Multiple-User Quantum Optical Communication

by

Brent J. Yen

S.B., M.Eng., Electrical Engineering and Computer Science,
S.B., Mathematics,
Massachusetts Institute of Technology, 2000

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2005

Author .....
Department of Electrical Engineering and Computer Science
September 29, 2004

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

Accepted by .....
Arthur C. Smith
Chairman, Department Committee on Graduate Students

Multiple-User Quantum Optical Communication

by

Brent J. Yen

Submitted to the Department of Electrical Engineering and Computer Science
on September 29, 2004, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

A fundamental understanding of the information carrying capacity of optical channels requires the signal and physical channel to be modeled quantum mechanically. This thesis considers the problems of distributing multi-party quantum entanglement to distant users in a quantum communication system and determining the ability of quantum optical channels to reliably transmit information.

A recent proposal for a quantum communication architecture that realizes long-distance, high-fidelity qubit teleportation is reviewed. Previous work on this communication architecture is extended in two primary ways. First, models are developed for assessing the effects of amplitude, phase, and frequency errors in the entanglement source of polarization-entangled photons, as well as fiber loss and imperfect polarization restoration, on the throughput and fidelity of the system. Second, an error model is derived for an extension of this communication architecture that allows for the production and storage of three-party entangled Greenberger-Horne-Zeilinger states. A performance analysis of the quantum communication architecture in qubit teleportation and quantum secret sharing communication protocols is presented.

Recent work on determining the channel capacity of optical channels is extended in several ways. Classical capacity is derived for a class of Gaussian Bosonic channels representing the quantum version of classical colored Gaussian-noise channels. The proof is strongly motivated by the standard technique of whitening Gaussian noise used in classical information theory. Minimum output entropy problems related to these channel capacity derivations are also studied. These single-user Bosonic capacity results are extended to a multi-user scenario by deriving capacity regions for single-mode and wideband coherent-state multiple access channels. An even larger capacity region is obtained when the transmitters use non-classical Gaussian states, and an outer bound on the ultimate capacity region is presented as well.

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

Acknowledgments

I would like to thank Prof. Jeffrey Shapiro for guiding me through my graduate school years. Beyond the innumerable things I have learned from his classes and from doing research with him, I am most grateful for his confidence in me and for his constant encouragement and support. I thank my thesis committee Prof. Isaac Chuang and Prof. Vincent Chan for their helpful suggestions. I thank Prof. David Forney for suggestions and advice on the replica method. For helping me learn about optical and quantum communication and many other things, I thank: Joe Aung, Baris Erkmen, Vittorio Giovannetti, Saikat Guha, Lorenzo Maccone, and Mohsen Razavi. Lastly, I would above all like to thank my family for their love and support.

This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Army Research Office under Grant DAAD19-00-1-0177 and by the Quantum Information Science and Technology Program under Army Research Office Contract DAAD19-01-1-0647.

Contents

Chapter 1

Introduction

Optical communication systems play a key role in handling today's increasing demand for high-capacity networks. It is clear that using light to transmit information presents important fundamental and practical problems, and it is thus highly desirable to understand the ability of optical channels to reliably transmit information. At a fundamental level, all physical communication channels are subject to the laws of quantum mechanics. But while quantum effects are negligible for radio-frequency systems, quantum noise can be a dominant factor at optical frequencies. For this reason, an accurate fundamental treatment of optical communication systems requires the signal and physical channel to be modeled quantum mechanically.

Researchers have long been interested in quantum limits on the capacity of optical channels [1],[2],[3]. These capacity results have been made rigorous through the use of the Holevo-Schumacher-Westmoreland theorem [4],[5], a quantum generalization of Shannon's channel capacity theorem [6] that establishes the maximum rates of classical information that can be transmitted reliably over quantum channels. Recently, the classical capacity of the Bosonic pure-loss channel was shown to be achievable by coherent-state codes [7] and that entangling codewords over channel uses is not required for achieving capacity. Additional study of the pure-loss channel capacity with specific transmitter and receiver structures as well as applications of these results to the free-space optical channel were considered in [8].

The laws of quantum mechanics not only place limitations on communication, they also offer resources for enhancing our ability to communicate. In particular, quantum mechanics

predicts that strong correlations known as entanglement can exist between separate quantum systems. Quantum entanglement is important in the study of local-hidden variable theories of physics. For purposes of communication, entanglement serves as a basic resource for communication protocols such as teleportation [9] and superdense coding [10]. The distribution of entanglement to distant users in a quantum communication system is difficult to achieve in practice. A feasible method for creating entanglement in a practical communication system must be able to overcome transmission losses and permit users to store their entanglement long enough to carry out communication protocols. An initial teleportation experiment using singlet states was reported in [11] and [12]. A theoretical problem of interest is to quantify the increase in capacity that can be achieved when the transmitters and receivers of a quantum communication channel possess shared entanglement. For single-user quantum channels, the classical information capacity of superdense coding was obtained in [13] and [14].

In this thesis, we assume the reader has some background in quantum information theory and quantum optics. The following two sections offer brief reviews of these topics and references for those readers who desire a more thorough introduction. We end this chapter with an outline of the work in this thesis.

1.1 Quantum Information

The basic concepts in quantum information theory that will be required for the remainder of this thesis will be reviewed in this section. For additional details on quantum information the reader should consult [15].

1.1.1 Quantum States and Density Operators

The state of a quantum mechanical system is the totality of information that can be known about that system. It is represented mathematically as a unit-length vector, also known as a ket, $|\psi\rangle$, in a complex Hilbert space $\mathcal{H}$. Associated with each ket $|\psi\rangle$ is its dual vector, or bra, denoted by $\langle\psi|$. Given a fixed complete basis $\{|\phi_n\rangle\}$ of $\mathcal{H}$, we can think of $|\psi\rangle$ as a column vector of complex numbers and $\langle\psi|$ as the row vector equal to the Hermitian conjugate of $|\psi\rangle$.

A quantum bit (qubit), viz., the state of any two-level quantum system, is the basic

unit of quantum information. A qubit lives in a two-dimensional Hilbert space $\mathcal{H}_2$ and can be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis and α, β are complex numbers that satisfy $|\alpha|^2 + |\beta|^2 = 1$. In contrast to classical bits, which can assume only one of two values, 0 or 1, qubits can exist in a superposition of the states $|0\rangle$ and $|1\rangle$. More generally, the state of n qubits is a quantum state in the Hilbert space $\mathcal{H}_2^{\otimes n}$, which has dimension 2^n. For example, the state of three qubits A, B, and C, is the following superposition of eight basis states:

$$|\psi\rangle_{ABC} = \sum_{k,m,n=0,1} \alpha_{kmn}|k\rangle_A \otimes |m\rangle_B \otimes |n\rangle_C, \tag{1.2}$$

where the α_{kmn} satisfy the normalization condition $\sum_{k,m,n} |\alpha_{kmn}|^2 = 1$.

Classical uncertainty about the state of a physical system is incorporated into our description through the use of density operators. If it is known that the state of the system is $|\psi_m\rangle$ with probability p_m, then the density operator for the system is defined as

$$\hat{\rho} = \sum_m p_m |\psi_m\rangle\langle\psi_m|. \tag{1.3}$$

From this definition, it can be easily verified that $\hat{\rho}$ is a positive definite operator with unit trace. It follows that the eigenvalues $\{\lambda_n\}$ of $\hat{\rho}$ form a probability distribution. In the special case in which the state is known with certainty, the density operator consists of a single term and is a projection operator $\hat{\rho} = |\psi\rangle\langle\psi|$.

When we deal with composite systems, the density operators of the component systems are referred to as the reduced density operators. Let $\hat{\rho}_{AB}$ be the density operator for the composite system consisting of quantum systems A and B. Then, the reduced density operator for A is given by

$$\hat{\rho}_A = \mathrm{tr}_B(\hat{\rho}_{AB}), \tag{1.4}$$

where tr_B is the partial trace over system B. The partial trace operator is defined on tensor products by

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2|(\langle b_2|b_1\rangle), \tag{1.5}$$

for any vectors $|a_1\rangle$, $|a_2\rangle$ of system A and $|b_1\rangle$, $|b_2\rangle$ of system B. The definition is extended

to general mixed states $\hat{\rho}_{AB}$ by requiring the partial trace operator to be linear.

1.1.2 Measurements

Quantum measurements are commonly discussed in terms of observables, the dynamical variables of a quantum system. An observable of a quantum system is represented by a Hermitian operator $\hat{A}$. The outcome of measuring the observable $\hat{A}$ is always one of the eigenvalues a_n of $\hat{A}$, and given the state $\hat{\rho}$ of the quantum system, the probability of obtaining measurement outcome a_n is

$$p(a_n) = \langle a_n|\hat{\rho}|a_n\rangle. \tag{1.6}$$

The state immediately after the measurement is $|a_n\rangle$, the eigenket corresponding to a_n. The system is said to collapse into the post-measurement state $|a_n\rangle$.

The measurement of an observable as described above is not the most general measurement procedure one can make on a quantum system. A more general procedure involves performing a measurement on the system of interest together with an auxiliary system prepared in some initial state. This general measurement can be described by the positive operator valued measure (POVM) formalism. A POVM measurement is defined by a set of positive semidefinite operators $\{\hat{E}_m\}$ that satisfy the condition $\sum_m \hat{E}_m = \hat{I}$. If the system is in state $\hat{\rho}$, then outcome m of the POVM measurement is obtained with probability

$$p(m) = \mathrm{tr}(\hat{\rho}\hat{E}_m). \tag{1.7}$$

A POVM, without additional information, does not determine a post-measurement state. However, if the post-measurement state is not needed for a particular problem, then the POVM formalism provides a convenient way to study general measurement statistics on a quantum system.

1.1.3 Information Quantities

Von Neumann entropy is a measure of mixedness of a quantum density operator, and is defined as

$$S(\hat{\rho}) = -\mathrm{tr}(\hat{\rho}\log\hat{\rho}) = H(\{\lambda_n\}), \tag{1.8}$$

where $\{\lambda_n\}$ are the eigenvalues of $\hat{\rho}$ and $H(\cdot)$ is the Shannon entropy from classical information theory. Von Neumann entropy is an important quantity in quantum information theory, as it appears in fundamental theorems dealing with compression and coding over noisy quantum channels. One basic property of von Neumann entropy is subadditivity. For two quantum systems A and B, the entropy of the joint system satisfies

$$S(\hat{\rho}_{AB}) \leq S(\hat{\rho}_A) + S(\hat{\rho}_B), \tag{1.9}$$

where $\hat{\rho}_A$ and $\hat{\rho}_B$ are the reduced density operators of $\hat{\rho}_{AB}$. Equality holds in this expression if and only if $\hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B$. This property is analogous to the corresponding property of Shannon entropy for classical joint random variables.

Suppose that Alice sends classical messages to Bob by encoding her messages on the states of a quantum mechanical system. To send message m, Alice prepares the signal state $\hat{\rho}_m$ with a priori probability p_m. Bob attempts to obtain information about the message m by performing a suitable POVM on the signal ensemble $\{p_m, \hat{\rho}_m\}$ that gives a low probability of error. In [16] Holevo derived an upper bound on the amount of information that Bob can obtain from his received output $\hat{M}$ about Alice's input M. Accessible information I_a is the maximum mutual information $I(M;\hat{M})$ over all possible decoding POVMs. Holevo showed that the mutual information between input and output satisfies

$$I(M;\hat{M}) \leq \chi(p_m, \hat{\rho}_m) \equiv S\left(\sum_m p_m \hat{\rho}_m\right) - \sum_m p_m S(\hat{\rho}_m). \tag{1.10}$$

In particular, accessible information is upper bounded by the Holevo information: $I_a \leq \chi$. In general, the Holevo bound cannot be attained for any decoding POVM, and in fact can be a weak bound [17]. In Section 1.1.5, we discuss a result which says that the Holevo bound can be approached through the use of block codes and entangled measurements.

1.1.4 Entanglement

Entanglement is a feature of quantum mechanics that has received much attention recently as a physical resource which can be used to enhance the performance of communication and computational protocols. Entanglement is a correlation between multiple physical systems that is stronger than can be predicted by any local theory of physics. It is this "spooky"

correlation that led to the Einstein-Podolsky-Rosen (EPR) paradox [18], which argues that quantum mechanics is incomplete as a description of physical reality.

Quantum systems $A_1, \ldots, A_n$ are said to be entangled if their joint density operator $\hat{\rho}_{A_1,\ldots,A_n}$ cannot be written as a convex sum of product states:

$$\sum_i p_i \hat{\rho}_i^{A_1} \otimes \cdots \otimes \hat{\rho}_i^{A_n}. \tag{1.11}$$

A state that is not entangled is called separable. A pure state is entangled if it cannot be written as a tensor product of pure states. An example of a maximally entangled pure state of two qubits, as measured by the von Neumann entropy of the reduced density operator, is the singlet state

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}). \tag{1.12}$$

It can be verified that the singlet state cannot be expressed a product $|\psi\rangle_A \otimes |\phi\rangle_B$.

Teleportation and Superdense Coding Here, we consider two basic communication protocols, teleportation [9] and superdense coding [10], that demonstrate how entanglement can be used as a resource for communication. In the teleportation protocol, shared entanglement acts as a quantum channel for the transmission of quantum information. Suppose two parties, Alice and Bob, are spatially separated and that each possesses one qubit of a singlet state (1.12). Alice wishes to send a message qubit $|\phi\rangle_M = \alpha|0\rangle_M + \beta|1\rangle_M$ to Bob. The idea of the teleportation protocol is for Alice to make a measurement on the combined system of her two qubits, send the two-bit result of the measurement to Bob over a classical channel, then for Bob to perform a unitary operation on his qubit to recover the message qubit. A detailed procedure for the teleportation protocol is as follows.

1. The initial state of the three qubits is $|\phi\rangle_M \otimes |\psi^-\rangle_{AB}$. Alice performs a measurement in the Bell basis $\{|\psi^\pm\rangle_{MA} = (|01\rangle_{MA} \pm |10\rangle_{MA})/\sqrt{2}, |\phi^\pm\rangle_{MA} = (|00\rangle_{MA} \pm |11\rangle_{MA})/\sqrt{2}\}$ that yields two bits of classical information which will be needed at the receiver to reproduce the message qubit.

2. Alice sends the two-bit outcome of her Bell-state measurement over a classical channel to Bob.

3. Depending on which message Bob receives, he performs one of four unitary transfor-

mation, known as the Pauli operators, on his qubit. The Pauli operators are defined as

$$\hat{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{1.13}$$

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.14}$$

When Bob receives one of the messages $\{\psi^-, \psi^+, \phi^-, \phi^+\}$, he applies the corresponding transformation from the set $\{\hat{I}, \hat{Z}, \hat{X}, \hat{Y}\}$. Then, up to some overall phase, Bob will possess the message qubit.

Alice's two qubits collapse into one of the four Bell states immediately after performing her measurement. Thus, at the completion of this procedure, Bob will possess the only copy of the message qubit in accordance with the no-cloning theorem [19].

The superdense coding protocol is in some sense the dual procedure of teleportation. Instead of transmitting quantum information, a shared singlet state enables the transmission of classical information. Suppose Alice and Bob each possess one qubit of a singlet state. Alice encodes a two-bit classical message by performing one of four unitary operators $\{\hat{I}, \hat{X}, \hat{Y}, \hat{Z}\}$ on her share of the singlet state, and sends this qubit to Bob over a quantum channel. Depending on which message Alice has encoded, the joint state of qubits A and B will be one of the four Bell states. Because the Bell states are orthogonal, Bob can perform a measurement on the combined systems A and B to determine which measurement Alice performed. In this way, Alice can transmit two classical bits to Bob over a qubit channel.

1.1.5 Quantum Channels

A closed quantum system in initial state $|\psi(t_0)\rangle$ evolves in time according to the Schrodinger equation

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = \hat{H}|\psi(t)\rangle, \tag{1.15}$$

where $\hat{H}$ is the Hamiltonian of the system. Solving this differential equation shows that the state of a closed system at time $t \geq t_0$ is given by

$$|\psi(t)\rangle = \hat{U}(t, t_0)|\psi(t_0)\rangle, \tag{1.16}$$

where $\hat{U}(t,t_0) = \exp(-i\hat{H}(t-t_0)/\hbar)$ is the unitary time-evolution operator. In terms of density operators, unitary time evolution is expressed as $\hat{\rho}(t) = \hat{U}(t,t_0)\hat{\rho}(t_0)\hat{U}^\dagger(t,t_0)$. In practice, the quantum systems we are interested in are not isolated, but rather are coupled to their environment. The interaction of a system with its environment leads to non-unitary time evolution. The general formalism described below has been developed for studying non-unitary system dynamics.

Consider a quantum channel that takes as input a density operator from Hilbert space $\mathcal{H}_{\text{in}}$ and outputs a density operator in Hilbert space $\mathcal{H}_{\text{out}}$, i.e., a quantum channel is a map $\mathcal{E} : B(\mathcal{H}_{\text{in}}) \rightarrow B(\mathcal{H}_{\text{out}})$, where $B(\mathcal{H})$ denotes the set of bounded operators in $\mathcal{H}$. A quantum channel satisfies the following axioms:

1. $\mathcal{E}$ is trace preserving: $\text{tr}(\mathcal{E}(\hat{\rho})) = 1$, where $\hat{\rho}$ is any density operator in $\mathcal{H}_{\text{in}}$.
2. $\mathcal{E}$ is a convex-linear map on the set of density operators: $\mathcal{E}(\sum_i p_i\hat{\rho}_i) = \sum_i p_i\mathcal{E}(\hat{\rho}_i)$, for any probability distribution $\{p_i\}$.
3. $\mathcal{E}$ is a completely positive map. This means that if I_Q is the identity operator on some auxiliary system Q, then

$$\hat{A} \geq 0 \Rightarrow (\mathcal{E} \otimes I_Q)(\hat{A}) \geq 0, \tag{1.17}$$

   for $\hat{A}$ an operator on the composite space $\mathcal{H}_{\text{in}} \otimes Q$.

These axioms are physically reasonable properties for a quantum channel to satisfy. A quantum channel is often referred to as a TPCP (trace-preserving, completely-positive) map. It can be shown that every TPCP map $\mathcal{E}$ has an operator-sum representation

$$\mathcal{E}(\hat{\rho}) = \sum_k \hat{A}_k\hat{\rho}\hat{A}_k^\dagger, \tag{1.18}$$

where $\{\hat{A}_k\}$, called the Kraus operators, satisfy the trace-preserving condition $\sum_k \hat{A}_k^\dagger\hat{A}_k = \hat{I}$.

The classical capacity C is the number of bits that can be reliably transmitted over a quantum channel $\mathcal{E}$. The HSW (Holevo-Schumacher-Westmoreland) theorem [20],[4],[5] says that the capacity of a quantum channel $\mathcal{E}$, normalized to the number of channel uses, is given by

$$C = \lim_{M\rightarrow\infty} \frac{C_M}{M} = \sup_M \frac{C_M}{M}, \tag{1.19}$$

where the M-shot capacity is defined in terms of the product channel $\mathcal{E}^{\otimes M}$ as

$$C_M = \max_{p_i, \hat{\rho}_i} \chi(p_i, \mathcal{E}^{\otimes M}(\hat{\rho}_i)). \tag{1.20}$$

In classical information theory, Shannon's coding theorem says that capacity is calculated by maximizing the mutual information between the input and output of a communication channel. The HSW theorem extends Shannon's result and shows that in the quantum case, classical capacity is obtained by maximizing the Holevo information of a quantum channel. The normalization in (1.19) is necessary because it is unknown whether Holevo information is super-additive, i.e., whether entangling over inputs can increase capacity.

1.2 Quantum Optics

Some basic knowledge of quantum optics is assumed in this thesis, and for background we refer to [21] and [22]. In this section, we provide a brief review of quantum optics, emphasizing the concepts that will be useful in this thesis.

1.2.1 Field Quantization

A single mode of monochromatic light is expressed classically as

$$E(t) = \frac{1}{2}(Ee^{-i\omega t} + E^* e^{i\omega t}) = X_1 \cos\omega t + X_2 \sin\omega t, \tag{1.21}$$

where the quadrature components X_1 and X_2 are the real and imaginary parts of the complex field amplitude $E = X_1 + iX_2$. In the quantum theory of radiation, a single-mode field is described by the annihilation operator $\hat{a}$ and its Hermitian conjugate creation operator $\hat{a}^\dagger$, which obey the Boson commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$. The eigenkets $\{|n\rangle: n = 0, 1, 2, \ldots\}$ of the number operator $\hat{n} = \hat{a}^\dagger\hat{a}$ form a complete orthonormal basis, and the nth-excited state can be expressed in terms of the vacuum state as $|n\rangle = (\hat{a}^\dagger)^n|0\rangle/\sqrt{n!}$.

Coherent states of light are those generated by lasers operating well above threshold and represent the closest equivalent to classical light with a definite complex amplitude. Mathematically, coherent states $\{|\alpha\rangle : \alpha \in \mathbb{C}\}$ can be defined as the eigenkets of the annihilation operator $\hat{a}$, or alternatively, as displacements of the vacuum state in phase

space: $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$, where $\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$. From the number-state expansion,

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{1.22}$$

we see that coherent states give Poisson statistics in photon counting measurements. In phase space, a coherent state is circularly symmetric and the fluctuations of the quadrature operators, $\hat{a}_1 = (\hat{a}+\hat{a}^\dagger)/2$ and $\hat{a}_2 = (\hat{a}-\hat{a}^\dagger)/2i$, have the minimum product in the uncertainty relation: $\langle\Delta\hat{a}_1^2\rangle\langle\Delta\hat{a}_2^2\rangle = 1/16$.

1.2.2 Gaussian States

For any density operator $\hat{\rho}$, define the mean $\mathrm{tr}(\hat{\rho}\hat{a})$ and variance matrix

$$V = \begin{pmatrix} V_1 & V_{12} \\ V_{12} & V_2 \end{pmatrix} = \begin{pmatrix} \langle\Delta\hat{a}_1^2\rangle & \langle\Delta\hat{a}_1\Delta\hat{a}_2 + \Delta\hat{a}_2\Delta\hat{a}_1\rangle/2 \\ \langle\Delta\hat{a}_1\Delta\hat{a}_2 + \Delta\hat{a}_2\Delta\hat{a}_1\rangle/2 & \langle\Delta\hat{a}_2^2\rangle \end{pmatrix}. \tag{1.23}$$

A Gaussian state has a symmetrically-ordered characteristic function of the form $\chi_W^\rho(\zeta) \equiv \mathrm{tr}(\hat{\rho}\hat{D}(\zeta)) = \exp(\phi(\zeta,\zeta^*))$, where $\phi(\zeta,\zeta^*)$ is quadratic in (ζ,ζ^*). Equivalently, Gaussian states can be defined as those density operators of the form $\hat{\rho} \propto \exp(f(\hat{a},\hat{a}^\dagger))$, where $f(\hat{a},\hat{a}^\dagger)$ is quadratic in $(\hat{a},\hat{a}^\dagger)$. Like classical Gaussian probability distributions, quantum Gaussian states are characterized by their mean and variance matrix. In what follows, assume zero-mean Gaussian states.

Squeezed states are an important class of Gaussian states. A zero-mean squeezed state is obtained by squeezing the vacuum state, $|0,z\rangle \equiv \hat{S}(z)|0\rangle$, where the unitary squeeze operator $\hat{S}(z)$ is defined as

$$\hat{S}(z) = \exp\left[\frac{r}{2}(e^{-i\theta}\hat{a}^2 - e^{i\theta}\hat{a}^{\dagger 2})\right], \tag{1.24}$$

and $z = re^{i\theta}$. It is convenient to introduce the parametrization $\mu = \cosh r$ and $\nu = e^{i\theta}\sinh r$. The degree of attenuation and amplification is determined by $r = |z|$ and θ determines the phase of the squeezing. The squeezed state $|0,z\rangle$ has variance matrix

$$V = \frac{1}{4}\begin{pmatrix} |\mu-\nu|^2 & -2\,\mathrm{Im}(\mu\nu) \\ -2\,\mathrm{Im}(\mu\nu) & |\mu+\nu|^2. \end{pmatrix}. \tag{1.25}$$

An important property of squeezed states with phase $\theta = 0$ is the fact that they have the minimum uncertainty product $\langle \Delta \hat{a}_1^2 \rangle \langle \Delta \hat{a}_2^2 \rangle = 1/16$, with

$$\langle \Delta \hat{a}_1^2 \rangle = \frac{1}{4} e^{-2r} \tag{1.26}$$

$$\langle \Delta \hat{a}_2^2 \rangle = \frac{1}{4} e^{2r}. \tag{1.27}$$

Fluctuations in one quadrature can be reduced below the standard quantum limit at the expense of increasing fluctuations in the other quadrature.

Another important example of a Gaussian state is the thermal state

$$\hat{\rho}_T(N) = \frac{1}{N+1} \left(\frac{N}{N+1} \right)^{\hat{a}^\dagger \hat{a}}, \tag{1.28}$$

with mean photon number N. We can show that every Gaussian state is unitarily equivalent to a thermal state [23]. Applying the squeeze operator to a Gaussian state $\hat{\rho} \propto \exp(f(\hat{a}, \hat{a}^\dagger))$ with variance matrix V gives the state

$$\hat{S}(z) \hat{\rho} \hat{S}^\dagger(z) \propto \hat{S}(z) \exp(f(\hat{a}, \hat{a}^\dagger)) \hat{S}^\dagger(z) = \exp(f(\mu \hat{a} + \nu \hat{a}^\dagger, \mu \hat{a}^\dagger + \nu^* \hat{a})). \tag{1.29}$$

By choosing the squeeze parameters as

$$|\nu| = \left(\frac{V_1 + V_2}{4|V|^{1/2}} - \frac{1}{2} \right)^{1/2} \tag{1.30}$$

$$\arg(\nu) = \tan^{-1} \left(\frac{2V_{12}}{V_1 - V_2} \right) \tag{1.31}$$

$$\mu = (|\nu|^2 + 1)^{1/2}, \tag{1.32}$$

the quadratic exponent $f(\mu \hat{a} + \nu \hat{a}^\dagger, \mu \hat{a}^\dagger + \nu^* \hat{a})$ is diagonalized to the form (1.28) with mean photon number $\bar{n}_T = 2|V|^{1/2} - 1/2$. Thus, the Gaussian state $\hat{\rho}$ is unitarily equivalent to the thermal state $\hat{\rho}_T(\bar{n}_T)$. Since unitary transformations leave eigenvalues invariant, this result shows that the entropy of a single-mode Gaussian state is given by

$$S(\hat{\rho}) = g(\bar{n}_T) = g \left(2|V|^{1/2} - \frac{1}{2} \right). \tag{1.33}$$

We also note that the variance matrix of $\hat{\rho}$ can be expressed in terms of the squeeze param-

eters as

$$V = |V|^{1/2} \begin{pmatrix} |\mu + \nu|^2 & 2\,\mathrm{Im}(\mu\nu) \\ 2\,\mathrm{Im}(\mu\nu) & |\mu - \nu|^2 \end{pmatrix}. \tag{1.34}$$

1.3 Thesis Outline

Entanglement is a feature of quantum mechanics that has recently been recognized as an important resource for quantum communications. In Chapter 2, we study a quantum communication architecture [24], which is being developed for high-fidelity, long-distance transmission and storage of polarization-entangled photons by a team of researchers from the Massachusetts Institute of Technology (MIT) and Northwestern University (NU). An initial experimental demonstration of teleportation using singlet states was performed by Bouwmeester et al. [11],[12], but only one of the Bell states was measured, the demonstration was a table-top experiment, and it did not include a quantum memory. The MIT/NU proposal for a singlet-based quantum communication system remedies all of these limitations. An initial assessment of the system's throughput versus fidelity performance was presented in [24]. We will extend and generalize previous work on this architecture by considering the effects of system errors that limit its performance in qubit teleportation. We also study an extension of the MIT/NU architecture that allows for the distribution of three-party entangled Greenberger-Horne-Zeilinger states and consider its performance in the quantum secret sharing protocol.

In Chapter 3, we study the problem of superdense coding over quantum multiple access channels (MACs) in finite-dimensional spaces. Superdense coding is a communication protocol which uses entanglement to enhance classical information transmission over quantum channels. We will extend previous analyses of the superdense coding protocol by deriving the capacity region of the superdense coding MAC. The transmitters in the superdense coding MAC are restricted to unitary encodings. We also consider the capacity of the entanglement-assisted MAC in which transmitters encode input messages with general local operations.

We are interested in understanding the limitations the laws of quantum mechanics place on our ability to communicate over optical channels. We extend recent work [7],[25] on the capacity of quantum optical communication channels. In Chapter 4, we derive the classical capacity C for Gaussian Bosonic channels that represent the quantum version of

classical colored Gaussian-noise channels. In classical information theory, whitening filters are used to reduce colored Gaussian-noise channels to standard additive white Gaussian noise channels. In the quantum problem, non-commuting operators require us to modify this classical whitening approach. Putting this together with a conjecture for the capacity of the thermal-noise channel gives us the desired capacity result. We will also solve minimum output entropy problems that are related to the thermal-noise capacity conjecture.

In Chapter 5, we generalize these capacity results to an optical MAC in which multiple transmitters send classical information over a quantum optical channel to a common receiver. The capacity for quantum optical MACs with coherent-state inputs is derived. We generalize a single-user Gaussian code to achieve higher rates on the optical MAC, and we derive bounds for the ultimate capacity region.

Summary and directions for future work are discussed in Chapter 6.

Chapter 2

MIT/NU Communication Architecture

A team of researchers from the Massachusetts Institute of Technology (MIT) and Northwestern University (NU) has proposed a quantum communication architecture [24] that permits long-distance high-fidelity teleportation using the Bennett et al. singlet-state protocol [9] described in Section 1.1.4. This architecture uses a novel ultrabright source of polarization-entangled photon pairs [26] and trapped-atom quantum memories [27] in which all four Bell states can be measured. By means of quantum-state frequency conversion and time-division multiplexed polarization restoration, it is able to employ standard telecommunication fiber for long-distance transmission of the polarization-entangled photons.

In this chapter we carry out a performance analysis of the MIT/NU communication architecture. In previous work [28], a Werner state error model was derived for the joint state of the quantum memories, and the use of error mitigation techniques was considered for improving the performance of the communication architecture. The present work [29],[30],[31] extends on this analysis in two primary ways. First, an error model for the long-distance teleportation system is developed to assess the effects of errors in the entanglement source as well as fiber loss and imperfect transmission of the entangled photon pairs. This analysis follows the approach taken in [28] to derive single-photon error models from the joint state of the loaded memory cavities. We present the throughput and fidelity assessments that follow from these error models. Second, an error model is derived for an extension of the MIT/NU architecture that allows for the production and storage of GHZ states. The GHZ-

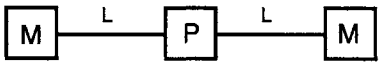


Figure 2-1: Schematic of long-distance quantum communication system. P = ultrabright narrowband source of polarization-entangled photon pairs; $L = L$ km of standard telecommunications fiber; M = trapped-atom quantum memory.

state system error model is used to study the performance of the quantum secret sharing protocol [32] as well as the use of quantum error correction and entanglement purification protocols to improve the performance of the GHZ system.

2.1 Long-Distance Qubit Teleportation System

A schematic diagram of the MIT/NU communication architecture is shown in Fig. 2-1. The P block is an ultrabright narrowband source of polarization-entangled photon pairs. It combines the signal and idler output beams from two type-II phase matched optical parametric amplifiers. Each M block is a quantum memory consisting of a single ultracold ^{87}Rb atom confined by a CO_2-laser trap in a single-ended optical cavity. A 795 nm photon in an arbitrary polarization can be absorbed by the atom, transferring the quantum information to long-lived storage levels in the atom. Upon successful loading of the singlet state, $|\psi^-\rangle_{TR} = (|01\rangle_{TR} - |10\rangle_{TR})/\sqrt{2}$, the memories can serve as transmitter and receiver stations for qubit teleportation.

2.1.1 Ultrabright Source of Polarization-Entangled Photons

Polarization-entangled photons are transmitted from the source over L km of standard optical fiber to be loaded into trapped-atom quantum memories. The Fig. 2-1 system requires a source of entangled photons at the 795 nm line of its rubidium atom quantum memories. Furthermore, only those pairs within a narrow frequency band ($\sim$10 MHz) of the 795 nm line will successfully load the memory, so the Fig. 2-1 system places a premium on source brightness. Spontaneous parametric downconversion is the standard approach for generating polarization-entangled photons. It is so broadband ($\sim 10^{13}$ Hz), however, that its pair-generation rate in the narrow bandwidth needed for coupling into the rubidium atom is extremely low: $\sim$15 pairs/sec in a 30 MHz bandwidth. The P block in Fig. 2-1 represents an ultrabright narrowband source [26], which is capable of producing 1.5×10^6 pairs/sec

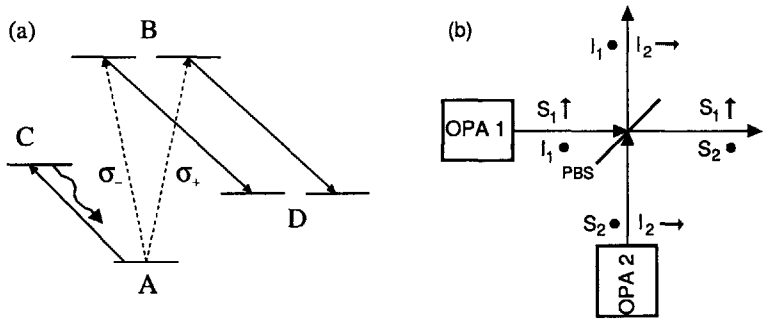


Figure 2-2: Essential components of the singlet-state quantum communication system from Fig. 1. (a) Simplified energy-level diagram of the trapped rubidium atom quantum memory. The A-to-B transition occurs when a photon is absorbed. The B-to-D transition is coherently driven to enable storage in the long-lived D levels. The A-to-C cycling transition is used for nondestructive verification of a loading event. (b) Ultrabright narrowband source of polarization-entangled photon pairs. The polarizations $\hat{x}$ and $\hat{y}$ are denoted by arrows and bullets, respectively; PBS=polarizing beam splitter.

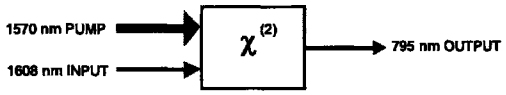


Figure 2-3: Schematic diagram of quantum-state frequency conversion: a strong pump beam at 1570 nm converts a qubit photon received at 1608 nm (in the low-loss fiber transmission window) to a qubit photon at the 795 nm wavelength of the ^{87}Rb quantum memory via a single-pass interaction in a second-order ($\chi^{(2)}$) nonlinear crystal.

in a 30 MHz bandwidth by combining the signal and idler output beams from two doubly resonant type-II phase matched optical parametric amplifiers (OPAs), as sketched in Fig. 2-2(b).

Quasi-phase-matching in periodically-poled nonlinear materials makes it possible to choose the OPA wavelength, for our polarization-entanglement source, to suit the application at hand. In particular, by using periodically-poled potassium titanyl phosphate (PPKTP), a quasi-phase-matched type-II nonlinear material, we can produce $\sim 10^6$ pairs/sec at the 795 nm wavelength of the rubidium memory for direct memory-loading (i.e., local-storage) applications. For long-distance transmission to remotely located memories, we can use a different PPKTP crystal and pump wavelength to generate 10^6 pairs/sec in the 1.55 μm wavelength low-loss fiber transmission window. After fiber propagation we shift the entanglement to the 795 nm wavelength needed for the rubidium-atom memory via quantum-state frequency conversion [33],[34], shown in Fig. 2-3.

Reference [26] reported a lumped-element analysis for a continuous-wave, doubly-resonant.

dual-OPA system with amplitude-matched, anti-phased, nondepleting pumps and no excess losses. That analysis was used in [24] to demonstrate that such an arrangement produces the high-brightness, narrowband singlet states needed for qubit teleportation. More recently, a broadband traveling-wave treatment of a type-II phase matched, doubly-resonant, dual OPA system has been shown to reproduce the lumped element results when the former is limited to a few cavity linewidths about a double resonance [35]. Because the trapped-atom quantum memory in the MIT/NU architecture will only respond to that portion of the dual-OPA's output that lies within a narrow spectral region about the 795 nm atomic line, we shall employ the lumped-element source theory in what follows. Because we are interested in the effects that pump amplitude, phase, and frequency errors will have on the throughput and fidelity of the teleportation system, we need to generalize somewhat the dual-OPA source model from [24],[26].

Following [36], we have that the equations of motion governing the intracavity annihilation operators, $\{\,\hat{a}_{k_j}(t) : k = S, I,\ j = 1, 2\,\}$, of the signal and idler modes for the jth OPA are,

$$\left(\frac{\mathrm{d}}{\mathrm{d}t} + \Gamma\right)\hat{a}_{S_j}(t) = (-1)^{j-1} G_j \Gamma \hat{a}^{\dagger}_{I_j}(t) + \sqrt{2\gamma}\hat{A}^{\mathrm{IN}}_{S_j}(t) + \sqrt{2(\Gamma-\gamma)}\hat{A}^{v}_{S_j}(t), \qquad (2.1)$$

$$\left(\frac{\mathrm{d}}{\mathrm{d}t} + \Gamma\right)\hat{a}_{I_j}(t) = (-1)^{j-1} G_j \Gamma \hat{a}^{\dagger}_{S_j}(t) + \sqrt{2\gamma}\hat{A}^{\mathrm{IN}}_{I_j}(t) + \sqrt{2(\Gamma-\gamma)}\hat{A}^{v}_{I_j}(t), \qquad (2.2)$$

where $\{\hat{A}^{\mathrm{IN}}_{k_j}(t)e^{-i\omega_k t}, \hat{A}^{v}_{k_j}(t)e^{-i\omega_k t}\}$ are the positive-frequency, photon-units input field and OPA-cavity loss operators for the signal and idler fields, all of which are taken to be in their vacuum states. In these equations we have assumed that the two OPAs are phase matched at a double resonance which occurs for signal frequency ω_S and idler frequency ω_I. We have also assumed that all four OPA modes see identical cavities, with common linewidth Γ and output-coupling rate $\gamma \leq \Gamma$. To capture the effects of pump amplitude, phase, and frequency errors, we allow each OPA to have a different, complex-valued normalized pump strength G_j, where $|G_j|^2$ equals the pump power divided by the threshold power for oscillation, and we allow the center frequencies ω_S and ω_I to be detuned from frequency degeneracy by $\Delta\omega$ and $-\Delta\omega$, respectively. The $(-1)^{j-1}$ factors in these equations imply that $\arg(G_1) = \arg(G_2)$ corresponds to the anti-phased pumping required for generating the polarization-entangled singlet state which is needed in the Bennett et al. teleportation protocol.

The OPAs' output fields are given by

$$\hat{A}_{S_j}^{\mathrm{OPA}}(t) = \sqrt{2\gamma}\hat{a}_{S_j}(t) - \hat{A}_{S_j}^{\mathrm{IN}}(t), \tag{2.3}$$

$$\hat{A}_{I_j}^{\mathrm{OPA}}(t) = \sqrt{2\gamma}\hat{a}_{I_j}(t) - \hat{A}_{I_j}^{\mathrm{IN}}(t), \tag{2.4}$$

and it is the statistics of these output fields that characterize the quality of the dual-OPA as an entanglement source for use in teleportation.

Equations (2.1)–(2.4) are easily solved, in the frequency domain, yielding a pair of two-mode Bogoliubov transformations relating the input and output field operators for each OPA. These in turn imply that the OPAs produce signal and idler beams in zero-mean, entangled, Gaussian states which are completely characterized by the following normally-ordered and phase-sensitive correlation functions,

$$\begin{aligned} K_{\mathrm{OPA}_j}^{(n)}(\tau) &= \langle \hat{A}_{k_j}^{\mathrm{OPA}\dagger}(t+\tau)\hat{A}_{k_j}^{\mathrm{OPA}}(t)\rangle \\ &= \frac{|G_j|\gamma}{2}\left[\frac{e^{-(1-|G_j|)\Gamma|\tau|}}{1-|G_j|} - \frac{e^{-(1+|G_j|)\Gamma|\tau|}}{1+|G_j|}\right], \end{aligned} \tag{2.5}$$

and

$$\begin{aligned} K_{\mathrm{OPA}_j}^{(p)}(\tau) &= \langle \hat{A}_{S_j}^{\mathrm{OPA}}(t+\tau)\hat{A}_{I_j}^{\mathrm{OPA}}(t)\rangle \\ &= \frac{G_j\gamma}{2}\left[\frac{e^{-(1-|G_j|)\Gamma|\tau|}}{1-|G_j|} + \frac{e^{-(1+|G_j|)\Gamma|\tau|}}{1+|G_j|}\right]. \end{aligned} \tag{2.6}$$

2.1.2 Quantum-State Transmission over Fiber

Successful singlet transmission requires that polarization not be degraded by the propagation process. Yet, propagation through standard telecommunication fiber produces random, slowly-varying (~msec time scale) polarization variations, so a means for polarization restoration is required. The approach taken for polarization restoration in the MIT/NU architecture, shown schematically in Fig. 2-4, relies on time-division multiplexing (TDM). Time slices from the signal beams from the two OPAs are sent down one fiber in the same linear polarization but in nonoverlapping time slots, accompanied by a strong out-of-band pulse. By tracking and restoring the linear polarization of the strong pulse, we can restore the linear polarization of the signal-beam time slices at the far end of the fiber. After this

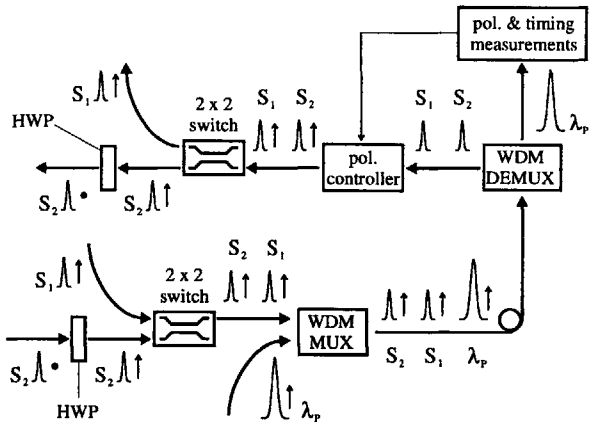


Figure 2-4: Transmission of time-division multiplexed signal beams from OPAs 1 and 2 through an optical fiber. λ_p = pilot pulse, WDM MUX = wavelength-division multiplexer, WDM DEMUX = wavelength-division demultiplexer, HWP = half-wave plate.

linear-polarization restoration, we then reassemble a time-epoch of the full vector signal beam by delaying the first time slot and combining it on a polarizing beam splitter with the second time slot after the latter has had its linear polarization rotated by 90°. A similar procedure is performed to reassemble idler time-slices after they have propagated down the other fiber. This approach, which is inspired by the Bergman et al. two-pulse fiber-squeezing experiment [37], common-modes out the vast majority of the phase fluctuations and the polarization birefringence incurred in the fiber, permitting standard telecommunication fiber to be used in lieu of the lossier and much more expensive polarization-maintaining fiber.

2.1.3 Trapped-Atom Quantum Memory

Each M block in Fig. 2-1 is a quantum memory in which a single ultra-cold ^{87}Rb atom (~6 MHz linewidth) is confined by a far-off-resonance laser trap in an ultra-high-vacuum chamber with cryogenic walls within a high-finesse (~15 MHz linewidth) single-ended optical cavity. This memory can absorb a 795 nm photon, in an arbitrary polarization state, transferring the qubit from the photon to the degenerate B levels of Fig. 2-2(a) and thence to long-lived storage levels, by coherently driving the B-to-D transitions. (We are using abstract symbols here for the hyperfine levels of rubidium; see [27] for the actual atomic levels involved as well as a complete description of the memory and its operation.) With a liquid helium cryostat, so that the background pressure is less than 10^{-14} Torr, the expected lifetime of the trapped rubidium atom will be more than an hour. Fluctuations in

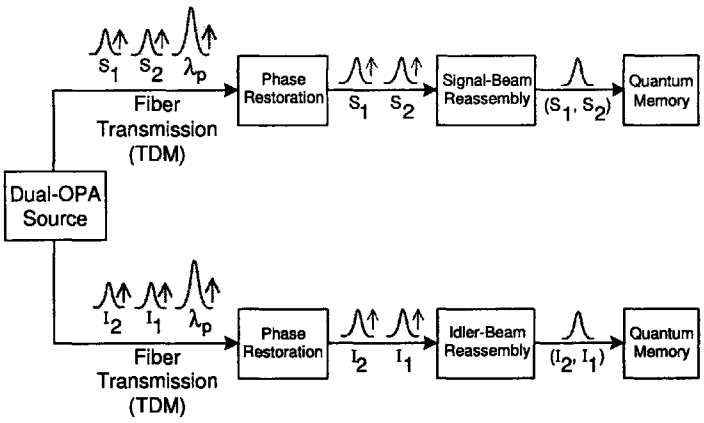


Figure 2-5: Signal and idler beams from the dual-OPA polarization entanglement source are transmitted down optical fibers for loading into remote quantum memories.

the residual magnetic field, however, will probably limit the atom's decoherence time to a few minutes.

By using optically off-resonant Raman (OOR) transitions, the Bell states of two atoms in a single vacuum-chamber trap can be converted to superposition states of one of the atoms. All four Bell measurements can then be made, sequentially, by detecting the presence (or absence) of fluorescence as an appropriate sequence of OOR laser pulses is applied to the latter atom [27]. The Bell-measurement results in one memory can be sent to a distant memory, where at most two additional OOR pulses are needed to complete the Bennett et al. state transformation. The qubit stored in a trapped rubidium atom can be converted back into a photon by reversing the Raman excitation process that occurs during memory loading.

2.2 Fiber Transmission Error Model

In this section we develop a model for propagation loss and imperfect polarization restoration in TDM transmission of polarization-entangled photons through a pair of optical fibers, see Fig. 2-5.

2.2.1 Propagation Loss

As suggested by Fig. 2-1, we will take the dual-OPA source to be equidistant from the two quantum memories, and thus we may assume that the signal and idler beams encounter the same transmission factor, $\eta_L < 1$, in propagation to their respective quantum memories. It is then easy to show that the effects of this propagation loss can be lumped into the source model itself, i.e., we can consider the fibers to be lossless by changing the dual-OPA's normally-ordered and phase-sensitive correlation functions to be,

$$K^{(n)}_{\mathrm{OPA}_j}(\tau) = \frac{\eta_L |G_j| \gamma}{2} \left[\frac{e^{-(1-|G_j|)\Gamma|\tau|}}{1-|G_j|} - \frac{e^{-(1+|G_j|)\Gamma|\tau|}}{1+|G_j|} \right], \tag{2.7}$$

$$K^{(p)}_{\mathrm{OPA}_j}(\tau) = \frac{\eta_L G_j \gamma}{2} \left[\frac{e^{-(1-|G_j|)\Gamma|\tau|}}{1-|G_j|} + \frac{e^{-(1+|G_j|)\Gamma|\tau|}}{1+|G_j|} \right], \tag{2.8}$$

in lieu of the expressions from Eqs. (2.5) and (2.6).

2.2.2 Imperfect Polarization Restoration

The narrowband nature of the dual-OPA's signal and idler beams, which obviates any concern about dispersive pulse spreading, combined with the short duration ($\sim$1 μsec [24]) of the TDM sequence compared to the msec time scale over which fiber fluctuations occur, imply that we need only concern ourselves with simple, time-independent polarization transformations for $\{\lambda_p, S_1, S_2\}$ on one fiber and $\{\lambda_p, I_1, I_2\}$ on the other fiber. In particular, suppose we use the x polarization as the input to the fibers and

$$\hat{\boldsymbol{A}}_{k_j}(t) \equiv \left(\hat{A}^{\mathrm{OPA}}_{k_j}(t) \quad \hat{A}^{f}_{k_j}(t) \right)^T \tag{2.9}$$

to denote the vector field operators for the signal and idler time slots at the input to the fiber, where the y-polarized operators are all in vacuum states. The corresponding vector field operators at the output of the fiber will then be given by

$$\hat{\boldsymbol{A}}'_{k_j}(t) = \mathcal{F}_k(\theta_k, \varphi_k, \varphi'_k, \psi_k) \hat{\boldsymbol{A}}_{k_j}(t), \tag{2.10}$$

where we have suppressed the L/c-sec propagation delay and $\mathcal{F}_k$ is the unitary polarization-transformation matrix for fiber k ($k = S, I$),

$$\mathcal{F}_k(\theta_k, \varphi_k, \varphi'_k, \psi_k) = \begin{pmatrix} e^{i\psi_k}\cos(\theta_k/2) & -e^{i(\psi_k+\varphi_k)}\sin(\theta_k/2) \\ e^{i(\psi_k+\varphi'_k)}\sin(\theta_k/2) & e^{i(\psi_k+\varphi_k+\varphi'_k)}\cos(\theta_k/2) \end{pmatrix}, \tag{2.11}$$

for $\theta_k \in [0, \pi]$ and $\varphi_k, \varphi'_k, \psi_k \in [0, 2\pi)$.

The pilot pulses in each fiber, which undergo these same polarization transformations, are sufficiently strong that they behave classically, thus affording high signal-to-noise ratio measurements of $\{\, \theta_k, \varphi'_k : k = S, I \,\}$ but no information about $\{\, \psi_k, \varphi_k : k = S, I \,\}$. Polarization restoration is then performed on $\{S_1, S_2\}$ and $\{I_1, I_2\}$ using the putative inverse transformations,

$$\mathcal{F}_k^{-1}(\tilde{\theta}_k, \tilde{\varphi}'_k) = \begin{pmatrix} \cos(\tilde{\theta}_k/2) & e^{-i\tilde{\varphi}'_k}\sin(\tilde{\theta}_k/2) \\ -\sin(\tilde{\theta}_k/2) & e^{-i(\tilde{\varphi}'_k)}\cos(\tilde{\theta}_k/2) \end{pmatrix}, \tag{2.12}$$

where $\{\, \tilde{\theta}_k, \tilde{\varphi}'_k : k = S, I \,\}$ are estimated values derived from the pilot-pulse measurements. If these measurements are perfect, then the vector signal and idler fields *after* polarization restoration will be

$$\begin{aligned} \hat{\boldsymbol{A}}_{k_j}^{\mathrm{OUT}}(t) &= \mathcal{F}_k^{-1}(\theta_k, \varphi'_k)\mathcal{F}_k(\theta_k, \varphi_k, \varphi'_k, \psi_k)\hat{\boldsymbol{A}}_{k_j}(t) \\ &= e^{i\psi_k}\left(\hat{A}_{k_j}^{\mathrm{OPA}}(t) \quad e^{i\varphi_k}\hat{A}_{k_j}^{f}(t)\right)^T, \end{aligned} \tag{2.13}$$

hence accomplishing perfect restoration of the signal and idler time slots, up to an unimportant pair of absolute phase factors.

Errors may occur in estimating the parameters of the fiber transformations, in realizing inverse transformations based on these estimates, in extracting the x-polarized components from the polarization-restored fiber outputs, and in reassembling the polarization-entangled signal and idler fields. Collectively, these errors can all be subsumed into the following input/output transformations for lossless, imperfect polarization-restored fiber propagation:

$$\hat{\boldsymbol{A}}_S^{\mathrm{OUT}}(t) = \begin{pmatrix} \hat{A}_{S_x}^{\mathrm{OUT}}(t) \\ \hat{A}_{S_y}^{\mathrm{OUT}}(t) \end{pmatrix} = \begin{pmatrix} \cos(\theta_S/2)\hat{A}_{S_1}^{\mathrm{OUT}}(t) - e^{i\varphi_S}\sin(\theta_S/2)\hat{A}_{S_1}^{f}(t) \\ \cos(\theta_S/2)\hat{A}_{S_2}^{\mathrm{OUT}}(t) - e^{i\varphi_S}\sin(\theta_S/2)\hat{A}_{S_2}^{f}(t) \end{pmatrix}, \tag{2.14}$$

and

$$\hat{\boldsymbol{A}}_I^{\mathrm{OUT}}(t) = \begin{pmatrix} \hat{A}_{I_x}^{\mathrm{OUT}}(t) \\ \hat{A}_{I_y}^{\mathrm{OUT}}(t) \end{pmatrix} = \begin{pmatrix} \cos(\theta_I/2)\hat{A}_{I_2}^{\mathrm{OUT}}(t) - e^{i\varphi_I}\sin(\theta_I/2)\hat{A}_{I_2}^{f}(t) \\ \cos(\theta_I/2)\hat{A}_{I_1}^{\mathrm{OUT}}(t) - e^{i\varphi_I}\sin(\theta_I/2)\hat{A}_{I_1}^{f}(t) \end{pmatrix}, \tag{2.15}$$

where we have omitted some absolute phase factors that do not affect the cavity-loading analysis, given below, and $\{\theta_k, \varphi_k : k = S, I\}$ are now polarization-restoration *error* phases, rather than the fiber *propagation* phases appearing in Eq. (2.11). Because these input/output relations are linear and phase insensitive, it follows, by combining the propagation loss and imperfect polarization restoration models, that vector output fields—which serve as inputs to the quantum memories—are in zero-mean, joint Gaussian states which are completely characterized by the following correlation functions:

$$\begin{pmatrix} K_{S_x}^{(n)}(\tau) \\ K_{S_y}^{(n)}(\tau) \end{pmatrix} = \begin{pmatrix} \langle \hat{A}_{S_x}^{\mathrm{OUT}\dagger}(t+\tau)\hat{A}_{S_x}^{\mathrm{OUT}}(t)\rangle \\ \langle \hat{A}_{S_y}^{\mathrm{OUT}\dagger}(t+\tau)\hat{A}_{S_y}^{\mathrm{OUT}}(t)\rangle \end{pmatrix} = \cos^2(\theta_S/2) \begin{pmatrix} K_{\mathrm{OPA}_1}^{(n)}(\tau) \\ K_{\mathrm{OPA}_2}^{(n)}(\tau) \end{pmatrix}, \tag{2.16}$$

$$\begin{pmatrix} K_{I_x}^{(n)}(\tau) \\ K_{I_y}^{(n)}(\tau) \end{pmatrix} = \begin{pmatrix} \langle \hat{A}_{I_x}^{\mathrm{OUT}\dagger}(t+\tau)\hat{A}_{I_x}^{\mathrm{OUT}}(t)\rangle \\ \langle \hat{A}_{I_y}^{\mathrm{OUT}\dagger}(t+\tau)\hat{A}_{I_y}^{\mathrm{OUT}}(t)\rangle \end{pmatrix} = \cos^2(\theta_I/2) \begin{pmatrix} K_{\mathrm{OPA}_2}^{(n)}(\tau) \\ K_{\mathrm{OPA}_1}^{(n)}(\tau) \end{pmatrix}, \tag{2.17}$$

and

$$\begin{pmatrix} K_{S_xI_y}^{(p)}(\tau) \\ K_{S_yI_x}^{(p)}(\tau) \end{pmatrix} = \begin{pmatrix} \langle \hat{A}_{S_x}^{\mathrm{OUT}}(t+\tau)\hat{A}_{I_y}^{\mathrm{OUT}}(t)\rangle \\ \langle \hat{A}_{S_y}^{\mathrm{OUT}}(t+\tau)\hat{A}_{I_x}^{\mathrm{OUT}}(t)\rangle \end{pmatrix} = \cos(\theta_S/2)\cos(\theta_I/2) \begin{pmatrix} K_{\mathrm{OPA}_1}^{(p)}(\tau) \\ K_{\mathrm{OPA}_2}^{(p)}(\tau) \end{pmatrix}. \tag{2.18}$$

As expected, because OPA_1 produces entangled x-polarized signal and y-polarized idler fields and OPA_2 independently produces entangled y-polarized signal and x-polarized idler fields, these correlation functions show that the joint state (density operator) of the vector signal and idler fields arriving at the quantum memories factors according to,

$$\hat{\rho}_{\mathbf{SI}} = \hat{\rho}_{S_xI_y} \otimes \hat{\rho}_{S_yI_x}. \tag{2.19}$$

2.3 Cavity-Loading Analysis

To derive the joint state of the quantum memories, we neglect the atom-field coupling and treat the simpler cold-cavity system, following the procedure introduced in [24]. Moreover we will postpone accounting for dual-OPA pump detuning by assuming that $\omega_S = \omega_I = \omega_P/2 = \omega_c = \omega_a$, where ω_P is the pump frequency and ω_c is the memory cavity resonance, and ω_a is the ^{87}Rb atomic line.

Let $\hat{a}_S(T_c)$ and $\hat{a}_I(T_c)$ be the internal annihilation operators of the quantum memory cavities after a T_c-second long loading interval. Assume the memory cavities have input-coupling rate γ_c and cavity linewidth $\Gamma_c \geq \gamma_c$. Then the vector (x and y) internal annihilation operators are related to the input fields by

$$\hat{\boldsymbol{a}}_k(T_c) = \hat{\boldsymbol{a}}_k(0)e^{-\Gamma_c T_c} + \int_0^{T_c} e^{-\Gamma_c(T_c-t)}\left[\sqrt{2\gamma_c}\hat{\boldsymbol{A}}_k^{\mathrm{OUT}}(t) + \sqrt{2(\Gamma_c-\gamma_c)}\hat{\boldsymbol{A}}_k^{c}(t)\right]\mathrm{d}t, \quad (2.20)$$

for $k = S, I$, where the initial internal annihilation operators and memory-cavity loss operators $\{\hat{\boldsymbol{a}}_k(0), \hat{\boldsymbol{A}}_k^c(t)\}$ are in vacuum states. Once again we have a linear, phase-insensitive transformation, which implies that $\{\hat{\boldsymbol{a}}_S(T_c), \hat{\boldsymbol{a}}_I(T_c)\}$ are in a zero-mean joint Gaussian state. The nonzero second moments of these memory-cavity modes can be found from Eqs. (2.16)–(2.18) and (2.20) via standard techniques. When $\Gamma_c T_c \gg 1$, as we shall assume, the results of such moment calculations are:

$$\langle \hat{a}_{S_l}^\dagger(T_c)\hat{a}_{S_l}(T_c)\rangle = \bar{n}_{S_l}, \quad \text{for } l = x, y \quad (2.21)$$

$$\langle \hat{a}_{I_l}^\dagger(T_c)\hat{a}_{I_l}(T_c)\rangle = \bar{n}_{I_l}, \quad \text{for } l = x, y \quad (2.22)$$

$$\langle \hat{a}_{S_x}(T_c)\hat{a}_{I_y}(T_c)\rangle = \tilde{n}_{S_xI_y} \quad (2.23)$$

$$\langle \hat{a}_{S_y}(T_c)\hat{a}_{I_x}(T_c)\rangle = -\tilde{n}_{S_yI_x} \quad (2.24)$$

with

$$\bar{n}_{S_x} = \cos^2(\theta_S/2)(|I_{1-}| - |I_{1+}|) \tag{2.25}$$

$$\bar{n}_{S_y} = \cos^2(\theta_S/2)(|I_{2-}| - |I_{2+}|) \tag{2.26}$$

$$\bar{n}_{I_x} = \cos^2(\theta_I/2)(|I_{2-}| - |I_{2+}|) \tag{2.27}$$

$$\bar{n}_{I_y} = \cos^2(\theta_I/2)(|I_{1-}| - |I_{1+}|) \tag{2.28}$$

$$\tilde{n}_{S_xI_y} = \cos(\theta_S/2)\cos(\theta_I/2)(I_{1-} + I_{1+}) \tag{2.29}$$

$$\tilde{n}_{S_yI_x} = \cos(\theta_S/2)\cos(\theta_I/2)(I_{2-} + I_{2+}) \tag{2.30}$$

$$\tag{2.31}$$

and

$$I_{j\pm} = \frac{\eta_L \gamma \gamma_c}{\Gamma \Gamma_c} \frac{G_j}{(1 \pm |G_j|)(1 \pm |G_j| + \Gamma_c/\Gamma)}, \tag{2.32}$$

for $j = 1, 2$. In terms of these moments, we have that the joint anti-normally ordered characteristic function for the $\{\hat{\boldsymbol{a}}_S(T_c), \hat{\boldsymbol{a}}_I(T_c)\}$ modes is the Gaussian form,

$$\chi_A(\zeta_{S_x}, \zeta_{S_y}, \zeta_{I_x}, \zeta_{I_y}) = \exp[- (1 + \bar{n}_{S_x})|\zeta_{S_x}|^2 - (1 + \bar{n}_{S_y})|\zeta_{S_y}|^2 \tag{2.33}$$

$$- (1 + \bar{n}_{I_x})|\zeta_{I_x}|^2 - (1 + \bar{n}_{I_y})|\zeta_{I_y}|^2 \tag{2.34}$$

$$+ 2\,\mathrm{Re}(\tilde{n}^*_{S_xI_y}\zeta_{S_x}\zeta_{I_y}) - 2\,\mathrm{Re}(\tilde{n}^*_{S_yI_x}\zeta_{S_y}\zeta_{I_x})]. \tag{2.35}$$

2.4 Single-Photon Error Model

The cold-cavity loading analysis includes the possibility that more than one photon may be loaded into either memory, yet this is clearly not possible for the actual trapped-atom memory. As a result, the initial assessment of throughput versus fidelity, reported in [24], treated the loading of a singlet state into the two memories as a *success*, and any other event in which one or more photons were loaded into each memory as an *error*. Load intervals in which one or both of the memories fail to absorb a photon were considered to be *erasures*, because they could be detected, nondestructively, by means of the A-to-C cycling transition shown in Fig. 2-2(a), see [24] and [27] for details. Erasures reduce teleportation throughput in the Fig. 2-1 architecture, but not its fidelity. A better approximation to performance

analysis for the Fig. 2-1 architecture was presented in [30] (see also [28]), where multiple-atom arrays at each memory location were used to convert multi-photon error events from [24] into erasures. Both the analysis in [24] and that in [30] assume amplitude matched, anti-phased pumping in the dual-OPA source, viz., $G_1 = G_2 = G$, and perfect polarization restoration, i.e., $\theta_S = \theta_I = 0$. Our task, in this section, is to generalize the single-photon error model of [30] to include amplitude and phase errors in the dual-OPA's pumps as well as imperfect polarization restoration. The results we obtain here will then enable us to evaluate the impact these effects have on the teleportation throughput and fidelity.

Define the computational basis of the quantum memories to be $|0\rangle_k = |10\rangle_{k_x k_y}$ and $|1\rangle_k = |01\rangle_{k_x k_y}$ for $k = S, I$, where $|10\rangle_{S_x S_y}$ denotes the memory state generated by absorption of an x-polarized signal photon, etc. To compute the entries of the conditional density matrix for the memories, given that each has absorbed a single photon, we first write the density operators $\hat{\rho}_{S_x I_y}$ and $\hat{\rho}_{S_y I_x}$ in terms of their respective anti-normally ordered characteristic functions via the operator-valued inverse Fourier transform relations,

$$\hat{\rho}_{S_x I_y} = \iint \chi_A^{\rho_{S_x I_y}}(\zeta_S, \zeta_I)\, e^{-\zeta_S \hat{a}^\dagger_{S_x} - \zeta_I \hat{a}^\dagger_{I_y}} e^{\zeta_S^* \hat{a}_{S_x} + \zeta_I^* \hat{a}_{I_y}} \frac{d\zeta_S\, d\zeta_I}{\pi^2}, \tag{2.36}$$

and

$$\hat{\rho}_{S_y I_x} = \iint \chi_A^{\rho_{S_y I_x}}(\zeta_S, \zeta_I)\, e^{-\zeta_S \hat{a}^\dagger_{S_y} - \zeta_I \hat{a}^\dagger_{I_x}} e^{\zeta_S^* \hat{a}_{S_y} + \zeta_I^* \hat{a}_{I_x}} \frac{d\zeta_S\, d\zeta_I}{\pi^2}, \tag{2.37}$$

where, for the sake of brevity, we have suppressed the T_c time argument of the cavity-mode annihilation operators. The characteristic function associated with $\hat{\rho}_{S_x I_y}$ can be expressed as

$$\chi_A^{\rho_{S_x I_y}}(\boldsymbol{\zeta}) = \frac{\pi^2 p_{S_x I_y}(\boldsymbol{\zeta})}{D_1}, \tag{2.38}$$

where $D_1 = (1 + \bar{n}_{S_x})(1 + \bar{n}_{I_y}) - |\tilde{n}_{S_x I_y}|^2$ and $p_{S_x I_y}(\boldsymbol{\zeta})$ is a classical probability density for the zero-mean, complex-valued Gaussian random vector $\boldsymbol{\zeta} = (\zeta_S \quad \zeta_I)^T$ with second-moment matrices

$$\langle \boldsymbol{\zeta}\boldsymbol{\zeta}^\dagger \rangle_{p_{S_x I_y}} = \frac{1}{D_1} \begin{pmatrix} 1 + \bar{n}_{I_y} & 0 \\ 0 & 1 + \bar{n}_{S_x} \end{pmatrix}, \tag{2.39}$$

$$\langle \boldsymbol{\zeta}\boldsymbol{\zeta}^T \rangle_{p_{S_x I_y}} = \frac{1}{D_1} \begin{pmatrix} 0 & \tilde{n}_{S_x I_y} \\ \tilde{n}_{S_x I_y} & 0 \end{pmatrix}. \tag{2.40}$$

Similarly, we have

$$\chi_A^{\rho_{S_yI_x}}(\boldsymbol{\zeta}) = \frac{\pi^2 p_{S_yI_x}(\boldsymbol{\zeta})}{D_2}, \tag{2.41}$$

where $D_2 = (1+\bar{n}_{S_y})(1+\bar{n}_{I_x}) - |\tilde{n}_{S_yI_x}|^2$ and $p_{S_yI_x}(\boldsymbol{\zeta})$ is a classical probability density for the zero-mean, complex-valued Gaussian random vector $\boldsymbol{\zeta} = (\zeta_S \quad \zeta_I)^T$ with second-moment matrices

$$\langle \boldsymbol{\zeta}\boldsymbol{\zeta}^\dagger \rangle_{p_{S_yI_x}} = \frac{1}{D_2}\begin{pmatrix} 1+\bar{n}_{I_x} & 0 \\ 0 & 1+\bar{n}_{S_y} \end{pmatrix}, \tag{2.42}$$

$$\langle \boldsymbol{\zeta}\boldsymbol{\zeta}^T \rangle_{p_{S_yI_x}} = \frac{1}{D_2}\begin{pmatrix} 0 & -\tilde{n}_{S_yI_x} \\ -\bar{n}_{S_yI_x} & 0 \end{pmatrix}. \tag{2.43}$$

The conditional single-photon density matrix will be computed in the standard basis, $\{|00\rangle_{SI}, |01\rangle_{SI}, |10\rangle_{SI}, |11\rangle_{SI}\}$. Define the quantities

$$N_{S_x} = \bar{n}_{S_x}(1+\bar{n}_{I_y}) - |\tilde{n}_{S_xI_y}|^2 \tag{2.44}$$

$$N_{S_y} = \bar{n}_{S_y}(1+\bar{n}_{I_x}) - |\tilde{n}_{S_yI_x}|^2 \tag{2.45}$$

$$N_{I_x} = \bar{n}_{I_x}(1+\bar{n}_{S_y}) - |\tilde{n}_{S_yI_x}|^2 \tag{2.46}$$

$$N_{I_y} = \bar{n}_{I_y}(1+\bar{n}_{S_x}) - |\tilde{n}_{S_xI_y}|^2. \tag{2.47}$$

Then the ten density matrix entries we need to compute are:

$$_{SI}\langle 00|\hat{\rho}_{\mathbf{SI}}|00\rangle_{SI} = \langle 10|\hat{\rho}_{S_xI_y}|10\rangle\langle 01|\hat{\rho}_{S_yI_x}|01\rangle \tag{2.48}$$

$$= \frac{\langle 1-|\zeta_S|^2\rangle_{p_{SxIy}}\langle 1-|\zeta_I|^2\rangle_{p_{SyIx}}}{D_1 D_2} \tag{2.49}$$

$$= \frac{N_{S_x}N_{I_x}}{D_1^2 D_2^2}, \tag{2.50}$$

$$_{SI}\langle 00|\hat{\rho}_{\mathbf{SI}}|01\rangle_{SI} = \langle 10|\hat{\rho}_{S_xI_y}|11\rangle\langle 01|\hat{\rho}_{S_yI_x}|00\rangle \tag{2.51}$$

$$= \frac{\langle (1-|\zeta_S|^2)\zeta_I^*\rangle_{p_{SxIy}}\langle -\zeta_I\rangle_{p_{SyIx}}}{D_1 D_2} \tag{2.52}$$

$$= 0, \tag{2.53}$$

$$
\begin{aligned}
{}_{SI}\langle 00|\hat{\rho}_{\mathbf{SI}}|10\rangle_{SI} &= \langle 10|\hat{\rho}_{S_xI_y}|00\rangle\langle 01|\hat{\rho}_{S_yI_x}|11\rangle && (2.54)\\
&= \frac{\langle -\zeta_S\rangle_{p_{S_xI_y}}\langle \zeta_S^*(1-|\zeta_I|^2)\rangle_{p_{S_yI_x}}}{D_1D_2} && (2.55)\\
&= 0, && (2.56)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 00|\hat{\rho}_{\mathbf{SI}}|11\rangle_{SI} &= \langle 10|\hat{\rho}_{S_xI_y}|01\rangle\langle 01|\hat{\rho}_{S_yI_x}|10\rangle && (2.57)\\
&= \frac{\langle -\zeta_S\zeta_I^*\rangle_{p_{S_xI_y}}\langle -\zeta_S^*\zeta_I\rangle_{p_{S_yI_x}}}{D_1D_2} && (2.58)\\
&= 0, && (2.59)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 01|\hat{\rho}_{\mathbf{SI}}|01\rangle_{SI} &= \langle 11|\hat{\rho}_{S_xI_y}|11\rangle\langle 00|\hat{\rho}_{S_yI_x}|00\rangle && (2.60)\\
&= \frac{\langle (1-|\zeta_S|^2)(1-|\zeta_I|^2)\rangle_{p_{S_xI_y}}}{D_1D_2} && (2.61)\\
&= \frac{N_{S_x}N_{I_y}+|\tilde{n}_{S_xI_y}|^2}{D_1^3D_2} && (2.62)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 01|\hat{\rho}_{\mathbf{SI}}|10\rangle_{SI} &= \langle 11|\hat{\rho}_{S_xI_y}|00\rangle\langle 00|\hat{\rho}_{S_yI_x}|11\rangle && (2.63)\\
&= \frac{\langle \zeta_S\zeta_I\rangle_{p_{S_xI_y}}\langle \zeta_S^*\zeta_I^*\rangle_{p_{S_yI_x}}}{D_1D_2} && (2.64)\\
&= -\frac{\tilde{n}_{S_xI_y}\tilde{n}^*_{S_yI_x}}{D_1^2D_2^2}, && (2.65)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 01|\hat{\rho}_{\mathbf{SI}}|11\rangle_{SI} &= \langle 11|\hat{\rho}_{S_xI_y}|01\rangle\langle 00|\hat{\rho}_{S_yI_x}|10\rangle && (2.66)\\
&= \frac{\langle -\zeta_S(1-|\zeta_I|^2)\rangle_{p_{S_xI_y}}\langle \zeta_S^*\rangle_{p_{S_yI_x}}}{D_1D_2} && (2.67)\\
&= 0, && (2.68)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 10|\hat{\rho}_{\mathbf{SI}}|10\rangle_{SI} &= \langle 00|\hat{\rho}_{S_xI_y}|00\rangle\langle 11|\hat{\rho}_{S_yI_x}|11\rangle && (2.69)\\
&= \frac{\langle (1-|\zeta_S|^2)(1-|\zeta_I|^2)\rangle_{p_{S_yI_x}}}{D_1D_2} && (2.70)\\
&= \frac{N_{I_x}N_{S_y}+|\tilde{n}_{S_yI_x}|^2}{D_1D_2^3}, && (2.71)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 10|\hat{\rho}_{\mathbf{SI}}|11\rangle_{SI} &= \langle 00|\hat{\rho}_{S_xI_y}|01\rangle\langle 11|\hat{\rho}_{S_yI_x}|10\rangle && (2.72)\\
&= \frac{\langle \zeta_I^*\rangle_{p_{SxIy}}\langle -(1-|\zeta_S|^2)\zeta_I\rangle_{p_{SyIx}}}{D_1D_2} && (2.73)\\
&= 0, && (2.74)
\end{aligned}
$$

$$
\begin{aligned}
{}_{SI}\langle 11|\hat{\rho}_{\mathbf{SI}}|11\rangle_{SI} &= \langle 01|\hat{\rho}_{S_xI_y}|01\rangle\langle 10|\hat{\rho}_{S_yI_x}|10\rangle && (2.75)\\
&= \frac{\langle 1-|\zeta_I|^2\rangle_{p_{SxIy}}\langle 1-|\zeta_S|^2\rangle_{p_{SyIx}}}{D_1D_2} && (2.76)\\
&= \frac{N_{S_y}N_{I_y}}{D_1^2D_2^2}. && (2.77)
\end{aligned}
$$

The right-hand side of the first equality in all these density matrix evaluations has broken the calculational basis into its constituent $\{S_x, I_y\}$ and $\{S_y, I_x\}$ photon-state components. Equations (2.62) and (2.71) were obtained via the Gaussian moment-factoring theorem

The conditional single-photon density matrix resulting from the Gaussian state (2.33) in the standard basis, for fixed values of the dual-OPA pump and fiber polarization-restoration parameters, is the trace-normalized version of the preceding matrix elements:

$$
\hat{\rho} = \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & b_1 & c & 0 \\ 0 & c^* & b_2 & 0 \\ 0 & 0 & 0 & a_2 \end{pmatrix}, \qquad (2.78)
$$

where

$$
\begin{aligned}
a_1 &= N_{S_x}N_{I_x}D_1D_2/D' && (2.79)\\
a_2 &= N_{S_y}N_{I_y}D_1D_2/D' && (2.80)\\
b_1 &= (N_{S_x}N_{I_y} + |\tilde{n}_{S_xI_y}|^2)D_2^2/D' && (2.81)\\
b_2 &= (N_{S_y}N_{I_x} + |\tilde{n}_{S_yI_x}|^2)D_1^2/D' && (2.82)\\
c &= -\tilde{n}_{S_xI_y}\tilde{n}^*_{S_yI_x}D_1D_2/D', && (2.83)
\end{aligned}
$$

and

$$
D' = (N_{S_x}N_{I_x} + N_{S_y}N_{I_y})D_1D_2 + (N_{S_x}N_{I_y} + |\tilde{n}_{S_xI_y}|^2)D_2^2 + (N_{S_y}N_{I_x} + |\tilde{n}_{S_yI_x}|^2)D_1^2. \quad (2.84)
$$

The single-photon density matrix $\hat{\rho}$ depends on the normalized pump magnitudes, $\{|G_1|, |G_2|\}$, the differential-phase error between the pumps, $\Delta\psi = \arg(G_1) - \arg(G_2)$, and the polarization-restoration error angles $\{\theta_S, \theta_I\}$. Note that, in general, $\hat{\rho}$ is not a Bell-diagonal state. We can apply a change of basis to show that the density matrix in the Bell basis, $\{|\psi^-\rangle_{SI}, |\psi^+\rangle_{SI}, |\phi^-\rangle_{SI}, |\phi^+\rangle_{SI}\}$, is 2×2 block diagonal, viz.,

$$\hat{\rho} = \begin{pmatrix} \rho_{11} & \mathbf{0} \\ \mathbf{0} & \rho_{22} \end{pmatrix}, \tag{2.85}$$

where

$$\rho_{11} = \frac{1}{2} \begin{pmatrix} b_1 + b_2 - 2\mathrm{Re}(c) & b_1 - b_2 + 2i\,\mathrm{Im}(c) \\ b_1 - b_2 - 2i\,\mathrm{Im}(c) & b_1 + b_2 + 2\mathrm{Re}(c) \end{pmatrix} \tag{2.86}$$

and

$$\rho_{22} = \frac{1}{2} \begin{pmatrix} a_1 + a_2 & a_1 - a_2 \\ a_1 - a_2 & a_1 + a_2 \end{pmatrix}. \tag{2.87}$$

It will be useful to know the eigendecomposition of the single-photon density matrix $\hat{\rho}$ for the performance analysis in the next section. The eigenvalues of $\hat{\rho}$ are $\{a_1, a_2, \lambda^+, \lambda^-\}$ with corresponding unit-length eigenkets $\{|00\rangle_{SI}, |11\rangle_{SI}, |\lambda^+\rangle_{SI}, |\lambda^-\rangle_{SI}\}$, where

$$\lambda^{\pm} = \frac{b_1 + b_2}{2} \pm \frac{1}{2}\sqrt{(b_1 - b_2)^2 + 4|c|^2} \tag{2.88}$$

$$|\lambda^+\rangle_{SI} = u_1|01\rangle_{SI} + u_2|10\rangle_{SI} \tag{2.89}$$

$$|\lambda^-\rangle_{SI} = v_1|01\rangle_{SI} + v_2|10\rangle_{SI}. \tag{2.90}$$

The eigenket coefficients u_1, u_2, v_1, v_2 are found by converting the following unnormalized eigenkets to unit length:

$$|\lambda^{\pm}\rangle_{SI} = \frac{b_1 - b_2 \pm \sqrt{(b_1 - b_2)^2 + 4|c|^2}}{2c^*}|01\rangle_{SI} + |10\rangle_{SI}. \tag{2.91}$$

2.5 Performance Analysis

In this section, we will examine the effects of system errors on the average fidelity of the Fig. 2-1 teleportation architecture. We shall also give some consideration to the achievable throughput that can be obtained when each quantum memory is capable of loading a

succession of singlet states by repeated application of the memory-loading protocol, cf. [24],[30].

2.5.1 Teleportation Fidelity

Suppose the qubit that we wish to teleport is $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. If the received state that results from sending this state via the Fig. 2-1 teleportation system is $\hat{\rho}'$, then the *conditional* fidelity, given that $|\phi\rangle$ was teleported, is $\langle\phi|\hat{\rho}'|\phi\rangle$. The *average* fidelity is obtained by taking $|\phi\rangle$ to be uniformly distributed over the Bloch sphere and averaging the conditional fidelity using this input distribution. We will calculate the average fidelity in the single-photon error model developed in Section 2.4. To do so, we first calculate four pure-state average fidelities: the average fidelities realized when the quantum memories are in one of the eigenkets of the single-photon-error density matrix, $\{|00\rangle_{SI}, |11\rangle_{SI}, |\lambda^+\rangle_{SI}, |\lambda^-\rangle_{SI}\}$. Multiplying each eigenket's fidelity by its associated eigenvalue and summing the results then yields the average fidelity for the single-photon-error density matrix, $\hat{\rho}$.

Teleportation when the quantum memories are in either the $|00\rangle_{SI}$ or $|11\rangle_{SI}$ states is equivalent to a channel that sends an input qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ into the mixed state $|\beta|^2|0\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|$, and hence a conditional fidelity of $2|\alpha|^2|\beta|^2$. Averaging this expression over the Bloch sphere yields fidelity $F = 1/3$.

Teleportation when the quantum memories are in the $|\lambda^+\rangle_{SI} = u_1|01\rangle_{SI} + u_2|10\rangle_{SI}$ state takes the input qubit to the mixed state

$$|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| - 2\alpha\beta^*\mathrm{Re}(u_1^*u_2)|0\rangle\langle 1| - 2\alpha^*\beta\mathrm{Re}(u_1^*u_2)|1\rangle\langle 0|, \tag{2.92}$$

and hence a conditional fidelity $1 - 2|\alpha|^2|\beta|^2[1 + 2\mathrm{Re}(u_1^*u_2)]$. Averaging this expression over the Bloch sphere yields fidelity $F = 2[1 - \mathrm{Re}(u_1^*u_2)]/3$. Similarly, teleportation when the quantum memories are in the $|\lambda^-\rangle_{SI} = v_1|01\rangle_{SI} + v_2|10\rangle_{SI}$ state has average fidelity $F = 2[1 - \mathrm{Re}(v_1^*v_2)]/3$.

Performing the required eigenvalue weighting and summation on the preceding pure-state fidelities we obtain the average fidelity for the single-photon-error model's density matrix:

$$F = \frac{2 - a_1 - a_2 - 2[\lambda^+\mathrm{Re}(u_1^*u_2) + \lambda^-\mathrm{Re}(v_1^*v_2)]}{3}. \tag{2.93}$$

This is the average teleportation fidelity, with the input qubit $\alpha|0\rangle + \beta|1\rangle$ uniformly dis-

tributed over the Bloch sphere, for fixed values of the error parameters.

To develop insight into how teleportation performance is degraded by errors in the dual-OPA's pump amplitudes and phases as well as by imperfect polarization restoration, we shall examine these effects one at a time.

2.5.2 Imperfect Polarization Restoration

Here we assume the dual-OPA's pumps have equal magnitudes, $|G_1| = |G_2| = |G|$, and are anti-phased, $\Delta\psi = 0$. In this case, the single-photon-error density matrix is diagonal in the Bell basis, and given by

$$\hat{\rho} = \mathrm{diag}\Big(P_s \quad (1-P_s)/3 \quad (1-P_s)/3 \quad (1-P_s)/3\Big), \tag{2.94}$$

where

$$P_s = \frac{N_S N_I + 2\tilde{n}^2}{4N_S N_I + 2\tilde{n}^2} \tag{2.95}$$

$$N_S = \bar{n}_S(1+\bar{n}_I) - \tilde{n}^2 \tag{2.96}$$

$$N_I = \bar{n}_I(1+\bar{n}_S) - \tilde{n}^2 \tag{2.97}$$

$$\bar{n}_S = \cos^2(\theta_S/2)(I_- - I_+) \tag{2.98}$$

$$\bar{n}_I = \cos^2(\theta_I/2)(I_- - I_+) \tag{2.99}$$

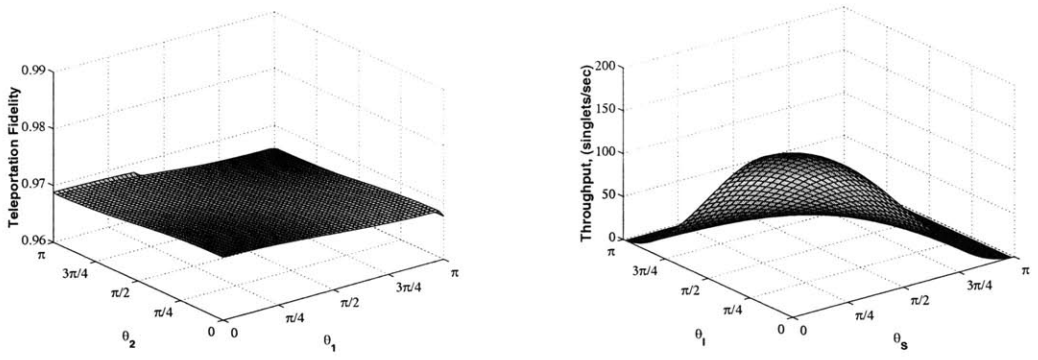
$$\tilde{n} = \cos(\theta_S/2)\cos(\theta_I/2)(I_- + I_+) \tag{2.100}$$

$$I_\pm = \frac{\eta_L \gamma\gamma_c}{\Gamma\Gamma_c} \frac{|G|}{(1\pm|G|)(1\pm|G|+\Gamma_c/\Gamma)}. \tag{2.101}$$

The density matrix is a Werner state, so teleporting a qubit with this state is equivalent to transmitting the qubit over a depolarizing channel with fidelity P_s. The average teleportation fidelity with this error model is $F = (2P_s + 1)/3$.

In Fig. 2-6(a), the teleportation fidelity is plotted versus polarization-restoration error parameters $\theta_S, \theta_I \in [0, \pi]$. The calculations assume a source-to-memory path length $L = 25$ km and the operating conditions listed in the caption. The fidelity of the teleportation system is insensitive to θ_S and θ_I. The maximum fidelity, $F = 0.978$, occurs at $\theta_S = \theta_I = 0$ and the minimum fidelity, $F = 0.974$, occurs at $\theta_S = \theta_I = \pi$.

Although teleportation fidelity is insensitive to imperfect polarization restoration, these



(a) (b)

Figure 2-6: (a) Teleportation fidelity versus polarization-restoration error parameters $\theta_S, \theta_I \in [0, \pi]$. We assume OPAs operate at 1% of oscillation threshold, 0.2 dB/km fiber loss, 5 dB excess loss in each source-to-memory link, $\Gamma_c/\Gamma = 0.5$ memory-cavity linewidth to source-cavity linewidth ratio, and source-to-memory path length $L = 25$ km. (b) Throughput of singlet states versus polarization-restoration error parameters $\theta_S, \theta_I \in [0, \pi]$.

errors imply a significant loss of singlet-state throughput. Figure 2-6(b) plots the throughput of singlet states versus $\theta_S, \theta_I \in [0, \pi]$, assuming that the teleportation system has an array of trapped-atom memories at the end of each fiber and that these memories can be loaded by running the protocol from [24] at a 500 kHz rate. We see from Fig. 2-6(b) that maximum throughput at $L = 25$ km is approximately 184 singlets/sec and this occurs when the polarization restoration is perfect, $\theta_S = \theta_I = 0$. The throughput decreases to zero when θ_S or θ_I approaches π rad. In essence, $\cos(\theta_S/2)$ and $\cos(\theta_I/2)$ act as asymmetric loss factors on the signal and idler fiber channels, respectively. For small values of θ_S and θ_I it is possible to obtain a simple analytic expression for the success probability, P_s, by Taylor-series expansion:

$$P_s \approx \frac{N_0^2 + 2\tilde{n}_0^2}{4N_0^2 + 2\tilde{n}_0^2} - \frac{3N_0\tilde{n}_0^2(\tilde{n}_0^2 - \bar{n}_0^2)}{8(2N_0^2 + \tilde{n}_0^2)^2}(\theta_S^2 + \theta_I^2), \tag{2.102}$$

where $N_0 = \bar{n}_0(1 + \bar{n}_0) - \tilde{n}_0^2$ with $\bar{n}_0 = I_- - I_+$ and $\tilde{n}_0 = I_- + I_+$. Thus, to lowest order, the throughput of the Fig. 2-1 teleportation system degrades with the sum of the squares of the polarization-restoration errors θ_S and θ_I.

2.5.3 OPA Pump-Phase Error

Here we assume $|G_1| = |G_2| = |G|$ and $\theta_S = \theta_I = 0$, and consider the impact of a pump-phase error, i.e., of having $\Delta\psi = \arg(G_1) - \arg(G_2) \neq 0$. In this case the single-photon-error

density matrix in the Bell basis is

$$\hat{\rho} = \begin{pmatrix} b - \mathrm{Re}(c) & i\,\mathrm{Im}(c) & 0 & 0 \\ -i\,\mathrm{Im}(c) & b + \mathrm{Re}(c) & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix}, \tag{2.103}$$

where

$$a = \frac{N^2}{4N^2 + 2\tilde{n}^2} \tag{2.104}$$

$$b = \frac{N^2 + \tilde{n}^2}{4N^2 + 2\tilde{n}^2} \tag{2.105}$$

$$c = -\frac{e^{i\Delta\psi}\tilde{n}^2}{4A^2 + 2\tilde{n}^2} \tag{2.106}$$

$$A = \bar{n}(1 + \bar{n}) - \tilde{n}^2 \tag{2.107}$$

$$\bar{n} = I_- - I_+ \tag{2.108}$$

$$\tilde{n} = I_- + I_+ \tag{2.109}$$

$$I_\pm = \frac{\eta_L \gamma\gamma_c}{\Gamma\Gamma_c} \frac{|G|}{(1 \pm |G|)(1 \pm |G| + \Gamma_c/\Gamma)}. \tag{2.110}$$

The density matrix is not Bell-diagonal. Its eigenkets are $\{|00\rangle_{SI}, |11\rangle_{SI}, |\lambda^+\rangle_{SI}, |\lambda^-\rangle_{SI}\}$, where

$$|\lambda^\pm\rangle_{SI} = \frac{1}{\sqrt{2}}(|01\rangle_{SI} \mp e^{-i\Delta\psi}|10\rangle_{SI}). \tag{2.111}$$

From Eq. (2.88), the eigenvalues associated with $|\lambda^\pm\rangle_{SI}$ are $\lambda^\pm = b \pm |c|$. From the expressions above, we see that $\lambda^- = a$. Substituting the values $u_1 = v_1 = 1/\sqrt{2}$, $-u_2 = v_2 = e^{-i\Delta\psi}/\sqrt{2}$, and $\lambda^+ = 1 - 3a$ into the Eq. (2.93) gives the average teleportation fidelity

$$F = \frac{2 - 2a + (1 - 4a)\cos\Delta\psi}{3}. \tag{2.112}$$

We have plotted the fidelity from Eq. (2.112) versus the pump-phase error $\Delta\psi$ in Fig. 2-7, assuming $L = 25$ km source-to-memory path length and the same operating conditions as in Fig. 2-6. Figure 2-7 shows that pump-phase errors have serious consequences: at $\Delta\psi = \pi$, the dominant eigenket $|\lambda^+\rangle_{SI}$ equals the triplet state, making the average fidelity close to the triplet-state value, $F = 1/3$. For small values of the pump-phase error we can use a

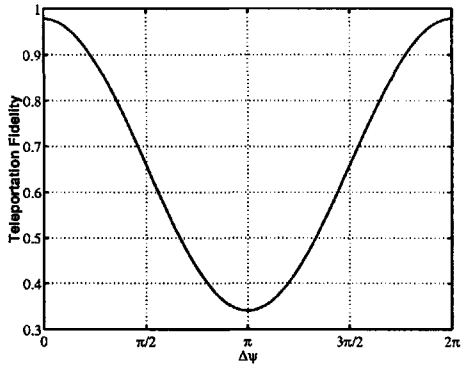


Figure 2-7: Teleportation fidelity with dual-OPA pump-phase error $\Delta\psi \in [0, 2\pi)$. At $\Delta\psi = \pi$, the dominant eigenket of $\hat{\rho}$ is the triplet state, so the teleportation fidelity is approximately 1/3. We assume the same operating conditions as in Fig. 2-6.

Taylor-series expansion to show that

$$F \approx F_0 - \frac{(1-4a)\Delta\psi^2}{6}, \tag{2.113}$$

where F_0 is the average fidelity for anti-phased pumps, i.e., when $\Delta\psi = 0$.

2.5.4 OPA Pump-Amplitude Fluctuations

Now we will study the effects of OPA pump-amplitude fluctuations—$|G_1|$ and $|G_2|$ will be taken to be statistically independent Gaussian random variables with mean values 0.1 and variances σ_G^2—when the pumps are anti-phased ($\Delta\psi = 0$) and the polarization restoration is perfect ($\theta_S = \theta_I = 0$). In this case the single-photon-error density matrix, given $\{G_1, G_2\}$, is

$$\hat{\rho} = \begin{pmatrix} \frac{1}{2}(b_1+b_2)-c & \frac{1}{2}(b_1-b_2) & 0 & 0 \\ \frac{1}{2}(b_1-b_2) & \frac{1}{2}(b_1+b_2)+c & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix}, \tag{2.114}$$

in the Bell basis, where, for $j = 1, 2$,

$$a = N_1 N_2 D_1 D_2 / D' \tag{2.115}$$

$$b_1 = (N_1^2 + \tilde{n}_1^2) D_2^2 / D' \tag{2.116}$$

$$b_2 = (N_2^2 + \tilde{n}_2^2) D_1^2 / D' \tag{2.117}$$

$$c = -\tilde{n}_1 \tilde{n}_2 D_1 D_2 / D' \tag{2.118}$$

$$N_j = \bar{n}_j (1 + \bar{n}_j) - \tilde{n}_j^2 \tag{2.119}$$

$$D_j = (1 + \bar{n}_j)^2 - \tilde{n}_j^2 \tag{2.120}$$

$$D' = 2 N_1 N_2 D_1 D_2 + (N_1^2 + \tilde{n}_1^2) D_2^2 + (N_2^2 + \tilde{n}_2^2) D_1^2 \tag{2.121}$$

$$\bar{n}_j = I_{j-} - I_{j+} \tag{2.122}$$

$$\tilde{n}_j = I_{j-} + I_{j+} \tag{2.123}$$

$$I_{j\pm} = \frac{\eta_L \gamma \gamma_c}{\Gamma \Gamma_c} \frac{G_j}{(1 \pm G_j)(1 \pm G_j + \Gamma_c / \Gamma)}. \tag{2.124}$$

Figure 2-8 shows simulation results for the average teleportation fidelity in the presence of these pump-amplitude fluctuations. The calculations assume an $L = 25\,\text{km}$ source-to-memory path length and same operating conditions as in Fig. 2-6. We see from this figure that pump-amplitude fluctuations should not be problematic: for 1% pump-power fluctuations with a mean pump power that is ~1% of oscillation threshold we have that $\sigma_G^2 \sim 10^{-4}$.

2.5.5 Detuning

At this juncture we turn to the effects of pump frequency errors. Suppose that the pumps have equal amplitudes and are anti-phased with $G_1 = G_2 = G > 0$, and that the polarization restoration is perfect. So far we have assumed that the dual-OPA's signal and idler frequencies are equal and equal to both the memory cavities' resonance frequency and the ^{87}Rb atomic line, i.e., $\omega_S = \omega_I = \omega_c = \omega_a$. In this final assessment of teleportation system errors we shall consider two possible cases of frequency detuning. In case 1 we shall assume that the dual-OPA operates somewhat off frequency degeneracy, so that the signal and idler frequencies are $\omega_S = \omega_P/2 + \Delta\omega$ and $\omega_I = \omega_P/2 - \Delta\omega$, with the frequency degeneracy point satisfying, $\omega_P/2 = \omega_c = \omega_a$, i.e., matched to the memory cavity and the ^{87}Rb atomic

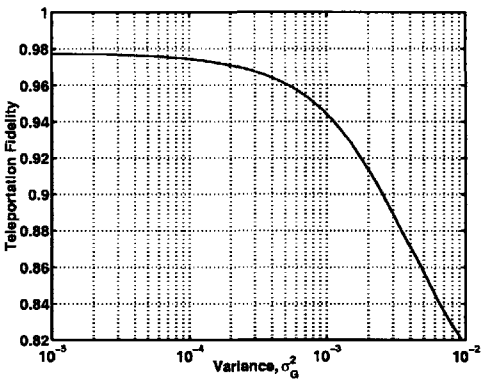


Figure 2-8: Teleportation fidelity with OPA gain fluctuations. The gain parameters G_1 and G_2 are taken to be statistically independent, identically distributed Gaussian random variables with means 0.1 and variances σ_G^2. We assume the same operating conditions as in Fig. 2-6.

line. In case 2 the dual-OPA operates at frequency degeneracy, $\omega_S = \omega_I = \omega_P/2$, but this frequency degeneracy point is detuned from the memory cavity and the atomic line, viz., $\omega_P/2 = \omega_c - \Delta\omega = \omega_a - \Delta\omega$.

It is not hard to study the effects of these two cavity detuning cases within the construct of our single-photon error model, because their resulting density matrices are both Werner states of the form given in Eq. (2.94). In particular, their success probabilities are given by

$$P_{s_j} = \frac{[\bar{n}(1+\bar{n}) - |\tilde{n}_j|^2]^2 + 2|\tilde{n}_j|^2}{4[\bar{n}(1+\bar{n}) - |\tilde{n}_j|^2]^2 + 2|\tilde{n}_j|^2} \tag{2.125}$$

where

$$\bar{n} = I_- - I_+ \tag{2.126}$$

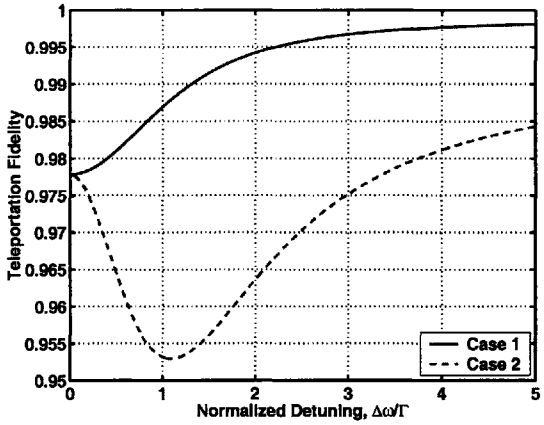
$$\tilde{n}_1 = I_- + I_+ \tag{2.127}$$

$$\tilde{n}_2 = I'_- + I'_+, \tag{2.128}$$

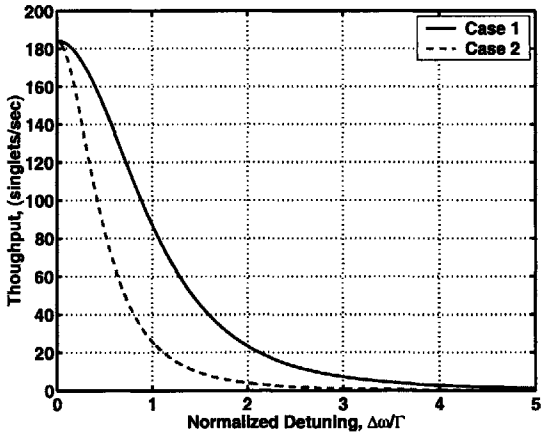
with

$$I_\pm = \frac{\eta_L \gamma \gamma_c}{\Gamma \Gamma_c} \frac{G}{(1 \pm G)\left[1 \pm G + \Gamma_c/\Gamma + \dfrac{\Delta\omega^2/\Gamma^2}{1 \pm G + \Gamma_c/\Gamma}\right]} \tag{2.129}$$

$$I'_\pm = \frac{\eta_L \gamma \gamma_c}{\Gamma(\Gamma_c + i\Delta\omega)} \frac{G}{(1 \pm G)(1 \pm G + \Gamma_c/\Gamma + i\Delta\omega/\Gamma)}. \tag{2.130}$$



(a)



(b)

Figure 2-9: (a) Teleportation fidelity versus normalized detuning, $\Delta\omega/\Gamma$. Case 1 assumes the signal and idler center frequencies are detuned from $\omega_P/2$. Case 2 assumes the atomic frequency is detuned from $\omega_P/2$. (b) Throughput of singlet states assuming cycling rate $R = 500$ kHZ. We assume the same operating conditions as in Fig. 2-6.

The average teleportation fidelity, $F_j = (2P_{s_j}+1)/3$ for $j = 1, 2$ is plotted versus normalized detuning in Fig. 2-9(a). We see that fidelity actually improves slightly as the normalized detuning is increased. However, this modest fidelity improvement is accompanied by a dramatic loss of singlet-state throughput, as seen in Fig. 2-9(b), when the detuning exceeds the OPA cavity's linewidth.

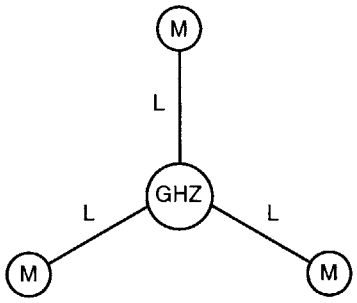


Figure 2-10: Schematic of long-distance GHZ communication system. GHZ = source of polarization-entangled photons from either Fig. 2-11(a) or (b); $L = L$ km of standard telecommunications fiber; M = trapped-atom quantum memory.

2.6 GHZ-State Communication

There has been much interest in Greenberger-Horne-Zeilinger (GHZ) states [38] because they can be used in a nonstatistical disproof of local hidden-variable theories of physics and as resources for multiparty quantum communication protocols [32]. As discussed in [24], the MIT/NU teleportation architecture has an extension that permits long-distance transmission and storage of three-party GHZ states,

$$|\psi_{\mathrm{GHZ}}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}. \tag{2.131}$$

In this section, we present single-photon error models for two versions of the proposed GHZ quantum communication system: one using dual degenerate parametric amplifiers (dual-DPAs) for its entanglement source, and the other using a DPA plus a heralded source of single photons. We will use these error models in the next section to develop performance analyses for the GHZ-state communication system in the quantum secret sharing (QSS) protocol.

2.6.1 GHZ-State Systems

Figure 2-10 is a schematic diagram for a long-distance quantum communication system that allows for the transmission and storage of the GHZ states required for multiparty quantum communication protocols such as QSS. This system uses an ultrabright source of polarization-entangled photons produced from optical parametric amplifiers. We employ quantum-state frequency conversion and time-division multiplexing polarization restoration

[24] to transmit the entangled photons over standard telecommunications fiber to be loaded into ^{87}Rb trapped-atom quantum memories [27] for storage and processing. By using this protocol to sequentially load an array of atomic memories at each location in Fig. 2-10, we can build up a reservoir of GHZ states that are shared by these memories.

We consider two possible source arrangements for the GHZ block in Fig. 2-10. The first is an ultrabright, narrowband variant of the source used by Bouwmeester et al. in an initial experimental demonstration of GHZ-state generation [39]. That experiment was an annihilative table-top measurement and had extremely low flux: 1 GHZ state every 150 sec. Our version of the Bouwmeester et al. source—shown in Fig. 2-11(a)—replaces their parametric downconverter with a pair of doubly-resonant, type-II phase matched DPAs. With this source, the Fig. 2-10 arrangement permits a throughput comparable to what Bouwmeester et al. produced in the laboratory to be realized at a source-to-memory radius of 10 km [24]. More important, though, is the fact that the memories in the Fig. 2-10 architecture allow the GHZ state to be stored for use in applications of three party entanglement.

Recent work has shown that it may be possible to construct heralded single-photon sources [40]. With such a source, we can design a GHZ system with a substantially higher throughput than the configuration discussed above. In Fig. 2-11(b), the heralded source places a single photon in the proper spatio-temporal mode for coupling to the trapped-atom quantum memory during each loading cycle. With the heralded-plus-DPA GHZ source, throughput rises by three orders of magnitude over the dual-DPA system, to about 15 GHZ states/sec at a 10 km source-to-memory radius [24].

2.6.2 Single-Photon Error Models

In this section, we present the single-photon loading event models for the dual-DPA and heralded-plus-DPA GHZ-state quantum communication systems [31]. In our analysis of the GHZ systems, we ignore issues of phase and amplitude errors in the entanglement source that were studied for the qubit teleportation system. Furthermore, except for fiber loss, we assume perfect transmission of the entangled photon pairs.

Let A, B, and C represent a clockwise labeling of the memories in Fig. 2-10 starting

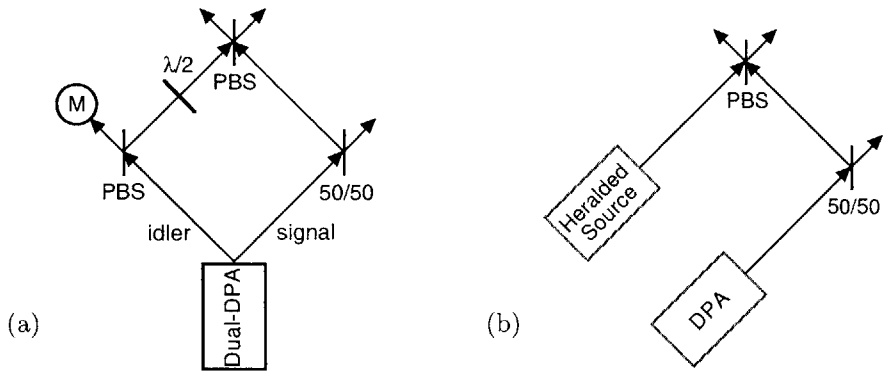


Figure 2-11: Source arrangements for the GHZ-state communication architecture in Fig. 2-10. (a) Dual-DPA GHZ system. The quantum memory in this figure represents a memory internal to the source block in Fig. 2-10; its loading is used as a trigger signal [24]. (b) Heralded single-photon source plus DPA system. PBS = polarizing beam splitter, $\lambda/2$ = half-wave plate.

from the lower left. We define the computational basis for these quantum memories to be,

$$|0\rangle_A = |01\rangle_{A_xA_y} \quad \text{and} \quad |1\rangle_A = |10\rangle_{A_xA_y}, \tag{2.132}$$

$$|0\rangle_B = |01\rangle_{B_xB_y} \quad \text{and} \quad |1\rangle_B = |10\rangle_{B_xB_y}, \tag{2.133}$$

$$|0\rangle_C = |10\rangle_{C_xC_y} \quad \text{and} \quad |1\rangle_C = |01\rangle_{C_xC_y}, \tag{2.134}$$

in terms of the number-ket representations for the x- and y-polarized photons that loaded these memories. With this computational basis, the GHZ state loaded by the Fig. 2-10 system is $|\psi_{\text{GHZ}}\rangle_{ABC} = (|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$.

It is not hard, using the basis,

$$\left\{ \frac{|000\rangle_{ABC} \pm |111\rangle_{ABC}}{\sqrt{2}}, |001\rangle_{ABC}, |110\rangle_{ABC}, |010\rangle_{ABC}, |101\rangle_{ABC}, |011\rangle_{ABC}, |100\rangle_{ABC} \right\}, \tag{2.135}$$

to compute the matrix elements of the joint conditional density operator for memories A, B, and C, given that an erasure has not occurred. The conditional density matrices for both the dual-DPA GHZ system and the heralded-plus-DPA GHZ system turn out to be diagonal in the Eq. (2.135) basis. (See [31] for a derivation of the diagonal elements.) For the dual-DPA source we find that,

$$\hat{\rho}_{ABC} = \text{diag}\Big(P_{G_d} \quad 0 \quad P_{e1_d} \quad P_{e1_d} \quad P_{e1_d} \quad P_{e1_d} \quad P_{e2_d} \quad P_{e2_d} \Big), \tag{2.136}$$

where

$$P_{G_d} = \frac{(N^2 + \tilde{n}^2)^2}{7N^4 + 12N^2\tilde{n}^2 + \tilde{n}^4}, \tag{2.137}$$

$$P_{e1_d} = \frac{N^2(N^2 + 2\tilde{n}^2)}{7N^4 + 12N^2\tilde{n}^2 + \tilde{n}^4}, \tag{2.138}$$

$$P_{e2_d} = \frac{N^2(N^2 + \tilde{n}^2)}{7N^4 + 12N^2\tilde{n}^2 + \tilde{n}^4}, \tag{2.139}$$

with $N \equiv \bar{n}(1 + \bar{n}) - \tilde{n}^2$. For the heralded-plus-DPA source we get,

$$\hat{\rho}_{ABC} = \mathrm{diag}\Big(P_{G_h} \quad 0 \quad P_{e1_h} \quad P_{e1_h} \quad P_{e2_h} \quad 0 \quad P_{e2_h} \quad 0\Big), \tag{2.140}$$

where

$$P_{G_h} = \frac{\eta(N^2 + \tilde{n}^2)D}{\eta(3N^2 + \tilde{n}^2)D + 2(1-\eta)N(N^2 + 2\tilde{n}^2)}, \tag{2.141}$$

$$P_{e1_h} = \frac{\eta N^2 D}{\eta(3N^2 + \tilde{n}^2)D + 2(1-\eta)N(N^2 + 2\tilde{n}^2)}, \tag{2.142}$$

$$P_{e2_h} = \frac{(1-\eta)N(N^2 + 2\tilde{n}^2)}{\eta(3N^2 + \tilde{n}^2)D + 2(1-\eta)N(N^2 + 2\tilde{n}^2)}, \tag{2.143}$$

with $D = (1 + \bar{n})^2 - \tilde{n}^2$. In calculating these matrix elements we have used the same transmission loss factor, $\eta = \eta_L\gamma\gamma_c/\Gamma\Gamma_c$, for each source-to-memory path in Figs. 2-10 and 2-11.

2.7 Quantum Secret Sharing

Secret sharing refers to cryptographic protocols that allow Alice to share secret information with Bob and Charlie in such a way that individually they have no means for learning Alice's secret, but by working together can they gain access to Alice's secret information. One classical implementation of secret sharing requires Alice to send Bob a random bit string r and to send Charlie the modulo-2 sum, $r \oplus m$, of the random bit string r and her message m. If Bob and Charlie act together, they can recover Alice's message m simply by adding their bit strings together. Of course, this protocol presumes that Bob cannot monitor Alice's transmission to Charlie and, likewise, that Charlie cannot intercept Alice's

		Charlie			
		$x+$	$x-$	$y+$	$y-$
Bob	$x+$	$x+$	$x-$	$y-$	$y+$
	$x-$	$x-$	$x+$	$y+$	$y-$
	$y+$	$y-$	$y+$	$x-$	$x+$
	$y-$	$y+$	$y-$	$x+$	$x-$

Table 2.1: QSS for classical information distribution. Lookup table for determining Alice's measurement outcome.

transmission to Bob.

Quantum secret sharing (QSS) protocols divide into two types, depending on whether Alice's secret information is classical or quantum. We will look at how GHZ states can be used to share classical and quantum secrets [32] and analyze the performance of our GHZ systems in the single-photon error model.

2.7.1 QSS for Classical Secrets

Hillery et al. presented a QSS protocol in [32] that allows Alice to send classical secret messages to Bob and Charlie by using GHZ states. The three parties first share N GHZ states, i.e., their joint state is $|\psi_{\text{GHZ}}\rangle_{ABC}^{\otimes N}$.[1] For each shared GHZ state,

$$|\psi_{\text{GHZ}}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}), \tag{2.144}$$

Alice, Bob, and Charlie measure on their own memories randomly in either the x basis or the y basis, where

$$|x\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |y\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle). \tag{2.145}$$

After making these measurements, Alice, Bob, and Charlie publicly announce their measurement bases. Bob and Charlie individually have no information about Alice's measurement outcomes, but in half of the cases—i.e., when Bob and Charlie used the same basis and Alice used the x basis, or when Bob and Charlie used different bases and Alice used the y basis—they can work together to determine Alice's results by using the lookup table

[1] Reference [32] does not present an architecture for establishing this shared entanglement over a long distance; we described just such an architecture, however, in Section 2.6.1. See also [24],[31].

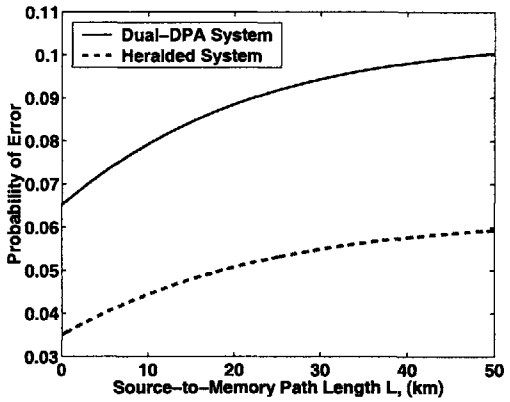


Figure 2-12: QSS bit error probabilities for dual-DPA and heralded-plus-DPA GHZ systems in the QSS protocol. These plots assume each DPA operates at 1% of its oscillation threshold, 5 dB excess loss in each source-to-memory path, 0.2 dB/km loss in each fiber, and $\Gamma_c/\Gamma = 0.5$ ratio of memory-cavity linewidth to source-cavity linewidth.

in Table 2.1. For example, if they all measure in the x basis and Bob and Charlie both obtain the result $x-$, then they know that Alice has the result $x+$.

Alice, Bob, and Charlie keep the measurement results from the cases in which they chose appropriate bases and discard the others. By associating Alice's $x+, y+$ results with bit 0 and Alice's $x-, y-$ results with bit 1, Alice now shares a joint key with Bob and Charlie with which she can encode classical messages.

In our error model, Alice, Bob, and Charlie will sometimes carry out the QSS protocol with an incorrect state from the ensemble of states in the basis (2.135). In an error event, it is possible for Bob and Charlie to obtain incorrect results from the lookup table. Shared key bits created with error states have error probability 1/2.

From the density matrices (2.136) and (2.140), we can compute the bit error probability for the QSS protocol. With the dual-DPA GHZ system a bit error probability of

$$P_e = 2P_{e1_d} + P_{e2_d} \tag{2.146}$$

is introduced into Alice's information transmission. With the heralded GHZ system, we have error probability

$$P_e = P_{e1_h} + P_{e2_h}. \tag{2.147}$$

The bit error probabilities (2.146) and (2.147) are plotted in Fig. 2-12. Possible methods for

improving the performance of our GHZ systems include purifying the three-party entangled state to reduce the number of error events or using classical error correction to transmit Alice's message.

2.7.2 QSS for Quantum Secrets

We now consider the performance of our GHZ systems for transmission of quantum information using the QSS protocol proposed in [32]. In this protocol, Alice, Bob, and Charlie share a GHZ state $|\psi_{\rm GHZ}\rangle_{ABC} = (|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$, and Alice's secret is the qubit $|\psi\rangle_S = \alpha|0\rangle_S + \beta|1\rangle_S$, which she wishes to send to Bob and Charlie in such a way that they must cooperate to obtain this quantum information. The joint state of Alice, Bob, and Charlie—including Alice's portion of the GHZ state *and* her quantum secret—at the start of the QSS protocol is $|\psi\rangle_S|\psi_{\rm GHZ}\rangle_{ABC}$.

Alice initiates the QSS protocol by making the Bell-state measurement, $\{|\psi^{\pm}\rangle_{SA}, |\phi^{\pm}\rangle_{SA}\}$, on her secret qubit and her portion of the GHZ state. Alice then labels as (m, n) the two classical bits she derives from these measurements, using the following scheme: $\psi^+ = (0,1), \psi^- = (1,1), \phi^+ = (0,0), \phi^- = (1,0)$. She sends m to Bob and $m \oplus n$ to Charlie, using secure classical channels so that Bob cannot intercept $m \oplus n$ and Charlie cannot obtain m. It follows that neither Bob nor Charlie has any information about Alice's secret—even after receiving the classical information from Alice—because their marginal density operators at this point in the protocol can be shown to be $\hat{\rho}_B = \hat{I}_B/2$ and $\hat{\rho}_C = \hat{I}_C/2$, respectively, where $\hat{I}$ is the identity operator.

For Bob and Charlie to learn Alice's secret qubit $|\psi\rangle_S$, they must cooperate. Because the no-cloning theorem precludes making two copies of this state, either Bob or Charlie—but *not* both of them—will possess a replica of $|\psi\rangle_S$ at the end of the QSS protocol. Let us arbitrarily assume that Bob and Charlie have agreed to let Charlie be the recipient of this replica. Having made that agreement, Bob measures his portion of the GHZ state in the x basis, $\{|\pm x\rangle_B \equiv (|0\rangle_B \pm |1\rangle_B)/\sqrt{2}\}$, and he sends Charlie the result of this measurement along with Alice's m bit. Together with Alice's $m \oplus n$—which he received earlier—Charlie now has all the information he needs to turn his portion of the GHZ state into a replica of Alice's secret via a local unitary operation.

Shared State	QSS Output	Fidelity	Dual-DPA	Heralded
$\|\psi_{\text{GHZ}}\rangle_{ABC}$	$\|\phi\rangle_S$	1	P_{G_d}	P_{G_h}
$\|001\rangle_{\text{ABC}}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e1_d}	P_{e1_h}
$\|110\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e1_d}	P_{e1_h}
$\|010\rangle_{ABC}$	$\|\alpha\|^2\|0\rangle_{SS}\langle 0\| + \|\beta\|^2\|1\rangle_{SS}\langle 1\|$	2/3	P_{e1_d}	P_{e2_h}
$\|101\rangle_{ABC}$	$\|\alpha\|^2\|0\rangle_{SS}\langle 0\| + \|\beta\|^2\|1\rangle_{SS}\langle 1\|$	2/3	P_{e1_d}	0
$\|011\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e2_d}	P_{e2_h}
$\|100\rangle_{ABC}$	$\|\beta\|^2\|0\rangle_{SS}\langle 0\| + \|\alpha\|^2\|1\rangle_{SS}\langle 1\|$	1/3	P_{e2_d}	0

Table 2.2: For each three-party state that might be shared by Alice, Bob, and Charlie, this table lists the output state that will result from application of the QSS protocol—in which Alice, Bob, and Charlie *assume* that they have shared the GHZ state $|\psi_{\text{GHZ}}\rangle_{ABC}$—the average fidelity that is achieved with this output state when the quantum secret $|\psi\rangle_S$ is uniformly distributed over the Bloch sphere, and the occurrence probabilities [from Eqs. (2.136) and (2.140), for the dual-DPA and heralded-plus-DPA sources, respectively] of these output states.

Uncoded Performance

Let F be the average fidelity of the preceding QSS protocol when Alice's secret, $|\psi\rangle_S$, is selected from a uniform distribution over the Bloch sphere. Using Table 2.2, we compute the average QSS fidelity for the dual-DPA GHZ system to be,

$$F = P_{G_d} + 2P_{e1_d} + 2P_{e2_d}/3, \tag{2.148}$$

and for the heralded-plus-DPA GHZ system,

$$F = P_{G_h} + 2P_{e1_h}/3 + P_{e2_h}. \tag{2.149}$$

Coded Performance

Quantum error correction can be used to improve the performance of the QSS protocol. We will illustrate this improvement by considering use of the five-qubit error-correcting code: [41]

$$|0_L\rangle = |00000\rangle + |00110\rangle + |01001\rangle + |01111\rangle + |10101\rangle - |10011\rangle + |11100\rangle + |11010\rangle, \tag{2.150}$$

$$|1_L\rangle = -|00101\rangle - |00011\rangle + |01100\rangle - |01010\rangle - |10000\rangle + |10110\rangle + |11001\rangle + |11111\rangle. \tag{2.151}$$

Table 2.2 lists the output states that result from application of the QSS protocol—in which Alice, Bob, and Charlie *assume* that they have shared the GHZ state $|\psi_{\rm GHZ}\rangle_{ABC}$—when in fact they have shared one of the states from the basis (2.135). From this table, we see that applying the QSS protocol, when a particular basis state has been shared, is equivalent to sending a qubit over one of the following three channels:

$$\mathcal{E}_I(\hat{\rho}) = \hat{\rho}, \tag{2.152}$$

$$\mathcal{E}_A(\hat{\rho}) = \hat{P}_0\hat{\rho}\hat{P}_0^\dagger + \hat{P}_1\hat{\rho}\hat{P}_1^\dagger, \tag{2.153}$$

$$\mathcal{E}_B(\hat{\rho}) = \hat{P}_2\hat{\rho}\hat{P}_2^\dagger + \hat{P}_2^\dagger\hat{\rho}\hat{P}_2, \tag{2.154}$$

where $\hat{P}_0 = |0\rangle\langle 0|$, $\hat{P}_1 = |1\rangle\langle 1|$, and $\hat{P}_2 = |0\rangle\langle 1|$. Channel $\mathcal{E}_A$ takes an input qubit $\alpha|0\rangle + \beta|1\rangle$ to the mixed state $|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$, and channel $\mathcal{E}_B$ gives the output state $|\beta|^2|0\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|$. Because the density matrix for the $\{A, B, C\}$ quantum memories is diagonal in the Eq. (2.135) basis, these three channel possibilities, $\{\mathcal{E}_I, \mathcal{E}_A, \mathcal{E}_B\}$, occur with probabilities

$$P_I = P_{G_d} \tag{2.155}$$

$$P_A = 2P_{e1_d} \tag{2.156}$$

$$P_B = 2P_{e1_d} + 2P_{e2_d}, \tag{2.157}$$

for the dual-DPA system, and

$$P_I = P_{G_h} \tag{2.158}$$

$$P_A = P_{e2_h} \tag{2.159}$$

$$P_B = 2P_{e1_h} + P_{e2_h}, \tag{2.160}$$

for the heralded-plus-DPA system.

The five-qubit coded QSS channel has the form

$$\mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \mathcal{E}_3 \otimes \mathcal{E}_4 \otimes \mathcal{E}_5(\hat{\rho}_{\rm enc}), \tag{2.161}$$

where $\hat{\rho}_{\rm enc}$ is the encoded qubit state and $\mathcal{E}_i \in \{\mathcal{E}_I, \mathcal{E}_A, \mathcal{E}_B\}$. Numerical evaluation of the five-qubit error-correcting code was used to obtain the average fidelity for each of the 243

Case	(n_I, n_A, n_B)	F_j	# of channels
1	$(5,0,0)$	1	1
2	$(4,1,0)$	1	5
3	$(4,0,1)$	1	5
4	$(3,2,0)$	5/6	10
5	$(3,1,1)$	2/3	20
6	$(3,0,2)$	1/3	10
7	$(2,3,0)$	7/10	10
8	$(2,2,1)$	47/90	30
9	$(2,1,2)$	19/45	30
10	$(2,0,3)$	7/15	10
11	$(1,4,0)$	37/60	5
12	$(1,3,1)$	29/60	20
13	$(1,2,2)$	17/36	30
14	$(1,1,3)$	31/60	20
15	$(1,0,4)$	11/20	5
16	$(0,5,0)$	7/12	1
17	$(0,4,1)$	29/60	5
18	$(0,3,2)$	29/60	10
19	$(0,2,3)$	31/60	10
20	$(0,1,4)$	31/60	5
21	$(0,0,5)$	5/12	1
total			243

Table 2.3: Coded QSS channel results. The 243 coded QSS channels are divided into 21 cases according to component distribution (n_I, n_A, n_B). For each case, we list the average fidelity F_j and the number of coded QSS channels belonging to that case.

possible coded QSS channels. For each coded QSS channel, let n_k be the number of $\mathcal{E}_k$ components, $k = I, A, B$. The 243 channels were divided into 21 different cases, according to the distribution (n_I, n_A, n_B). The results of the coded QSS channel simulations are displayed in Table 2.3. The average fidelity of the coded QSS channel is then calculated, using the multinomial distribution for (n_I, n_A, n_B), as follows,

$$F = \sum_{j=1}^{21} \Pr(\text{case } j) F_j = \sum_{j=1}^{21} \binom{5}{n_I, n_A, n_B} P_I^{n_I} P_A^{n_A} P_B^{n_B} F_j, \tag{2.162}$$

where F_j is the average fidelity of the five qubit code given that a coded QSS channel in case j occurs and the j-dependence of (n_I, n_A, n_B) is as given in Table 2.3.

Figure 2-13 shows the average QSS fidelity for the dual-DPA and heralded-plus-DPA GHZ systems with and without coding. We see that the heralded-plus-DPA GHZ system

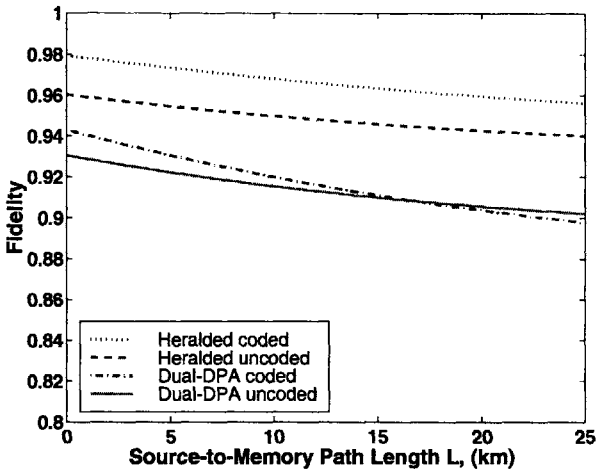


Figure 2-13: Average fidelity in the QSS protocol. We compare the performance of the dual-DPA and heralded-plus-DPA GHZ systems with and without coding. We assume the same operating conditions as in Fig. 2-12.

has significantly better performance than the dual-DPA system in the QSS protocol in both uncoded and coded operation. Coding improves the performance of the heralded-plus-DPA system for all path lengths shown in this figure, but beyond about 16 km source-to-memory path length coding reduces the fidelity of the dual-DPA system. The dual-DPA curves with and without error correction cross because the five-qubit code degrades performance when the incidence of multi-qubit errors is too high. Interestingly, the same thing does not occur for the heralded-plus-DPA system, because the conditional density matrix (2.140) reaches a limiting value for path length around $L = 50$ km.

Entanglement Purification

In this section an alternative approach for improving the performance of the GHZ system is studied: the use of an entanglement purification protocol. Let Alice, Bob, and Charlie possess a block of n mixed entangled three-party states. Through the use of local operations and classical communications, they can produce a smaller number $m < n$ of GHZ states with arbitrarily small probability of error for large n. The yield of an entanglement purification protocol is defined as $Y = m/n$ in the limit $n \to \infty$.

The entanglement purification scheme we shall consider is the multiparty hashing pro-

tocol [42]. Define the cat basis as the set of orthonormal states

$$|\psi_{p,i_1 i_2}\rangle_{ABC} = \frac{|0 i_1 i_2\rangle_{ABC} + (-1)^p |1\bar{i}_1\bar{i}_2\rangle_{ABC}}{\sqrt{2}}, \tag{2.163}$$

where $p, i_1, i_2 = 0, 1$. We call p the phase bit and i_1, i_2 the amplitude bits. Given an initial mixed entangled state $\hat{\rho}_{ABC}$, let $H(p), H(i_1)$, and $H(i_2)$ be the entropies of the phase and amplitude bits with respect to the diagonal cat-basis matrix entries of $\hat{\rho}_{ABC}$. From Table 2.4, we find that the entropies of the phase and amplitude bits for the dual-DPA GHZ system are

$$H(p) = H(P_{G_d} + 2P_{e1_d} + P_{e2_d}) \tag{2.164}$$

$$H(i_1) = H(P_{G_d} + 2P_{e1_d}) \tag{2.165}$$

$$H(i_2) = H(P_{G_d} + 2P_{e1_d}), \tag{2.166}$$

and for the heralded-plus-DPA GHZ system,

$$H(p) = H(P_{G_h} + P_{e1_h} + P_{e2_h}) \tag{2.167}$$

$$H(i_1) = H(P_{G_h} + 2P_{e1_h}) \tag{2.168}$$

$$H(i_2) = H(P_{G_h} + P_{e2_h}). \tag{2.169}$$

Maneva and Smolin [42] have shown that the yield of the multiparty hashing protocol is

$$Y = 1 - H(p) - \max\{H(i_1), H(i_2)\}, \tag{2.170}$$

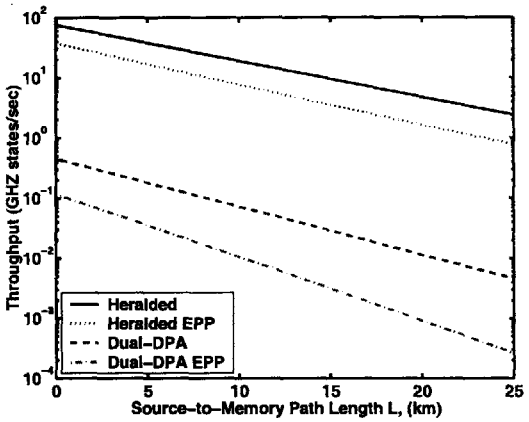
if the right-hand side is a positive quantity, and it is zero otherwise.

Figure 2-14 compares the performance of the GHZ-state systems with and without the use of the multiparty hashing protocol. Figure 2-14(a) shows normalized throughput, YN_{success}, versus source-to-memory path length, where $N_{\text{success}} = R\Pr(\psi_{GHZ})$ is the throughput of successful GHZ memory loadings/sec and yield $Y = 1$ when no entanglement purification is employed. The throughput lost through the application of the hashing protocol is modest for the heralded GHZ system and is more substantial for the dual-DPA system. Assuming perfect measurements at the transmitter and perfect qubit logic at the receiver in implementing the hashing protocol, the average QSS fidelity is unity in the limit

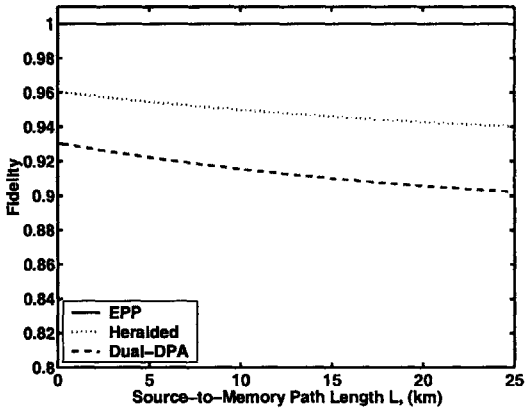
Cat State	p	i_1	i_2	Dual-DPA	Heralded
$\|000\rangle + \|111\rangle$	0	0	0	P_{G_d}	P_{G_h}
$\|000\rangle - \|111\rangle$	1	0	0	0	0
$\|001\rangle + \|110\rangle$	0	0	1	P_{e1_d}	P_{e1_h}
$\|001\rangle - \|110\rangle$	1	0	1	P_{e1_d}	P_{e1_h}
$\|010\rangle + \|101\rangle$	0	1	0	P_{e1_d}	$P_{e2_h}/2$
$\|010\rangle - \|101\rangle$	1	1	0	P_{e1_d}	$P_{e2_h}/2$
$\|011\rangle + \|100\rangle$	0	1	1	P_{e2_d}	$P_{e2_h}/2$
$\|011\rangle - \|100\rangle$	1	1	1	P_{e2_d}	$P_{e2_h}/2$

Table 2.4: The distribution for each bit of the unknown cat state is determined by the single-photon density matrices (2.136) and (2.140). The distributions can be used to compute the entropies $H(p), H(i_1)$, and $H(i_2)$.

of large block sizes, as shown in Fig. 2-14(b). The major drawback of utilizing entanglement purification, as compared to the much simpler five-qubit error correction code, is the enormous amounts of quantum memory that are needed at the transmitter and receiver to realize the large block sizes that validate use of the asymptotic yield expression (2.170).



(a)



(b)

Figure 2-14: Performance of dual-DPA and heralded GHZ systems with the multiparty hashing protocol. (a) Throughput of GHZ states with and without the hashing protocol. (b) Average fidelity for quantum secret sharing. With the hashing protocol, the fidelity of QSS approaches one as the block size $n \to \infty$. We assume the same operating conditions as in Fig. 2-12. EPP = entanglement purification protocol.

Chapter 3

Quantum Multiple Access Channels

In Section 1.1.4, we described the superdense coding communication protocol [10] for enhancing the transmission of classical information over a quantum channel through the use of shared prior entanglement. For channels with a single transmitter and a single receiver, the classical information capacity of superdense coding was obtained in [13] and [14]. In Section 3.1, we generalize these results by deriving the capacity region of the superdense coding multiple access channel (MAC). The MAC problem arises when multiple users wish to send classical information to a common receiver. The transmissions from any one user must contend with interference created by transmissions from all the other users, in addition to the usual sources of noise encountered on a single-user channel. The superdense coding protocol restricts transmitters to unitary encodings. In Section 3.2, we remove this restriction to study the capacity of quantum MACs with general encodings.

3.1 Superdense Coding MAC

In this section, we consider a multiple access superdense coding protocol for the transmission of classical information over a quantum channel that uses shared tripartite entanglement. To find the capacity region of the superdense coding MAC, we derive upper bounds on the information transmission rates and present an encoding scheme that achieves these upper bounds. A special case of this result was proved in [43] for pure bipartite entangled states. In our derivation, we consider a superdense coding MAC with mixed tripartite states in

spaces of dimension $d_A \times d_B \times d_C$. We also state the generalization to the case with $s > 2$ senders.

3.1.1 Quantum MAC

A quantum MAC with two transmitters, Alice and Bob, is modeled by the map: $(i,j) \to \hat{\rho}_{ij}$, where the output states $\hat{\rho}_{ij}$ live in a Hilbert space $\mathcal{H}$. The receiver performs a measurement on the state $\hat{\rho}_{ij}$ to learn the input messages i and j. Let $p_i^A p_j^B$ be a product probability distribution for the letter states $\hat{\rho}_{ij}$, and denote the average ensemble density matrices by

$$\hat{\rho} = \sum_i \sum_j p_i^A p_j^B \hat{\rho}_{ij}, \quad \hat{\rho}_i^A = \sum_j p_j^B \hat{\rho}_{ij}, \quad \hat{\rho}_j^B = \sum_i p_i^A \hat{\rho}_{ij} \tag{3.1}$$

and the conditional von Neumann entropies by

$$H_A = \sum_j p_j^B S(\hat{\rho}_j^B) \quad \text{and} \quad H_B = \sum_i p_i^A S(\hat{\rho}_i^A). \tag{3.2}$$

In this chapter, we will only consider the one-shot classical capacity, i.e., the $M = 1$ case described in Section 1.1.5. In this case, an (N_1, N_2, n)-code for the quantum MAC with letter states $\hat{\rho}_{ij}$ consists of N_1 i-sequences and N_2 j-sequences of length n. The codeword corresponding to the message sequences $(i_1, \ldots, i_n)$ and $(j_1, \ldots, j_n)$ is the product state $\hat{\rho}_{i_1 j_1} \otimes \cdots \otimes \hat{\rho}_{i_n j_n}$. The rate pair (R_1, R_2) is said to be achievable if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes for which the receiver Charlie can decode both Alice's and Bob's messages with probability of error $P_e \to 0$ as $n \to \infty$. The capacity region is defined as the closure of the set of all achievable rate pairs.

The capacity region for the transmission of classical information over a quantum MAC was derived in [44]. It is given by the closure of the convex hull of all (R_1, R_2) satisfying

$$R_1 < H_A - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.3}$$

$$R_2 < H_B - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.4}$$

$$R_1 + R_2 < S(\hat{\rho}) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}), \tag{3.5}$$

for some product distribution $p_i^A p_j^B$.

3.1.2 Superdense Coding

In the superdense coding MAC communication protocol, Alice, Bob, and Charlie share qudits in the initial state $\hat{\rho}_0$ that lives in the Hilbert space $\mathcal{H}_{d_A} \otimes \mathcal{H}_{d_B} \otimes \mathcal{H}_{d_C}$. Alice and Bob encode independent classical messages by applying local unitary operators to their qudits and sending their qudits over noiseless quantum channels to Charlie, who then decodes their messages with a measurement on the combined system of the three qudits. We will find the information rates that are achievable with this communication protocol.

Theorem 1 *The capacity region of the superdense coding MAC is the set of rate pairs* (R_1, R_2) *that satisfy*

$$R_1 \leq S(\hat{\rho}_{BC}) - S(\hat{\rho}_0) + \log d_A \tag{3.6}$$

$$R_2 \leq S(\hat{\rho}_{AC}) - S(\hat{\rho}_0) + \log d_B \tag{3.7}$$

$$R_1 + R_2 \leq S(\hat{\rho}_C) - S(\hat{\rho}_0) + \log d_A + \log d_B, \tag{3.8}$$

where $\hat{\rho}_{BC} = tr_A(\hat{\rho}_0)$, $\hat{\rho}_{AC} = tr_B(\hat{\rho}_0)$, *and* $\hat{\rho}_C = tr_{AB}(\hat{\rho}_0)$ *are the reduced densities of the initial state* $\hat{\rho}_0$.

Proof Suppose Alice and Bob utilize local unitary operators $\{\hat{U}_i^A\}$ and $\{\hat{U}_j^B\}$, respectively, with product distribution $p_i^A p_j^B$ to encode their messages. Then the ensemble density operators defined in (3.1) are

$$\hat{\rho} = \sum_i \sum_j p_i^A p_j^B (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_0 (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.9}$$

$$\hat{\rho}_i^A = \sum_j p_j^B (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_0 (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.10}$$

$$\hat{\rho}_j^B = \sum_i p_i^A (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_0 (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger. \tag{3.11}$$

By subadditivity of von Neumann entropy, we obtain the following upper bound on the

conditional entropy H_A:

$$H_A = \sum_j p_j^B S(\hat{\rho}_j^B) \tag{3.12}$$

$$\leq \sum_j p_j^B \left[S(\mathrm{tr}_A(\hat{\rho}_j^B)) + S(\mathrm{tr}_{BC}(\hat{\rho}_j^B)) \right] \tag{3.13}$$

$$= \sum_j p_j^B \left[S((\hat{U}_j^B \otimes \hat{I}^C)\hat{\rho}_{BC}(\hat{U}_j^B \otimes \hat{I}^C)^\dagger) + S(\mathrm{tr}_{BC}(\hat{\rho}_j^B)) \right] \tag{3.14}$$

$$\leq \sum_j p_j^B \left[S(\hat{\rho}_{BC}) + \log d_A \right] \tag{3.15}$$

$$= S(\hat{\rho}_{BC}) + \log d_A, \tag{3.16}$$

Similarly, $H_B \leq S(\hat{\rho}_{AC}) + \log d_B$. An upper bound for $S(\hat{\rho})$ is derived as

$$S(\hat{\rho}) \leq S(\mathrm{tr}_{AB}(\hat{\rho})) + S(\mathrm{tr}_C(\hat{\rho})) \tag{3.17}$$

$$= S\left(\sum_i \sum_j p_i^A p_j^B \mathrm{tr}_{AB}(\hat{\rho}_0) \right) + S(\mathrm{tr}_C(\hat{\rho})) \tag{3.18}$$

$$\leq S(\hat{\rho}_C) + \log d_A + \log d_B, \tag{3.19}$$

Thus, (3.6)-(3.8) are upper bounds on the transmission rates (R_1, R_2) for the superdense coding MAC with tripartite entanglement.

To achieve these upper bounds, Alice and Bob encode their messages with equiprobable ensembles of generalized Pauli operators [9]. In a d-dimensional Hilbert space, the Pauli operators are defined as

$$\hat{U}_{nm} = \sum_{k=0}^{d-1} \exp\left(\frac{2\pi i k n}{d}\right) |k\rangle\langle k+m|, \tag{3.20}$$

for $n, m = 0, 1, \ldots, d-1$. Let $\{\hat{U}_i^k\}, i = 0, 1, \ldots, d_k^2 - 1$, be the set of generalized Pauli operators in $\mathcal{H}_{d_k}$, with $\hat{U}_0^k = \hat{I}^k$, for $k = A, B, C$.

Expand the initial state in the Pauli operator basis,

$$\hat{\rho}_0 = \sum_{l=0}^{d_A^2-1} \sum_{m=0}^{d_B^2-1} \sum_{n=0}^{d_C^2-1} \lambda_{lmn} \hat{U}_l^A \otimes \hat{U}_m^B \otimes \hat{U}_n^C. \tag{3.21}$$

Then, the reduced densities can be written as

$$\hat{\rho}_{BC} = d_A \sum_m \sum_n \lambda_{0mn} \hat{U}_m^B \otimes \hat{U}_n^C, \tag{3.22}$$

$$\hat{\rho}_{AC} = d_B \sum_l \sum_n \lambda_{k0n} \hat{U}_l^A \otimes \hat{U}_n^C, \tag{3.23}$$

and

$$\hat{\rho}_C = d_A d_B \sum_n \lambda_{00n} \hat{U}_n^C, \tag{3.24}$$

using the trace of the Pauli operators, $\mathrm{tr}(\hat{U}_i^k) = d_k \delta_{0i}$. If Alice and Bob transmit their inputs with equal probability, i.e., $p_i^A = 1/d_A^2$ and $p_j^B = 1/d_B^2$, then the average ensemble density operator is

$$\hat{\rho} = \sum_i \sum_j p_i^A p_j^B (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_0 (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.25}$$

$$= \frac{1}{d_A^2 d_B^2} \sum_i \sum_j (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \left[\sum_l \sum_m \sum_n \lambda_{lmn} \hat{U}_l^A \otimes \hat{U}_m^B \otimes \hat{U}_n^C \right] (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.26}$$

$$= \frac{1}{d_A^2 d_B^2} \sum_l \sum_m \sum_n \lambda_{lmn} \sum_i (\hat{U}_i^A \hat{U}_l^A \hat{U}_i^{A\dagger}) \otimes \sum_j (\hat{U}_j^B \hat{U}_m^B \hat{U}_j^{B\dagger}) \otimes \hat{U}_n^C \tag{3.27}$$

$$= \frac{1}{d_A^2 d_B^2} \sum_l \sum_m \sum_n \lambda_{lmn} (d_A^2 \delta_{0l} \hat{I}^A) \otimes (d_B^2 \delta_{0m} \hat{I}^B) \otimes \hat{U}_n^C \tag{3.28}$$

$$= \frac{\hat{I}^A}{d_A} \otimes \frac{\hat{I}^B}{d_B} \otimes d_A d_B \sum_n \lambda_{00n} \hat{U}_n^C \tag{3.29}$$

$$= \frac{\hat{I}^A}{d_A} \otimes \frac{\hat{I}^B}{d_B} \otimes \hat{\rho}_C. \tag{3.30}$$

In line (3.28), we used the sum [13],[45]: $\sum_j (\hat{U}_j^k \hat{U}_i^k \hat{U}_j^{k\dagger}) = d_k^2 \delta_{0i} \hat{I}^k$, for $k = A, B, C$. We see that the average density operator is disentangled and has entropy $S(\hat{\rho}) = S(\hat{\rho}_C) + \log d_A +$

$\log d_B$. The average conditional density operator is

$$\hat{\rho}_j^B = \sum_i p_i^A (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_0 (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.31}$$

$$= \frac{1}{d_A^2} \sum_i (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C) \left[\sum_l \sum_m \sum_n \lambda_{lmn} \hat{U}_l^A \otimes \hat{U}_m^B \otimes \hat{U}_n^C \right] (\hat{U}_i^A \otimes \hat{U}_j^B \otimes \hat{I}^C)^\dagger \tag{3.32}$$

$$= \frac{1}{d_A^2} \sum_l \sum_m \sum_n \lambda_{lmn} \sum_i (\hat{U}_i^A \hat{U}_l^A \hat{U}_i^{A\dagger}) \otimes (\hat{U}_j^B \hat{U}_m^B \hat{U}_j^{B\dagger}) \otimes \hat{U}_n^C \tag{3.33}$$

$$= \sum_m \sum_n \lambda_{0mn} \hat{I}^A \otimes (\hat{U}_j^B \hat{U}_m^B \hat{U}_j^{B\dagger}) \otimes \hat{U}_n^C \tag{3.34}$$

$$= \frac{\hat{I}^A}{d_A} \otimes \left[(\hat{U}_j^B \otimes \hat{I}^C) \hat{\rho}_{BC} (\hat{U}_j^B \otimes \hat{I}^C)^\dagger \right]. \tag{3.35}$$

Thus, $S(\hat{\rho}_j^B)$ is independent of j and the conditional entropy is $H_A = S(\hat{\rho}_{BC}) + \log d_A$. Similarly, $H_B = S(\hat{\rho}_{AC}) + \log d_B$. This encoding scheme achieves upper bounds (3.6)-(3.8), and therefore establishes the capacity of the superdense coding MAC as the set of all rate pairs (R_1, R_2) that satisfy these inequalities. ∎

The capacity theorem in [44] applies for $s \geq 2$ senders, so we can generalize Theorem 1. The proof is similar to the one given for $s = 2$ senders, so we just state the result. Let the initial state $\hat{\rho}_0$ live in the Hilbert space $\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_{s+1}}$, with $\dim \mathcal{H}_{A_i} = d_{A_i}$, and define $\hat{\rho}_{J^c}$ as the reduced density of $\hat{\rho}_0$ in the space $\bigotimes_{i \in J^c \cup \{s+1\}} \mathcal{H}_{A_i}$. For $s \geq 2$ senders, the capacity of the superdense coding MAC is the set of all rates $(R_1, \ldots R_s)$ that satisfy, for all subsets $J \subseteq \{1, \ldots, s\}$:

$$\sum_{i \in J} R_i \leq S(\hat{\rho}_{J^c}) - S(\hat{\rho}_0) + \sum_{i \in J} \log d_{A_i}. \tag{3.36}$$

3.1.3 GHZ-State MAC

Superdense coding uses shared entanglement to enhance the transmission of classical information over a quantum MAC. With no shared entanglement, the transmission of a single qubit can convey at most one bit of information, which implies that the optimal capacity region of the quantum MAC with no shared entanglement is represented by the inner region in Fig. 3-1. The capacity result stated in Theorem 1 allows us to quantify the improvement in performance that can be derived from shared entanglement.

We will illustrate this capacity enhancement with the following two three-party qubit

states: the GHZ state,

$$|\psi_{\text{GHZ}}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}), \tag{3.37}$$

and the W state,

$$|\psi_{\text{W}}\rangle_{ABC} = \frac{1}{\sqrt{3}}(|001\rangle_{ABC} + |010\rangle_{ABC} + |100\rangle_{ABC}). \tag{3.38}$$

GHZ states were previously discussed in Section 2.6. The W state is the tripartite entangled state that is maximally robust against the loss of a qubit [46]. From Theorem 1, the capacity region for the GHZ-state MAC is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \leq 2, \quad R_2 \leq 2, \quad \text{and} \quad R_1 + R_2 \leq 3, \tag{3.39}$$

and the capacity region for the W-state MAC is given by

$$R_1 \leq H(1/3) + 1, \quad R_2 \leq H(1/3) + 1, \quad \text{and} \quad R_1 + R_2 \leq H(1/3) + 2, \tag{3.40}$$

where $H(p) \equiv -p \log p - (1-p)\log(1-p)$ is the binary entropy function. These capacity regions are shown in Fig. 3-1.

The GHZ-state MAC gives the largest possible capacity region for a qubit quantum MAC. We can describe an explicit coding scheme [47] for achieving this capacity region. Let Alice encode two bits on her qubit with the set of Pauli operators $\{\hat{I}, \hat{X}, \hat{Y}, \hat{Z}\}$, and let Bob encode one bit with the set $\{\hat{I}, \hat{X}\}$. The eight possible received states from this encoding are orthogonal, which means that Charlie can perform a measurement that reveals the messages sent by Alice and Bob. The rate of this code is $(R_1, R_2) = (2, 1)$. By symmetry, the rate $(1, 2)$ is also achievable. Thus, by time sharing between these two codes, the entire outer region in Fig. 3-1 is achievable.

3.1.4 Alternative Superdense Coding Protocol

The superdense coding protocol is restricted to encodings with local unitary operators. A step toward removing this restriction can be made by giving the senders, Alice and Bob, the option of discarding their share of the entangled state $\hat{\rho}_0$ and simply sending orthogonal

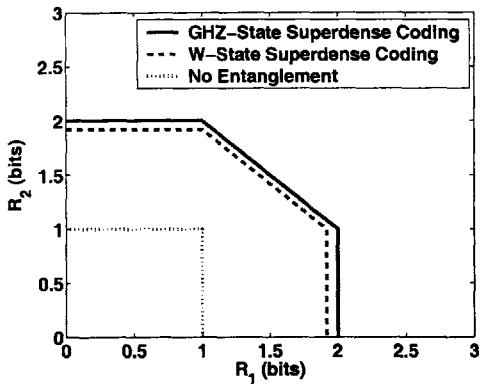


Figure 3-1: Capacity region of the superdense coding MAC with W-state and GHZ-state entanglement and the capacity of the quantum MAC with no shared entanglement.

qudits over their noiseless quantum channel. This alternative procedure has been considered for single-user channels [13],[48]. Suppose Alice is sending classical information to Charlie over a single-user quantum channel, and they share the entangled state $\hat{\rho}_{AC}$. The capacity of superdense coding [13] is given by

$$C = \log d_A + S(\hat{\rho}_C) - S(\hat{\rho}_{AC}), \tag{3.41}$$

where $\hat{\rho}_C = \mathrm{tr}_A(\hat{\rho}_{AC})$. If $S(\hat{\rho}_C) - S(\hat{\rho}_{AC}) < 0$, then superdense coding with the state $\hat{\rho}_{AC}$ is detrimental because Alice is better off sending orthogonal qudits over the quantum channel to achieve the rate $\log d_A$. In particular, it can be shown that any separable state is useless for superdense coding [13]. The capacity of the single-user channel, allowing this alternative encoding, can be expressed in terms of coherent information [49] as

$$C = \log d_A + I^C(\hat{\rho}_{AC}), \tag{3.42}$$

where coherent information is defined as $I^C(\hat{\rho}_{AC}) = \max\{S(\hat{\rho}_C) - S(\hat{\rho}_{AC}), 0\}$.

The alternative code can be applied to the quantum MAC. If $S(\hat{\rho}_{BC}) - S(\hat{\rho}_0) < 0$, then Alice can increase her transmission rate to $\log d_A$ by deciding not to encode with her share of $\hat{\rho}_0$. This occurs, for example, when the initial state $\hat{\rho}_0$ is separable $A - BC$, i.e., $\hat{\rho}_0 = \sum_i p_i \hat{\rho}_i^A \otimes \hat{\rho}_i^{BC}$. When Alice transmits at rate $\log d_A$ and Bob uses superdense coding

with the reduced state $\hat{\rho}_{BC}$, the rate of their joint code is

$$(R_1, R_2) = (\log d_A, \log d_B + S(\hat{\rho}_C) - S(\hat{\rho}_{BC})). \tag{3.43}$$

Let us give an example in which Alice can increase her capacity with this alternative code. Let $\hat{\rho}_0$ be the initial state of three qubits,

$$\hat{\rho}_0 = \frac{1}{2}\hat{I}_A \otimes |00\rangle_{BC}\langle 00|, \tag{3.44}$$

with reduced densities

$$\hat{\rho}_{AC} = \frac{1}{2}\hat{I}_A \otimes |0\rangle_C\langle 0|, \tag{3.45}$$

$$\hat{\rho}_{BC} = |00\rangle_{BC}\langle 00|, \tag{3.46}$$

$$\hat{\rho}_C = |0\rangle_C\langle 0|. \tag{3.47}$$

Then, the capacity region of the superdense coding protocol is the set of rate pairs (R_1, R_2) that satisfy the inequalities (3.6)-(3.8):

$$R_1 \leq 0, \quad R_2 \leq 1, \quad \text{and} \quad R_1 + R_2 \leq 1. \tag{3.48}$$

In other words, the superdense coding capacity region is just the line segment from $(0, 0)$ to $(0, 1)$. If Alice instead sends orthogonal qubits, $|0\rangle_A$ and $|1\rangle_A$, while Bob uses superdense coding, then the rate pair $(1, 1)$ can be achieved. Figure 3-2 shows the capacity region for the alternative superdense coding protocol. We see that by allowing an alternative encoding, the capacity region of the superdense coding MAC can be strictly increased.

The GHZ systems studied in Chapter 2 generate three-party entangled states that can be used as resources for superdense coding. We compute the quantities:

$$S(\hat{\rho}_{BC}) - S(\hat{\rho}_0), \quad S(\hat{\rho}_{AC}) - S(\hat{\rho}_0), \quad \text{and} \quad S(\hat{\rho}_{AB}) - S(\hat{\rho}_0), \tag{3.49}$$

where $\hat{\rho}_0$ is the joint conditional density operator for either the dual-DPA or heralded-plus-DPA GHZ system derived in the single-photon error model. If we had, for example, $S(\hat{\rho}_{BC}) - S(\hat{\rho}_0) < 0$, then from Alice's point of view, the entangled state $\hat{\rho}_0$ is useless for

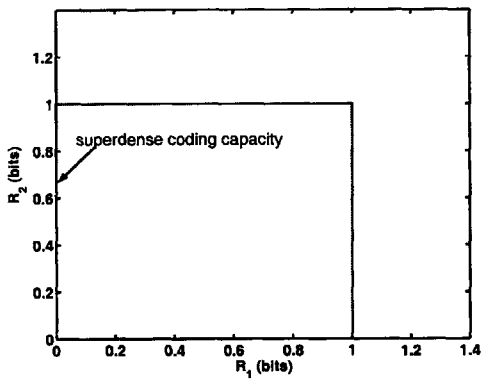


Figure 3-2: Superdense coding with initial state (3.44). Alice can increase her rate of transmission because $S(\hat{\rho}_{BC}) - S(\hat{\rho}_0) < 0$. In this example, the superdense coding capacity region consists of the line segment from (0,0) to (0,1). The rate pair (1,1) can be achieved if Alice sends orthogonal qubits and Bob uses superdense coding.

superdense coding. In Fig. 3-3, the quantities in (3.49), which we can think of as coherent informations, are computed for both the dual-DPA and heralded-plus-DPA GHZ systems. The coherent informations reach a positive limiting value at a path length around $L = 50$ km. This means that the three-party entangled states produced by the MIT/NU communication architecture are useful at all path lengths, in the sense that they can enhance the capacity region of noiseless quantum MACs through multiple-access superdense coding.

Figure 3-4 shows the capacity regions of the superdense coding MAC with the three-party entangled states produced by the dual-DPA and heralded-plus-DPA GHZ systems. We assume Alice and Bob are sending classical information to Charlie at a path length of $L = 25$ km. We see that the capacity region for the heralded system is larger than the capacity of the dual-DPA system. Superdense coding with the dual-DPA system can benefit both Alice's and Bob's transmission rates, which was implied by the positive coherent information computed in Fig. 3-3. However, for the dual-DPA system, there are some rate pairs that cannot be achieved with superdense coding that could be attained if both Alice and Bob discarded their share of the entangled state $\hat{\rho}_0$ and simply transmitted orthogonal qubits. In general, if the quantity $S(\hat{\rho}_C) - S(\hat{\rho}_0) < 0$, then the total transmission rate $R_1 + R_2$ can be improved if neither Alice nor Bob superdense code.

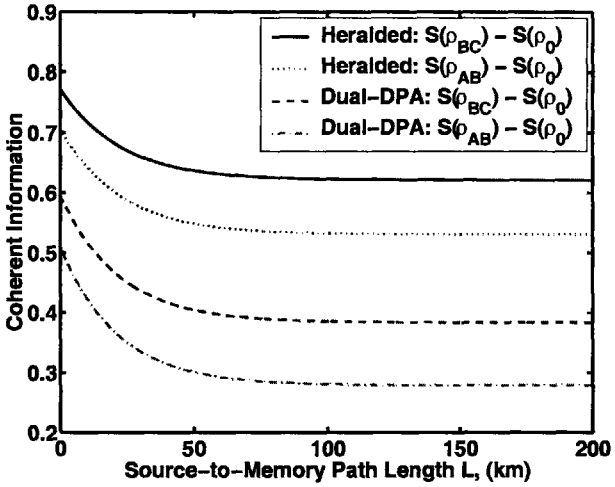


Figure 3-3: Coherent information for the dual-DPA and heralded-plus-DPA GHZ systems. For the dual-DPA system, we plot $S(\hat{\rho}_{BC}) - S(\hat{\rho}_0)$ and $S(\hat{\rho}_{AC}) - S(\hat{\rho}_0) = S(\hat{\rho}_{AB}) - S(\hat{\rho}_0)$. For the heralded system, we plot $S(\hat{\rho}_{AB}) - S(\hat{\rho}_0)$ and $S(\hat{\rho}_{AC}) - S(\hat{\rho}_0) = S(\hat{\rho}_{BC}) - S(\hat{\rho}_0)$.

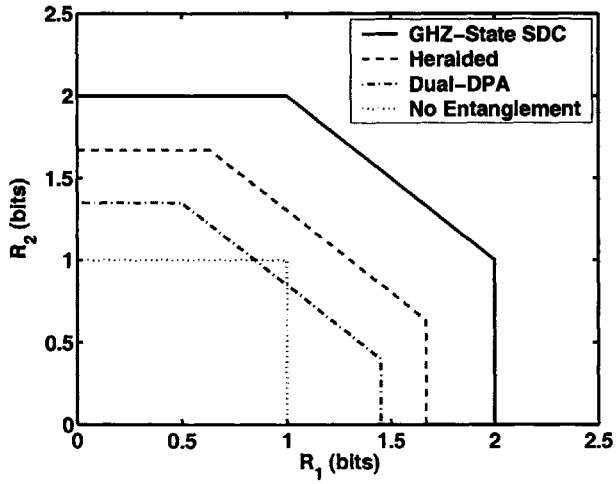


Figure 3-4: Capacity regions of superdense coding MAC with three-party entangled states produced by the dual-DPA and heralded-plus-DPA GHZ systems. For comparison, the capacities that can be achieved with no entanglement and with GHZ-state superdense coding are also shown.

3.2 Entanglement-Assisted MAC

The alternative encoding discussed in the previous section is an example of an entanglement-assisted MAC. For $i = 0, 1, \ldots, d_A - 1$, define the Kraus operators of Alice's channel $\mathcal{E}_i^A$ to be $\hat{E}_{i,k} = |i\rangle\langle k|$, so that

$$\mathcal{E}_i^A(\hat{\rho}) = \sum_{k=0}^{d_A-1} \hat{E}_{i,k}\hat{\rho}\hat{E}_{i,k}^\dagger = |i\rangle\langle i|. \tag{3.50}$$

Thus, the alternative encoding discussed above can be viewed as an example of a general encoding with local operations. In this section, we study the capacity region of the entanglement-assisted MAC with general local encodings.

3.2.1 Upper Bounds

Suppose Alice, Bob, and Charlie share the entangled state $\hat{\rho}_0$ in the Hilbert space $\mathcal{H}_{d_A} \otimes \mathcal{H}_{d_B} \otimes \mathcal{H}_{d_C}$. Alice and Bob encode independent classical messages by applying general local operators to their qudits and sending their qudits over noiseless quantum channels to Charlie, who then decodes the messages with a measurement on the combined system of the three qudits.

Suppose Alice and Bob utilize the local operators $\{\mathcal{E}_i^A\}$ and $\{\mathcal{E}_j^B\}$, respectively, with product distribution $p_i^A p_j^B$ to encode their messages. Denote the received states as

$$\hat{\rho}_{ij} = (\mathcal{E}_i^A \otimes \mathcal{E}_j^B \otimes I^C)(\hat{\rho}_0). \tag{3.51}$$

By subadditivity of von Neumann entropy, we can upper bound the right-hand side of (3.3)

as

$$H_A - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.52}$$

$$\leq \sum_j p_j^B \left[S\left(\mathrm{tr}_A \sum_i p_i^A \hat{\rho}_{ij} \right) + S\left(\mathrm{tr}_{BC} \sum_i p_i^A \hat{\rho}_{ij} \right) \right] - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.53}$$

$$\leq \log d_A + \sum_j p_j^B S\left(\mathrm{tr}_A \sum_i p_i^A \hat{\rho}_{ij} \right) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.54}$$

$$= \log d_A + \sum_j p_j^B S((\mathcal{E}_j^B \otimes I^C)(\hat{\rho}_{BC})) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.55}$$

$$= \log d_A + \sum_i \sum_j p_i^A p_j^B \left[S((\mathcal{E}_j^B \otimes I^C)(\hat{\rho}_{BC})) - S(\hat{\rho}_{ij}) \right] \tag{3.56}$$

$$\leq \log d_A + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S((\mathcal{E}^B \otimes I^C)(\hat{\rho}_{BC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right]. \tag{3.57}$$

Similarly, the right-hand side of (3.4) can be upper bounded as

$$H_B - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \leq \log d_B + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S((\mathcal{E}^A \otimes I^C)(\hat{\rho}_{AC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right]. \tag{3.58}$$

The right-hand side of (3.5) is upper bounded as

$$S(\hat{\rho}) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.59}$$

$$\leq S\left(\mathrm{tr}_C \sum_i \sum_j p_i^A p_j^B \hat{\rho}_{ij} \right) + S\left(\mathrm{tr}_{AB} \sum_i \sum_j p_i^A p_j^B \hat{\rho}_{ij} \right) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.60}$$

$$\leq \log d_A + \log d_B + S(\hat{\rho}_C) - \sum_i \sum_j p_i^A p_j^B S(\hat{\rho}_{ij}) \tag{3.61}$$

$$\leq \log d_A + \log d_B + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S(\hat{\rho}_C) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right]. \tag{3.62}$$

Summarizing, the rates for the entanglement-assisted quantum MAC are upper bounded as

$$R_1 \leq \log d_A + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S((\mathcal{E}^B \otimes I^C)(\hat{\rho}_{BC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right] \tag{3.63}$$

$$R_2 \leq \log d_B + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S((\mathcal{E}^A \otimes I^C)(\hat{\rho}_{BC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right] \tag{3.64}$$

$$R_1 + R_2 \leq \log d_A + \log d_B + \sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S(\hat{\rho}_C) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \right]. \tag{3.65}$$

3.2.2 Pure-State Entanglement

In this section, we prove the achievability of the rate upper bounds when $\hat{\rho}_0$ is a pure state. Let $\hat{\rho}_{AC}$, $\hat{\rho}_{BC}$, and $\hat{\rho}_C$ be the reduced densities of $\hat{\rho}_0 = |\psi_0\rangle\langle\psi_0|$. We need two facts involving the relative entropy of entanglement [50], defined as

$$E_{RE}(\hat{\sigma}_{AB}) = \min_{\hat{\rho}_{AB}} S(\hat{\sigma}_{AB} || \hat{\rho}_{AB}), \tag{3.66}$$

where the minimum is over all separable states $\hat{\rho}_{AB}$. First, let the state $\hat{\sigma}_{AB}$ have reduced densities $\hat{\sigma}_A$ and $\hat{\sigma}_B$. Then, the relative entropy of entanglement is lower bounded as

$$E_{RE}(\hat{\sigma}_{AB}) \geq \max\left\{S(\hat{\sigma}_A) - S(\hat{\sigma}_{AB}),\ S(\hat{\sigma}_B) - S(\hat{\sigma}_{AB})\right\}. \tag{3.67}$$

The second fact we need is that the relative entropy of entanglement is equal to the von Neumann reduced entropy for pure states [51], i.e., $E_{RE}(\hat{\sigma}_{AB}) = S(\hat{\sigma}_A) = S(\hat{\sigma}_B)$, if $\hat{\sigma}_{AB}$ is pure.

Using these facts, we have

$$\sup_{\mathcal{E}^A, \mathcal{E}^B} \left[S((\mathcal{E}^B \otimes I^C)(\hat{\rho}_{BC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0))\right] \tag{3.68}$$

$$\leq \sup_{\mathcal{E}^A, \mathcal{E}^B} E_{RE}^{A-BC}((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \tag{3.69}$$

$$\leq E_{RE}^{A-BC}(\hat{\rho}_0) \tag{3.70}$$

$$= S(\hat{\rho}_{BC}). \tag{3.71}$$

Line (3.70) follows because entanglement measures cannot increase under local operations.

The inequalities (3.63)-(3.65) can now be upper bounded as

$$R_1 \leq \log d_A + S(\hat{\rho}_{BC}) \tag{3.72}$$

$$R_2 \leq \log d_B + S(\hat{\rho}_{AC}) \tag{3.73}$$

$$R_1 + R_2 \leq \log d_A + \log d_B + S(\hat{\rho}_C). \tag{3.74}$$

These rates can be achieved with superdense coding. Thus, for a pure-state entanglement-assisted MAC, superdense coding is optimal.

3.2.3 Separable-States

Let the shared state initial state have the separable form,

$$\hat{\rho}_0 = \sum_i p_i |i\rangle_A\langle i| \otimes |i\rangle_B\langle i| \otimes |i\rangle_C\langle i|. \tag{3.75}$$

We use the relative entropy of entanglement upper bound again.

$$\sup_{\mathcal{E}^A,\mathcal{E}^B} \left[S((\mathcal{E}^B \otimes I^C)(\hat{\rho}_{BC})) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0))\right] \tag{3.76}$$

$$\leq \sup_{\mathcal{E}^A,\mathcal{E}^B} E_{RE}^{A-BC}((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \tag{3.77}$$

$$\leq E_{RE}^{A-BC}(\hat{\rho}_0) \tag{3.78}$$

$$= 0, \tag{3.79}$$

since the entanglement of a separable state must be zero. Also,

$$\sup_{\mathcal{E}^A,\mathcal{E}^B} \left[S(\hat{\rho}_C) - S((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0))\right] \tag{3.80}$$

$$\leq \sup_{\mathcal{E}^A,\mathcal{E}^B} E_{RE}^{AB-C}((\mathcal{E}^A \otimes \mathcal{E}^B \otimes I^C)(\hat{\rho}_0)) \tag{3.81}$$

$$\leq E_{RE}^{AB-C}(\hat{\rho}_0) \tag{3.82}$$

$$= 0. \tag{3.83}$$

Thus, the rate upper bounds are

$$R_1 \leq \log d_A \tag{3.84}$$

$$R_2 \leq \log d_B \tag{3.85}$$

$$R_1 + R_2 \leq \log d_A + \log d_B. \tag{3.86}$$

These bounds can be achieved by sending orthogonal qudits over the quantum channel. Thus, as should be expected, separable states are useless for enhancing the capacity region of a quantum MAC.

Chapter 4

Capacity of Gaussian Channels

We derive the classical capacity C for a class of Gaussian Bosonic channels, extending recent work [7],[25] that has yielded the capacity of pure-loss Bosonic channels as well as mathematical support for the capacity of the thermal-noise channel. After a review of Bosonic channels and known results, we consider the Gaussian-noise channel in Section 4.2. The Gaussian-noise channel represents the quantum version of a classical colored Gaussian-noise channel, so our approach is strongly motivated by the standard technique of whitening Gaussian noise used in classical information theory. Our derivations are based on a conjecture for the capacity of the thermal-noise channel [25]. In Section 4.3, we solve minimum output entropy problems that provide additional mathematical support for this conjecture.

4.1 Background: Bosonic Channels

In this section, we introduce the channel models that are studied in this chapter. We review known capacity results for the noiseless and pure-loss channels and discuss recent work on the thermal-noise channel capacity problem.

4.1.1 Channel Models

Consider the Gaussian Bosonic channel described by the Heisenberg evolution equation

$$\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{|1-\eta|}\hat{n} + \xi, \tag{4.1}$$

where $\hat{a}$ and $\hat{c}$ are the input and output annihilation operators, $\hat{n}$ is the noise operator, ξ is classical Gaussian noise, and η is a coupling coefficient. The noise operator is defined as

$$\hat{n} = \begin{cases} \hat{b} & \text{for } \eta < 1 \\ \hat{b}^\dagger & \text{for } \eta > 1, \end{cases} \tag{4.2}$$

where $\hat{b}$ is an annihilation operator in a zero-mean Gaussian state. We assume the classical noise ξ has a zero-mean, circularly symmetric Gaussian distribution. This channel model represents a broad class of channels containing special cases that are important in quantum optics. For example, if we set $\eta < 1$ and $\xi = 0$, then (4.1) is a lossy channel with transmissivity η. We will refer to the lossy channel with noise operator $\hat{b}$ in vacuum state as a pure-loss channel. For $\eta > 1$ and $\xi = 0$, we have an amplifying channel with gain η. Two closely related Gaussian Bosonic channels that will be particularly important in this chapter are the thermal-noise channel $\mathcal{E}_\eta^N$ and the classical-noise channel $\mathcal{N}_n$.

The thermal-noise channel $\mathcal{E}_\eta^N$ is the TPCP map obtained from tracing away the noise mode in the evolution given by $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$, where the noise mode $\hat{b}$ is in the thermal state

$$\hat{\rho}_T(N) = \frac{1}{N+1}\left(\frac{N}{N+1}\right)^{\hat{b}^\dagger \hat{b}} \tag{4.3}$$

with mean photon number N. The thermal-noise channel describes an input mode coupled to an environment in thermal equilibrium.

The classical-noise channel $\mathcal{N}_n$ is defined by the evolution equation $\hat{c} = \hat{a} + \xi$, which corresponds to setting $\eta = 1$ in (4.1). The TPCP map $\mathcal{N}_n$ is given by

$$\mathcal{N}_n(\hat{\rho}) = \int P_n(z)\hat{D}(z)\hat{\rho}\hat{D}^\dagger(z)dz, \tag{4.4}$$

where $P_n(z) = \exp(-|z|^2/n)/(\pi n)$ is a circularly symmetric Gaussian distribution and $\hat{D}(z) = \exp(z\hat{a}^\dagger - z^*\hat{a})$ is the displacement operator. The classical-noise channel is a unital map, i.e., it leaves the identity operator unaffected. It is also straightforward to check that coherent states are mapped to thermal states shifted in phase space, i.e.,

$$\mathcal{N}_n(|\alpha\rangle\langle\alpha|) = \hat{D}(\alpha)\hat{\rho}_T(n)\hat{D}^\dagger(\alpha), \tag{4.5}$$

where $\hat{\rho}_T(n)$ is a thermal state with mean photon number n.

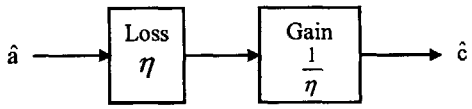


Figure 4-1: Representation of classical-noise channel $\mathcal{N}_n$ as a cascade of pure-loss and amplification channels. The noise modes are in vacuum state and $\eta = 1/(n+1)$.

To help better understand the classical-noise channel, we provide two alternative descriptions. First, $\mathcal{N}_n$ can be expressed as the limit of a thermal-noise channel. Through the use of quantum characteristic functions, it is possible to show that the thermal-noise channel $\mathcal{E}_\eta^{n/(1-\eta)}$ approaches the classical-noise channel $\mathcal{N}_n$ as $\eta \to 1$. The second representation of $\mathcal{N}_n$ is shown in Fig. 4-1. The noise modes associated with the attenuation and amplification processes are in vacuum state, and we set $\eta = 1/(n+1)$. The effects of loss and amplification cancel out, but the input mode still experiences additive classical noise.

The thermal-noise and classical-noise channels are related through the decomposition

$$\mathcal{E}_\eta^N = \mathcal{N}_{(1-\eta)N} \circ \mathcal{E}_\eta^0, \tag{4.6}$$

which says that the thermal-noise channel can be expressed as a pure-loss channel followed by a classical-noise channel. This decomposition allows results derived for the classical-noise channel to be directly applied to the thermal-noise channel. An extensive analysis of the relationship between the maps $\mathcal{E}_\eta^N$ and $\mathcal{N}_n$ is given in [25].

4.1.2 Noiseless Channel Capacity

States transmitted through a noiseless Bosonic channel are received undisturbed at the receiver. The classical capacity of the noiseless Bosonic channel was found in [2] and [3], where it was proved that a single-mode noiseless channel with average photon number constraint $\bar{n}$ has capacity

$$C = g(\bar{n}) \equiv (\bar{n}+1)\log(\bar{n}+1) - \bar{n}\log(\bar{n}), \tag{4.7}$$

in nats per use. Figure 4-2 shows a comparison of channel capacity with the rates achievable using input coherent states and conventional homodyne and heterodyne receivers [52]. The following is a list of encodings that achieve capacity on the single-mode noiseless channel:

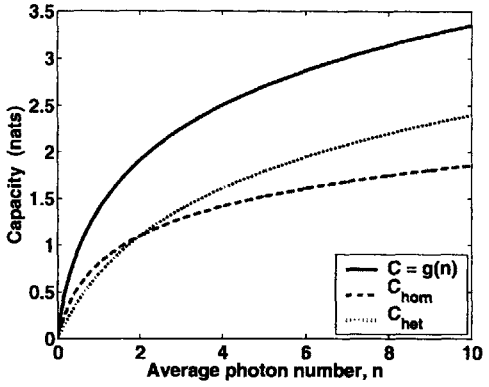


Figure 4-2: Capacity of a single-mode noiseless channel $C = g(\bar{n})$. For comparison, the communication rates with structured receivers are also plotted. Achievable rates with input coherent states and homodyne and heterodyne receivers are $C_{\text{hom}} = (1/2)\log(1+4\bar{n})$ and $C_{\text{het}} = \log(1+\bar{n})$, respectively.

1. Bose-Einstein distributed ensemble of number states with a photon-counting receiver; decoding errors *never* occur for distinct codewords,

2. Gaussian-distributed ensemble of coherent states with optimal entangled measurement [7],

3. Gaussian-distributed ensemble of coherent states with heterodyne detection, in the limit of large $\bar{n}$,

4. Gaussian-distributed ensemble of squeezed states with homodyne detection, in the limit of large $\bar{n}$; see Section 5.3 for a derivation.

For a noiseless wideband Bosonic channel with average power constraint P, the classical capacity is

$$C = \sqrt{\frac{\pi P}{3\hbar}}, \tag{4.8}$$

in nats per second. Random coding with number states and photon counting over independent frequency modes is optimal for the wideband channel, and the capacity-achieving power allocation requires transmitting with average photon number

$$\bar{n}(f) = \frac{1}{\exp(\pi h f/\sqrt{6hP}) - 1} \tag{4.9}$$

at frequency f.

4.1.3 Pure-Loss Channel Capacity

The results of the previous section were recently extended to the pure-loss channel $\mathcal{E}_\eta^0$ in [7], where it was shown that the classical capacity of the single-mode pure-loss channel is given by

$$C = g(\eta\bar{n}), \tag{4.10}$$

and that capacity can be achieved with a coherent-state encoding. Neither entanglement over successive channel uses nor nonclassical states, such as the number states, are required to achieve capacity for the pure-loss channel. The wideband capacity result (4.8) has a similar generalization. Although the optimal coherent-state encoding can be generated by classical sources of light, the proof of (4.10) makes use of a measurement that we do not know how to physically realize. See [8] for a study of communication rates achievable over the pure-loss channel using number-state and coherent-state encodings with structured receivers.

4.1.4 Thermal-Noise Channel Capacity

We review some recent work on the open problem of evaluating the capacity of the thermal-noise channel $\mathcal{E}_\eta^N$. Although a rigorous proof has yet to be found, we conjecture that the Holevo information of the thermal-noise channel is additive and that capacity is achievable with a coherent-state encoding. A lower bound on the capacity of the thermal-noise channel [53] is given by the single-use Holevo information with a Gaussian-distributed coherent-state code:

$$C \geq S\left(\mathcal{E}_\eta^N\left(\int \frac{e^{-|\alpha|^2/\bar{n}}}{\pi\bar{n}}|\alpha\rangle\langle\alpha|\,d\alpha\right)\right) - \int \frac{e^{-|\alpha|^2/\bar{n}}}{\pi\bar{n}} S\left(\mathcal{E}_\eta^N(|\alpha\rangle\langle\alpha|)\right) d\alpha \tag{4.11}$$

$$= g(\eta\bar{n} + (1-\eta)N) - g((1-\eta)N). \tag{4.12}$$

Next, we derive an upper bound for the thermal-noise channel capacity [54]. Let $\bar{\rho} = \sum_i p_i\hat{\rho}_i$ denote the average state of an input ensemble $\{p_i, \hat{\rho}_i\}$ subject to the mean photon number

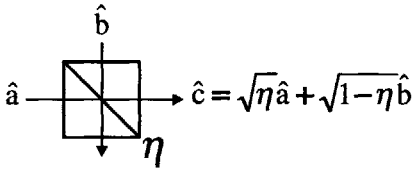


Figure 4-3: Gaussian-noise channel $\mathcal{E}$. The input mode and output modes are $\hat{a}$ and $\hat{c}$, respectively. The noise mode $\hat{b}$ is in a zero-mean Gaussian state $\hat{\rho}_b$ with variance matrix V_b.

constraint $\bar{n}$. Then, the normalized M-shot capacity is upper bounded as

$$\frac{C_M}{M} = \max_{p_i, \hat{\rho}_i} \frac{1}{M} \left[S\left((\mathcal{E}_\eta^N)^{\otimes M}(\bar{\rho}) \right) - \sum_i p_i S\left((\mathcal{E}_\eta^N)^{\otimes M}(\hat{\rho}_i) \right) \right] \tag{4.13}$$

$$\leq \max_{p_i, \hat{\rho}_i} \frac{S\left((\mathcal{E}_\eta^N)^{\otimes M}(\bar{\rho}) \right)}{M} - \min_{\hat{\rho}} \frac{S\left((\mathcal{E}_\eta^N)^{\otimes M}(\hat{\rho}) \right)}{M} \tag{4.14}$$

$$= g(\eta\bar{n} + (1-\eta)N) - \min_{\hat{\rho}} \frac{S\left((\mathcal{E}_\eta^N)^{\otimes M}(\hat{\rho}) \right)}{M}. \tag{4.15}$$

In (4.14), we separately maximized and minimized the two terms of the Holevo information. In (4.15), we used subadditivity of von Neumann entropy and upper bounded the first term by the capacity of a lossless channel with average input photon number $\eta\bar{n} + (1-\eta)N$ [55].

At this point, it is apparent that if the second term of (4.15) equals $g((1-\eta)N)$, then the upper and lower bounds coincide and thus equal the classical capacity C. This line of reasoning leads to the following minimum output entropy conjecture [25]:

$$\min_{\hat{\rho}} \frac{S\left((\mathcal{E}_\eta^N)^{\otimes M}(\hat{\rho}) \right)}{M} = g((1-\eta)N). \tag{4.16}$$

See [25] for numerous partial results obtained in the attempt to prove this conjecture. See also [8] for work on the strong (majorization) version of the conjecture. In Section 4.3, we solve related minimum output entropy problems that support conjecture (4.16).

4.2 Gaussian-Noise Channel

In this section, we assume the validity of conjecture (4.16) to derive the capacity of the Gaussian-noise channel. The Gaussian-noise channel model is shown in Fig. 4-3. Input mode $\hat{a}$ undergoes the Heisenberg evolution $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$, where the noise mode $\hat{b}$ is

in the zero-mean Gaussian state $\hat{\rho}_b$ with variance matrix

$$V_b = \begin{pmatrix} V_1^b & V_{12}^b \\ V_{12}^b & V_2^b \end{pmatrix}; \tag{4.17}$$

see Section 1.2.2 for background on Gaussian states, including the definition of a variance matrix. The Gaussian-noise channel is the TPCP map $\mathcal{E}$ obtained from tracing away the noise mode in this evolution. Assuming that conjecture (4.16) is true, i.e., the thermal-noise channel $\mathcal{E}_\eta^N$, with $V_b = (2N+1)I/4$, has capacity $C = g(\eta\bar{n} + (1-\eta)N) - g((1-\eta)N)$, we will prove the following capacity result.

Theorem 2 *The classical capacity of the Gaussian-noise channel $\mathcal{E}$ is given by*

$$C = g(\eta\bar{n} + (1-\eta)\bar{n}_b) - g\left((1-\eta)\left(2|V_b|^{1/2} - \frac{1}{2}\right)\right), \tag{4.18}$$

for input mean photon numbers $\bar{n} \geq \bar{n}_{\text{thresh}}$, where

$$\bar{n}_{\text{thresh}} = \frac{1}{\eta}\left((V_1' - V_2')^2 + 4V_{12}'^2\right)^{1/2} + V_1 + V_2 - \frac{1}{2}, \tag{4.19}$$

$$V' = \begin{pmatrix} V_1' & V_{12}' \\ V_{12}' & V_2' \end{pmatrix} = \eta V + (1-\eta)V_b, \tag{4.20}$$

$$V = \begin{pmatrix} V_1 & V_{12} \\ V_{12} & V_2 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} |\mu+\nu|^2 & 2\,\text{Im}(\mu\nu) \\ 2\,\text{Im}(\mu\nu) & |\mu-\nu|^2 \end{pmatrix}, \tag{4.21}$$

and the parameters μ and ν are chosen such that the squeeze operator $\hat{S}(z)$ whitens the Gaussian state $\hat{\rho}_b$ (see Section 1.2.2).

For sufficiently large input mean photon number $\bar{n}$, (4.18) gives the classical capacity of the Gaussian-noise channel. In Section 4.2.4, we study the capacity of the Gaussian-noise channel for $\bar{n}$ less than threshold $\bar{n}_{\text{thresh}}$.

To help motivate our proof of this result, we review the standard approach [56] for computing the capacity of a classical colored Gaussian-noise channel. In Fig. 4-4, the complex-valued column-vector input $\boldsymbol{x}$ has average power constraint $\text{tr}(C_{xx}) \leq P$, where $C_{xx} = \langle \boldsymbol{x}\boldsymbol{x}^\dagger \rangle$. The variance matrix of the noise vector is a positive semidefinite, Hermitian

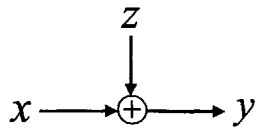


Figure 4-4: Classical colored Gaussian-noise channel. The complex-valued input vector $\boldsymbol{x}$ has variance matrix $C_{xx} = \langle \boldsymbol{x}\boldsymbol{x}^\dagger \rangle$ with average power constraint $\mathrm{tr}(C_{xx}) \leq P$. The complex-valued Gaussian noise vector $\boldsymbol{z}$ has variance matrix $C_{zz} = \langle \boldsymbol{z}\boldsymbol{z}^\dagger \rangle$.

matrix, so it can be diagonalized by a unitary matrix U as

$$C_{zz} = U \Lambda U^\dagger \tag{4.22}$$

$$\Lambda = \mathrm{diag}\begin{pmatrix} \lambda_1 & \cdots & \lambda_m \end{pmatrix}. \tag{4.23}$$

The receiver whitens the additive Gaussian noise $\boldsymbol{z}$ by passing the received vector $\boldsymbol{y}$ through the filter $U^\dagger$. The resulting output is then equivalent to a channel consisting of a set of independent additive white Gaussian-noise channels with variances equal to the eigenvalues λ_k, $k = 1, \ldots, m$. The optimal power allocation to each component of this channel is given by the water-filling solution.

The classical proof does not directly apply in the quantum case due to non-commuting operators, so we will present the quantum version of whitening additive colored Gaussian noise to derive the capacity of the Gaussian-noise channel $\mathcal{E}$. A capacity upper bound is derived by converting the Gaussian-noise channel to an equivalent thermal-noise channel, which in the quantum case plays the role of an additive white Gaussian-noise channel. For input powers above a given threshold, we obtain the capacity of the Gaussian-noise channel by presenting a code that achieves the capacity upper bound.

4.2.1 Capacity Upper Bound

We begin the derivation of the capacity upper bound by separately maximizing and minimizing the two terms of the Holevo information. Let $\bar{n}_b = V_1^b + V_2^b - 1/2$ denote the mean photon number of the Gaussian noise state $\hat{\rho}_b$. Then, from the derivation given in lines (4.13)-(4.15), which is still valid because $\hat{\rho}_b$ is zero-mean, we have

$$\frac{C_M}{M} \leq g(\eta\bar{n} + (1-\eta)\bar{n}_b) - \min_{\hat{\rho}} \frac{S\left(\mathcal{E}^{\otimes M}(\hat{\rho})\right)}{M}. \tag{4.24}$$

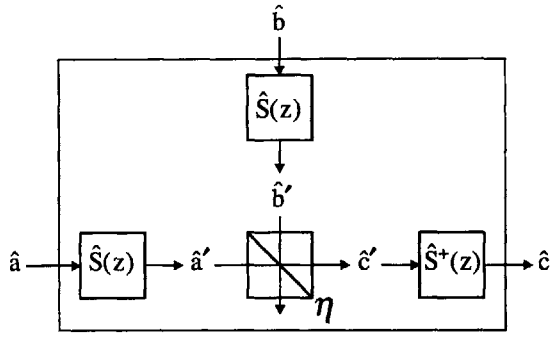


Figure 4-5: Equivalent thermal-noise channel $\mathcal{E}_\eta^{\bar{n}_T}$ from $\hat{a}'$ to $\hat{c}'$. The input mode $\hat{a}'$ is in state $\hat{\rho}'$, and the noise operator $\hat{b}'$ is in a thermal state with mean photon number $\bar{n}_T = 2|V_b|^{1/2} - 1/2$. The original Gaussian-noise channel takes input $\hat{a}$ to output $\hat{c}$.

We compute the minimum output entropy of the Gaussian-noise channel by converting it into the equivalent thermal-noise channel shown in Fig. 4-5. This process whitens the variance matrix V_b of the Gaussian noise state. Let $\mathcal{E}(\hat{\rho})$ be the original Gaussian-noise channel from input $\hat{a}$ to output $\hat{c}$, and let $\mathcal{E}_\eta^{\bar{n}_T}(\hat{\rho}')$ be the internal thermal-noise channel from $\hat{a}'$ to $\hat{c}'$. The unitary squeeze operator $\hat{S}(z)$ is described in Section 1.2.2. Its complex z-parameter is chosen such that noise operator $\hat{b}'$ is in a thermal state with mean photon number $\bar{n}_T = 2|V_b|^{1/2} - 1/2$.

The minimum output entropy is achieved over pure input states $\hat{\rho} = |\psi\rangle\langle\psi|$, so we have

$$\min_{\hat{\rho}} \frac{S\left(\mathcal{E}^{\otimes M}(\hat{\rho})\right)}{M} = \min_{\hat{\rho}} \frac{S\left((\hat{S}^\dagger(z))^{\otimes M}(\mathcal{E}_\eta^{\bar{n}_T})^{\otimes M}(\hat{\rho}')\hat{S}^{\otimes M}(z)\right)}{M} \tag{4.25}$$

$$= \min_{\hat{\rho}} \frac{S((\mathcal{E}_\eta^{\bar{n}_T})^{\otimes M}(\hat{\rho}'))}{M} \tag{4.26}$$

$$= \min_{\hat{\rho}'} \frac{S((\mathcal{E}_\eta^{\bar{n}_T})^{\otimes M}(\hat{\rho}'))}{M} \tag{4.27}$$

$$= g((1-\eta)\bar{n}_T) \tag{4.28}$$

$$= g\left((1-\eta)\left(2|V_b|^{1/2} - \frac{1}{2}\right)\right). \tag{4.29}$$

Lines (4.26) and (4.27) follow because $\hat{S}(z)$ is unitary, and the final result assumes the validity of conjecture (4.16). Thus, putting this together with (4.24), the capacity of the

Gaussian-noise channel is upper bounded as

$$C \leq g(\eta\bar{n} + (1-\eta)\bar{n}_b) - g\left((1-\eta)\left(2|V_b|^{1/2} - \frac{1}{2}\right)\right). \tag{4.30}$$

Under the assumption of conjecture (4.16), the minimum output entropy of the thermal-noise channel is achieved by the vacuum state; hence, the corresponding state of the input $\hat{a}$ in Fig. 4-5 is the squeezed vacuum state $|\psi\rangle = \hat{S}^\dagger(z)|0\rangle = |0, -z\rangle$. The variance matrix

$$V = \frac{1}{4}\begin{pmatrix} |\mu+\nu|^2 & 2\,\mathrm{Im}(\mu\nu) \\ 2\,\mathrm{Im}(\mu\nu) & |\mu-\nu|^2 \end{pmatrix} \tag{4.31}$$

of this squeezed state is proportional to the noise variance V_b; see Eq. (1.34). In this sense, the optimal input state is the pure Gaussian state that most closely matches the noise state $\hat{\rho}_b$.

4.2.2 Capacity Lower Bound

We obtain a lower bound for C from a squeezed-state encoding. To compute the rate of this squeezed-state code, we apply a capacity result derived in [57].

Holevo-Sohma-Hirota capacity result

In the Holevo-Sohma-Hirota (HSH) channel model [57], complex-valued messages α are encoded into the quantum states $\hat{\rho}(\alpha) = \hat{D}(\alpha)\hat{\rho}(0)\hat{D}^\dagger(\alpha)$, where $\hat{\rho}(0)$ is zero-mean Gaussian with variance matrix

$$V = \begin{pmatrix} V_1 & V_{12} \\ V_{12} & V_2 \end{pmatrix}. \tag{4.32}$$

The received state $\hat{\rho}(\alpha)$ is simply the initial state $\hat{\rho}(0)$ shifted in phase space. Let the variance matrix of the input distribution $P(\alpha)$ be

$$V_\alpha = \begin{pmatrix} V_1^\alpha & V_{12}^\alpha \\ V_{12}^\alpha & V_2^\alpha \end{pmatrix}. \tag{4.33}$$

In [57], it was shown that under the input constraint

$$\langle |\alpha|^2 \rangle = \int P(\alpha)|\alpha|^2 d\alpha = N, \tag{4.34}$$

the optimal input distribution $P(\alpha)$ is Gaussian, and the capacity of this channel is given by one of two different expressions depending on the input constraint N.

- If $N \geq ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2}$, then the capacity of the Holevo-Sohma-Hirota channel is

$$C_{\text{HSH}}(V, N) = g\left(V_1 + V_2 + N - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right). \tag{4.35}$$

- If $N < ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2}$, then

$$C_{\text{HSH}}(V, N) = g\left(2\left(\left(\frac{V_1 + V_2 + N}{2}\right)^2 - \left(\sqrt{\left(\frac{V_1 - V_2}{2}\right)^2 + V_{12}^2} - \frac{N}{2}\right)^2\right)^{1/2} - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right). \tag{4.36}$$

Our main interest is in the above-threshold result (4.35). For further discussion of the HSH capacity result, see Section 5.2.1.

Squeezed-state code

Define a Gaussian-distributed squeezed-state code over the Gaussian-noise channel $\mathcal{E}$. Let $\hat{\rho}_A(0) = |0, -z\rangle_A\langle 0, -z|$ be the zero-mean squeezed state with variance matrix V given by (4.31). The transmitted codewords

$$\hat{\rho}_A(\alpha) = \hat{D}(\alpha)\hat{\rho}_A(0)\hat{D}^\dagger(\alpha), \tag{4.37}$$

are shifted versions of the initial state $\hat{\rho}_A(0)$, and the input distribution $P(\alpha)$ is zero-mean Gaussian with variance matrix V_α. With this encoding, the channel output states can be written as

$$\mathcal{E}(\hat{\rho}_A(\alpha)) = \hat{D}(\sqrt{\eta}\alpha)\mathcal{E}(\hat{\rho}_A(0))\hat{D}^\dagger(\sqrt{\eta}\alpha), \tag{4.38}$$

where $\mathcal{E}(\hat{\rho}_A(0))$ is a zero-mean Gaussian state with variance $\eta V+(1-\eta)V_b$. If the transmitter is required to satisfy the mean photon number constraint

$$\mathrm{tr}\left(\hat{a}^\dagger\hat{a}\int P(\alpha)\hat{\rho}_A(\alpha)d\alpha\right) = V_1^\alpha + V_2^\alpha + V_1 + V_2 - \frac{1}{2} = \bar{n}, \tag{4.39}$$

then we can directly apply the Holevo-Sohma-Hirota capacity result to compute the rate of this code. Let

$$V' = \eta V + (1-\eta)V_b, \tag{4.40}$$

$$N' = \eta\left(\bar{n} - V_1 - V_2 + \frac{1}{2}\right). \tag{4.41}$$

In the above-threshold regime, $\bar{n} \geq \bar{n}_{\mathrm{thresh}}$, where

$$\bar{n}_{\mathrm{thresh}} = \frac{1}{\eta}\left((V_1' - V_2')^2 + 4V_{12}'^2\right)^{1/2} + V_1 + V_2 - \frac{1}{2}, \tag{4.42}$$

the capacity of the squeezed state code is

$$\begin{aligned}
C &= C_{\mathrm{HSH}}(V', N') && (4.43)\\
&= g\left(V_1' + V_2' + N' - \frac{1}{2}\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right) && (4.44)\\
&= g\left(\eta(V_1+V_2) + (1-\eta)(V_1^b + V_2^b) + \eta\left(\bar{n} - V_1 - V_2 + \frac{1}{2}\right) - \frac{1}{2}\right)\\
&\quad - g\left(2|V'|^{1/2} - \frac{1}{2}\right) && (4.45)\\
&= g\left(\eta\bar{n} + (1-\eta)\left(V_1^b + V_2^b - \frac{1}{2}\right)\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right) && (4.46)\\
&= g\left(\eta\bar{n} + (1-\eta)\bar{n}_b\right) - g\left((1-\eta)\left(2|V_b|^{1/2} - \frac{1}{2}\right)\right). && (4.47)
\end{aligned}$$

The last line follows from the fact that the squeezed state $|0,-z\rangle$ achieves the minimum output entropy (4.29). This code achieves the upper bound (4.30), thus the capacity of the Gaussian-noise channel is

$$C = g(\eta\bar{n} + (1-\eta)\bar{n}_b) - g\left((1-\eta)\left(2|V_b|^{1/2} - \frac{1}{2}\right)\right), \tag{4.48}$$

for all $\bar{n} \geq \bar{n}_{\mathrm{thresh}}$. This concludes the proof of Theorem 2.

For the thermal-noise channel $\mathcal{E}_\eta^N$, we can check that $\bar{n}_{\text{thresh}} = 0$ and that the capacity-achieving input distribution $P(\alpha)$ is circularly symmetric Gaussian. Thus, this result is consistent with our thermal-noise capacity conjecture. Let us now consider the more interesting special case of pure-state Gaussian noise $\hat{\rho}_b = |0,z\rangle\langle 0,z|$. In this case, we have

$$V' = V = V_b = \frac{1}{4}\begin{pmatrix} |\mu-\nu|^2 & -2\,\text{Im}(\mu\nu) \\ -2\,\text{Im}(\mu\nu) & |\mu+\nu|^2 \end{pmatrix}, \tag{4.49}$$

$$N' = \eta(\bar{n} - |\nu|^2), \tag{4.50}$$

and

$$\bar{n}_{\text{thresh}} = \frac{1}{\eta}\left((V_1' - V_2')^2 + 4V_{12}'^2\right)^{1/2} + V_1 + V_2 - \frac{1}{2} \tag{4.51}$$

$$= \frac{1}{\eta}\left(\left(\frac{|\mu-\nu|^2 - |\mu+\nu|^2}{4}\right)^2 + \text{Im}(\mu\nu)^2\right)^{1/2} + |\nu|^2 \tag{4.52}$$

$$= \frac{|\mu\nu|}{\eta} + |\nu|^2. \tag{4.53}$$

Thus, squeezed-noise channels have capacity

$$C = g(\eta\bar{n} + (1-\eta)|\nu|^2), \tag{4.54}$$

for $\bar{n} \geq \bar{n}_{\text{thresh}} = |\mu\nu|/\eta + |\nu|^2$. Note that this capacity is higher than the pure-loss capacity $g(\eta\bar{n})$ for the same transmissivity. Thus, phase-sensitive pure-state Gaussian noise enhances, rather than degrades channel capacity. The optimal input distribution $P(\alpha)$ is zero-mean Gaussian with variance matrix

$$V_\alpha = \frac{1}{2}\begin{pmatrix} \bar{n} - |\nu|^2 + \dfrac{\text{Re}(\mu\nu)}{\eta} & \dfrac{\text{Im}(\mu\nu)}{\eta} \\ \dfrac{\text{Im}(\mu\nu)}{\eta} & \bar{n} - |\nu|^2 - \dfrac{\text{Re}(\mu\nu)}{\eta} \end{pmatrix}. \tag{4.55}$$

When the input photon number constraint is above-threshold, the transmitter has sufficient energy to use the capacity-achieving squeezed-state code with its corresponding pure-state output ensemble. See Section 4.2.4 for squeezed-noise capacity in the below-threshold case.

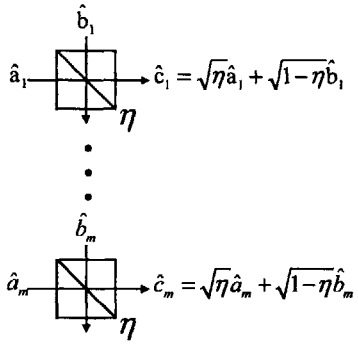


Figure 4-6: Multimode Gaussian-noise channel Λ. The noise operator $\hat{\boldsymbol{b}} = (\hat{b}_1, \ldots, \hat{b}_m)^T$ is in the zero-mean Gaussian state $\hat{\rho}_b$.

4.2.3 Multimode Gaussian-Noise Channel

We take a similar approach to study the capacity of the multimode Gaussian-noise channel, shown in Fig. 4-6. Denote the signal modes as $\hat{\boldsymbol{a}} = (\hat{a}_1, \ldots, \hat{a}_m)^T$, the noise modes as $\hat{\boldsymbol{b}} = (\hat{b}_1, \ldots, \hat{b}_m)^T$, and the output modes as $\hat{\boldsymbol{c}} = (\hat{c}_1, \ldots, \hat{c}_m)^T$. If we assume equal transmission factors, the multimode channel can be expressed as $\hat{\boldsymbol{c}} = \sqrt{\eta}\hat{\boldsymbol{a}} + \sqrt{1-\eta}\hat{\boldsymbol{b}}$. The noise operator $\hat{\boldsymbol{b}}$ is in a zero-mean Gaussian state $\hat{\rho}_b$ with mean photon number $\bar{n}_{b,k} = \mathrm{tr}(\hat{b}_k^\dagger \hat{b}_k \hat{\rho}_b)$ in the kth mode, $k = 1, \ldots, m$.

The capacity of the multimode Gaussian-noise channel Λ is the maximum Holevo information over input ensembles $\{p_i, \hat{\rho}_i\}$ that satisfy the input energy constraint

$$\mathrm{tr}\left(\sum_{k=1}^{m} \hbar\omega_k \hat{a}_k^\dagger \hat{a}_k \bar{\rho}\right) \leq E, \tag{4.56}$$

where $\bar{\rho} = \sum_i p_i \hat{\rho}_i$ is the average input state. Let $\{q_i, \hat{\sigma}_i\}$, with average state $\bar{\sigma} = \sum_i q_i \hat{\sigma}$, be the capacity-achieving ensemble for the product channel $\Lambda^{\otimes M}$. We then have the capacity

upper bound

$$\frac{C_M}{M} = \frac{1}{M}\left[S(\Lambda^{\otimes M}(\bar{\sigma})) - \sum_i q_i S(\Lambda^{\otimes M}(\hat{\sigma}_i))\right] \tag{4.57}$$

$$\leq \frac{S(\Lambda^{\otimes M}(\bar{\sigma}))}{M} - \min_{\hat{\rho}} \frac{S(\Lambda^{\otimes M}(\hat{\rho}))}{M} \tag{4.58}$$

$$\leq \frac{1}{M}\sum_{k=1}^{m}\sum_{l=1}^{M} S(\Lambda_{kl}(\bar{\sigma})) - \min_{\hat{\rho}} \frac{S(\Lambda^{\otimes M}(\hat{\rho}))}{M} \tag{4.59}$$

$$\leq \frac{1}{M}\sum_{k=1}^{m}\sum_{l=1}^{M} g(\eta\bar{n}'_{kl} + (1-\eta)\bar{n}_{b,k}) - \min_{\hat{\rho}} \frac{S(\Lambda^{\otimes M}(\hat{\rho}))}{M} \tag{4.60}$$

$$\leq \max_{\{\bar{n}_k\}} \sum_{k=1}^{m} g(\eta\bar{n}_k + (1-\eta)\bar{n}_{b,k}) - \min_{\hat{\rho}} \frac{S(\Lambda^{\otimes M}(\hat{\rho}))}{M}. \tag{4.61}$$

In line (4.59), we used subadditivity of entropy to upper bound the first term and wrote $\Lambda_{kl}(\bar{\sigma})$ to denote the reduced output state of the kth mode and lth channel use. In line (4.60), $\bar{n}'_{kl}$ is the input mean photon number of the kth mode and lth channel use. The optimal power allocation in the last line is given by the water-filling solution,

$$\bar{n}_k = \left(\frac{1}{\eta(e^{\lambda\hbar\omega_k/\eta} - 1)} - \frac{(1-\eta)\bar{n}_{b,k}}{\eta}\right)^+, \tag{4.62}$$

where $(x)^+ \equiv \max(x, 0)$, and the parameter λ is chosen to satisfy the energy constraint $\sum_{k=1}^{m} \hbar\omega_k \bar{n}_k = E$.

The second term in (4.61) is the minimum output entropy of the multimode Gaussian-noise channel. We compute this term by converting the channel into an equivalent thermal-noise channel, shown in Fig. 4-7. The unitary transformation $\hat{U}$ takes the noise state $\hat{\rho}_b$ into a product of thermal states [57]:

$$\hat{U}\hat{\rho}_b\hat{U}^\dagger = \hat{\rho}_T(N_1) \otimes \cdots \otimes \hat{\rho}_T(N_m). \tag{4.63}$$

For any Gaussian state $\hat{\rho}_b$, there is a unitary operator $\hat{U}$ with this property; see Appendix A. Let $\Lambda(\hat{\rho})$ be the multimode Gaussian-noise channel from input $\hat{\boldsymbol{a}}$ to output $\hat{\boldsymbol{c}}$, and let $\Lambda'(\hat{\rho}')$ be the internal thermal-noise channel from $\hat{\boldsymbol{a}}'$ to $\hat{\boldsymbol{c}}'$, as shown in Fig. 4-7. The minimum

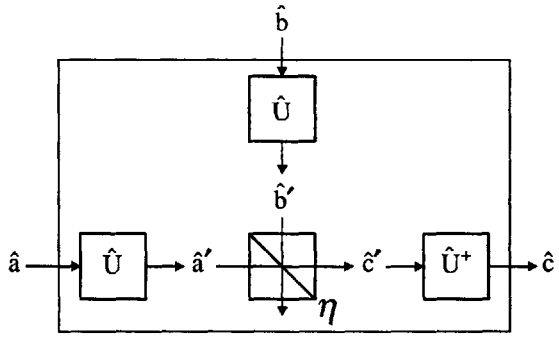


Figure 4-7: Equivalent thermal-noise channel for the multimode Gaussian-noise channel. The noise operator $\hat{b}'$ is in the product thermal state $\hat{\rho}_T(N_1) \otimes \cdots \otimes \hat{\rho}_T(N_m)$.

output entropy is achieved over pure input states $\hat{\rho} = |\psi\rangle\langle\psi|$, so we have

$$\min_{\hat{\rho}} \frac{S\left(\Lambda^{\otimes M}(\hat{\rho})\right)}{M} = \min_{\hat{\rho}} \frac{S\left((\hat{U}^\dagger)^{\otimes M}(\Lambda')^{\otimes M}(\hat{\rho}')\hat{U}^{\otimes M}\right)}{M} \tag{4.64}$$

$$= \min_{\hat{\rho}} \frac{S((\Lambda')^{\otimes M}(\hat{\rho}'))}{M} \tag{4.65}$$

$$= \min_{\hat{\rho}'} \frac{S((\Lambda')^{\otimes M}(\hat{\rho}'))}{M} \tag{4.66}$$

$$= \sum_{k=1}^{m} g((1-\eta)N_k). \tag{4.67}$$

In (4.67), we assumed that the minimum output entropy of m independent thermal-noise channels is achieved with the input vacuum state $\hat{\rho} = |\mathbf{0}\rangle\langle\mathbf{0}|$.

Putting these results together, we have the following upper bound for the capacity of the multimode Gaussian-noise channel:

$$C \leq \sum_{k=1}^{m} \left[g(\eta\bar{n}_k + (1-\eta)\bar{n}_{b,k}) - g((1-\eta)N_k)\right], \tag{4.68}$$

where the power allocation $\{\bar{n}_k\}$ is given by (4.62). We can show that in some cases, we can find an encoding that achieves the capacity upper bound (4.68).

Parallel thermal-noise channels

Suppose we have a multimode channel consisting of a set of m independent single-mode thermal-noise channels $\mathcal{E}_\eta^{N_k}$, $k = 1, \ldots, m$. The capacity upper bound (4.68) for this multi-

mode thermal-noise channel is

$$C \leq \sum_{k=1}^{m} C(\bar{n}_k, N_k), \tag{4.69}$$

where $C(\bar{n}, N) = g(\eta\bar{n} + (1-\eta)N) - g((1-\eta)N)$ is the capacity of the single-mode thermal-noise channel. By coding independently over each mode with the optimal power allocation, this upper bound can be achieved . Thus, the right-hand side of (4.69) is the capacity of the multimode thermal-noise channel under our minimum output entropy conjecture.

Gauge-invariant Gaussian-noise channel

A multimode gauge-invariant Gaussian state [57] is defined to be a state of the form

$$\hat{\rho} = \int \frac{1}{\pi^m |N|} \exp(-\boldsymbol{\alpha}^\dagger N^{-1} \boldsymbol{\alpha}) |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \, d\boldsymbol{\alpha}, \tag{4.70}$$

where $|\boldsymbol{\alpha}\rangle$ are the coherent states in $\mathcal{H}^{\otimes m}$. For the case $m = 1$, $\hat{\rho}$ is a thermal state. Let the noise state $\hat{\rho}_b$ of the multimode Gaussian-noise channel in Fig. 4-6 be the gauge-invariant Gaussian state with P-representation

$$P_b(\boldsymbol{\beta}) = \frac{1}{\pi^m |N_b|} \exp(-\boldsymbol{\beta}^\dagger N_b^{-1} \boldsymbol{\beta}). \tag{4.71}$$

States that possess a P-representation in the form of a probability distribution are classical mixtures of coherent states and hence are considered "classical states". The classical nature of the noise in a gauge-invariant Gaussian-noise channel allows us to use the simpler whitening procedure from classical information theory.

The variance matrix N_b is a positive semidefinite, Hermitian matrix, so it can be diagonalized as $N_b = U\Lambda U^\dagger$, where $UU^\dagger = I$ and $\Lambda = \mathrm{diag}[\lambda_1 \ \ldots \ \lambda_m]$ with $\lambda_k \geq 0$, $k = 1, \ldots, m$. We convert the gauge-invariant Gaussian-noise channel into an equivalent thermal-noise channel by applying the unitary transformation $U^\dagger$ to the channel output:

$$\hat{\boldsymbol{c}}' = U^\dagger \hat{\boldsymbol{c}} \tag{4.72}$$

$$= U^\dagger (\sqrt{\eta}\hat{\boldsymbol{a}} + \sqrt{1-\eta}\hat{\boldsymbol{b}}) \tag{4.73}$$

$$= \sqrt{\eta}\hat{\boldsymbol{a}}' + \sqrt{1-\eta}\hat{\boldsymbol{b}}'. \tag{4.74}$$

The P-representation of the noise state changes by the same unitary transformation, $\beta' =$

$U^\dagger\beta$, so the transformed noise mode $\hat{\boldsymbol{b}}$ is in the tensor product of thermal states, $\hat{\rho}_T(\lambda_1) \otimes \cdots \otimes \hat{\rho}_T(\lambda_m)$. Applying the result of the previous section, the capacity of the gauge-invariant Gaussian-noise channel is

$$C = \sum_{k=1}^{m} C(\bar{n}_k, \lambda_k), \tag{4.75}$$

where $\{\bar{n}_k\}$ is the optimal power allocation (4.62).

4.2.4 Below-Threshold Capacity

We derived the capacity of the single-mode Gaussian-noise channel $\mathcal{E}$ for mean photon numbers $\bar{n}$ above a certain threshold $\bar{n}_{\text{thresh}}$. In this section, we consider the problem of transmitting classical information over the Gaussian-noise channel in the below-threshold regime.

To study this problem, we will consider the Gaussian-noise channel with its noise operator $\hat{b}$ in a squeezed vacuum state $|0, z\rangle$. For input mean photon numbers $\bar{n} \geq \bar{n}_{\text{thresh}} = |\mu\nu|/\eta + |\nu|^2$, the capacity of this channel is

$$C_{\text{upperbd}} = g(\eta\bar{n} + (1-\eta)|\nu|^2). \tag{4.76}$$

Below threshold, C_{upperbd} is only an upper bound on capacity. Figure 4-8 shows capacity upper bound C_{upperbd} for a squeezed-noise channel with squeeze parameters $(\mu, \nu) = (\sqrt{11}, \sqrt{10})$ and the rates of various encodings explained below.

In Fig. 4-8, C_{sq} is the rate of the squeezed-state code, described on page 84, that achieves above-threshold capacity for the squeezed-noise channel. The input squeezed states $|\alpha, z\rangle$ in this encoding have the same squeeze parameter z as the noise state $\hat{\rho}_b$, thus making the corresponding channel outputs $\mathcal{E}(|\alpha, z\rangle\langle\alpha, z|)$ pure squeezed states. For input mean photon numbers $\bar{n} < 10$, the transmitter cannot use this encoding for the simple reason that it lacks the power to produce these squeezed states. For $10 \leq \bar{n} < \bar{n}_{\text{thresh}}$, the transmitter can squeeze hard enough to generate this encoding, but cannot use it to achieve upper bound C_{upperbd}. In this low-power regime, the transmitter makes a rough trade-off, represented by the two terms of Holevo information, between purifying the channel output and modulating the input to convey information. For $\bar{n} \geq \bar{n}_{\text{thresh}}$, where threshold $\bar{n}_{\text{thresh}} \approx 114.88$ in our example, the squeezed-state code achieves capacity.

Intuitively, one might believe that putting the noise operator $\hat{b}$ in vacuum state would

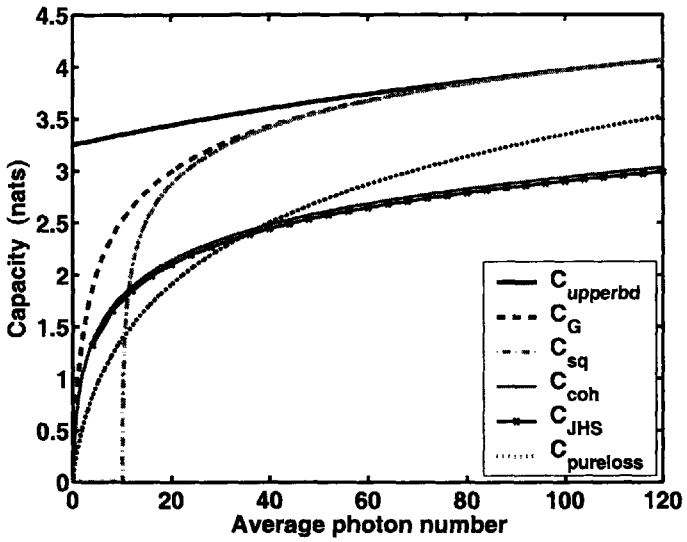


Figure 4-8: Squeezed-noise channel. The transmissivity is $\eta = 0.1$, and the noise operator is in the pure squeezed state $|0, z\rangle$ with $(\mu, \nu) = (\sqrt{11}, \sqrt{10})$ The threshold is $\bar{n}_{\text{thresh}} \approx 114.88$. $C_{\text{upperbd}} = g(\eta\bar{n} + (1-\eta)\nu^2)$ is capacity upper bound (4.76) derived in Section 4.2.1. C_G is the capacity achieved by Gaussian codes. C_{sq} is squeezed-state code capacity with squeeze parameters $(\mu, \nu) = (\sqrt{11}, \sqrt{10})$. C_{coh} is coherent-state capacity with optimal measurement. C_{JHS} is coherent-state with homodyne detection capacity (4.77). $C_{\text{pureloss}} = g(\eta\bar{n})$ is the capacity of the pure-loss channel $\mathcal{E}_\eta^0$.

result in the highest-capacity channel. As an easy way to demonstrate that this is in fact not true, one can verify that a squeezed-state code with a homodyne receiver over the squeezed-noise channel $\mathcal{E}$ achieves a rate higher than the capacity of the pure-loss channel $\mathcal{E}_\eta^0$ at low input mean photon numbers. More specifically, if the transmitter encodes information in the low-noise quadrature using coherent states $|\alpha_1\rangle$, $\alpha_1 \in \mathbb{R}$, then the rate

$$C_{\text{JHS}} = \frac{1}{2}\log\left(1 + \frac{4\bar{n}}{1 + \frac{1-\eta}{\eta}(\mu - \nu)^2}\right). \tag{4.77}$$

is achieved by using homodyne detection to measure the first quadrature of the channel output. In our example, C_{JHS} is greater than the capacity of the pure-loss channel $\mathcal{E}_\eta^0$ for $\bar{n} < 34.49$. This effect is similar to the improvement in SNR achieved with squeezed states in an optical waveguide tap [58]. Optimizing over all codes, Fig. 4-8 shows that the capacity of the squeezed-noise channel $\mathcal{E}$ is greater than the capacity of the pure-loss channel $\mathcal{E}_\eta^0$, for all $\bar{n}$.

In Fig. 4-8, we also plot the capacity C_{coh} that is achievable with input coherent states

optimized over receiver measurements. For $\bar{n} \geq \bar{n}_{\text{thresh}}$,

$$C_{\text{coh}} = g(\eta\bar{n} + (1-\eta)\nu^2) - g\left(\frac{1}{2}\left[(\eta + (1-\eta)(\mu-\nu)^2)(\eta + (1-\eta)(\mu+\nu)^2)\right]^{1/2} - \frac{1}{2}\right), \tag{4.78}$$

and a more complicated expression can be given for $0 \leq \bar{n} < \bar{n}_{\text{thresh}}$. Figure 4-8 shows that $C_{JHS} \approx C_{\text{coh}}$, so, in our example, homodyne detection provides a near-optimal measurement when the transmitter sends coherent states.

All of the codes we have considered so far are examples of Gaussian codes based on the Holevo-Sohma-Hirota model. For each value of $\bar{n}$, the optimal Gaussian code is found by searching over all possible input variances V. For the transmitter to have sufficient power to transmit a given code, the inequality $\bar{n} \geq V_1 + V_2 - 1/2$ must be satisfied. If this condition is satisfied, then the capacity of the Gaussian code is

$$C(\bar{n}, V) = \begin{cases} g\left(\eta\bar{n} + (1-\eta)\bar{n}_b\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } \bar{n} \geq \bar{n}_{\text{thresh}}(V) \\ g\left(2\left(\left(\frac{V_1'+V_2'+N'}{2}\right)^2 - \left(\sqrt{\left(\frac{V_1'-V_2'}{2}\right)^2 + V_{12}'^2} - \frac{N'}{2}\right)^2\right)^{1/2} - \frac{1}{2}\right) \\ \quad -g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } \bar{n} < \bar{n}_{\text{thresh}}(V), \end{cases} \tag{4.79}$$

where

$$\bar{n}_{\text{thresh}}(V) = \frac{1}{\eta}\left((V_1' - V_2')^2 + 4V_{12}'^2\right)^{1/2} + V_1 + V_2 - \frac{1}{2}, \tag{4.80}$$

$$V' = \eta V + (1-\eta)V_b. \tag{4.81}$$

We numerically computed

$$C_G(\bar{n}) = \max_V C(\bar{n}, V), \tag{4.82}$$

subject to the constraints

$$V_1 + V_2 - \frac{1}{2} \leq \bar{n} \tag{4.83}$$

$$V_1, V_2 \geq 0 \tag{4.84}$$

$$V_1 V_2 - V_{12}^2 \geq \frac{1}{16}. \tag{4.85}$$

The capacity C_G achieved using Gaussian codes is shown in Fig. 4-8. This is the best achievable rate we have for the below-threshold regime, but we have no reason to believe that it is capacity-achieving or even that below-threshold capacity can be analytically derived.

4.3 Minimum Output Entropy

The results of the previous section were based on the conjectured capacity of the thermal-noise channel $\mathcal{E}_\eta^N$. To prove this conjecture, it is sufficient to show that input coherent states minimize the output von Neumann entropy of the thermal-noise channel. A main reason for the difficulty in proving (4.16) is the intractability of the logarithm function in the definition of von Neumann entropy $S(\hat{\rho}) = -\mathrm{tr}(\hat{\rho}\log\hat{\rho})$. In this section, we outline an approach to solving this problem involving Rényi entropy [59] and discuss its connection with the replica method. We also show that coherent states minimize an additional entropy quantity known as Wehrl entropy. Although the results derived in this section do not prove (4.16), they lend additional mathematical support to our conjecture, demonstrating that coherent states produce the purest channel output as measured by all integer-order Rényi entropies ($r \geq 2$) as well as the channel output most localized in phase space as measured by Wehrl entropy.

4.3.1 Rényi Entropy

The Rényi entropies are a family of entropy functions defined as

$$S_r(\hat{\rho}) = -\frac{1}{r-1}\log\mathrm{tr}(\hat{\rho}^r), \tag{4.86}$$

where $r > 0$ is the order of the Rényi entropy. For fixed $\hat{\rho}$, Rényi entropy is continuous in r, and L'Hôpital's rule shows that von Neumann entropy is obtained in the limit $r \to 1$.

The main motivation for considering Rényi entropy is to avoid the logarithm function in the definition of von Neumann entropy, replacing it with a function that is easier to analyze. If we could show that output Rényi entropy is minimized by input coherent states for all $r > 1$, then our conjecture would follow by continuity. We consider a single use ($M = 1$) of the classical-noise channel $\mathcal{N}_n$, and what we want to show is that

$$\min_{\hat{\rho}} S_r(\mathcal{N}_n(\hat{\rho})) = \frac{\log[(n+1)^r - n^r]}{r-1} \tag{4.87}$$

holds for real $r > 1$. We have instead proved the weaker result that (4.87) is true for integer orders $r = 2, 3, 4, \ldots$. Note that the case $r = 2$ was solved in [60] in the context of maximizing the fidelity of continuous-variable teleportation.

Theorem 3 *The minimum output Rényi entropy of the classical-noise channel $\mathcal{N}_n$ is achieved by input coherent states, i.e.,*

$$\min_{\hat{\rho}} S_r(\mathcal{N}_n(\hat{\rho})) = \frac{\log[(n+1)^r - n^r]}{r-1}, \tag{4.88}$$

for integer orders $r = 2, 3, 4, \ldots$.

Proof Minimizing Rényi entropy $S_r(\mathcal{N}_n(\hat{\rho}))$ is equivalent to maximizing the r-purity $\mathrm{tr}((\mathcal{N}_n(\hat{\rho}))^r)$, and by concavity of Rényi entropy, we know that the minimum (4.88) is achieved on pure input states $\hat{\rho} = |\psi\rangle\langle\psi|$ Thus, we write

$$\mathrm{tr}((\mathcal{N}_n(\hat{\rho}))^r) = \mathrm{tr} \int P_n(z_1) \hat{D}(z_1) \hat{\rho} \hat{D}^\dagger(z_1)\, dz_1 \cdots \int P_n(z_r) \hat{D}(z_r) \hat{\rho} \hat{D}^\dagger(z_r)\, dz_r \tag{4.89}$$

$$= \int P_n(z_1) \cdots P_n(z_r)\, \mathrm{tr}(\hat{D}(z_1) \hat{\rho} \hat{D}^\dagger(z_1) \cdots \hat{D}(z_r) \hat{\rho} \hat{D}^\dagger(z_r))\, dz_1 \cdots dz_r \tag{4.90}$$

$$= \int P_n(z_1) \cdots P_n(z_r)\, \langle\psi|\hat{D}^\dagger(z_1)\hat{D}(z_2)|\psi\rangle \cdots \langle\psi|\hat{D}^\dagger(z_r)\hat{D}(z_1)|\psi\rangle\, dz_1 \cdots dz_r \tag{4.91}$$

$$= \int P_n(z_1) \cdots P_n(z_r) \exp\left(\frac{-z_1 z_2^* + z_1^* z_2}{2} + \cdots + \frac{-z_r z_1^* + z_r^* z_1}{2} \right) \chi_W^\rho(z_2 - z_1) \cdots \chi_W^\rho(z_1 - z_r)\, dz_1 \cdots dz_r. \tag{4.92}$$

We let $\chi_W^\rho(z) = \langle\psi|\hat{D}(z)|\psi\rangle$ denote the symmetrically-ordered characteristic function of the input state $\hat{\rho}$. Express each of the characteristic functions in (4.92) in terms of the Wigner

function $W(\alpha)$ through the Fourier transform relation

$$\chi_W^{\rho}(z) = \int W(\alpha) e^{z\alpha^* - z^*\alpha} d\alpha. \tag{4.93}$$

This gives us

$$\mathrm{tr}((\mathcal{N}_n(\hat{\rho}))^r) = \int W(\alpha_1) \cdots W(\alpha_r)\, g(\boldsymbol{\alpha})\, d\boldsymbol{\alpha}, \tag{4.94}$$

where the inner Gaussian integral is

$$g(\boldsymbol{\alpha}) = \frac{1}{(\pi n)^r} \int \exp\left(-\boldsymbol{z}^\dagger A \boldsymbol{z} + \boldsymbol{z}^\dagger B \boldsymbol{\alpha} - \boldsymbol{\alpha}^\dagger B^\dagger \boldsymbol{z}\right) d\boldsymbol{z}, \tag{4.95}$$

and we have defined the vectors $\boldsymbol{z} = (z_1, \ldots, z_r)^T$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r)^T$, and the matrices

$$A = \begin{bmatrix} 1/n & -1/2 & 0 & \cdots & 0 & 1/2 \\ 1/2 & 1/n & -1/2 & \cdots & 0 & 0 \\ 0 & 1/2 & 1/n & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & 1/2 & 1/n & -1/2 \\ -1/2 & 0 & 0 & 0 & 1/2 & 1/n \end{bmatrix} \tag{4.96}$$

$$B = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -1 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}. \tag{4.97}$$

A and B are both circulant matrices, so they can be diagonalized as

$$A = F^\dagger \Lambda_A F \tag{4.98}$$

$$B = F^\dagger \Lambda_B F \tag{4.99}$$

$$\Lambda_A = \mathrm{diag}\left(\lambda_1^A \quad \cdots \quad \lambda_r^A\right) \tag{4.100}$$

$$\Lambda_B = \mathrm{diag}\left(\lambda_1^B \quad \cdots \quad \lambda_r^B\right) \tag{4.101}$$

by the unitary Fourier matrix

$$F = \frac{1}{\sqrt{r}}[\omega^{-ij}] = \frac{1}{\sqrt{r}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(r-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{-(r-1)} & \omega^{-2(r-1)} & \cdots & \omega^{-(r-1)(r-1)} \end{bmatrix}, \tag{4.102}$$

where $\omega = \exp(2\pi i/r)$ is an r-th root of unity. The eigenvalues of A and B are

$$\lambda_k^A = \frac{1}{n} - i\,\mathrm{Im}(\omega^{k-1}), \quad \text{for } k = 1, \ldots, r, \tag{4.103}$$

and

$$\lambda_k^B = 1 - \omega^{-k+1}, \quad \text{for } k = 1, \ldots, r. \tag{4.104}$$

Rotating by the Fourier matrix F with the change of variables

$$\boldsymbol{\beta} = F\boldsymbol{\alpha} \tag{4.105}$$

$$\boldsymbol{y} = F\boldsymbol{z}, \tag{4.106}$$

the Gaussian integral is

$$g(\boldsymbol{\alpha}) = \frac{1}{(\pi n)^r} \int \exp\left(-\boldsymbol{z}^\dagger A \boldsymbol{z} + \boldsymbol{z}^\dagger B \boldsymbol{\alpha} - \boldsymbol{\alpha}^\dagger B^\dagger \boldsymbol{z}\right) d\boldsymbol{z} \tag{4.107}$$

$$= \frac{1}{(\pi n)^r} \int \exp\left(-\boldsymbol{y}^\dagger \Lambda_A \boldsymbol{y} + \boldsymbol{y}^\dagger \Lambda_B \boldsymbol{\beta} - \boldsymbol{\beta}^\dagger \Lambda_B^\dagger \boldsymbol{y}\right) d\boldsymbol{y} \tag{4.108}$$

$$= \frac{1}{(\pi n)^r} \prod_{k=1}^{r} \int \exp\left(-\lambda_k^A |y_k|^2 + y_k^* \lambda_k^B \beta_k - \beta_k^* \lambda_k^{B*} y_k\right) dy_k \tag{4.109}$$

$$= \frac{1}{n^r} \prod_{k=1}^{r} \frac{1}{\lambda_k^A} \exp\left(-\frac{|\lambda_k^B|^2 |\beta_k|^2}{\lambda_k^A}\right) \tag{4.110}$$

$$= \frac{1}{n^r \det A} \exp\left(-\sum_{k=1}^{r} \frac{|\lambda_k^B|^2 |\beta_k|^2}{\lambda_k^A}\right). \tag{4.111}$$

Thus, the output r-purity is

$$\mathrm{tr}((\mathcal{N}_n(\hat{\rho}))^r) = \int W(\alpha_1)\cdots W(\alpha_r)\, g(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} \tag{4.112}$$

$$= \frac{1}{n^r \det A} \int W_b(\boldsymbol{\beta}) \exp\left(-\sum_{k=1}^{r} \frac{|\lambda_k^B|^2 |\beta_k|^2}{\lambda_k^A} \right) d\boldsymbol{\beta} \tag{4.113}$$

$$= \frac{1}{n^r \det A} \left\langle \exp\left(-\sum_{k=1}^{r} \frac{|\lambda_k^B|^2 |\beta_k|^2}{\lambda_k^A} \right) \right\rangle_{W_b(\boldsymbol{\beta})} . \tag{4.114}$$

As discussed in Appendix B, this means that the output r-purity can be expressed as the expectation of a thermal operator $\hat{G}$ acting on an extended Hilbert space $\mathcal{H}^{\otimes r}$. On this extended Hilbert space, the annihilation operators $\hat{\boldsymbol{a}} = (\hat{a}_1, \ldots, \hat{a}_r)^T$ are in the product input state $\hat{\rho}^{\otimes r}$ with Wigner function $W_a(\boldsymbol{\alpha}) = W(\alpha_1)\cdots W(\alpha_r)$. The annihilation operators $\hat{\boldsymbol{b}} = (\hat{b}_1, \ldots, \hat{b}_r)^T$, which are related to $\hat{\boldsymbol{a}}$ through a rotation by the Fourier matrix

$$\hat{\boldsymbol{b}} = F\hat{\boldsymbol{a}}, \tag{4.115}$$

are in the state with Wigner function $W_b(\boldsymbol{\beta}) = W_a(F^\dagger \boldsymbol{\beta})$.

We upper bound the output r-purity by the maximum absolute value of the eigenvalues of $\hat{G}$. From (B.18),

$$\mathrm{tr}((\mathcal{N}_n(\hat{\rho}))^r) = \langle \hat{G} \rangle \leq \left| \prod_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \right| , \tag{4.116}$$

which is achieved by the eigenvalue of $\hat{G}$ associated with the product vacuum state $|0\rangle^{\otimes r}$ of the annihilation operators $\hat{b}_k$. But since the sets of annihilation operators $\hat{\boldsymbol{a}}$ and $\hat{\boldsymbol{b}}$ are related through a unitary transformation, this means that the output r-purity is maximized by the input vacuum state $\hat{\rho} = |0\rangle\langle 0|$. Thus, we have proved (4.88), which says that output Rényi entropy of the classical-noise channel $\mathcal{N}_n$ is minimized by input coherent states for integer orders $r \geq 2$. ∎

For completeness, we can evaluate the right-hand side of (4.116) to show that it does give us the right-hand side of (4.87). From (4.103) and (4.104),

$$\prod_{k=1}^{r}\left(\lambda_k^A+\frac{|\lambda_k^B|^2}{2}\right)=\prod_{k=0}^{r-1}\left(\frac{1}{n}-i\,\mathrm{Im}(\omega^k)+\frac{|1-\omega^{-k}|^2}{2}\right) \tag{4.117}$$

$$=\prod_{k=0}^{r-1}\left(\frac{1}{n}-i\,\mathrm{Im}(\omega^k)+1-\mathrm{Re}(\omega^k)\right) \tag{4.118}$$

$$=\prod_{k=0}^{r-1}\left(\frac{1+n}{n}-\omega^k\right) \tag{4.119}$$

$$=\left(\frac{1+n}{n}\right)^r-1. \tag{4.120}$$

Thus, (4.116) reduces to

$$\prod_{k=1}^{r}\frac{2/n}{2\lambda_k^A+|\lambda_k^B|^2}=\frac{1}{n^r\prod_{k=1}^{r}\left(\lambda_k^A+\frac{|\lambda_k^B|^2}{2}\right)}=\frac{1}{(n+1)^r-n^r}. \tag{4.121}$$

Finally, using decomposition (4.6), the output Rényi entropy of the thermal-noise channel is lower bounded as

$$\min_{\hat{\rho}} S_r(\mathcal{E}_\eta^N(\hat{\rho}))=\min_{\hat{\rho}} S_r((\mathcal{N}_{(1-\eta)N}\circ\mathcal{E}_\eta^0)(\hat{\rho})) \tag{4.122}$$

$$\geq \min_{\hat{\rho}} S_r(\mathcal{N}_{(1-\eta)N}(\hat{\rho})) \tag{4.123}$$

$$=\frac{\log[((1-\eta)N+1)^r-((1-\eta)N)^r]}{r-1}. \tag{4.124}$$

Input coherent states achieve this lower bound, so (4.124) is the minimum output Rényi entropy of the thermal-noise channel for integer orders $r\geq 2$.

Recently, the same approach was used to extend the above proof to multiple channel uses in [61], where it was shown that the minimum integer-order output Rényi entropy of the classical-noise channel is additive. In another related result, [62] shows that the minimum output Rényi entropy of a general class of Gaussian channels, including our classical-noise channel as a special case, is additive for all $r\in(1,\infty)$ when the inputs are restricted to be Gaussian states.

4.3.2 Replica Method

The replica method was developed in statistical mechanics for evaluating free energy densities in situations for which an explicit calculation is not possible. The major obstacle in the free energy calculation is the expectation of a logarithm, $E[\log Z]$, where Z is called the partition function. Recently, replica-method analyses have started to appear in classical-communication problems, e.g., [63], [64]. The typical such approach proceeds as follows.

1. Use the identity

$$\log A = \lim_{m \to 0} \frac{dA^m}{dm} \tag{4.125}$$

and assume that expectation and limit can be interchanged, so that

$$E[\log Z] = E\left[\lim_{m \to 0} \frac{dZ^m}{dm}\right] \tag{4.126}$$

$$= \lim_{m \to 0} \frac{1}{E[Z^m]} \frac{dE[Z^m]}{dm} \tag{4.127}$$

$$= \lim_{m \to 0} \frac{d \log E[Z^m]}{dm}. \tag{4.128}$$

2. Assume that free energy is self-averaging. Let K be a size parameter for the given problem. Then, our assumption is that free energy converges to its expectation for large K.

$$\mathcal{F} = \lim_{K \to \infty} \frac{1}{K} E[\log Z] \tag{4.129}$$

$$= \lim_{K \to \infty} \lim_{m \to 0} \frac{d \log E[Z^m]}{dm} \tag{4.130}$$

$$= \lim_{m \to 0} \frac{d}{dm} \lim_{K \to \infty} \frac{1}{K} \log E[Z^m] \tag{4.131}$$

3. Evaluate $(1/K) \log E[Z^m]$ for integer values of m using the saddle-point method or large deviation theory to asymptotically compute an integral.

4. Assume analytic continuity for the function $\lim_{K \to \infty} (1/K) \log E[Z^m]$. Take derivative and let $m \to 0$.

Although the replica method lacks a rigorous mathematical justification, it is an accepted procedure in the field of spin glasses, for which the method was originally developed [65].

Furthermore, the replica method has been successfully applied to problems in communication and information processing; see references in [63].

In the replica method analysis, identity (4.125) is introduced to avoid taking the expectation of a logarithm. In our minimum output entropy analysis, we considered the parameterized family of Rényi entropies for the same reason. If we shift the order parameter in the definition of Rényi entropy by setting $s = r - 1$, then the fact that Shannon entropy $H(X) \equiv -E[\log p(X)]$ reduces to Rényi entropy of order $r = 1$ can be expressed as

$$H(X) = -\lim_{s \to 0} \frac{\log E[p(X)^s]}{s}, \tag{4.132}$$

whereas the replica method approach (4.128) gives us

$$H(X) = -\lim_{s \to 0} \frac{d \log E[p(X)^s]}{ds}. \tag{4.133}$$

An application of L'Hôpital's rule to (4.132) demonstrates the equivalence of these two expressions.

One way to get a connection with the replica method is to define the minimum entropy functions

$$S_r^*(\mathcal{N}_n(\hat{\rho})) = \min_{\hat{\rho}} S_r(\mathcal{N}_n(\hat{\rho})) \tag{4.134}$$

$$S^*(\mathcal{N}_n(\hat{\rho})) = \min_{\hat{\rho}} S(\mathcal{N}_n(\hat{\rho})). \tag{4.135}$$

Then, an application of the replica method to our minimum output entropy problem can be summarized as follows.

1. Assume it is valid to interchange minimization and limit, so that

$$S^*(\mathcal{N}_n(\hat{\rho})) = \min_{\hat{\rho}} \lim_{r \to 1} S_r(\mathcal{N}_n(\hat{\rho})) \tag{4.136}$$

$$= \lim_{r \to 1} \min_{\hat{\rho}} S_r(\mathcal{N}_n(\hat{\rho})) \tag{4.137}$$

$$= \lim_{r \to 1} S_r^*(\mathcal{N}_n(\hat{\rho})) \tag{4.138}$$

2. Evaluate the function $S_r^*(\mathcal{N}_n(\hat{\rho}))$ at integer values $r = 2, 3, 4, \ldots$.

3. Assume analytic continuity for the function $S_r^*(\mathcal{N}_n(\hat{\rho}))$ and take the limit $r \to 1$.

In the typical replica method analysis, the evaluation of the function at integer values of m requires a self-averaging assumption and an asymptotic calculation in the size parameter K. In our analysis, the dimension of the noise Hilbert space serves as an infinite size parameter, and we have rigorously derived the minimum output Rényi entropies for integer values of $r \geq 2$. This connection with the replica method provides us with additional support for our minimum entropy conjecture (4.16).

4.3.3 Wehrl Entropy

The Wehrl entropy of a density operator $\hat{\rho}$ is the Shannon entropy of its Husimi Q-function,

$$S_W(\hat{\rho}) = -\int \langle\alpha|\hat{\rho}|\alpha\rangle \log\langle\alpha|\hat{\rho}|\alpha\rangle \frac{d\alpha}{\pi} \tag{4.139}$$

$$= -\int Q(\alpha) \log(\pi Q(\alpha))\, d\alpha, \tag{4.140}$$

where $Q(\alpha) \equiv \langle\alpha|\hat{\rho}|\alpha\rangle/\pi$ is the Q-function. This entropy quantity is a measure of the localization of a state in phase space. The statistics of ideal heterodyne detection, which provides a physical realization of a two-quadrature field measurement, are characterized by the probability density $Q(\alpha)$ [66]. The fact that the Q-function cannot be precisely localized in phase space is due to the Heisenberg uncertainty principle, which prevents both quadratures from simultaneously having zero variance. Wehrl conjectured [67] and Lieb proved [68] that coherent states minimize Wehrl entropy, i.e.,

$$\min_{\hat{\rho}} S_W(\hat{\rho}) = 1. \tag{4.141}$$

In this section, we prove the following result.

Theorem 4 *The minimum output Wehrl entropy of the classical-noise channel $\mathcal{N}_n$ is achieved by input coherent states, i.e.,*

$$\min_{\hat{\rho}} S_W(\mathcal{N}_n(\hat{\rho})) = 1 + \log(n+1). \tag{4.142}$$

Proof The addition of classical noise to the input mode multiplies the anti-normally ordered characteristic function by the factor $e^{-n|\zeta|^2}$. Taking inverse Fourier transforms, the Q-

function at the output of the classical-noise channel is the convolution

$$Q'(\alpha) = (Q * P_n)(\alpha) = \int Q(\beta) P_n(\alpha - \beta)\, d\beta. \tag{4.143}$$

For an input coherent state $\hat{\rho} = |\alpha_0\rangle\langle\alpha_0|$, the output Q-function is

$$Q'(\alpha) = \frac{e^{-|\alpha-\alpha_0|^2}}{\pi} * \frac{e^{-|\alpha|^2/n}}{\pi n} = \frac{\exp\left[-\frac{|\alpha-\alpha_0|^2}{n+1}\right]}{\pi(n+1)}, \tag{4.144}$$

so the output Wehrl entropy corresponding to an input coherent state is given by

$$S_W(\mathcal{N}_n(|\alpha_0\rangle\langle\alpha_0|)) = h(Q'(\alpha)) - \log\pi \tag{4.145}$$

$$= \log(\pi e(1+n)) - \log\pi \tag{4.146}$$

$$= 1 + \log(1+n), \tag{4.147}$$

where $h(f) \equiv -\int f(x)\log f(x)\, dx$ is the differential Shannon entropy. Thus, the output Wehrl entropy produced by a coherent-state input is independent of the input mean amplitude α_0. We claim that this is the minimum output Wehrl entropy.

To lower bound the output Wehrl entropy, we apply the entropy power inequality [68], [56]. Let f and g be two-dimensional probability distributions. The entropy power inequality provides a lower bound on the entropy of a convolution, and the form of the inequality we will use is [68]

$$h(f * g) \geq \lambda h(f) + (1-\lambda)h(g) - \lambda\log\lambda - (1-\lambda)\log(1-\lambda), \tag{4.148}$$

valid for all $0 \leq \lambda \leq 1$. Applying the entropy power inequality to the classical-noise channel

gives us the lower bound

$$S_W(\mathcal{N}_n(\hat{\rho})) = h(Q * P_n) - \log \pi \tag{4.149}$$

$$\geq \lambda h(Q) + (1-\lambda)h(P_n) - \lambda \log \lambda - (1-\lambda)\log(1-\lambda) - \log \pi \tag{4.150}$$

$$\geq \lambda(1 + \log \pi) + (1-\lambda)\log(\pi e n) - \lambda \log \lambda - (1-\lambda)\log(1-\lambda) - \log \pi \tag{4.151}$$

$$= 1 + (1-\lambda)\log n - \lambda \log \lambda - (1-\lambda)\log(1-\lambda) \tag{4.152}$$

$$\geq 1 + \log(n+1), \tag{4.153}$$

where we applied (4.141) in (4.151) and set $\lambda = 1/(1+n)$ to obtain the final result. Thus, input coherent states achieve the minimum output Wehrl entropy. ∎

These arguments also apply to the thermal-noise channel $\mathcal{E}_\eta^N$ and show that output Wehrl entropy is minimized by input coherent states:

$$\min_{\hat{\rho}} S_W(\mathcal{E}_\eta^N(\hat{\rho})) = 1 + \log[(1-\eta)N + 1]. \tag{4.154}$$

Chapter 5

Capacity of the Optical MAC

In Chapter 3, we studied the capacity region of the quantum MAC with prior shared entanglement. In this chapter, we continue our study of the quantum MAC by generalizing our classical-capacity analysis for the single-user Bosonic channel to the optical MAC. In contrast to the channels we studied in Chapter 3, the optical MAC is a continuous-variable, noisy Bosonic channel without shared entanglement. In Section 5.1, we define our channel model and derive the maximum rates for reliably transmitting classical information over the optical MAC when the transmitters are restricted to classical states. In Section 5.2, we generalize the Gaussian encodings from Chapter 4 to achieve higher rates over the optical MAC. We derive an outer bound for the ultimate capacity region of the optical MAC in Section 5.3 and show that the sum-rate upper bound is achievable with a coherent-state encoding. We also show that the ultimate capacity region can be asymptotically achieved in the limit of large input mean photon numbers.

5.1 Coherent-State MAC

We consider the optical MAC, shown in Fig. 5-1, in which two senders, Alice and Bob, transmit classical information to a common receiver Charlie, and each sender has access to one input port of a beam splitter with transmissivity $0 \leq \eta \leq 1$. For a single mode of the optical MAC, the output is given by $\hat{c} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{b}$, where $\hat{a}$ and $\hat{b}$ are the annihilation operators of Alice's and Bob's input modes, and $\hat{c}$ is the annihilation operator of the mode that Charlie measures. In this section, we derive the capacity of the optical MAC when Alice and Bob encode complex-valued input messages α and β as coherent states $|\alpha\rangle_A \otimes |\beta\rangle_B$

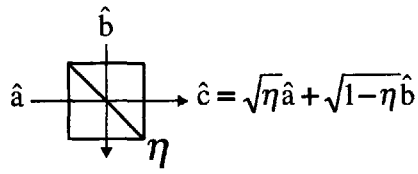


Figure 5-1: Optical multiple access channel. Transmitters Alice and Bob have access to input modes $\hat{a}$ and $\hat{b}$, respectively. Charlie receives the output mode $\hat{c} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{b}$.

with independent input distributions $p_A(\alpha)$ and $p_B(\beta)$. The corresponding received output state is the coherent state $|\sqrt{\eta}\alpha + \sqrt{1-\eta}\beta\rangle_C$, so we will refer to this system as the (single-mode) coherent-state MAC. As in Chapter 3, we will only consider the one-shot (M=1) classical capacity of the optical MAC.

5.1.1 Coherent-State MAC Capacity

We first consider the capacity region of the coherent-state MAC when Charlie uses homodyne or heterodyne detection. With these receiver measurements, the coherent-state MAC is equivalent to a corresponding classical additive Gaussian noise MAC. The capacity region of the scalar Gaussian channel corresponding to homodyne reception is the set of rate pairs (R_1, R_2) that satisfy [56]

$$R_1 \leq \frac{1}{2}\log(1 + 4\eta\bar{n}_A) \tag{5.1}$$

$$R_2 \leq \frac{1}{2}\log(1 + 4(1-\eta)\bar{n}_B) \tag{5.2}$$

$$R_1 + R_2 \leq \frac{1}{2}\log(1 + 4\eta\bar{n}_A + 4(1-\eta)\bar{n}_B), \tag{5.3}$$

and the capacity region of the vector Gaussian channel corresponding to heterodyne reception is given by

$$R_1 \leq \log(1 + \eta\bar{n}_A) \tag{5.4}$$

$$R_2 \leq \log(1 + (1-\eta)\bar{n}_B) \tag{5.5}$$

$$R_1 + R_2 \leq \log(1 + \eta\bar{n}_A + (1-\eta)\bar{n}_B). \tag{5.6}$$

It is possible to generalize these results to the m-user optical MAC. If the ith transmitter sends coherent state $|\alpha_i\rangle$, for $i = 1, \ldots, m$, then the output of the m-user optical MAC is the

coherent state $|\sum_{i=1}^{m}\sqrt{\eta_i}\alpha_i\rangle$, where the transmissivity factors η_i sum to one. The capacity region with homodyne detection is the set of rates $(R_1,\ldots,R_m)$ that satisfy the inequalities

$$\sum_{i\in S} R_i \leq \frac{1}{2}\log\left(1+4\sum_{i\in S}\eta_i\bar{n}_i\right), \tag{5.7}$$

for all subsets $S\subseteq\{1,\ldots,m\}$, where $\bar{n}_i$ is the input constraint for the ith user. The capacity region with heterodyne detection is given by the inequalities

$$\sum_{i\in S} R_i \leq \log\left(1+\sum_{i\in S}\eta_i\bar{n}_i\right), \tag{5.8}$$

for all subsets $S\subseteq\{1,\ldots,m\}$.

We now derive the capacity of the coherent-state MAC with optimal receiver measurements. If we assume that quantum MAC capacity result (3.3)-(3.5) is valid for continuous-variable quantum systems, then the capacity region of the coherent-state MAC is the convex closure of all rate pairs (R_1,R_2) that satisfy

$$R_1 \leq \int p_B(\beta)S(\hat{\rho}_\beta^B)\,d\beta \tag{5.9}$$

$$R_2 \leq \int p_A(\alpha)S(\hat{\rho}_\alpha^A)\,d\alpha \tag{5.10}$$

$$R_1+R_2 \leq S(\bar{\rho}), \tag{5.11}$$

for some product distribution $p_A(\alpha)p_B(\beta)$, where the conditional and average density operators are defined as

$$\hat{\rho}_\beta^B = \int p_A(\alpha)|\alpha'+\beta'\rangle\langle\alpha'+\beta'|\,d\alpha \tag{5.12}$$

$$\hat{\rho}_\alpha^A = \int p_B(\beta)|\alpha'+\beta'\rangle\langle\alpha'+\beta'|\,d\beta \tag{5.13}$$

$$\bar{\rho} = \int\int p_A(\alpha)p_B(\beta)|\alpha'+\beta'\rangle\langle\alpha'+\beta'|\,d\alpha\,d\beta \tag{5.14}$$

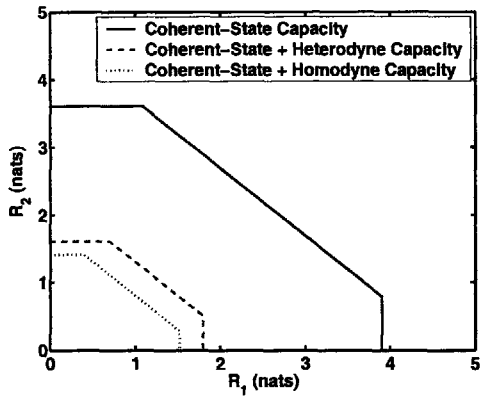


Figure 5-2: Coherent-state capacity of the optical MAC. The capacity region is given by inequalities (5.17). The capacity regions with homodyne and heterodyne measurements are also shown. The transmissivity is $\eta = 1/2$, and the average input photon numbers are $\bar{n}_A = 10$ and $\bar{n}_B = 8$.

with $\alpha' = \sqrt{\eta}\alpha$ and $\beta' = \sqrt{1-\eta}\beta$. Then, circularly symmetric Gaussian distributions

$$p_A(\alpha) = \frac{1}{\pi \bar{n}_A} \exp\left(-\frac{|\alpha|^2}{\bar{n}_A}\right), \tag{5.15}$$

$$p_B(\beta) = \frac{1}{\pi \bar{n}_B} \exp\left(-\frac{|\beta|^2}{\bar{n}_B}\right). \tag{5.16}$$

are the optimal input distributions, and evaluating the rate upper bounds gives the coherent-state MAC capacity region:

$$R_1 \leq g(\eta \bar{n}_A), \quad R_2 \leq g((1-\eta)\bar{n}_B), \quad \text{and} \quad R_1 + R_2 \leq g(\eta \bar{n}_A + (1-\eta)\bar{n}_B). \tag{5.17}$$

Figure 5-2 shows the capacity region of the coherent-state MAC optimized over receiver measurements and with suboptimal homodyne and heterodyne receivers.

5.1.2 Wideband Capacity

The preceding single-mode results for the coherent-state MAC can be extended to the case of wideband operation, in which Alice and Bob may employ photons of any frequency, subject to constraints, P_A and P_B, on the average transmitted powers. For a frequency-multiplexed scheme, in which the frequency domain is divided into bins of width $b = 1/T$, the channel output for the ith mode is

$$\hat{c}_i = \sqrt{\eta}\,\hat{a}_i + \sqrt{1-\eta}\,\hat{b}_i, \tag{5.18}$$

where $\hat{a}_i$ and $\hat{b}_i$ are the input modes at frequency $f_i = i/T$, $i = 1, 2, 3, \ldots$, and η is the frequency-independent transmissivity. We derive the capacity region for the wideband coherent-state MAC, subject to power constraints

$$\sum_i bhf_i E[|\alpha_i|^2] \leq P_A \tag{5.19}$$

$$\sum_i bhf_i E[|\beta_i|^2] \leq P_B, \tag{5.20}$$

where Alice and Bob allocate mean photon numbers $\bar{n}_A(f_i) = E[|\alpha_i|^2]$ and $\bar{n}_B(f_i) = E[|\beta_i|^2]$ at frequency f_i, respectively.

We first derive the capacity region of the wideband coherent-state MAC with homodyne detection. With homodyne receiver measurements, the wideband coherent-state MAC is equivalent to a set of parallel classical MACs with independent zero-mean Gaussian noise. We derive upper bounds on the individual rates R_1, R_2 and the sum rate $R_1 + R_2$ from separate Lagrange multiplier calculations. For Alice's rate, we maximize

$$R_1 = b\sum_i \frac{1}{2}\log(1 + 4\eta E[\alpha_{i,1}^2]), \tag{5.21}$$

such that (5.19) is satisfied. In the limit $b \to 0$, we obtain the wideband solution

$$R_1 = \sqrt{\frac{P'_A}{\pi\hbar}} \tag{5.22}$$

$$\bar{n}'_A(f) = \frac{1}{f}\sqrt{\frac{P'_A}{2h}} - \frac{1}{4}, \qquad \text{for } f \leq 2\sqrt{\frac{2P'_A}{h}}, \tag{5.23}$$

where we let $\bar{n}'_A(f) = \eta\bar{n}_A(f)$ and $P'_A = \eta P_A$. We see from (5.23), that Alice's optimal mean photon number allocation, $\bar{n}_A(f)$, is given by water-filling, as is found in classical information theory. Similarly, maximum wideband rates for R_2 and $R_1 + R_2$ are given by

$$R_2 = \sqrt{\frac{P'_B}{\pi\hbar}} \tag{5.24}$$

$$\bar{n}'_B(f) = \frac{1}{f}\sqrt{\frac{P'_B}{2h}} - \frac{1}{4}, \qquad \text{for } f \leq 2\sqrt{\frac{2P'_B}{h}}, \tag{5.25}$$

and

$$R_1 + R_2 = \sqrt{\frac{P'_A + P'_B}{\pi\hbar}} \tag{5.26}$$

$$\bar{n}'_{AB}(f) = \frac{1}{f}\sqrt{\frac{P'_A + P'_B}{2h}} - \frac{1}{4}, \qquad \text{for } f \leq 2\sqrt{\frac{2(P'_A + P'_B)}{h}}, \tag{5.27}$$

where $\bar{n}'_B(f) = (1-\eta)\bar{n}_B(f)$, $\bar{n}'_{AB}(f) = \bar{n}'_A(f) + \bar{n}'_B(f)$, and $P'_B = (1-\eta)P_B$. The rates (5.22),(5.24), and (5.26) describe a pentagon region which serves as an outer bound for the capacity of the wideband coherent-state MAC. Here, $\bar{n}_B(f)$ is Bob's optimal average photon number allocation, and the role of $\bar{n}'_{AB}(f)$ will be elaborated below.

With average photon number allocations $(\bar{n}_A(f), (\bar{n}'_{AB}(f) - \bar{n}'_A(f))/(1-\eta))$ for Alice and Bob, the lower-right corner point

$$\left(\sqrt{\frac{P'_A}{\pi\hbar}}, \sqrt{\frac{P'_A + P'_B}{\pi\hbar}} - \sqrt{\frac{P'_B}{\pi\hbar}}\right) \tag{5.28}$$

of the outer bound can be achieved. Similarly, $((\bar{n}'_{AB}(f) - \bar{n}'_B(f))/\eta, \bar{n}_B(f))$ achieves the upper-left corner. Thus, the entire region is achievable and hence is equal to the capacity region. A similar derivation shows that the wideband coherent-state MAC with heterodyne detection has the same capacity region.

We can generalize the result to the m-user wideband coherent-state MAC. Suppose the kth user sends coherent states $|\alpha_{k,i}\rangle$. The channel output of the ith mode is the coherent state $|\sum_{k=1}^{m}\sqrt{\eta_k}\alpha_{k,i}\rangle$, where the transmissivities η_k sum to one, and the input power constraint for the kth user is

$$\sum_i bhf_i E[|\alpha_{k,i}|^2] \leq P_k, \tag{5.29}$$

for $k = 1, \ldots, m$. If the receiver uses homodyne or heterodyne detection, then the wideband capacity region is defined by the inequalities

$$\sum_{k\in S} R_i \leq C\left(\sum_{k\in S}\eta_k P_k\right), \tag{5.30}$$

where $C(x) = \sqrt{x/\pi\hbar}$, for all $S \subseteq \{1, \ldots, m\}$.

In the derivations above, we assumed that structured receivers are used to perform measurements at the channel output. We can follow the same approach to optimize the receiver

measurement over the wideband coherent-state MAC. Single-user wideband solutions are applied to derive upper bounds on the individual rates R_1, R_2, and the sum rate $R_1 + R_2$. Then, we check that the resulting outer bound is achievable. This gives us the capacity region

$$R_1 \leq \sqrt{\frac{\pi P'_A}{3\hbar}} \tag{5.31}$$

$$R_2 \leq \sqrt{\frac{\pi P'_B}{3\hbar}} \tag{5.32}$$

$$R_1 + R_2 \leq \sqrt{\frac{\pi (P'_A + P'_B)}{3\hbar}}. \tag{5.33}$$

with the optimal power allocations

$$\bar{n}'_A(f) = \frac{1}{\exp\left(\frac{\pi h f}{\sqrt{6hP'_A}}\right) - 1}, \tag{5.34}$$

$$\bar{n}'_B(f) = \frac{1}{\exp\left(\frac{\pi h f}{\sqrt{6hP'_B}}\right) - 1}, \tag{5.35}$$

$$\bar{n}'_{AB}(f) = \frac{1}{\exp\left(\frac{\pi h f}{\sqrt{6h(P'_A+P'_B)}}\right) - 1}. \tag{5.36}$$

The optimal receiver gives a factor $\pi/\sqrt{3}$ improvement over the conventional receivers.

5.2 Gaussian MAC

Now let us return to the single-mode case and relax our assumption that the transmitters use coherent-state encodings, i.e., we will allow them to use non-classical states in their quest for the largest possible capacity region. As a step toward finding the ultimate capacity region of the optical MAC, let us allow Alice and Bob to employ arbitrary Gaussian states, instead of just coherent states.

5.2.1 Holevo-Sohma-Hirota MAC

We first derive the capacity region for a multiple access version of the Holevo-Sohma-Hirota channel model described in Section 4.2.2. Let $\hat{\rho}(0)$ be a zero-mean, Gaussian state with

variance matrix

$$V = \begin{pmatrix} V_1 & V_{12} \\ V_{12} & V_2 \end{pmatrix}. \tag{5.37}$$

We define a multiple access channel model in which Alice and Bob send classical messages α and β, subject to input constraints

$$\langle |\alpha|^2 \rangle = \int |\alpha|^2 p_A(\alpha)\, d\alpha = N_A, \tag{5.38}$$

$$\langle |\beta|^2 \rangle = \int |\beta|^2 p_B(\beta)\, d\beta = N_B, \tag{5.39}$$

and Charlie receives the state $\hat{\rho}(\alpha, \beta) = \hat{D}(\alpha+\beta)\hat{\rho}(0)\hat{D}^\dagger(\alpha+\beta)$, which is a shifted version of the initial state $\hat{\rho}(0)$. From the quantum MAC result (3.3)-(3.5), the capacity region of the Holevo-Sohma-Hirota MAC is given by the convex hull of all rate pairs (R_1, R_2) satisfying

$$R_1 \leq S(\bar{\rho}_A) - S(\hat{\rho}(0)) \tag{5.40}$$

$$R_2 \leq S(\bar{\rho}_B) - S(\hat{\rho}(0)) \tag{5.41}$$

$$R_1 + R_2 \leq S(\bar{\rho}_{AB}) - S(\hat{\rho}(0)), \tag{5.42}$$

for some product distribution $p_A(\alpha)p_B(\beta)$, where we defined the ensemble averages

$$\bar{\rho}_A = \int p_A(\alpha)\hat{D}(\alpha)\hat{\rho}(0)\hat{D}^\dagger(\alpha)\, d\alpha \tag{5.43}$$

$$\bar{\rho}_B = \int p_B(\beta)\hat{D}(\beta)\hat{\rho}(0)\hat{D}^\dagger(\beta)\, d\beta \tag{5.44}$$

$$\bar{\rho}_{AB} = \int p_A(\alpha)p_B(\beta)\hat{\rho}(\alpha, \beta)\, d\alpha\, d\beta. \tag{5.45}$$

To evaluate this capacity region, we first maximize each of the rate upper bounds for R_1, R_2, and $R_1 + R_2$ separately. We then show that the region described by these maximum rates is achievable.

To maximize the right-hand side of (5.40), we follow the proof of the Holevo-Sohma-Hirota result in [57]. A similar result holds for maximizing the right-hand side of (5.41). For any input distribution $p_A(\alpha)$ that satisfies constraint (5.38), let $\tilde{p}_A(\alpha)$ be the zero-mean Gaussian distribution with the same second moments as $p_A(\alpha)$. Then, $\tilde{p}_A(\alpha)$ satisfies

constraint (5.38) and

$$\tilde{\rho}_A = \int \tilde{p}_A(\alpha)\hat{D}(\alpha)\hat{\rho}(0)\hat{D}^\dagger(\alpha)\,d\alpha \tag{5.46}$$

is a Gaussian state. If $F(\hat{a},\hat{a}^\dagger)$ is any second-order polynomial in $(\hat{a},\hat{a}^\dagger)$, then

$$\begin{aligned}
\mathrm{tr}\bar{\rho}_A F(\hat{a},\hat{a}^\dagger) &= \int p_A(\alpha)\,\mathrm{tr}\left(\hat{D}(\alpha)\hat{\rho}(0)\hat{D}^\dagger(\alpha)F(\hat{a},\hat{a}^\dagger)\right)d\alpha &(5.47)\\
&= \int p_A(\alpha)\,\mathrm{tr}\left(\hat{\rho}(0)F(\hat{a}+\alpha,\hat{a}^\dagger+\alpha^*)\right)d\alpha &(5.48)\\
&= \int \tilde{p}_A(\alpha)\,\mathrm{tr}\left(\hat{\rho}(0)F(\hat{a}+\alpha,\hat{a}^\dagger+\alpha^*)\right)d\alpha &(5.49)\\
&= \mathrm{tr}\tilde{\rho}_A F(\hat{a},\hat{a}^\dagger), &(5.50)
\end{aligned}$$

where we used the fact that $\mathrm{tr}\left(\hat{\rho}(0)F(\hat{a}+\alpha,\hat{a}^\dagger+\alpha^*)\right)$ is a second-order polynomial in (α,α^*). Thus, $\bar{\rho}_A$ and $\tilde{\rho}_A$ have the same second moments, and it follows that $S(\tilde{\rho}_A) \geq S(\bar{\rho}_A)$, i.e., we can restrict to Gaussian input distributions.

When the input distribution $p_A(\alpha)$ is Gaussian, the rate upper bound for R_1 can be expressed as

$$S(\bar{\rho}_A) - S(\hat{\rho}(0)) = g\left(2|V+V_\alpha|^{1/2}-\frac{1}{2}\right) - g\left(2|V|^{1/2}-\frac{1}{2}\right), \tag{5.51}$$

where the variance matrix of $p_A(\alpha)$ is

$$V_\alpha = \begin{pmatrix} V_1^\alpha & V_{12}^\alpha \\ V_{12}^\alpha & V_2^\alpha \end{pmatrix}. \tag{5.52}$$

Thus, the optimization problem we need to solve is

$$\max_{V_\alpha} f(V_\alpha) = |V+V_\alpha|, \tag{5.53}$$

subject to the positive semidefinite and input power constraints

$$\begin{aligned}
V_\alpha &\geq 0, &(5.54)\\
\mathrm{tr}(V_\alpha) &= V_1^\alpha + V_2^\alpha = N_A. &(5.55)
\end{aligned}$$

This constraint region is the interior of a circle in the $V_1^\alpha - V_{12}^\alpha$ plane, which has the

parameterization

$$V_1^\alpha = r\cos\theta + \frac{N_A}{2} \tag{5.56}$$

$$V_{12}^\alpha = r\sin\theta \tag{5.57}$$

$$V_2^\alpha = -r\cos\theta + \frac{N_A}{2}, \tag{5.58}$$

as r and θ take values $0 \le r \le N_A/2$ and $0 \le \theta < 2\pi$, respectively. Now, write

$$f(V_\alpha) = |V + V_\alpha| \tag{5.59}$$

$$= (V_1 + V_1^\alpha)(V_2 + V_2^\alpha) - (V_{12} + V_{12}^\alpha)^2 \tag{5.60}$$

$$= \left(V_1 + r\cos\theta + \frac{N_A}{2}\right)\left(V_2 - r\cos\theta + \frac{N_A}{2}\right) - (V_{12} + r\sin\theta)^2 \tag{5.61}$$

$$= \left(\frac{V_1 + V_2 + N_A}{2}\right)^2 - \left(\frac{V_1 - V_2}{2} + r\cos\theta\right)^2 - (V_{12} + r\sin\theta)^2. \tag{5.62}$$

In terms of the parameters r and θ, our maximization problem is

$$\max_{V_\alpha} f(V_\alpha) = \left(\frac{V_1 + V_2 + N_A}{2}\right)^2 - \min_{r,\theta}\left[\left(\frac{V_2 - V_1}{2} - r\cos\theta\right)^2 + (-V_{12} - r\sin\theta)^2\right]. \tag{5.63}$$

This maximization has two different solutions, depending on whether the point $((V_2 - V_1)/2, -V_{12})$ lies in the circle centered at the origin with radius $N_A/2$. If $((V_2 - V_1)/2, -V_{12})$ lies in the circle, then the minimum on the right-hand side of (5.63) is zero. If $((V_2 - V_1)/2, -V_{12})$ lies outside the circle, then a simple geometric calculation gives the minimum on the right-hand side of (5.63). We thus obtain the maximum individual rates

$$R_{\max 1} = \max_{V_\alpha} S(\bar{\rho}_A) - S(\hat{\rho}(0)) \tag{5.64}$$

$$= \begin{cases} g\left(V_1 + V_2 + N_A - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_A \ge ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2} \\ g\left(2\left[\left(\frac{V_1+V_2+N_A}{2}\right)^2 - \left(\sqrt{\left(\frac{V_1-V_2}{2}\right)^2 + V_{12}^2} - \frac{N_A}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_A < ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2} \end{cases} \tag{5.65}$$

and

$$R_{\max 2} = \max_{V_\beta} S(\bar{\rho}_B) - S(\hat{\rho}(0)) \tag{5.66}$$

$$= \begin{cases} g\left(V_1 + V_2 + N_B - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_B \geq ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2} \\ g\left(2\left[\left(\frac{V_1+V_2+N_B}{2}\right)^2 - \left(\sqrt{\left(\frac{V_1-V_2}{2}\right)^2 + V_{12}^2} - \frac{N_B}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_B < ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2}. \end{cases} \tag{5.67}$$

To maximize the rate sum upper bound, we follow the same approach. It is again sufficient to consider Gaussian input distributions $p_A(\alpha)$ and $p_B(\beta)$, so our maximization problem is

$$\max_{V_\alpha, V_\beta} h(V_\alpha, V_\beta) = |V + V_\alpha + V_\beta|, \tag{5.68}$$

subject to the positive semidefinite and input power constraints

$$V_\alpha \geq 0 \tag{5.69}$$

$$V_\beta \geq 0 \tag{5.70}$$

$$\mathrm{tr}(V_\alpha) = V_1^\alpha + V_2^\alpha = N_A \tag{5.71}$$

$$\mathrm{tr}(V_\beta) = V_1^\beta + V_2^\beta = N_B. \tag{5.72}$$

This constraint region is the interior of two circles with the parameterizations

$$V_1^\alpha = r_A \cos\theta_A + \frac{N_A}{2} \tag{5.73}$$

$$V_{12}^\alpha = r_A \sin\theta_A \tag{5.74}$$

$$V_2^\alpha = -r_A \cos\theta_A + \frac{N_A}{2}, \tag{5.75}$$

where $0 \le r_A \le N_A/2$ and $0 \le \theta_A < 2\pi$, and

$$V_1^\beta = r_B \cos\theta_B + \frac{N_B}{2} \tag{5.76}$$

$$V_{12}^\beta = r_B \sin\theta_B \tag{5.77}$$

$$V_2^\beta = -r_B \cos\theta_B + \frac{N_B}{2}, \tag{5.78}$$

where $0 \le r_B \le N_B/2$ and $0 \le \theta_B < 2\pi$. This parameterization allows us to write $h(V_\alpha, V_\beta)$ as

$$\begin{aligned}
&h(V_\alpha, V_\beta) \\
&= |V + V_\alpha + V_\beta| && (5.79)\\
&= (V_1 + V_1^\alpha + V_1^\beta)(V_2 + V_2^\alpha + V_2^\beta) - (V_{12} + V_{12}^\alpha + V_{12}^\beta)^2 && (5.80)\\
&= \left(V_1 + r_A\cos\theta_A + r_B\cos\theta_B + \frac{N_A+N_B}{2}\right)\left(V_2 - r_A\cos\theta_A - r_B\cos\theta_B + \frac{N_A+N_B}{2}\right) \\
&\quad - (V_{12} + r_A\sin\theta_A + r_B\sin\theta_B)^2 && (5.81)\\
&= \left(\frac{V_1+V_2+N_A+N_B}{2}\right)^2 - \left(\frac{V_1-V_2}{2} + r_A\cos\theta_A + r_B\cos\theta_B\right)^2 \\
&\quad - (V_{12} + r_A\sin\theta_A + r_B\sin\theta_B)^2. && (5.82)
\end{aligned}$$

Thus,

$$\begin{aligned}
&\max_{V_\alpha, V_\beta} h(V_\alpha, V_\beta) \\
&= \left(\frac{V_1+V_2+N_A+N_B}{2}\right)^2 \\
&\quad - \min_{r_A, r_B, \theta_A, \theta_B} \left[\left(\frac{V_2-V_1}{2} - r_A\cos\theta_A - r_B\cos\theta_B\right)^2 + (-V_{12} - r_A\sin\theta_A - r_B\sin\theta_B)^2\right].
\end{aligned} \tag{5.83}$$

The second term on the right in (5.83) is the minimum squared distance between the points $((V_2 - V_1)/2, -V_{12})$ and $(r_A\cos\theta_A + r_B\cos\theta_B,\ r_A\sin\theta_A + r_B\sin\theta_B)$. If $((V_2 - V_1)/2, -V_{12})$ lies in the circle centered at the origin with radius $(N_A + N_B)/2$, then the second term vanishes. Otherwise, a simple calculation gives this minimum distance. We obtain the

maximum sum rate

$$R_{\max 12} = \max_{V_\alpha, V_\beta} S(\bar{\rho}_{AB}) - S(\hat{\rho}(0)) \tag{5.84}$$

$$= \begin{cases} g\left(V_1 + V_2 + N_A + N_B - \frac{1}{2}\right) - g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_A + N_B \geq ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2} \\ g\left(2\left[\left(\frac{V_1+V_2+N_A+N_B}{2}\right)^2 - \left(\sqrt{\left(\frac{V_1-V_2}{2}\right)^2 + V_{12}^2} - \frac{N_A+N_B}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) \\ \quad -g\left(2|V|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N_A + N_B < ((V_1 - V_2)^2 + 4V_{12}^2)^{1/2}. \end{cases} \tag{5.85}$$

We claim that the capacity region $C_{\text{HSH}}(V, N_A, N_B)$, with initial variance matrix V and input constraints N_A and N_B, is the region defined by the inequalities

$$R_1 \leq R_{\max 1} \tag{5.86}$$

$$R_2 \leq R_{\max 2} \tag{5.87}$$

$$R_{12} \leq R_{\max 12}. \tag{5.88}$$

To verify this claim, we show that the corners of this region are achievable. The result then follows by timesharing. Let the point $((V_2 - V_1)/2, -V_{12})$ have coordinates (r_V, θ_V) and suppose that $N_B > N_A$. To show that the lower corner $(R_{\max 1}, R_{\max 12} - R_{\max 2})$ is achievable, we need to find points (r_A, θ_A) and (r_B, θ_B) that simultaneously minimize the distance between (r_V, θ_V) and (r_A, θ_A) and the distance between (r_V, θ_V) and $(r_A, \theta_A) + (r_B, \theta_B)$. Similarly, to show that the upper corner $(R_{\max 12} - R_{\max 1}, R_{\max 2})$ is achievable, we need to minimize the distance between (r_V, θ_V) and (r_B, θ_B) and the distance between (r_V, θ_V) and $(r_A, \theta_A) + (r_B, \theta_B)$. There are four cases to consider: see Fig. 5-3. For each case, we list the coordinates (r_A, θ_A) and (r_B, θ_B) corresponding to the capacity-achieving input distributions.

- Case I.
  - lower corner: $(r_A, \theta_A) = (r_V, \theta_V)$ and $(r_B, \theta_B) = (0, 0)$
  - upper corner: $(r_A, \theta_A) = (0, 0)$ and $(r_B, \theta_B) = (r_V, \theta_V)$

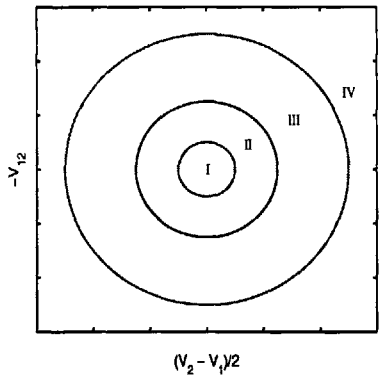


Figure 5-3: Regions. Case I: $r_V \leq N_A/2$. Case II: $N_A/2 < r_V \leq N_B/2$. Case III: $N_B/2 < r_V \leq (N_A + N_B)/2$. Case IV: $r_V > (N_A + N_B)/2$.

- Case II.
  - lower corner: $(r_A, \theta_A) = (N_A/2, \theta_V)$ and $(r_B, \theta_B) = (r_V - N_A/2, \theta_V)$
  - upper corner: $(r_A, \theta_A) = (0, 0)$ and $(r_B, \theta_B) = (r_V, \theta_V)$
- Case III.
  - lower corner: $(r_A, \theta_A) = (N_A/2, \theta_V)$ and $(r_B, \theta_B) = (r_V - N_A/2, \theta_V)$
  - upper corner: $(r_A, \theta_A) = (r_V - N_B/2, \theta_V)$ and $(r_B, \theta_B) = (N_B/2, \theta_V)$
- Case IV.
  - lower corner: $(r_A, \theta_A) = (N_A/2, \theta_V)$ and $(r_B, \theta_B) = (N_B/2, \theta_V)$
  - upper corner: $(r_A, \theta_A) = (N_A/2, \theta_V)$ and $(r_B, \theta_B) = (N_B/2, \theta_V)$.

5.2.2 Gaussian MAC Capacity

We now apply the capacity result derived in the previous section to the optical MAC in Fig. 5-1. Alice and Bob encode their classical messages α and β using input states of the form

$$\hat{\rho}_A(\alpha) = \hat{D}(\alpha)\hat{\rho}_A(0)\hat{D}^\dagger(\alpha) \tag{5.89}$$

$$\hat{\rho}_B(\beta) = \hat{D}(\beta)\hat{\rho}_B(0)\hat{D}^\dagger(\beta), \tag{5.90}$$

where $\hat{\rho}_A(0)$ and $\hat{\rho}_B(0)$ are zero-mean Gaussian states with variance matrices V_A and V_B, respectively. This is a modulation code for which the coherent-state encoding is the special case in which $\hat{\rho}_A(0)$ and $\hat{\rho}_B(0)$ are vacuum states. Charlie receives the output ensemble

$$\{p_A(\alpha)p_B(\beta),\ \mathcal{E}(\hat{\rho}_A(\alpha)\otimes\hat{\rho}_B(\beta))\}, \tag{5.91}$$

where the channel output $\mathcal{E}(\hat{\rho}_A(\alpha)\otimes\hat{\rho}_B(\beta))$ is the Gaussian state with mean $\sqrt{\eta}\alpha+\sqrt{1-\eta}\beta$ and variance $\eta V_A+(1-\eta)V_B$. Define

$$V' = \eta V_A + (1-\eta)V_B \tag{5.92}$$

$$N'_A = \eta\left(\bar{n}_A - V_1^A - V_2^A + \frac{1}{2}\right) \tag{5.93}$$

$$N'_B = (1-\eta)\left(\bar{n}_B - V_1^B - V_2^B + \frac{1}{2}\right), \tag{5.94}$$

where $\bar{n}_A$ and $\bar{n}_B$ are the input mean photon number constraints. The capacity of the Gaussian MAC is the region $C_{\text{HSH}}(V', N'_A, N'_B)$:

$$R_1 \leq R_{\text{max1}} \tag{5.95}$$

$$R_2 \leq R_{\text{max2}} \tag{5.96}$$

$$R_{12} \leq R_{\text{max12}}, \tag{5.97}$$

where the rate upper bounds are given by

$$R_{\text{max1}} = \begin{cases} g\left(\eta\bar{n}_A + (1-\eta)(V_1^B + V_2^B - \frac{1}{2})\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_A \geq ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2} \\ g\left(2\left[\left(\frac{V'_1+V'_2+N'_A}{2}\right)^2 - \left(\sqrt{\left(\frac{V'_1-V'_2}{2}\right)^2 + V'^2_{12}} - \frac{N'_A}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) \\ \quad -g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_A < ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2}, \end{cases} \tag{5.98}$$

$$R_{\max 2} = \begin{cases} g\left(\eta(V_1^A + V_2^A - \frac{1}{2}) + (1-\eta)\bar{n}_B\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_B \geq ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2} \\ g\left(2\left[\left(\frac{V'_1+V'_2+N'_B}{2}\right)^2 - \left(\sqrt{\left(\frac{V'_1-V'_2}{2}\right)^2 + V'^2_{12}} - \frac{N'_B}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) \\ \quad -g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_B < ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2}, \end{cases} \tag{5.99}$$

and

$$R_{\max 12} = \begin{cases} g(\eta\bar{n}_A + (1-\eta)\bar{n}_B) - g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_A + N'_B \geq ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2} \\ g\left(2\left[\left(\frac{V'_1+V'_2+N'_A+N'_B}{2}\right)^2 - \left(\sqrt{\left(\frac{V'_1-V'_2}{2}\right)^2 + V'^2_{12}} - \frac{N'_A+N'_B}{2}\right)^2\right]^{1/2} - \frac{1}{2}\right) \\ \quad -g\left(2|V'|^{1/2} - \frac{1}{2}\right), \\ \qquad \text{for } N'_A + N'_B < ((V'_1 - V'_2)^2 + 4V'^2_{12})^{1/2}. \end{cases} \tag{5.100}$$

For input photon numbers $\bar{n}_A$ and $\bar{n}_B$ sufficiently large, the capacity region of the Gaussian MAC is the set of rate pairs that satisfy

$$R_1 \leq g\left(\eta\bar{n}_A + (1-\eta)\left(V_1^B + V_2^B - \frac{1}{2}\right)\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right) \tag{5.101}$$

$$R_2 \leq g\left(\eta\left(V_1^A + V_2^A - \frac{1}{2}\right) + (1-\eta)\bar{n}_B\right) - g\left(2|V'|^{1/2} - \frac{1}{2}\right) \tag{5.102}$$

$$R_1 + R_2 \leq g(\eta\bar{n}_A + (1-\eta)\bar{n}_B) - g\left(2|V'|^{1/2} - \frac{1}{2}\right). \tag{5.103}$$

This achievable rate region reduces to the coherent-state formulas, Eqs. (5.17), when $V_A = V_B = I/4$. As shown in Fig. 5-4, it is possible to find V_A and V_B, for example,

$$V_A = V_B = \begin{pmatrix} \frac{1}{32} & 0 \\ 0 & 2 \end{pmatrix}, \tag{5.104}$$

such that the Gaussian MAC region is larger than the coherent-state MAC region (5.17). Numerical optimization can further enlarge the capacity region beyond that achieved by this example, but we do not know how to determine the capacity region achieved by Gaussian codes analytically. In the next section, we show that in the limit of large $\bar{n}_A$ and $\bar{n}_B$, transmitting Gaussian states is asymptotically optimal.

5.3 Capacity Outer Bound

Achieving the ultimate capacity region of the optical MAC may require the use of non-Gaussian states, so the capacity of the Gaussian MAC is still only an inner bound. In this section, we develop an outer bound on the ultimate capacity region of the optical MAC. Let Alice and Bob use input states—averaged over their respective random-coding ensembles—$\bar{\rho}_A$ and $\bar{\rho}_B$ that are subject to the average photon number constraints $\bar{n}_A$ and $\bar{n}_B$. Because von Neumann entropy is invariant to mean fields, we know that the optimum $\bar{\rho}_A$ and $\bar{\rho}_B$ will be zero-mean-field states. This, in turn implies that $\langle \hat{c}^\dagger \hat{c} \rangle = \eta \bar{n}_A + (1-\eta)\bar{n}_B$, from which it is easily shown that

$$R_1 + R_2 \leq S(\mathcal{E}(\bar{\rho}_A \otimes \bar{\rho}_B)) \leq g\left(\eta \bar{n}_A + (1-\eta)\bar{n}_B\right). \tag{5.105}$$

The sum-rate upper bound in (5.105) coincides with the coherent-state MAC result appearing in (5.17). Hence, we have shown that the sum rate for the capacity region is achieved by coherent-state encoding in conjunction with optimum (joint-measurement) reception. More generally, the Gaussian-state encoding is a sum-rate-achieving code in the above-threshold regime, i.e., (5.103) coincides with (5.105), whenever $\mathcal{E}(\rho_A(0) \otimes \rho_B(0))$ is pure. Moreover, from (10) it can be shown that heterodyne reception is asymptotically optimum for the sum rate in the limit $\eta \bar{n}_A + (1-\eta)\bar{n}_B \to \infty$.

To upper bound the individual rates R_1 and R_2, consider a super receiver that has access to both output ports of the beam splitter representing the optical MAC. A super receiver can apply the inverse unitary beam splitter transformation to undo the effects of the optical MAC. Thus, the individual rate upper bounds reduce to single-user Holevo informations, and we have the upper bounds $R_1 \leq g(\bar{n}_A)$ and $R_2 \leq g(\bar{n}_B)$. Our optical MAC results are illustrated in Fig. 5-4. Here we have plotted the sum rate for a single-mode quantum optical MAC with $\eta = 1/2$, $\bar{n}_A = 10$, and $\bar{n}_B = 8$, along with the capacity region for heterodyne

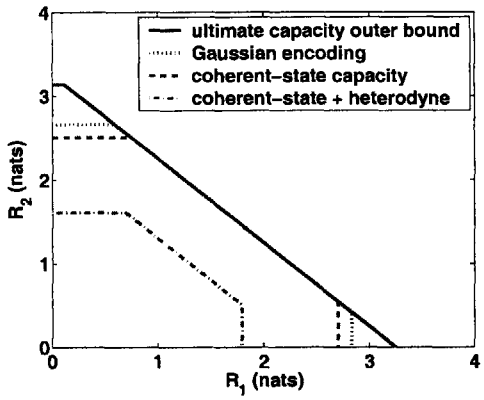


Figure 5-4: Optical MAC capacity region. Inner bounds and the outer bound given by $R_1 \leq g(\bar{n}_A)$, $R_2 \leq g(\bar{n}_B)$, and $R_1 + R_2 \leq g(\eta\bar{n}_A + (1-\eta)\bar{n}_B)$ are shown for the ultimate capacity region of the optical MAC. The Gaussian-state capacity region is evaluated with input variance matrices V_A and V_B given by (5.104). The transmissivity is $\eta = 1/2$, and the average input photon numbers are $\bar{n}_A = 10$ and $\bar{n}_B = 8$.

reception, the individual rate limits for coherent-state encoding, and the individual rate limits for the Gaussian-state encoding from Eq. (5.104).

We have presented codes which achieve the sum-rate upper bound, but it is unknown exactly how far we can reach into the corners of the outer bound region. One thing we can demonstrate is that the individual rate upper bounds are asymptotically achievable in the limit of large $\bar{n}_A$ and $\bar{n}_B$. Let Alice transmit real-valued classical messages α_1 using squeezed states $|\alpha_1, r\rangle$ excited in the first quadrature with squeezing parameter r. Let Bob transmit the zero-mean squeezed state $|0, R\rangle$ with squeezing parameter $R = \sinh^{-1}(\sqrt{\bar{n}_B})$, i.e., Bob squeezes as hard as possible. A rate of

$$R_1 = \frac{1}{2}\log\left(1 + \frac{4(\bar{n}_A - \sinh^2 r)}{e^{-2r} + \frac{1-\eta}{\eta}e^{-2R}}\right) \tag{5.106}$$

is achieved if Charlie uses homodyne detection to decode Alice's message. After substituting the optimal squeezing parameter $r = \log(2\bar{n}_A + 1)/2$ and several applications of L'Hôpital's

rule, we obtain the ratio

$$\lim_{\bar{n}_A \to \infty} \lim_{\bar{n}_B \to \infty} \frac{R_1}{g(\bar{n}_A)} = \lim_{\bar{n}_A \to \infty} \frac{\frac{1}{2} \log \left(1 + 4e^{2r}(\bar{n}_A - \sinh^2 r)\right)}{g(\bar{n}_A)} \tag{5.107}$$

$$= \lim_{\bar{n}_A \to \infty} \frac{\log(1 + 2\bar{n}_A)}{g(\bar{n}_A)} \tag{5.108}$$

$$= 1. \tag{5.109}$$

Thus, this squeezed-state code with homodyne reception is asymptotically optimal for large input photon numbers $\bar{n}_A$ and $\bar{n}_B$. For the special case $\eta = 1$, Bob is irrelevant and the above argument says that the squeezed-state/homodyne code is asymptotically optimal for the single-user noiseless Bosonic channel.

Chapter 6

Summary and Future Work

Our focus has been on deriving the classical capacity of quantum optical communication channels. Capacity results for a general class of Gaussian-noise single-user optical channels were developed and extended to an analysis of the optical MAC. We have also considered the problem of distributing entanglement to distant users in a quantum communication system and derived capacity results for entanglement-assisted MACs.

6.1 Summary of Results

A quantum communication architecture is being developed by a team of researchers at MIT and Northwestern University for long-distance transmission and storage of polarization-entangled photons. In Chapter 2, we derived a single-photon error model for the joint states of the quantum memories of this communication system to assess the effects of source errors and fiber transmission imperfections on teleportation performance. Our results show that while the system's fidelity is not very sensitive to these errors, significant loss of singlet-state throughput may be incurred in some cases. We also studied an extension of the MIT/NU teleportation system that allows for the transmission and storage of GHZ states. The GHZ-state system single-photon error model was derived for two different source configurations, and performance analyses were presented for quantum secret sharing of either classical or quantum information.

In Chapter 3, we studied the superdense coding protocol for transmitting classical information over a quantum MAC in a finite-dimensional space. Theorem 1 states that the capacity region of the three-party superdense coding channel is defined by the set of rates

satisfying the bounds in (3.6)-(3.8). The extension of this result to more than two senders was given in (3.36). We discussed the potential for increasing transmission rates by allowing a user to discard their share of the entanglement resource and sending $\log d$ bits instead. We then considered general non-unitary encoding schemes and determined: (a) unitary superdense coding is optimal for pure entangled states, and (b) separable states are useless for enhancing communication over quantum MACs.

Recently, there has been much progress [7], [53] in determining the classical and quantum communication capacities of Bosonic channels. It was discovered that, surprisingly, single-use coherent-state encodings can achieve the capacity of pure-loss channels and (we conjecture) thermal-noise channels. In Chapter 4, we derived the classical capacity of a class of Gaussian Bosonic channels based on minimum output entropy conjecture (4.16). This class of Gaussian channels represents the quantum version of classical colored Gaussian-noise channels, and our method was motivated by the standard whitening approach used to solve the classical case. We also made an attempt to justify minimum output entropy conjecture (4.16) by showing that coherent input states in fact minimize integer-order output Rényi entropy, for $r \geq 2$, as well as output Wehrl entropy. It seems as if we can minimize all entropy quantities except the one which rigorously proves our channel capacity results.

We studied the capacity of the optical MAC in Chapter 5. For classical light sources, we have derived the capacity of the optical MAC and extended the result to the wideband case through water-filling. We described a more general Gaussian code for enlarging the coherent-state region and provided upper bounds for the sum rate and the individual rates of the ultimate capacity region. Our inner bound achieves the sum-rate upper bound, and we showed that the entire outer bound region is asymptotically achievable in the limit of large input photon numbers $\bar{n}_A$ and $\bar{n}_B$.

6.2 Future Work

Future work on the MIT/NU communication architecture will involve developing improved error models for quantum communication. For the GHZ-state communication system, the OPA and polarization restoration error models presented in Sections 2.1.1 and 2.2 could be developed and applied to the performance analysis of QSS. As mentioned in Section 2.1.1, the lumped element approach taken in the present work is valid for OPAs operating within

a few linewidths about a double resonance. Recent analysis [35] of the dual OPA system, which uses a broadband traveling-wave treatment, could serve to confirm the results developed here as well as to gain additional insight into our communication architecture. It is also desirable to develop new error correction techniques and new methods for overcoming transmission loss.

As discussed in Chapter 3, we would like to derive the capacity for a quantum MAC in which Alice and Bob utilize general local quantum operations to encode their messages. It would be interesting to determine the entanglement-assisted channel capacity beyond the special cases we have studied. A basic assumption in our model is that Alice and Bob are able to transmit their particles over noiseless quantum channels. It would be of interest to generalize capacity results for entanglement-assisted single-user channels [69] to the case of noisy quantum MACs.

In Chapter 4, the capacity of the Gaussian-noise channel was derived for input mean photon numbers exceeding a given threshold. Below this threshold, analytical results are more difficult to obtain. We expect that new techniques need to be developed to better understand the capacity of these channels in the below-threshold regime. We have already discussed at length the open problem of providing a rigorous proof for minimum output entropy conjecture (4.16). A general problem in quantum information theory is additivity of classical information capacity, i.e., whether channel capacity requires coding over multiple channel uses. There is ongoing work on the additivity question for Gaussian Bosonic channels [62] and many other quantum channels.

We studied the capacity of a multiple access quantum optical channel in Chapter 5. The MAC is the simplest multi-user channel to analyze, so there are more communication scenarios to be explored. In the classical theory, channels such as broadcast channels, two-way channels, relay channels, and others have been studied. The corresponding study of their quantum counterparts could be the source of future work.

Appendix A

Multimode Gaussian States

We discuss the unitary transformation $\hat{U}$ for whitening multimode Gaussian states introduced in Section 4.2.3. Let $\hat{\rho}$ be a multimode Gaussian state on the Hilbert space $\mathcal{H}^{\otimes m}$, and define the column vector of position and momentum operators

$$\hat{\xi} = \left(\hat{x}_1, \ \cdots, \ \hat{x}_m, \hat{p}_1, \ \cdots, \ \hat{p}_m\right)^T, \tag{A.1}$$

with commutation matrix

$$\sigma = \left([\hat{\xi}_i, \hat{\xi}_j]\right) = \hbar \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \tag{A.2}$$

The variance matrix $V = (V_{ij})$ of the density operator $\hat{\rho}$ is defined as the matrix with elements

$$V_{ij} = \left\langle \frac{\hat{\xi}_i \hat{\xi}_j + \hat{\xi}_j \hat{\xi}_i}{2} \right\rangle. \tag{A.3}$$

Real linear transformations of the operators $\hat{\xi}_i$ that preserve the commutation relations are called canonical transformations. Every canonical transformation S satisfies

$$S \sigma S^T = \sigma, \tag{A.4}$$

which is the defining relation of the group $\mathrm{Sp}(2m, R)$. For each canonical transformation S that takes $\hat{\xi} \to S\hat{\xi}$, there is a corresponding unitary transformation $\hat{U}(S)$ that acts on the Hilbert space of states: $\hat{\rho} \to \hat{U}(S)\hat{\rho}\hat{U}(S)^\dagger$. By Williamson's theorem, there exists a

canonical transformation S that diagonalizes the variance matrix V to the form:

$$V' = SVS^T = \begin{pmatrix} c_1 & & & & & \\ & \ddots & & & & \\ & & c_m & & & \\ & & & c_1 & & \\ & & & & \ddots & \\ & & & & & c_m \end{pmatrix}. \tag{A.5}$$

This says that a multimode Gaussian state is unitarily equivalent to a product of thermal states. It is possible to compute the values of c_k, $k = 1, \ldots, m$, in this diagonal form. Note that the diagonal elements of V' are not the eigenvalues of V, because V does not undergo a similarity transformation. However, the matrix $\sigma^{-1}V$ evolves under S as

$$\sigma^{-1}V \to \sigma^{-1}SVS^T \tag{A.6}$$

$$= (\sigma S^T)^{-1}VS^T \tag{A.7}$$

$$= (S^T)^{-1}\sigma^{-1}VS^T, \tag{A.8}$$

where we used the relation $\sigma^{-1}S = (\sigma S^T)^{-1}$ which follows from (A.4). This shows that $\sigma^{-1}V$ does undergo a similarity transformation, so its eigenvalues are the same as those of

$$\sigma^{-1}V' = \frac{1}{\hbar}\begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}\begin{pmatrix} c_1 & & & & & \\ & \ddots & & & & \\ & & c_m & & & \\ & & & c_1 & & \\ & & & & \ddots & \\ & & & & & c_m \end{pmatrix} \tag{A.9}$$

$$= \frac{1}{\hbar}\begin{pmatrix} & & & -c_1 & & \\ & & & & \ddots & \\ & & & & & -c_m \\ c_1 & & & & & \\ & \ddots & & & & \\ & & c_m & & & \end{pmatrix} \tag{A.10}$$

The matrix $(\sigma^{-1}V)^2$ has eigenvalues

$$\left\{-\frac{c_1^2}{\hbar^2}, \ldots, -\frac{c_m^2}{\hbar^2}\right\}, \tag{A.11}$$

where each eigenvalue appears with multiplicity two. Thus, the diagonal entries c_k can be found by computing the eigenvalues of the matrix $(\sigma^{-1}V)^2$.

Appendix B

Thermal Operator

Here, we derive an expression for the thermal operator $\hat{G}$ used in Section 4.3.1 and upper bound the absolute value of its eigenvalues.

B.1 Ordered Expansions

One way to evaluate the expectation of an operator $\hat{F}$ is to average one of its associated functions over phase space [70]. In this thesis, we are interested specifically in the symmetrically-ordered (or Weyl-ordered) associated function $F^{(w)}(\alpha, \alpha^*)$. The relationship between an operator and its symmetrically-ordered associated function can be seen by looking at the symmetrically-ordered power series

$$\hat{F}(\hat{a}, \hat{a}^\dagger) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} f_{nm} \{\hat{a}^{\dagger n} \hat{a}^m\}_{\text{sym}} \tag{B.1}$$

and

$$F^{(w)}(\alpha, \alpha^*) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} f_{nm}\, \alpha^{*n} \alpha^m, \tag{B.2}$$

where $\{\hat{a}^{\dagger n} \hat{a}^m\}_{\text{sym}}$ is the average of all ways of ordering the operators. For example,

$$\{\hat{a}^2 \hat{a}^\dagger\}_{\text{sym}} = \frac{1}{3}(\hat{a}^2 \hat{a}^\dagger + \hat{a}\hat{a}^\dagger \hat{a} + \hat{a}^\dagger \hat{a}^2) \tag{B.3}$$

$$\{\hat{a}^2 \hat{a}^{\dagger 2}\}_{\text{sym}} = \frac{1}{6}(\hat{a}^2 \hat{a}^{\dagger 2} + \hat{a}\hat{a}^\dagger \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}^{\dagger 2} \hat{a} + \hat{a}^\dagger \hat{a}^2 \hat{a}^\dagger + \hat{a}^\dagger \hat{a}\hat{a}^\dagger \hat{a} + \hat{a}^{\dagger 2} \hat{a}^2). \tag{B.4}$$

The symmetrically-ordered function of the density operator is called the Wigner function, $W(\alpha) \equiv \rho^{(w)}(\alpha, \alpha^*)/\pi$. Carrying out an evaluation of the expectation $\langle \hat{F} \rangle$ with the symmetrically-ordered associated function $F^{(w)}(\alpha, \alpha^*)$ requires averaging with the Wigner function $W(\alpha)$ as follows:

$$\langle \hat{F} \rangle = \langle F^{(w)}(\alpha, \alpha^*) \rangle_{W(\alpha)} \equiv \int F^{(w)}(\alpha, \alpha^*) W(\alpha) d\alpha. \tag{B.5}$$

B.2 Thermal Operator

In Section 4.3.1, the output r-purity of the classical-noise channel was expressed in (4.114) as an average over phase space weighted by a Wigner function. Our problem is to find the operator $\hat{G}(\hat{\boldsymbol{b}}, \hat{\boldsymbol{b}}^\dagger)$ that has the symmetrically-ordered associated function

$$G^{(w)}(\boldsymbol{\beta}, \boldsymbol{\beta}^\dagger) = \frac{1}{n^r \det A} \exp\left(-\sum_{k=1}^{r} \frac{|\lambda_k^B|^2 |\beta_k|^2}{\lambda_k^A} \right). \tag{B.6}$$

It will suffice to show that the single-mode thermal operator

$$\hat{F} = \frac{2\lambda}{2\lambda + 1} \left(\frac{2\lambda - 1}{2\lambda + 1} \right)^{\hat{a}^\dagger \hat{a}} \tag{B.7}$$

has the symmetrically-ordered associated function $F^{(w)}(\alpha, \alpha^*) = e^{-|\alpha|^2/\lambda}$. To show this, we use the following closed form expression [70]:

$$F^{(w)}(\alpha, \alpha^*) = 2e^{2|\alpha|^2} \int \langle -\beta | \hat{F} | \beta \rangle \, e^{-2\beta\alpha^* + 2\beta^*\alpha} \frac{d\beta}{\pi} \tag{B.8}$$

$$= \frac{4\lambda}{2\lambda + 1} e^{2|\alpha|^2} \int \langle -\beta | \left(\frac{2\lambda - 1}{2\lambda + 1} \right)^{\hat{a}^\dagger \hat{a}} | \beta \rangle \, e^{-2\beta\alpha^* + 2\beta^*\alpha} \frac{d\beta}{\pi} \tag{B.9}$$

$$= \frac{4\lambda}{2\lambda + 1} e^{2|\alpha|^2} \int \exp\left(-\frac{4\lambda}{2\lambda + 1} |\beta|^2 - 2\beta\alpha^* + 2\beta^*\alpha \right) \frac{d\beta}{\pi} \tag{B.10}$$

$$= e^{-|\alpha|^2/\lambda}. \tag{B.11}$$

Thus, we know that

$$\left\langle e^{-|\alpha|^2/\lambda} \right\rangle_{W(\alpha)} = \frac{2\lambda}{2\lambda + 1} \left\langle \left(\frac{2\lambda - 1}{2\lambda + 1} \right)^{\hat{a}^\dagger \hat{a}} \right\rangle. \tag{B.12}$$

Extending this to the multimode case gives us our thermal operator

$$\hat{G} = \frac{1}{n^r \det A} \bigotimes_{k=1}^{r} \frac{2\lambda_k^A}{2\lambda_k^A + |\lambda_k^B|^2} \left(\frac{2\lambda_k^A - |\lambda_k^B|^2}{2\lambda_k^A + |\lambda_k^B|^2} \right)^{\hat{b}_k^\dagger \hat{b}_k} \tag{B.13}$$

$$= \bigotimes_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \left(\frac{2\lambda_k^A - |\lambda_k^B|^2}{2\lambda_k^A + |\lambda_k^B|^2} \right)^{\hat{b}_k^\dagger \hat{b}_k} . \tag{B.14}$$

The thermal operator $\hat{G}$ is diagonalized in the number-state basis $\{|m_k\rangle\}$ of the annihilation operators $\hat{b}_k$ with eigenvalues of the form

$$\prod_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \left(\frac{2\lambda_k^A - |\lambda_k^B|^2}{2\lambda_k^A + |\lambda_k^B|^2} \right)^{m_k} , \tag{B.15}$$

where the m_k are non-negative integers. We will bound the expectation of $\hat{G}$ by the maximum absolute value of its eigenvalues. Since the λ_k^A have positive real parts, see (4.103), it follows that

$$\langle \hat{G} \rangle \leq \max_{m_k} \left| \prod_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \left(\frac{2\lambda_k^A - |\lambda_k^B|^2}{2\lambda_k^A + |\lambda_k^B|^2} \right)^{m_k} \right| \tag{B.16}$$

$$= \left| \prod_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \right| \max_{m_k} \prod_{k=1}^{r} \left| \frac{2\lambda_k^A - |\lambda_k^B|^2}{2\lambda_k^A + |\lambda_k^B|^2} \right|^{m_k} \tag{B.17}$$

$$= \left| \prod_{k=1}^{r} \frac{2/n}{2\lambda_k^A + |\lambda_k^B|^2} \right| . \tag{B.18}$$

Equality is achieved by the eigenvalue associated with the product vacuum state $|0\rangle^{\otimes r}$ of the annihilation operators $\hat{b}_k$.

Bibliography

[1] J. P. Gordon. Information capacity of a communications channel in the presence of quantum effects. In J. R. Singer, editor, *Advances in Quantum Electronics*, page 509. Columbia University, New York, 1961.

[2] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems. *Phys. Rev. Lett.*, 70:363–366, 1993.

[3] C. M. Caves and P. D. Drummond. Quantum limits on bosonic communication rates. *Rev. Mod. Phys.*, 66:481–537, 1994.

[4] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inform. Theory*, 44:269–273, 1998.

[5] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56:131–138, 1997.

[6] C. E. Shannon. A mathematical theory of communication. *Bell Sys. Tech. Journal*, 27:379–423, 623–656, 1948.

[7] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen. Classical capacity of the lossy bosonic channel: The exact solution. *Phys. Rev. Lett.*, 92:027902, 2004.

[8] S. Guha. Classical capacity of the free-space quantum-optical channel. S. M. thesis, Massachusetts Institute of Technology, 2004.

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[10] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[11] D. Bouwmeester, J-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[12] D. Bouwmeester, K. Mattle, J-W. Pan, H. Weinfurter, A. Zeilinger, and M. Zukowski. Experimental quantum teleportation of arbitrary quantum states. *Appl. Phys. B*, 67:749–752, 1998.

[13] G. Bowen. Classical information capacity of superdense coding. *Phys. Rev. A*, 63:022302, 2001.

[14] T. Hiroshima. Optimal dense coding with mixed state entanglement. *J. Phys. A: Math. Gen.*, 34:6907–6912, 2001.

[15] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[16] A. S. Holevo. Information theoretical aspects of quantum measurements. *Probl. Peredachi Inf.*, 9:177, 1973.

[17] A. Peres and W. K. Wootters. Optimal detection of quantum information. *Phys. Rev. Lett.*, 66:1119–1122, 1991.

[18] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[19] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[20] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A*, 54:1869–1876, 1996.

[21] W. H. Louisell. *Quantum Statistical Properties of Radiation.* John Wiley & Sons, 1973.

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

[23] C. W. Gardiner and P. Zoller. *Quantum Noise.* Springer-Verlag, 2000.

[24] J. H. Shapiro. Architectures for long-distance quantum communication. *New J. Phys.*, 4:47.1–47.18, 2002.

[25] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro. Minimal output entropy of bosonic channels: a conjecture. *Phys. Rev. A*, 70:032315, 2004.

[26] J. H. Shapiro and N. C. Wong. An ultrabright narrowband source of polarization-entangled photon pairs. *J. Opt. B: Quantum and Semiclass. Opt.*, 2:L1–L4, 2000.

[27] S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer. Long-distance, unconditional teleportation of atomic states via complete Bell state measurements. *Phys. Rev. Lett.*, 87:167903, 2001.

[28] J. Aung. Quantum error modelling and correction in long distance teleportation using singlet states. S. M. thesis, Massachusetts Institute of Technology, 2002.

[29] B. J. Yen and J. H. Shapiro. Error models for long-distance qubit teleportation. *IEEE J. Select. Topics Quantum Electron.*, 9:1483–1494, 2003.

[30] J. H. Shapiro, J. Aung, and B. J. Yen. Quantum error models and error mitigation for long-distance teleportation architectures. Feynman Festival conference, Aug. 2002, quant-ph/0211086.

[31] B. J. Yen and J. H. Shapiro. Error models and error mitigation for long-distance, high-fidelity quantum secret sharing. In D. Abbott, J. H. Shapiro, and Y. Yamamoto, editors, *Fluctuations and Noise in Photonics and Quantum Optics*, volume 5111 of *Proc. of SPIE*, pages 104–117, 2003.

[32] M. Hillery, V. Buzek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, 1999.

[33] P. Kumar. Quantum frequency conversion. *Opt. Lett.*, 15:1476–1478, 1990.

[34] J. M. Huang and P. Kumar. Observation of quantum frequency conversion. *Phys. Rev. Lett.*, 68:2153–2156, 1992.

[35] J. H. Shapiro. Generating quantum interference and polarization entanglement with optical parametric amplifiers. *Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing*, pages 153–158, 2003.

[36] N. C. Wong, K. W. Leong, and J. H. Shapiro. Quantum correlation and absorption spectroscopy in an optical parametric oscillator in the presence of pump noise. *Opt. Lett.*, 15:891–893, 1990.

[37] K. Bergman, C. R. Doerr, H. A. Haus, and M. Shirasaki. Sub-shot-noise measurement with fiber-squeezed optical pulses. *Opt. Lett.*, 18:643–645, 1993.

[38] D. M. Greenberger, M. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Quantum Theory, and Conceptions of the Universe*, pages 73–76. Kluwer Academic, 1989.

[39] D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger. Observation of three-photon Greenberger-Horne-Zeilinger entanglement. *Phys. Rev. Lett.*, 82:1345–1349, 1999.

[40] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto. Triggered single photons from a quantum dot. *Phys. Rev. Lett.*, 86:1502–1505, 2001.

[41] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77:198–201, 1996.

[42] E. N. Maneva and J. A. Smolin. Improved two-party and multi-party purification protocols. quant-ph/0003099.

[43] M. Huang, Y. Zhang, and G. Hou. Classical capacity of a quantum multiple-access channel. *Phys. Rev. A*, 62:052106, 2000.

[44] A. Winter. The capacity of the quantum multiple-access channel. *IEEE Trans. Inform. Theory*, 47:3059–3065, 2001.

[45] R. F. Werner. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen*, 34:7081–7094, 2001.

[46] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, 2000.

[47] S. Bose, V. Vedral, and P. L. Knight. Multiparticle generalization of entanglement swapping. *Phys. Rev. A*, 57:822–829, 1998.

[48] S. Bose and V. Vedral. Mixedness and teleportation. *Phys. Rev. A*, 61:040101(R), 2000.

[49] M. Horodecki, P. Horodecki, R. Horodecki, D. W. Leung, and B. M. Terhal. Classical capacity of a noiseless quantum channel assisted by noisy entanglement. *Q. Info. and Comp.*, 1:70, 2001.

[50] M. B. Plenio, S. Virmani, and P. Papadopoulos. Operator monotones, the reduction criterion and the relative entropy. *J. Phys. A: Math. Gen.*, 33:L193–L197, 2000.

[51] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619–1633, 1998.

[52] J. P. Gordon. Quantum effects in communications systems. *Proc. IRE*, 50:1898, 1962.

[53] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor. Broadband channel capacities. *Phys. Rev. A*, 68:062323, 2003.

[54] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, B. J. Yen, and H. P. Yuen. Information capacity of bosonic channels. Presented at ISIT-2004, IEEE Internation Symposium on Information Theory.

[55] H. P. Yuen. Communication and measurement with squeezed states. In P. D. Drummond and Z. Ficek, editors, *Quantum Squeezing*. Springer-Verlag, 2004. quant-ph/0109054.

[56] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991.

[57] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum gaussian channels. *Phys. Rev. A*, 59:1820–1828, 1999.

[58] J. H. Shapiro. Optical waveguide tap with infinitesimal insertion loss. *Opt. Lett.*, 5:351–353, 1980.

[59] V. Giovannetti, S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen. Minimal Rényi and Wehrl entropies at the output of bosonic channels. *Phys. Rev. A*, 70:022328, 2004.

[60] C. M. Caves and K. Wódkiewicz. Classical phase-space descriptions of continuous-variable teleportation. *Phys. Rev. Lett.*, 93:040506, 2004.

[61] V. Giovannetti and S. Lloyd. Additivity properties of a gaussian channel. *Phys. Rev. A*, 69:062307, 2004.

[62] A. Serafini, J. Eisert, and M. M. Wolf. Multiplicativity of maximal output purities of Gaussian channels under Gaussian inputs. quant-ph/0406065.

[63] T. Tanaka. A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors. *IEEE Trans. Inform. Theory*, 48:2888–2910, 2002.

[64] R. R. Müller. Channel capacity and minimum probability of error in large dual antenna array systems with binary modulation. *IEEE Trans. Signal Processing*, 51:2821–2828, 2003.

[65] M. Mézard, G. Parisi, and M. A. Virasoro. *Spin Glass Theory and Beyond.* Singapore: World Scientific, 1987. World Scientific Lecture Notes in Physics, vol. 9.

[66] H. P. Yuen and J. H. Shapiro. Optical communication with two-photon coherent states – Part III: Quantum measurements realizable with photoemissive detectors. *IEEE Trans. Inform. Theory*, IT-26:78–92, 1980.

[67] A. Wehrl. On the relation between classical and quantum-mechanical entropy. *Rep. Math. Phys.*, 16:353, 1979.

[68] E. H. Lieb. Proof of an entropy conjecture of Wehrl. *Commun. Math. Phys.*, 62:35–41, 1978.

[69] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Trans. Inform. Theory*, 48:2637–2655, 2002.

[70] G. S. Agarwal and E. Wolf. Calculus for functions of noncommuting operators and general phase-space methods in quantum mechanics. I. Mapping theorems and ordering of functions of noncommuting operators. *Phys. Rev. D*, 2:2161–2186, 1970.