we assess the performance of communication links operating with full-wave or phase-only BDAO with AWGN, we present the means of the full-wave and phase-only power transfers achieved by BDAO systems operating with no noise, SNR$_0 = 6$ dB, and SNR$_0 = 3$ dB in an FSO link with parameters given in Table 2.3. Because we are considering the performance of communication links in a free-space link, we assume that the extinction loss $e^{-\alpha L}$ takes on the less-than-unity value given in Table 2.3.

Figures 7-8 through 7-10 plot the average power transfers for varying SNR. The ultimate upper bound on the link's power transfer $\langle \eta_1 \rangle^{\text{UB}}$ and the no-turbulence power transfer $e^{-\alpha L} \eta_1^{\text{vac}}$ are plotted as solid and dashed blue lines, respectively, while the average no-pass and no-noise power-in-aperture, $\langle \eta_{\text{recAO}} \rangle$ is plotted with red crosses. Figures 7-8 through 7-10 show that for all turbulence strengths, the power transfers of phase-only BDAO are all less than their corresponding full-wave power transfers by $\approx 1$ dB, regardless of the BDAO conjugate transmitter's initial SNR.
Figure 7-8: Moderate turbulence, $\sigma_k^2 = 0.137$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for SNR$_0 = 6$ dB and $3$ dB vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. The crosses connected by lines are the average no-pass power-in-aperture $\langle \eta_{\text{recAO}} \rangle$, while $\langle \eta_1 \rangle^{\text{UB}}$ and $e^{-\alpha L} \eta_{\text{vac}}^{\text{vac}}$ are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers $\langle \eta_1^{\text{full}} \rangle$ in no noise and $\langle \eta_1^{\text{full-noise}} \rangle$ in AWGN are stars, while the steady state phase-only BDAO power transfers $\langle \eta_1^{\text{phase}} \rangle$ in no noise and $\langle \eta_1^{\text{phase-noise}} \rangle$ in AWGN are squares.
We omit the figure for the steady-state power transfers of full-wave and phase-only BDAO with noise operating in mild turbulence because the mean power transfers are essentially the same as the mean power transfers in moderate turbulence. Figure 7-8 shows steady-state power transfers of FSO links using full-wave and phase-only BDAO with varying levels of noise in moderate turbulence. For a BDAO system operating with a conjugate transmitter making wavefront measurements with SNR₀ = 6 dB, the steady state power transfer is lower than the noiseless no-pass power-in-aperture power transfer for a Fresnel-number product $D_f < 1$ or $D_f > 10$. For a full-wave BDAO system operating with SNR₀ = 3 dB, the BDAO steady state power transfer ($\langle \eta_{\text{full-noise}} \rangle$) lies underneath that of the no-pass power-in-aperture power transfer. We surmise that this is because in moderate turbulence, the noise added to the wavefront measurement couples poorly to the dominant spatial eigenmode of the atmosphere, which will have a larger coherence area than that of the added noise. Fascinatingly, while the power transfers achieved by phase-only BDAO with no noise are slightly lower than the full-wave BDAO power transfers, phase-only BDAO appears to tolerate added noise far better than full-wave BDAO. In Fig. 7-8b, the $\langle \eta_{\text{phase-noise}} \rangle$ for both SNR₀ = 6 dB and 3 dB lie almost directly underneath $\langle \eta_{\text{phase}} \rangle$ for the $D_f$ values shown and are in fact higher than their full-wave counterparts.

Both Figs. 7-9 and 7-10 demonstrate that in strong and very strong turbulence, the added noise has very little effect on the mean steady-state power transfers of either full-wave BDAO, $\langle \eta_{\text{full-noise}} \rangle$, or phase-only BDAO $\langle \eta_{\text{phase-noise}} \rangle$. In fact, in both Figs. 7-9 and 7-10, the power transfers for SNR₀ = 6 dB and 3 dB lie almost exactly underneath the mean power transfers achieved with noiseless BDAO. Moreover, in Fig. 7-10, the mean power transfers for SNR₀ = 6 dB and 3 dB lie directly on top of one another in both the full-wave and phase-only plots.

We next consider the ergodic secret-key rates of an FSO link implementing ds-BB84 QKD and using phase-only BDAO with AWGN that has an initial SNR of either SNR₀ = 6 dB or 3 dB. We assume that the FSO link has the parameters listed in Table 2.3, that the QKD link experiences background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and that the link's modulation rate $R_{\text{mod}} = 10$ Gbps.
Figure 7-9: Strong turbulence, $\sigma_\chi^2 = 1.37$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for SNR$_0 = 6$ dB and 3 dB vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. The crosses connected by lines are the average no-pass power-in-aperture $\langle \tilde{\eta}_{\text{FresAO}} \rangle$, while $\langle \eta_1 \rangle^{UB}$ and $e^{-\alpha L} \eta_1^{\text{vac}}$ are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers $\langle \tilde{\eta}_1^{\text{full}} \rangle$ in no noise and $\langle \tilde{\eta}_1^{\text{full-noise}} \rangle$ in AWGN are stars, while the steady state phase-only BDAO power transfers $\langle \tilde{\eta}_1^{\text{phase}} \rangle$ in no noise and $\langle \tilde{\eta}_1^{\text{phase-noise}} \rangle$ in AWGN are squares.
Figure 7-10: Very strong turbulence, $\sigma^2 = 13.67$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers for $\text{SNR}_0 = 6 \text{ dB}$ and $3 \text{ dB}$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO with AWGN. The crosses connected by lines are the average no-pass power-in-aperture $\langle \tilde{\eta}_{\text{recAO}} \rangle$, while $\langle \eta_1 \rangle^{\text{UB}}$ and $e^{-\alpha L} \eta_1^{\text{vac}}$ are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers $\langle \tilde{\eta}_1^{\text{full}} \rangle$ in no noise and $\langle \tilde{\eta}_1^{\text{full-noise}} \rangle$ in AWGN are stars, while the steady state phase-only BDAO power transfers $\langle \tilde{\eta}_1^{\text{phase}} \rangle$ in no noise and $\langle \tilde{\eta}_1^{\text{phase-noise}} \rangle$ in AWGN are squares.
Figure 7-11: Moderate turbulence, $\sigma^2_\alpha = 0.137$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10\text{Gbps}$. Crosses are the average power-in-aperture secret-key rate $\langle R_{\text{ds-BB84}}(\eta_{\text{recAO}}) \rangle$. The upper bound $\langle \eta_1 \rangle^{\text{UB}} R_{\text{ds-BB84}}(1)$ and no-turbulence rate lower bound $R_{\text{ds-BB84}}(e^{-\alpha L} \eta_1^{\text{vac}})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{\text{ds-BB84}}(\eta_1^{\text{phase-noise}}) \rangle$ (and $\langle R_{\text{ds-BB84}}(\eta_1^{\text{phase-noise}}) \rangle$) for varying SNR (no noise) are squares.

Figures 7-11 through 7-13 plot these ergodic rates for moderate, strong, and very strong turbulence, respectively.

Figures 7-11 and 7-12 show that there are almost no differences in the ergodic secret-key rates achieved by the noiseless or noisy phase-only BDAO systems. Figure 7-13 demonstrates that the added noise yields a slightly higher ergodic secret-key rate in the far-field regime than that of the noiseless phase-only BDAO system. The most interesting feature of these plots, however, is the fact that phase-only BDAO is very tolerant to noise, presumably due to the decreasing effects of the fixed noise power as the signal power at each iteration is boosted by the application of phase-only BDAO.

Having shown that the secret-key rates of a ds-BB84 communication link (and re-
Figure 7-12: Strong turbulence, $\sigma^2 = 1.37$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{\text{ds-BB84}}(\eta_1) \rangle$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{\text{mod}} = 10$ Gbps. Crosses are the average power-in-aperture secret-key rate $\langle R_{\text{ds-BB84}}(\eta_{\text{recAO}}) \rangle$. The upper bound $\langle \eta_1 \rangle^{UB} R_{\text{ds-BB84}}(1)$ and not-turbulence rate lower bound $R_{\text{ds-BB84}}(e^{-\alpha L \eta_1^{\text{vac}}})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{\text{ds-BB84}}(\eta_1^{\text{phase-noise}}) \rangle$ for varying SNR (no noise) are squares.
Figure 7-13: Very strong turbulence, $\sigma^2 = 13.67$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{ds-BB84}(\xi_1) \rangle$ vs. Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $\eta_0 = 10^{-4}$ photons/channel use, and modulation rate $R_{mod} = 10$ Gbps. Crosses are the average power-in-aperture secret-key rate $\langle R_{ds-BB84}(\xi_{freAo}) \rangle$. The upper bound $\langle \eta_1 \rangle^{UB} R_{ds-BB84}(1)$ and no-turbulence rate lower bound $R_{ds-BB84}(e^{-\alpha L_y^{vac}})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{ds-BB84}(\xi_{1\text{phase-noise}}) \rangle$ for varying SNR (no noise) are squares.
ally, any communication link) are almost unaffected by phase-only conjugate transmitters making noisy measurements, we now assess the effect of time-varying turbulence on the steady-state power transfer of links applying either full-wave or phase-only BDAO.

7.2 FSO links operating with non-instantaneous BDAO in wind

In Chapter 2, we assumed that the atmosphere, with its coherence time on the order of milliseconds, was frozen relative to the nanosecond-long duration of a single bit in a Gbps-communication link. This nanosecond time scale is a reasonable assumption for a high-rate communication link with a transmitter that encodes information on the power-transfer optimizing spatial modes to which a BDAO system has converged. It is not clear, however, whether a BDAO system operating in time-varying turbulence would converge or would even offer a significant performance increase, especially if the conjugate transmitters themselves require a time on the order of the atmospheric coherence time to measure and generate conjugate optical waves. BDAO’s convergence and guarantee of ultimate performance relies on the reciprocity of the turbulence kernel between the $z = 0$ and $z = L$ planes for the duration of the feedback algorithm. Thus, it behooves us to relax our frozen-turbulence assumption and incorporate wind speed into our turbulence simulations to gauge the performance decrease, if any, caused by wind speeds experienced in conjunction with time delays in the BDAO conjugate transmitters.

7.2.1 Full-wave and phase-only bidirectional compensation with wind

Figures 7-14 and 7-15 depict full-wave and phase-only BDAO protocols operating in the presence of wind along the propagation path. In both scenarios, we assume that the conjugate transmitter makes noiseless measurements of the incoming wave at its
aperture and then generates either the full-wave conjugate of the measured wavefront or applies the conjugate of the phase to a focused uniform-intensity beam.

![Diagram](image)

Figure 7-14: A model for $k^{th}$ iteration bidirectional full-wave compensation with time-delayed compensation through atmospheric turbulence that is time varying because of a transverse wind with speed $v_w$.

In the case of BDAO operation with wind, however, the turbulence can no longer be viewed as frozen, thus necessitating that we introduce a time delay $t_\Delta$ into the conjugate transmitter to approximate the fact that making a continuous measurement of a wave front and generating its conjugate will take some finite amount of time. In the case of BDAO (full-wave or phase-only) conjugate transmitters using an array of heterodyne receivers to measure the wavefront and electro-optic modulators to generate their (full-wave or phase-only) conjugate beams, the time it takes the heterodyne receivers to integrate their respective photocurrent count to get a measurement will add latency and staleness to the outgoing beam if the coherence time of the atmospheric turbulence is on the order of the $t_\Delta$-delays being introduced at each iteration of BDAO. Thus, in the absence of exact fourth-order statistics for time-varying turbulence that would allow us to calculate the power transfers at each iteration of full-wave and phase-only BDAO in the presence of wind, we use POPS to simulate the power transfers of such non-instantaneous BDAO systems operating in time-varying turbulence.

The power transfer on the $k^{th}$ pass of the full-wave BDAO algorithm in wind achieved when transmitting $v_k(\rho)$ will be denoted as $\bar{\eta}_1^{\text{full-wind}}(k)$, and $U_0(\rho)$ will be
used as the initial beacon signal. Its steady-state power transfer (if it converges), \( \tilde{\eta}_1^{\text{full-wind}}(k \rightarrow \infty) \), will be denoted as \( \tilde{\eta}_1^{\text{full-wind}} \). The power transfer on the \( k \)th pass of the phase-only BDAO algorithm in wind achieved when transmitting \( v_k(\rho) \) will be denoted as \( \tilde{\eta}_1^{\text{phase-wind}}(k) \), and \( U_0(\rho) \) will be used as the initial beacon signal. Its steady state power transfer (if it converges), \( \tilde{\eta}_1^{\text{phase-wind}}(k \rightarrow \infty) \), will be denoted as \( \tilde{\eta}_1^{\text{phase-wind}} \).

### 7.2.2 Power transfer statistics of full-wave and phase-only BDAO with wind

In this section, we present POPS-simulated results for the statistics of the \( \tilde{\eta}_1^{\text{full-wind}}(k) \) and \( \tilde{\eta}_1^{\text{phase-wind}}(k) \) values after four passes through the atmosphere. The FSO link parameters assumed here are those given in Table 2.3. We compare the POPS-simulated power transmissivities of an FSO link operating with full-wave or phase-only BDAO with a delay \( t_\Delta = 0.5 \text{ ms} \) at a wind speed of \( v_w = 12 \text{ m/s} \) transverse to the propagation direction of the wave\(^1\) to the corresponding power transmissivities for frozen turbulence from Fig. 2-4.

We begin by considering the convergence behavior of the clear-weather turbulence,

\(^1\)According to the Beaufort Wind Scale [94], a wind velocity of \( v_w = 12 \text{ m/s} \) on land is a strong breeze that causes large tree branches to move.
extinction-loss neglecting \((e^{-\alpha L} = 1)\) power transfers \(\tilde{n}_1^{\text{full-wind}}(k)\) and \(\tilde{n}_1^{\text{phase-wind}}(k)\) simulated by POPS for this choice of \(t_\Delta\) and \(v_w\) for all Fresnel-number products \(D_f\) listed in our notional case in Table 2.3. Beta distributions were fit to each \(\tilde{n}_1^{\text{full-wind}}(k)\) and \(\tilde{n}_1^{\text{phase-wind}}(k)\) resulting in probability distributions

\[
\beta_{\tilde{n}_1^{\text{full-wind}}}(\eta; a(D_f, \sigma_X^2), b(D_f, \sigma_X^2)) \quad \text{and} \quad \beta_{\tilde{n}_1^{\text{phase-wind}}}(\eta; a(D_f, \sigma_X^2), b(D_f, \sigma_X^2))
\]

(which we abbreviate as \(\beta_{\tilde{n}_1^{\text{full-wind}}}(k)\) and \(\beta_{\tilde{n}_1^{\text{phase-wind}}}(k)\)).

To check the convergence of the \(\beta_{\tilde{n}_1^{\text{full-wind}}}(k)\) and \(\beta_{\tilde{n}_1^{\text{phase-wind}}}(k)\) with increasing \(k\) for a given \(D_f\) and \(\sigma_X^2\), we use the Kullback-Liebler (KL) divergence test to see whether the \(\beta_{\tilde{n}_1^{\text{full-wind}}}(k)\) (\(\beta_{\tilde{n}_1^{\text{phase-wind}}}(k)\)) for \(k = 0, 1, 2, 3\) converge to a steady state distribution, which we take to be \(\beta_{\tilde{n}_1^{\text{full-wind}}}(4)\) (\(\beta_{\tilde{n}_1^{\text{phase-wind}}}(4)\)) for full-wave BDAO (phase-only BDAO) operating with \(v_w = 12\) m/s and \(t_\Delta = 0.5\) ms.

In Fig. 7-16, the \(D\left(\beta_{\tilde{n}_1^{\text{full-wind}}}(k)\|\beta_{\tilde{n}_1^{\text{full-wind}}}(4)\right)\) and \(D\left(\beta_{\tilde{n}_1^{\text{phase-wind}}}(k)\|\beta_{\tilde{n}_1^{\text{phase-wind}}}(4)\right)\) vs. the Fresnel number product for moderate \((\sigma_X^2 = 0.137)\), strong \((\sigma_X^2 = 1.367)\), and very strong turbulence \((\sigma_X^2 = 13.67)\) are plotted for \(k = 0, 1, 2, 3\). We omit the KL divergence for the mild \((\sigma_X^2 = 0.014)\) case because the steady-state distributions \(\beta_{\tilde{n}_1^{\text{full-wind}}}\) and \(\beta_{\tilde{n}_1^{\text{phase-wind}}}\) converge almost immediately at \(k \geq 1\) and are nearly Dirac-delta functions (or beta distributions with very small variance) in mild turbulence. We see that for all Fresnel-number products \(D_f\) and turbulence strengths \(\sigma_X^2\), \(D\left(\beta_{\tilde{n}_1^{\text{full-wind}}}(k)\|\beta_{\tilde{n}_1^{\text{full-wind}}}(4)\right)\) and \(D\left(\beta_{\tilde{n}_1^{\text{phase-wind}}}(k)\|\beta_{\tilde{n}_1^{\text{phase-wind}}}(4)\right)\) for \(k = 3\) are much closer to 0 than for any \(k < 3\), showing that the beta distributions fitted to \(\tilde{n}_1^{\text{full-wind}}(4)\) and \(\tilde{n}_1^{\text{phase-wind}}(4)\) are fairly good approximations to the steady state single-spatial-mode power transfers \(\tilde{n}_1^{\text{full-wind}}\) and \(\tilde{n}_1^{\text{phase-wind}}\), allowing us to treat \(\tilde{n}_1^{\text{full-wind}}(4)\) and \(\tilde{n}_1^{\text{phase-wind}}(4)\) as such.

Figure 7-17 plots the histograms for \(\tilde{n}_1^{\text{full}}\) (plotted with filled green bars) and \(\tilde{n}_1^{\text{phase}}\) (plotted with open green bars) and their corresponding beta-distribution fits as well as the histograms for \(\tilde{n}_1^{\text{full-wind}}\) (plotted with solid purple bars) and \(\tilde{n}_1^{\text{phase-wind}}\) (plotted with open purple bars) and their beta distribution fits for varying turbulence strengths and Fresnel-number product \(D_f = 0.05\) with all other parameters given in Table 2.3. For \(t_\Delta = 0.5\) ms, the wind speed of \(v = 12\) m/s clearly affects the probability distribution of the power transfer. In moderate, strong, and very strong
Figure 7-16: Convergence behavior of the power transmissivity distributions $\eta_{\text{full-wind}}(k)$ and $\eta_{\text{phase-wind}}(k)$ for full-wave and phase-only BDAO for an FSO link with no extinction loss and parameters given in Table 2.3 for moderate ($\sigma_\chi^2 = 0.137$), strong ($\sigma_\chi^2 = 1.367$), and very strong turbulence ($\sigma_\chi^2 = 13.67$) operating with $v_w = 12$ m/s and $t_\Delta = 0.5$ ms. KL divergences $D \left( \beta_{\eta_{\text{full-wind}}(k)} || \beta_{\eta_{\text{full-wind}}(4)} \right)$ for full-wave BDAO and $D \left( \beta_{\eta_{\text{phase-wind}}(k)} || \beta_{\eta_{\text{phase-wind}}(4)} \right)$ and phase-only BDAO are plotted for $k = 0, 1, 2,$ and 3.
Figure 7-17: Histograms for $\hat{\eta}^{\text{full}}_1$ (plotted with filled green bars) and $\hat{\eta}^{\text{phase}}_1$ (plotted with open green bars) and their corresponding beta-distribution fits plus histograms for $\hat{\eta}^{\text{full-noise}}_1$ (plotted with solid orange bars) and $\hat{\eta}^{\text{phase-noise}}_1$ (plotted with open orange bars) operating with wind speed $v_w = 12 \text{ m/s}$ and time delay $t_\Delta = 0.5 \text{ ms}$ for an FSO link with $D_f = 0.05$, no extinction loss, and parameters given in Table 2.3.
turbulence, the $\langle \eta_{\text{full-wind}} \rangle$ and $\langle \eta_{\text{phase-wind}} \rangle$ is less than the no-wind, no-noise average power transfers $\langle \eta_{\text{full}} \rangle$ and $\langle \eta_{\text{phase}} \rangle$. Additionally, in strong and very strong turbulence, the distributions of the $\eta_{\text{full-wind}}$ and $\eta_{\text{phase-wind}}$ skew more heavily towards zero than do the distributions of $\eta_{\text{full}}$ and $\eta_{\text{phase}}$.

### 7.2.3 Communication over FSO links with extinction

Figures 7-18 through 7-20 plot the average power transfers for BDAO operating with no time delay in frozen turbulence and for BDAO operating with a time delay $t_{\Delta} = 0.5$ ms in a wind blowing transversely at either 3 m/s or 12 m/s. An FSO link with the parameters listed in Table 2.3 is assumed. The ultimate upper bound on the link’s power transfer in frozen turbulence, $\langle \eta_{\text{UB}} \rangle$, and the no-turbulence power transfer in frozen turbulence, $e^{-\alpha L} \eta_{\text{vac}}$, are plotted as solid and dashed blue lines, respectively, while the average no-pass power-in-aperture, $\langle \hat{\eta}_{\text{RecAO}} \rangle$, is plotted with red crosses. The first point that emerges from Figs. 7-18 through 7-20 is that for all turbulence strengths, the power transfers of phase-only BDAO are all less than their corresponding full-wave power transfers in both the frozen and time-varying turbulence cases.

In moderate turbulence, the effect of the 5 ms delay at the conjugate transmitter in combination with the 3 m/s or 12 m/s is so minimal that the steady-state power transfers of $\langle \eta_{\text{full-wind}} \rangle$ ($\langle \eta_{\text{phase-wind}} \rangle$) lie almost directly on top of the no-wind steady-state power transfers $\langle \eta_{\text{full}} \rangle$ ($\langle \eta_{\text{phase}} \rangle$) for full-wave (phase-only) BDAO. Figure 7-19 shows that even a wind of 12 m/s has the same minimal effect in strong turbulence, although the steady-state power transfers of links with $D_f \leq 0.05$ are slightly below $\langle \hat{\eta}_{\text{RecAO}} \rangle$. In very strong turbulence, the wind-speed induced decreases are similarly minimal.

Thus, we conclude that higher wind-speeds can have slightly deleterious effects on links operating in the far-field. This is not surprising given that the coherence time of the atmosphere is a function of both its coherence length and the wind speed along the link. In the far field, increasing the wind speed to until the $z = 0$ and $z = L$ apertures no longer see the same set of turbulence screens at each iteration.
Figure 7-18: Moderate turbulence, \( \sigma_x^2 = 0.137 \): Upper and lower bounds on \( \langle \eta_l \rangle \) and average BDAO power-transfers vs. the Fresnel-number product \( D_f \) for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay \( t_\Delta = 0.5 \) ms. The crosses connected by lines are the average no-pass power-in-aperture (\( \bar{\eta}_\text{recAO} \)), while \( \langle \eta_l \rangle^{UB} \) and \( e^{-\alpha L} \eta_l^{\text{vac}} \) in frozen turbulence are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers (\( \bar{\eta}_l^{\text{full}} \)) in no wind and (\( \bar{\eta}_l^{\text{full-wind}} \)) in wind are stars, while the steady state phase-only BDAO power transfers (\( \bar{\eta}_l^{\text{phase}} \)) in no wind and (\( \bar{\eta}_l^{\text{phase-noise}} \)) in wind are squares.
Figure 7-19: Strong turbulence, $\sigma^2 = 1.37$: Upper and lower bounds on $\langle \eta_1 \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay $t_\Delta = 0.5$ ms. The crosses connected by lines are the average no-pass power-in-aperture $\langle \tilde{\eta}_{\text{frecAO}} \rangle$, while $\langle \eta_1 \rangle^{\text{UB}}$ and $e^{-\alpha L} \eta_1^{\text{vac}}$ in frozen turbulence are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers $\langle \tilde{\eta}_1^{\text{full}} \rangle$ in no wind and $\langle \tilde{\eta}_1^{\text{full-wind}} \rangle$ in wind are stars, while the steady state phase-only BDAO power transfers $\langle \tilde{\eta}_1^{\text{phase}} \rangle$ in no wind and $\langle \tilde{\eta}_1^{\text{phase-noise}} \rangle$ in wind are squares.
Figure 7-20: Very strong turbulence, $\sigma_x^2 = 13.67$: Upper and lower bounds on $\langle \eta \rangle$ and average BDAO power-transfers vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3 operating with BDAO in no wind and in a wind of speed 3 m/s or 12 m/s with a BDAO time delay $t_\Delta = 0.5$ ms. The crosses connected by lines are the average no-pass power-in-aperture $\langle \tilde{\eta}_{\text{freeAO}} \rangle$, while $\langle \eta \rangle^{UB}$ and $e^{-\alpha L \eta_{\text{vac}}}$ in frozen turbulence are plotted as solid and dashed blue lines. The steady state full-wave BDAO power transfers $\langle \tilde{\eta}_1^{\text{full}} \rangle$ in no wind and $\langle \tilde{\eta}_1^{\text{full-wind}} \rangle$ in wind are stars, while the steady state phase-only BDAO power transfers $\langle \tilde{\eta}_1^{\text{phase}} \rangle$ in no wind and $\langle \tilde{\eta}_1^{\text{phase-noise}} \rangle$ in wind are squares.
Figure 7-21: Moderate turbulence, $\sigma^2_z = 0.137$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{ds-BB84}(\eta_1) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{mod} = 10$ Gbps. Crosses are the average power-in-aperture secret-key rate $\langle R_{ds-BB84}(\bar{\eta}_{recAO}) \rangle$. The upper bound $\langle \eta_1 \rangle^{UB} R_{ds-BB84}(1)$ and no-turbulence rate lower bound $R_{ds-BB84}(e^{-\alpha L \eta_1^{vac}})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{ds-BB84}(\bar{\eta}_{phase}) \rangle$ for varying wind speeds (no wind) with a BDAO time delay $t_\Delta = 0.5$ ms are squares.

would decrease the steady-state power transfer of a BDAO link. In this scenario, the time-varying atmosphere no longer appears to be frozen from the perspective of the conjugate transmitters operating at $z = 0$ and $z = L$ with time delay $t_\Delta$.

Next we consider the ergodic secret-key rates of an FSO link implementing ds-BB84 QKD and using phase-only BDAO with a time delay $t_\Delta = 0.5$ ms in a wind blowing at speed 3 m/s or 12 m/s. We assume that the FSO link has the parameters listed in Table 2.3, that the QKD link experiences background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and that the link’s modulation rate is $R_{mod} = 10$ Gbps. Figures 7-21 through 7-23 plot these ergodic rates for moderate, strong, and very strong turbulence, respectively.

In moderate turbulence, the wind speeds we consider have little effect on the
Figure 7-22: Strong turbulence, $\sigma_X^2 = 1.37$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{ds-BB84}(\eta) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-1}$ photons/channel use, and modulation rate $R_{mod} = 10$ Gbps. Crosses are the average power-in-aperture secret-key rate $\langle R_{ds-BB84}(\eta_{unc}) \rangle$. The upper bound $\langle \eta \rangle_{UB}^{U} R_{ds-BB84}(1)$ and no-turbulence rate lower bound $R_{ds-BB84}(e^{-\alpha L} \eta_{unc})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{ds-BB84}(\eta_{phase-Wind}) \rangle$ for varying wind speeds (no wind) with a BDAO time delay $t_\Delta = 0.5$ ms are squares.
Figure 7-23: Very strong turbulence, $\sigma^2 = 13.67$: Upper and lower bounds on ergodic ds-BB84 secret-key rate $\langle R_{ds-BB84}(\bar{\eta}) \rangle$ vs. the Fresnel-number product $D_f$ for an FSO link with parameters listed in Table 2.3, background plus dark count rate $n_b = 10^{-4}$ photons/channel use, and modulation rate $R_{mod} = 10$ Gbps. Crosses are the average power-in-aperture secret-key rate $\langle R_{ds-BB84}(\bar{\eta}_{recAO}) \rangle$. The upper bound $\langle \eta \rangle^UB R_{ds-BB84}(1)$ and no-turbulence rate lower bound $R_{ds-BB84}(e^{-\alpha L \eta_{vac}})$ are plotted as solid and dashed blue lines. The steady state phase-only BDAO ergodic secret-key rates $\langle R_{ds-BB84}(\bar{\eta}_{recAO}) \rangle$ for varying wind speeds (no wind) with a BDAO time delay $t_\Delta = 0.5$ ms are squares.
ergodic ds-BB84 QKD rate achieved by the FSO link. In strong turbulence, the ergodic secret-key rate for a link operating in 3 m/s wind with $D_f \leq 0.05$ with phase-only BDAO is only slightly lower than the ergodic secret-key rate of a link operating with no BDAO, while somewhat stronger degradation of the ergodic secret key rate is found for a link operating in 12 m/s wind with $D_f \leq 0.1$. In very strong turbulence, the ergodic secret key rates of an FSO link operating in a 12 m/s wind only begin to decrease sharply for $D_f \leq 0.03$. Even so, operating at $D_f = 0.01$ phase-only BDAO in a 12 m/s wind still offers a half an order of magnitude rate improvement over relying on receiver-only adaptive optics. This occurs because the Fresnel-number product $D_f = 0.01$ is achieved with aperture sizes of $d_T = d_R = 4$ cm for the link parameters assumed in Table 2.3, which is more than ten times as large as the atmospheric coherence length in very strong turbulence, $\rho_0 = 0.3$ cm. Thus, while the effects of the wind are felt, the link with $D_f = 0.01$ still has a large enough aperture to increase its power transfer by applying BDAO.

Having discussed the effects of measurement noise and wind speed on the performance of FSO links implementing ds-BB84 QKD, we conclude that extreme cases of BDAO implemented with a great deal of noise or with a large time delay relative to the coherence time of the atmosphere can degrade the performance of FSO links operating with BDAO. However, we have also shown that systems with near-unity and near-field Fresnel-number products operating in strong or very strong turbulence can still benefit greatly from the application of BDAO. Given that a typical terrestrial free-space link will experience a wide range of turbulence strengths over the course of the day, due to temperature changes and varying wind speeds, we suggest that BDAO implemented with non-ideal conjugate transmitters (which either experience appreciable time delays and/or make measurements with an extremely poor SNR) are best utilized in links that: (1) are required to provide high secret-key or data rates regardless of the turbulence strength; or (2) will consistently experience stronger than moderate turbulence during the majority of their operating conditions. Furthermore, given the apparent insensitivity of the mean power transfers achieved by phase-only BDAO in the presence of added noise or time-varying turbulence, as
well as its comparatively simple implementation, we tentatively recommended that
phase-only BDAO be implemented rather than full-wave BDAO when incorporating
BDAO into an FSO link.
Chapter 8

Conclusions and Future Work

In this thesis, we have developed bounds on and presented results for ultimate power transfers that can be achieved by FSO optical links operating with ideal and non-ideal bidirectional adaptive optics systems in atmospheric turbulence. We have filled a long-existing gap in the knowledge of the statistics of the ultimate power transfers of FSO links with near-unity Fresnel-number products operating in volumetric turbulence — a scenario which is particularly useful given a burgeoning interest in and need for purely terrestrial short-haul FSO links that can provide high-rate communication in densely populated cities or underserved rural regions.

In Chapter 2, we characterized the gap between the average power transmissivities achieved by FSO links using either no adaptive optics or receiver adaptive optics and the average power transmissivities achieved by FSO links employing either ideal or non-ideal versions of BDAO. The bounds were derived by applying the extended Huygens-Fresnel principle in combination with its normal-mode decomposition. Ideal, full-wave BDAO was shown to be a clear way to take advantage of the atmosphere’s reciprocity and achieve maximum power transfer. Because a full-wave BDAO protocol required components capable of measuring a wavefront’s magnitude and phase and then generating its conjugate, we introduced a simpler, phase-only BDAO protocol that could be implemented with commercially available components like wavefront sensors and deformable mirrors. For the case of a notional link, the single-spatial-mode power transfers enabled by full-wave and phase-only BDAO in varying turbu-
lence strengths were simulated. We showed for moderate or weaker turbulence, a system with receiver-only adaptive optics would achieve near scintillation-free performance. For strong turbulence, we found that BDAO provided order-of-magnitude improvements in the power transfers of links with near-unity Fresnel-number products. Moreover, although BDAO could not achieve scintillation-free performance in very strong turbulence, it still offered an order-of-magnitude improvement in the power transmissivity over receiver-only adaptive optics. Finally, we demonstrated that phase-only BDAO yielded power transfers that were only slightly lower than the power transfers achieved by full-wave BDAO.

In Chapters 3 through 5, bounds on the ergodic rates of classical and quantum communication protocols in terms of the average power transfer bounds in Chapter 2 were derived. We also compared these bounds on the ergodic rates to the actual ergodic rates calculated from the simulation-derived probability distributions of the full-wave and phase-only power transfers. We showed that both full-wave and phase-only BDAO enabled five-fold increases in classical communication rates in very strong turbulence as compared to receiver-only adaptive optics. The BDAO-enabled secret-key rate increases in FSO communication links were even more dramatic, due to the thresholding behavior of the QKD secret-key rates with respect to an FSO link’s power transfer. For an FSO link implementing ds-BB84 QKD, we showed that BDAO enabled significant secret-key rate increases in links with near-unity Fresnel-number products operating in strong or very strong turbulence. We also demonstrated that an FSO link using BDAO in conjunction with the FL-QKD protocol could achieve secret-key rates that were multiple-order of magnitudes higher than FSO links using ds-BB84 QKD.

In Chapter 6, we summarized results from our previous work [88, 89] that bounded the ultimate rates of multi-spatial-mode classical communication, and then derived new bounds on the ergodic secret-key rates of multi-spatial-mode FSO links implementing either ds-BB84 QKD or FL-QKD. In Chapter 7, we considered the operation of full-wave and phase-only BDAO links that either made noisy wavefront measurements or operated with a time delay in time-varying turbulence. We found that in-
corporating AWGN with a particular initial SNR into full-wave or phase-only BDAO resulted in a near-constant decrease in the average power transfers from the average power transfers achievable with the corresponding noiseless system for all Fresnel-number products in moderate turbulence, while in stronger turbulence AWGN had almost no effect. In the case of a system operating in time-varying turbulence with a delay, the power transfers and communication rates at far-field Fresnel-number products, whose aperture sizes were on the order of the atmospheric coherence area, were significantly affected by wind along the propagation path. After analysis of the average power transfers and the ergodic ds-BB84 secret-key rates, we concluded that phase-only BDAO operating in time-varying turbulence with a significant delay or phase-only BDAO operating with large AWGN still yielded large increases in the secret-key rate in strong or very strong turbulence, but suffered some decreases in the secret-key rate in moderate or weaker turbulence.

Having given the reader some idea of the Fresnel-number product regions and turbulence strengths in which even non-ideal, noisy, or time-delayed BDAO has great utility, we now discuss possible extensions to and implementations of BDAO. At the time of publication of [35, 36], the major issue that prevented further research into the implementation of full-wave BDAO architectures was the lack of available technologies with which to implement perfect (or even imperfect) wavefront measurement and conjugation. Today, these enabling technologies exist, making implementation of full-wave BDAO far closer to reality. Any such physical implementations of conjugate transmitters will necessarily be imperfect (in the sense that they will experience both noise and will not be able to generate conjugated wavefronts instantaneously) thus reducing the degree to which the average power transfers approach those of ideal, full-wave BDAO systems discussed in Chapter 2.

Two principal approaches to realizing full-wave conjugate transmitters are as follows. In the first, a measurement of the incoming wavefront is made using an array of heterodyne receivers. Heterodyne receivers are particularly attractive because their operation can be limited solely by signal-light quantum noise if the power of their local oscillator is sufficiently high. However, implementation of this coherent array
architecture has its challenges as well. Because the local oscillator (LO) sets the reference phase from which a heterodyne quadrature measurement is made, the LO will have to be split and shared among every heterodyne detector in the array in order to ensure accurate measurement of the entire incoming wavefront. Additionally, the coherent array and number of heterodyne receivers in the array will have to be sized such that good spatial mode coupling between the incoming, turbulence-distorted wavefront and each individual heterodyne detector is achieved to minimize any potential losses at the receiver. A possible way to implement a phase-only conjugate transmitter would be to apply the conjugate of the measured phase to a field with a fixed amplitude like a Gaussian electromagnetic mode.

A second candidate for the implementation of a full-wave conjugate transmitter is an array of tunable Mach-Zehnder interferometers (MZIs). Advances in the fabrication of integrated photonic circuits have enabled the design and fabrication of arrays of tunable MZIs [95, 96] that are capable of approximately measuring both the magnitude and phase of incident wavefronts and then generating the conjugates of those wavefronts, in combination with the correct optical setup of fibers and optical circulators [97]. While the individual mode extractors composed of Mach-Zehnder interferometers have the potential to be lossier than their corresponding heterodyne detection elements, the fact that they could potentially be manufactured in a scalable and reliable fashion suggests that these MZI mode converters may be the most sustainable option for implementing a near-ideal conjugate transmitter with a large number of array elements.

In order to accurately predict the performance of these systems, one would have to combine the time delays and incorporate the noise statistics of the individual heterodyne detectors or MZI arrays into our POPS simulation of BDAO. Most importantly, POPS would have to take the spatially discretized measurements made by the array of MZIs or heterodyne detectors into account. It could become prohibitive to use POPS simulation to make a comprehensive assessment of the average single-spatial-mode power transfer achieved as a function of the noise strength, time delays, and spatial quantization. Thus, it behooves us to find a way to derive the statistics (or even sim-
ply the mean) of the single-spatial-mode power transfer of a non-ideal BDAO system when given the probability distribution of the power transfer of a single-spatial-mode FSO link operating with ideal, full-wave BDAO. We believe that a way forward lies in the work of Baran [98], whose thesis dealt with conservation in signal-processing systems. While conservation theory cannot guarantee the convergence of our BDAO system to a steady-state power transfer, it can give us the value of the average steady-state power transfer if the BDAO algorithm does, in fact, converge. Most important, however, is the fact that conservation has a mechanism to deal with operations like noise, quantization, and time delays being incorporated into our conjugate transmitters. Thus, we would strongly recommend that this be the next line of analysis considered when assessing the performance of non-ideal BDAO systems.
Appendix A

Scaling property of the turbulent channel's mutual coherence function

Here we shall derive an important scaling property for the eigenspectra—and inter-modal crosstalks—when the turbulence is uniformly distributed along the propagation path in the propagation geometry from Fig. 2-1. Specifically, we shall show that the \{\gamma_m\}, the \{\gamma_m^{\text{ad}}\}, and the \{\{h_{nm}^{\text{non}}\}\} only depend on the Fresnel number product, \(D_f\), the Rytov-theory logamplitude variance, \(\sigma_\chi^2\), and the ratio of the transmitter and receiver side lengths, \(d_T/d_R\).

Let \(\{\Phi_m^{(0)}(\xi) : 1 \leq m \leq M\}\) and \(\{\phi_m^{(0)}(\xi') : 1 \leq m \leq M\}\) be orthonormal function sets on the domains \(\tilde{A}_T = \{\xi = (\xi_x, \xi_y) : |\xi_x| \leq 1/2, |\xi_y| \leq 1/2\}\) and \(\tilde{A}_R = \{\xi' = (\xi'_x, \xi'_y) : |\xi'_x| \leq 1/2, |\xi'_y| \leq 1/2\}\). We define

\[
\tilde{h}_{nm}^{\text{non}} = \int_{\tilde{A}_R} d\xi' \int_{\tilde{A}_T} d\xi \tilde{\phi}_n^{(0)\ast}(\xi') \tilde{h}(\xi', \xi) \tilde{\Phi}_m^{(0)}(\xi), \tag{A.1}
\]

where

\[
\tilde{h}(\xi', \xi) = -i \sqrt{D_f} \exp(ikL - i2\pi \sqrt{D_f} \xi' \cdot \xi) \\
\times \exp[\chi(\xi'd_R, \xi d_T) + i\phi(\xi'd_R, \xi d_T)]. \tag{A.2}
\]
Now, let
\[ \Phi_m^{(0)}(\rho) = e^{-ik|\rho|^2/2L} \tilde{\Phi}_m^{(0)}(\rho/d_T)/d_T, \] for \( 1 \leq m \leq M, \) \hspace{1cm} (A.3)

and
\[ \phi_n^{(0)}(\rho') = e^{ik|\rho'|^2/2L} \tilde{\phi}_n^{(0)}(\rho'/d_R)/d_R, \] for \( 1 \leq m \leq M, \) \hspace{1cm} (A.4)

making the \( \{\Phi_m^{(0)}(\rho)\} \) and the \( \{\phi_n^{(0)}(\rho')\} \) orthonormal function sets on \( A_T = \{\rho = (x, y) : |x| \leq d_T/2, |y| \leq d_T/2\} \) and \( A_R = \{\rho' = (x', y') : |x'| \leq d_R/2, |y| \leq d_R/2\}, \) respectively. From Eqs. (A.1)-(A.4) we then have that
\[ h_n^{\text{non}} = \int_{A_R} d\rho' \int_{A_T} d\rho \phi_n^{(0)*}(\rho') h(\rho', \rho) \Phi_m^{(0)}(\rho), \] \hspace{1cm} (A.5)

which equals \( h_n^{\text{non}} \), the \( nm \)th element of the non-adaptive channel matrix \( H_{\text{non}} \).

All the scaling properties that we are seeking can be derived from the behavior of \( \langle h_{kn}^{\text{non}} h_{km}^{\text{non}} \rangle \). From Eqs. (A.2) and (A.5) we get that
\[ \langle h_{kn}^{\text{non}} h_{km}^{\text{non}} \rangle = \int_{A_R} d\xi_1 \int_{A_R} d\xi_2 \int_{A_T} d\xi_1 \int_{A_T} d\xi_2 \]
\[ \times \phi_k^{(0)}(\xi_1) \phi_k^{(0)*}(\xi_1) \Phi_m^{(0)}(\xi_2) \Phi_m^{(0)}(\xi_2) \]
\[ \times \tilde{\Phi}_n^{(0)*}(\xi_2) \tilde{\Phi}_n^{(0)}(\xi_1). \] \hspace{1cm} (A.6)

Here, the input and output mode functions only depend on the Fresnel number product, \( D_f \), so we need only examine the behavior of
\[ \langle \tilde{h}^*(\xi_1, \xi_1) \tilde{h}(\xi_2, \xi_2) \rangle = D_f \exp[-i2\pi \sqrt{D_f} (\xi_1 \cdot \xi_1 - \xi_2 \cdot \xi_2)] \]
\[ \times \exp[-D(\Delta \xi'd_R, \Delta \xi d_T)/2], \] \hspace{1cm} (A.7)

where \( \Delta \xi' = \xi_1' - \xi_2' \) and \( \Delta \xi = \xi_1 - \xi_2 \). The wave structure function in Eq. (A.7) is given by
\[ D(\Delta \xi'd_R, \Delta \xi d_T) = 2.91k^2C_n^2 L(d_T d_R)^{5/6} \]
for a uniform turbulence-strength distribution. Because the coefficient in this expression can be reduced as follows,

\[ 2.91k^2 C_n^2 L (d_T d_R)^{5/6} = 108.5 \sigma_x^2 D_f^{5/12}, \]  

(A.9)

we have shown that \( \langle h_{kn}^\text{non} h_{km}^\text{non} \rangle \) depends only on \( D_f, \sigma_x^2, \) and \( d_T/d_R \) when we use the 5/3-law structure function. If we use our square-law approximation for the wave structure function then we get

\[ D(\Delta \xi'^d_R, \Delta \xi'^d_T) = \frac{d_T d_R}{\rho_0^2} (|\xi'|^2 d_T + \xi' \cdot \xi + |\xi|^2 d_T / d_R), \]  

(A.10)

where the coefficient obeys

\[ d_T d_R / \rho_0^2 = 85.3 \sigma_x^{12/5} \sqrt{D_f}, \]  

(A.11)

which shows that that \( \langle h_{kn}^\text{non} h_{km}^\text{non} \rangle \) depends only on \( D_f, \sigma_x^2, \) and \( d_T/d_R \) when we use the square-law structure function.

At this point we are essentially done with what we wanted to show. The average intermodal crosstalks, \( \langle |h_{nm}^\text{non}|^2 \rangle \), have already been shown to have the desired scaling behavior; just set \( kn = nm \) and \( km = nm \) in the previous paragraph's results. For the non-adaptive system we have that

\[ (\langle K_{\text{non}} \rangle)_{nm} = \sum_{k=1}^{M} \langle h_{kn}^\text{non} h_{kn}^\text{non} \rangle, \]  

(A.12)

so the eigenvalues of this matrix, i.e., the \( \{ \gamma_m^\text{non} \} \), depend only on \( D_f, \sigma_x^2 \) and \( d_T/d_R \). If we augment the \( \{ \tilde{\phi}_m^{(0)}(\xi') : 1 \leq m \leq M \} \) to a CON set, \( \{ \tilde{\phi}_m^{(0)}(\xi') : 1 \leq m < \infty \} \)
on $\tilde{A}_R$, then the completeness relation for this augmented set allows us to write

$$\langle K_{ad} \rangle_{nm} = \sum_{k=1}^{\infty} \langle h_{kn}^{\text{non}} h_{km}^{\text{non}} \rangle.$$  \hspace{1cm} (A.13)

Because the derivation in the previous paragraph is agnostic with respect to the $\{\phi_m^{(0)}(\xi')\}$, we have that the eigenvalues of $\langle K_{ad} \rangle$, which are the $\{\gamma_m^{ad}\}$, depend only on $D_f$, $\sigma_x^2$, and $d_T/d_R$. 
Appendix B

Verification and validation procedures for POPS

The Parallel Optical Propagation Software (POPS) used to simulate the performance of various implementations of BDAO throughout this thesis was developed at MIT Lincoln Laboratory in 2003. Initially created as a tool to study the effects of thermal blooming in the atmosphere, its development was redirected towards studying the propagation of optical waves through atmospheric turbulence.

Prior to this thesis, POPS had only been used to simulate ground-to-satellite links, which typically have Fresnel-number products $D_f \ll 1$. Moreover, as shown in Fig. B-1, the distribution of turbulence along these links can be regarded concentrated near one end of the propagation path because the turbulence is negligible beyond the troposphere so the relevant atmospheric path length $L_{atm}$ is much shorter than the total link length $L$. As a result, POPS simulations of ground-to-satellite links were able to achieve good performance by simulating the turbulence as one or two phase screens that lay close to the aperture on the ground. This thesis, however, demands that the volumetric nature of turbulence along a purely terrestrial link be considered and correctly simulated. Previous work with POPS did not consider the upper or lower bounds on single-spatial-mode power transfers derived in this thesis. Thus, in this appendix, we will introduce the POPS simulation parameters that must be carefully selected in order to return power-transfer statistics consistent with the upper
bound $\langle \eta \rangle^{UB}$ and lower bound $\langle \eta_{recAO} \rangle$ for optical propagation through atmospheric turbulence.

POPS simulates turbulence propagation by modeling electromagnetic fields as rectangular arrays of $n_{Pixel}$ complex elements. POPS models propagation through vacuum as a discrete Fourier transform (DFT). Thus, numerical ringing effects will be introduced unless a spatial filter is applied at each propagation step. In other words, if a spatial filter that rolls off the power at the edges of the phase screen is not applied to the field, POPS will, essentially, simulate the propagation of an electromagnetic field through a metal box. The intensity of a field propagated without a spatial filter is shown in Fig. B-2.

The spatial ringing observed in Fig. B-2 is an artifact of the use of a DFT to simulate propagation of an optical wavefront. To mitigate these spatial artifacts, POPS simulates propagation of a field at $z = 0$ through a phase screen at $z = L_1$ to a final transverse plane at $z = L_2$ as shown in Fig. B-3 and described below: As shown in Fig. B-3,

1. POPS instantiates the $n_{Pixel}$-sized array (where the physical area represented
Figure B-2: Intensity plot of a POPS-propagated field displaying grid-like spatial artifacts as a result of its propagation with a too-large \texttt{rVaryCos} filter radius.


d
\begin{figure}[h]
\centering
\includegraphics[width=0.7\textwidth]{figure.png}
\caption{POPS propagation of a field at $z = 0$ through a phase screen at $z = L_1$ to a final transverse plane at $z = L_2$.}
\end{figure}

d

2. POPS multiplies the propagated field by a radial cosine filter that is unity over the radial percentage, \texttt{rVaryCos} (which ranges from 0 to 100), of the \texttt{nPixel} mesh, and then drops off with a quarter cosine wave to 0 at 95\% of the mesh's radius.

3. POPS applies a DFT to propagate the field through vacuum from $z = 0$ to $z = L_1$.

4. POPS multiplies the field by the phase screen at $z = L_1$. 

by each pixel is $d^2/n\text{Pixel}$.

201
5. POPS multiplies the field by a radial cosine filter with radius \( r_{\text{VaryCos}} \).

6. POPS propagates the field from \( z = L_1 \) to \( z = L_2 \).

Now, we introduce verification procedures to ensure that: (1) a sufficient number of phase screens are chosen to properly simulate volumetric atmospheric turbulence; (2) sufficiently large values of \( n_{\text{Pixel}} \) are chosen; and (3) appropriate values of the spatial filter radius \( r_{\text{VaryCos}} \) are chosen.

For simulating the performance of full-wave or phase-only BDAO, the following tests must hold.

1. The coherence length of an optical field on the \( k = 0 \) iteration of BDAO, in which the \( U_0(\rho) \) has passed through turbulence and arrived at the receiver plane at \( z = L \), must have, approximately, the coherence length \( \rho_0 \) given by (2.18).

2. The average no-pass power in aperture, \( \langle \eta_{\text{recAO}} \rangle \), must be equal to the 5/3-law expression for \( \langle \eta_{\text{recAO}} \rangle \) given in (2.21).

3. All simulated power transfers must be less than \( \min(1, D_f) \), where we neglect extinction loss because POPS does not simulate it.

For a link with Fresnel-number product \( D_f \) and aperture sizes \( d_T = d_R = d \) whose BDAO performance is being simulated over a range of turbulence strengths with Rytov-logamplitude variance \( \sigma^2_{\chi}, d^2/n_{\text{Pixel}} \) must be at most \((\rho_0/5)^2\) to ensure that turbulence-distorted fields will not be undersampled. We recommend selecting the number of phase screens along the path and \( r_{\text{VaryCos}} \) simultaneously by making few-iteration runs of full-wave BDAO for candidate ranges of phase screens (which, for the 10 km path length we set as our notional case, ranged from 10 to 15) and all possible \( r_{\text{VaryCos}} \) values ranging from 1 to 99. Then, select the number of phase screens and \( r_{\text{VaryCos}} \) value that: (2) minimize unwanted spatial artifacts in the generated fields; (2) produce fields whose spatial coherence lengths are approximately \( \rho_0 \); and (3) lead to mean power transfers that are consistent with the extinction-loss neglected upper and lower bounds \( \langle \eta_1 \rangle^{UB} \) and \( \langle \eta_{\text{recAO}} \rangle \). Far-field links with \( D_f \ll 1 \) will require smaller \( r_{\text{VaryCos}} \) values, while near-field links with \( D_f \gg 1 \) will require large \( r_{\text{VaryCos}} \) values.
Figure B-4: Field intensities at $z = L$ received when the focused, flat-intensity beam $U_0(\rho)$ is transmitted for an FSO link with $D_f = 4$ and parameters listed in Table 2.3 in strong ($\sigma^2_X = 1.37$) and very strong turbulence ($\sigma^2_X = 13.67$). For this geometry, the aperture sizes are $d = 17\, \text{cm}$, and the atmospheric coherence areas are shown next to the field intensities to highlight that they have the correct correlation length.

to correctly simulate power transfer statistics that adhere to the results predicted by theory.

Figure B-4 displays the intensity plots of fields at the receiver for a single instance of turbulence in a link with $D_f = 4$ and all other assumed parameters given in Table 2.3, yielding an aperture size of $d = 17\, \text{cm}$. Squares of sides $\rho_0$, drawn to scale against the $17\, \text{cm}$ receiver aperture, are displayed next to the intensity plots. It is absolutely vital that npixel, rVaryCos, and the number of phase screens along a path be set properly for varying strengths of turbulence and Fresnel-number products for an FSO link operating with full-wave BDAO before other variants of BDAO (like phase-only BDAO or BDAO with noise or wind) are analyzed.
Appendix C

Probability distribution fits for $\tilde{\eta}_1^{\text{full}}$ and $\tilde{\eta}_1^{\text{phase}}$

The grid of beta distribution parameter values $a(D_f, \sigma_\chi^2)$ and $b(D_f, \sigma_\chi^2)$ derived from the fits applied to the $\tilde{\eta}_1^{\text{full}}$ and the $\tilde{\eta}_1^{\text{phase}}$ histograms for a given Fresnel-number product $D_f$ and Rytov-theory logamplitude variance $\sigma_\chi^2$ were fitted with a continuous function. The natural logarithms of $a(D_f, \sigma_\chi^2)$ and $b(D_f, \sigma_\chi^2)$ vs. $\ln(D_f)$ and $\ln(\sigma_\chi^2)$ were, more or less, polynomial surfaces. Thus, we were able to fit a polynomial that is fifth-order in $\ln(D_f)$ and fourth-order in $\ln(\sigma_\chi^2)$ to the $\ln(a(D_f, \sigma_\chi^2))$ and $\ln(b(D_f, \sigma_\chi^2))$ surfaces derived from either full-wave BDAO single-spatial-mode power transfer statistics or phase-only BDAO single-spatial-mode power transfer statistics. The general equation of the polynomial is given in (C.1).

$$f(D_f, \sigma_\chi^2) = \exp \left( p_{00} + p_{10}x + p_{01}y + p_{20}x^2 + p_{11}xy + p_{02}y^2 ight)$$

$$+ p_{30}x^3 + p_{21}x^2y + p_{12}xy^2 + p_{03}y^3$$

$$+ p_{40}x^4 + p_{31}x^3y + p_{22}x^2y^2 + p_{13}xy^3 + p_{04}y^4$$

$$+ p_{50}x^5 + p_{41}x^4y + p_{32}x^3y^2 + p_{23}x^2y^3 + p_{14}xy^4$$

where $x = \ln(D_f)$, $y = \ln(\sigma_\chi^2)$, $f = a$ or $b$  \hspace{1cm} (C.1)
Table C.1 and Table C.2 contain the values of the fitted coefficients $p_{ij}$ and their 95% confidence intervals for integers $0 \leq i \leq 5$ and $0 \leq j \leq 5$ for the beta distribution parameters $a$ and $b$ applied to $\hat{\eta}_{1}^{\text{full}}$ for full-wave BDAO and $\hat{\eta}_{1}^{\text{phase}}$ for phase-only BDAO, respectively.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
$i$ & $p_{ij}$ & $q_{ij}$ \\
\hline
0 & 1.355 (1.217, 1.493) & 2.707 (2.561, 2.852) \\
0.5464 (0.4741, 0.6186) & -0.5466 (-0.6228, -0.4705) \\
-0.8463 (-0.931, -0.7615) & -0.0834 (-0.1728, 0.05983) \\
0.2272 (0.2016, 0.2528) & 0.2109 (0.1839, 0.2379) \\
-0.1302 (-0.1616, -0.0987) & -0.008604 (-0.04178, 0.02457) \\
0.2025 (0.1829, 0.2221) & 0.2332 (0.2126, 0.2539) \\
-0.008543 (-0.01746, 0.003714) & 0.01806 (0.008659, 0.02746) \\
-0.03408 (-0.04039, -0.02776) & -0.03209 (-0.03875, -0.02543) \\
-0.02661 (-0.03243, -0.02079) & -0.01946 (-0.02559, -0.01332) \\
0.06043 (0.0505, 0.07037) & 0.04438 (0.0339, 0.05485) \\
-0.003232 (-0.004376, -0.002088) & -0.001729 (-0.002935, -0.0005231) \\
0.001728 (0.0005448, 0.002912) & -0.0007838 (-0.002032, 0.0004639) \\
-0.008161 (-0.00983, -0.006492) & -0.008121 (-0.00988, -0.006361) \\
0.00599 (0.002782, 0.009198) & 0.006241 (0.002859, 0.009623) \\
0.004973 (0.003784, 0.006161) & 0.003338 (0.002086, 0.004591) \\
0.0002907 (-9.702e-06, 0.0005911) & -0.0003702 (-0.0006869, 5.345e-05) \\
0.0005263 (0.0002876, 0.000765) & 0.0004824 (0.0002307, 0.000734) \\
0.0003111 (8.324e-05, 0.0005389) & 0.0001371 (-0.0001031, 0.0003773) \\
-0.0006479 (-0.0009037, -0.0003922) & -0.0006916 (-0.0009612, -0.0004219) \\
0.0009987 (0.000606, 0.001391) & 0.001059 (0.0006453, 0.001473) \\
\hline
\end{tabular}
\caption{Parameters with 95% confidence intervals for the polynomial fit function given in (2.39) for the parameters $a(D, \sigma^2)$ and $b(D, \sigma^2)$ of the $\beta$ distribution $\beta_{\eta_{1}^{\text{full}}}(\eta; a, b)$ of the steady-state power transmissivity $\eta_{1}^{\text{full}}$ for full-wave BDAO operation in an FSO link with no extinction loss and with parameters given in Table 2.3.}
\end{table}
Table C.2: Parameters with 95% confidence intervals for the polynomial fit function given in (2.39) for the parameters $a(D_f, \sigma_X^2)$ and $b(D_f, \sigma_X^2)$ of the $\beta$ distribution $\beta_{\text{phase}}(\eta; a, b)$ of the steady-state power transmissivity $\eta_{\text{phase}}$ for full-wave BDAO operation in an FSO link with no extinction loss and with parameters given in Table 2.3.
Appendix D

Secret-key rate of BB84 QKD with decoy states

In this appendix, we will briefly review the derivation of the secret key rate for BB84 with decoy states. In this protocol, Alice sends a phase-randomized coherent state, $|\sqrt{n_s}e^{i\theta}\rangle$, with average photon number $n_s$ as her signal state. Its density operator $\hat{\rho}_A$ is therefore

$$\hat{\rho}_A = \sum_{k=0}^{\infty} \frac{n_s^k}{k!} e^{-n_s} |k\rangle \langle k|,$$

where the $\{|k\rangle\}$ are photon-number states. Alice sends signal states for only a fraction of her transmission time. The rest of the time, she polls the transmissivity-$\eta$ Alice-to-Bob channel with phase-randomized coherent states of average photon number not equal to $n_s$, i.e. $\{|\sqrt{n}e^{i\theta}\rangle\}$. In this manner, she completely characterizes the channel in terms of its error probabilities for varying $k$-photon states and is able to defeat a photon-number splitting attack.

We begin by defining the conditional probability, $p_B^k$, that Bob gets a detection given that Alice’s $|\sqrt{n_s}e^{i\theta}\rangle$ transmission contained $k$ photons:

$$p_B^k = (1 - (1 - \eta)^k) + (1 - e^{-n_b}) - (1 - (1 - \eta)^n)(1 - e^{-n_b})$$

$$= 1 - (1 - \eta)^k e^{-n_b},$$

where $n_b$ is the background noise level.
where (D.2) is the probability of the union of two independent events: (1) Bob gets a
detection from one of the $k$ photons; and (2) Bob gets a detection due to background
light or dark counts. When $n_b \ll 1$ is assumed, (D.3) reduces to

$$p^B_k = 1 - (1 - \eta)^k (1 - n_b).$$  
(D.4)

All following results will be derived for $n_b \ll 1$.

The probability of Bob’s getting a detection when Alice’s $|\sqrt{n_s}e^{i\theta}\rangle$ transmission
contains 1 photon is then

$$P^B_{1:n_s} = n_s e^{-n_s} p^B_1 = n_s e^{-n_s} (n_b + (1 - n_b)\eta),$$  
(D.5)

and the probability of Bob’s getting a detection from Alice’s $|\sqrt{n_s}e^{i\theta}\rangle$ transmission is

$$P^B_{n_s} = \sum_{k=0}^{\infty} \frac{e^{-n_s} n_s^k}{k!} p^B_k = 1 - (1 - n_b) e^{-n_s}.$$  
(D.6)

We assume that all errors at Bob’s end are due to background plus dark counts at
his two detectors. Thus, the error rate for a 0-photon signal would be 1/2, since the
detected output would be totally random in that case. Thus, the quantum bit error
rate (QBER) $e_k$ when Alice’s $|\sqrt{n_s}e^{i\theta}\rangle$ transmission contains $k$ photons is

$$e_k = \frac{\frac{1}{2} (1 - e^{-n_b})}{p^B_k} = \frac{\frac{1}{2} n_b}{p^B_k},$$  
(D.7)

for $n_b \ll 1$. For a single-photon signal and $n_b \ll 1$,

$$e_1 = \frac{\frac{1}{2} n_b}{p^B_1}.$$
The QBER for Alice's $|\sqrt{n_s}e^{i\theta}\rangle$ signal state is therefore

$$\frac{1}{2}n_b \quad \frac{1}{1 - (1 - n_b)(1 - \eta)}. \quad (D.8)$$

Now, we can write out the decoy-state BB84 secret key rate in bits/channel use for an \(\eta\)-transmissivity Alice-to-Bob channel as

$$\Delta I = \max[0, P_{1:n_s}^B(1 - H_2(e_1)) - P_{n_s}^B H_2(E_{n_s})], \quad (D.10)$$

where \(H_2(x)\) is the binary entropy function.

Lemma D.1 For fixed average background plus dark counts \(n_b\), where \(n_b \ll 1\), and fixed average photon number \(n_s\), the function

$$\Delta I = \max \left[0, P_{1:n_s}^B(\eta, n_s, n_b)(1 - H_2(e_1(\eta, n_s, n_b))) - P_{n_s}^B(\eta, n_s, n_b)H_2(E_{n_s}(\eta, n_s, n_b))\right] \quad (D.11)$$

is increasing in the overall power transmissivity \(\eta\).

Proof We will show that \(\frac{\partial \Delta I}{\partial \eta} \geq 0\) for fixed \(n_b \ll 1\) and \(n_s \leq 1\) for \(0 \leq \eta \leq 1\) when

$$P_{1:n_s}^B(\eta, n_s, n_b)(1 - H_2(e_1(\eta, n_s, n_b))) - P_{n_s}^B(\eta, n_s, n_b)H_2(E_{n_s}(\eta, n_s, n_b)) \geq 0. \quad (D.12)$$

Since

$$\frac{\partial \Delta I}{\partial \eta} = \frac{e^{-n_s(1+\eta)}(1 - n_b)n_s}{\ln(2)} \times \left(e^{n_s} \ln \left(1 - \frac{n_b}{2(1 - e^{-n_s\eta}(1 - n_b))}\right) + e^{n_s} \ln \left(2 - \frac{n_b}{n_b + \eta(1 - n_b)}\right)\right)$$

$$= n_s(1 - n_b) \left(e^{-n_s \log_2 (1 - E_{n_s})} + e^{-n_s \log_2 (2(1 - e_1))}\right)$$
we must prove that
\[ e^{-(1-\eta)n_s} \log_2 (2(1-e_1)) + \log_2 (1 - E_{n_s}) \geq 0 \] (D.14)
to complete the proof. Noting that \( \Delta I \) can be rewritten as
\[ \Delta I = \frac{n_b}{2} \left( n_s e^{-n_s} \left( 1 - H_2(e_1) \right) \frac{1 - E_{n_s}}{e_1} - \frac{H_2(E_{n_s})}{E_{n_s}} \right) \] (D.15)
where the right-hand side is nonnegative, we show that (D.14) is an upper bound on \( \Delta I \) as follows:
\[ \Delta I = n_s e^{-n_s} \left( \log_2 (2(1-e_1)) + \log \left( \frac{e_1}{1-e_1} \right) \right) + \frac{1 - E_{n_s}}{E_{n_s}} \log_2 (1 - E_{n_s}) + \log_2 (E_{n_s}) \] (D.16)
\[ \leq n_s e^{-n_s} \log_2 (2(1-e_1)) + \frac{1 - E_{n_s}}{E_{n_s}} \log_2 (1 - E_{n_s}) \] (D.17)
\[ \leq n_s e^{-n_s} \log_2 (2(1-e_1)) + \log_2 (1 - E_{n_s}) \] (D.18)
\[ \leq e^{-(1-\eta)n_s} \log_2 (2(1-e_1)) + \log_2 (1 - E_{n_s}) \] (D.19)
where (D.17) follows from \( 0 \leq e_1, E_{n_s} \leq 1/2 \), which means that \( \log_2(e_1/(1-e_1)) \) and \( \log_2(E_{n_s}) \) are both negative. (D.18) follows from \( \frac{1 - E_{n_s}}{E_{n_s}} \geq 1 \) and \( \log_2 (1 - E_{n_s}) \leq 0 \).
To arrive at (D.19), which is the same as the left-hand side of (D.14), we use the fact that \( \log_2 (2(1-e_1)) \geq 0 \) since \( e_1 \leq 1/2 \).

We must now prove that \( n_s e^{-n_s} \) is bounded above by \( e^{-(1-\eta)n_s} \) for all candidate values of \( n_s \) and all possible values of \( \eta \). Using the fact that \( x - 1 \) is an upper bound on \( \ln(x) \), we obtain the condition \( n_s \) that ensures the upper bound holds:
\[ n_s e^{-n_s} \leq e^{-(1-\eta)n_s} \implies n_s \eta \geq \ln(n_s) \]
For \( n_s \leq 1 \), as is the case for ds-BB84 quantum key distribution, the right-hand side
of the preceding condition is non-positive, whereas the left-hand side is non-negative, so it is always satisfied. Thus, (D.14) is an upper bound on $\Delta I$, which in turn is nonnegative. We have now completed our proof that $\frac{\partial \Delta I}{\partial \eta} \geq 0$ for fixed $n_b \ll 1$, $n_s \leq 1$, and $\eta$ where $\Delta I \geq 0$.

**Lemma D.2** For fixed average background plus dark counts $n_b$, where $n_b \ll 1$, and fixed average photon number $n_s$,

$$S_1(\eta, n_s, n_b) = P^B_{n_s}(\eta, n_s, n_b)(1 - H_2(e_1(\eta, n_s, n_b)))$$  \hspace{1cm} (D.20)

is convex in $\eta$.

**Proof** We will show that $\frac{\partial^2 S_1}{\partial \eta^2} \geq 0$ for fixed $n_b$ and $n_s$ and $0 \leq \eta \leq 1$. Straightforward differentiation gives

$$\frac{\partial^2 S_1}{\partial \eta^2} = \frac{e^{-n_s}(1 - n_b)^2n_bn_s}{n^3_b + 3(1 - n_b)n_b\eta + 2(1 - n_b)^2\eta^2}$$  \hspace{1cm} (D.21)

$$\geq 0,$$

where both the numerator and denominator of (D.21) are positive because $0 \leq \eta, n_b \leq 1$, and $\eta, n_s \geq 0$.

**Lemma D.3** For fixed average background plus dark counts $n_b$, where $n_b \ll 1$, fixed average photon number $n_s$, and $P^B_{n_s}(\eta, n_s, n_b)$ and $E_{n_s}(\eta, n_s, n_b)$ defined as in (D.6) and (D.9), the function

$$S_2(\eta, n_s, n_b) = P^B_{n_s}(\eta, n_s, n_b)H_2(E_{n_s}(\eta, n_s, n_b))$$  \hspace{1cm} (D.22)

is concave in $\eta$.

**Proof** We will show that $\frac{\partial^2 S_2}{\partial \eta^2} \leq 0$ for fixed $n_b$ and $n_s$ for $0 \leq \eta \leq 1$. Straightforward
differentiation yields
\[
\frac{\partial^2 S_2}{\partial \eta^2} = \frac{-(1 - n_b) n_s^2}{\ln(2)} \left( \frac{(1 - n_b) n_b e^{-2 \eta s}}{(1 - e^{-\eta s} (1 - n_b))(2(1 - n_b)(1 - e^{-\eta s}) + n_b e^{-\eta s})} + \right.
\]
\[
\times - e^{-\eta s} \ln \left(1 - \frac{n_b}{2(1 - e^{-\eta s} + n_b)} \right) \right)
\]
(D.23)
\[
\leq 0,
\]
(D.24)

where (D.24) follows from (D.23) by noting that: (1) the coefficient is negative; and (2) each of the terms in the sum is positive since \(0 \leq n_b, e^{-\eta s} \leq 1\).

**Lemma D.4** For a fixed \(n_s, n_b > 0\), the unoptimized instantaneous secret key rate \(\Delta I(\eta, n_s, n_b)\) in bits per channel use is convex in \(\eta\), the power transmissivity of the Alice-to-Bob channel.

**Proof** \(\Delta I(\eta, n_s, n_b) = S_1(\eta, n_s, n_b) + (-S_2(\eta, n_s, n_b))\) is the sum of two convex functions as proven in Lemma D.2 and Lemma D.3. It follows that \(\Delta I(\eta, n_s, n_b)\) is convex.

**Lemma D.5** For a fixed \(n_b > 0\), the multi-mode decoy-state BB84 secret key rate \(R_{ds-BB84,M}(\mu, n_b)\) is both convex and Schur-convex in \(\mu\), the vector of the Alice-to-Bob channel’s modal power transmissivities.

**Proof** Because \(R_{ds-BB84,M}(\mu, n_b)\) is symmetric in the elements of \(\mu\), its convexity will imply its Schur-convexity [90]. To prove that \(R_{ds-BB84,M}(\mu, n_b)\) is convex in \(\mu\), consider any two vectors \(\mu^a\) and \(\mu^b\), whose elements are nonincreasing and lie in the interval \([0, 1]\). Now let \(\mu^c = p\mu^a + (1 - p)\mu^b\) for arbitrary \(p \in [0, 1]\). Defining \(n^c\) to be the modal photon allocation that achieves \(R_{\text{tot}}(\mu^c, n_b)\), we have that

\[
R_{ds-BB84,M}(\mu^c, n_b) = \max_n \sum_{m=1}^M R_{\text{mod}} \Delta I(\mu^c_m, n_m, n_b)
\]
\[
= \sum_{m=1}^M R_{\text{mod}} \Delta I(\mu^c_m, n^c_m, n_b)
\]
\[
\leq \sum_{m=1}^M (pR_{\text{mod}} \Delta I(\mu^a_m, n^a_m, n_b)
\]
\[
\leq \sum_{m=1}^M (pR_{\text{mod}} \Delta I(\mu^b_m, n^b_m, n_b)
\]
\[(1 - p)R_{\text{mod}} \Delta I (\mu_m^b, n_m^c, n_b^c) \]
\[\leq p R_{\text{ds-BB84},M}(\mu^a, n_b) + (1 - p) R_{\text{ds-BB84},M}(\mu^b, n_b) \] (D.26)

Inequality (D.25) follows from the convexity of \(\Delta I (\mu_m, n_m, n_b)\) in \(\mu_m\). Inequality (D.26), which proves that \(R_{\text{ds-BB84},M}(\mu, n_b)\) is convex (and hence Schur-convex) in \(\mu\), follows from the suboptimality of the photon modal allocation \(n^c\) for transmissivity vectors \(\mu^a\) and \(\mu^b\).
Appendix E

Secret-key rate of floodlight QKD

Lemma E.1 Alice’s mutual information, $I_A$, is concave in $\eta_{\text{atm}}$ for fixed EDFA gain $G_B$, EDFA noise $N_B$, time-frequency mode number $M = TW$, signal strength per mode $N_s \ll 1$, Bob’s tap value $\kappa_B$, and Eve’s intrusion parameter $f_E$.

Proof For fixed EDFA gain $G_B$, EDFA noise $N_B$, mode number $M = TW$, signal strength per mode $N_s$ where $N_s \ll 1$, Alice’s tap values $\kappa_A$ and $\kappa_C$, Bob’s tap value $\kappa_B$, and Eve’s intrusion parameter $f_E$, Alice’s mutual information with Bob is bits/channel use is

$$I_A = (1 - H_2(P_{\text{err}}^{\text{Alice}})).$$  \hspace{1cm} (E.1)

Here,

$$P_{\text{err}}^{\text{Alice}} = Q(\kappa_{\text{err}} \sqrt{\eta_{\text{atm}}}).$$  \hspace{1cm} (E.2)

where the constant $\kappa_{\text{err}}$ is

$$\kappa_{\text{err}} = \sqrt{2M(G_B/N_B)(1 - \kappa_B)(1 - \kappa_A)(1 - \kappa_C)(1 - f_E)N_s},$$  \hspace{1cm} (E.3)

is clearly positive, and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{u^2}{2}} du$ is the tail probability of the standard
normal distribution. Thus, $I_A$ may be written as

$$I_A(\kappa_{\text{err}}, \eta_{\text{atm}}) = 1 - H_2(Q(\kappa_{\text{err}}\sqrt{\eta_{\text{atm}}}))$$  \hspace{1cm} \text{(E.4)}$$

Now, we will show that $\frac{\partial^2 I_A}{\partial \eta_{\text{atm}}^2} \leq 0$. We have that

$$\frac{\partial^2 I_A}{\partial \eta_{\text{atm}}^2} = \frac{\alpha^4}{4 \pi^3} \left[ \frac{\partial H_2(u)}{\partial u} \left( \frac{\partial Q(t)}{\partial t} \right)_{\eta_{\text{atm}}} + \frac{\partial^2 Q(t)}{\partial t^2} \right]$$

$$- \frac{\partial^2 H_2(u)}{\partial u^2} \left( \frac{\partial Q(t)}{\partial t} \right)_{\eta_{\text{atm}}}^2,$$  \hspace{1cm} \text{(E.5)}$$

where $x = \kappa_{\text{err}}\sqrt{\eta}$, $P_{\text{err}}^{\text{Alice}} = Q(x)$, and

$$\frac{\partial H_2(p)}{\partial p} = \log_2 \left( \frac{1 - p}{p} \right)$$

$$\frac{\partial^2 H_2(p)}{\partial p^2} = \frac{-1}{p(1 - p)}$$

$$\frac{\partial Q(t)}{\partial t} = -\frac{e^{-x^2/2}}{\sqrt{2\pi}}$$

$$\frac{\partial^2 Q(t)}{\partial t^2} = x\frac{e^{-x^2/2}}{\sqrt{2\pi}}.$$  \hspace{1cm} \text{(E.5)}$$

Making the appropriate substitutions, we may write $\frac{\partial^2 I_A}{\partial \eta_{\text{atm}}^2}$ as

$$\frac{\partial^2 I_A}{\partial \eta_{\text{atm}}^2} = \frac{\kappa_{\text{err}} e^{-x^2/2}}{4 \pi^3 \sqrt{2\pi}} \left[ -(x^2 + 1) \log_2 \left( \frac{1 - P_{\text{err}}^{\text{Alice}}}{P_{\text{err}}^{\text{Alice}}} \right) - \frac{x}{(1 - P_{\text{err}}^{\text{Alice}}) P_{\text{err}}^{\text{Alice}}} \right]$$

$$\leq 0.$$  \hspace{1cm} \text{(E.6)}$$

The constraints $\kappa_{\text{err}} \geq 0$ and $0 \leq \eta \leq 1$ imply that $x \geq 0$, which in turn ensures that $0 \leq P_{\text{err}}^{\text{Alice}} \leq \frac{1}{2}$. The leading coefficient $\frac{\kappa_{\text{err}} e^{-x^2/2}}{4 \pi^3 \sqrt{2\pi}}$ is positive by inspection. Inequality (E.6) follows from $\log_2 \left( (1 - P_{\text{err}}^{\text{Alice}})/(P_{\text{err}}^{\text{Alice}}) \right) \geq 0$, thus ensuring that the term within brackets is negative for all $\alpha \geq 0$ and all $\eta : 0 \leq \eta \leq 1$.

So, we have proven that $I_A$, is concave in $\eta_{\text{atm}}$ for fixed $\kappa_{\text{err}}$ with $\kappa_{\text{err}} > 0$ and $0 \leq \eta_{\text{atm}} \leq 1$. Thus, $I_A$ is concave in $\eta_{\text{atm}}$ for fixed $G_B$, $N_B$, $M = TW$, $\kappa_A$, $\kappa_B$, $\kappa_C$, $\alpha_1$, $\alpha_2$, $\alpha_3$.
Lemma E.2 For fixed $G_B \gg 1$, $N_s \ll 1$, and $0 \leq f_E \leq 1$, $\Upsilon_E(\eta_{\text{atm}}, N_s)$ is concave in $\eta_{\text{atm}}$.

Proof We will show that $\frac{\partial^2 \Upsilon_E}{\partial \eta_{\text{atm}}^2} \leq 0$. For fixed EDFA gain $G_B$ where $G_B \gg 1$ and signal strength per mode $N_s$ where $N_s \ll 1$, we have

$$
\Upsilon_E(\eta_{\text{atm}}, N_s) = g(G_B(\eta_{\text{atm}}N_s + 1) - 1) \\
+ g((N_s\eta_{\text{atm}})^2(f_E(1-f_E)) + N_s(1-(1-f_E)\eta_{\text{atm}})) \\
+ g((N_s\eta_{\text{atm}})^2(f_E(1-f_E)) + N_s(f_E\eta_{\text{atm}})) \\
- g(N_s(1-(1-f_E)\eta_{\text{atm}}(1+N_s(1+\eta_{\text{atm}})))) \\
- g(G_B(\eta_{\text{atm}}N_s + 1) - 1 - N_s(1-(1+2f_E)\eta_{\text{atm}})), 
$$

(E.7)

where $g(x) = (x+1)\log(x+1) - x\log(x)$.

Straightforward differentiation followed by Taylor-series approximations about $N_s$ and $\frac{1}{G_B}$ yields

$$
\frac{\partial^2 \Upsilon_E}{\partial \eta_{\text{atm}}^2} = -\left(N_s \frac{f_E}{\eta_{\text{atm}}} + N_s^2 \frac{1}{1-(1-f_E)\eta_{\text{atm}}} \delta(f_E, \eta_{\text{atm}}, N_s)\right),
$$

(E.8)

with $\delta(f_E, \eta_{\text{atm}}, N_s) = 2(1-f_E)(1-(1-f_E)\eta_{\text{atm}})$

$$
\times \left(-(1-2f_E)\ln(N_s) - (1-f_E)\ln(1-(1-f_E)\eta_{\text{atm}})\right)
$$

(E.9)

Both $N_s \frac{f_E}{\eta_{\text{atm}}}$ and $N_s^2 \frac{1}{1-(1-f_E)\eta_{\text{atm}}}$ are positive since $N_s \geq 0$ and $0 \leq \eta_{\text{atm}}, f_E \leq 1$. By inspection, the $2(1-f_E)(1-(1-f_E)\eta_{\text{atm}})$ coefficient of $\delta(f_E, \eta_{\text{atm}}, N_s)$, is positive since $0 \leq f_E, \eta_{\text{atm}} \leq 1$. Moreover, the remaining factor in $\delta(f_E, \eta_{\text{atm}}, N_s)$ is also positive by inspection, since $N_s \leq 1$ and $(1-f_E)\eta_{\text{atm}} \leq 1$. Thus, we have proven that $\frac{\partial^2 \Upsilon_E}{\partial \eta_{\text{atm}}^2} \leq 0$, which makes $\Upsilon_E(\eta_{\text{atm}}, N_s)$ concave in $\eta_{\text{atm}}$.

Lemma E.3 For $N_s \ll 1$, $G_B \gg 1$, and $N_B \gg 1$, the lower bound on the multi-spatial mode FL-QKD secret key rate $R_{FL,M}^{LB}(\mu)$ is both convex and Schur-convex in $\mu$. 

219
Proof Because $R_{FL,M}^L(\mu)$ is symmetric in the elements of $\mu$, its convexity will imply its Schur-convexity [90]. Recalling that

$$R_{FL,M}^L(\mu) = \sum_{m=1}^{M} R_{FL}^L(\mu_m),$$

(E.10)

and that

$$R_{FL}^L(\mu_m) = \max_{R_{mod,m}:R_{mod,m} \leq R_{max,m}, N_m} R_{mod,m}(L^L_A(\mu_m) - \chi^L_E(\mu_m))$$

(E.11)

$$= \max_{R_{mod,m}:R_{mod,m} \leq R_{max,m}, N_m} \Delta R_{FL}(\mu_m, R_m, N_m),$$

(E.12)

we prove that $\Delta R_{FL}(\mu_m, R_m, N_m)$ is convex in $\mu_m$. Because

$$I_A^L(\mu_m) = \mu_m(1 - H_2(P_{err}^A|\eta_{nat}=1))$$

(E.13)

$$= \mu_m \kappa_{ent},$$

(E.14)

where $\kappa_{ent}$ does not depend on $\mu_m$, $I_A^L(\mu_m)$ is clearly convex in $\mu_m$. Moreover, we already have that $\chi^L_E(\mu_m)$ is concave in $\mu_m$ because $T_E(\mu_m, N_m)$ is concave in $\mu_m$ by Lemma E.2. So, because $\Delta R_{FL}(\mu_m, R_m, N_m)$ is the result of subtracting a concave function from a convex function, it is convex.

To prove that $R_{FL,M}^L(\mu)$ is convex in $\mu$, consider any two vectors $\mu^a$ and $\mu^b$, whose elements are nonincreasing and lie in the interval $[0, 1]$. Now let $\mu^c = p\mu^a + (1 - p)\mu^b$ for arbitrary $p \in [0, 1]$. Defining $N^c$ and $R^c$ to be the modal photon allocation and the modal rate modulation that achieves $R_{FL,M}^L(\mu)$, we have that

$$R_{FL,M}^L(\mu^c) = \max_{N,R} \sum_{m=1}^{M} \Delta R_{FL}(\mu^c_m, R_m, N_m).$$

(E.15)

$$= \sum_{m=1}^{M} \Delta R_{FL}(\mu^c_m, N^c_m, R^c_m)$$

(E.16)

$$\leq \sum_{m=1}^{M} p(\Delta R_{FL}(\mu^a_m, N^c_m, R^c_m) + (1 - p)\Delta R_{FL}(\mu^b_m, N^c_m, R^c_m))$$

(E.17)

$$\leq pR_{FL,M}^L(\mu^a) + (1 - p)R_{FL,M}^L(\mu^b)$$

(E.18)
Inequality (E.17) follows from the convexity of $\Delta R_{FL}(\mu_m, R_m, N_m)$ in $\mu_m$. Inequality (E.18), which proves that $R_{FLM}^{LB}(\mu)$ is convex (and hence Schur-convex) in $\mu$, follows from the suboptimality of the photon modal allocation $N^c$ and modulation allocation $R^c$ for transmissivity vectors $\mu^a$ and $\mu^b$. 

221
Bibliography


[72] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure


www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt

[75] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key

quantum key distribution over 10km in daylight and at night,” in Nonlinear
Optics: Materials, Fundamentals and Applications. Optical Society of America,

F. Marsili, S. Assefa, K. K. Berggren, and D. Englund, “On-chip detection of non-
vol. 6, Jan. 2015.


[79] S. H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola,


[81] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, “Entan-

quantum key distribution: A practical route to gigabit-per-second secret-key

key distribution: Demonstrating a new framework for high-rate secure commu-


229


