



Quantum Information Theory in Infinite Dimensions with Application to Optical Channels

Vinod Sharma* and Konchady Gautam Shenoy

Abstract | Information theory deals with the efficient representation of information sources as well as providing fundamental limits to the amount of information communicated reliably over channels. These sources and channels are generally classical, i.e., represented by standard probability distributions. Quantum information theory takes it to the next level where we allow for the sources as well as channels to be quantum. From the representation of quantum states to the communication over quantum channels, the theory not only essentially encapsulates classical information theoretic methods but also accounts for quantum effects such as superposition, entanglement, interference, etc. In this article, we will review and focus on the information theoretic analysis of quantum channels with infinite dimensions. Infinite dimensionality is needed to model quantum optical channels which are ubiquitous in today's practical networks, distributed quantum communication and quantum internet. The infinite dimensionality introduces some unique problems when compared with finite-dimensional channels and has not been deeply explored in literature from the quantum information theoretic perspective. For these channels, we provide the essential concepts and state-of-the-art channel capacity results. To make this paper self-contained, we also recall the finite dimensional results.

Keywords: Bosonic channel, Optical channel, Quantum channel capacity, Quantum information, Entanglement

1 Introduction

Information theory is a field of applied probability that deals with the quantification of uncertainty. Initiated by a landmark paper by Claude Shannon¹, it was originally intended to be used for data compression and to determine the fundamental limits of communication. Today, however, it finds a variety of applications including portfolio optimization² and evolutionary biology³. Recently, there has also been work in characterizing quantum mechanical interactions as channels and viewing them from information theoretic perspective. This allows us to obtain channel capacity results for those interactions similar to classical case. Moreover, there are some new notions of capacity (e.g., Quantum Capacity)

which are specific to quantum communication. While there do exist extensive surveys⁴ on finite dimensional quantum information theory, there are very few for infinite-dimensional cases. Interesting channels such as Gaussian Bosonic channels, used in optical channels, fall in this purview.

When considering classical channel coding problems, the channel is modelled as a conditional probability mass function (pmf) where given a certain input, an output is generated with respect to the pmf. In quantum channel coding problems, the channel is modeled as a *completely positive trace preserving* (CPTP) map⁵⁻⁷. These recover the classical channel results as special cases. What makes quantum channels special is in the usage of *entangled*

¹ ECE Department, Indian Institute of Science, Bengaluru, Karnataka 560012, India.
*vinod@iisc.ac.in

states and superpositions of states⁸, which do not have classical equivalents that aid in boosting channel capacity. An elementary example is that of *superdense coding*⁹, where in the presence of entanglement, 2 bits of information may be sent using one entangled qubit. Thus the study of quantum information theory promises significant gains in telecommunications provided we can get around the intricacies involved. For example, quantum modeling of optical fibers can provide higher transmission rate of classical information than possible via classical modeling (see¹⁰); in fact, even for semi-classical modeling with direct, homodyne or heterodyne detection.

While there are several potential benefits in switching to quantum communications, it must be noted that there are some restrictions that prevent us from abusing the technology. This is characterized by the so-called *no-go* theorems. For instance, the *no cloning* theorem^{11–13} states that there is no unitary operation that can clone an arbitrary unknown state. This is unlike classical communication where bits may be copied. Then there is the *no communication* theorem¹⁴ which states that the very act of measuring an entangled state does not communicate information. This is important as measuring a state in quantum systems is very unlike in classical systems and it does not help in communication. Finally, the *quantum teleportation* protocol^{15,16} may lead to the incorrect conclusion that, as the state transfer was instant, we communicated faster than speed of light¹⁷. In fact, that protocol is constricted by an auxiliary classical channel which forces the information transfer to be limited by the speed of light. Without the classical channel outputs, the receiver cannot extract any useful information from its state. These are just some of the many examples that illustrate the limitations of quantum technology.

When restricted to finite-dimensional Hilbert spaces, most results and techniques nearly mimic that of classical information theory^{5,7}. For example, achievability of classical discrete memoryless channel capacity is derived using a method called *typical sets*². The quantum analog of this is *typical subspaces* which uses a similar proof technique to derive the achievability bound. There are quantum analogs of several classical information theory concepts, e.g., *quantum entropy* (also known as von Neumann Entropy), *quantum KL Divergence*, *quantum mutual information* to name a few (see^{5–7}). For the concepts that have no classical analog, e.g., coherent information, quantum capacity, finite-dimensional quantum information theory is still tractable for several classes of

channels. To aid in the understanding of infinite-dimensional results, we will recall the finite dimensional results wherever applicable.

Other interesting applications of quantum information theory (QIT) include quantum error correction (QECC)^{8,18,19}, quantum source coding (QSC)^{20,21}, quantum key distribution (QKD), private capacity and quantum internet, to name a few. We do not cover these in our survey but briefly comment in the following.

Classical error correction deals with the design of coding techniques to safeguard messages from a specified number of errors. This is done by adding redundant symbols to the message which serve to recover the message when an error occurs. When the messages are binary, the errors are merely bit flips. In QECC, the error could be a qubit flip (X Gate), phase flip (Z Gate), Y-Gate errors or any superposition of these. Thus there are more types of errors and so, the coding techniques are more sophisticated. The first type of Quantum ECC was the *Shor 9-Qubit code*²² which required 8 additional qubits to protect a single qubit from any type of Pauli gate (X, Z or Y gate) errors. The idea that the uncountable number of errors can be efficiently corrected started with²², refined in Calderbank-Shor-Steane (CSS) codes²³, culminating into stabilizer codes⁸. We require far more qubits (five) to protect a qubit than the bits needed in classical ECC. Moreover, unlike bits, qubits have a tendency to decohere and, therefore, lose their information unless extreme conditions (near zero Kelvin temperature, superconductivity, etc.) are maintained. This led to the field of fault-tolerant quantum computing²⁴ which also takes into account the failure rate of the qubits. However, it is still a far cry to build a sustainable fault-tolerant quantum system. The above references are on QECC for discrete (qubit) variables. But there has been extensive work on extension of these to continuous variables as well (see^{24,25}). An interesting no-go theorem here is that error correction of Gaussian noise imposed on Gaussian states using only Gaussian operations is impossible²⁶.

Classical information theory gives a lower bound on the number of bits required to describe a source, known as the *source coding theorem*^{1,2}. In QIT, a quantum source, that output's quantum states instead are considered. The states need not be orthonormal and are output with a corresponding pmf. The quantum source coding result by Schumacher^{5,20} is analogous to the classical one, in that the von Neumann entropy of the averaged state of the source is the minimum number of qubits required to represent

the source. For more recent results on it, see²⁷. Shannon's rate distortion theory² has also been extended. See²⁸ for previous references and further extensions.

Transmitting secret messages over a public channel can be achieved by private key or by a public key protocol. Private key protocol was invented by Shannon¹. It is provably secure. However, it requires a secret key between the transmitter and the receiver which is as long as the message to be transmitted and can be used only once. Thus public key cryptography is commonly used. However, the secrecy in this is ensured only due to difficulty in computing some functions, e.g., in RSA²⁹, the difficulty in factoring large integers is exploited. But with Shor's algorithm³⁰, this can be accomplished efficiently if quantum computers are available. The QKD algorithm BB84 (Bennett and Brassard³¹) helps in distributing a secret key between the transmitter and the receiver unconditionally. This can be used in private key protocol. In this protocol, due to no cloning theorem, the eavesdropper cannot copy the message from the channel without being noticed. An improvement to the protocol, SARG04 in³² was proposed in 2004. Of all the quantum protocols mentioned so far, it is QKD that is closest to being implemented in practice³³. See³⁴ for different variations of QKD. For continuous (Gaussian) variables, see^{35–37}. Scarani et al.³⁶ has extensive comparison of discrete and continuous variable QKD.

Private classical capacity refers to the classical capacity of communication which is provably secret via a suitable secrecy metric. A good reference is the book El Gamal and Kim³⁸. In the quantum setting, major strides were made by Devetak³⁹ which extended the HSW capacity results to private capacity and by Ke Li et al.⁴⁰ which showed that private classical capacity was non-additive. Private classical capacity is the maximum rate at which a secret key can be established between two users in QKD. For finite dimensions, it is lower bounded by the quantum capacity^{5,6}. For degradable channels, it equals the quantum capacity. For infinite dimensions, recent contributions are⁴¹ and⁴², where for some Gaussian channels, private classical capacity is shown to be equal to the quantum capacity.

A widespread use of quantum computing and communication requires a *quantum internet*^{43–45}. In quantum internet, all communications between multiple parties is carried out using quantum protocols and secrecy is ensured using QKD. Thus, a major issue in quantum internet is to establish an entangled state between two or

more distributed nodes. This is needed for QKD, to transmit quantum information, say through teleportation, and distributed quantum computation. We will also see in this review that entanglement between the transmitter and the receiver can increase the classical and quantum capacity of the quantum channel. However, entanglement between two nodes cannot be generated via a classical communication link; a quantum channel is required also. Thus in the design of a quantum network efficiently, one needs to compute the entanglement generation capacity of point-to-point and general networks. For finite-dimensional point-to-point quantum channels, it equals the quantum capacity⁷ studied in this review. For some infinite-dimensional channels, this equality has been shown in⁴². Another important consideration in quantum internet is the two-way capacities of networks of channels. In our review, we do not consider these capacities although they are intimately connected to one-way communication between point-to-point channels studied in this review. See^{45,46} and the references therein for more details on these issues.

The useful concepts of zero-error channel capacity and network coding have also been extended to quantum domain⁴.

The trouble starts when we venture into infinite-dimensional Hilbert spaces. Without a suitable framework, most, if not all, of the machinery developed for finite-dimensional Hilbert spaces are inapplicable. This is because the proof techniques revolve around the finiteness of the dimensionality of the underlying Hilbert space. Moreover, without additional constraints on the states of the Hilbert space, the channels under study may be absurd and have a trivial infinite classical capacity. Unfortunately, as mentioned earlier, a very important class of channels, namely the Gaussian Bosonic channels are constrained channels in infinite dimensions. These model optical channels, which are encountered in fiber optic as well as free space optical communications^{47,48}.

There are two ways to circumvent these issues as follows: One is to find an alternate finite-dimensional or parameter representation of the states and work with that. Fortunately, Bosonic Gaussian channels in constrained space are amenable to it. The other is to use suitable limit theorems that allow us to obtain the results we desire via a simple limit. As we are not providing proofs, we may not see it but we will recall those results.

Major milestones in the development of QIT are the following: Quantum entropy was defined by von Neumann in 1927. Holevo⁴⁹ proved the

first theorem of QIT and provided an upper bound on the mutual information between transmitter and receiver. The quantum source coding theorem, corresponding to the Shannon's¹ source coding theorem was proved by Schumacher²⁰. Two early communication protocols, namely quantum teleportation¹⁵ and quantum dense coding⁹, have turned out fundamental in QIT. Holevo⁵⁰ and Schumacher, Westmoreland⁵¹ independently proved the HSW theorem providing the classical capacity result for a quantum channel.

Entanglement-assisted classical capacity was obtained by Bennett, Shor, Smolin and Thapliyal in⁵².

Quantum information transmission via a quantum channel was initiated in Schumacher and Nielsen⁵³, Adami and Cerf⁵⁴ along with others. The quantum capacity for finite-dimensional channels was proved in Devetak³⁹. Shor⁴⁷ proved that non-additivity of Holevo capacity is a result of non-additivity of minimum output entropy. An early survey providing far more references is found in⁵⁵.

The quantum teleportation and dense coding algorithms have been extended to continuous variables in⁵⁶ and⁵⁷. For infinite-dimensional channels, the classical capacity for energy-constrained quantum channel is obtained in⁵⁸. The results for entanglement-assisted classical capacity are provided in⁵⁵. The energy-constrained quantum capacity is studied in⁴². A major breakthrough was in⁵⁹ and Holevo⁶⁰ for linear bosonic Gaussian gauge covariant or contravariant channels where additivity of the minimum output entropy was shown and hence a single-letter characterization of classical capacity was obtained.

The surveys^{4,6,55,61,62} provide a lot more information on the topics mentioned above. The book⁶³ addresses the application of these issues in practical communication systems.

The paper is organized as follows: In Sect. 2, we provide the notation and basic definitions and results in QIT. We also particularize these for Gaussian states. Section 3 introduces C–Q channels, which are the most basic form of a quantum channel and we provide classical capacity results for the finite as well as the available results for the Gaussian C–Q channels. In Sect. 4, we provide the classical capacity results for quantum channels and then juxtapose them with the single mode Gaussian channel results. We also discuss the various types of Gaussian channels and discuss quantum channels with entanglement assistance. Section 5 discusses quantum capacities of the channels we studied so far. In Sect. 6, we

discuss an elementary model for free space optical channels and in Sect. 6.1, we match the model obtained earlier with the Gaussian channels we studied and obtain corresponding capacity results. Section 7 discusses the multiuser versions of the quantum channels. In Sect. 8, we discuss recent developments and some open questions in this field. Finally, we conclude the survey.

Our focus, therefore, will be on quantum communication problems in infinite dimensions with special attention to Gaussian channels. We will provide the classical as well as quantum capacity expressions, for the cases where they are known.

2 Preliminaries

A good introduction to the following topics is in^{6,64}: Let \mathcal{H} be a *separable* Hilbert space, which may be infinite dimensional. Let $\mathcal{B}(\mathcal{H})$ be the Banach Algebra of linear bounded operators on \mathcal{H} .

For $A \in \mathcal{B}(\mathcal{H})$, let

$$|A| \triangleq \sqrt{A^*A}, \quad \text{Tr}(A) = \sum_i \langle e_i | A e_i \rangle, \quad (1)$$

$$\|A\|_1 \triangleq \text{Tr}(|A|),$$

where A^* is the adjoint of A and $\{e_i\}$ is an orthonormal basis (o.n.b) in \mathcal{H} and $\langle \cdot | \cdot \rangle$ denotes the inner product of \mathcal{H} . $\|A\|_1$ is called the *trace norm* of A . It is independent of the chosen basis. The set

$$\Gamma(\mathcal{H}) = \{A \in \mathcal{B}(\mathcal{H}) : \|A\|_1 < \infty\}$$

is a Banach space (with norm $\|\cdot\|_1$) of operators. Its elements are called the *trace class operators*.

The operator norm (or simply norm unless otherwise specified) of $A \in \mathcal{B}(\mathcal{H})$

$$\|A\| \triangleq \sup_{\|x\| \leq 1} \|Ax\| \quad (2)$$

satisfies $\|A\| \leq \|A\|_1$ and the dual $\Gamma(\mathcal{H})^* = \mathcal{B}(\mathcal{H})$.

We will use the following definitions:

Definition 1 *Density Operator*. An operator $A \in \Gamma(\mathcal{H})$ is called a density operator if it is positive semidefinite (denoted by $A \geq 0$) and $\text{Tr}(A) = 1$.

A density operator A defines the state of a quantum system with the underlying space \mathcal{H} . Let $\mathcal{S}(\mathcal{H})$ be the space of all density operators on \mathcal{H} . It is a closed convex subset of $\Gamma(\mathcal{H})$. It is also a complete separable metric space with metric

$$\rho(S_1, S_2) = \|S_1 - S_2\|_1, \tag{3}$$

for any $S_1, S_2 \in \mathcal{S}(\mathcal{H})$.

For separable Hilbert spaces \mathcal{H}_1 and \mathcal{H}_2 , $\mathcal{H}_1 \otimes \mathcal{H}_2$ denotes the tensor product space. A density operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$ is *separable* if it is in the closure of the convex hull of product states $S_1 \otimes S_2 \in \Gamma(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Otherwise, it is called an *entangled* state.

Definition 2 *Partial Trace operators* Operators Tr_A and Tr_B are linear operators on $\Gamma(\mathcal{H}_1 \otimes \mathcal{H}_2)$ defined via $\text{Tr}_A(A \otimes B) = B\text{Tr}(A)$ and $\text{Tr}_B(A \otimes B) = A\text{Tr}(B)$. If ρ^{AB} is a state of a system in $\mathcal{H}_A \otimes \mathcal{H}_B$, then $\text{Tr}_A(\rho^{AB})$ and $\text{Tr}_B(\rho^{AB})$ are the corresponding states of the subsystems on \mathcal{H}_A and \mathcal{H}_B , respectively.

Definition 3 *Weak Convergence.* A sequence of operators A_n converges weakly to operator A , denoted by $A_n \xrightarrow{w} A$, if for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$,

$$\langle \psi | A_n \phi \rangle \rightarrow \langle \psi | A \phi \rangle. \tag{4}$$

One can show⁶ that $S_n \xrightarrow{w} S$ weakly in $\mathcal{S}(\mathcal{H})$ if and only if $\|S_n - S\|_1 \rightarrow 0$.

Let e_i be an o.n.b in \mathcal{H} and f_i , a real valued lower bounded sequence. Let $F \in \mathcal{B}(\mathcal{H})$ be defined as

$$F|\psi\rangle = \sum_j f_j |e_j\rangle \langle e_j | \psi \rangle. \tag{5}$$

It is self-adjoint with eigenvalues $\{f_j\}$ with corresponding eigenvectors $\{|e_j\rangle\}$. These will be referred to as *operators of type \mathcal{F}* .

If S is a density operator, then

$$\text{Tr}(SF) = \sum_j f_j \langle e_j | S e_j \rangle \leq \infty \tag{6}$$

is the expectation of S with respect to F . The mapping $S \mapsto \text{Tr}(SF)$ is affine, lower semicontinuous on $\mathcal{S}(\mathcal{H})$. For $E < \infty$,

$$\mathcal{S}_E = \{S : \text{Tr}(SF) \leq E\} \tag{7}$$

is a compact set.

Definition 4 *von Neumann Entropy.*⁵⁻⁷ For a density operator S with spectral decomposition $S = \sum_i s_i |e_i\rangle \langle e_i|$, the *von Neumann entropy* is defined as

$$H(S) = - \sum_i s_i \log s_i = -\text{Tr}(S \log S). \tag{8}$$

Also for density operators S and T , the *relative entropy* of S w.r.t T is

$$H(S; T) = \text{Tr}(S \log S) - \text{Tr}(S \log T). \tag{9}$$

For \mathcal{H} finite dimensional, $H(S) < \infty$ and $H(S)$ and $H(S; T)$ are continuous in $\|\cdot\|_1$ topology^{5,42}. But when \mathcal{H} is infinite dimensional, $H(S)$ may be infinite and $S \mapsto H(S)$ and $(S, T) \mapsto H(S; T)$ are only lower semicontinuous⁶. However, the following important result holds: Let

$$\exp(-\theta F)|\psi\rangle = \sum_j \exp(-\theta f_j) |e_j\rangle \langle e_j | \psi \rangle \tag{10}$$

for all $\theta > 0$.

Lemma 1 ⁶ If $\text{Tr}(\exp(-\theta F)) < \infty$, then $H(S)$ is bounded and continuous on \mathcal{S}_E .

2.1 Gaussian States

Gaussian states are ubiquitous in quantum systems. Any physical quantum system, in small oscillation limit can be represented by a ground state or a thermal equilibrium state. These are Gaussian states. In the following, we will first define general single mode Bosonic states and then the subclass of Gaussian states. See^{6,62,65} for details.

Consider Hilbert space $\mathcal{H} = L^2(\mathbb{R})$, where $L^2(\mathbb{R})$ is the space of square integrable real-valued functions on \mathbb{R} . For $|\psi\rangle \in \mathcal{H}$, define position operator q and momentum operator p , as

$$(q(\psi))(x) = x\psi(x), \quad (p(\psi))(x) = -i\hbar \frac{d}{dx} \psi(x), \tag{11}$$

where \hbar is the normalized Planck's constant. Operators p, q , called canonical variables, are unbounded, self-adjoint with dense domains. For $\omega \in \mathbb{R}^+$, define

$$a = \frac{1}{\sqrt{2\hbar\omega}}(\omega q + ip), \quad a^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega q - ip). \tag{12}$$

In electromagnetics, a, a^\dagger represent a mode of the EM field corresponding to frequency ω at a particular polarization. Also define the *number* operator

$$\mathcal{N} = a^\dagger a = aa^\dagger - I. \tag{13}$$

Also define

$$|n\rangle \triangleq \frac{(a^\dagger)^n}{\sqrt{n!}} |0\rangle, \quad \text{for } n = 0, 1, 2, \dots \tag{14}$$

where $|0\rangle$ is the eigenstate of a corresponding to eigenvalue 0. The set $\{|n\rangle, n = 0, 1, 2, \dots\}$ forms a countable o.n.b for the space \mathcal{H} , called *Fock space*. Thus \mathcal{H} is a separable Hilbert space. State $|n\rangle$ has n photons with frequency ω .

We have $a|n\rangle = \sqrt{n}|n-1\rangle$, for $n \geq 1$ and $a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$ for $n \geq 0$. Thus a^\dagger is called the *creation* operator and a , the *annihilation* operator and ω their frequency. Each $z \in \mathbb{C}$ is an eigenvalue of a with eigenvector z . Operator \mathcal{N} has spectral decomposition

$$\mathcal{N} = \sum_{n=0}^{\infty} n|n\rangle. \tag{15}$$

The variance of $p(\psi) = \|(p-y)|\psi\rangle\|^2$ and of $q(\psi) = \|(q-x)|\psi\rangle\|^2$, where $y = \langle\psi|p\psi\rangle$ and $x = \langle\psi|q\psi\rangle$, satisfy the following *uncertainty principle*:

$$\text{Var}(p(\psi))\text{Var}(q(\psi)) \geq \frac{\hbar^2}{4}. \tag{16}$$

For a probability density p on \mathbb{C} , the set of complex numbers, we can define a density operator

$$S = \int_{z \in \mathbb{C}} |z\rangle\langle z|p(z)d^2z. \tag{17}$$

This is called a *single-mode Bosonic state*. A Bosonic state that maximizes entropy for a fixed energy is called a *Thermal state*.

As a special case, a single mode *Gaussian state* with mean μ and variance N is defined as

$$S_\mu = \frac{1}{\pi N} \int_{z \in \mathbb{C}} |z\rangle\langle z| \exp\left(-\frac{|z-\mu|^2}{N}\right) d^2z, \tag{18}$$

where $\mu \in \mathbb{C}$. Then we can show that for $\mu = 0$,

$$S_0 = \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1}\right)^n |n\rangle\langle n| \quad \text{and} \tag{19}$$

$$H(S_0) = \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1}\right)^n [(n+1)\log(N+1) - n\log N] = g(N), \tag{20}$$

where

$$g(n) = (n+1)\log(n+1) - n\log n \tag{21}$$

and $g(0) = 0$. S_μ is *pure* or *coherent* iff $N = 0$ and then $S_\mu = |\mu\rangle\langle\mu|$. A thermal state is a Gaussian state with $\mu = 0$.

The *characteristic function* of S_μ is defined as

$$\text{Tr}(S_\mu D(z)) = \exp(2i\mathcal{I}(\mu z) - \left(N + \frac{1}{2}\right)|z|^2), \tag{22}$$

where $D(z)\psi(\xi) = \exp\left(\frac{iy}{\hbar}\left(\xi - \frac{x}{2}\right)\psi(\xi - x)\right)$ for $z = \frac{\omega x + iy}{\sqrt{2\hbar\omega}}$ and $\mathcal{I}(z)$ is the imaginary part of z .

Even though Gaussian states have infinite-dimensional support, they can be completely described by first and second moments. Thus these are much more theoretically tractable, especially after using symplectic formulation provided below.

3 C–Q Channels

Let \mathcal{X} be a completely separable metric space with a σ -algebra of Borel sets.

Definition 5 A weakly continuous mapping $\Phi : x \mapsto S_x$, from \mathcal{X} to $\mathcal{S}(\mathcal{H})$ is called a *C–Q* (classical-quantum) channel.

At the output S_x of the channel, we take measurements via non-negative measurement operators $M = M_y, y \in \mathcal{Y}$ for some output alphabet \mathcal{Y} . These operators satisfy $\sum_{y \in \mathcal{Y}} M_y = I$. With these measurements, if input is x , then the probability of measuring y , post measurement, is given by

$$p(y|x) = \text{Tr}(S_x M_y) \tag{23}$$

The above probability effectively defines a classical channel between alphabets \mathcal{X} and \mathcal{Y} .

We consider n independent uses of this channel with the transition probability given by (23). If we input the codeword $x = (x_1, x_2, \dots, x_n)$, where $x_j \in \mathcal{X}$, to this channel then the probability of output $y = (y_1, y_2, \dots, y_n)$ is given by

$$P(y|x) = \prod_{i=1}^n \text{Tr}(S_{x_i} M_{y_i}). \tag{24}$$

Thus, this is a *memoryless* channel. Let $P_e(W, M)$ be the maximum probability of error for codebooks W of codeword length n , with measurements M , with codewords chosen uniformly from W . Then for n channel uses and N_n codewords, the maximum probability of error for the channel is given by

$$P_e(n, N_n) = \min_{W, M} P_e(W, M), \tag{25}$$

where minimum is taken over all codebooks W and measurements M .

3.1 Classical Capacity of a C–Q channel

Definition 6 The classical capacity C of a C–Q channel is defined as the supremum of the rates $R = \lim_{n \rightarrow \infty} \frac{\log N_n}{n}$ where n, N_n are such that

$$\lim_{n \rightarrow \infty} P_e(n, N_n) = 0.$$

C is the maximum rate per channel use of classical information that can be transmitted with arbitrarily low probability of error. This is an asymptotic quantity. To achieve this rate, one may have to use the channel an infinite number of times. If $\dim(\mathcal{H}) < \infty$ (we can then take \mathcal{X} finite dimensional), then we have the following:

Theorem 1 (Holevo, Schumacher, Westmoreland)^{5–7} The classical capacity of a C–Q channel is given by

$$C = \max_{\pi} \left[H \left(\sum_x \pi(x) S_x \right) - \sum_x \pi(x) H(S_x) \right] \triangleq \max_{\pi} \chi(\pi), \tag{26}$$

where the max is over all probability distributions π on \mathcal{X} . The quantity $\chi(\pi)$ is known as Holevo’s information. \square

If $\dim(\mathcal{H}) = \infty$, the capacity in (26) could be infinite and the input energy used also infinite^{6,65}. This happens in classical information theory also. Thus, for channels of interest, an input energy constraint is imposed. In practice, also one needs to impose such constraints. Let $f : \mathcal{X} \rightarrow \mathbb{R}^+$ be a Borel measurable function. Define

$$\mathcal{P}_E = \left\{ \text{Probability measures } \pi \text{ on } \mathcal{X} : \int f(x)\pi(dx) \leq E \right\},$$

for $0 < E < \infty$. Denote $\bar{S}_{\pi} = \int S_x \pi(dx)$. Assume $H(\bar{S}_{\pi}) < \infty$ and define

$$\chi(\pi) = H(\bar{S}_{\pi}) - \int H(S_x)\pi(dx). \tag{27}$$

Then we have

Theorem 2 ⁶Let F be a self adjoint operator of type \mathcal{F} satisfying $\text{Tr}(\exp(-\theta F)) < \infty$ for all $\theta > 0$, and $f(x) \geq \text{Tr}(S_x F)$ for all $x \in \mathcal{X}$. Then $\sup_{\pi \in \mathcal{P}_E} H(\bar{S}_{\pi}) < \infty$ and classical

capacity of C–Q channel $x \mapsto S_x$ with constraint $\int f(x)\pi(dx) \leq E$ is given by

$$C_{\chi} = \sup_{\pi \in \mathcal{P}_E} \chi(\pi) < \infty. \tag{28}$$

This capacity is achievable iff f is lower semicontinuous (l.s.c) and $\{x : f(x) \leq K\}$ is compact for any K with $0 < K < \infty$. \square

In practice, one picks F so that it provides a meaningful energy constraint at the input. If f is l.s.c, then finitely supported probability distributions are dense in \mathcal{P}_E . This helps in proving Theorem 2 from Theorem 1.

3.2 Gaussian C–Q Channel

We can define for each $\mu \in \mathbb{C}$, mapping $\mu \mapsto S_{\mu}$, where S_{μ} is a Gaussian state as defined in (18). This C–Q channel is called a Gaussian C–Q channel. For transmission, we can use codeword $w = (\mu_1, \mu_2, \dots, \mu_n)$ with energy constraint

$$\sum_{i=1}^n |\mu_i|^2 \leq nE. \tag{29}$$

Then the conditions of Theorem 2 are satisfied with $F = a^{\dagger}a = \mathcal{N}$. Therefore the classical capacity of this channel is^{6,62},

$$C = \max_{\pi \in \mathcal{P}_E} \left[H(\bar{S}_{\pi}) - \int H(S_{\mu})\pi(d^2\mu) \right]. \tag{30}$$

where $\mathcal{P}_E = \{\pi \text{ dist. } : \int |\mu|^2 \pi(d^2\mu) \leq E\}$.

We have $H(S_{\mu}) = H(S_0) = g(N)$ (from (20)). The maximum in (30) is attained by the Gaussian density operator and⁶

$$C = C_{\chi} = g(N + E) - g(N) = \log \left(1 + \frac{E}{N + 1} \right) + (N + E) \log \left(1 + \frac{1}{N + E} \right) - N \log \left(1 + \frac{1}{N} \right). \tag{31}$$

This formula behaves as $\log \left(1 + \frac{E}{N+1} \right)$ for large

N , and hence is a quantum generalization of Shannon’s formula.

4 Quantum Channel

To define a quantum channel, we first define the following terms:

Definition 7 *Trace preserving mapping.* For separable Hilbert spaces \mathcal{H}_A and \mathcal{H}_B , a mapping $\Phi : \Gamma(\mathcal{H}_A) \rightarrow \Gamma(\mathcal{H}_B)$ is called *trace preserving* if for all trace class operators T , $\text{Tr}(\Phi(T)) = \text{Tr}(T)$.

Definition 8 *Completely positive map.* A mapping $\Phi : \Gamma(\mathcal{H}_A) \rightarrow \Gamma(\mathcal{H}_B)$ is *completely positive* if $\Phi \otimes I_n$ maps positive semidefinite operators to positive semidefinite operators for all $n \geq 1$, where I_n is the identity operator in \mathbb{C}^n . This definition holds for infinite dimensional spaces \mathcal{H}_A and \mathcal{H}_B .

With these two definitions, we define a *channel*⁵⁻⁷ as a linear bounded map from $\Gamma(\mathcal{H}_A)$ to $\Gamma(\mathcal{H}_B)$ that is both trace preserving and completely positive. The C–Q channels are special cases.

Definition 9 *Complementary channel and Entropy exchange.* For a channel $\Phi : \Gamma(\mathcal{H}_A) \rightarrow \Gamma(\mathcal{H}_B)$, there exists a Hilbert space \mathcal{H}_E and an isometry $V : \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$, such that

$$\Phi(S) = \text{Tr}_E(VSV^*), \tag{32}$$

where Tr_E is the partial trace wrt space \mathcal{H}_E . (32) is known as the *Stinespring representation* of the channel Φ . Similarly we have the channel

$$\Psi(S) = \text{Tr}_B(VSV^*), \tag{33}$$

called the *complementary channel* of Φ . The *entropy exchange* of state S wrt Φ , is

$$H(S; \Phi) = H(\Psi(S)). \tag{34}$$

We provide some examples of channels that would be useful later.

Definition 10 For finite $\dim(\mathcal{H}_A)$, the channel $\Phi(S) = (1 - p)S + p\Pi$, where $0 < p < 1$ and Π is the maximally mixed state, is called a *depolarizing channel*.

Definition 11 *Degradable and Anti-Degradable Channels.*^{5,7} Channel Φ is *degradable* if there exists a channel Ψ such that $\tilde{\Phi} = \Psi \circ \Phi$, where $\tilde{\Phi}$ is the complementary channel of Φ . Similarly, Φ is *antidegradable* if $\tilde{\Phi}$ is degradable.

Definition 12 *Entanglement Breaking Channels.*^{5,7} A channel Φ is *entanglement breaking* if for any input state S_{AB} , $(\Phi \otimes I_d)S_{AB}$ is separable.

All entanglement breaking channels are anti-degradable.

Definition 13 A channel Φ is (*irreducible*) *gauge covariant* if there exists a continuous, projective, unitary (irreducible) representation $g \mapsto V_g$ of a symmetric group \mathcal{G} in \mathcal{H} such that

$$\Phi(V_g \rho V_g^*) = U_g \Phi(\rho) U_g^*,$$

where U_g is a unitary operator. Similarly, Φ is *gauge contravariant* if $\Phi(V_g \rho V_g^*) = U_g^* \Phi(\rho) U_g$.

4.1 Classical Capacity

Block code Σ^n for n channel uses of this channel is a C–Q channel that maps message i to state $S_i^{(n)}$ of $\mathcal{H}_A^{\otimes n}$ and measurement $M^{(n)}$ on Hilbert space $\mathcal{H}_B^{\otimes n}$ decoding output state $\Phi^{\otimes n}(S_i^{(n)})$ to classical message j . The probability of decoding j given message i is $\text{Tr}(\Phi^{\otimes n}(S_i^{(n)})M_j^{(n)}) \triangleq P(\Sigma^n, M^{(n)}, (i, j))$.

The maximum probability of error for this code is

$$P_e(\Sigma^n, M^{(n)}) = \max_i (1 - P(\Sigma^n, M^{(n)}, (i, i))).$$

Define $P_e(n, 2^{nR}) = \min_{\Sigma^n, M^{(n)}} P_e(\Sigma^n, M^{(n)})$.

Definition 14 The *classical capacity* $C(\Phi)$ of the quantum channel Φ is the supremum of rates R , such that $\lim_{n \rightarrow \infty} P_e(n, 2^{nR}) = 0$.

For a fixed probability $\Pi^{(n)}$ on the input alphabet and observations $M^{(n)}$, the classical capacity can be obtained via Shannon’s Theorem. Let $\mathcal{J}_n(\Pi^{(n)}, M^{(n)})$ be the classical mutual information between input and output for n channel uses. Then, the classical capacity of the channel is

$$C(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{\Pi^{(n)}, M^{(n)}} \mathcal{J}_n(\Pi^{(n)}, M^{(n)}). \tag{35}$$

From classical information theory², $C(\Phi)$ is the maximum number of bits that can be transmitted on this channel with arbitrarily low probability of error.

In contrast to C–Q channels, there is no fixed input alphabet \mathcal{X} , so we need to optimize over states $\{S_i^{(n)}\}$ also. Let us define

$$C_{\mathcal{X}}(\Phi) = \sup_{\Pi} \left\{ H \left(\sum_i \Pi_i \Phi(S_i) \right) - \sum_i \Pi_i H(\Phi(S_i)) \right\} \tag{36}$$

$$\leq \sup_S H(\Phi(S) - \min_S H(\Phi(S))), \tag{37}$$

where $C_\chi(\Phi)$ is known as the *Holevo Capacity* of channel Φ and $\min_S H(\Phi(S))$ the minimal output entropy of Φ .

Theorem 3 Holevo Schumacher Westmoreland (HSW) Theorem^{50,51}. For finite-dimensional Hilbert spaces, we get

$$C(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}). \tag{38}$$

□

In general $C_\chi(\Phi_1 \otimes \Phi_2) \geq C_\chi(\Phi_1) + C_\chi(\Phi_2)$. Strict inequality may hold because an entangled input to $\Phi_1 \otimes \Phi_2$ may increase the mutual information with output compared to any product input states. If the Holevo capacity is additive for channel Φ , i.e., $C_\chi(\Phi \otimes \Psi) = C_\chi(\Phi) + C_\chi(\Psi)$ for any channel Ψ , then $C_\chi(\Phi^{\otimes n}) = nC_\chi(\Phi)$ for every $n \geq 1$ and hence $C(\Phi) = C_\chi(\Phi)$. This, for instance, holds for all C-Q, entanglement breaking and depolarizing channels. From this, we obtain Theorem 1.

By subadditivity of entropy, $\max_{S^{(n)}} H(\Phi^{\otimes n}(S^{(n)})) = n \max_S H(\Phi(S))$. Thus from (37), $C_\chi(\Phi^{\otimes n}) = nC_\chi(\Phi)$ if we have equality in (37) and the minimal output entropy is additive. Equality in (37) holds for irreducibly covariant and contravariant channels.

Once again, for infinite-dimensional Hilbert spaces, we impose a finite input energy constraint as for the C-Q channel. Let F be an operator of type \mathcal{F} on \mathcal{H}_A . Consider the input states $S^{(n)}$ of channel $\Phi^{\otimes n}$ that satisfy

$$\text{Tr}(S^{(n)} F^{(n)}) \leq nE, \tag{39}$$

for some finite $E > 0$, where

$$F^{(n)} = F \otimes I^{\otimes n-1} + I \otimes F \otimes I^{\otimes n-2} + \dots + I^{\otimes n-1} \otimes F. \tag{40}$$

Theorem 4^{6,66} Let Φ satisfy

$$\sup_{S: \text{Tr}(SF) \leq E} H(\Phi(S)) < \infty, \tag{41}$$

where F is an operator of type \mathcal{F} satisfying conditions of Lemma 1. Then the classical capacity $C(\Phi, F, E)$ of Φ is finite and

$$C(\Phi, F, E) = \lim_{n \rightarrow \infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}, F^{(n)}, nE) \tag{42}$$

where

$$C_\chi(\Phi, F, E) = \sup_{\Pi: \text{Tr}(\bar{S}_\Pi F) \leq E} \left\{ H(\Phi(\bar{S}_\Pi)) - \sum_i \Pi_i H(\Phi(S_i)) \right\} \tag{43}$$

and $\bar{S}_\Pi = \int \Pi(dx) S_x$ □

For entanglement breaking channels, $C(\Phi, F, E) = C_\chi(\Phi, F, E)$.

In the following, we will describe Gaussian Bosonic channels in detail. However, first we consider an important Bosonic non-Gaussian channel which models decoherence in fiber optic channels and some quantum circuits. Decoherence in fiber optic channels can occur due to Kerr non-linearities and imprecision in path length. An m -mode Bosonic dephasing channel maps a state ρ to a state

$$\int_{-\pi}^{\pi} d^m(\phi) p(\phi) \exp(-i \sum_{j=1}^m a_j^\dagger a_j \phi_j) \rho \exp(i \sum_{j=1}^m a_j^\dagger a_j \phi_j), \tag{44}$$

where $\phi = (\phi_1, \dots, \phi_m)$ and p is a probability density on $[-\pi, \pi]^m$. This is a degradable channel. For the $m = 1$ case and energy constraint E^{41} ,

$$C(\Phi, F, E) = C_\chi(\Phi, F, E) = g(E). \tag{45}$$

In⁶⁷, another infinite-dimensional general non-Gaussian Bosonic channel is considered. Even though C_χ is non-additive in this case, tight upper and lower bounds on classical capacity are obtained.

4.2 Gaussian Channel

In this section, we specialize quantum channels to Gaussian quantum channels. The optical channels (fiber optic as well as free space channels) used in practice are Gaussian quantum channels. Gaussian channels also model natural physical phenomena such as linear photon amplification / loss and adding thermal noise. Often, nonlinear operations can also be accurately approximated by Gaussian channels.

First, we generalize the concepts of single mode Bosonic and Gaussian states^{6,62,65}. We consider $\mathcal{H} = L^2(\mathbb{R}^d)$, where \mathbb{R}^d is the coordinate space of the underlying classical system. For each co-ordinate j , we define q_j and p_j , position and momentum operators resp., as before and specify frequency $\omega_j \neq 0$. Define for $x = (x_1, \dots, x_d)$, $y = (y_1, \dots, y_d)$,

$$\begin{aligned}
 V_x &= \exp\left(i \sum_{j=1}^d x_j q_j\right), \\
 U_y &= \exp\left(i \sum_{j=1}^d y_j p_j\right), \\
 W(z) &= \exp\left(\frac{i}{2} y^T x\right) V_x U_y,
 \end{aligned}
 \tag{46}$$

where $W(z)$ is called the *Weyl operator* and $z = (x_1, y_1, x_2, y_2, \dots, x_d, y_d)$. For z, z' , define

$$\Delta(z, z') = \sum_j (x_j y'_j - x'_j y_j).
 \tag{47}$$

The space $Z = \mathbb{R}^{2d}$ with non-degenerate skew symmetric $\Delta(z, z')$ is called a *symplectic* vector space of the classical system corresponding to the quantum system. $W(z)$ is a multimodal generalization of displacement operator $D(z)$.

A quantum state on Z will be called a general Bosonic state with d modes. Its characteristic function is

$$\phi_S(z) \triangleq \text{Tr}(SW(z)), \quad z \in \mathbb{R}^{2d}.
 \tag{48}$$

This is called the *non-commutative Fourier transform*. The state S can be uniquely obtained from $\phi_S(z)$ using the following inversion formula:

$$S = \frac{1}{(2\pi)^d} \int \phi_S(z) W(-z) d^{2d}z.
 \tag{49}$$

The state S is a *general d mode Gaussian state* if its characteristic function is of the following form:

$$\phi(z) = \exp\left(imz - \frac{1}{2}\alpha(z, z)\right),
 \tag{50}$$

where $\alpha(z, z) = z^T \alpha z$. If $m = 0$, we call the state *centered*, denoted by S_0 . For $\phi(z)$ to be a Gaussian state, it is necessary and sufficient that $\alpha \geq \pm \frac{i\Delta}{2}$. The corresponding Gaussian state is then given by

$$S_m = W(-\Delta^{-1}m^T)S_0W(-\Delta^{-1}m^T)^*.
 \tag{51}$$

A general Gaussian S_m can be decomposed into elementary one-mode Gaussian states as

$$S = \bigotimes_{j=1}^d S^{(j)}.
 \tag{52}$$

State S is *pure* iff each of $S^{(j)}$ is pure. The entropy of S is given by

$$H(S) = \sum_{j=1}^d H(S^{(j)}).
 \tag{53}$$

A Gaussian state has maximum entropy of all states with mean m and covariance α .

A multimode Bosonic channel^{6,65,68} can be best described via its Stinespring dilation. The channel Φ from \mathcal{H}_A to \mathcal{H}_B will be described by associating with its environment \mathcal{H}_D (at the input) and \mathcal{H}_E at the output. Let the corresponding symplectic spaces be Z_A, Z_B, Z_D and Z_E . Also note that $\mathcal{H}_A \otimes \mathcal{H}_D = \mathcal{H}_B \otimes \mathcal{H}_E$. It evolves according to symplectic transformation

$$T = \begin{bmatrix} K & L \\ K_D & L_D \end{bmatrix},
 \tag{54}$$

with $K : Z_B \rightarrow Z_A, L : Z_E \rightarrow Z_A, K_D : Z_B \rightarrow Z_D$ and $L_D : Z_E \rightarrow Z_D$. The characteristic function $\phi_B(z_B)$ of the output state is related to the characteristic function $\phi_A(z_A)$ of the input state by

$$\phi_B(z_B) = \phi_A(Kz_B)f(z_B),
 \tag{55}$$

$$f(z_B) = \phi_D(K_Dz_B).
 \tag{56}$$

If additionally,

$$f(z_B) = \exp(il(z_B) - \frac{1}{2}\alpha(z_B, z_B)),
 \tag{57}$$

where $l(z_B) = m_D(K_Dz_B)$ and $\alpha(z_B, z'_B) = \alpha_D(K_Dz_B, K_Dz'_B)$, the channel is called a *Gaussian channel* with parameters (K, l, α) provided $\alpha \geq \pm \frac{i}{2}(\Delta_B - K^T \Delta_A K)$. Here α_D is the covariance of the Gaussian input environment noise.

Gaussian channels transform Gaussian states to Gaussian states via relations

$$m_B = m_A K + l, \quad \alpha_B = K^T \alpha_A K + \alpha,
 \tag{58}$$

where m_A and α_A are mean and variance of the input state and m_B and α_B of the output state. Without loss of generality, we can take $l = 0$. A concatenation of Gaussian channels is a Gaussian channel.

A general Bosonic Gaussian channel is irreducibly gauge covariant / contravariant if it satisfies the conditions of Definition 13 under the $z \rightarrow W(z)$ group. Gaussian channel $(K, 0, \alpha)$ is *gauge covariant* if there exists an operator J in (Z, Δ) with $J^2 = -I$ such that $[K, J] = 0$ and $[\Delta^{-1}\alpha, J] = 0$.

A Gaussian channel $(K, 0, \alpha)$ is entanglement breaking if and only if α admits a decomposition $\alpha = \alpha_A + \alpha_B$, where $\alpha_A \geq \frac{i}{2}K^T \Delta_A K$ and

$\alpha_B \geq \frac{i}{2} \Delta_B$ ⁶. Thus if $K^T \Delta_A K = 0$, then the channel is entanglement breaking.

For Gaussian channels taking $F = R\epsilon R^T$, where ϵ is a positive definite matrix and $R = (q_1, p_1, \dots, q_d, p_d)^T$, satisfies the conditions of Theorem 4. However, for a general Gaussian channel, computing the classical capacity from (43) explicitly is possible only if additivity of Holevo capacity holds. Due to this, the classical capacity of general Gaussian channels is unknown. More recently, it was shown⁵⁹ that for a Gaussian gauge-covariant or contravariant channel, with finite second moment, the minimal output entropy of the channel is additive and attained at a Gaussian state. Thus, for such channels, the Holevo capacity is additive⁶ and hence $C(\Phi, F, E) = C_\chi(\Phi, F, E)$. It is also true for entanglement breaking channels. Gaussian gauge contravariant channels are entanglement breaking.

However, it is challenging to even compute $C_\chi(\Phi, F, E)$ except for C-Q channels and Gauge symmetric channels⁶.

4.2.1 Single Mode Gaussian Channels

As mentioned earlier, a Gaussian channel can be characterized by (K, l, α) . If we take $l = 0$ the characteristic function of the output state simplifies to

$$\phi_B(z) = \phi_A(Kz) \exp\left(-\frac{1}{2}z^T \alpha z\right). \tag{59}$$

For single mode, the Gaussian channels can be classified as follows. Let I_k denote the identity matrix in k dimensions.

Theorem 5 ^{6,62} *Let N_0 be the mean number of photons in the environment. Then all single mode Gaussian channels can be classified into one of the following classes:*

- (A1) $K = 0, \alpha = (N_0 + \frac{1}{2})I_2, N_0 \geq 0$.
- (A2) $K = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \alpha = (N_0 + \frac{1}{2})I_2, N_0 \geq 0$.
- (B1) $K = I_2, \alpha = \frac{1}{2}(N_0 + \frac{1}{2})I_2$.
- (B2) $K = I_2, \alpha = N_c I_2, N_c \geq 0$.
- (C) $K = kI_2, k > 0, k \neq 1, \alpha = \left(N_0 + \frac{k^2-1}{2}\right)I_2$.
- (D) $K = k \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, k > 0, k \neq 1, \alpha = \left(N_0 + \frac{k^2+1}{2}\right)I_2. \square$

The above channels can be related to the environment as follows. If the input state is described by canonical variables q and p , the environment as Gaussian states described by q_E and p_E , the output states by q' and p' , and environment states at the output by q'_E and p'_E , then the above channels can be specified by the following maps:

- (A1) Completely depolarizing: $q' = q_E, p' = p_E$.
- (A2) A degenerate classical signal q with additive quantum Gaussian noise q_E : $q' = q + q_E, p' = p_E$.
- (B1) Quantum signal plus degenerate classical Gaussian noise: $q'_E = q, p'_E = p - p_E$. p_E has variance $\frac{1}{2}$ and (q_E, p_E) is in vacuum state. It is the complementary channel of (A2).
- (B2) Non-degenerate additive classical Gaussian noise. $q' = q + \zeta, p' = p + \eta$, where ζ, η are i.i.d. Gaussian with mean 0 and variance N_c .
- (C) Attenuation (if $k < 1$), with quantum noise:

$$q' = kq + \sqrt{1-k^2}q_E, p' = kp + \sqrt{1-k^2}p_E. \tag{60}$$

Amplification (if $k > 1$), with quantum noise:

$$q' = kq + \sqrt{k^2-1}q_E, p' = kp + \sqrt{k^2-1}p_E. \tag{61}$$

- (D) Attenuation / amplification with phase conjugation: $q' = q, p' = -p$.

For these channels we take $F = a^\dagger a$ and then the energy constraint $\text{Tr}(SF) \leq E$ is the mean number of photons in the input state $\leq E$. Then the conditions of Theorem 4 are satisfied. Channels (A1), (B2) and (C) are gauge covariant and channel (D) is gauge contravariant. Thus, $C(\Phi, F, E) = C_\chi(\Phi, F, E)$. Also (A1), (A2), (D) and (C) with $k \leq \frac{1}{\sqrt{2}}$ are anti-degradable.

Channels (B1), (B2), (C) are also called *phase insensitive Bosonic Gaussian channels*. In particular, channel (C) is called *quantum thermal channel*. For applications, (C) and (B2) are most interesting. Channel (C) with $k < 1$ represents a fiber optic channel and for $k > 1$, a linear optical amplifier. Maximization in $C_\chi(\Phi, F, E)$ is a finite-dimensional optimization problem which is the quantum analog of *waterfilling* in classical information theory.

For channels (B2) and (C)⁶, more explicitly,

$$C(\Phi, F, E) = g(k^2E + N_C + \max(0, k^2 - 1)) - g(N_C + \max(0, k^2 - 1)), \tag{62}$$

where $N_C = |k^2 - 1|N_0$ and $g(\cdot)$ is as defined in (21). When $N_C = 0$ and $k < 1$, we have a pure loss channel and then $C(\Phi, F, E) = g(k^2E)$. A pure loss channel with $k \geq \frac{1}{\sqrt{2}}$ is degradable.

For channel (B2), $k = 1$ and (62) simplifies to $C(\Phi, F, E) = g(E + N_C) - g(N_C)$.

4.3 Entanglement-Assisted Classical Capacity

One can increase the classical capacity of a quantum channel by apriori preparing an entangled state between the transmitter and the receiver. Of course preparing an initial entangled state has a cost which is not considered in the following:

Let $\Phi : \Gamma(\mathcal{H}_A) \rightarrow \Gamma(\mathcal{H}_B)$ be a quantum channel. Let S_{AB} be an entangled pure state on $\mathcal{H}_A \otimes \mathcal{H}_B$. Classical message i arriving with probability Π_i is encoded into ε_A^i on \mathcal{H}_A and this acts as operation

$$(\varepsilon_A^i \otimes I_B)(S_{AB}) \triangleq S_{AB}^i. \tag{63}$$

The input part of this state is sent on Φ and measurements are made at the receiver to get the classical information. The maximum rate transmissible via this protocol is called the *entanglement assisted classical capacity* $C_{ea}(\Phi)$.

Theorem 6 ^{5,7,52} For a finite dimensional \mathcal{H}_A ,

$$C_{ea}(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} C'_{ea}(\Phi^{\otimes n}) = I(S_A; \Phi), \tag{64}$$

where

$$C'_{ea}(\Phi) = \sup_{\Pi_i, \varepsilon_A^i, S_{AB}^i} \chi(\Pi, (\Phi \otimes I_B)S_{AB}^i), \tag{65}$$

$$\chi(\Pi, \Psi(S)) = H\left(\sum_i \Pi_i \Psi(S_i)\right) - \sum_i \Pi_i H(\Psi(S_i)) \text{ and} \tag{66}$$

$$I(S_A; \Phi) = H(S_A) + H(\Phi(S_A)) - H(S_A; \Phi). \tag{67}$$

□

One can show that

$$C_\chi(\Phi) \leq C_{ea}(\Phi) \leq \log d + C_\chi(\Phi), \tag{68}$$

where $d = \dim(\mathcal{H}_A)$. Also, $C(\Phi) \leq C_{ea}(\Phi)$.

For $\dim(\mathcal{H}_A) = \infty$, the entanglement-assisted classical capacity for the constrained input channel is given by the following theorem:

Theorem 7 ^{6,69} Let F be an operator satisfying $\text{Tr}(\exp(-\theta F)) < \infty$ for all $\theta > 0$. Let F' be a self adjoint operator of type \mathcal{F} satisfying $\text{Tr}(\exp(-\theta F')) < \infty$ for all $\theta > 0$ and $\text{Tr}(\Phi(S)F') \leq \text{Tr}(SF)$, for all $S \in \mathcal{S}(\mathcal{H}_A)$. Then

$$C_{ea}(\Phi, F, E) = \max_{S: \text{Tr}(SF) \leq E} I(S; \Phi), \tag{69}$$

where $I(S; \Phi) = H(S) + H(\Phi(S)) - H(S; \Phi)$ and $H(S; \Phi)$ is the entropy exchange.

Moreover, if $\sup_{S \in \mathcal{S}(\mathcal{H}_A)} I(S; \Phi) = \infty$, then the sup is achieved on a density operator S with $\text{Tr}(SF) = E$. □

For the Gaussian channel, if the input is restricted to the set of states with mean m and covariance α , then from Theorem 7, the entanglement-assisted classical capacity is

$$\sup_{S \in \Sigma(m, \alpha)} I(S; \Phi) \tag{70}$$

and the max is attained on a Gaussian state.

For channels (B2) and (C), taking $F = a^\dagger a$, we obtain for $\text{Tr}(SF) \leq E$, from the following Theorem 7:

$$C_{ea}(\Phi) = g(E) + g(E') + g\left(\frac{D + E' - E - 1}{2}\right) + g\left(\frac{D - E' + E - 1}{2}\right), \tag{71}$$

where $E' = k^2E + \max(0, k^2 - 1) + N_C$ and $D = ((E + E' + 1)^2 - 4k^2E(E + 1))/2$. The energy constraint implies that E is the mean number of photons of the signal. From (62) and (71), for channel (C),

$$1 \leq \frac{C_{ea}(\Phi)}{C(\Phi)} \rightarrow \infty \tag{72}$$

as $E \rightarrow 0$ when $\max(0, k^2 - 1) + N_C > 0$. Thus entanglement can significantly increase the capacity when signal energy is low. For $N_C = 0$, $k < 1$, the pure loss channel⁷⁰,

$$C_{ea}(\Phi, F, E) = g(E) + g(k^2E) - g((1 - k^2)E), \tag{73}$$

and $\frac{C_{ea}(\Phi, F, E)}{C(\Phi, F, E)} \rightarrow 2$ as $E \rightarrow 0$.

5 Quantum Capacity

The above capacity results are the fundamental limits on transmitting classical information on quantum channels. Limits on transmission of quantum information are also considered. Correspondingly, there are quantum capacity and entanglement assisted quantum capacity.

Consider Hilbert spaces \mathcal{M} and \mathcal{N} . Consider an isometric map $V : \mathcal{M} \rightarrow \mathcal{N}$. A quantum code is a map, $\varepsilon : S \mapsto VSV^*$. Repetition codes cannot be used due to no-cloning theorem.

Definition 15 Quantum Capacity. Consider a quantum channel $\Phi : \Gamma(\mathcal{H}_A) \rightarrow \Gamma(\mathcal{H}_B)$. A rate R is achievable if there exist Hilbert spaces $\mathcal{H}^{(n)}$ such that

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log \dim(\mathcal{H}^{(n)}) = R$$

and a sequence of encodings

$$\mathcal{E}^{(n)} : \Gamma(\mathcal{H}^{(n)}) \rightarrow \Gamma(\mathcal{H}_A^{\otimes n})$$

and decodings

$$\mathcal{D}^{(n)} : \Gamma(\mathcal{H}_B^{\otimes n}) \rightarrow \Gamma(\mathcal{H}^{(n)})$$

such that

$$\lim_{n \rightarrow \infty} F_s(\mathcal{H}^{(n)}, \mathcal{D}^{(n)} \circ \Phi^{\otimes n} \mathcal{E}^{(n)}) = 1,$$

where F_s is the subspace fidelity, a measure of closeness of two spaces and is defined as

$$F_s(\mathcal{H}, \Phi) = \min_{\psi \in \mathcal{H}, \|\psi\|=1} \langle \psi | \Phi(|\psi\rangle\langle\psi|) \psi \rangle. \tag{74}$$

The supremum of all achievable rates here is the quantum capacity $Q(\Phi)$ of the channel Φ .

$Q(\Phi)$ is the maximum number of qubits per channel use that can be transmitted on the channel Φ reliably.

Define the coherent information as

$$I_C(S; \Phi) = H(\Phi(S)) - H(S; \Phi). \tag{75}$$

Theorem 8 ^{5,7,71,72} For finite-dimensional \mathcal{H}_A , we have

$$Q(\Phi) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_S I_C(S; \Phi^{\otimes n}). \tag{76}$$

□

Since $I_C(S; \Phi) \leq C_\chi(\Phi; S)$, $Q(\Phi) \leq C(\Phi)$.

If Φ is degradable, then $I_C(S; \Phi) \geq 0$. Also then $I_C(S; \Phi^{\otimes n}) = nI_C(S; \Phi)$ and $Q(\Phi) = \max_S I_C(S; \Phi)$ ⁷². If Φ is antidegradable, then $I_C(S; \Phi) \leq 0$ and hence it has a Quantum

Capacity of 0. Note that while coherent information could be negative, quantum capacity cannot be.

A unique aspect of quantum capacity is *superactivation*. We can have two channels Φ_1 and Φ_2 such that $Q(\Phi_1) = Q(\Phi_2) = 0$ but $Q(\Phi_1 \otimes \Phi_2) > 0$ ⁷. This is not possible in classical information theory.

For $\dim(\mathcal{H}_A) = \infty$, $Q(\Phi)$ defined by (76) is still finite even without any energy constraint. $Q(\Phi)$ with input energy constraint $\text{Tr}(SF) \leq E$ can be shown to be

$$Q(\Phi, F, E) = \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{S: \text{Tr}(SF) \leq E} I_C(S; \Phi^{\otimes n}), \tag{77}$$

under the conditions of Theorem 4⁴². For degradable channels, $Q(\Phi, F, E) = \sup_{\text{Tr}(SF) \leq E} I_C(S; \Phi)$.

Since m -mode Bosonic dephasing channel is degradable, its quantum capacity without energy constraint is⁴¹ $m \log_2(2\pi) - h(p)$, where $h(p)$ is the classical differential entropy of p . Under energy constraint E , $Q(\Phi, F, E)$ is unavailable but is upper bounded by $m \log_2(2\pi) - h(p)$.

The maximal achievable rate with the assistance of entanglement between the transmitter and the receiver states (as is for C_{ea}) is called the *entanglement-assisted quantum capacity* $Q_{ea}(\Phi)$. Using quantum teleportation and dense coding, we can show that $Q_{ea}(\Phi) = \frac{1}{2} C_{ea}(\Phi)$ ^{5,7}. Also $Q(\Phi) \leq Q_{ea}(\Phi)$. This holds for infinite-dimensional channels as well.

5.1 Gaussian Channels

If Φ is a degradable Gaussian channel, $Q(\Phi) = \sup_S I_C(S; \Phi)$ is achievable by taking the supremum over all Gaussian states with mean m and covariance α , where m and α satisfy the energy constraints. Its explicit expression for phase insensitive channels is provided in⁴².

Regarding single-mode Gaussian channels provided in Theorem 5, the channels (A1), (A2) and (D) are antidegradable and hence have zero quantum capacity. Moreover, it is known that for Gaussian channels Φ of type (C) without any energy constraints⁴⁶

$$Q(\Phi) = 0, \quad \text{if } k \leq \frac{1}{\sqrt{2}} \text{ or } k \geq \frac{1}{\sqrt{2}} \tag{78}$$

and $N_C \geq \frac{1}{2}(k^2 - |k^2 - 1|)$.

Under above conditions, channel (C) is degradable. For $1 \geq k^2 \geq \frac{N_0+1}{N_0+2}$, from⁷³, channel (C) is not degradable but we have $Q(\Phi) \leq -\log 2((1-k^2)k^{N_0}) - g(N_0)$. There are other upper bounds for channel (C) in⁷³.

For $N_C = 0$, $k^2 \in [\frac{1}{2}, 1]$, with mean number

of photons in input state $\leq E$, we get the quantum capacity from (77) as $g(k^2E) - g((1-k^2)E)$. This can be taken as an upper bound for the channel with $N_C > 0$ and energy constraint E . For $N_C = 0$, taking $E \rightarrow \infty$, we get $\log \frac{k^2}{1-k^2}$. Furthermore, from⁴², we can generalize it to an m mode parallel pure loss channel with energy constraint E . Then

$$Q(\Phi) = \sum_{j=1}^m g(k^2 N_j(\beta)) - g((1-k^2) N_j(\beta)), \tag{79}$$

where $N_j(\beta) = \frac{1}{e^{\beta \omega_j} + 1}$ and β is such that

$\sum_{j=1}^m N_j(\beta) = E$. Here ω_j is the frequency of the j^{th} mode of the channel. The result extends to the case when k_j , for mode j , are different, each satisfy $k_j^2 \in [\frac{1}{2}, 1]$.

An example of superactivation in Gaussian channels is provided in⁷⁴.

6 Modeling Optical Light and Channels

Consider electromagnetic wave (EM wave) in free space, transmitted by a transmitter in $z = 0$ plane, in pupil \mathcal{A}_0 , and measured by a receiver in $z = L$ plane, in pupil \mathcal{A}_L during time $0 \leq t \leq T$. Then^{48,62,65,75} the electric field at input, in normal mode decomposition, can be written as

$$E_0(\rho, t) = \sum_{n,m} c_{n,m} \Phi_n(\rho) \theta_m(t), \tag{80}$$

$$\rho \in \mathcal{A}_0, \quad 0 \leq t \leq T,$$

and at the receiver as

$$E_L(\rho, t) = \sum_{m,n} k_n c_{n,m} \Psi_n(\rho) \theta_m\left(t - \frac{L}{c}\right), \tag{81}$$

$$\rho \in \mathcal{A}_L, \quad 0 \leq t - \frac{L}{c} \leq T,$$

where $0 \leq k_n \leq 1$, $\{\theta_m(t)\}$ are a completely orthonormal set of functions, Φ_n and Ψ_n are the input and output eigenfunctions respectively

(independent of the input field applied) and c is the speed of light. The corresponding quantized electric fields are

$$\widehat{E}_0(\rho, t) = \sum_{n,m} a_{n,m} \Phi_n(\rho) \theta_m(t), \tag{82}$$

at $z = 0$ and

$$\widehat{E}_L(\rho, t) = \sum_{m,n} (k_n a_{n,m} + \sqrt{1-k_n^2} e_{n,m}) \Psi_n(\rho) \theta_m\left(t - \frac{L}{c}\right), \tag{83}$$

for $z = L$, where $0 \leq k_n \leq 1$; $a_{n,m}$ are the annihilator operators at the input corresponding to coefficients $c_{m,n}$ and $e_{n,m}$ are annihilator operators from the environment. Thus the state of the input field can be described by the joint density operator $a_{n,m}$ and that of the output field by $b_{n,m} = k_n a_{n,m} + \sqrt{1-k_n^2} e_{n,m}$. The mapping from $\{a_{n,m}\}$ to $\{b_{n,m}\}$ defines the channel for this optical system.

If $\widehat{E}_0(\rho, t)$ has only one term then it is a single-mode Bosonic channel, a beam-splitter discussed in more detail in next subsection. If e_{11} is in a vacuum state then it is a Gaussian (C) class pure loss channel (because now $N_c = 0$). If e_{11} is in a thermal state then it is called a thermal noise channel. The $C(\Phi, F, E)$ of the channels is provided in (62) and $C_{ea}(\Phi, F, E)$ in (71). For pure loss channel, results are given more explicitly. For $k \geq \frac{1}{\sqrt{2}}$, the pure loss channel is degra-

dable and hence its quantum capacity has single-letter characterization and is provided in the discussion preceding (79). For $k < \frac{1}{\sqrt{2}}$, it is

antidegradable and hence has quantum capacity 0.

When there is more than one term in (83), and each mode is a pure loss mode with corresponding $k_{mn}^2 \in [\frac{1}{2}, 1]$, then the quantum capac-

ity can be obtained from (79), modified for different k_{mn} .

For classical capacity with energy constraints, if the general m -mode channel is with $e_{n,m}$ in vacuum states, we obtain Bosonic Gaussian covariant channel and hence from the results of Section 4, $C(\Phi, F, E) = C_\chi(\Phi, F, E)$ and is attained via Gaussian input. Thus we can compute it numerically. For single mode, it equals $g(k^2E)$. For

multimode case, we need to optimize the energy used in different modes. Similarly, one can obtain $C_{ea}(\Phi, F, E)$ from Sect. 4.3.

6.1 Optical Systems as Gaussian Quantum Systems

Coherent state $|\alpha\rangle$, $\alpha \in \mathbb{C}$ is eigenstate of a with eigenvalue α . It is a special case of a Gaussian state (when $var = 0$), models a state of an ideal laser light beam. The simplest state $|0\rangle$ is the vacuum state. The coherent states are min uncertainty states of p and q . For $\alpha \in \mathbb{C}$, the coherent state $|\alpha\rangle$ can be expanded in basis $\{|n\rangle\}$ as

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{84}$$

$$= \exp(\alpha a^\dagger - \alpha^* a) |0\rangle. \tag{85}$$

It has average number of photons

$$\mu = \langle \alpha | a^\dagger a | \alpha \rangle = |\alpha|^2, \tag{86}$$

also called its intensity.

A coherent state can also be characterized by its intensity μ and phase θ by

$$|\mu, \theta\rangle = \exp(\sqrt{\mu} e^{i\theta} a^\dagger - \mu/2) |0\rangle. \tag{87}$$

The phase θ of light pulse from an ordinary laser device is random, uniformly distributed on $[0, 2\pi]$. Then a coherent state with intensity μ is a classical mixture with Poisson distribution of photons

$$\rho_\mu = \frac{1}{2\pi} \int_0^{2\pi} |\mu, \theta\rangle \langle \mu, \theta| d\theta = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n|. \tag{88}$$

If μ is small and the state is not $|0\rangle$, then we can approximate it with the first two terms with $n = 0$ and 1 in (88). This is light with a single photon. Coherent states have same variance in p and q coordinates. (see^{6,62,65} for more details).

Thermal states have a representation as described in (19), where N is the mean number of photons in them.

Squeezed states are generalizations of coherent states. In these states, one quadrature may have less uncertainty than the other, resulting in higher uncertainty in the other, due to the uncertainty principle. Then the covariance matrix has one eigenvalue larger than the other.

A single mode squeezed state is

$$|\zeta, 0\rangle = S(\zeta) |0\rangle, \tag{89}$$

where $S(\zeta) = \exp\left(-\frac{\zeta}{2}(a^\dagger)^2 + \frac{\zeta^*}{2}a^2\right)$. If $\zeta = r e^{i\phi}$,

then the covariance matrix is

$$\begin{bmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{bmatrix}. \tag{90}$$

The variance of position is e^{-2r} and of momentum is e^{2r} .

The coherent states and thermal states are like classical sinusoidal states with well-defined amplitude and phase. But Fock states $|n\rangle$ and squeezed states do not have a classical equivalent.

Two-mode squeezed states are very useful and can be used as entangled states. These are generated by the squeezing operator

$$S = \exp(-\zeta^* a_1 a_2 + \zeta a_1^\dagger a_2^\dagger). \tag{91}$$

A beam splitter is a widely used optical device (can be taken as an example of a quantum channel). It has a two-mode input beam and a two-mode output beam. One input mode can be taken in vacuum state and the other in single photon. Thus the input state is $|1\rangle \otimes |0\rangle$. The output state is denoted by

$$|\psi\rangle_{\text{out}} = U_B |10\rangle, \tag{92}$$

where U_B is the operator specified by the beam splitter. A 50 : 50 beam-splitter gives

$$|\psi\rangle_{\text{out}} = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle), \tag{93}$$

i.e., a maximally entangled state. If the input is a coherent state, then the output is a separable state. We can also obtain a two-mode squeezed state at the output given one-mode squeezed state at input. Thus a beam splitter is a very versatile laser device and is used often in quantum information processing.

7 Capacity of Multiuser Channels

The results provided so far are for point-to-point quantum channels. However, just as for classical information theory³⁸, several of these results have been extended to multiuser channel situation. The focus, as in classical case, has been on multiple access channels, broadcast channels, interference channels and general multihop networks of quantum channels. In the following, we only provide the references for the aforementioned channels with brief comments.

We first consider multiple access channels (MAC). In a MAC, multiple users transmit to one receiver. Winter⁷⁶ provided the capacity region for classical information on the C–Q MACs. The capacity region obtained is similar to that of classical MAC⁷⁷ extended this result to a MAC with C–Q channels as well as quantum–quantum (q–q) channels and obtained the capacity results for both classical as well as quantum information. As for point-to-point quantum channels, there are no single-letter characterizations of the capacity region for the general channels. However, for the degradable channel, single-letter characterizations were obtained. In⁷⁸, capacity of entanglement-assisted case has been studied for quantum–quantum MACs with two users⁷⁹ studies a MAC with classical inputs and quantum outputs with discrete or continuous variables⁸⁰ studies finite-dimensional and Bosonic thermal noise channels with more than two users.

The broadcast channel consists of one transmitter and multiple receivers.⁸¹ studied this channel when classical information is transmitted to multiple users over quantum channels. Inner and outer bounds on the capacity region are provided. Next, they consider the case when information transmitted to some of the users is classical while for others quantum.

In⁸², an interference channel is considered where there are two transmitters and two receivers. Each transmitter transmits to one of the receivers (no common receiver) and acts as an interference to the other. For such channels, even in classical information theory, the capacity of the information to individual users is known only in special cases⁸² generalizes this channel to the quantum setting. The case when the classical inputs are provided and quantum outputs received (C–Q channel) is studied in detail. Capacity of the channel is obtained for the very strong and strong interference case, as in the classical setting. Han–Kobayashi (see^{2,38}) type of results are also obtained.

Savov's PhD Thesis⁸³ considers several networks of C–Q channels. In these networks, classical inputs are provided and the network outputs quantum signals. Thus classical encoding with quantum decoding is used. Multiple access, broadcast, interference and relay channels are considered in the finite-dimensional setting. These results can be extended to quantum input and quantum output channels. Savov's thesis also considers Bosonic quantum interference channels with classical inputs and continuous variable quantum state outputs.

8 Recent Developments and Future Directions

Capacity in classical and quantum information theory is an asymptotic concept. It provides the supremum on the achievable rates per channel use as the number of channel uses goes to infinity. In practice, we use only a finite number of channel uses. Then the probability of error in transmission will be non-zero for any positive achievable rate and the capacity is not achievable with arbitrarily low probability of error for most channels of interest.

More recently, in classical information theory, for a given probability of error ε , upper and lower bounds on the achievable rate for a given number of channel uses have been obtained^{84,85}. Extensions of these results to quantum systems for finite-dimensional channels have been summarized in^{86–89}. A systematic book-length treatment is provided in⁹⁰ and the upper and lower bounds obtained are used in providing the channel capacity and rates of convergence of the achievable rate to the channel capacity.

The finite-length achievable rates, rates of convergence to the capacity and continuity of capacity for infinite-dimensional channels have been studied in^{58,70,91}. We provide the results of⁷⁰ in more detail. These concern the achievable rates for the classical capacity of C–Q channels for finite block length case.

Consider a C–Q channel $\Phi(x) = S_x$, where $x \in \mathcal{X}$ can be a continuous set and S_x is a state on an infinite dimensional, separable Hilbert space. Let $M^*(\Phi^{\otimes n}, \varepsilon)$ be the maximum size of the codebook that can be transmitted in n channel uses of Φ with probability of error $\leq \varepsilon$, where $0 < \varepsilon < 1$. Then

$$\log M^*(\Phi^{\otimes n}, \varepsilon) \geq nH(\rho) - \sqrt{nV(\rho)}Q^{-1}(\varepsilon) + O(\log n), \quad (94)$$

where ρ the state and $V(\rho)$ are obtained as follows: Let P be a probability density on \mathcal{X} ; then

$$\rho \triangleq E_{x \sim P}[|S_x\rangle\langle S_x|], \quad (95)$$

$$V(\rho) = \text{Var}(-\log P(x)). \quad (96)$$

Also $Q(\cdot)$ is the complementary cdf of a Gaussian distribution with zero mean and unit variance. This lower bound is similar to the second-order expansions of achievable rates in classical information theory.

We apply the inequality (94) to a pure loss bosonic channel with Heisenberg evolution

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}, \quad (97)$$

where $\eta \in [0, 1]$, subject to an input photon number constraint $\text{Tr}(a^\dagger a \rho) \leq N_S$, $N_S > 0$. Now for pure state $|\alpha\rangle$, the output is $|\eta\alpha\rangle$. We take $\eta = 1$ for convenience and distribution P as isotropic complex Gaussian with variance N_S ,

$$P_{N_S}(\alpha) = \frac{1}{\pi N_S} \exp\left(-\frac{|\alpha|^2}{N_S}\right). \quad (98)$$

Then, for the average state ρ ,

$$H(\rho) = g(N_S), \quad (99)$$

$$V(\rho) = N_S(N_S + 1)(\log(N_S + 1) - \log N_S)^2, \quad (100)$$

where $g(\cdot)$ is defined in (20).

For general $\eta \in [0, 1]$, the bound is obtained by replacing N_S with ηN_S .

For more general Bosonic channels, this type of results are unavailable but would be of interest. Notice also that (94) is a lower bound but a non-trivial upper bound is elusive. If we were to apply the upper bound results provided in⁸⁷ and⁸⁸, we would run into issues, such as finite condition numbering, which automatically force the dimensions of the Hilbert spaces to be finite. A suitable upper bound, therefore, would be desirable and the result is likely to resemble (94), as it does in classical information theory for additive white Gaussian noise (AWGN) channels⁸⁵. It would also be worthwhile to study the finite blocklength effects on the second-order terms in the presence of entanglement assistance.

As far as quantum capacity is concerned, there are no results of the finite blocklength type available, except for finite dimensions. In fact, as seen in Sect. 5, we do not even have a proper characterization of $Q(\Phi)$ except for a very specific class of channels. These are most sought after in applications such as QKD and quantum internet.

9 Conclusion

In this survey, we have introduced and discussed QIT for various quantum channels with a focus on Gaussian channels with single mode. We have discussed and compared capacity, both classical and quantum, with and without entanglement assistance for these channels. We have also discussed the multiuser variants of these channels. While the infinite-dimensional space

is useful, as that is where the useful channels lie, it is also significantly more complex than finite-dimensional analysis. As a result, a large number of open issues still remain and for these reasons, this field will be vibrant for many years to come.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Declarations

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

OpenAccess

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Received: 8 June 2022 Accepted: 23 June 2022
Published online: 23 August 2022

References

1. Shannon CE (1948) A mathematical theory of communication. *Bell Syst Tech J* 27(3):379–423
2. Cover TM, Thomas JA (1999) *Elements of information theory*. Wiley
3. Adami C (2012) The use of information theory in evolutionary biology. *Ann N York Acad Sci* 1256(1):49–65
4. Gyongyosi L, Imre S, Nguyen HV (2018) A survey on quantum channel capacities. *IEEE Commun Surv Tutor* 20(2):1149–1205
5. Wilde MM (2016) *Quantum information theory*. Cambridge University Press, Cambridge
6. Holevo AS (2019) *Quantum systems, channels, information*. de Gruyter, 2nd Edition

7. Watrous J (2018) The theory of quantum information. Cambridge University Press, Cambridge
8. Nielsen MA, Chuang IL (2001) Quantum computation and quantum information. *Phys Today* 54(2):60
9. Bennett CH, Wiesner SJ (1992) Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys Rev Lett* 69(20):2881
10. Shapiro JH (2012) Information capacities for optical communications: conventional versus quantum reception. In: Conference on Lasers and Electro-Optics
11. Park JL (1970) The concept of transition in quantum mechanics. *Found Phys* 1(1):23–33
12. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. *Nature* 299(5886):802–803
13. Kalev A, Hen I (2008) No-broadcasting theorem and its classical counterpart. *Phys Rev Lett* 100(21):210502
14. Popescu S, Rohrlich D (1998) Causality and nonlocality as axioms for quantum mechanics. *Causality and locality in modern physics*. Springer, Berlin, pp 383–389
15. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK (1993) Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys Rev Lett* 70(13):1895
16. Boschi D, Branca S, De Martini F, Hardy L, Popescu S (1998) Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys Rev Lett* 80(6):1121
17. Eberhard PH, Ross RR (1989) Quantum field theory cannot provide faster-than-light communication. *Found Phys Lett* 2(2):127–149
18. Lidar DA, Brun TA (2013) Quantum error correction. Cambridge University Press, Cambridge
19. La Guardia GG (2020) Quantum error correction. Springer, Berlin
20. Schumacher B (1995) Quantum coding. *Phys Rev A* 51(4):2738
21. Petz D, Mosonyi M (2001) Stationary quantum source coding. *J Math Phys* 42(10):4857–4864
22. Calderbank AR, Shor PW (1996) Good quantum error-correcting codes exist. *Phys Rev A* 54(2):1098
23. Steane AM (1999) Enlargement of Calderbank–Shor–Steane quantum codes. *IEEE Trans Inform Theory* 45(7):2492–2495
24. Lund AP, Ralph TC, Haselgrove HL (2008) Fault-tolerant linear optical quantum computing with small-amplitude coherent states. *Phys Rev Lett* 100(3):030503
25. Niset J, Andersen UL, Cerf NJ (2008) Experimentally feasible quantum erasure-correcting code for continuous variables. *Phys Rev Lett* 101(13):130503
26. Niset J, Fiurášek J, Cerf NJ (2009) No-go theorem for gaussian quantum error correction. *Phys Rev Lett* 102(12):120501
27. Datta N, Leditzky F (2014) Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions. *IEEE Trans Inform Theory* 61(1):582–608
28. Wilde MM, Datta N, Hsieh M-H, Winter A (2013) Quantum rate-distortion coding with auxiliary resources. *IEEE Trans Inform Theory* 59(10):6755–6773
29. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM* 21(2):120–126
30. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE
31. Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. *Proc IEEE Int Conf Comput Syst Signal Process* 175:8
32. Scarani V, Acin A, Ribordy G, Gisin N (2004) Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys Rev Lett* 92(5):057901
33. Weissberger, A.: Verizon Trials Quantum Key Distribution for Encryption over Fiber Optic Links. <https://techblog.comsoc.org/2020/09/04/verizon-trials-quantum-key-distribution-for-encryption-over-fiber-optic-links/> Accessed 2020-09-04
34. Abushgra AA (2022) Variations of QKD protocols based on conventional system measurements: a literature review. *Cryptography* 6(1):12
35. Grosshans, F., Grangier, P.: Reverse reconciliation protocols for quantum cryptography with continuous variables. arXiv preprint quant-ph/0204127 (2002)
36. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M (2009) The security of practical quantum key distribution. *Rev Mod Phys* 81(3):1301
37. Khan I, Elser D, Dirmeier T, Marquardt C, Leuchs G (2017) Quantum communication with coherent states of light. *Philos Trans R Soc A Math Phys Eng Sci* 375(2099):20160235
38. El Gamal A, Kim Y-H (2011) Network information theory. Cambridge University Press, Cambridge
39. Devetak I, Shor PW (2005) The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun Math Phys* 256(2):287–303
40. Li K, Winter A, Zou X, Guo G (2009) Private capacity of quantum channels is not additive. *Phys Rev Lett* 103(12):120501
41. Lami L, Wilde MM (2022) Exact solution for the quantum and private capacities of bosonic dephasing channels. arXiv preprint [arXiv:2205.05736](https://arxiv.org/abs/2205.05736)
42. Wilde MM, Qi H (2018) Energy-constrained private and quantum capacities of quantum channels. *IEEE Trans Inform Theory* 64(12):7802–7827
43. Kimble HJ (2008) The quantum internet. *Nature* 453(7198):1023–1030

44. Wehner S, Elkouss D, Hanson R (2018) Quantum internet: a vision for the road ahead. *Science* 362(6412):9288
45. Azuma K, Bäuml S, Coopmans T, Elkouss D, Li B (2021) Tools for quantum network design. *AVS Quant Sci* 3(1):014101
46. Pirandola S, Laurenza R, Ottaviani C, Banchi L (2017) Fundamental limits of repeaterless quantum communications. *Nat Commun* 8(1):1–15
47. Shapiro JH, Giovannetti V, Guha S, Lloyd S, Maccone L, Yen BJ (2004) Capacity of bosonic communications. In: *AIP Conference Proceedings*, vol. 734, pp. 15–20. American Institute of Physics
48. Shapiro JH (2009) The quantum theory of optical communications. *IEEE J Select Top Quant Electron* 15(6):1547–1569
49. Holevo AS (1973) Bounds for the quantity of information transmitted by a quantum communication channel. *Probl Pered Inform* 9(3):3–11
50. Holevo AS (1998) The capacity of the quantum channel with general signal states. *IEEE Trans Inform Theory* 44(1):269–273
51. Schumacher B, Westmoreland MD (1997) Sending classical information via noisy quantum channels. *Phys Rev A* 56(1):131
52. Bennett CH, Shor PW, Smolin JA, Thapliyal AV (1999) Entanglement-assisted classical capacity of noisy quantum channels. *Phys Rev Lett* 83(15):3081
53. Schumacher B, Nielsen MA (1996) Quantum data processing and error correction. *Phys Rev A* 54(4):2629
54. Adami C, Cerf NJ (1997) von Neumann capacity of noisy quantum channels. *Phys Rev A* 56(5):3470
55. Holevo AS (1998) Quantum coding theorems. *Russ Math Surv* 53(6):1295
56. Ralph TC, Lam PK (1998) Teleportation with bright squeezed light. *Phys Rev Lett* 81(25):5668
57. Braunstein SL, Kimble HJ (2000) Dense coding for continuous variables. *Quantum information with continuous variables*. Springer, Berlin, pp 95–103
58. Shirokov ME (2017) Tight uniform continuity bounds for the quantum conditional mutual information, for the holevo quantity, and for capacities of quantum channels. *J Math Phys* 58(10):102202
59. Giovannetti V, Holevo AS, Garcia-Patron R (2015) A solution of gaussian optimizer conjecture for quantum channels. *Commun Math Phys* 334(3):1553–1571
60. Holevo AS (2015) Gaussian optimizers and the additivity problem in quantum information theory. *Russ Math Surv* 70(2):331
61. Braunstein SL, Van Loock P (2005) Quantum information with continuous variables. *Rev Mod Phys* 77(2):513
62. Weedbrook C, Pirandola S, García-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, Lloyd S (2012) Gaussian quantum information. *Rev Mod Phys* 84(2):621
63. Pape GC, Blahut RE (2019) *Lightwave communications*. Cambridge University Press, Cambridge
64. Holevo AS (2011) *Probabilistic and statistical aspects of quantum theory*, vol 1, 2nd edn. Springer, Berlin
65. Serafini A (2017) *Quantum continuous variables: a primer of theoretical methods*. CRC Press.
66. Holevo AS (2003) Classical capacities of quantum channels with constrained inputs. *Probab Theory Appl*: 359–374
67. Huber S, König R (2018) Coherent state coding approaches the capacity of non-gaussian bosonic channels. *J Phys A Math Theor* 51(18):184001
68. Caruso F, Eisert J, Giovannetti V, Holevo AS (2008) Multi-mode bosonic gaussian channels. *N J Phys* 10(8):083030
69. Shirokov ME (2006) The holevo capacity of infinite dimensional channels and the additivity problem. *Commun Math Phys* 262(1):137–159
70. Wilde MM, Renes JM, Guha S (2016) Second-order coding rates for pure-loss bosonic channels. *Quant Inform Process* 15(3):1289–1308
71. Shor P (2002) Quantum channel capacity and coherent information. *MSRI Workshop on Quantum Computation*
72. Devetak I (2005) The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans Inform Theory* 51(1):44–55
73. Sharma K, Wilde MM, Adhikari S, Takeoka M (2018) Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic gaussian channels. *N J Phys* 20(6):063025
74. Smith G, Smolin JA, Yard J (2011) Quantum communication with gaussian channels of zero quantum capacity. *Nat Photon* 5(10):624–627
75. Walls DF, Milburn GJ (2007) *Quantum optics*, 2nd edn. Springer, Berlin
76. Winter A (2001) The capacity of the quantum multiple-access channel. *IEEE Trans Inform Theory* 47(7):3059–3065
77. Yard J, Hayden P, Devetak I (2008) Capacity theorems for quantum multiple-access channels: classical-quantum and quantum-quantum capacity regions. *IEEE Trans Inform Theory* 54(7):3091–3113
78. Hsieh M-H, Devetak I, Winter A (2008) Entanglement-assisted capacity of quantum multiple-access channels. *IEEE Trans Inform Theory* 54(7):3078–3090
79. Czekaj L, Korbicz J, Chhajlany RW, Horodecki P (2012) Schemes of transmission of classical information via quantum channels with many senders: discrete-and continuous-variable cases. *Phys Rev A* 85(1):012316
80. Shi H, Hsieh M-H, Guha S, Zhang Z, Zhuang Q (2021) Entanglement-assisted capacity regions and protocol designs for quantum multiple-access channels. *Quant Inform* 7(1):1–9
81. Yard J, Hayden P, Devetak I (2011) Quantum broadcast channels. *IEEE Trans Inform Theory* 57(10):7147–7162
82. Fawzi O, Hayden P, Savov I, Sen P, Wilde MM (2012) Classical communication over a quantum interference channel. *IEEE Trans Inform Theory* 58(6):3670–3691

83. Savov I (2012) Network information theory for classical-quantum channels. PhD thesis, McGill University, School of Computer Science, USA
84. Hayashi M (2009) Information spectrum approach to second-order coding rate in channel coding. *IEEE Trans Inform Theory* 55(11):4947–4966
85. Polyanskiy Y, Poor HV, Verdú S (2010) Channel coding rate in the finite blocklength regime. *IEEE Trans Inform Theory* 56(5):2307–2359
86. Hayashi M (2017) Finite-block-length analysis in classical and quantum information theory. *Proce Jpn Acad Ser B* 93(3):99–124
87. Tomamichel M, Hayashi M (2013) A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Trans Inform Theory* 59(11):7693–7710
88. Tomamichel M, Tan VY (2015) Second-order asymptotics for the classical capacity of image-additive quantum channels. *Commun Math Phys* 338(1):103–137
89. Rouzé C, Datta N (2017) Finite blocklength and moderate deviation analysis of hypothesis testing of correlated quantum states and application to classical-quantum channels with memory. *IEEE Trans Inform Theory* 64(1):593–612
90. Khatri S, Wilde MM (2020) Principles of quantum communication theory: a modern approach. arXiv preprint [arXiv:2011.04672](https://arxiv.org/abs/2011.04672)
91. Becker S, Datta N (2020) Convergence rates for quantum evolution and entropic continuity bounds in infinite dimensions. *Commun Math Phys* 374(2):823–871



Vinod Sharma received his B.Tech. in EE in 1978 from Indian Institute of Technology, Delhi, India, and Ph.D. in ECE from Carnegie Mellon University in 1984. He worked at Northeastern University, Boston, and University of California in Los Angeles before joining Indian Institute of Science (IISc), Bangalore, in 1988. In IISc, he has been the Chair of ECE dept, TATACHEM chair professor and Dean of Engineering faculty and has superannuated in July 2022. He won Prof. Rustom Choksi award for excellence in research in 2017 and ACCS-CDAC award in 2012. He is an elected fellow of Indian National Academy of Engineering (INAE). His research interests are in communication networks, wireless

communications and information theory and has more than 200 papers in international journals and conferences in these areas.



Konchady Gautam Shenoy completed his Bachelors in Engineering from NMAM Institute of Technology, Nitte, Karnataka, in 2008, followed by a Masters in Technology from Indian Institute of Technology, Bombay, in 2011. He is currently pursuing a PhD at Indian Institute of Science, Bengaluru, and working at Qualcomm India since 2020. His research interests include wireless communication and information theory as well as quantum information theory.