SCUOLA NORMALE SUPERIORE

Class of Sciences

PhD thesis in Nanosciences

XXXIII Cycle, Academic year 2022/2023

Quantum communication with side infromation

Candidate
Farzad Kianvash

Supervisor
Vittorio Giovannetti

Abstract

Quantum communication capacities refer to the maximum amount of quantum information that can be reliably transmitted through a noisy communication channel. However, evaluating these capacities for many quantum channels is challenging due to the superadditivity phenomenon. In this thesis, we tackle this problem by proposing the design of multiple degradable extensions for different important discrete and continuous variable channels. By introducing these extensions, we can establish upper bounds on the quantum and private capacities of the original channels. These extended channels often rely on a set of sufficient conditions that determine the degradability of flagged extensions, which are channels formed as convex combinations of other channels with some side information, commonly referred to as flags. Verifying these conditions is straightforward and greatly simplifies the process of constructing degradable extensions. This approach not only provides a practical solution for estimating the capacities of realistic channels but also enhances our understanding of their behavior in terms of degradability. We apply this technique to both discrete and continuous variable channels, expanding its applicability across different scenarios.

Acknowledgments

I would like to express my heartfelt gratitude to my supervisor, Vittorio Giovannetti, for his invaluable guidance, support, and mentorship throughout the course of my thesis. His expertise and dedication have been instrumental in shaping my research and academic journey.
I would also like to extend my appreciation to my colleague, Marco Fanizza, for his collaboration, insightful discussions, and assistance during this thesis. His contributions have greatly enriched my work and I am grateful for his friendship.
Furthermore, I would like to thank my friends and family for their unwavering encouragement, understanding, and belief in my abilities. Their constant support has been a source of motivation and inspiration throughout this endeavor.
Lastly, I am grateful for the wonderful experiences and the enriching life I have had in Pisa.
I am sincerely thankful to all those who have played a part in my thesis journey, and I am excited to embark on the next chapter of my academic and personal life.

Contents

Chapter 1

Introduction

Studying Communication (from Latin: communicare, meaning "to share") in a world in which everything is connected is of great importance. In common use, communication refers to the propagation of information, and as usual in physics we find mathematical models to describe this phenomena. Claude Shannon, a father of classical information theory, by modelling the propagation of information in the noisy environment, found the ultimate rate of transmission of information [Sha48]. Being one of the most cited scientific papers of all time, the work of Shannon had an immense impact on the development of communication technology, in fact almost any communication device that we use is based on his work.

In the scenario proposed by Shannon, the messages are encoded to bits of information, and are transmitted through a noisy medium called as channels, then the receiver decodes the information to recover the original messages. Surprisingly, he showed that the optimal rate of transmission over many uses of the channel is equal to the maximization of an entropic function, mutual information, over one channel use (This is usually called as single letter formula since it only involves optimization on one channel use). This fact makes the evaluation of the optimal rate computationally feasible.

Analogously, quantum Shannon theory [Wil17; Hol19] provides a characterization of the maximum achievable transmission rates (capacities) for classical or quantum data through a quantum channel, as maximizations of entropic functionals. In contrast to the classical case, in most cases available characterizations capacities cannot be computed algorithmically, since they involve a limit of an infinite sequence of optimization problems, one for any number of uses of the channel. Superadditivity of quantum entropic functionals makes such regularization necessary [SS96; DSS98; SS07; FW08; Has09; SSY11; LLS18a; BL20; SG21; Sid20b; Sid20a; NPJ20], and can hinder the evaluation of capacities even for simple fundamental channels.

As Shannon probably could not imagine the impact of his work in scientific and technological advancement, it is likely that we are not yet fully aware of the influence of quantum communication and quantum Shannon theory on the future of communication too. In quantum communication, the promising progress in the field transformed the academic research into almost a commercial technology. In fact, we had never been this close to realizing commercial quantum communication technology, therefore this is the right moment to study it. With this motivation, in the presented thesis we address the long standing open problem of quantum Shannon theory, namely finding the quantum and private capacity of quantum channel. Quantum and private capacity determine the optimal transmission rates of quantum states and private classical information over a quantum channel, and they are characterized as optimization of the coherent information and the private information, respectively [Wil17].

As mentioned before, due to the superadditivity phenomena, it is hard to get a single letter formula for the quantum and private capacity, therefore computing them in the general case is computationally demanding. However, it is important to improve our best understanding of the capacities of channels of physical interest. in fact, there is a series of work to estimate, upper and lower bound, the quantum and private capacity [DSS98; AC97; Bru+98; Rai99; Cer00; Rai01; SS07; FW08; Smi08; SSW08; SS08; Ouy14; Sut+17; LDS18; LLS18b; BL21], and etc. Most of our results in the thesis, contribute to this literature.

A standard strategy to upper bound the quantum and private capacity of channels is to design extended channels, channels which can be reduced to the original channel after pre or post-processing operations, with known (or computable) capacities. Degradable channels are an important class of channels for which the quantum and private capacity can be calculated. In the literature many works used this strategy, designing degradable extensions, to upper bound the quantum and private capacity [SS08; Sut+17; RMG18; LLS18b]. In this thesis most of the results to upper bound the quantum and private capacity is based on the same strategy. We use a particular class of degradable extension known as flagged channels to bound the capacities. The idea was first introduced in [SS08] where the authors extended depolarizing channel by introducing an ancillary system which gives some side information about the Kraus operator acting on the input state. In [SS08] the ancillary states, known also as flag states, are in different orthogonal states, and the proof of degradablity is quite straightforward. We generalized this method to flagged extensions with non orthogonal flags which results to better bounds and more accurate estimation of capacities [FKG20; FKG21; KFG22].

1.1 Outline

The presented thesis is divided into two parts. In the first three chapters, we briefly review the fundamental concepts in quantum information and communication. In the

remaining four chapters, we present the our results during my Ph.D, which are mostly about estimating, more precisely upper bounding, the quantum and private capacity of quantum channels.
Here, we present a more detailed presentation of each chapter.

1.1.1 Chapter 2: Quantum States, Measurement, and Channels

In chapter 2 we review the basic notions in quantum mechanics and quantum information, and present the notation that we used throughout the thesis.
More specifically, we first present Dirac notation, then study quantum states, quantum measurements, and quantum channels. Then in the end we briefly review an important class of quantum channels, namely Pauli channels.

1.1.2 Chapter 3: Quantum Shannon Theory

Quantum Shannon theory is a central topic throughout the thesis, and we devoted a chapter to discuss the fundamental concepts. We start this chapter by reviewing Von Neumann entropy and some of its properties. Then we define capacities of quantum channels, namely classical capacity, Entanglement assisted classical capacity, private capacity, quantum capacity, and discussed the superadditivity phenomena. In the last section of chapter 3, we discuss the previous bounds on private and quantum capacity.

1.1.3 Chapter 4: Continuous Variable Systems

Continuous variable systems, and in particular Gaussian systems are of a great importance to realize quantum communication protocols. Therefore, we dedicated a chapter to review it and establish the notation we use for Gaussian systems. More precisely, in the first two sections we presented some important definitions such as position and moment operators, canonical commutation relation, displacement operator, creation, and annihilation operators. Then we present three equivalent characterizations of Gaussian states:

- Thermal states of second order Hamiltonian.
- Characterization of Gaussian states using first and second moments.
- Using the characteristic function

In the last section of chapter 4 we present the most general characterization of Gaussian channels and some useful theorems about maximizing coherent information of degradable Gaussian channels. The material presented in this chapter are used extensively in chapters 7 and 8.

1.1.4 Chapter 5: Optimal Subtracting Machine

This chapter is based on

- Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Optimal quantum subtracting machine". In: *Physical Review A* 99.5 (2019), p. 052319. DOI: 10.1103/PhysRevA.99.052319. arXiv: 1811.07187

We studied the impossibility of undoing the mixing of a quantum message with an unknown quantum state. After proving the no go theorem, we found the optimal machines to undo the mixing process for pure qubit states. We considered the the scenario of having different copies of the mixed state and unknown states, and for each case, using the symmetries of the problem, we calculated the optimal fidelity. We used analytical methods for determining the optimal machine for few copies and numerical ones when the number of copies, and consequently the number of parameters, are larger.
This problem can be seen also from quantum communication point of view: The noisy signal is the mixed state and we have some quantum information i.e. copies of the unknown state about the noise to recover the original message.

1.1.5 Chapter 6: Degradable Flagged Extensions: Discrete Channels

This chapter is based on the following two articles

- Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Quantum Flags and New Bounds on the Quantum Capacity of the Depolarizing Channel". In: *Physical Review Letters* 125.2 (2020), p. 020503. DOI: 10.1103/PhysRevLett.125.020503. arXiv: 1911.01977
- Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Bounding the quantum capacity with flagged extensions". In: *Quantum* 6 (2022), p. 647. DOI: 10.22331/q-2022-02-09-647

In this chapter, we introduce a general technique to design degradable extension of convex combination of quantum channels. This particular degradable extension, flagged channels, are constructed by introducing an ancillary system, flag state, that gives some quantum information about which channel in the convex combination acts on the input system. We apply this method to a wide variety of qudit channels of interest and find new upper bounds for their quantum and private capacity. In particular, d-dimensional depolarizing, BB-84, and generalized amplitude damping channel are studied.

1.1.6 Chapter 7: Degradable Extension: Gaussian channels

This chapter is based on the following article

- Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Estimating Quantum and Private Capacities of Gaussian Channels via Degradable Extensions". In: *Phys. Rev. Lett.* 127 (21 2021), p. 210501. DOI: `10.1103/PhysRevLett.127.210501`

Chapter 7 is dedicated to the study of upper bounds on the quantum and private capacity of some Gaussian channels which model real quantum communication channels, namely thermal attenuator, thermal amplifier, and additive Gaussian noise. First, we generalize the flagged channel technique introduced in chapter 6 to the continuous variable channel, and upper bound the capacities of additive Gaussian noise. Then we combine this result with some information processing inequality to bound the capacities of thermal amplifier. In the last part, we the bound the capacities of thermal attenuator by design a degradable extension, and calculating its quantum capacity. The presented upper bounds beat the previous results in the following parameter regions: low temperature and high transmissivity for the thermal attenuator, low temperature for additive Gaussian noise, high temperature and intermediate amplification for the thermal amplifier.

1.1.7 Chapter 8: Improving Bounds for Thermal Attenuator Using Decomposition Rules

We improve the previous bound for the quantum and private capacity of thermal attenuator using information processing inequalities. Thermal attenuator with fixed transmissivity and average bath energy can be written as the composition of thermal amplifier and thermal attenuator with different parameters. Such information processing inequalities, decomposition rules, are often used to find the bounds but had never been used to the fullest extent. In chapter 8, we consider them in the most general form and improve the previous bounds bounds for thermal attenuator. In addition, we show that any given bound should follow a certain symmetry otherwise one can construct a better bound using the decomposition rules.

Chapter 2

Quantum states, Measurements and channels

2.1 Dirac Notations

A Hilbert space is complex linear space for which the inner product is properly defined. In this section, we work with finite dimensional Hilbert spaces, However almost all the definitions and theorems can be generalized to the infinite dimensional case too, and we will treat the infinite dimensional case in Chapter 4.
In Dirac notation, any vector in a Hilbert space $\mathcal{H}$ is represented by $|\psi\rangle$ (which is a column vector). Correspondingly, $\langle\phi|$ is a row vector defined in such a way that the matrix multiplication of $\langle\phi|$ and $|\psi\rangle$ is equal to the inner product of ϕ and ψ. In a formal way, $\langle\phi|$ is a linear function on $\mathcal{H}$ defined by the inner product [Hol19]

$$\langle\phi| : \psi \to \langle\phi|\psi\rangle\,, \quad \psi \in \mathcal{H}\,. \tag{2.1}$$

With this definition the norm of any state $|\psi\rangle$ can be written as $\|\psi\|^2 = \langle\psi|\psi\rangle$.
In a similar way, $A := |\psi\rangle\langle\phi|$ (note that A belongs to the algebra of all linear operators acting on $\mathcal{H}$ i.e. $A \in \Sigma(\mathcal{H})$) is the matrix multiplication of a column and row vectors, which is a rank one operator and its action on any vector $|\xi\rangle$ is as follows

$$A|\xi\rangle = \langle\phi|\xi\rangle\,|\psi\rangle\ . \tag{2.2}$$

For any linear operator A acting on $\mathcal{H}$ its adjoint $A^\dagger$ is defined as

$$\langle\phi| A^\dagger |\psi\rangle = (\langle\psi| A |\phi\rangle)^* \tag{2.3}$$

with $*$ denoting the complex conjugate, and A is Hermitian if and only if $A = A^\dagger$ (in finite dimensional Hilbert spaces being Hermitian is equivalent to being self adjoint).
A Unitary operator is an operator for which $UU^\dagger = I$. For the finite-dimensional Hilbert spaces, this implies that $U^\dagger U = UU^\dagger = I$. Any operator $V_{A\to B} : \mathcal{H}_A \to \mathcal{H}_B$ is an isometry if it preserves the inner product which is equivalent to the condition $V_{A\to B}V^\dagger_{B\to A} = I$.
In Quantum Mechanics, we often deal with Hermitian operators and the following theorem about Hermitian operators is helpful.

Theorem 2.1.1 (Spectral Decomposition). *For any Hermitian Operator A, there exists a set of orthonormal eigenvectors with corresponding real eigenvalues such that*

$$A = \sum \lambda_i \left|\lambda_i\right\rangle \left\langle\lambda_i\right| \,. \tag{2.4}$$

Operator A is positive semi-definite if for any $|\psi\rangle \in \mathcal{H}$, $\langle\psi| A |\psi\rangle \geq 0$. For the Hermitian operators this is equivalent to the fact that all of the eigenvalues λ_i are greater than or equal to zero.
For any arbitrary orthonormal basis $\{|e_i\rangle\}$, trace of an operator is defined as $\text{tr}(A) := \sum \langle e_i| A |e_i\rangle$. Trace does not depend on the chosen basis, and its cyclic i.e. $\text{tr}(AB) = \text{tr}(BA)$.

2.2 Quantum states

In the standard formalism of Quantum Mechanics any physical system is described by a density matrix. Density matrices provide information about the probability of different outcomes of measurements. Any density matrix should have three properties

- $\rho = \rho^\dagger$,
- $\text{tr}(\rho) = 1$,
- $\rho \geq 0$,

and the space of all density matrices is denoted by $\mathcal{D}(\mathcal{H})$. The dimension of the Hilbert space $\mathcal{H}$ can be finite or infinite. For instances, when we measure the spin of an electron there are two possible outcomes, and the dimension of the corresponding Hilbert space is two. On the other hand, if we measure the position of an electron there are infinite possible outcomes, therefore to represent its position we use infinite dimensional matrices, and such infinite dimensional Hilbert space is isomorphic to the space of square integrable functions on $\mathbb{R}^n$, $L^2(\mathbb{R}^n)$.
if a state can be written as $\rho = |\psi\rangle\langle\psi|$ we call that a pure state, this condition is equivalent to $\text{tr}(\rho^2) = 1$ or $\rho^2 = \rho$, and all the other states are mixed.

The Hilbert space of two quantum systems A and B, with the corresponding Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, is $\mathcal{H}_A \otimes \mathcal{H}_B$. Assume that $\{|i\rangle\}$ is a basis for $\mathcal{H}_A$ and $\{|j\rangle\}$ is a basis for $\mathcal{H}_B$, therefore $\{|ij\rangle\}$ is a basis for the joint Hilbert space, and any $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written as

$$|\psi\rangle = \sum \psi_{ij} |ij\rangle \tag{2.5}$$

For any $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the marginal state ρ_A is defined as

$$\rho_A := \operatorname{tr}_B(\rho_{AB}) = \sum_j (I_A \otimes \langle j|)\rho_{AB}(I_A \otimes |j\rangle)\,. \tag{2.6}$$

Product states are the form $\rho_{AB} = \rho_A \otimes \rho_B$ and a state ρ_{AB} is separable if and only if it can be written as $\rho_{AB} = \sum p_i \rho_A \otimes \rho_B$ with $\{p_i\}$ being a probability distribution. All other states are entangled, and among all the entangled states, the maximally entangled state is a pure state defined as $|\Gamma\rangle_{AB} := \sum_{i=1}^{\min(d_A,d_B)} \frac{1}{\sqrt{\min(d_A,d_B)}} |i\rangle_A \otimes |i\rangle_B$ with d_A and d_B being the dimension of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively.

2.3 Quantum measurements

Any measurement on a finite dimensional quantum system can be described by a set of positive operator-valued measure (POVM) operators. A set $\{M_i\}$ is a POVM (quantum measurement) if it has the following property [NC02]

- $\sum_i M_i^\dagger M_i = I$.

operators $\{M_i\}$ are related to the different outcomes of measurements. If the initial state of the system is ρ the probability of the i'th outcome is given by $\Pr(i) = \operatorname{tr}\left(M_i \rho M_i^\dagger\right)$, and the state after the i'th outcome is $\rho_i = \frac{M_i \rho M_i^\dagger}{\Pr(i)}$. The average state after the measurement is (without looking at the outcomes) $\sum_i M_i \rho M_i^\dagger$. Orthogonal measurements are the ones for which $M_i M_j = \delta_{i,j} M_i$.
Any observable is a random variable that can be sampled from a measurement. In the standard formalism of Quantum Mechanics, observables are associated to Hermitian operators. A Hermitian operator O with the spectral decomposition

$$O = \sum_i \lambda_i |\lambda_i\rangle \langle\lambda_i| \ , \tag{2.7}$$

associates the real eigenvalue λ_i to the quantum state $|\lambda_i\rangle$. The probability of finding a quantum state ρ in the pure state $|\lambda_i\rangle$ is $\Pr(\lambda_i) = \operatorname{tr}(\rho |\lambda_i\rangle \langle\lambda_i|)$ (orthogonal POVM operators are $M_i = \{|\lambda_i\rangle \langle\lambda_i|\}$), therefore the mean value of O on ρ is

$$\mathbb{E}_\rho[O] := \operatorname{tr}[O\rho] = \sum_i \Pr(\lambda_i)\lambda_i\,. \tag{2.8}$$

One can generalise these notions to the continuous variable case too (the detailed conditions of the generalisation can be found in [Hol11], however here we present the important example of position operator). The function $\psi(x)$ is a state in the space of square integrable functions. The position operator X acts as following

$$X\psi(x) := x\psi(x)\,. \tag{2.9}$$

To find the eigenvalues of such operator one should solve the following equation

$$x\psi_{x_0}(x) := x_0\psi_{x_0}(x)\,. \tag{2.10}$$

For which the solutions are the Dirac delta functions centred at x_0 i.e. $\delta(x - x_0)$. In the Dirac notations, the eigenvectors of the position operators are represented by $|x\rangle$ i.e. $X|x\rangle = x|x\rangle$. In this notation one can write

$$X = \int x\,|x\rangle\langle x|\;. \tag{2.11}$$

The inner product of two eigenvectors is equal to $\langle x|x'\rangle = \delta(x - x')$ and $\langle x|\psi\rangle = \psi(x)$ which its absolute value squared i.e. $|\psi(x)|^2$ is the probability density function.

2.4 Quantum channels

As we saw in the previous section, the most general description of quantum systems is given by density matrices. In this section, we briefly review the most general physical maps that transform quantum density matrices.
A linear operator (or super operator) $\Lambda_{A\to B} : \Sigma(\mathcal{H}_A) \to \Sigma(\mathcal{H}_B)$ describes a physical transformation of a quantum system if and only if it has the following two properties [NC02]

- $\Lambda_{A\to B} \otimes \mathcal{I}_C[X] \geq 0$ if $X \geq 0$ (completely positive);
- $\mathrm{tr}[\Lambda[X]] = \mathrm{tr}[X]$ (trace preserving).

The first property means that any extension of super operator $\Lambda_{A\to B}$ with the identity, maps positive operators to positive operators. Completely Positive Trace Preserving (CPTP) maps describe any noise in quantum hardware and communication lines, and are often called as quantum channels. The following theorem gives a decomposition for any CPTP map

Theorem 2.4.1 (Kraus Decomposition). *Given any CPTP map $\Lambda_{A\to B}$ there exists a set of Kraus operator $\{K_i\}$ such that*

- $\mathcal{N}_{A\to B}[X] = \sum_i K_i X K_i^\dagger$*;*

- $\sum_i K_i^\dagger K_i = I$.

For the finite dimensional case, the maximum number of Kraus operators needed in this representation is equal to $d_A.d_B$ where d_A and d_B are dimensions of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. In the infinite dimensional case, the number of Kraus operators can be infinite. The Kraus representation is not unique and different Kraus representations are related to each other by isometry operators i.e. $K_i' = \sum_j V_{ij} K_j$. Unitary channels are the one with unitary Kraus operators (normalized to one with a probability distribution) A more physical representation of quantum channels is given by Stinespring representation. In this representation, any quantum channel can be written as the unitary interaction between the system and the environment and then tracing out the environment.

Theorem 2.4.2 (Stinespring Representation). *Any quantum channel $\mathcal{N}_{A\to B}$ can be written as*

$$\Lambda_{A\to B}[X] = \mathrm{tr}_{E'}[U_{AE\to BE'} X_A \otimes |\tau\rangle\langle\tau|_E \, U^\dagger_{AE\to BE'}] \,. \tag{2.12}$$

where $U_{AE\to BE'}$ is a unitary operator mapping the system AE to BE'.

The complementary channel is defined as

$$\tilde{\Lambda}_{A\to E'}[X] = \mathrm{tr}_{B}[U_{AE\to BE'} X_A \otimes |\tau\rangle\langle\tau|_E \, U^\dagger_{AE\to BE'}] \,.$$

if there exists a channel W such that $W \circ \Lambda = \tilde{\Lambda}$ we say that Λ is a degradable channel, and if $W \circ \tilde{\Lambda} = \Lambda$ the channel is anti-degradable.
Another useful tool in studying quantum channels is Choi-Jamiolkowski isomorphism. For any channel $\Lambda_{A\to B}$ one can define the Choi state as

$$J_\Lambda = (\Lambda_{A\to B} \otimes \mathcal{I}_R)\left[|\Gamma\rangle\langle\Gamma|_{AR}\right] , \tag{2.13}$$

where $|\Gamma\rangle_{AR}$ is the maximally entangled state, and R is a subsystem isomorphic to A i.e. $\mathcal{H}_R \cong \mathcal{H}_A$. Quantum channel Λ is a CPTP if and only if $J_\Lambda \geq 0$, and J_Λ has all the information about $\Lambda_{A\to B}$ [NC02]

$$\Lambda_{A\to B}[\rho] = \mathrm{tr}_R(J_\Lambda \, . \, I_B \otimes \rho_R^\intercal) \,. \tag{2.14}$$

For the infinite-dimensional case a similar Choi-Jamioljowski generalization can found in [Hol11].

2.5 Pauli channels

In this section, we concentrate on an important subclass of unitary channels, the Pauli channels, which describe random bit flip and phase flip errors in qubits, and their generalization to qudits models. As we will mention later in Chapter 3 Pauli channels are superadditive, and their quantum and private capacity is unknown. However in Chapter 6, we will upper bound their private and quantum capacity using their symmetries. The following treatment of generalized Pauli channels follows the phase-space description of finite dimensional quantum mechanics [Woo87; App05; Gro06; GE08; dBe13; GNW21].

2.5.1 Qubit Pauli group

We start by recalling the Pauli group of one qubit:

$$\mathcal{P} := \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}, \tag{2.15}$$

where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The elements of the Pauli group of n qubits is obtained by the tensor product of n elements of one qubit Pauli group $\mathcal{P}^n := \{\otimes_{j=1}^n \omega_j | \omega_j \in \mathcal{P}\}$. For our purposes it suffices to consider $\mathsf{P}^n := \mathcal{P}^n / C^n$, the quotient of the Pauli group with its center $C^n := \{\pm I^{\otimes n}, \pm i I^{\otimes n}\}$. Each element of P^n is both hermitian and unitary and can be identified by a pair of n bit-strings $x = (q, p)$ according to the definition

$$P_{(q,p)} := i^{-p\cdot q} \otimes_{j=1}^n Z^{p_j} X^{q_j}. \tag{2.16}$$

It is then immediate to see that for any two $x = (q,p), y = (q', p')$ we have $P_x P_y = (-1)^{\langle x,y \rangle} P_y P_x$, where

$$\langle x, y\rangle = p \cdot q' - q \cdot p' \mod 2 \,, \tag{2.17}$$

and that $\mathrm{Tr}[P_x] = 2\delta_{x,0}$.

2.5.2 Qudit Pauli group

The unitary generalization of the Pauli group for one qudit is the group $\mathcal{W}_d$ generated by τI ($\tau := e^{\frac{(d^2+1)\pi i}{d}}$), and the Weyl-Heisenberg operators X, Z acting as

$$X\,|j\rangle = |j+1\rangle \mod d, \qquad Z\,|j\rangle = e^{j\frac{2\pi i}{d}}\,|j\rangle \qquad j = 0, ..., d-1. \tag{2.18}$$

For several qudits, likewise we set $\mathcal{W}_d^n := \{\otimes_{j=1}^n \omega_j | \omega_j \in \mathcal{W}_d\}$. The center of this group is still a set of multiples of the identity $C_d^n = \{\tau^j I^{\otimes n} : j = 0, ..., D-1\}$, where $D = d$ if d is odd and $D = 2d$ if d is even; we define $\mathsf{W}_d^n := \mathcal{W}_d^n / C_d^n$. Each element of W_d^n can be identified by a pair of n Dit-strings $x = (q,p) \in \mathbb{Z}_D^{2n}$ according to the definition

$$W_{(q,p)} := e^{-\frac{(d^2+1)\pi i}{d}(p\cdot q)} \otimes_{j=1}^n Z^{p_j} X^{q_j}. \tag{2.19}$$

By close inspection it holds that

$$W_x W_y = e^{\frac{2\pi i}{d}\langle x,y\rangle} W_y W_x, \tag{2.20}$$

where now

$$\langle x,y\rangle = p\cdot q' - q\cdot p' \mod D. \tag{2.21}$$

Moreover, for any $x, z \in \mathbb{Z}_D^{2n}$ we have

$$W_{x+dz} = (-1)^{(d+1)\langle x,z\rangle} W_x, \tag{2.22}$$

and $\mathrm{Tr}[W_x] = d^n \delta_{x,0}$.

2.5.3 Pauli channels

Pauli channels are defined as convex combination of Pauli unitaries:

$$\Phi_{\mathbf{w}}[\rho] = \sum_{x\in\mathbb{Z}_d^{2n}} w_x W_x \rho W_x^\dagger, \tag{2.23}$$

where now it suffices to sum over $\mathbb{Z}_d^{2n}$ instead of $\mathbb{Z}_D^{2n}$ because of Eq. (2.22), and they are parametrically described by the probability distribution $\mathbf{w}(x) = w_x$. Each element of W_d^n is a unitary matrix, therefore it describes a reversible evolution of the system of n qudits.
An important one qudit Pauli channel is depolarizing channel which is characterized by $w_x = \delta_{x,0}(1-p) + \frac{p}{d^2}$

$$\Phi_p^d[\rho] := (1 - \frac{d^2-1}{d^2}p)\rho + \frac{p}{d^2}\sum_{x\in\mathbb{Z}_d^2\setminus\{0\}} W_x\rho W_x^\dagger \tag{2.24}$$

$$= (1-p)\rho + p\frac{I}{d}\,. \tag{2.25}$$

where we just used the fact that for any operator $A \in \Sigma(\mathbb{C}^{dn})$

$$\frac{1}{d^{2n}}\sum_{x\in\mathbb{Z}_d^{2n}} W_x A W_x^\dagger = \mathrm{Tr}(A)\frac{I}{d^n}\,. \tag{2.26}$$

Another one qubit Pauli channel that we consider is the channel that describes the famous quantum key distribution protocol by Bennett and Brassard [BB14a]. In its general form the channel is

$$B_{p_X,p_Z}[\rho] = (1-p_X-p_Z+p_Xp_Z)\rho + (p_X - p_Xp_Z)X\rho X + (p_Z - p_Zp_X)Z\rho Z + p_Xp_ZY\rho Y\,. \tag{2.27}$$

Chapter 3

Quantum Shannon theory

To have a better understanding of Quantum Shannon theory and Von Neumann entropy it is useful to briefly review its classical counter part i.e. Classical Shannon Theory and Shannon entropy. Claude Shannon in his historical article [Sha48] solved two important problems.

Firstly, he calculated how much a message can be compressed. More precisely, he showed that messages of length $n >> 1$ composed of letters $\{x_i\}$ from an alphabet with k different letters $(0 \leq i \leq k)$ with the associated probability distribution $\{p_i\}$ with no memory can be faithfully compressed to messages with $n \sum_{i=0}^{k} -p_i \log_2(p_i)$ bits. The intuition behind this is the fact that typically in a message of length $n >> 1$, the letter x_i is repeated np_i times (*typical messages*). With this motivation it is natural to define Shannon entropy as $S(p) := \sum_{i=0}^{k} -p_i \log_2(p_i)$.

Secondly, Shannon calculated the optimal rate of transmission of information through a noisy channel. In the standard Alice and Bob scenario, Alice wants to send $M >> 1$ different messages to Bob. To do so, she encodes her messages to different n-bit strings and send them to Bob using $n >> 1$ times the shared noisy channel. If Bob finds a decoding strategy to recover Alice's messages faithfully for large n and M, the quantity $\frac{\log_2(M)}{n}$ is an achievable rate of transmission of information. The capacity of a noisy channel is the maximum of the all achievable rates, and Shannon managed found a closed formula for this quantity.

Quantum Shannon theory generalizes this approach to quantum states and quantum channels. In contrast to the classical case, one can define different notions of capacity depending on the communication tasks. In many cases, calculation of different capacities is not easy and there is no closed formula for them. In the rest of this section, I present some important definitions and theorems. The proof of the presented results can be found in any standard book of quantum information like [Wil17; Hol19].

3.1 Von Neumann entropy

For quantum states the generalization of Shannon entropy is Von Neumann entropy defined as follows

Definition 3.1.1 (von Neumann entropy).

$$S(\rho_A) := -\operatorname{Tr}[\rho_A \log_2 \rho_A] \,. \tag{3.1}$$

In fact, Von Neumann entropy is the Shannon entropy of the eigenvalues of ρ. Similar to Shannon compression theorem, in [Sch95] Schumacher showed that Von Neumann entropy is the the fundamental limit of quantum data compression.
There are handful mathematical properties of $S(\rho)$ that we are going to use often in this thesis

- Positivity: $S(\rho) \geq 0$ for any state ρ, with equality only for pure states.
- Maximum: if ρ has d non zero eigenvalues, then $S(\rho) \leq d$.
- Invariance under Isometry operators: $S(\rho_A) = S(V_{A\to B}\rho_A V_{A\to B}^\dagger)$ for any isometry $V_{A\to B}$.
- Concavity: For any probability distribution $\{\lambda_i\}$ and any collection of quantum states $\{\rho_i\}$ we have
$$S(\sum_i \lambda_i \rho_i) \geq \sum_i \lambda_i S(\rho_i) \,. \tag{3.2}$$
- Subadditivity: For a bipartite system AB in the state ρ_{AB}
$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B) \tag{3.3}$$
with the equality only for product states $\rho_{AB} = \rho_A \otimes \rho_B$.
- For a pure a state $|\psi\rangle_{AB}$ the entropy of the marginal states are equal i.e. $S(\rho_A) = S(\rho_B)$.
- Strong subadditivity: $S(\rho_{ABC}) + S(\rho_C) \leq S(\rho_{AC}) + S(\rho_{BC})$.

In contrast with the classical case, it is not trivial to prove the strong subadditivity of Von Neumann entropy [LR73a; LR73b; Lin75].
two important entropic quantities are mutual information and coherent information which are defined as

$$\begin{aligned} I(A;B)_\rho :=& S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \,, \\ I_c(A;B)_\rho :=& S(\rho_B) - S(\rho_{AB}) \,. \end{aligned} \tag{3.4}$$

Using strong subadditivity one can show that mutual information and coherent information are monotonic under the action of quantum channels. More precisely, for any two channels $\Lambda_{A\to A'}, \Lambda'_{B\to B'}$ and any state ρ_{AB}, defining $\sigma_{A'B'} = \Lambda_{A\to A'} \otimes \Lambda'_{B\to B'}[\rho_{AB}]$, we have $I(A;B)_\rho \geq I(A';B')_\sigma$. In addition, for any channel $\Lambda_{A\to A'}$, and any state ρ_{AB}, defining $\sigma_{AB'} = \mathcal{I}_A \otimes \Lambda_{B\to B'}[\rho_{AB}]$, we have $I(A;B)_\rho \geq I(A;B')_\sigma$.

3.2 Capacities of a quantum channel

Shannon in [Sha48] calculated the optimal rate of transmission of information through a classical channel. In contrast to the classical case, for quantum channels the situation is more complex: depending on what kind information one wants to transmit (classical or quantum information), and what are the resources, different capacities of a quantum channel can be defined. Here we review the definition and basic properties of capacities. For more detailed analysis one can see [Wil17; Hol19].

3.2.1 Classical capacity of quantum channels

Consider the scenario of using quantum channels to send classical messages. To do so, one encodes M different classical messages to M quantum states $\{\rho_i^{(n)} \in \Sigma(\mathcal{H}_A^{\otimes n})\}$, and send them using the channel n times $\Lambda^{\otimes n} : \Sigma(\mathcal{H}_A^{\otimes n}) \to \Sigma(\mathcal{H}_B^{\otimes n})$. The receiver decodes the received states by performing a measurement characterized by $\{K_i^{(n)}\}$. The maximum probability of error of the encoding and decoding process (coding) is equal to

$$P_e = \max_{1\leq i\leq M}[1 - \mathrm{tr}\Big(K_i^{(n)}\Lambda^{\otimes n}[\rho_i^{(n)}]K_i^{(n)\dagger}\Big)]\,. \tag{3.5}$$

The good codes are the one for which the probability of error P_e is sufficiently small for large n, and the rate of such a code is $R := \frac{\log_2(M)}{n}$ (usually called an achievable rate). The classical capacity of a channel $C(\Lambda)$ is the minimum upper bound of all the achievable rates. In [Hol98; SW97], the authors found an expression for the classical capacity

Theorem 3.2.1 (Classical capacity). *For any n, the classical capacity of Λ is greater or equal than*

$$C(\Lambda) \geq C_n(\Lambda) := \frac{\chi(\Lambda^{\otimes n})}{n}. \tag{3.6}$$

with the Holevo quantity defined as

$$\chi(\Lambda) := \sup_{\{p_i,\rho_i\}} S(\sum_i p_i\Lambda(\rho_i)) - p_i S(\Lambda(\rho_i)),$$

where $\{p_i\}$ being a probability distribution and $\{\rho_i\}$ a set of density matrices. And, for large n we have $\lim_{n\to\infty} C_n(\Lambda) = C(\Lambda)$.

In general, the Holevo quantity can be superadditive: for two arbitrary channels Λ_1 and Λ_2 the Holevo quantity of the joint channel can be greater than the sum of the Holevo quantities i.e. $\chi(\Lambda_1 \otimes \Lambda_2) \geq \chi(\Lambda_1) + \chi(\Lambda_2)$. This means that using entangled states across different channel uses can improve the communication capacity, and the computation of the classical capacity is hard since the number of parameters in the the optimization to find $\chi(\Lambda^{\otimes n})$ grows exponentially with n (regularized formula). Historically speaking, in the beginning for some years the Holevo quantity thought to be additive (additivity conjecture), and Shor [Sho04] showed that several different additivity conjectures in quantum information theory are all equivalent. However, Hasting in [Has09], by giving a counter-example, showed that the additivity conjecture and its equivalent forms are false. Although the additivity conjecture in general is wrong, for many quantum channels it holds. For example, the classical capacity of finite dimensional entanglement breaking channels [Sho02a], infinite dimensional entangle breaking channels [Shi06], unital qubit channels [Kin02], qudit depolarizing channel [Kin03], Hadamard channels[Kin06; Kin+05], and phase insensitive Gaussian channels [Gio+04; Gio+14; GHGP15] are all additive.

3.2.2 Entanglement assisted classical capacity

Similar to the classical capacity, the sender wants to send classical bits to the receiver, however the sender and receiver share unlimited entanglement as a resource. In [AC97; Ben+99; Ben+02], the authors found a closed formula to compute the entanglement assisted capacity

Theorem 3.2.2 (Entanglement assisted classical capacity). *The ultimate rate of transmission of classical information through a quantum channel with an unlimited resource of entanglement, entanglement assisted classical capacity, is equal to*

$$C_e(\Lambda) = \sup_{\rho} I(\Lambda, \rho) := \sup_{\rho} S(\rho) + S(\Lambda(\rho)) - S(\Lambda \otimes I(|\rho\rangle\rangle\langle\langle\rho|)) \,, \tag{3.7}$$

where $|\rho\rangle\rangle$ is a purification of ρ.

Unlike the classical capacity, entanglement assisted classical capacity is additive i.e. $C_e(\Lambda_1 \otimes \Lambda_2) = C_e(\Lambda_1) + C_e(\Lambda_2)$, and the optimization in Eq. 3.7 is only on one use of the channel (single letter formula). The quantity $I(\Lambda, \rho)$ is concave in ρ [Wil17], this fact can be helpful to solve the optimization problem in Eq. 3.7.

3.2.3 Private capacity of a quantum channel

Consider the classical communication case in Sec. 3.2.1, the sender (Alice) wants to send classical messages through a quantum channel to the receiver (BOB). In addition, there is a third party (Eve) that have access to the environment (complementary channel) and wants to steal some information. The optimal rate of transmission of information when Eve cannot steal any information is private capacity. More precisely, Alice encodes her M different classical messages to M quantum states $\{\rho_i^{(n)}\}$, and send them to Bob through n uses of the quantum channel $\Lambda^{\otimes n}$. Bob receives $\{\Lambda^{\otimes n}(\rho_i^{(n)})\}$, and decodes them using a POVM measurement characterized by the set of operators $\{K_i^{(n)}\}$. In the same time, Eve receives states $\{\tilde{\Lambda}^{\otimes n}(\rho_i^{(n)})\}$ and tries infer the messages. The rate $R = \frac{\log_2(M)}{n}$ is achievable if and only if the following two quantities can be sufficiently small for large n

$$P_e^{(n)} = \max_{1\leq i\leq M}[1 - \mathrm{tr}\Big(K_i^{(n)}\Lambda^{\otimes n}[\rho_i^{(n)}]K_i^{(n)\dagger}\Big)] \,, \tag{3.8}$$

$$\nu^{(n)} = \max_{0\leq i,j\leq M} \mathrm{Tr}\left|\tilde{\Lambda}^{\otimes n}(\rho_i^{(n)}) - \tilde{\Lambda}^{\otimes n}(\rho_j^{(n)})\right| . \tag{3.9}$$

The private capacity is the minimum upper bound for all the achievable rates.
The condition that $\lim_{n\to\infty} P_e^{(n)} = 0$ guarantees that Bob actually can decode the information with vanishing error, and the other conditions $\lim_{n\to\infty} \nu^{(n)} = 0$ assures that Eve gets almost the same states and cannot steal any information. In [Dev05; CWY04], they found a regularized formula for the private capacity

Theorem 3.2.3 (Private capacity). *For any n, the private capacity of Λ is greater or equal than*

$$C_p(\Lambda) \geq C_p^{(n)}(\Lambda) := \frac{1}{n}\max_{\{p_i,\rho_i\}} \chi(\{p_i, \Lambda^{\otimes n}[\rho_i]\}) - \chi(\{p_i, \tilde{\mathcal{N}}^{\otimes n}[\rho_i]\}). \tag{3.10}$$

with the Holevo quantity of an ensemble $\{p_i, \rho_i\}$ defined as

$$\chi(\{p_i, \rho_i\}) = S\left(\sum_i p_i\rho_i\right) - \sum_i p_i S(\rho_i) \tag{3.11}$$

where $\{p_i\}$ being a probability distribution and $\{\rho_i\}$ a set of density matrices. And, in the limit of large n we have $\lim_{n\to\infty} C_p^{(n)}(\Lambda) = C_p(\Lambda)$.

For degradable channels, the private capacity is additive [Hol19] i.e. $C_p(\Lambda) = C_p^{(1)}(\Lambda)$. However, there are examples for which the private capacity is not additive [SRS08; ES15], and the use of entangled states over different uses of the channel can improve the communication capacity.

3.2.4 Quantum capacity of a quantum channel

Quantum capacity of a quantum channel is the ultimate rate of transmission of quantum information, quantum states, through a quantum channel. In the standard Alice and Bob scenario, Alice wants to send an arbitrary state $\rho \in \mathcal{D}(\mathcal{H})$, with $\dim(\mathcal{H}) = M$, to

Bob using a quantum channel $\Lambda : \Sigma(\mathcal{H}_A) \to \Sigma(\mathcal{H}_B)$ n-times. To do so, Alice uses the encoding channel $\mathcal{E}^{(n)} : \Sigma(\mathcal{H}) \to \Sigma(\mathcal{H}_A^{\otimes n})$, and send the encoded states to Bob through $\Lambda^{\otimes n}$, and Bob decodes the received states using $\mathcal{D}^{(n)} : \Sigma(\mathcal{H}_B^{\otimes n}) \to \Sigma(\mathcal{H})$. The rate $\frac{\log_2(M)}{n}$ is achievable if and only if there exists coding and decoding channels for which the following quantity is vanishingly small for large n.

$$E^{(n)} = \sup_{\rho \in \mathcal{H}} \operatorname{Tr} \left| \rho - (\mathcal{D}^{(n)} \circ \Lambda^{\otimes n} \circ \mathcal{E}^{(n)})[\rho] \right|. \tag{3.12}$$

The quantum capacity of the channel $Q(\Lambda)$ is the minimum upper bound of all achievable rates. In [Llo97; Sho02b; Dev05] they found a regularized formula for the quantum capacity

Theorem 3.2.4 (Quantum capacity). *For any natural number n, the quantum capacity of a channel Λ is always greater than*

$$Q(\Lambda) \geq Q_n(\Lambda) = \frac{I_c(\Lambda^{\otimes n})}{n} \tag{3.13}$$

where $I_c(\Lambda) := \sup_\rho S(\Lambda(\rho)) - S(\tilde{\mathcal{N}}(\rho))$, and in the large n limit it is exactly equal to the quantum capacity i.e. $Q(\Lambda) = \lim_{n\to\infty Q_n(\Lambda)}$.

As the optimization of coherent information is on the arbitrary large number of channel uses, to compute the quantum capacity one should solve an optimization problem with exponentially growing number of parameters. However, There are classes of channels for which the coherent information is additive i.e. $Q_1(\Lambda) = Q(\Lambda)$, therefore the quantum capacity is relatively easy to compute. For instance, degradable channels are additive [Dev05], and anti-degradable channels have zero capacity (note that entanglement breaking channels are a subclass of anti-degradable channels.) [Hol19]. There are other cases for which the quantum capacity can be calculate, for the details please see [GJL18a; GJL18b; CG21a; CG21b; Led+22].
The following theorem about the concavity of the coherent information of degradable channels is often helpful to compute the coherent information and consequently the quantum capacity of degradable channels [YHD08]

Theorem 3.2.5 (Concavity of coherent information for degradable channels). *If a channel Λ is degradable, for any ensemble $\{p_i, \rho_i\}$ we have*

$$I_c(\Lambda, \sum_{i=1}^{n} p_i \rho_i) \geq \sum_{i=1}^{n} p_i I_c(\Lambda, \rho_i). \tag{3.14}$$

We also note that in general the private and quantum capacity have different values, for instance there exist channels with positive private information and zero quantum capacity [HHH98]. However, for degradable channels the private capacity is also additive and

it coincides with the quantum capacity i.e. $C_p(\Lambda) = Q(\Lambda) = Q_1(\Lambda)$ [Smi08].
In contrast to additive channels, in many cases the quantum capacity is super additive i.e. $Q_1(\Lambda) < Q(\Lambda)$. Super additivity has been shown for many channels [SS96; DSS98; SS07; FW08; SSY11; LLS18a; BL20; SG21; Sid20b; Sid20a; NPJ20], and also it has been experimentally observed [Yu+20]. In [Cub+15] the authors showed that there exist quantum channels for which it is necessary to compute the coherent information of unbounded uses of the channels for finding the quantum capacity. In [SY08; SSY11] the super activation of quantum capacity has been demonstrated i.e. two quantum capacity with zero capacity can have positive capacity if used together.
One can also define entanglement assisted quantum capacity $Q_E(\Lambda)$ which is actually the optimal rate of sending quantum states with unlimited entanglement shared between sender and receiver. It has been shown that $2Q_E(\Lambda) = C_E(\Lambda)$ [DHW04], the intuition behind this is the fact that C_E can be seen as the optimal noisy superdense coding, and Q_E is the ultimate rate of noisy quantum teleportation.
In addition,The two-way quantum capacity $Q^{\leftrightarrow}(\Lambda)$ is defined as the quantum capacity assisted by classical communication between sender and receiver (forward and backward communication). From the practical point of view, this is a relevant quantity as classical communication with classical channels is cheep. In [Ben+96; BKN00] the authors Showed that forward classical communication from sender to receiver does not increase the quantum capacity, however classical feedback (classical communication from receiver to sender) does. In a similar way, one can define two-way private capacity $P^{\leftrightarrow}(\Lambda)$, however there is no characterization of these two quantities in terms of entropic functions (there is no regularized or single letter formula).

3.3 Brief review on the bounds on private and quantum capacities

As we have seen in the previous chapter, due to the super additivity phenomena, computing the capacities of quantum channels is hard in most of the cases. As we mentioned earlier, there exist quantum channels for which it is necessary to compute the coherent information of unbounded uses of the channels for finding the quantum capacity [Cub+15]. Therefore, finding upper and lower bounds for the capacities is important, and bounding quantum and private capacity is the main focus of this thesis.
In Chapter 6 we will present a method, namely flagged extension, to obtain upper bounds on the quantum and private capacity of discrete channels which has a wide applicability. In Chapter 7 we extend this method to Gaussian channels to improve the previous upper bounds on Gaussian channels. Finally, in Chapter 8 we use the so called decomposition rules for thermal attenuator to improve the bounds presented in Chapter 7.
To begin with, we review the previous lower bounds for the quantum capacity found

in the literature. The standard method of finding lower bounds for quantum capacity is computing coherent information for some input state, and observing super additivity phenomena is usually an interesting result. For instance, Pauli channels exhibit super additivity in the high noise regime which result to the best lower bounds [SS96; DSS98; SS07; FW08], the most recent and comprehensive being [BL21]. Another example is dephrasure channel which is the composition of a dephasing and an erasure channel. This channel exhibits superadditivity for two uses coherent information which results to the best lower bound for the quantum capacity of dephrasure channel [LLS18a].
We do not know of any superadditivity evidence for Gaussian channels (see Chapter 4 for Gaussian channels), even in the energy-constrained setting. This is due to the fact that, in most cases, computing the coherent information for non Gaussian states is complicated, therefore maximizing the coherent information even only on one channel use is challenging. However, if we restrict the input states to be Gaussian, for the single-mode thermal attenuator at constrained energy, the superadditivity has been shown in [NPJ20].

In the following, we will concentrate on upper bounds. First of all, any capacity $\tilde{C}$ is monotonic under any arbitrary decomposition rule $\Lambda = \Lambda_1 \circ \Lambda_2$, i.e. $\tilde{C}(\Lambda) \leq \min\{\tilde{C}(\Lambda_1), \tilde{C}(\Lambda_2)\}$ [Hol19]. Therefore, knowing the quantum capacity of Λ_1 or Λ_2 results to an upper bound to the capacity of the original channel Λ. As we mentioned earlier, there are classes of channels for which the coherent information is additive and the private and quantum capacity can be calculated, namely degradable, anti-degradable, and entanglement breaking channels. Therefore, an established way to upper bound the quantum capacity of a channel is to decompose it to degradable (or anti-degradable) channels, and compute the capacity of the degradable channel. Note that this strategy also works for upper bounding the private capacity too, since for degradable channels the quantum and private capacity are equal.
For example, thermal amplifier and attenuator and the additive Gaussian noise channel (see Chapter 4) are not degradable, however they can be decomposed into zero temperature attenuator and amplifier, which are instead either degradable or antidegradable. In this way, zero capacity area which strictly includes entanglement-breaking channels [Hol08] has been found in [CGH06], and upper bounds have been found in [WQ16; Sha+18; RMG18; NAJ19; FKG21]. For discrete systems similar methods were applied to upper bound the quantum capacity of generalized amplitude damping channel [KSW20; KFG22].
A particular class of decomposition rules is the one where Λ_1 is the trace channel and Λ_2 is degradable. In this case, Λ_2 is called as the degradable extension of Λ. Flagged channels are a particular class of extended channels which we will study in detail in Chapters 6 and 7.

Definition 3.3.1 (Flagged extension of a convex combination of channels). For a channel $\Lambda = \sum_j p_j \Lambda_j$ with probability distribution $\{p_j\}$, $\{\Lambda_j\}$ channels, and a collection of states $\{\sigma_j\}$, a flagged extension is

$$\mathbb{\Lambda} = \sum_j p_j \Lambda_j \otimes \sigma_j. \tag{3.15}$$

To upper bound the quantum capacity of Λ, flag states are chosen in such a way that the resulting flagged extension to be degradable. In [SS08], a degradable extension of qubit Pauli channels with orthogonal flags was introduced. In fact, convex combination of degradable channels with orthogonal flags is always degradable. This idea was generalized in [Ouy14] to qudit Pauli channels, and developed in [LDS18], where optimization of upper bounds from flagged convex combinations of degradable and antidegradable channels were considered. In Chapters 6 we introduced degradable flagged extensions with non-orthogonal flags, and in 7 we extended this technique to Gaussian channels.

In [CG06], the authors introduced the notion of weak degradability, and later in [CGH06] they used this notion to classify single-mode Gaussian channels

Definition 3.3.2 (Weak degradability). Let $\Lambda_{A\to B}$ be

$$\Lambda_{A\to B}[X] = \mathrm{tr}_{E'}[U_{AE\to BE'} X_A \otimes \rho_E U^{\dagger}_{AE\to BE'}], \tag{3.16}$$

where ρ_E is a generic mixed state. $\Lambda_{A\to B}$ is called weakly degradable if there exists a channel $\mathcal{W}_{B\to E'}$

$$\mathrm{tr}_B[U_{AE\to BE'} X_A \otimes \rho_E U^{\dagger}_{AE\to BE'}] = \mathcal{W}_{B\to E'} \circ \Lambda_{A\to B}[X]. \tag{3.17}$$

As the name suggest, degradable channels are also weakly degradable, but the converse is not true.
Given a weakly degradable channel, it is quite easy to construct a degradable extension of the weakly degradable channel. Suppose that Λ is weakly degradable and $|\tau\rangle\langle\tau|_{EB'}$ is a purification of ρ_E. Then, one can simply show that channel ${\Lambda^E}_{A\to BB'} = \mathrm{tr}_{E'}[(U_{AE\to BE'} \otimes I_{B'}) X_A \otimes |\tau\rangle\langle\tau|_{EB'} (U_{AE\to BE'} \otimes I_{B'})^{\dagger}]$ is a degradable extension of Λ.

In the study conducted by the authors in [LS09], they demonstrated the continuity of quantum capacities. Specifically, they established that if two channels are close in terms of the diamond norm, their quantum capacities will also be close. Subsequently, in [Sut+17], the concept of approximate degradability was introduced. The authors proposed the degradability parameter as a means to quantify the proximity of an arbitrary channel to a degradable channel. This parameter can be computed by solving a semi-definite program. By calculating the degradability parameter, one can derive upper bounds on the quantum capacity of the channel under consideration. In [LLS18c], the

authors provided an analytical estimation of the degradability parameter for low noise channels, based on the diamond norm distance to the identity channel. They utilized the complementary channel as a potential degrading map in this estimation process.
In a related study [Sha+18], the concept of approximate degradability was employed to establish bounds on the quantum and private capacities of thermal attenuators and amplifiers, taking into account an energy constraint. Additionally, the work of [WQ16] explored the quantum and private capacity of infinite-dimensional systems under energy constraints.

Interestingly, these results based on degradability provide the most accurate bounds currently available for significant finite-dimensional channels. However, it is worth noting that bounds applicable to the two-way quantum capacity, which involves quantum communication assisted by unlimited forward-backward classical communication, have been proven to be state-of-the-art in low noise regimes for thermal attenuators, amplifiers, and additive Gaussian noise [Pir+17; WTB17]. As far as we know, this is the only scenario where upper bounds for two-way capacities are on par with the upper bounds provided by (approximate) degradability.

Chapter 4

Continuous Variable Systems

To explain the behaviour of many physical systems we need to use infinite dimensional Hilbert spaces, and the typical example is a particle in a quadratic potential (quantum harmonic oscillator) which can be described by continuous variables like position and momentum. Other examples of continuous-variable quantum systems include quantized modes of bosonic systems such as the different degrees of freedom of the electromagnetic field, vibrational modes of solids, atomic ensembles, nuclear spins in a quantum dot, Josephson junctions, and Bose-Einstein condensates [ARL14]. Such quantum systems can be used for quantum information processing tasks. For instance, quantum information and correlation can be encoded in the continuous degrees of freedom of photons in an optical fibre, therefore studying continuous variable systems is of a great importance from the practical point of view.

An important class of continuous variable systems is Gaussian systems. Gaussian states are the thermal states of systems with linear or quadratic Hamiltonians, and Gaussian operations describe the evolution of such systems. Gaussian systems play a fundamental role in quantum optics and field theories for two reasons. First, second-order Hamiltonians are typically dominant, therefore relevant to the real experiments. Second, it is relatively easy to deal with quadratic Hamiltonians.

In this chapter, first we briefly review the phase space formalism and notations. Then we discuss the characterization of Gaussian states and channels using symplectic matrices. The material presented in this chapter can be mostly found in [Hol19; Ser17]. The notation we adopted here is similar to [Ser17], and we mostly used [Hol19] for the communication properties of Gaussian channels.

4.1 Continuous variables

In continuous variable system, we deal with the Hilbert space of square integrable functions $L^2(\mathbb{R})$. Even if the dimension of $\mathcal{H}$ is infinite, the space is still supposed to be separable which means that there exists a countable set of vectors $\{|j\rangle, j \in \mathbb{N}\}$, so that any vector $|v\rangle \in \mathcal{H}$ can be expressed as an infinite sum in such a basis i.e. $|v\rangle = \sum_{i=1}^{\infty} |j\rangle$. Bounded operators on $\mathcal{H}$, like $\hat{A}$ [1], are the ones for which there exists a real number m such that $|\langle v| H |v\rangle| \leq m \langle v|v\rangle, \quad \forall |v\rangle \in \mathcal{H}$. For finite dimensional Hilbert spaces any bounded operator is also trace class, i.e., it admits a well-defined and finite trace. However, this is not the case for infinite dimensional Hilbert spaces. Identity operator $\hat{I}$ is a simple counter example, it is trivially bounded but not trace class. For finite dimensional Hilbert spaces, being Hermitian and self adjoint [2] are equivalent, however this is not the case for infinite dimensional case, and the spectral decomposition holds for self adjoint operators
The action of the position and momentum operators on a vector $|f\rangle \in L^2(\mathbb{R})$ are defined as

$$\begin{aligned} \hat{x}\,|f\rangle &:= xf(x) \\ \hat{p}\,|f\rangle &:= -i\frac{d}{dx}f(x)\,, \end{aligned} \tag{4.1}$$

and they satisfy the canonical commutation relation $[\hat{x}, \hat{p}] = i\hat{I}$. The eigenstates of $\hat{x}$ (and $\hat{p}$) cannot be normalized and do not belong to $L^2(\mathbb{R})$. Actually, they are linear forms acting on $L^2(\mathbb{R})$, however we use the same Dirac notation for them $|x\rangle$ (and $|p\rangle$). The inner product between two eigenstates is $\langle y|x\rangle = \delta(x-y)$, and $\langle x|f\rangle = f(x)$. As $|x\rangle$ is an eigenvector of the position operator $\hat{x}$, one can write the spectral decomposition of $\hat{x}$ as

$$\hat{x} = \int x\,|x\rangle\!\langle x|\,dx\,. \tag{4.2}$$

These pseudo vectors form a basis for $L^2(\mathbb{R})$ i.e. $\int |x\rangle\!\langle x|\,dx = \hat{I}$, and for any trace class operator $\hat{O}$ on $L^2(\mathbb{R})$ the trace is equal to $\mathrm{Tr}\left(\hat{O}\right) = \int \langle x|\,\hat{O}\,|x\rangle\,dx$ (for a mathematically rigorous discussion see [Hol19; Ser17]).

[1] Throughout this thesis all linear operators acting on square integrable functions wear a hat. Thus I and $\hat{I}$ are the identity operators acting on a finite and infinite dimensional Hilbert spaces respectively.

[2] A self-adjoint operator is Hermitian on a dense domain with respect to the topology induced, on $\mathcal{H}$, by the inner product.

4.2 Position and Momentum operators

Consider $L^2(\mathbb{R}^n)$, one can define position and momentum operators for each n different modes with the following canonical commutation relation

$$[\hat{x}_i, \hat{p}_j] = i\delta_{i,j}\hat{I}\,, \quad [\hat{x}_i, \hat{x}_j] = 0\,, \quad [\hat{p}_i, \hat{p}_j] = 0\,. \tag{4.3}$$

One can define the vector operator $\hat{\mathbf{r}}$ as

$$\hat{\mathbf{r}} := \begin{pmatrix} \hat{x}_1 \\ \hat{p}_1 \\ \vdots \\ \hat{x}_n \\ \hat{p}_n \end{pmatrix} \tag{4.4}$$

and grouping all the commutation relation in the following compact form

$$[\hat{r}_i, \hat{r}_j] = i\Omega_{ij}\hat{I}, \tag{4.5}$$

with

$$\Omega := \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{4.6}$$

being a $2n$ dimensional anti-symmetric matrix.
The creation and annihilation operators $\hat{a}_i^\dagger$, $\hat{a}_i$ are defined as

$$\hat{a}_i = \frac{\hat{x}_i + \hat{p}_i}{\sqrt{2}}, \tag{4.7}$$

They satisfy $[a_i^\dagger, a_j] = \delta_{i,j}\hat{I}$, and can be grouped as

$$\hat{\mathbf{a}} := \begin{pmatrix} \hat{a}_1 \\ \vdots \\ \hat{a}_n \end{pmatrix}. \tag{4.8}$$

The number operator on n modes is defined as

$$\hat{N} := \sum_{1=1}^{n} \hat{a}_i^\dagger a_i\,. \tag{4.9}$$

The eigenvectors of $\hat{N}$ are labelled by natural numbers $\{j_i : j_i \in \mathbb{N}\}$, and

$$\hat{N}\,|j_1, ..., j_n\rangle = (\sum_{i=1}^{n} j_i)\,|j_1, ..., j_n\rangle\ . \tag{4.10}$$

They are called Fock states and form a orthonormal basis for $L^2(\mathbb{R}^n)$.
Displacement operator on n modes is defined as

$$\hat{D}(\mathbf{r}) := \exp\left(\mathrm{i}\mathbf{r}^\intercal \Omega \hat{\mathbf{r}}\right), \qquad \mathbf{r} \in \mathbb{R}^{2m}. \tag{4.11}$$

which shifts the combined position and momentum operator

$$\hat{D}(\mathbf{r})\hat{\mathbf{r}}\hat{D}(\mathbf{r})^\dagger = \hat{\mathbf{r}} + \mathbf{r}\,. \tag{4.12}$$

As the argument of the exponential function is an anti-hermitian, displacement operators are unitary and satisfy

$$\hat{D}(\mathbf{r}_1 + \mathbf{r}_2) = \hat{D}(\mathbf{r}_1)\hat{D}(\mathbf{r}_2)e^{\mathrm{i}\mathbf{r}_1^\intercal \Omega \mathbf{r}_2/2}, \tag{4.13}$$

Displacement operators form a basis for the space of all bounded operators on $L^2(\mathbb{R}^n)$ [Ser17]. More precisely, one can write any bounded operator $\hat{O}$ as

$$\hat{O} = \frac{1}{\pi}\int d\mathbf{r}\,\mathrm{Tr}\left[\hat{O}\hat{D}(-\mathbf{r})\right]\hat{D}(\mathbf{r})\,, \tag{4.14}$$

where $d\mathbf{r} = dx_1 dp_1..dx_n dp_n$, and displacement operators are orthogonal

$$\mathrm{tr}\left[\hat{D}(\mathbf{r}_1)\hat{D}(-\mathbf{r}_2)\right] = (2\pi)^n \delta(\mathbf{r}_1 - \mathbf{r}_2). \tag{4.15}$$

Therefore, the characteristic function defined as $\chi(\mathbf{r}) := \mathrm{Tr}\left[\hat{O}\hat{D}(-\mathbf{r})\right]$ provides the full characterization of any trace class operator $\hat{O}$.
One can do a simple change of parameters $\alpha_i := \frac{x_i + p_i}{\sqrt{2}}$, and define an n dimensional vector of complex numbers $\boldsymbol{\alpha}^\intercal := (\alpha_1, ..., \alpha_n)$. In this notation, the displacement operator can be written in terms of creation and annihilation operators as $\hat{D}(\boldsymbol{\alpha}) = e^{\sum_i \alpha a_i - \alpha_i^* a_i^\dagger}$. Coherent states defined as $|\boldsymbol{\alpha}\rangle = \hat{D}(\boldsymbol{\alpha})\,|0\rangle$ are the eigenvectors of $\hat{\mathbf{a}}$ with the following eigenvalues

$$\hat{\mathbf{a}}\,|\boldsymbol{\alpha}\rangle := \hat{a}_1\,|\alpha_1\rangle\,...\hat{a_n}\,|\alpha\rangle_n = (\prod_{i=1}^{n}\alpha_i)\,|\boldsymbol{\alpha}\rangle\,. \tag{4.16}$$

Note that $|\boldsymbol{\alpha}\rangle$ are always product states, and form a resolution of the identity

$$\int \frac{d^2\boldsymbol{\alpha}}{\pi^n}\,|\boldsymbol{\alpha}\rangle\!\langle\boldsymbol{\alpha}| = \hat{I}, \tag{4.17}$$

4.3 Gaussian states

Second-order Hamiltonian are Hamiltonians which can be expressed as a polynomial of order two in terms of the vector of operators $\hat{\mathbf{r}}$, so the most general form of such Hamiltonians is

$$\hat{H} = \frac{1}{2}\hat{\mathbf{r}^\intercal} H \hat{\mathbf{r}} + \hat{\mathbf{r}^\intercal}\mathbf{r} \tag{4.18}$$

where $\mathbf{r}$ is a $2n$ dimensional vector and $H > 0$ is a symmetric positive definite matrix. H is assumed to be symmetric since any anti symmetric component can only contribute to an identity term because of the canonical commutation relations. H is supposed to be positive definite since we only analyse the stable Hamiltonians. Second order Hamiltonian are significantly important as often the higher order terms are negligible in many physical system quantum such as quantum optics.
Gaussian states are the thermal states of second order Hamiltonians, and there exist three equivalent characterizations of Gaussian states:

- **Describing the Gaussian states diagonalizing the quadratic Hamiltonian:** Using Williamsons's Theorem [Ser17], one can show that thermal states of the quadratic Hamiltonian in Eq. 4.18 can be written as

$$\hat{\rho}_G = \frac{e^{-\beta \hat{H}}}{\mathrm{tr}\left[e^{-\beta \hat{H}}\right]}\,, \tag{4.19}$$

  with $\beta \geq 0$ being the inverse temperature. It can be shown that such state can be written as

$$\hat{\rho}_G = \hat{D}(-\bar{\mathbf{r}})\hat{S}\frac{\bigotimes_{j=1}^{n} e^{-\beta \hat{H}_{\omega_j}}}{\prod_{j=1}^{n} \mathrm{tr}\left(e^{-\beta \hat{H}_{\omega_j}}\right)}\hat{S}^{\dagger}\hat{D}(\bar{\mathbf{r}}) \tag{4.20}$$

  where

$$\begin{aligned} \bar{\mathbf{r}} &:= H^{-1}\mathbf{r}\,, \\ \hat{H}_{\omega_j} &:= \omega_j(\hat{x}_j^2 + \hat{p}_j^2)\,, \end{aligned} \tag{4.21}$$

  and $\{\omega_j\}$ being the eigenvalues of $|i\Omega H|$ which come in pairs ($|i\Omega H|$ has $2n$ eigenvalues and any ω_j appears two times in the spectrum of $|i\Omega H|$). $\{\omega_j\}$ are often called as the symplectic eigenvalues of H. The operator $\hat{S}$ can be shown to be a unitary [Ser17], however its explicit form may not be a a matter of interest in this thesis. Using the Eq. 4.20, then it is easy to calculate the spectrum of Gaussian states, as $\hat{D}_{\bar{\mathbf{r}}}$ and $\hat{S}$ are unitary operators, and what remains is a tensor product of one mode Gaussian states which are easy to deal with.

- **Describing Gaussian states using the first and second moments:** The first and second moments of a Gaussian state $\hat{\rho}_G$ are defined as

$$\begin{aligned} \bar{\mathbf{r}} &:= \mathrm{tr}[\hat{\mathbf{r}}\hat{\rho}_G]\,, \\ \boldsymbol{\sigma} &:= \mathrm{tr}\left[\{(\hat{\mathbf{r}} - \bar{\mathbf{r}}), (\hat{\mathbf{r}} - \bar{\mathbf{r}})^{\mathrm{T}}\}\hat{\rho}_G\right] \end{aligned}$$

  with the anti-commutator defined as $\{\hat{A}, \hat{B}\} := \hat{A}\hat{B} + \hat{B}\hat{A}$. It can be shown that the first and second moments fully characterize the Gaussian states. In fact, the first momentum is equal to $\bar{\mathbf{r}}$ in Eq. 4.21, and the symplectic eigenvalues of the second moment $\{\nu_j\}$ (the eigenvalues of $|i\Omega\boldsymbol{\sigma}|$) are related to $\{\omega_j\}$ as follows [Ser17]

$$\nu_j = \frac{1 + e^{-\beta\omega_j}}{1 - e^{-\beta\omega_j}} .$$

Therefore, the second moment (often called as variance matrix) fully characterizes the spectrum of any Gaussian state.

- **Describing Gaussian states using the characteristic function:** The characteristic function defined in the previous section, fully determines any bounded operator. The characteristic function of Gaussian states are Gaussian and it can be written in terms of first and second moments as follows [Ser17]

$$\chi_{\hat{\rho}}(\mathbf{r}) = \exp\left(-\frac{1}{4}\mathbf{r}^{\mathsf{T}}\Omega^{\mathsf{T}}\boldsymbol{\sigma}\Omega\mathbf{r} + \mathrm{i}\mathbf{r}^{\mathsf{T}}\Omega\bar{\mathbf{r}}\right) . \tag{4.22}$$

Combining Eq.4.20,4.22, and doing simple algebra we note that the entropy of any Gaussian state with variance matrix $\boldsymbol{\sigma}$ is

$$S(\hat{\rho}) = \sum_{i=1}^{m} h(\nu_i) \qquad h(x) := \frac{x+1}{2}\log\frac{x+1}{2} - \frac{x-1}{2}\log\frac{x-1}{2} . \tag{4.23}$$

where $\{\nu_j\}$ being the symplectic eigenvalues of $\boldsymbol{\sigma}$.
An important one mode Gaussian state is thermal state. A thermal state with energy N (the average of number operator $\hat{N}$) is defined as

$$\hat{\tau}_N := \frac{1}{N+1}\sum_{i=1}^{n}\left(\frac{N}{N+1}\right)^{i} |i\rangle\langle i| . \tag{4.24}$$

The first and second moments are $\bar{\mathbf{r}} = 0$ and $\boldsymbol{\sigma} = (2N+1)I_2$ respectively.
The purification of thermal state is two mode squeezed state $|\tau_N\rangle$ and has the following first and second moments

$$\begin{aligned} \bar{\mathbf{r}}_{|\tau_N\rangle} &= 0 \\ \boldsymbol{\sigma}_{|\tau_N\rangle} &= \begin{pmatrix} (2N+1)I_2 & 2\sqrt{N(N+1)}\sigma_3 \\ 2\sqrt{N(N+1)}\sigma_3 & (2N+1)I_2 \end{pmatrix} , \end{aligned} \tag{4.25}$$

with I_2 being two dimensional identity and

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{4.26}$$

Another one mode Gaussian state that we will later use in Chapter 7 is single mode squeezed state which is pure, and defined as

$$|r\rangle = \exp\Big(\frac{r}{2}(\hat{a}^2 - \hat{a}^{\dagger 2})\Big)\,|0\rangle\,, \tag{4.27}$$

with the following first and second momentums $\bar{\mathbf{r}} = 0$ and $\boldsymbol{\sigma} = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}$.

4.4 Gaussian Channels

Gaussian channels describe the dynamics of open systems interacting with a Gaussian environment through a quadratic Hamiltonian. As this can be described in Stinespring representation, such maps are CPTP, and they transform Gaussian states to Gaussian states. The action of Gaussian channel on the first and second moments of Gaussian states fully characterizes the Gaussian channels [Ser17]. The following theorem gives the characterization of n mode Gaussian channels

Theorem 4.4.1 (Classification of Gaussian channels). *Any Gaussian channel* $\Lambda : \Sigma(L^2(\mathbb{R}^n)) \to \Sigma(L^2(\mathbb{R}^n))$ *transforms the first and second moments of Gaussian states as*

$$\begin{aligned} \bar{\mathbf{r}} &\to X\bar{\mathbf{r}} + \mathbf{r} \\ \boldsymbol{\sigma} &\to X\boldsymbol{\sigma}X^{\mathsf{T}} + Y \end{aligned} \tag{4.28}$$

with X, Y *real* $n \times n$ *matrices,* $\mathbf{r}$ *an* n *dimensional real vector, and*

$$Y + i\Omega \geq iX\Omega X^{\mathsf{T}}. \tag{4.29}$$

Equivalently, this can be expressed in terms of characteristic function

$$\chi_{\hat{\rho}}(\mathbf{r}) \to \chi_{\Lambda[\hat{\rho}]}(\mathbf{r}) = \chi_{\hat{\rho}}(\Omega^{\mathsf{T}}X\Omega\mathbf{r})e^{-\frac{1}{4}\mathbf{r}^{\mathsf{T}}\Omega^{\mathsf{T}}Y\Omega\mathbf{r}}. \tag{4.30}$$

An important class of Gaussian channels are gauge covariant [Hol19] channels which have the following symmetry

$$\Lambda[e^{-i\theta\hat{N}}\rho e^{i\theta\hat{N}}] = e^{-i\theta\hat{N}}\Lambda[\rho]e^{i\theta\hat{N}}, \tag{4.31}$$

We will also refer to these channels as phase-insensitive channels. For gauge covariant channels the Holevo information is additive, and therefore the classical capacity is known [Gio+14; Hol19]. However, for the coherent information and quantum capacity no such simplification is known. In particular, the quantum capacity of single mode phase insensitive Gaussian channels, namely thermal attenuator, thermal amplifier, and

Additive Gaussian noise, is not known. We first introduce these channels, and will put bounds on their quantum capacities in Chapters 7.

Thermal attenuator $\mathcal{E}_{\eta,N}$, also called as thermal loss, describes the attenuation of signals in the presence of thermal environment. thermal attenuators are good realistic models to describe the noise in the optical fibres, therefore they are so important from the practical point of view. In Stinespring representation, the interaction between the system and environment is given by a beam splitter with parameter η and environment is in thermal state (or its purification i.e. two mode squeezed state) with parameter N

$$\mathcal{E}_{\eta,N}[\hat{\rho}_A] := \mathrm{Tr}_E[\hat{U}_\eta(\hat{\rho}_A \otimes (|\tau_N\rangle\langle\tau_N|_E)\hat{U}_\eta^\dagger] \tag{4.32}$$

where $\hat{U}_\eta$ $(0 \leq \eta \leq 1)$ is a two-mode unitary operator transforming $\hat{\mathbf{r}}$ as

$$\hat{U}_\eta \hat{\mathbf{r}} \hat{U}_\eta^\dagger = \begin{pmatrix} \sqrt{\eta} I_2 & \sqrt{1-\eta} I_2 \\ -\sqrt{1-\eta} I_2 & \sqrt{\eta} I_2 \end{pmatrix} \hat{\mathbf{r}} \tag{4.33}$$

and $|\tau_N\rangle$ is defined in 4.25. Doing simple algebra, one can show that the action of thermal attenuator on the first and second moment of Gaussian states is as follows [CGH06]

$$\bar{\mathbf{r}} \xrightarrow{\mathcal{E}_{\eta,N}} \bar{\mathbf{r}}' = \sqrt{\eta}\bar{\mathbf{r}} \;, \tag{4.34}$$

$$\boldsymbol{\sigma} \xrightarrow{\mathcal{E}_{\eta,N}} \boldsymbol{\sigma}' = \eta\boldsymbol{\sigma} + (1-\eta)(2N+1)I_2 \,, \tag{4.35}$$

We also briefly review single-mode thermal amplifiers $\Phi_{g,N}$. In the Stinespring representation of thermal amplifier, the input state interacts with a thermal bath through a two mode squeezing operator with parameter $g \geq 1$ In this case the input state interacts with a thermal bath through a two mode squeezing operator with parameter $g \geq 1$

$$\Phi_{g,N}[\hat{\rho}_A] := \mathrm{Tr}_E[\hat{S}_g(\hat{\rho}_A \otimes (|\tau_N\rangle\langle\tau_N|)_E)\hat{S}_g^\dagger] \,, \tag{4.36}$$

with $\hat{S}_k$ mapping the operator $\hat{\mathbf{r}}$ as

$$\hat{S}_g \hat{\mathbf{r}} \hat{S}_g^\dagger = \begin{pmatrix} \sqrt{g} I_2 & \sqrt{g-1}\sigma_3 \\ \sqrt{g-1}\sigma_3 & \sqrt{g} I_2 \end{pmatrix} \hat{\mathbf{r}}. \tag{4.37}$$

with simple calculations we can show that thermal amplifier transforms the first and second moments as

$$\bar{\mathbf{r}} \xrightarrow{\Phi_{g,N}} \bar{\mathbf{r}}' = \sqrt{g}\bar{\mathbf{r}} \;, \tag{4.38}$$

$$\boldsymbol{\sigma} \xrightarrow{\Phi_{g,N}} \boldsymbol{\sigma}' = g\boldsymbol{\sigma} + (g-1)(2N+1)I_2 \,. \tag{4.39}$$

Finally, the single mode additive Gaussian noise channel Λ_β can be written as

$$\Lambda_\beta[\hat{\rho}] := \frac{\beta}{2\pi}\int_{\mathbb{R}^2} \mathrm{d}\mathbf{r} e^{-\frac{\beta}{2}\mathbf{r}^\intercal\mathbf{r}}\hat{D}(\mathbf{r})\hat{\rho}\hat{D}(\mathbf{r})^\dagger, \tag{4.40}$$

where $\beta > 0$. Its action on first and second moments is as follows

$$\bar{\mathbf{r}} \xrightarrow{\Lambda_\beta} \bar{\mathbf{r}}' = \bar{\mathbf{r}}\ , \tag{4.41}$$

$$\boldsymbol{\sigma} \xrightarrow{\Lambda_\beta} \boldsymbol{\sigma}' = \boldsymbol{\sigma} + 2I_2/\beta\,, \tag{4.42}$$

Additive Gaussian noise has a symmetric structure, and adds uniform noise, with an intensity proportional to $1/\beta$, to the state. Additive Gaussian noise is important for its symmetrical structure and the fact that it is the quantum counterpart of white noise.

Additive Gaussian noise is an example of classical mixing channel [Ser17], characterized as follows

$$\mathbf{m} \xrightarrow{\Lambda_Y} \mathbf{m}' = \mathbf{m}\ , \qquad V \xrightarrow{\Lambda_Y} V' = V + Y\ , \tag{4.43}$$

where $Y \geq 0$ is a positive operator. In fact, classical mixing channels can be written in Kraus representation in the following form

$$\Lambda_Y[\hat{\rho}] := \int_{S(Y)} \mathrm{d}\mathbf{r}\frac{e^{-\mathbf{r}^\intercal Y^{\ominus 1}\mathbf{r}}}{\sqrt{\pi}^{\dim S(Y)}\sqrt{\det_+ Y}}\hat{D}(\mathbf{r})\hat{\rho}\hat{D}(\mathbf{r})^\dagger\ , \tag{4.44}$$

where eigenvalues $\{\lambda_i\}$ are the eigenvalues of Y, and $S(Y)$ indicates the support of Y. $\det_+ Y = \prod_{i:\lambda_i>0}\lambda_i$, and $Y^{\ominus 1}$ is the pseudoinverse of Y.

The following theorem, characterizes the coherent information of degradable channels [Hol19], and we will later use it in Chapter 7 to compute the quantum capacity of degradable extensions of single mode phase intensive quantum channels to find some useful upper bounds.

Theorem 4.4.2 (Coherent information of degradable Gaussian channels). *For a degradable Gaussian channel* Λ *i.e.* $\tilde{\mathcal{N}} = \Gamma \circ \Lambda$*, with a Gaussian degrading map* Γ*, Gaussian states maximize the coherent information* $I_c(\Lambda, \hat{\rho})$*. In particular, If* Λ *is phase-insensitive, the coherent information is maximized on gauge-invariant Gaussian states.*

The final statement in the theorem can be simply shown using the concavity of coherent information of degradable channels, Theorem 3.2.5. More precisely, for a phase-covariant degradable channel

$$I_c(\Lambda, \Phi_m[\hat{\rho}]) \geq \frac{1}{2\pi}\int_0^{2\pi} d\theta I_c(\Lambda, \hat{U}(\theta)\hat{\rho}\hat{U}(\theta)) = I_c(\Lambda, \hat{\rho}), \tag{4.45}$$

the inequality due to concavity and the equality due to phase covariance, simply writing $I_c(\Lambda, \hat{\rho}) = S(\Lambda[\hat{\rho}]) - S(\Lambda \otimes \mathcal{I}[|\rho\rangle\langle\rho|])$, where $|\rho\rangle$ is a purification of $\hat{\rho}$. This means that we can maximize among gauge-invariant states, and therefore gauge-invariant Gaussian states by the first part of Theorem 4.4.2.

Chapter 5

Optimal Subtracting Machine

5.1 Preface

The material in this chapter is based on the published article [KFG19]:

- Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Optimal quantum subtracting machine". In: *Physical Review A* 99.5 (2019), p. 052319.

In this chapter, the impossibility of undoing a mixing process is analysed in the context of quantum information theory. The optimal machine to undo the mixing process is studied in the case of pure states, focusing on qubit systems. Exploiting the symmetry of the problem we parametrise the optimal machine in such a way that the number of parameters grows polynomially in the size of the problem. This simplification makes the numerical methods feasible. For simple but non-trivial cases we computed the analytical solution, comparing the performance of the optimal machine with other protocols.

5.2 Introduction

A fundamental fact in quantum information theory is that not all maps between quantum states are possible: even before considering practical difficulties, quantum theory itself limits the operations that can be performed. A series of quantum no-go theorems [WZ82; Wer01; Die82; NC97; PB00; PHH08; AR+15; Osz+16] shows that transformations which would be very valuable from the point of view of information processing are in fact impossible. The most celebrated of them is the no-cloning theorem [WZ82]: the impossibility of cloning makes many processing tasks (e.g. state estimation) non-trivial. Nonetheless, the importance of these impossible transformations drives the search for approximate implementations of them: optimal cloners [Sca+05] have been extensively studied, and similar efforts have been spent for other no-go theorems [AR+15; Osz+16; DKK17; Dog+18; Hay+21].

Here we introduce the no-subtracting theorem, which states the impossibility of undoing the mixing operation that involves a target state we wish to recover and an external noise source, and define the optimal subtractor operation which solves the problem with the best allowed approximation. This task is somehow related to those discussed in [BRS07] and references therein, where one aims to perform quantum information processing of some sort (e.g. the recovery of the target state) when some classical knowledge (i.e. the reference frame for [BRS07] and the amount of mixed noise for us) is replaced by bounded information encoded into the density matrix of an ancillary quantum system. Finding the optimal subtractor corresponds to a semidefinite program involving a number of variables that in principle grows exponentially with the input data (system copies). However, by exploiting the symmetry of the problem and a proper parametrisation of the N to 1 qubit covariant channels (analogous to those introduced in [GS08; Boi+08]), the number of effective parameters can be reduced to a subset which only scales polynomially. This reduction of the parameters makes the numerical optimisation feasible, and for small enough input data, allows also for analytical treatment.

As a final consideration we would also to point out that the problem we address in the present paper can also be seen as an instance of quantum machine learning [Wit14; Bia+17; DB17], an emerging area of quantum information theory that deals with tasks that generalise the “learning from example" concept in a genuine quantum information theory setting. In these tasks a machine should be trained to perform a certain quantum operation and this training can be done through quantum processing, that means with quantum training data and quantum operations. The fundamental difference with classical training tasks is that there is not an a priori separation between the training and the execution phases, because of entanglement. Indeed, in our analysis we search for the best machine that can be trained with copies of the noise in order to make it able to recover disturbed signals, with the only requirement that the machine is allowed by quantum mechanics.

This chapter is organized as follows: we start in Sec. 5.3 by formalizing the problem. In Sec. 5.4 we present some preliminary results on the efficiency of a universal quantum subtractor which can drawn from general consideration on the problem without passing the explicit optimization stage. In Sec. 5.5 we then proceed with the explicit solution of the optimization problem. The paper ends with Sec. 5.6. Technical derivations are presented in the Appendix.

5.3 Optimal Subtractor

An Universal Quantum Subtracting machine UQS is a two-inputs/one-output transformation acting on two isomorphic discrete quantum systems A and B. When provided by factorised input states of the form $(p\rho_0 + (1-p)\rho_1) \otimes \rho_0$, with $p \in [0,1]$ assigned and $\rho_0, \rho_1 \in \mathcal{D}(\mathcal{H})$ arbitrary density matrices, it returns as output the system A into the state ρ_1 realizing the mapping

$$\mathrm{UQS}\big[\rho_{\mathrm{mix}}(p) \otimes \rho_0\big] = \rho_1 \;, \tag{5.1}$$

which effectively allows one to recover ρ_1 from the mixture $\rho_{\mathrm{mix}}(p) := p\rho_0 + (1-p)\rho_1$ by “removing" the perturbing state ρ_0 and renormalizing the result. Unfortunately the possibility of physically realizing an UQS machine for $p > 0$, turns out to be in contradiction with the basic requirements that any quantum evolution has to fulfil, see e.g. Ref. [Hol19]. Indeed, invoking linearity and using the fact that for $\rho_1 = \rho_0$ one has $\mathrm{UQS}[\rho_0 \otimes \rho_0] = \rho_0$, Eq. (5.1) can be cast in the following form

$$(1-p)\mathrm{UQS}[\rho_1 \otimes \rho_0] = \rho_1 - p\rho_0, \tag{5.2}$$

which, as long as the parameter p is strictly different from 0, will produce unphysical non-positive results as soon as the support of ρ_0 admits a non trivial overlap with the kernel of ρ_1. Yet, as in the case of other better studied impossible quantum machines [Wer01], there could be still room for approximate implementations of the mapping (5.1). In what follows we shall hence try to identify the implementation of an optimal UQS, i.e. a machine which, being physically realizable via a Completely Positive and Trace Preserving (CPTP) map [Hol19], would give us the best approximation of the transformation (5.1). More generally we are also interested in a generalisation of the problem where instead of a single copy of the mixture $p\rho_1 + (1-p)\rho_0$ and of the noise state ρ_0, we are now provided with n_1 copies of the first and n_2 copies of the second, i.e. in the optimal CPTP implementation of the $\Sigma(\mathcal{H}^{\otimes n_1+n_2}) \to \Sigma(\mathcal{H})$ mapping

$$\mathrm{UQS}^{(n_1,n_2)}\big[(p\rho_0 + (1-p)\rho_1)^{\otimes n_1} \otimes \rho_0^{\otimes n_2}\big] = \rho_1 \;. \tag{5.3}$$

As a figure of merit we shall consider the fidelity [NC02] between the obtained output and the intended target states, properly averaged with respect to all possible inputs. To simplify the analysis in what follows we restrict ourself to the special case where both ρ_0 and ρ_1 are pure states of the d-dimensional space $\mathcal{H}$, namely $\rho_1 = |\psi\rangle\langle\psi|$ and $\rho_0 = |\phi\rangle\langle\phi|$, where without loss of generality we adopt the parametrisation $|\psi\rangle := U|\uparrow\rangle$ and $|\phi\rangle := V|\uparrow\rangle$, with $|\uparrow\rangle$ being a fixed vector and U, V are arbitrary elements of the unitary set $SU(d)$. Indicating hence with Λ the CPTP mapping that we want to test as a candidate for the implementation of $\mathrm{UQS}^{(n_1,n_2)}$, we evaluate its performance through the function

$$F_{n_1,n_2}(\Lambda) := \iint d\mu_U d\mu_V \, \langle\psi| \Lambda[\rho_{\mathrm{mix}}^{\otimes n_1}(p) \otimes \rho_0^{\otimes n_2}] |\psi\rangle \;, \tag{5.4}$$

where the integral are performed via the Haar measure of $SU(d)$ to ensure a uniform distribution of $|\psi\rangle$ and $|\phi\rangle$ on $\mathcal{H}$. Before entering into the technical derivation, it is worth commenting that while the problem we are facing can be seen as a sort of purification procedure, it is definitely different from the task addressed by Cirac et al. in Ref. [CEM99], which is designed to remove the largest fraction of complete mixed state from ρ_{mix} having access to some copies of it, but with no prior information on ρ_0 or p.

5.3.1 Connection to Quantum Error Correction

Equation (5.1) can be described as the formal inversion of the transformation $\text{IQA}[\rho_0 \otimes \rho_1] = \rho_{\text{mix}}(p)$, which we may dub Incoherent Quantum Adder. At variance with the Coherent Quantum Adder analyzed in Refs. [AR+15; DKK17; Dog+18], an IQA can be easily implemented as it merely consists in creating a probability mixture out of two input configurations. In particular, IQA can be interpreted as an open quantum evolution [Hol19; NC02; Kin03] in which the state ρ_0 of the input B, plays the role of the environment. In this scenario, the aim is to undo the action of IQA and recover ρ_1 not having the full knowledge about the environment, the only information available being encoded through copies of ρ_0. In view of this observation the optimal quantum subtracting problem can be seen as a first example of a new way of approaching quantum error correction schemes. We are thinking for instance to communication scenarios where, the transformation tampering the received state at the output of the channel is affected by interactions with an external environment E that is susceptible to modifications on which the communicating parties (say Alice and Bob) do not have a complete record. To be more precise, imagine the following realistic situation where Alice uses a noisy channel to communicate with Bob. Therefore, the states that Alice wants to send to Bob ρ_1, interacts with the environment ρ_0. The coupling Hamiltonian H between the information carrier S and E and the transfer time τ of the communication are somehow fixed and known. while the state ρ_0 of the environment is not – ρ_0 is a sort of a random, possibly time-dependent variable of the problem. Accordingly, Bob receives by $\rho_1' = \text{Tr}_E[U_{SE}(\rho_1 \otimes \rho_0)U_{SE}^\dagger]$ with $U_{SE} = \exp[-iH\tau]$ and $\text{Tr}_E[...]$ being the partial trace over E. The fundamental task for the receiver of the message is clearly to recover ρ_1 from ρ_1': in the standard approach to quantum communication this is facilitated by the assumption that Alice and Bob have also perfect knowledge about ρ_0 which in our setting is no longer granted. To compensate for this lack of information it is hence important for the receiver of the message to sample the state of E in real time during the information exchange, a scenario which we can model e.g. by assuming Bob to have access to some copies of ρ_0. The optimal subtracting scheme we discuss in the manuscript addresses exactly this problem for the special (yet not trivial) case where U_{SE} describes a partial swap gate (see e.g. [Sca+02]).

Given the above premise it should be now clear that the possibility of constructing an UQS machine will have a profound impact in many practical applications, spanning from quantum computation [NC02; Lad+10], where it could be employed as an effective error correction procedure for certain kind of errors, to quantum communication [GT07], where instead it could be used as a decoding operation to distill the intended messages from the received deteriorated signals.

5.4 Preliminary results

The maximum of Eq. (5.4) with respect to all possible CPTP transformations

$$F^{(\max)}_{n_1,n_2} := \max_{\Lambda \in \text{CPTP}} F_{n_1,n_2}(\Lambda), \tag{5.5}$$

is the quantity we are going to study in the following. Since one can always neglect part of the input copies, this functional is clearly non-decreasing in n_1 and n_2, i.e.

$$F^{(\max)}_{n_1,n_2} \le F^{(\max)}_{n_1+1,n_2}, F^{(\max)}_{n_1,n_2+1}, \tag{5.6}$$

with no ordering between the last two terms been foreseen from first principles. In particular, we are interested in comparing $F^{(\max)}_{n_1,n_2}$ with the performances achievable via a trivial "doing nothing" (DN) strategy in which one emulates the mapping (5.3) by simply returning as output one of the qubits of the register A, i.e. the state $\rho_{\text{mix}}(p)$. In this case, the associated average fidelity can be easily computed by exploiting the depolarizing identity

$$\int d\mu_U |\psi\rangle\langle\psi| = \int d\mu_U U\,|\uparrow\rangle\,\langle\uparrow|\,U^\dagger = I/d\,, \tag{5.7}$$

obtaining

$$F_{n_1,n_2}(\text{DN}) := 1 - p(d-1)/d\,, \tag{5.8}$$

which, by construction constitutes a lower bound for $F^{(\max)}_{n_1,n_2}$, i.e.

$$F^{(\max)}_{n_1,n_2} \ge 1 - p(d-1)/d\,, \tag{5.9}$$

(incidentally for the qubit case, $F_{n_1,n_2}(\text{DN})$ coincides with the average fidelity on would obtain by adapting the optimal protocol of the Cirac et al. scheme [CEM99] to our setting, see Ref. [CEM99]). Determining the exact value of $F^{(\max)}_{n_1,n_2}$ is typically very demanding apart from the case where we have a single copy of A, i.e. for $n_1 = 1$. In this scenario in fact, irrespectively from the value of n_2, one can prove that the DN strategy is optimal, transforming the inequality (5.9) into the identity

$$F^{(\max)}_{1,n_2} = 1 - p(d-1)/d\,. \tag{5.10}$$

One way to see this is to show that (5.10) holds in the asymptotic limit of infinitely many copies of the B state, i.e. $n_2 \to \infty$, and then invoke the monotonicity under n_2 to extent such result to all the other cases. As a matter of fact when n_2 diverges one can use quantum tomography to recover the classical description of B from the input data: accordingly the optimal implementation of $\mathrm{UQS}^{(1,\infty)}$ formally coincides with the optimal recovery map [Ipp+15] aiming to invert the CPTP transformation that takes a generic element $\rho_1 \in \mathcal{D}(\mathcal{H})$ into $\rho_{\mathrm{mix}}(p)$. In this case (5.4) gets replaced by

$$F_{1,\infty}(\Lambda) := \int d\mu_U \langle\psi| \Lambda[(1-p)|\psi\rangle\langle\psi| + p|\phi\rangle\langle\phi|] |\psi\rangle \ , \tag{5.11}$$

which thanks to the depolarizing identity can be easily shown to admit $F_{n_1,n_2}(\mathrm{DN})$ not just as a lower bound but also as an upper bound, leading to

$$F_{1,\infty}^{(\max)} = 1 - p(d-1)/d \ , \tag{5.12}$$

and hence to (5.10).

As n_1 gets larger than 1, we expect to see a non trivial improvement with respect to the DN strategy. This is clearly evident at least in the case where both n_1 and n_2 diverge (i.e. $n_1, n_2 \to \infty$). In this regime, similarly to the case of optimal quantum cloner [WZ82; BH96; Wer98; GM97; Bru+98; Sca+05], Eq. (5.3) becomes implementable by means of a simple measure-and-prepare (MP) strategy based on performing full quantum tomography on both inputs A and B, yielding the optimal value $F_{\infty,\infty}^{(\max)} = 1$ which clearly surpasses the DN threshold. In the next sections, we shall clarify a procedure that one can follow to solve the optimisation of Eq. (5.4) for finite values of the input copies. For the sake of simplicity we present it for the special cases where A and B are just qubit systems and we use such technique to analytically compute the exact value of $F_{n_1,n_2}^{(\max)}$ for the simplest but non-trivial scenario where $n_1 = 2$ and $n_2 = 1$. Via numerical methods we also solve the optimisation problem for some selected values of p, n_1 and n_2, see Fig. 5.2.

5.5 Channel optimisation

The problem we are considering has special symmetries that allows for some simplifications. Invoking the linearity of Λ and the invariance of the Haar measure we can rewrite (5.4) as $F_{n_1,n_2}(\Lambda) = \langle\uparrow| \Lambda_c[\Omega_{n_1 n_2}] |\uparrow\rangle$, where $\Omega_{n_1 n_2}$ is the density operator

$$\Omega_{n_1 n_2} \ := \ \int d\mu_V \left(p|\uparrow\rangle\langle\uparrow| + (1-p)V|\uparrow\rangle\langle\uparrow|V^\dagger\right)^{\otimes n_1} \ \otimes \ \left(V|\uparrow\rangle\langle\uparrow|V^\dagger\right)^{\otimes n_2} . \tag{5.13}$$

The channel Λ_c appearing in the expression for $F_{n_1,n_2}(\Lambda)$ is obtained from Λ through the following integral

$$\Lambda_c[\cdots] = \int d\mu_U \ U\Lambda[U^{\dagger^{\otimes N}} \cdots U^{\otimes N}]U^\dagger \ , \tag{5.14}$$

which ensures that Λ_c is a N qubits to 1 qubit covariant map, i.e. a CPTP transformation fulfilling the condition

$$U^\dagger \Lambda_c[\cdots]U = \Lambda_c[U^{\dagger\otimes N} \cdots U^{\otimes N}] \;, \tag{5.15}$$

$\forall U \in SU(2)$ [Hol02]. Notice also that if Λ is already covariant, then it coincides with its associated Λ_c, i.e. $\Lambda_c = \Lambda$. Exploiting these facts we can hence conclude that the maximisation of $F_{n_1,n_2}(\Lambda)$ can be performed by just focusing on this special set of transformations which now we shall parametrise. The integral appearing in (5.14) motivates us to choose the total angular momentum eigenbasis as the basis for the Hilbert space $\mathcal{H}_2^{\otimes N}$ where the channel operates. Specifically we shall write such vectors as $|j,m,g\rangle$ with j the total angular momentum of N spin 1/2 particles, m the total angular momentum in z direction, and g labelling different equivalent representations with total angular momentum j. Following the derivation presented in A we can then verify that, indicating with $\{|j=\frac{1}{2},s\rangle\}_{s=\pm\frac{1}{2}}$ the angular momentum basis for a single qubit (no degeneracy being present), one has

$$\begin{aligned}\langle \tfrac{1}{2}, s|\,\Lambda_c\left[|j,m,g\rangle\langle j',m',g'|\right]|\tfrac{1}{2},s'\rangle &= (-1)^{m-m'} \\ \times\delta_{s-m,s'-m'} \sum_{q\in Q_{j,j'}} C^{q\quad s-m}_{\frac{1}{2}\,s,j\;-m}\, C^{q\quad s'-m'}_{\frac{1}{2}\,s',j'\,-m'}\; W^{j,j'}_{q,g,g'}\;,\end{aligned} \tag{5.16}$$

where the summation over the index q runs over

$$Q_{j,j'} := \{j \pm \frac{1}{2}\} \cap \{j' \pm \frac{1}{2}\} \;, \tag{5.17}$$

(if the set is empty then the associated matrix element is automatically null), where

$$C^{J\quad M}_{j\,m,j'\,m'} := \langle J,M|j,m\rangle \otimes |j',m'\rangle \;, \tag{5.18}$$

is a Clebsch-Gordan coefficient, and where finally

$$W^{j,j'}_{q,g,g'} := \mathbf{v}^j_{q,g} \cdot (\mathbf{v}^{j'}_{q,g'})^\dagger \;, \tag{5.19}$$

represents the scalar product between the complex row vectors $\mathbf{v}^j_{q,g}$ and $\mathbf{v}^{j'}_{q,g'}$ constructed from the Kraus operators of Λ and explicitly defined in A. Equation (5.16) tells us which are the parameters characterizing Λ_c that enter into the optimization problem. The number of $W^{j,j'}_{q,g,g'}$ grows exponentially in n_1 and n_2: the multiplicity of the representation with total angular momentum j grows exponentially in general, therefore g and g' can take an exponential number of different values. It is worth observing that this quantity does not depend on m, s, m', s' which only appear in the Clebsch-Gordan coefficients. Also, the structure of the covariant channels specified in Eq. (5.16) indicates that the action of Λ_c on the off-diagonal elements in the total angular momentum basis is zero unless $|m - m'| = 1$ and $|j - j'| = 1$. In principle there is no selection rule on g and g', and at this level the number of variables of the problem still scales exponentially in n_1 and n_2. A dramatic simplification arises by using the symmetry properties of $\Omega_{n_1n_2}$. First of all $[\Omega_{n_1n_2}, J_z] = 0$, from which $\langle j,m,g|\,\Omega_{n_1n_2}\,|j',m',g'\rangle$ is zero unless $m = m'$. Moreover, by Schur-Weyl duality [FH04] the Hilbert space of the problem can be decomposed as $\mathcal{H} = \bigoplus_{D_1,D_2}(j_{D_1}\otimes\alpha_{D_1})\otimes(j_{D_2}\otimes\alpha_{D_2})$, where j_{D_i} and α_{D_i} are the irreducible representations of $SU(2)$ and the symmetric group S_{n_i} with Young diagram D. We notice that $\Omega_{n_1n_2}$ is symmetric under permutations acting independently on the first n_1 and the second n_2 qubits, hence by Schur's lemma $\Omega_{n_1n_2}$ must have the form $\Omega_{n_1n_2} = \bigoplus_{D_1,D_2}(\Omega_{D_1}\otimes \mathbf{1}_{D_1})\otimes(\Omega_{D_2}\otimes\mathbf{1}_{D_2})$, with $\Omega_{D_1},\Omega_{D_2}$ positive-semidefinite operators. In particular, since $(V\,|\uparrow\rangle\,\langle\uparrow|\,V^\dagger)^{\otimes n_2}$ is supported on the completely symmetric subspace for each V, $\Omega_{D_2} = 0$ unless D_2 is the completely symmetric Young diagram. From this observation it follows that $\Omega_{n_1n_2}$ is supported on a space spanned by orthonormal vectors labelled as $|j,m,g_{j_1}\rangle$, where we use the same conventions as before for the total angular momentum indices, and we simplify the notation using g_{j_1} as a shortcut for the couple (j_{D_1}, g_{D_1}) which indexes a basis of α_{D_1}. Putting all together we have proved that $\langle j,m,g_{j_1}|\Omega_{n_1n_2}|j',m',g'_{j'_1}\rangle = \Omega_{n_1n_2}(j,j',m,j_1,p)\delta_{m,m'}\delta_{g_{j_1},g'_{j'_1}}$, with the function $\Omega_{n_1n_2}(j,j',m,j_1,p)$ depending only on j,j',m,j_1,p and being explicitly computed in A. Exploiting these properties of $\Omega_{n_1n_2}$ the fidelity can then be expressed as

$$F_{n_1,n_2}(\Lambda) = \sum_{j,j',j_1,q} C^{j,j'}_{q,j_1}(p)W^{j,j'}_{q,j_1}\,, \tag{5.20}$$

where $C^{j,j'}_{q,j_1}(p)$ is a contraction of Clebsch-Gordan coefficients defined in A, and

$$W^{j,j'}_{q,j_1} := \Big(\sum_{g_{j_1}} W^{j,j'}_{q,g_{j_1},g_{j_1}}\Big)/\#g_{j_1}\;, \tag{5.21}$$

with

$$\#g_{j_1} = \frac{(n_1)!(2j_1+1)}{(\frac{n_1-2j_1}{2})(\frac{n_1+2j_1}{2}+1)}\;, \tag{5.22}$$

being the multiplicity of the representation j_1. Further constraints associated with the Completely Positivity condition of Λ_c are also automatically included in the parametrisation via $W^{j,j'}_{q,g,g'}$ through the connection between the vectors $\mathbf{v}^j_{q,g}$ and the Kraus operators of Λ. The trace preserving requirement reduces instead to $\sum_{s=\pm\frac{1}{2}}\langle\frac{1}{2},s|\Lambda_c\,[|j,m,g\rangle\langle j',m',g'|]\,|\frac{1}{2},s\rangle = \delta_{j,j'}\delta_{m,m'}\delta_{g,g'}$, which via some manipulations A can be cast in the equivalent form

$$\tfrac{2+2j}{(1+2j)}\;W^{j,j}_{q,j_1}\Big|_{q=j+\frac{1}{2}} + \tfrac{2j}{1+2j}\;W^{j,j}_{q,j_1}\Big|_{q=j-\frac{1}{2}} = 1\;. \tag{5.23}$$

We notice that the linearity of $F_{n_1,n_2}(\Lambda)$ and the convexity of the set of channels allows us to restrict the search for the maximum fidelity among those Λs for which $W^{j,j'}_{q,g_{j_1},g'_{j_1}} =$

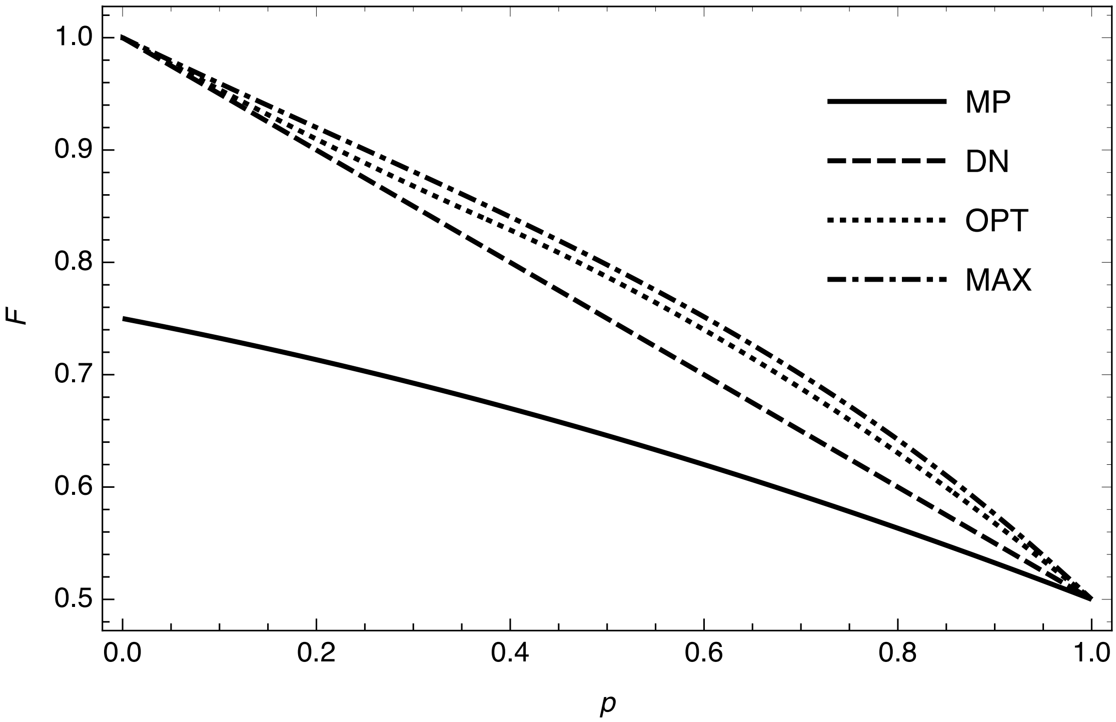

Figure 5.1: Average fidelity (5.24) for the optimal UQS machine for $n_1 = 2$ and $n_2 = 1$ as a function of the probability parameter p (dotted line), together with the average fidelities of the DN strategy (dashed line), the optimal expression for $n_1 = 2$ and $n_2 = \infty$ corresponding to have classical knowledge of the perturbing state (dotted-dashed line), and the upper bound $F^{\text{upper}}_{n_1=2}(\Lambda^{\text{MP}})$ attainable with MP procedures (continuous line).

$\delta_{g_{j_1},g'_{j_1}} W^{j,j'}_{q,j_1}$. Accordingly, the latter become the effective variables over which one has to perform the maximization of (5.20). As explicitly shown in A their number grows polynomially in n_1 and n_2, reducing the problem to a semidefinite program which let us perform numerical optimisation.

5.5.1 Results

As explicitly shown in A the maximization of Eq. (5.20) for case $n_1 = 2$ and $n_2 = 1$ can be performed analytically leading to

$$F^{(\max)}_{2,1} = \begin{cases} \frac{(1-p)(51+23p)}{54} + \frac{(1-p)(3+p)^2}{27(6-7p)} + \frac{p^2}{2}, & 0 \leq p \leq \frac{3}{8} \\ \frac{(1-p)(51+23p)}{54} + \frac{p(1-p)}{3} + \frac{p^2}{2}, & \frac{3}{8} \leq p \leq 1\,. \end{cases} \tag{5.24}$$

In Fig. 5.1 we report Eq. (5.24) together with the average fidelity for the DN strategy, with the function $F^{(\max)}_{2,\infty}$ which we computed in A following the same approach used for

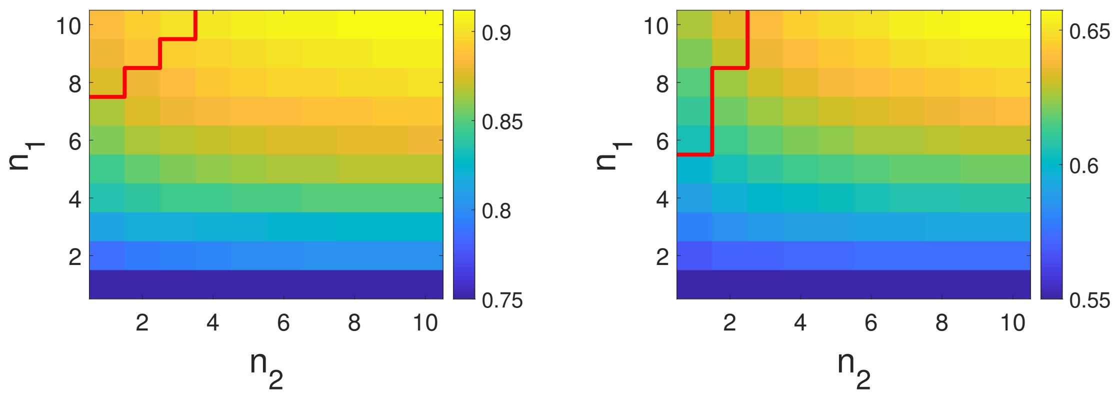

Figure 5.2: Numerical results for the maximum fidelity for $p = 0.5$ (left) and $p = 0.9$ (right) for $n_1 = 1, .., 10$ and $n_2 = 1, .., 10$. The red line indicates the following: as long as $(n_2, n_1 + 1)$ is below the red line, $F^{(\max)}_{n_1+1,n_2} > F^{(\max)}_{n_1,n_2+1}$, otherwise $F^{(\max)}_{n_1+1,n_2} < F^{(\max)}_{n_1,n_2+1}$. For example, in $p = 0.5$ (left), for $n_1 = 8$ and $n_2 = 2$, the fidelity is larger if we add one copy of the input B instead of the input A.

$F^{(\max)}_{1,\infty}$, and with the curve

$$F^{\text{upper}}_{n_1=2}(\Lambda^{\text{MP}}) := (9 - 2p - p^2)/12 \,, \tag{5.25}$$

which, as we detail in A, provides an upper bound to the average fidelity attainable when resorting on MP strategies when having $n_1 = 2$ copies of A and arbitrary copies of ρ_0. The curves show that for the low value n_1 we are considering here, the MP procedures are ineffective even with respect to the trivial DN strategy. $F^{(\max)}_{2,1}$ on the contrary is strictly larger than the DN score. Also it is very close to $F^{(\max)}_{2,\infty}$, showing that for $n_1 = 2$, the possibility of having just a single copy of the perturbing state ρ_0 provides us almost all the benefit one could obtain by having a classical knowledge of the latter. For larger values of n_1 and n_2 analytical treatment becomes cumbersome and we resort to numerical analysis using Mathematica [Wol18] to compute the parameters of the problem and CVX, a package for specifying and solving convex programs [MAT10; GB14] in Matlab, to calculate the maximum fidelity values. Results are reported in Fig. 5.2 for $n_1 = 1, 2, .., 10$ and $n_2 = 1, 2, .., 10$ and $p = \frac{1}{2}, \frac{9}{10}$.

5.6 Conclusions

The gap between $F^{(\max)}_{2,1}$ and the DN strategy (which is optimal in the $n_1 = 1$ scenario and independent from the explicit value of n_2) shows that even a small redundancies on the input A, can be beneficial. On the contrary, the very small distance between $F^{(\max)}_{2,1}$

and $F_{2,\infty}^{(\max)}$ clarifies that gathering more information on the mixing term ρ_0 (the noise of the model) does not help too much. As can be seen from Fig. 5.2 for larger n_1 and n_2 one can instead see a noise-dependent separation line between two regions, one where it is indeed advantageous to increase n_1 instead of n_2 and the other where the opposite holds.

The symmetry of the problem allowed us to reduce exponentially the number of variables involved in the optimisation. The same analysis should be relevant also in a broader perspective for general noise models.

Chapter 6

Degradable Flagged Extensions: Discrete Channels

6.1 Preface

The material in this chapter is based on the published article [KFG22]:

- Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Bounding the quantum capacity with flagged extensions". In: *Quantum* 6 (2022), p. 647. DOI: `10.22331/q-2022-02-09-647`

The ideas we used in [KFG22] are mostly from our previous article [FKG20]

- Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Quantum Flags and New Bounds on the Quantum Capacity of the Depolarizing Channel". In: *Physical Review Letters* 125.2 (2020), p. 020503. DOI: `10.1103/PhysRevLett.125.020503`. arXiv: `1911.01977`

In this chapter, we consider flagged extensions of convex combination of qudit quantum channels, and find general sufficient conditions for the degradability of the flagged extension. An immediate application is a bound on the quantum and private capacities of any qudit channel being a mixture of a unitary map and another channel, with the probability associated to the unitary component being larger than $\frac{1}{2}$. We then specialize our sufficient conditions to flagged Pauli channels, obtaining a family of upper bounds on quantum and private capacities of Pauli channels. In particular, we establish new state-of-the-art upper bounds on the quantum and private capacities of the depolarizing channel, BB84 channel and generalized amplitude damping channel. Moreover, the flagged construction can be naturally applied to tensor powers of channels with less restricting degradability conditions, suggesting that better upper bounds could be found by considering a larger number of channel uses.

6.2 Introduction

Protecting quantum states against noise is a fundamental requirement for harnessing the power of quantum computers and technologies. In a transmission line or in a memory, noise is modeled as a quantum channel, and several accesses to the channel together with careful state preparation and decoding can protect quantum information against noise. As discussed in Chapter 3.2 the quantum capacity Q of a channel is the maximal amount of qubits which can be transmitted reliably, per use of the channel. It can be expressed in terms of an entropic functional, the coherent information I_c, which can be computed as a maximization over quantum states used as inputs of the communication line. The quantum capacity [Llo97; Sho02b; Dev05] of a channel can then be obtained as a limit for large n of I_c per use of the channel, for n uses of the channel. A striking feature of the problem is the potential super-additivity of the coherent information [SS96; DSS98; SS07; FW08; SY08; SSY11; Cub+15; LLS18a; SG21; Sid20b; Sid20a; NPJ20; Yu+20; BL21], which which hinders the direct evaluation of the quantum capacity imposing an infinite number of optimizations on Hilbert spaces of dimension that grows exponentially in n. The existence of an algorithmically feasible evaluation of the quantum capacity remains as one of the most important open problems in quantum Shannon theory [Hol19; Wil17], while finding computable upper or lower bounds on the quantum capacity constitutes important progress.

As we have seen in Chapter 3.2, the phenomenon of superadditivity is not restricted to the quantum capacity, as it shows up also for the classical capacity [Has09], the classical private capacity [Li+09] and the trade-off capacity region [ZZS17; Zhu+19]. In this chapter, we are also interested in the classical private capacity, which is the optimal rate for classical communication protected by any eavesdropper [CWY04; Dev05]. In general this capacity is larger than the quantum capacity, but the upper bounds we obtain in this paper hold for both capacities.

In this chapter we present [KFG22] where we formulated sufficient conditions to obtain non-trivial upper bounds on the quantum capacity, using the so-called flagged extensions. A flagged extension of a channel that can be written as convex combinations of other channels is such that the receiver gets, together with the output of one of the channels in the convex combination, a flag carrying the information about which of the channels acted. This technique is particularly effective for a class of channels of physical significance, the Pauli channels. A qubit Pauli channel describes random bit flip and phase flip errors, which is a fundamental noise model; moreover, any qubit channel can be mapped to a Pauli channel by a twirling map [HHH98], which does not increase the quantum capacity [BKN00]. With these new flagged extensions we improve the results of [FKG20; WW19] for two important Pauli channels: the depolarizing channel and BB84 channel, which are both superadditive [SS96; DSS98; BL21], and their quantum capacities are not known, despite a long history of efforts [DSS98; AC97; Bru+98; Rai99; Cer00; Rai01; SS07; FW08; Smi08; SSW08; Ouy14; Sut+17; LDS18; LLS18b; BL21]. We also present state-of-the-art bounds for quantum capacity of the generalized amplitude damping channel [GP+09; BL20; RMG18; KSW20; WW19], improving the results of [WW19]. The bounds we obtained in [KFG22] are not necessarily the best bounds available with these techniques, being just good guesses among all the instances of flagged channels that satisfy the sufficient conditions. In fact, there is an infinite sequence of optimization problem depending on the number of uses of the channel, each of which gives a bound on the capacity. It is not clear if a phenomenon analogous to superadditivity appears in this scenario. Even with one use of the channel, different choices of Kraus operators give different bounds.

These bounds are based on the most fruitful technique to obtain upper bounds on the quantum capacity: finding a degradable extension of the channel (e.g. [Smi08; SSW08; Ouy14; LDS18].) In fact, degradable channels [DS05; CRS08] have the property that the coherent information is additive, therefore the quantum capacity is obtainable as the coherent information of the channel. Moreover, a fundamental property of capacities is that they are generically decreasing under composition of channels, a fact that has a clear operational justification. It is also known that the quantum capacity of a degradable channel is equal to its private capacity, therefore the quantum capacity of a flagged degradable extension of a channel is also an upper bound for the private capacity of the original channel. Moreover, when the channel is approximately degradable useful bounds can still be obtained [Sut+17; LLS18b].

In a previous paper [FKG20] we contributed to this line of work by considering a flagged degradable extension of the depolarizing channel. While previous constructions [WPG07; Smi08; SSW08; LDS18] used orthogonal flags, our contribution was to consider non-orthogonal flags, showing that degradable extensions can be obtained even in this less restricted setting, obtaining better bounds. In a subsequent work [WW19] the author combined non-orthogonal flags with approximate degradability, improving the bounds further by searching for the flagged extension with the best bound from approximate degradability. However, from careful inspection it seems that the advantage of the approximate degradability technique in this context is that it finds exactly degradable extensions for a choice of flags that our analysis did not cover. In fact, in [KFG22] we extend the sufficient conditions for degradability for flagged channels and we found even better bounds by exploiting richer flag structures, while being able to reproduce the bounds already obtained with approximate degradability techniques. In principle, the new bounds could be obtained by extending the space of the flags, evaluating the bounds with the approximate degradability method applied to the flagged extension, and minimizing over the possible flags. Unfortunately, this brute force search with more flags and in a larger Hilbert space for the flags becomes rapidly unpractical.

The outline of the paper is the following: first we show the derivation of the sufficient conditions for degradability of flagged channels in Section 6.3. We then apply this result to obtain a general bound on the quantum capacity of any channel which is the convex combination of a unitary channel and any other channel in Section 6.4. In Section 6.5, we briefly review qudit Pauli channels, then rewrite our sufficient conditions for Pauli channels, where the bounds on the quantum capacity appear to have a simpler form; we also show that two explicit choices of degradable extensions give state-of-the-art bounds for the quantum and private capacities of the depolarizing channel and the BB84 channel. In Section 6.6, we apply the our method to bound the quantum and private capacity of the generalized amplitude damping channel. In Section 6.7 we add some observations about the possibility of getting even better bounds with this method. We conclude with a summary of the results.

6.3 Sufficient conditions for degradability of flagged extensions

We outline a systematic construction of degradable flagged extensions for any convex combination of channels, i.e. channels of the form $\Lambda = \sum_{i=0}^{l} p_i \Lambda_i$, with $\{p_i\}_{i=0,\cdots l}$ a set of probabilities and with Λ_i channels themselves. We establish the following:

Proposition 6.3.1 (Sufficient conditions for degradability of flagged extensions). *Let Λ be a channel acting on the quantum system A and its flagged extension*

$$\mathbb{\Lambda} = \sum_{i=0}^{l} p_i \Lambda_i \otimes |\phi_i\rangle\langle\phi_i| \;, \tag{6.1}$$

with $|\phi_i\rangle$ normalized states of an auxiliary system F. The map $\mathbb{\Lambda}$ is degradable if there exists a choice of Kraus operators $\{K_j^{(i)}\}_{j=1,\dots,r_i}$ for each channel Λ_i and an orthonormal basis $\{|i\rangle\}_i$ for the space of F, such that

$$\langle i'|\phi_i\rangle \sqrt{p_i} K_{j'}^{(i')\dagger} K_j^{(i)} = \langle i|\phi_{i'}\rangle \sqrt{p_{i'}} K_j^{(i)\dagger} K_{j'}^{(i')} \qquad \forall i,j,i',j' \,. \tag{6.2}$$

Proof. Observe that starting from a Kraus set $\{K_j^{(i)}\}_{j=1,\dots,r_i}$ of the channel Λ_i, we can construct the following isometric Stinespring dilation for such channel,

$$V_i \left|\psi\right\rangle_A := \sum_{j=1}^{r_i} K_j^{(i)} \left|\psi\right\rangle_A \left|i\right\rangle_B \left|j\right\rangle_{\bar{B}} , \tag{6.3}$$

for all $\left|\psi\right\rangle_A$ states of A, with the systems B and $\bar{B}$ playing the role of the effective channel environment. A Stinespring representation of the flagged channel (6.1) can then be obtained as

$$V \left|\psi\right\rangle_A := \sum_{i=0}^{l} \sqrt{p_i} V_i \left|\psi\right\rangle_A \left|\phi_i\right\rangle_F \ , \tag{6.4}$$

which, via Eq. (**??**) allows to express the complementary of the flagged channel as

$$\tilde{\mathbb{A}}[\left|\psi\right\rangle_A \left\langle\psi\right|] = \sum_{i,j} \sqrt{p_i p_j}\, {}_F\langle\phi_j|\phi_i\rangle_F \,\mathrm{Tr}_A[V_i \left|\psi\right\rangle_A \left\langle\psi\right| V_j^\dagger] \ . \tag{6.5}$$

Our goal is to find a channel such as W that degrades the flagged channel to its complementary channel i.e. $W \circ \mathbb{A} = \tilde{\mathbb{A}}$. A natural candidate for the Stinespring representation of the degrading channel is as follows

$$V' \left|\psi\right\rangle_A \left|i\right\rangle_F := V_i \left|\psi\right\rangle_A \ . \tag{6.6}$$

Consider hence the following state

$$\begin{aligned} V'V \left|\psi\right\rangle_A &= \sum_{i=0}^{l} \sqrt{p_i} V' V_i \left|\psi\right\rangle_A \left|\phi_i\right\rangle_F = \sum_{i=0}^{l}\sum_{i'=0}^{l} \sqrt{p_i} \left\langle i' \middle| \phi_i \right\rangle V_{i'} V_i \left|\psi\right\rangle_A \\ &= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_i}\sum_{j'=1}^{r_{i'}} \left\langle i' \middle| \phi_i \right\rangle \sqrt{p_i} K_{j'}^{(i')} K_j^{(i)} \left|\psi\right\rangle_A \left|i\right\rangle_B \left|j\right\rangle_{\bar{B}} \left|i'\right\rangle_{B'} \left|j'\right\rangle_{\bar{B}'} \ , \end{aligned} \tag{6.7}$$

where for ease of notation $\langle i'|\phi_i\rangle$ stands for ${}_F\langle i'|\phi_i\rangle_F$. By construction the states of subsystem $B\bar{B}$ and $B'\bar{B}'$ are equal to $\tilde{\mathbb{A}}[\left|\psi\right\rangle\left\langle\psi\right|]$ and $W\circ\mathbb{A}[\left|\psi\right\rangle\left\langle\psi\right|]$ respectively. Therefore, a sufficient condition for the degradability of $\mathbb{A}$ is that $V'V\left|\psi\right\rangle_A$ is invariant if we swap subsystem $B\bar{B}$ with $B'\bar{B}'$. Writing the swap operator as $S_\leftrightarrow$, we have

$$\begin{aligned} S_\leftrightarrow V'V \left|\psi\right\rangle_A &= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_i}\sum_{j'=1}^{r_{i'}} \left\langle i' \middle| \phi_i \right\rangle \sqrt{p_i} K_{j'}^{(i')} K_j^{(i)} \left|\psi\right\rangle_A \left|i\right\rangle_B \left|j\right\rangle_{\bar{B}} \left|i'\right\rangle_{B'} \left|j'\right\rangle_{\bar{B}'} \\ &= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_i}\sum_{j'=1}^{r_{i'}} \left\langle i' \middle| \phi_i \right\rangle \sqrt{p_i} K_{j'}^{(i')} K_j^{(i)} \left|\psi\right\rangle_A \left|i'\right\rangle_B \left|j'\right\rangle_{\bar{B}} \left|i\right\rangle_{B'} \left|j\right\rangle_{\bar{B}'} \\ &= \sum_{i=0}^{l}\sum_{i'=0}^{l}\sum_{j=1}^{r_i}\sum_{j'=1}^{r_{i'}} \langle i|\phi_{i'}\rangle \sqrt{p_{i'}} K_j^{(i)} K_{j'}^{(i')} \left|\psi\right\rangle_A \left|i\right\rangle_B \left|j\right\rangle_{\bar{B}} \left|i'\right\rangle_{B'} \left|j'\right\rangle_{\bar{B}'} \ , \\ &= V'V \left|\psi\right\rangle_A , \end{aligned} \tag{6.8}$$

where we used Eq. (6.2) in the second equality. Since $S_{\leftrightarrow}V'V|\psi\rangle_A = V'V|\psi\rangle_A$, the flagged channel $\mathbb{A}$ is degradable.

□

In this way we reduced the degradability conditions to commutation conditions on the Kraus operators. In the case that all the Kraus operators commute, we choose all of the flags to be equal to $|\phi_i\rangle = |\phi\rangle = \sum_j \sqrt{p_j}|j\rangle$ to satisfy the degradability conditions, therefore the original channel itself is degradable. In this way we can recover the known fact that channels with commuting Kraus operators are degradable [DS05]. In the case that the Kraus operators of each Λ_i commute with each other i.e. $K_j^{(i)}K_{j'}^{(i)} = K_{j'}^{(i)}K_j^{(i)} \quad \forall j, j', i$, we can choose orthogonal flags $|\phi_i\rangle = |i\rangle$ to construct a degradable extension. However, our proof is not sufficient to recover the known fact that orthogonal flagged convex combination of degradable channels are degradable. Nonetheless, by allowing in our construction more freedom in the choice of V' we can recover this fact. In particular, one can use $V'|\psi\rangle_A|i\rangle_F = \sum_{j=1}^{r_i} D_j^{(i)}|\psi\rangle_A|i\rangle_{B'}|j\rangle_{\bar{B}'}$, where $D_j^{(i)}$ are the Kraus operators of the complementary of the degrading map of Λ_i. Therefore, allowing arbitrary $D_j^{(i)}$ and checking for equality of partial traces in the systems BB' and $\bar{B}\bar{B}'$ one obtains more general sufficient conditions, covering both the case of Proposition 3.1 and orthogonal flagged convex combination of degradable channels.

6.4 General applications

6.4.1 Convex combination of a unitary operation with an arbitrary channel

Consider a channel that is obtained as a convex combination of a unitary mapping induced by the unitary operator U plus an extra CPTP term Λ_1, i.e.

$$\Lambda[\rho] = (1-p)U\rho U^\dagger + p\Lambda_1[\rho] = (1-p)U\rho U^\dagger + p\sum_{j=1}^{r} K_j\rho K_j^\dagger\,, \tag{6.9}$$

where $p \in [0,1]$ and the K_i being a Kraus set of Λ_1. As the quantum and private capacities are invariant under unitary transformations, in what follow without loss of generality we shall set U as the identity map I, redefining the rest accordingly if necessary. Following the construction of the previous section we hence define the flagged extension (see Eq. (6.1)) of Λ as

$$\mathbb{A}[\rho] = (1-p)\rho\otimes|\phi_0\rangle\langle\phi_0| + p\Lambda_1[\rho]\otimes|\phi_1\rangle\langle\phi_1|\,, \tag{6.10}$$

for which the degradability conditions in Eq. (6.2) becomes

$$\langle 1|\phi_0\rangle\sqrt{1-p} = \langle 0|\phi_1\rangle\sqrt{p}\,, \qquad \langle 1|\phi_1\rangle K_jK_{j'} = \langle 1|\phi_1\rangle K_{j'}K_j\,. \tag{6.11}$$

Since K_j operators do not need to commute, we set $\langle 1|\phi_1\rangle = 0$ and if $p \leq 1/2$ we get the following solution

$$|\phi_1\rangle = |0\rangle\,, \qquad |\phi_0\rangle = \sqrt{\frac{1-2p}{1-p}}\,|0\rangle + \sqrt{\frac{p}{1-p}}\,|1\rangle\ . \tag{6.12}$$

Surprisingly, without any assumption on the form of Λ_1 we found a regime for which the channel in Eq. (6.10) is degradable with non-orthogonal flags. Therefore, we get the following upper bound

$$Q(\Lambda) \leq Q(\mathbb{A}) = Q_1(\mathbb{A})\,. \tag{6.13}$$

Note that, in the same regime $p \leq 1/2$, one also has that the extension with orthogonal flags is degradable. Consider indeed a map acting as follows on product states (it can be trivially extended): $W[\rho \otimes |\phi_0\rangle\langle\phi_0|] = \frac{1-2p}{1-p}|0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0| + \frac{p}{1-p}\tilde{\Lambda}_1[\rho] \otimes |\phi_1\rangle\langle\phi_1|$, $W[\rho \otimes |\phi_1\rangle\langle\phi_1|] = |0\rangle\langle 0| \otimes |\phi_0\rangle\langle\phi_0|$. One can verify that this map is a valid degrading map. However, the extension with non-orthogonal flags has a lower quantum capacity and therefore gives a better upper bound. Note also that one can also consider the family of extensions

$$\mathbb{A}_c[\rho] := (1-c^2)(1-p)\rho \otimes |\phi_0\rangle\langle\phi_0| + \big(c^2(1-p)\rho + p\Lambda_1[\rho]\big) \otimes |\phi_1\rangle\langle\phi_1|\ , \tag{6.14}$$

which according to Eq. (6.12) are degradable for $|\langle\phi_0|\phi_1\rangle|^2 = \frac{1-2(p+c^2-pc^2)}{1-(p+c^2-pc^2)}$, for $0 \leq c^2 \leq \frac{1-2p}{2(1-p)}$. Each of these extensions gives an upper bound, and the best bound is found by minimization.

$$Q(\Lambda) \leq \min_{0\leq c^2 \leq \frac{1-2p}{2(1-p)}} Q_1(\mathbb{A}_c)\,. \tag{6.15}$$

Putting $\Lambda_1[\rho] = I/d$, one recovers degradable flagged extension of depolarizing channel. The best previous upper bound for qubit depolarizing channel is given in [WW19]. In [WW19], by fixing the structure of the flagged extension as in Eq. (6.10), the author found the optimal upper bound for the quantum capacity of the qubit depolarizing channel using approximate degradability, and minimizing over flagged extensions. In fact, the best bound with this method is obtained for an exactly degradable extension, and the flags giving the optimal upper bound in [WW19] are the same that we find analytically in Eq. (6.11). On the other hand, considering the family of extensions Eq. (6.14) we can also recover mixed state flags associated to the identity channel, by writing

$$\mathbb{A}_c[\rho] = (1-p)\rho \otimes \big((1-c^2)|\phi_0\rangle\langle\phi_0| + c^2|\phi_1\rangle\langle\phi_1|\big) + p\Lambda_1[\rho] \otimes |\phi_1\rangle\langle\phi_1|\ . \tag{6.16}$$

For $c^2 = \frac{1-2p}{2(1-p)}$, $\langle\phi_0|\phi_1\rangle = 0$ and we recover the best bound from [FKG20], obtained with the same flag structure. The minimization over c gives in general some improvement on this class of upper bounds.

Another non-trivial construction is the following: if $K_j = \sqrt{p_j} U_j$ for some unitaries U_j, with $\sum_{i=1}^r p_j = 1 - p$, then we can consider the mixed unitary flagged channel,

$$\Lambda[\rho] = (1-p)\rho \otimes |\phi_0\rangle\langle\phi_0| + \sum_{j=1}^r p_j U_j \rho U_j^\dagger \otimes |\phi_j\rangle\langle\phi_j| \ , \tag{6.17}$$

and any flag choice such that

$$\langle i|\phi_j\rangle = 0 \ \text{ if } i \neq 0 \, \text{and} \, j \neq 0 \, \text{and} \, i \neq j \ , \tag{6.18}$$

gives a degradable extension. The best upper bounds we obtain from degradable extensions with more than two flags, for the depolarizing channel and BB84 channel, have exactly this flag structure. However, the degradability conditions are more general than this and we give a more specialized treatment to these channels in the following sections. Finally, as an extension of the argument presented in Eq. (6.16), we remark that even general extensions with mixed flags can be considered in this framework, by changing the convex combination considered. For example, a rank two flag can be introduced by splitting a term $K\rho K^\dagger \otimes (q\,|0\rangle\langle 0| + (1-q)\,|1\rangle\langle 1|) = \sqrt{q}K\rho\sqrt{q}K^\dagger \otimes |0\rangle\langle 0| + \sqrt{1-q}K\rho\sqrt{1-q}K^\dagger \otimes |1\rangle\langle 1|$, where we now flag a channel with new Kraus operators $\sqrt{q}K$ and $\sqrt{1-q}K$, each with a pure flag associated.

6.5 Flagged Pauli channels

In this section, we concentrate on an important subclass of mixed unitary channels, the Pauli channels, which describe random bit flip and phase flip errors in qubits and their generalization to qudits models. For this class of channels the structure of degradable flagged extensions is quite rich and the upper bounds can be made more explicit. We use the notation introduce in Section 2.5 for Pauli channels.

Pauli channels are defined as convex combination of Pauli unitaries with a given discrete probability distribution $\{w_x\}$:

$$\Phi_{\mathbf{w}}[\rho] = \sum_{x \in \mathbb{Z}_d^{2n}} w_x W_x \rho W_x^\dagger \, . \tag{6.19}$$

For these channels, our sufficient conditions for degradability are less stringent than in general, because of the relations (2.20) occurring for any couple of Pauli unitaries. To construct the flagged version of these channels, we note that the flags live, without loss of generality, in a Hilbert space $\mathcal{H}_F$ of dimension d^{2n}, with computational basis $\{|x\rangle\}_{x \in \mathbb{Z}_d^{2n}}$. We also consider the space $\mathcal{H}_C \otimes \mathcal{H}_F$, with $\mathcal{H}_C$ isomorphic to $\mathcal{H}_F$, and denote the partial trace with respect to $\mathcal{H}_C$ as $\mathrm{Tr}_C[\cdot]$.

Consider a flagged Pauli channel $\Phi_{\mathbf{\Psi}}$

$$\Phi_\Psi[\rho] = \sum_{x\in\mathbb{Z}_d^{2n}} w_x W_x \rho W_x^\dagger \otimes |\phi_x\rangle\langle\phi_x| \,, \tag{6.20}$$

where the label Ψ determines Φ_Ψ through the definition of the state $|\Psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_F$ as

$$|\Psi\rangle = \sum_{x\in\mathbb{Z}_d^{2n}} \sqrt{w_x}\,|x\rangle_C \otimes |\phi_x\rangle_F = \sum_{x\in\mathbb{Z}_d^{2n}, y\in\mathbb{Z}_d^{2n}} \sqrt{w_x}\,\langle y|\phi_x\rangle\,|x\rangle_C \otimes |y\rangle_F \,. \tag{6.21}$$

We define the projectors Π_j on $\mathcal{H}_C \otimes \mathcal{H}_F$ projecting on $\mathrm{span}\{|x\rangle\,|y\rangle - e^{j\frac{2\pi i}{d}}\,|y\rangle\,|x\rangle \,:\, \langle x,y\rangle = j \bmod d\}$. For a probability vector $\mathbf{w}$ over $\mathbb{Z}_d^{2n}$, we denote its Shannon entropy as $S(\mathbf{w}) := -\sum_{x\in\mathbb{Z}_d^{2n}} w_x \log w_x$. With these definitions, we are equipped to establish the following proposition:

Proposition 6.5.1 (Upper bound on the quantum capacity of Pauli channels). *Given a Pauli channel $\Phi_{\mathbf{w}}$, for any $|\Psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_F$ satisfying*

$$\mathrm{Tr}[\Pi_j\,|\Psi\rangle\langle\Psi|] = 0 \;\; \forall j \in \{0,...,d-1\} \qquad \mathrm{Tr}[(|x\rangle\langle x| \otimes I)\,|\Psi\rangle\langle\Psi|] = w_x \qquad \forall x \in \mathbb{Z}_d^{2n}. \tag{6.22}$$

the quantum and private capacities of $\Phi_{\mathbf{w}}$ satisfy

$$Q(\Phi_{\mathbf{w}}) \leq P(\Phi_{\mathbf{w}}) \leq n\log d - S(\mathbf{w}) + S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|]). \tag{6.23}$$

In particular, the optimal upper bound is obtained by minimizing $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|])$ with the constraints (6.22).

Proof. Given a channel of the form (6.20), consider a state on $\mathcal{H}_C \otimes \mathcal{H}_F$ of the form

Any state $|\Psi\rangle$ on $\mathcal{H}_C \otimes \mathcal{H}_F$ satisfying the second condition in Eq. (6.22) can be written as

$$|\Psi\rangle = \sum_{x\in\mathbb{Z}_d^{2n}} \sqrt{w_x}\,|x\rangle_C \otimes |\phi_x\rangle_F = \sum_{x\in\mathbb{Z}_d^{2n}, y\in\mathbb{Z}_d^{2n}} \sqrt{w_x}\,\langle y|\phi_x\rangle\,|x\rangle_C \otimes |y\rangle_F \,, \tag{6.24}$$

identifying a flagged extension Φ_Ψ of $\Phi_{\mathbf{w}}$. Moreover, the degradability conditions for Φ_Ψ can be rewritten as

$$\mathrm{Tr}[\Pi_j\,|\Psi\rangle\langle\Psi|] = 0 \;\; \forall j \in \{0,...,d-1\}, \tag{6.25}$$

therefore Φ_Ψ is degradable. For flagged degradable Pauli channels, $Q_1 = Q$ has a very simple form. By the covariance property of (flagged) Pauli channels, i.e. $\Phi_\Psi[W_x \rho W_x^\dagger] =$

$(W_x \otimes I)\Phi_\Psi[\rho](W_x^\dagger \otimes I)$ for all $W_x \in \mathcal{W}_d^n$. Moreover, we can also write the coherent information as $I_c(\Phi_{\mathbf{\Psi}}, \rho) = S(\Phi_\Psi[\rho]) - S(\Phi_\Psi \otimes \mathcal{I}[|\rho\rangle\rangle\langle\langle\rho|])$, for any purification $|\rho\rangle\rangle$ of ρ and $\mathcal{I}$ identity channel, therefore using unitarily invariance of the von Neumann entropy and covariance we have $I_c(\Phi_{\mathbf{\Psi}}, \rho) = I_c(\Phi_{\mathbf{\Psi}}, W_x \rho W_x^\dagger)$. By concavity of coherent information for degradable channels [YHD08], we thus get

$$I_c(\Phi_{\mathbf{\Psi}}, \rho) = \frac{1}{d^{2n}} \sum_{x \in \mathbb{Z}_d^{2n}} I_c(\Phi_{\mathbf{\Psi}}, W_x \rho W_x^\dagger) \leq I_c(\Phi_{\mathbf{\Psi}}, \frac{1}{d^{2n}} \sum_{x \in \mathbb{Z}_d^{2n}} W_x \rho W_x^\dagger) = I_c(\Phi_{\mathbf{\Psi}}, \frac{I}{d^n}). \tag{6.26}$$

Therefore, the maximum of coherent information corresponds to the maximally mixed state, which is purified by the maximally entangled state $|\Xi\rangle = \frac{1}{d^{n/2}} \sum_{j=0,\ldots,d-1} |j\rangle \otimes |j\rangle$. It holds that $\langle \Xi| W_x^\dagger W_y \otimes I |\Xi\rangle = \frac{1}{d^n} \operatorname{Tr}\left[W_x^\dagger W_y\right] = \delta_{x,y}$, therefore

$$\begin{aligned} Q_1(\Phi_{\mathbf{\Psi}}) = S\left(\Phi_{\mathbf{\Psi}}\left[\frac{I}{d^n}\right]\right) - S(\Phi_{\mathbf{\Psi}} \otimes I[|\Xi\rangle\langle\Xi|]) = n \log d + S(\sum_{x \in \mathbb{Z}_d^{2n}} w_x |\phi_x\rangle\langle\phi_x|) - S(\mathbf{w}) \\ = n \log d - S(\mathbf{w}) + S(\operatorname{Tr}_C[|\Psi\rangle\langle\Psi|]), \end{aligned} \tag{6.27}$$

hence leading to Eq. (6.23). □

Note that the minimization problem suggested by Proposition (6.5.1) is non-convex, therefore it is hard to treat numerically. Its solution is also not unique in general. However, some useful upper bounds on the quantum capacity can be obtained, case by case, by simply minimizing over families of states which satisfy the constraints, but can be expressed in terms of a few parameters. In this way, we obtain state-of-the art results for the depolarizing channel and the BB84 channel. As a side comment, the treatment in this section does not seem to cover the flag choice of [FKG20; WW19] for the depolarizing channel. However, this is easily amended by splitting the Kraus operator proportional to the identity in Eq. (6.19) into two Kraus operators with suitable probabilities, and assigning a different flag to each of them, respecting the sufficient conditions for degradability (see the comments after Eq. (6.13)).

6.5.1 Flagged depolarizing channel

The depolarizing channel on one qudit is

$$\Lambda_p^d[\rho] := (1 - \frac{d^2-1}{d^2} p)\rho + \frac{p}{d^2} \sum_{x \in \mathbb{Z}_d^2 \setminus \{0\}} W_x \rho W_x^\dagger \,. \tag{6.28}$$

The symmetries of this channel causes some potential redundancies in the states that achieve the optimal upper bound according to Proposition (6.5.1). Consider the unitary operation U_σ indexed by permutations $\sigma \in S_{d^2-1}$ which act by permuting the orthogonal set $\{|x\rangle\}_{x\in\mathbb{Z}_d^2\setminus\{0\}}$ while leaving $|0\rangle$ invariant. Then, for any state $|\Psi\rangle$ satisfying the constraints, $U_\sigma \otimes U_\sigma |\Psi\rangle$ also satisfies the constraints, and it has the same entanglement entropy $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|]) = S(\mathrm{Tr}_C[U_\sigma \otimes U_\sigma |\Psi\rangle\langle\Psi| (U_\sigma \otimes U_\sigma)^\dagger])$. We cannot establish if the minimization problem has a unique solution, but if this was the case, then we could restrict the candidate states to those which are invariant under $U_\sigma \otimes U_\sigma$ for every $\sigma \in S_{d^2-1}$. We just take this observation as a suggestion for a guess, and we minimize $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|])$ on this restricted family of states. This is convenient because $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|])$ can be determined analytically and we can reduce the problem to a one-parameter minimization.

Proposition 6.5.2. *Any $|\Psi\rangle$ satisfying the constraint Eq. (6.24) for the map of Eq. (6.28) and the condition $|\Psi\rangle = U_\sigma \otimes U_\sigma |\Psi\rangle$ can be parametrized with three complex variables $\alpha = \langle 0,0|\Psi\rangle$, $\beta = \langle 0,x|\Psi\rangle$ for $x \neq 0$, $\gamma = \langle x,x|\Psi\rangle$ for $x \neq 0$. Accordingly we can write*

$$S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|]) = -(d^2-2)|\gamma|^2 \log\big(|\gamma|^2\big) - v_+ \log v_+ - v_- \log v_-, \tag{6.29}$$

with

$$v_\pm = \frac{1}{2}(|\alpha|^2 + |\gamma|^2 + 2|\beta|^2(d^2-1) \pm \sqrt{(|\alpha|^2 - |\gamma|^2)^2 + 4(d^2-1)|\beta|^2|\alpha+\gamma^*|^2}). \tag{6.30}$$

Proof. From the constraints we have that $\beta = \langle 0,x|\Psi\rangle = \langle x,0|\Psi\rangle$, and from the action of a permutation U_{xy} that exchanges $x, y \neq 0$ we have $\langle 0,x| U_{xy} \otimes U_{xy} |\Psi\rangle = \langle 0,y|\Psi\rangle$. From the constraints we have that $\langle x,y|\Psi\rangle = e^{-\frac{2\pi i}{d}\langle x,y\rangle} \langle y,x|\Psi\rangle$ for $x \neq y$, $x,y \neq 0$, then $\langle x,y| U_{xy} \otimes U_{xy} |\Psi\rangle = \langle y,x|\Psi\rangle = e^{-\frac{2\pi i}{d}\langle x,y\rangle} \langle y,x|\Psi\rangle = 0$. Also, $\langle x,x|\Psi\rangle = \langle x,x| U_{xy} |\Psi\rangle = \langle y,y|\Psi\rangle = \gamma$ when $x,y \neq 0$. This completes the parametrization. The eigenvalues of $\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|]$ can be determined from the singular values of the matrix M_{xy} of coefficients of $|\Psi\rangle = \sum_{x\in\mathbb{Z}_d^{2n}, y\in\mathbb{Z}_d^{2n},} M_{xy} |x\rangle_C \otimes |y\rangle_F$. We have that the coefficients of $M^\dagger M$ are

$$M^\dagger M_{0,0} = |\alpha|^2 + |\beta|^2(d^2-1) \qquad M^\dagger M_{0,x} = \alpha\beta^* + \beta\gamma^*,\ x \neq 0 \tag{6.31}$$

$$M^\dagger M_{x,y} = |\beta|^2,\ x \neq y,\ x,y \neq 0 \qquad M^\dagger M_{x,x} = |\beta|^2 + |\gamma|^2,\ x \neq 0\ . \tag{6.32}$$

Then $M^\dagger M - |\gamma|^2 I$ has rank 2 and the nonzero eigenvalues can be determined by solving a quadratic equation.

□

Proposition 6.5.3. *For $|\Psi\rangle$ satisfying $|\Psi\rangle = U_\sigma \otimes U_\sigma |\Psi\rangle$, the minimization of $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|])$ is a one-parameter minimization problem.*

Proof. From the expression of $S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|])$ in Eq. (6.29) and from Eq. (6.30) it's evident that the result does not depend on the phases of α, β and γ except for the term $|\alpha+\gamma^*|$, which should be maximized. This happens without loss of generality if α and γ^* are real and positive. Then the two constraints $|\alpha|^2+(d^2-1)|\beta|^2=(1-\frac{d^2-1}{d^2}p)$ and $|\beta|^2+|\gamma|^2=\frac{p}{d^2}$ eliminate the remaining two parameters, with the constraint that γ is such that $|\alpha|,|\beta|,|\gamma|<1$. □

Summarizing, from Proposition 6.5.1 and 6.5.2 we obtain

$$\begin{aligned} Q(\Lambda_p^d) &\le P(\Lambda_p^d) \le \log d - S(\mathbf{w}) + S(\mathrm{Tr}_C[|\Psi\rangle\langle\Psi|]) \\ &= \log d - \left(1-\frac{d^2-1}{d^2}p\right)\log\left(1-\frac{d^2-1}{d^2}p\right) - \frac{p(d^2-1)}{d^2}\log\frac{p}{d^2} \\ &\quad - (d^2-2)|\gamma|^2\log\big(|\gamma|^2\big) - v_+(|\gamma|^2)\log v_+(|\gamma|^2) - v_-(|\gamma|^2)\log v_-(|\gamma|^2), \end{aligned} \tag{6.33}$$

where the allowed values of γ and the dependence on γ of $v_+(|\gamma|^2)$ and $v_-(|\gamma|^2)$ are obtained as in the argument of Proposition 6.5.3, i.e.

$$\begin{aligned} v_\pm(x) = \frac{1}{2}\big(1-(d^2-2)x\big) \pm \frac{1}{2}\Bigg\{ &\left(1-2\frac{d^2-1}{d^2}p+(d^2-2)x\right)^2 \\ &+ 4(d^2-1)\left(\frac{p}{d^2}-x\right)\left(xd^2+2\sqrt{x}\sqrt{x\,(d^2-1)-2\frac{p(d^2-1)}{d^2}+1}-2\frac{p(d^2-1)}{d^2}+1\right)\Bigg\}^{1/2}. \end{aligned} \tag{6.34}$$

The bound Q_{fmin} obtained from this one-parameter minimization [KFG22] can be combined with the no-cloning bound [Bru+98; Cer00; Smi08; Ouy14]

$$Q(\Lambda_p^d) \le \big(1-\tfrac{2p(d+1)}{d}\big)\log d\,. \tag{6.35}$$

using the fact that the convex hull of upper bounds from degradable extensions of the depolarizing channel is itself an upper bound [Smi08; Ouy14]. A comparison between the most competitive upper bounds for $d=2$ is shown in Figure 6.1, where we can see that the bound we obtained outperforms all previous bounds in the whole parameter region. An improvement with respect to previous bounds can be obtained also for generic d, and we show as an example the bound for $d=4$ in Figure 6.2. In this latter case, the bound from the convex hull is improved considering also the bound from Eq. (6.15).

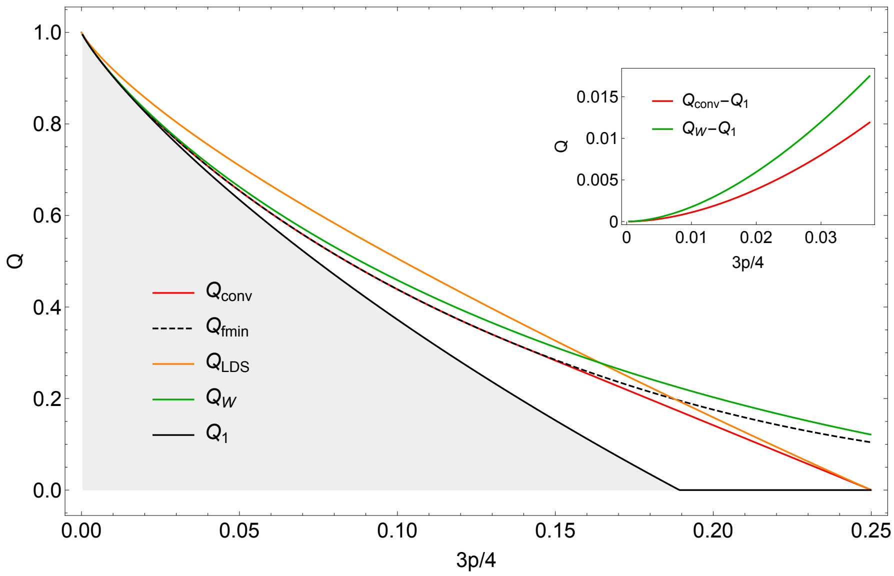

Figure 6.1: Bounds on the quantum capacity of the depolarizing channel for $d = 2$. Here Q_{conv} is the convex hull of the available upper bounds from degradable extensions, Q_{fmin} is the upper bound in [KFG22], obtained from Eq. (6.23) by plugging in the expression Eq. (6.29) and minimizing over γ, eliminating the other parameters as explained in the proof of Proposition 6.5.3. Q_1 is the lower bound given by the coherent information of one use of the channel. Q_{LDS} is the bound from [LDS18] and Q_W is the bound from [WW19].

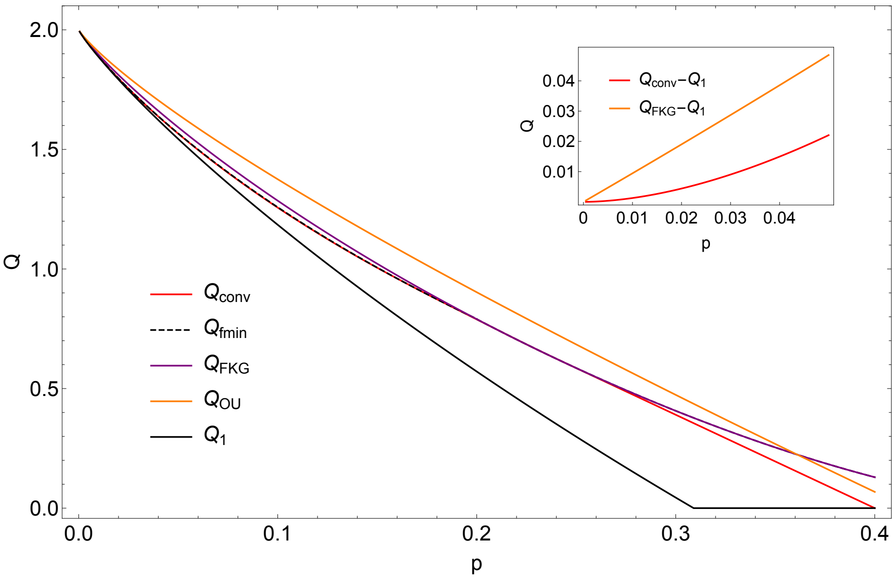

Figure 6.2: Bounds on the quantum capacity of the depolarizing channel for $d = 4$. Here $Q_{\rm conv}$ is the convex hull of the available upper bounds from degradable extensions, $Q_{\rm fmin}$ is the bound in [KFG22], and Q_1 is the lower bound given by the coherent information of one use of the channel. Q_{FKG} is the bound from [FKG20] and $Q_{\rm OU}$ is the bound from [Ouy14]. Note that in the main plot $Q_{\rm fmin}$ is the bound in Eq. (6.15), since at scale used the bound with more flags is not noticeably better; the situation is different for very small p, in the regime plotted in the inset: here we report $Q_{\rm conv}$ obtained from Eq. (6.23) by plugging in the expression Eq. (6.29) and minimizing over γ, eliminating the other parameters as explained in the proof of Proposition 6.5.3 (see Eq. (6.33) and Eq. (6.34)).

6.5.2 Flagged BB84 channel

In this section we consider the channel that describes the famous quantum key distribution protocol by Bennett and Brassard [BB14b]. In its general form the channel is

$$B_{p_X,p_Z}[\rho] = (1 - p_X - p_Z + p_X p_Z)\rho + (p_X - p_X p_Z)X\rho X + (p_Z - p_Z p_X)Z\rho Z + p_X p_Z Y\rho Y, \tag{6.36}$$

As in [Sut+17] and [WW19] we restrict to the case $p_X = p_Z = p$. The flagged extension we consider is

$$\begin{aligned} B_{p,\Psi}[\rho] = {} & (1-p)^2 \rho \otimes |\phi_0\rangle\langle\phi_0| + p(1-p)X\rho X \otimes |\phi_1\rangle\langle\phi_1| + p(1-p)Z\rho Z \otimes |\phi_2\rangle\langle\phi_2| \\ & + p^2 Y\rho Y \otimes |\phi_3\rangle\langle\phi_3| \ . \end{aligned} \tag{6.37}$$

We choose the following parametrization for the flags

$$\begin{aligned} |\phi_0\rangle &= \sqrt{1-2\alpha^2-\beta^2}\,|0\rangle + \alpha\,|1\rangle + \alpha\,|2\rangle + \beta\,|3\rangle \\ |\phi_1\rangle &= a\,|0\rangle + \sqrt{1-a^2-\gamma^2}\,|1\rangle - \gamma\,|3\rangle \\ |\phi_2\rangle &= a\,|0\rangle + \sqrt{1-a^2-\gamma^2}\,|2\rangle - \gamma\,|3\rangle \\ |\phi_3\rangle &= b\,|0\rangle + c\,|1\rangle + c\,|2\rangle + \sqrt{1-b^2-2c^2}\,|3\rangle \ , \end{aligned} \tag{6.38}$$

where we impose the parameters $\alpha, \beta, \gamma, a, b, c$ to be real and satisfying the normalization conditions for the vectors in Eq. (6.38). The degradability conditions in Eq. (6.2) imply that $\alpha = a\sqrt{\frac{p(1-p)}{(1-p)^2}}$, $\beta = \frac{bp}{1-p}$ and $\gamma = c\sqrt{\frac{p}{1-p}}$. This is not the most general parametrization for the flags, however, because of the symmetry between the bit flip and phase flip error in Eq. (6.36), we chose this parametrization. Any set of flags in the form of Eq. (6.38) will result in a degradable extension of BB84 channel. Therefore, to get the best upper bound for the quantum capacity or private capacity of BB84 we should minimize the coherent information of its flagged channel with respect to three free parameters a, b, c. We have compared the result of the optimization with the previous bounds in Figure 6.3. The bound in [WW19] by Wang can be reproduced in our framework just by choosing $a = b = 1$, $c = 0$.

6.6 Flagged generalized amplitude damping

In this section we consider a bound on the quantum capacity of the generalized amplitude damping channel, which is a model of thermal loss on a qubit, relevant for quantum

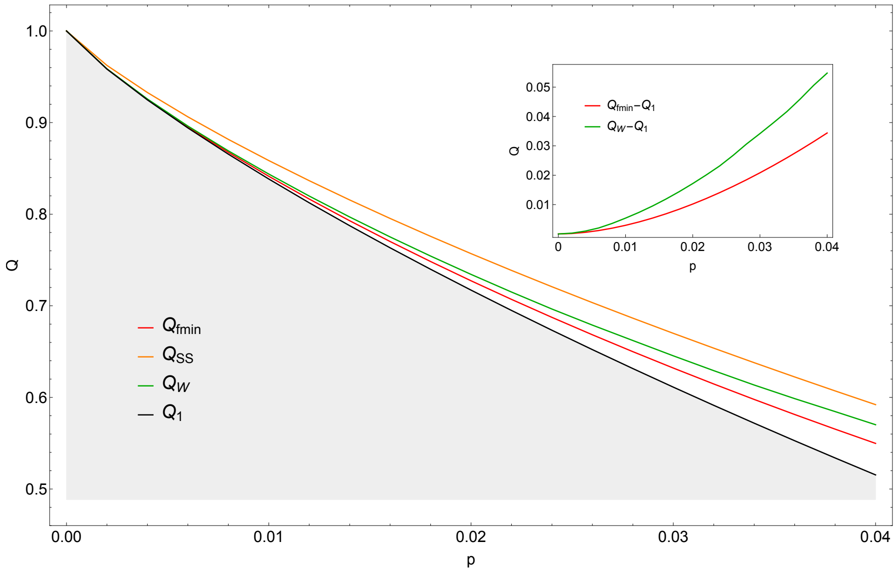

Figure 6.3: Bounds on the quantum and private capacity of BB84 channel. Q_1 is the coherent information of BB84 channel. Q_{fmin} is the upper bound obtained in [KFG22], from Eq. (6.23), using the parametrization for the flags in Eq. (6.38), for a suitable choice of the parameters. Q_W is the upper bound obtained in [WW19]. Q_{SS} is the upper bound derived in [Smi08].

superconducting processors [CB08]. The generalized amplitude damping channel can be written as

$$\mathcal{A}_{y,N}[\rho] = N\,\mathcal{A}_y[\rho] + (1-N)\,X\circ\mathcal{A}_y\circ X[\rho], \tag{6.39}$$

where $\mathcal{A}_{y,N}$ is the conventional amplitude damping channel, with Kraus operators $K_1 = (|0\rangle\langle 0| + \sqrt{1-y}\,|1\rangle\langle 1|)$ and $K_2 = \sqrt{y}\,|1\rangle\langle 0|$. While $\mathcal{A}_y$, and $X\circ\mathcal{A}_y\circ X$ are degradable and their quantum capacity can be computed [GF05], their convex combination is not, and its quantum capacity is not determined. Previous upper bounds have been obtained by [RMG18; KSW20; GP+09; WW19]. In particular [WW19] used the following flagged extension together with approximate degradability to get the tightest bound available:

$$\mathcal{A}^F_{y,N}[\rho] = N\,\mathcal{A}_y[\rho]\otimes|0\rangle\langle 0| + (1-N)\,X\circ\mathcal{A}_y\circ X[\rho]\otimes|1\rangle\langle 1|\,, \tag{6.40}$$

In fact this extension is exactly degradable: the output of a complementary channel is

$$\tilde{\mathcal{A}}^F_{y,N}[\rho] = N\,\tilde{\mathcal{A}}_y[\rho]\otimes|0\rangle\langle 0| + (1-N)\,X\circ\tilde{\mathcal{A}}_y\circ X[\rho]\otimes|1\rangle\langle 1|\,, \tag{6.41}$$

and if the degrading map of A_y is W_y, we have $\tilde{\mathcal{A}}^F_{y,N}[\rho] = (W_y\otimes|0\rangle\langle 0| + X\circ W_y\circ X\otimes|1\rangle\langle 1|)\circ\mathcal{A}^F_{y,N}[\rho]$. The quantum capacity of this extension can be evaluated to be $Q(\mathcal{A}^F_{y,N}) \le (1-N)I_c(A_y,\rho)+NI_c(X\circ A_y\circ X,\rho) = Q(A_y)$. This simple bound introduced in [KFG22], and the actual quantum capacity $Q(\mathcal{A}^F_{y,N})$ is very close to it. Moreover, the structure of the generalized amplitude damping is such that one can get better bounds from different degradable extensions, where we adapt the argument by [Smi08] on the depolarizing channel:

Proposition 6.6.1 (Combining bounds of degradable extensions of generalized amplitude damping). *For any collection of degradable extensions $\mathcal{A}^{ext,i}_{y,N}$, $i = 1,...,l$, for any y_0 the quantum capacity of $\mathcal{A}_{y_0,N}$ is upper bounded by the convex hull of $Q(\mathcal{A}^{ext,i}_{y_0,N})$, $i = 1,...,l$, as functions of the variable N.*

Proof. For any N_1, N_2 such that $N = qN_1 + (1-q)N_2$, $1-N = 1-qN_1+(1-q)N_2 = q(1-N_1)+(1-q)(1-N_2)$, we have

$$\mathcal{A}_{y,N}[\rho] = q(N_1\,\mathcal{A}_y[\rho]+(1-N_1)\,X\circ\mathcal{A}_y\circ X[\rho])+(1-q)(N_2\,\mathcal{A}_y[\rho]+(1-N_2)\,X\circ\mathcal{A}_y\circ X[\rho]) \tag{6.42}$$

If $\mathcal{A}^{ext,i}_{y,N_1}$ and $\mathcal{A}^{ext,j}_{y,N_2}$ are degradable extensions of $\mathcal{A}_{y,N_1}$ and $\mathcal{A}_{y,N_2}$ respectively, then $q\mathcal{A}^{ext,i}_{y,N_1}\otimes|0\rangle\langle 0| + (1-q)\mathcal{A}^{ext,j}_{y,N_2}\otimes|1\rangle\langle 1|$ is a degradable extension of $\mathcal{A}_{y,N}$ with quantum capacity less than $qQ(\mathcal{A}^{ext,i}_{y,N_1}) + (1-q)Q(\mathcal{A}^{ext,j}_{y,N_2})$.

□

In addition to the extension proposed by [WW19], we find two other degradable extensions using the results of this paper. The first is obtained observing that the following set is also a good choice of Kraus operators

$$A_1 = \sqrt{N(1-N)}(\sqrt{1-y}+1)(|0\rangle\langle 0| + |1\rangle\langle 1|) = \sqrt{N(1-N)}(\sqrt{1-y}+1)I \quad (6.43)$$

$$A_2 = \sqrt{(1-N)y}\,|1\rangle\langle 0| \quad (6.44)$$

$$A_3 = ((1-N) - N\sqrt{1-y})\,|0\rangle\langle 0| + ((1-N)\sqrt{1-y} - N)\,|1\rangle\langle 1| \quad (6.45)$$

$$A_4 = \sqrt{Ny}\,|0\rangle\langle 1| \quad (6.46)$$

We notice that A_1 is a rescaled unitary operator, therefore we can directly apply the bound of Eq. (6.13) with $(1-p) = N(1-N)(\sqrt{1-y}+1)^2$. This bound is applicable if $N(1-N)(\sqrt{1-y}+1)^2 > 1/2$. Moreover, at $N = 1/2$, the generalized amplitude damping becomes a Pauli channel:

$$\mathcal{A}_{y,0.5}(\rho) = \frac{1 - y/2 + \sqrt{1-y}}{2}\rho + \frac{1 - y/2 - \sqrt{1-y}}{2}Z\rho Z + \frac{y}{4}(Y\rho Y + X\rho X) \quad (6.47)$$

and we get a more refined bound $Q_{\text{fmin}}(y)$ [KFG22], using the techniques of the previous sections, in particular with the same flag structure of BB84 Eq. (6.38). Putting all together, we observe that the bound by [WW19] remains the best one at high y, but at low y it is beaten by the following bound allowed by the convex hull argument:

$$Q_{\text{conv}}(y, N) = 2NQ_{\text{fmin}}(y) + (1-2N)Q(\mathcal{A}_y) \quad (6.48)$$

and using the full convex hull bound does not give substantial improvements. We plot the results in Figure 6.4.

6.7 Discussion

In the examples we provided we did not try to numerically optimize in the whole parameter region allowed by the sufficient conditions for degradability. Indeed, the minimization of the upper bound is not a convex optimization problem and would require brute force search, but there are already many parameters for Pauli channels and $d = 2$, $n = 1$. However, we stress the fact that the family of upper bounds for the quantum and private capacity of a channel Λ is even larger in principle, as one can consider the flagged extension of $\Lambda^{\otimes k}$: a degradable flagged extension of Λ gives also a degradable flagged extension of $\Lambda^{\otimes k}$ but the converse is not true. We tried to search for a better upper bound of the quantum capacity of the depolarizing channel with two uses, by restricting brute force search to certain parametrizations of the flags, but the attempts we made did

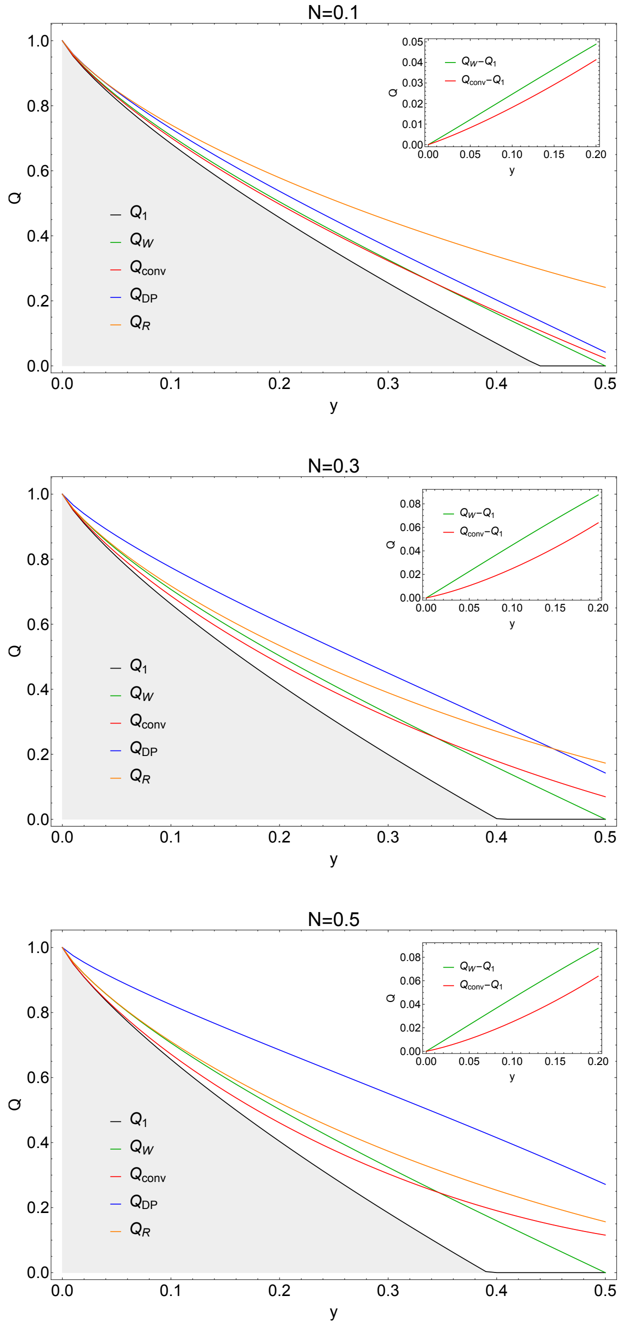

Figure 6.4: Bounds on the quantum capacity of the generalized amplitude damping, for three values of N. Q_1 is the lower bound given by the coherent information of one use of the generalized amplitude damping (see also lower bounds from [BL20], which give improvements mildly visible at this scale). Q_{conv} is the upper bound from Eq. (6.48) introduced in [KFG22], Q_W is the upper bound obtained by Wang [WW19], Q_{DP} and Q_R are obtained in [KSW20] respectively from data-processing and Rains information. Previous upper bounds [RMG18; GP+09] are worse and not plotted.

not show anything better than the $k = 1$ bound. It is desirable to further investigate if $k = 1$ gives already the best upper bound or a phenomenon similar to superadditivity shows up for flagged extensions. Moreover, the extensions we obtained are explicitly dependent on the Kraus representation chosen, which is not unique. We did not find a way to identify an optimal choice of Kraus operators. Since for any channel the number of Kraus operators can be increased arbitrarily by a suitable isometry, it is conceivable that one needs to look at an unbounded space of flags to optimize the upper bound of degradable extensions. As a side note, we point out that the mixed flags extensions as considered in [FKG20] can be treated in the formalism of this paper, just by splitting the Kraus operators into Kraus operators with proper probabilities.

6.8 Conclusions

We have introduced a method to construct degradable extension of quantum channels which can be written as the convex sum of other channels. This method is of general applicability, and we showed that it gives state-of-the-art upper bounds on the quantum and private capacity of two important Pauli channels, the depolarizing channel and the BB84 channel, and of the generalized amplitude damping channel. By virtue of its simplicity, we believe it can be used with success for many other channels too. The method could in principle give better bounds by considering different Kraus representations and flagged extensions of several uses of a channel, and it would be interesting to study its limitations.

Chapter 7

Degradable Extensions: Gaussian Channels

7.1 Preface

The material presented in this chapter is mostly based on

- Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Estimating Quantum and Private Capacities of Gaussian Channels via Degradable Extensions". In: *Phys. Rev. Lett.* 127 (21 2021), p. 210501. DOI: 10.1103/PhysRevLett.127.210501

Here, we present upper bounds on the quantum and private capacity of single-mode, phase-insentitive Bosonic Gaussian Channels based on degradable extensions. Our findings are state-of-the-art in the following parameter regions: low temperature and high transmissivity for the thermal attenuator, low temperature for additive Gaussian noise, high temperature and intermediate amplification for the thermal amplifier.

7.2 Introduction

After discussing degradable extension of discrete channels in the previous section, we bring our attention to Gaussian quantum channels. We consider realistic single-mode noise models for communication across free space or optical fiber: thermal attenuators, thermal amplifiers and additive Gaussian noise [CD94; HG12; Wee+12; Ser17]. As we have seen in Chapter 4.4, these channels are known as phase-insensitive, single-mode Bosonic Gaussian Channels, and can be understood as unitary interactions with a single-mode thermal environment mediated by Hamiltonians which are quadratic in the operators fields of the model. The quantum and private capacities of these type of channels have been extensively studied [Pir+17; WTB17; Sha+18; RMG18; NAJ19; Lim+19b; NPJ20], but they are still unknown. Interesting variations are Gaussian interaction with general environment [Lim+19a; Lam+20], and environmental assisted communication [OMW22].

In [FKG21], we found new state-of-the-art upper bounds on the quantum and private capacity of thermal attenuators, amplifiers and additive Gaussian noise, using degradable extensions. As discussed in Chapter 3.3 an established strategy to find upper bounds for quantum and private capacity is to exploit (approximately) degradable channels which reduce to the channel of interest after pre and/or post-processing. These are so called degradable extensions for which the quantum capcity is additive, and can be calculated.

In particular, to upper bound the quantum capacity of the additive Gaussian noise, we introduced a flagged extension of the additive Gaussian noise which is degradable [FKG21]. As we have seen in the previous chapter, in discrete variable quantum information, degradable flagged extensions offer the best known upper bounds to several important channels [WFD19; KFG22]. In [FKG21], we extended this approach to continuous variable systems. In particular, we were inspired by the sufficient conditions of degradability of finite-dimensional flagged channels introduced in [KFG22]. The upper bound is state-of-the-art in the low temperature regime. Using this upper bound and data-processing, we also bounded the quantum capacity of thermal amplifier, obtaining a state-of-the-art bound in the high temperature regime, for intermediate amplification values. We also improved the construction in [RMG18] based on weak degradability to find a noisier degradable extension of the thermal attenuator, and show that it gives the best upper bound in the low noise regime, for low temperature and high transmissivity.

In the following, we first present the flagged extension of the additive Gaussian noise and the extension of the thermal attenuator. In both cases, we compute their quantum and private capacities, and compare the new available bounds.

7.3 Upper bounds for the Additive Gaussian Noise

Additive Gaussian noise Λ_β (see Eq. 4.40) is known to have zero capacity in the high temperature regime (i.e. for $1/\beta \geq 0.5$) [Hol19]. In particular in [NAJ19], the following upper bound is computed using data-processing:

$$Q(\Lambda_\beta) \leq Q_{\mathrm{NAJ}}(\beta) = \max\{\log_2(\beta - 1), 0\}, \tag{7.1}$$

and correctly gives $Q(\Lambda_\beta) = 0$ for $1/\beta \geq 0.5$. In the low temperature instead we only have a lower bound for $Q(\Lambda_\beta)$ given by the coherent information for one use of the channel, evaluated on an infinite temperature state, i.e.

$$Q(\Lambda_\beta) \geq Q_L(\Lambda_\beta) := \max\{\log_2 \beta - 1/\ln 2, 0\} \ , \tag{7.2}$$

and the inequality,

$$Q(\Lambda_\beta) \leq Q_{\mathrm{PLOB}}(\beta) = \log_2 \beta - 1/\ln 2 + 1/(\beta \ln 2) \ , \tag{7.3}$$

which follows from an upper bound for the generic two-way quantum capacity [Pir+17].

Generalizing the procedure introduced in [KFG22] we present an improved upper bound considering the following flagged extension of Λ_β, i.e.

$$\Lambda^e_\beta[\hat{\rho}] := \frac{\beta}{2\pi} \int_{\mathbb{R}^2} \mathrm{d}\mathbf{r} e^{-\frac{\beta}{2}\mathbf{r}^\intercal \mathbf{r}} \hat{D}_\mathbf{r} \hat{\rho} \hat{D}^\dagger_\mathbf{r} \otimes |\phi_\mathbf{r}\rangle\langle\phi_\mathbf{r}| \ , \tag{7.4}$$

where setting $\mathbf{r} := (x, p)$, $|\phi_\mathbf{r}\rangle$ are product of displaced squeezed states defined by

$$|\phi_\mathbf{r}\rangle := \hat{D}_{(0,-p/2)} |\beta/2\rangle \otimes \hat{D}_{(0,x/2)} |\beta/2\rangle \ , \tag{7.5}$$

with $|\beta/2\rangle$ being a single-mode squeezed vacuum with mean values $\bar{\mathbf{r}} = 0$ and covariance matrix $\boldsymbol{\sigma} = \begin{pmatrix} 2/\beta & 0 \\ 0 & \beta/2 \end{pmatrix}$. As explicitly shown in Appendix C Λ^e_β is degradable: here we notice that the intuition for choosing the flags states as in (7.5) comes from a result by the same authors on finite dimensional channels [KFG22]. Indeed there we proved that if $\{\sqrt{p_i}\hat{U}_i\}_{i=1,\dots,n}$ are unitary Kraus operators of a CPTP map $\mathcal{N}$ and $\{|i\rangle\}_{i=1,\dots,n}$ is an orthonormal basis for flags, sufficient conditions for the degradability of $\mathcal{N}^e[\hat{\rho}] := \sum_{i=1}^n p_i \hat{U}_i \hat{\rho} \hat{U}_i^\dagger \otimes |\phi_i\rangle \langle\phi_i|$ are the following

$$\langle i'|\phi_i\rangle \sqrt{p_i} \hat{U}_{i'} \hat{U}_i = \langle i|\phi_{i'}\rangle \sqrt{p_{i'}} \hat{U}_i \hat{U}_{i'} \quad \forall i, i' \ . \tag{7.6}$$

If we can use a continuous set of flags, replacing the orthonormal basis for the flag space withc the (two-mode) pseudo-eigenbasis $\{|\mathrm{x}_1, \mathrm{x}_2\rangle\}_{\mathrm{x}_1,\mathrm{x}_2 \in \mathbb{R}}$ of the position operators of the ancillary modes, applying this result to Λ^e_β we get

$$\langle \gamma x', \gamma p'|\phi_\mathbf{r}\rangle \, e^{-\frac{\beta}{4}\mathbf{r}^\intercal \mathbf{r}} \hat{D}_{\mathbf{r}'} \hat{D}_\mathbf{r} = \langle \gamma x, \gamma p|\phi_{\mathbf{r}'}\rangle \, e^{-\frac{\beta}{4}\mathbf{r}'^\intercal \mathbf{r}'} \hat{D}_\mathbf{r} \hat{D}_{\mathbf{r}'} \ , \tag{7.7}$$

for all $\mathbf{r}' = (x', p'), \mathbf{r} = (x, p) \in \mathbb{R}^2$ with γ a suitable rescaling factor to determine. With the choice (7.5) of the flags we have explictly

$$\langle \gamma x', \gamma p'|\phi_\mathbf{r}\rangle = \sqrt{\frac{\beta}{2\pi}} e^{-\beta \frac{\gamma^2 x'^2 + \gamma^2 p'^2}{4} - \gamma \frac{i p' x - i x' p}{2}} , \tag{7.8}$$

which satisfies the condition (7.7) with $\gamma = 1$. Exploiting the degradability of Λ^e_β and the fact that it is gauge-covariant (in a generalized sense that we specify in C), the capacity of this map, using Theorem 4.4.2, can be easily computed leading to the following inequality

$$Q(\Lambda_\beta) \leq Q(\Lambda_\beta^e) = \log_2 \beta - 1/\ln 2 + 2h\left(\sqrt{1 + 1/\beta^2}\right) , \tag{7.9}$$

with $h(x) := \frac{x+1}{2} \log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2} \log_2\left(\frac{x-1}{2}\right)$ (see Appendix C for details). As shown in Fig. 7.1, upper bound. (7.9) is better than (7.3) where $Q(\Lambda_\beta)$ is supposed to be non-zero, i.e. for $1/\beta \leq 0.5$.

7.4 Upper bounds for the thermal amplifier

Invoking data-processing inequality [Wil17], we can use Eq. (7.9) to upper bound the quantum capacity thermal amplifier $\Phi_{g,N}$ (a similar argument could also be invoked for the thermal attenuator $\mathcal{E}_{\eta,N}$ but the result we get is worst than the bounds reported in the next section). As a matter of fact any thermal amplifier can be written as a composition of a zero temperature amplifier and an additive Gaussian noise i.e. $\Phi_{g,N} = \Lambda_{\frac{1}{\kappa}} \circ \Phi_{g,0}$ with $\kappa = (g-1)N$. Therefore we get

$$Q(\Phi_{g,N}) \leq Q(\Lambda_{\frac{1}{\kappa}}) \leq Q_{\rm FKG}^{\rm amp}(g, N) := Q_{\rm FKG}^{\rm amp}(\kappa) := Q(\Lambda_{\frac{1}{\kappa}}^e) , \tag{7.10}$$

$$Q(\Phi_{g,N}) \leq Q(\Lambda_{\frac{1}{\kappa}}) \leq Q_{\rm NAJ}^{\rm amp}(g, N) := Q_{\rm NAJ}(\kappa) , \tag{7.11}$$

The bound of Eq. (7.11) comes directly to the data-processing decompositions, but to our knowledge it was not explicitly pointed out before our work [FKG21], being implicit in Proposition 12.65 of [Hol19]. It is the best bound at high g for any N, and it gives zero quantum capacity for the lowest g. The bound in Eq. (7.10), in the high temperature regime $N > 5$ and for intermediate values of g is provably better than the previous best bound reported in [Pir+17]:

$$Q(\Phi_{g,N}) \leq Q_{\rm PLOB}^{\rm amp}(g, N) := \log_2(\tfrac{g^{N+1}}{g-1}) - h(2N+1) . \tag{7.12}$$

A comparison between these function is reported in Fig. 7.2, together with the lower bound given by the coherent information for one use of the channel, evaluated on an infinite energy thermal state,

$$Q(\Phi_{g,N}) \geq Q_{\rm low}^{\rm amp}(g, N) := \max\{\log_2(\tfrac{g}{g-1}) - h(2N+1), 0\} . \tag{7.13}$$

7.5 Upper bounds for the thermal attenuator

To deal with the quantum capacity of the channel $\mathcal{E}_{\eta,N}$ introduced in chapter 4, we construct a degradable extension of such map. We first define the passive unitary operator

$$\hat{W}_\eta := \hat{U}_{\eta AE} \otimes \hat{U}_{\eta A'E'} , \tag{7.14}$$

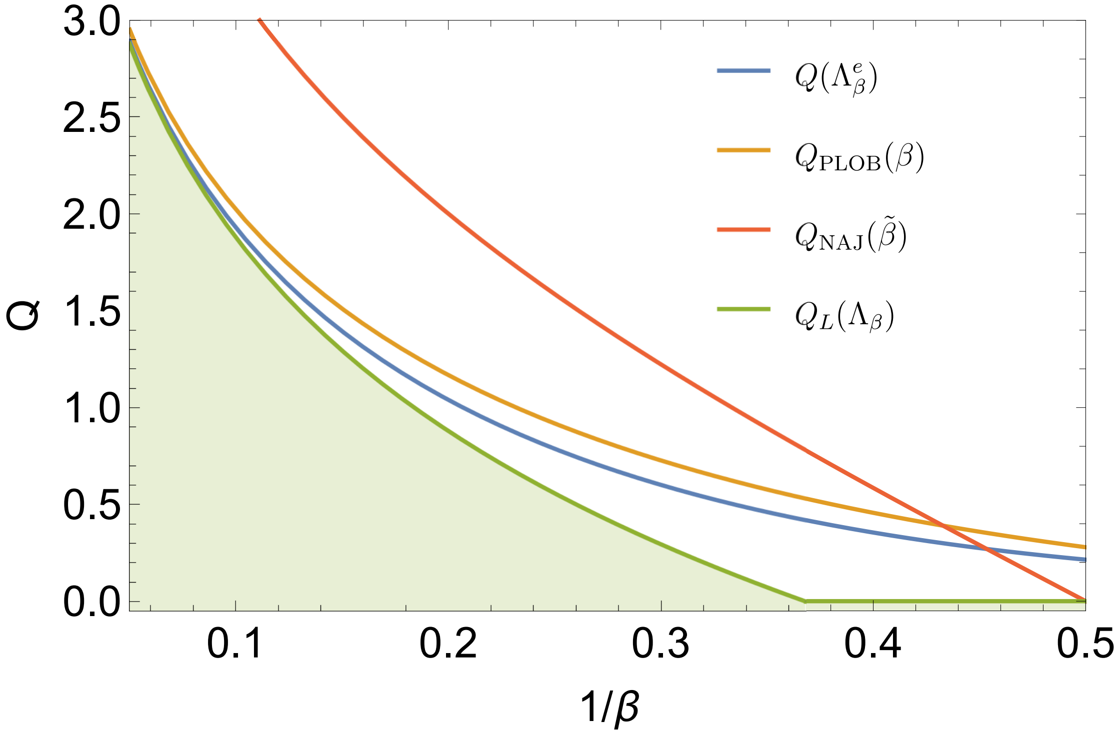

Figure 7.1: Quantum capacity region for the Additive Gaussian noise Λ_β: comparison of the upper bound $Q(\Lambda_\beta^e)$ of Eq. (7.9) in [FKG21] with Q_{PLOB} in Eq. (7.3) [Pir+17] and $Q_{\text{NAJ}}(\beta)$ in Eq. (7.1) [NAJ19]. $Q_L(\Lambda_\beta)$ is the lower bound of Eq. (7.2).

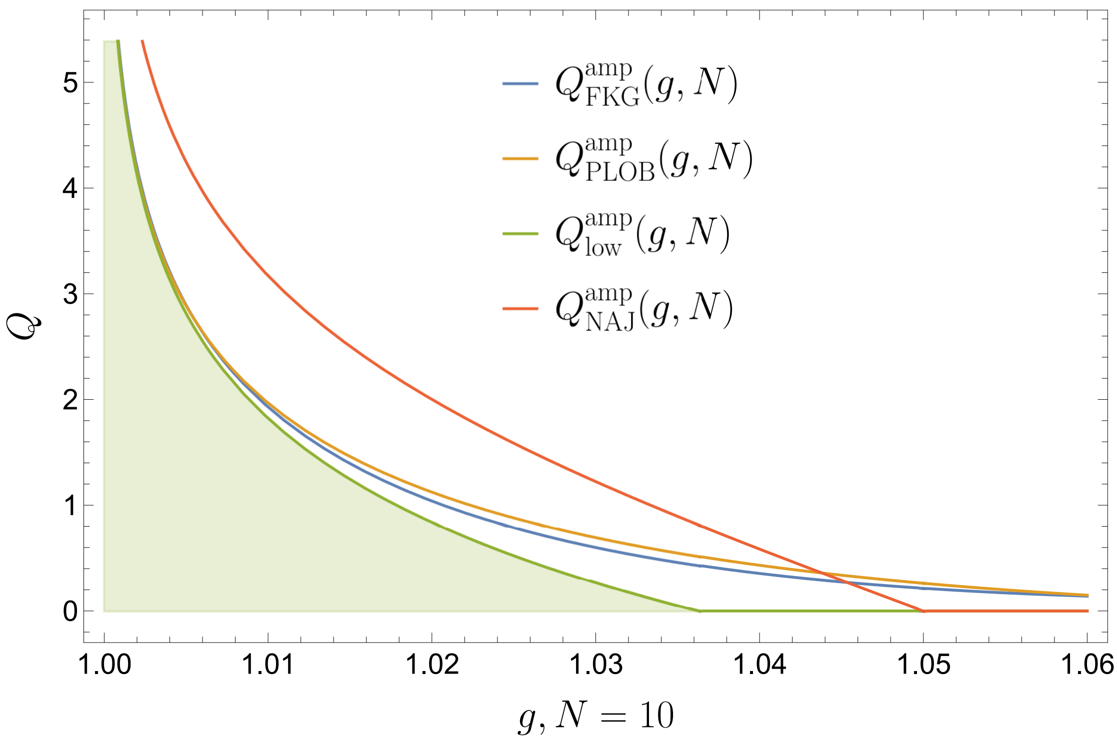

Figure 7.2: Quantum capacity region for the thermal amplifier channel $\Phi_{g,N}$: comparison between the upper bound $Q^{\text{amp}}_{\text{FKG}}(g,N)$ of Eq. (7.10) in [FKG21] with $Q^{\text{amp}}_{\text{PLOB}}(g,N)$ of Eq. (7.12) [Pir+17] and $Q^{\text{amp}}_{\text{NAJ}}(g,N)$ in Eq. (7.1) [NAJ19] for $N = 10$. $Q^{\text{amp}}_{\text{low}}(g,N)$ is the lower bound of Eq (7.13)

where $\hat{U}_{\eta AE}$ and $\hat{U}_{\eta A'E'}$ are beam splitters transformations acting respectively on the pair of modes A, E and A', E'. We introduce hence the channel

$$\mathcal{F}_{\eta,N}[\rho_{AA'}] := \mathrm{Tr}_{EE'}[\hat{W}_\eta(\rho_{AA'} \otimes |\tau\rangle\langle\tau|_{EE'})\hat{W}_\eta^\dagger], \tag{7.15}$$

and define the extension of $\mathcal{E}_{\eta,N}$ as

$$\mathcal{E}^e_{\eta,N}[\rho_A] := \mathcal{F}_{\eta,N}(\rho_A \otimes |0\rangle\langle 0|_{A'}). \tag{7.16}$$

The map $\mathcal{F}_{\eta,N}$ is manifestly Gaussian, and its action on the first and second moments is

$$\bar{\mathbf{r}} \xrightarrow{\mathcal{F}_{\eta,N}} \bar{\mathbf{r}}' = \sqrt{\eta}\bar{\mathbf{r}} \ , \tag{7.17}$$

$$\boldsymbol{\sigma} \xrightarrow{\mathcal{F}_{\eta,N}} \boldsymbol{\sigma}' = \eta\boldsymbol{\sigma} + (1-\eta)\boldsymbol{\sigma}_{|\tau\rangle} \ , \tag{7.18}$$

With the Stinespring representation in Eq. (7.15) the complementary channel can now computed as $\tilde{\mathcal{F}}_{\eta,N} = \mathcal{F}_{1-\eta,N}$. Simple algebra shows that if $\eta > 1/2$ then

$$\tilde{\mathcal{F}}_{\eta,N} = \mathcal{F}_{1-\eta,N} = \mathcal{F}_{(1-\eta)/\eta,N} \circ \mathcal{F}_{\eta,N} \ , \tag{7.19}$$

implying that in such regime $\mathcal{F}_{\eta,N}$ (and thus $\mathcal{E}^e_{\eta,N}$) is degradable. The quantum capacity of $\mathcal{E}^e_{\eta,N}$ can be thus calculated by evaluating the coherent information of the channel leading to (see Appendix C)

$$\begin{aligned} &Q(\mathcal{E}_{\eta,N}) \leq Q^{\mathrm{att}}_{\mathrm{FKG}}(\eta, N) := Q(\mathcal{E}^e_{\eta,N}) = \\ &\log_2(\tfrac{\eta}{1-\eta}) + h((1-\eta)(2N+1)+\eta) - h(\eta(2N+1)+1-\eta) \, . \end{aligned} \tag{7.20}$$

Once more this upper bound should be compared with previous upper bounds. At low noise, that is at low N and high η, the best upper bound available is once more an upper bound for the generic two-way quantum capacity [Pir+17]:

$$Q(\mathcal{E}_{\eta,N}) \leq Q^{\mathrm{att}}_{\mathrm{PLOB}}(\eta, N) = -\log_2((1-\eta)\eta^N) - h(2N+1) \ . \tag{7.21}$$

Other bounds come from data processing [RMG18; Sha+18; NAJ19], the best in the low noise regime being:

$$Q(\mathcal{E}_{\eta,N}) \leq Q(\mathcal{E}_{\eta-N(1-\eta),0}) = \log_2 \tfrac{\eta-N(1-\eta)}{(N+1)(1-\eta)} \ , \tag{7.22}$$

which implies that for

$$N \geq \frac{2\eta-1}{2(1-\eta)} \tag{7.23}$$

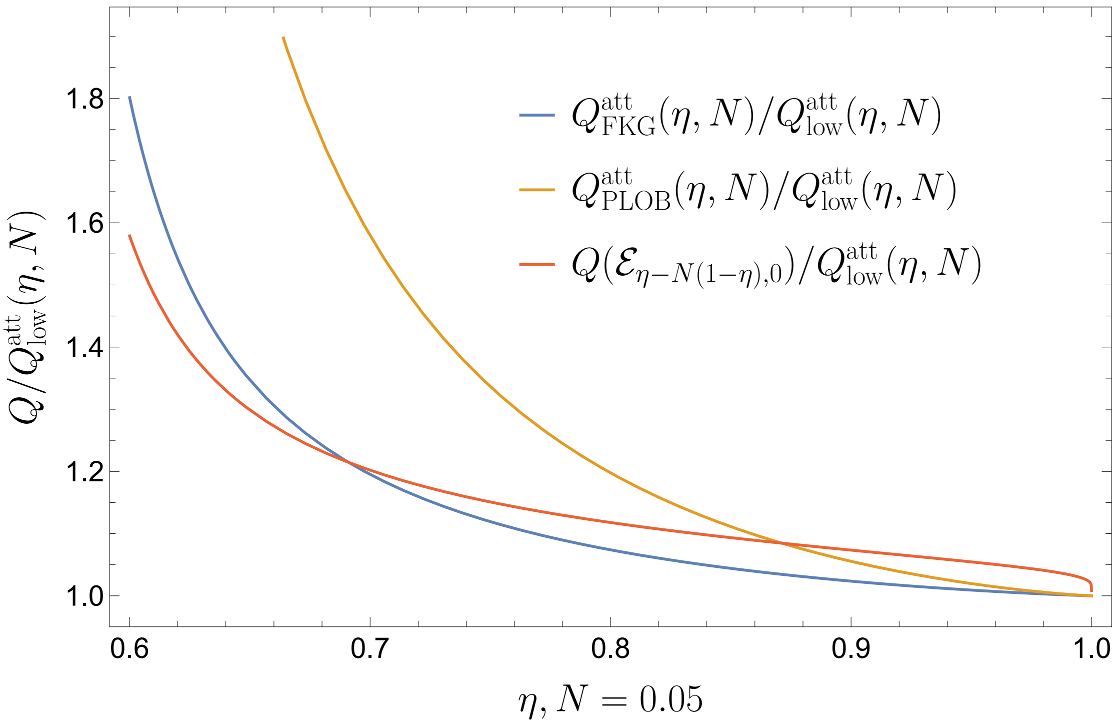

Figure 7.3: Thermal attenuator: ratio between the upper bounds $Q(\mathcal{E}_{\eta-N(1-\eta),0})$ [RMG18], $Q^{\text{att}}_{\text{PLOB}}(\eta, N)$ [Pir+17], $Q^{\text{att}}_{\text{FKG}}(\eta, N)$ [FKG21], and $Q_L(\mathcal{E}_{\eta,N})$ for $N = 0.05$.

the quantum capacity is zero.
A lower bound on $Q(\mathcal{E}_{\eta,N})$ is given by the coherent information for one use of the channel, evaluated on an infinite temperature state,

$$Q(\mathcal{E}_{\eta,N}) \geq Q_{\text{low}}^{\text{att}}(\eta, N) := \max\{\log_2(\tfrac{\eta}{1-\eta}) - h(2N+1), 0\}. \tag{7.24}$$

A comparison between all these curves is reported in Fig. 7.3, showing that while our inequality (7.20) performs worse than (7.22) for low η, it gives an improvement with respect to (7.21) for high η. We finally remark that in our construction the choice of $|0\rangle\langle 0|_{A'}$ in the definition Eq. (7.16) of the extended attenuator is not necessarily optimal. Other Gaussian states could be chosen and the analysis could be done in the same way. In particular, the extension $\mathcal{F}_{\eta,N} \otimes \mathcal{I}[\rho_A \otimes |\tau'\rangle\langle\tau'|_{A'B}]$, with $|\tau'\rangle$ being a two mode squeezed state with some average energy, gives a slightly better upper bound (optimizing over the single parameter in $|\tau'\rangle$ states), not noticeable on the plot in Fig. 7.3.

7.6 Conclusion and Remarks

The bounds we found in [FKG21] complement the bounds in [Pir+17; Sha+18; RMG18; NAJ19]. They have been determined using degradable extensions and data-processing. Our contribution in [FKG21] extends the applicability of this technique, which now gives the best upper bounds at low noise for a large collection of channels of physical interest. In particular, the flagged extension of the Additive Gaussian noise nicely generalizes the construction of flagged extensions to infinite dimensional channels, improving the upper bound on the quantum capacity by a considerable margin.

We mention also that the presented results could be easily applied also for the case of energy constrained quantum capacity.

Chapter 8

Improving Bounds for Thermal Attenuator Using Decomposition Rules.

8.1 Abstract

We present new upper bounds on the quantum capacity of thermal attenuator using data processing inequalities. We write thermal attenuator as a composition of thermal attenuator and thermal amplifier (decomposition rules), and improve the previously known upper bounds using data processing inequalities. In addition, we show that any upper bound on the capacity of thermal attenuator should have a specific symmetry, otherwise one can construct a better upper bound using the decomposition rules.

8.2 Introduction

An established strategy to upper bound the quantum and private capacity is using data processing inequalities. One can obtain upper bounds for the quantum capacity of a channel by decomposing it to another channels for which the capacities are already known (or already upper bounded) [SS08; Sut+17; Ouy14; LLS18c; LDS18; RMG18; Sha+18; FKG20; KFG22; WFD19; FKG21; NAJ19]. In this article, we use this method to improve the previous bounds in [RMG18; Pir+17; NAJ19; FKG21] for the quantum and private capacity of thermal attenuator, and we have two main results.
First, we introduce a set of decomposition rules for thermal attenuator, and by using our previous uppers bound in [FKG21] and data processing inequality, we get an upper bound for each decomposition rule. By optimizing over this set of upper bounds, we find

the optimal bound. This is mainly presented in Theorems 8.4.1 and 8.4.2
Second, by studying the decomposition rules from a more general prospective, we find a structure for the phase space of the parameters of thermal attenuator. More precisely, for a given thermal attenuator, we find regions in the phase space of the parameters of thermal attenuator where the quantum capacity is higher or lower than the quantum capacity of the given channel. This structure (higher and lower capacity regions) can be used to improve any given lower or upper bound. This is mainly presented in Theorem 8.5.1.

First, in Sec. 8.3 we review the decomposition rules for thermal attenuator. Then, in Sec. **??**, we review state-of-the-art upper bounds for quantum capacity of Gaussian channels. In section 8.4, combine our previous result in [FKG21] with decomposition rules to find the optimal upper bound for thermal attenuator. In Sec. 8.5, we find a structure of the phase space of the parameters of thermal attenuator by studying the decomposition rules. Finally in Sec. 8.7, we conclude by suggesting problems that can be studied in the future.

8.3 Decomposition rules

Using the definitions of thermal attenuator and thermal amplifier in chapter. 4, one can show that for $\eta, \eta' \in [0,1], g \geq 1, N, N_2, N_1 \geq 0$ any lossy thermal channel $\mathcal{E}_{\eta,N}$ can be expressed as

$$\mathcal{E}_{\eta,N} = \mathcal{E}_{\eta',N_1} \circ \Phi_{g,N_2} \ , \tag{8.1}$$

if the condition holds

$$\mathbf{C1} = \begin{cases} (1-\eta')(2N_1+1) + (\eta-\eta')(2N_2+1) = \\ (1-\eta)(2N+1) \ , \\ \\ \eta' g = \eta \, , \end{cases} \tag{8.2}$$

or equivalently as

$$\mathcal{E}_{\eta,N} = \Phi_{g,N_2} \circ \mathcal{E}_{\eta',N_1} \ , \tag{8.3}$$

if instead the parameters fulfil the constraint

$$\mathbf{C2} = \begin{cases} (g-1)(2N_2+1) + (g-\eta)(2N_1+1) = \\ (1-\eta)(2N+1) \ , \\ \\ \eta' g = \eta \, , \end{cases} \tag{8.4}$$

Later, we use Eq. 8.18.3 to improve previous upper bounds on thermal attenuator.

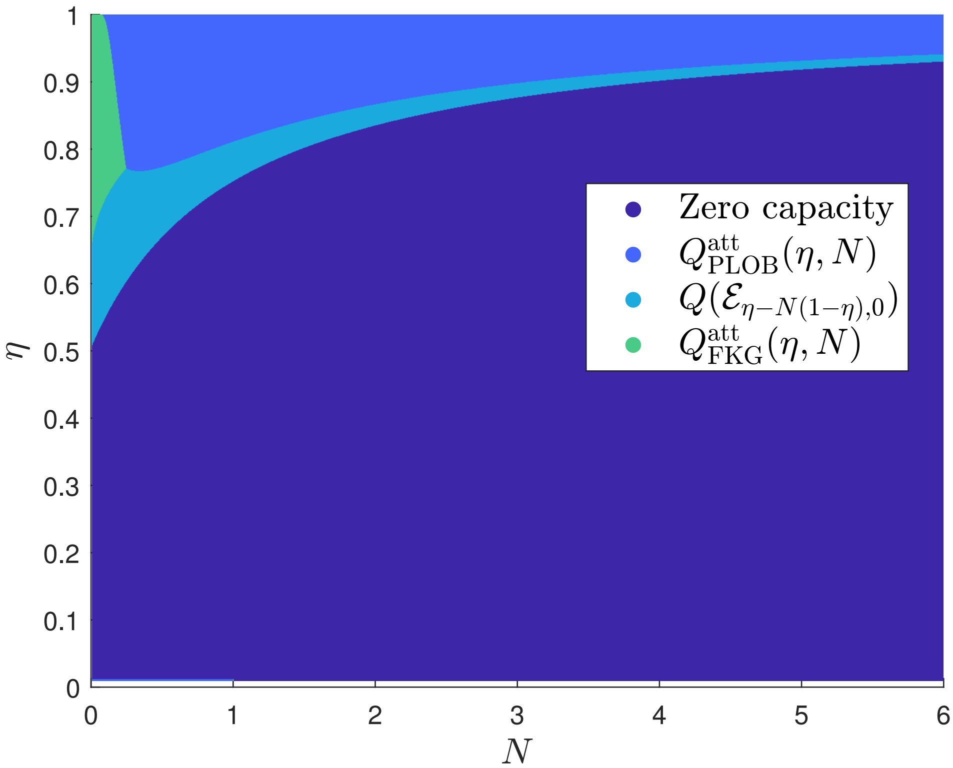

Figure 8.1: Each region with different colour indicates which result is the best upper bound for the quantum capacity of thermal attenuator. Purple region is where the quantum capacity is zero (one of the upper bounds is equal to zero). Light blue is where the result in [RMG18; NAJ19] is the best upper bound, dark blue is for [Pir+17], and green area is where our previous result in [FKG21] is best upper bound.

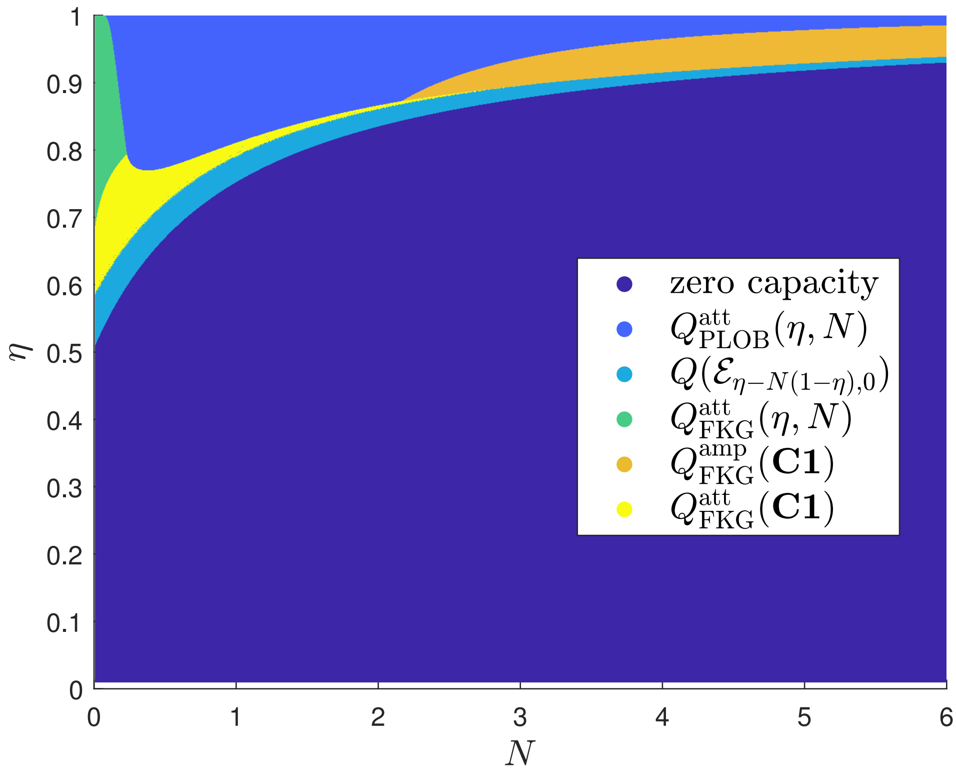

Figure 8.2: The updated version of Fig. 8.1 after considering $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ and $Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1})$. The yellow and orange regions are where $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ and $Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1})$ are strictly lower than the other bounds (note that in the green and light blue regions, $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ is equal to $Q^{\text{att}}_{\text{FKG}}$ and $Q(\mathcal{E}_{\eta-N(1-\eta),0})$, and our analysis does not improve the bounds).

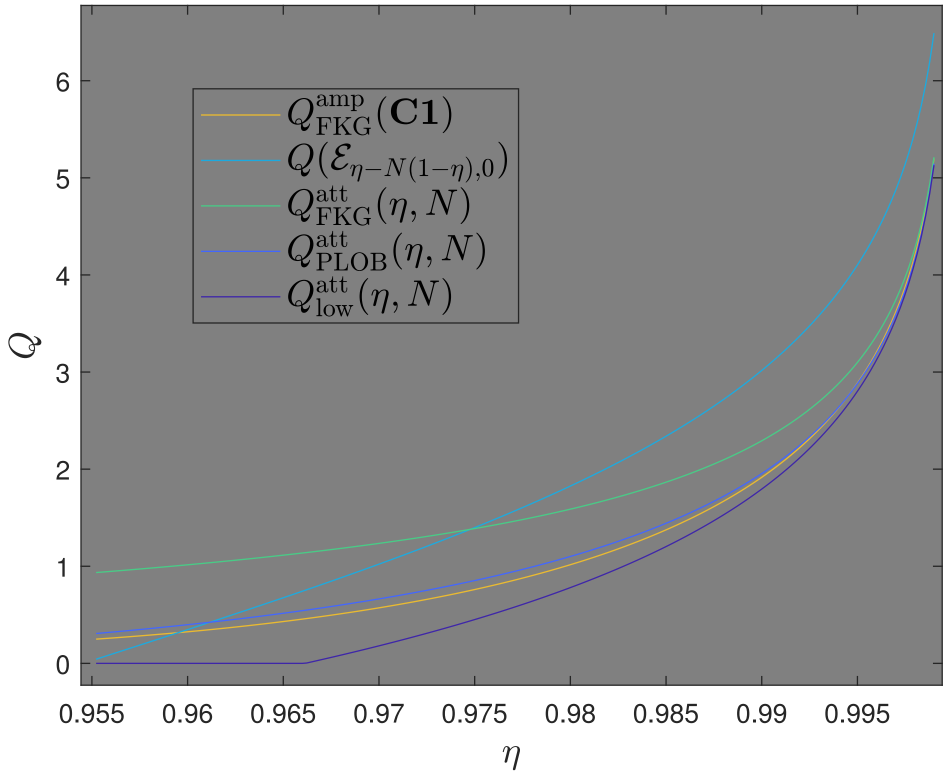

Figure 8.3: The comparison between state of the art upper bounds on the capacity of thermal attenuator for $N = 10$. The light blue, green, and dark blue lines represent the the results presented in [RMG18; NAJ19], [FKG21], and [Pir+17], respectively. The purple line is a lower bound, and the orange line is the result of the optimization in $Q^{\mathrm{amp}}_{\mathrm{FKG}}(\mathbf{C1})$.

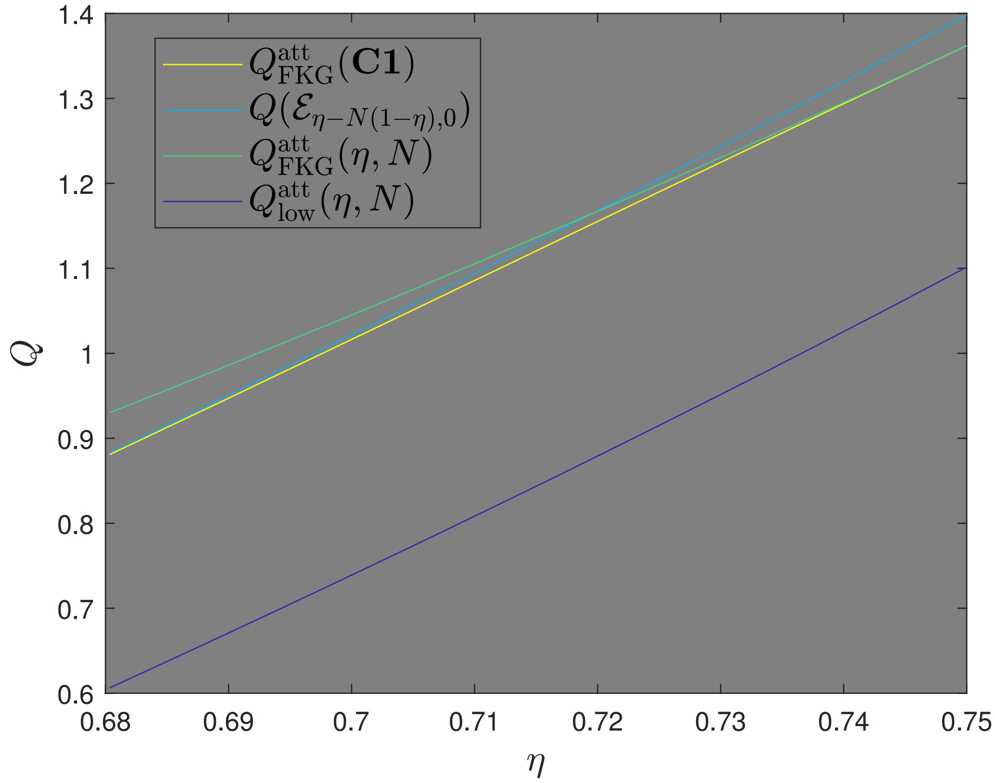

Figure 8.4: Comparison between different upper bounds on the quantum capacity of thermal attenuator for $N = 0.1$. The green and light blue lines show the results in [FKG21] and [RMG18; NAJ19], respectively. The purple line is the lower bound, and the yellow line is $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$. We did not present the result in [Pir+17] here as it is outperformed by the other bounds in this region.

8.4 Combining upper bound in [FKG21] with decomposition rules

In this section, by using the general decomposition rules in Eq. 8.1,8.3 and previous upper bounds in [FKG21] , we introduce a new bound for thermal attenuator. Then, compare it to the previous upper bounds for thermal attenuator. This method naturally reproduces the upper bounds for thermal attenuator found in [FKG21] and [RMG18; NAJ19] too. Applying the data-processing inequality to Eq. 8.1 and Eq. 8.3 introduced above we can establish the following upper bounds

$$Q(\mathcal{E}_{\eta,N}) \leq \min\{ \quad Q^{\text{att}}_{\text{FKG}}(\mathbf{C1}), Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1}), \tag{8.5}$$

$$Q^{\text{att}}_{\text{FKG}}(\mathbf{C2}), Q^{\text{amp}}_{\text{FKG}}(\mathbf{C2})\} \tag{8.6}$$

where for $j = 1, 2$ we have

$$Q^{\text{att}}_{\text{FKG}}(\mathbf{Cj}) := \min_{\mathbf{Cj}} Q^{\text{att}}_{\text{FKG}}(\eta', N_1) \ , \tag{8.7}$$

$$Q^{\text{amp}}_{\text{FKG}}(\mathbf{Cj}) := \min_{\mathbf{Cj}} Q^{\text{amp}}_{\text{FKG}}((g-1)N_2) \tag{8.8}$$

where, for fixed $\eta \in [0, 1]$ and $N \geq 0$, the minimization has to be performed over the set of the parameters $\eta' \in [0, 1], g \geq 1, N_2, N_1 \geq 0$ such that the condition **Cj** holds true.

Theorem 8.4.1 (evaluation of $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$). *given any η and N*

$$Q^{\text{att}}_{\text{FKG}}(\mathbf{C1}) = \min_{N_1 \in [0,N]} Q^{\text{att}}_{\text{FKG}}(\eta'_{opt}(N_1), N_1) \ . \tag{8.9}$$

with

$$\eta'_{opt}(N_1) \quad = \quad \max\left\{1 - (1-\eta)\frac{N+1}{N_1+1}, 0\right\} \ . \tag{8.10}$$

Remark. *Observe that for $N_1 = N$ we get the bound in [FKG21] i.e. $Q^{\text{att}}_{\text{FKG}}(\eta'_{opt}(N), N) = Q^{\text{att}}_{\text{FKG}}(\eta, N)$ while for $N_1 = 0$ we have the bound in[RMG18; NAJ19] i.e. $Q^{\text{att}}_{\text{FKG}}(\eta'_{opt}(0), 0) = Q(\mathcal{E}_{\eta - N(1-\eta),0})$. The minimum value of $Q^{\text{att}}_{\text{FKG}}(\eta'_{opt}(N_1), N_1)$ can be attained for values which are in the interior of $[0, N]$ so $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ is potentially an improvement of the two. In Fig. 8.1 the yellow region is where $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ outperforms the other bounds. In Fig. 8.4 we did the optimization to evaluate $Q^{\text{att}}_{\text{FKG}}(\mathbf{C1})$ numerically and presented a comparison between this upper bound and and other bounds.*

Proof. The first condition of **C1** can be written as

$$(1 - \eta')(N_1 + N_2 + 1) = (1 - \eta)(N + N_2 + 1) \ . \tag{8.11}$$

Considering that in order to have $g \geq 1$ we have to impose $\eta' \in [0, \eta]$, this implies that the constraint can be fulfilled only taking $N_1 \leq N$, a condition that we shall enforce in the following. Notice that (8.11) imposes

$$\begin{aligned} 1 - \eta' &= (1-\eta)\frac{N + N_2 + 1}{N_1 + N_2 + 1} \\ &= (1-\eta)\left(1 + \frac{N - N_1}{N_1 + N_2 + 1}\right) \\ &\leq \min\left\{(1-\eta)\left(1 + \frac{N - N_1}{N_1 + 1}\right), 1\right\} \\ &= \min\left\{(1-\eta)\frac{N+1}{N_1+1}, 1\right\} , \end{aligned} \tag{8.12}$$

with the upper bound being achievable by setting $N_2 \geq 0$ sufficiently small. With this choice we get the lowest possible value of η' for fixed η, N and N'. Therefore, remembering that $Q^{\rm att}_{\rm FKG}(\eta, N)$ is non decreasing in η for fixed N, we can conclude that on **C1** the optimal value of η' is now

$$\begin{aligned} \eta'_{opt}(N_1) &:= 1 - \min\left\{(1-\eta)\frac{N+1}{N_1+1}, 1\right\} \\ &= \max\left\{1 - (1-\eta)\frac{N+1}{N_1+1}, 0\right\} , \end{aligned} \tag{8.13}$$

so that

$$Q^{\rm att}_{\rm FKG}(\mathbf{C1}) = \min_{N_1 \in [0,N]} Q^{\rm att}_{\rm FKG}(\eta'_{opt}(N_1), N_1) . \tag{8.14}$$

□

Theorem 8.4.2 (Evaluation of $Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$). *Given any η and N for which the $Q(\mathcal{E}_{\eta,N})$ is potentially greater than zero i.e. $N \leq \frac{2\eta-1}{2(1-\eta)}$, we have*

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C1}) = Q^{\rm amp}_{FKG}\left(\frac{(1-\eta)N}{\eta}\right) . \tag{8.15}$$

Remark. *In Fig. 8.1 the orange region is where $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ outperforms the other bounds. In Fig. 8.3 we presented a comparison between this upper bound and and other bounds.*

Proof. As in the previous case solutions of the constraint are only possible for $N_1 \leq N$,

$\eta' \leq \eta$. Doing some algebra one can rewrite the first condition in Eq. (8.4) as

$$\begin{aligned} \kappa = (g-1)N_2 &= \frac{(1-\eta)(N-N_1)N_2}{\eta(N+N_2+1)-(N-N_1)} \\ &= \frac{1-\eta}{\eta}(N-N_1)\frac{N_2}{N_2-A} \\ &= \frac{1-\eta}{\eta}(N-N_1)\left(1+\frac{A}{N_2-A}\right) \end{aligned} \tag{8.16}$$

with $A := \frac{(1-\eta)N-N_1-\eta}{\eta}$. We note that the only relevant case is where $(1-\eta)N-\eta \leq 0$, because for $(1-\eta)N-\eta \geq 0$ we already know that the quantum capacity is zero (see the zero capacity condition in 7.23). Therefore, $A \leq 0$, and κ as a function of N_2 is monotonically increasing, spanning for $\kappa = 0$ (a value obtained for $N_2 = 0$) to its maximum value (attained for $N_2 \to \infty$)

$$\begin{aligned} \kappa_{max}(N_1) &:= \frac{1-\eta}{\eta}(N-N_1) \\ &\leq \kappa_{max} := \frac{(1-\eta)N}{\eta}\ , \end{aligned} \tag{8.17}$$

where κ_{max} being achieved for the minimum value of N_1 in the domain. Accordingly we can write

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C1}) = \min_{\kappa\in[0,\kappa_{\rm max}]} Q^{\rm amp}_{FKG}(\kappa)\ . \tag{8.18}$$

We can distinguish two cases depending whether or not $\kappa_{\rm max} = \frac{(1-\eta)N}{\eta}$ is larger or smaller than κ_0 (point where $Q^{\rm amp}_{FKG}(\kappa)$ reaches its minimal value). For $\kappa_{\rm max} \leq \kappa_0$ we get

$$\begin{aligned} &Q^{\rm amp}_{\rm FKG}(\mathbf{C1}) = Q^{\rm amp}_{FKG}(\kappa_{\rm max}) = \\ &= Q^{\rm amp}_{FKG}\left(\frac{(1-\eta)N}{\eta}\right)\ . \end{aligned} \tag{8.19}$$

However, for $\kappa_{\rm max} \geq \kappa_0$ we already know that the quantum capacity is zero, because $\kappa_0 > \frac{1}{2}$ (see the zero capacity condition in 7.23).

□

We can evaluate $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ and $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$ too, however there is no region in which these two bounds outperform the other bounds. For the details see the supplementary materials C.1.

8.5 Lower and higher capacity regions

The composition rules of Bosonic Gaussian Channels allows us to draw some useful relations that can help in strengthening the upper and lower bounds on their capacities.

We start with a theorem determining regions in the parameter space where the capacity is guaranteed to be smaller than the capacity of a given point, and with a similar argument we determine regions where the quantum capacity is greater than the given point. Then, given a lower or upper bound, we construct new bounds utilizing the structure of the parameter space of thermal attenuator.

Theorem 8.5.1 (lower and higher capacity region). *For any η and N*

$$Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'}) \qquad \forall(\eta', N') \in R_{\eta,N} \ , \tag{8.20}$$

with

$$\begin{aligned} R_{\eta,N} : \ &= \ \{(\eta', N') : \eta' \leq \eta, N' \geq N^{(att)}_{\eta,N}(\eta')\} \cup \\ & \quad\ \{(\eta, N) : \eta' \geq \eta, N' \geq N^{(amp)}_{\eta,N}(\eta')\} \ . \end{aligned}$$

where $N^{(att)}_{\eta,N}(\eta')$ and $N^{(amp)}_{\eta,N}(\eta')$ are defined as

$$\begin{aligned} N^{(att)}_{\eta,N}(\eta') \ &:= \ \left(\frac{1-\eta}{\eta}\right) N \left(\frac{\eta'}{1-\eta'}\right) \ , \\ N^{(amp)}_{\eta,N}(\eta') \ &:= \ \frac{\eta' - \eta + (1-\eta)N}{1-\eta'} \ . \end{aligned} \tag{8.21}$$

Similarly, for the higher capacity region

$$Q(\mathcal{E}_{\eta,N}) \leq Q(\mathcal{E}_{\eta',N'}) \qquad \forall(\eta', N') \in S_{\eta,N} \ . \tag{8.22}$$

with

$$\begin{aligned} S_{\eta,N} : \ &= \ \{(\eta', N') : \eta' \geq \eta, N' \leq N^{(att)}_{\eta,N}(\eta')\} \cup \\ & \quad\ \{(\eta, N) : \eta' \leq \eta, N' \leq N^{(amp)}_{\eta,N}(\eta')\} \ . \end{aligned}$$

Proof. We present the proof for the lower capacity region and the proof for the higher capacity region is similar.
We remind that given two thermal channels $\mathcal{E}_{\eta,N}$, $\mathcal{E}_{\eta_1,N_1}$ we have that

$$\mathcal{E}_{\eta_2,N_2} \circ \mathcal{E}_{\eta,N} = \mathcal{E}_{\eta',N'} \ , \tag{8.23}$$

is also a thermal channel with

$$\eta' \ = \ \eta\eta_2 \ , \tag{8.24}$$

$$N' \ = \ \frac{(1-\eta)\eta_2 N + (1-\eta_2)N_2}{1-\eta\eta_2} \geq \frac{(1-\eta)\eta_2}{1-\eta\eta_2} N, \tag{8.25}$$

and we can invoke the pipeline inequality to write $Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'})$. Equivalently this can be formalized as

$$Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'}) \qquad \forall (\eta', N') \in R^{(att)}_{\eta,N} \;, \tag{8.26}$$

where

$$R^{(att)}_{\eta,N} \;\; := \;\; \Big\{ (\eta', N') : \eta' \leq \eta \;, N' \geq N^{(att)}_{\eta,N}(\eta') \Big\} \;, \tag{8.27}$$

with

$$N^{(att)}_{\eta,N}(\eta') := \left(\frac{1-\eta}{\eta} \right) N \left(\frac{\eta'}{1-\eta'} \right) \;. \tag{8.28}$$

To extend the inequality (8.26) we now use the concatenation of thermal attenuators and amplifier. In particular we remind that

$$\mathcal{E}_{\eta,N} \circ \Phi_{g,M} = \mathcal{E}_{\eta',N'} \;, \tag{8.29}$$

with

$$\begin{aligned} \eta' &= g\eta \geq \eta \;, & (8.30) \\ N' &= \frac{(1-\eta)(2N+1) + \eta(g-1)(2M+1)}{2(1-\eta')} - 1/2 \\ &= \frac{\eta' - \eta + (1-\eta)N}{1-\eta'} + \frac{\eta(g-1)}{2(1-\eta')} M \\ &\geq \frac{\eta' - \eta + (1-\eta)N}{1-\eta'} \;. & (8.31) \end{aligned}$$

Hence we can conclude that

$$Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'}) \qquad \forall (\eta', N') \in R^{(amp)}_{\eta,N} \;, \tag{8.32}$$

where

$$R^{(amp)}_{\eta,N} \;\; := \;\; \Big\{ (\eta', N') : \eta' \geq \eta \;, N' \geq N^{(amp)}_{\eta,N}(\eta') \Big\} \;, \tag{8.33}$$

and

$$N^{(amp)}_{\eta,N}(\eta') := \frac{\eta' - \eta + (1-\eta)N}{1-\eta'} \;. \tag{8.34}$$

Sumarizing we arrive to the following conclusion

$$Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'}) \qquad \forall (\eta', N') \in R_{\eta,N} \;, \tag{8.35}$$

with $R_{\eta,N}$ union of the regions $R^{(att)}_{\eta,N}$ and $R^{(amp)}_{\eta,N}$, i.e.

$$R_{\eta,N} \quad := R^{(att)}_{\eta,N} \cup R^{(amp)}_{\eta,N} \;, \tag{8.36}$$

represented by the grey area of Fig. 8.5, i.e. the region whose boundaries are defined by the curves

$$\mathcal{C}^{(att,-)}_{\eta,N} := \Big\{(\eta', N') : \eta' \leq \eta, N' = N^{(att)}_{\eta,N}(\eta'))\Big\} \;, \tag{8.37}$$

$$\mathcal{C}^{(amp,+)}_{\eta,N} := \Big\{(\eta', N') : \eta' \geq \eta, N' = N^{(amp)}_{\eta,N}(\eta'))\Big\} \;. \tag{8.38}$$

With a similar argument one can find the higher capacity region (yellow region in Fig. 8.5) with the following boundaries

$$\mathcal{C}^{(att,+)}_{\eta,N} := \Big\{(\eta', N') : \eta' \geq \eta, N' = N^{(att)}_{\eta,N}(\eta'))\Big\} \;, \tag{8.39}$$

$$\mathcal{C}^{(amp,-)}_{\eta,N} := \Big\{(\eta', N') : \eta' \leq \eta, N' = N^{(amp)}_{\eta,N}(\eta'))\Big\} \;. \tag{8.40}$$

□

Here, we present some observations about Theorem 8.5.1:

Remark. *Notice that simple geometric considerations imply that the inequality in 8.26 imposes that $Q(\mathcal{E}_{\eta,N})$ must be a decreasing function in η for fixed N and more generally that $Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'})$ for all $\eta' \leq \eta$, $N' \geq N$. For an independent derivation of the latter inequalities take $\eta_2 = \eta$, $N_2 = N + \Delta N$ with $\Delta N \geq 0$ and observe that now $N' = N + \frac{\eta-\eta'}{\eta(1-\eta')}\Delta N$ can be made arbitrarily larger by choosing ΔN sufficiently big. Notice also that reversing the order of the composition will lead us to determine that $Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'})$ for all $\eta' \leq \eta$ and $N' \geq \left(\frac{1-\eta}{1-\eta'}\right) N$: this result however is less performant than (8.26) since channels $\mathcal{E}_{\eta',N'}$ that fulfil the latter also fulfil the former.*

Remark. *Observe that reversing the ordering of the concatenation in (8.29) we get an inequality which is provably less performant than (8.32): indeed this case we have that $Q(\mathcal{E}_{\eta,N}) \geq Q(\mathcal{E}_{\eta',N'})$ can be shown to hold for all $\eta' \geq \eta$ and $N' \geq \frac{g-1+(g-\eta')N}{1-\eta'} = \frac{\eta'-\eta+\eta'(1-\eta)N}{\eta(1-\eta')}$, a condition that is already implied by (8.32). The points (η', N') with $N' = \frac{\eta'-\eta+\eta'(1-\eta)N}{\eta(1-\eta')}$ are represented in Fig. 8.5 by the green curve of the plot. This is the same case for the higher capacity region too, more precisely changing the order in Eq. (8.29) does not result to any advantage.*

Remark. *Notice that for $\eta = 0.5$, $N = 0$, we get*

$$Q(\mathcal{E}_{\eta',N'}) \qquad \forall(\eta', N') = 0 \in R^{(amp)}_{\eta=0.5,N=0} \;, \tag{8.41}$$

where we used the fact that $Q(\mathcal{E}_{\eta=0.5,N=0}) = 0$. *Note that by construction it follows that* $R_{\eta=0.5,N=0} = R^{(amp)}_{\eta=0.5,N=0}$, *because* $R^{(att)}_{\eta=0.5,N=0}$ *is formed only by points on the N axis which are inside* $R^{(amp)}_{\eta=0.5,N=0}$. *It turns out that the zero capacity region* $R^{(amp)}_{0.5,0}$ *corresponds to the zero capacity region identified by the [RMG18] bound. In the supplementary materials C.2, we presented a more detailed analysis for the zero capacity region.*

Corollary 8.5.1 (Monotonic behaviour along the curves). *for any* $\eta_1 \leq \eta_2$ *and* $N_1 = N^{(att)}_{\eta,N}(\eta_1)$, $N_2 = N^{(att)}_{\eta,N}(\eta_2)$ *we can write*

$$Q(\mathcal{E}_{\eta_1,N_1}) \leq Q(\mathcal{E}_{\eta_2,N_2}) \,. \tag{8.42}$$

Similarly, for any $\eta_1 \leq \eta_2$ *and* $N_1 = N^{(amp)}_{\eta,N}(\eta_1)$, $N_2 = N^{(amp)}_{\eta,N}(\eta_2)$ *we can write*

$$Q(\mathcal{E}_{\eta_1,N_1}) \geq Q(\mathcal{E}_{\eta_2,N_2}) \,. \tag{8.43}$$

Proof. Note that $(\eta_1, N_1) \in R^{(att)}_{\eta_2,N_2} \subset R_{\eta_2,N_2}$, because $\eta_1 \leq \eta_2$ and

$$\begin{aligned} N^{att}_{\eta_2,N_2}(\eta_1) &= (\frac{1-\eta_2}{\eta_2})N_2(\frac{\eta_1}{1-\eta_1}) \\ &= (\frac{1-\eta}{\eta})N(\frac{\eta_1}{1-\eta_1}) \\ &= N^{(att)}_{\eta,N}(\eta_1) = N_1 \,. \end{aligned} \tag{8.44}$$

As $(\eta_1, N_1) \in R_{\eta_2,N_2}$, using Theorem 8.5.1 we conclude that $Q(\mathcal{E}_{\eta_1,N_1}) \leq Q(\mathcal{E}_{\eta_2,N_2})$.

Similarly for the second part of the theorem, we can show that $(\eta_2, N_2) \in R^{(amp)}_{\eta_1,N_1} \subset R_{\eta_1,N_1}$, because $\eta_1 \leq \eta_2$ and

$$N^{(amp)}_{\eta_1,N_1}(\eta_2) = N^{(amp)}_{\eta,N}(\eta_2) = N_2 \,. \tag{8.45}$$

Therefore, $Q(\mathcal{E}_{\eta_1,N_1}) \geq Q(\mathcal{E}_{\eta_2,N_2})$. □

Corollary 8.5.2 (stable bounds). *Suppose that the functions* $Q^{(+)}(\eta, N)$, $Q^{(-)}(\eta, N)$ *are respectively upper and lower bounds for* $Q(\mathcal{E}_{\eta,N})$, *i.e.*

$$Q^{(+)}(\eta, N) \geq Q(\mathcal{E}_{\eta,N}) \geq Q^{(-)}(\eta, N) \,. \tag{8.46}$$

One can construct new functions as

$$\begin{aligned} \bar{Q}^{(+)}(\eta, N) &:= \min_{(\eta',N')\in S_{\eta,N}} Q^{(+)}(\eta', N') \\ &\leq Q^{(+)}(\eta, N) \,, \end{aligned} \tag{8.47}$$

$$\begin{aligned} \bar{Q}^{(-)}(\eta, N) &:= \max_{(\eta',N')\in R_{\eta,N}} Q^{(-)}(\eta', N') \\ &\geq Q^{(-)}(\eta, N) \,. \end{aligned} \tag{8.48}$$

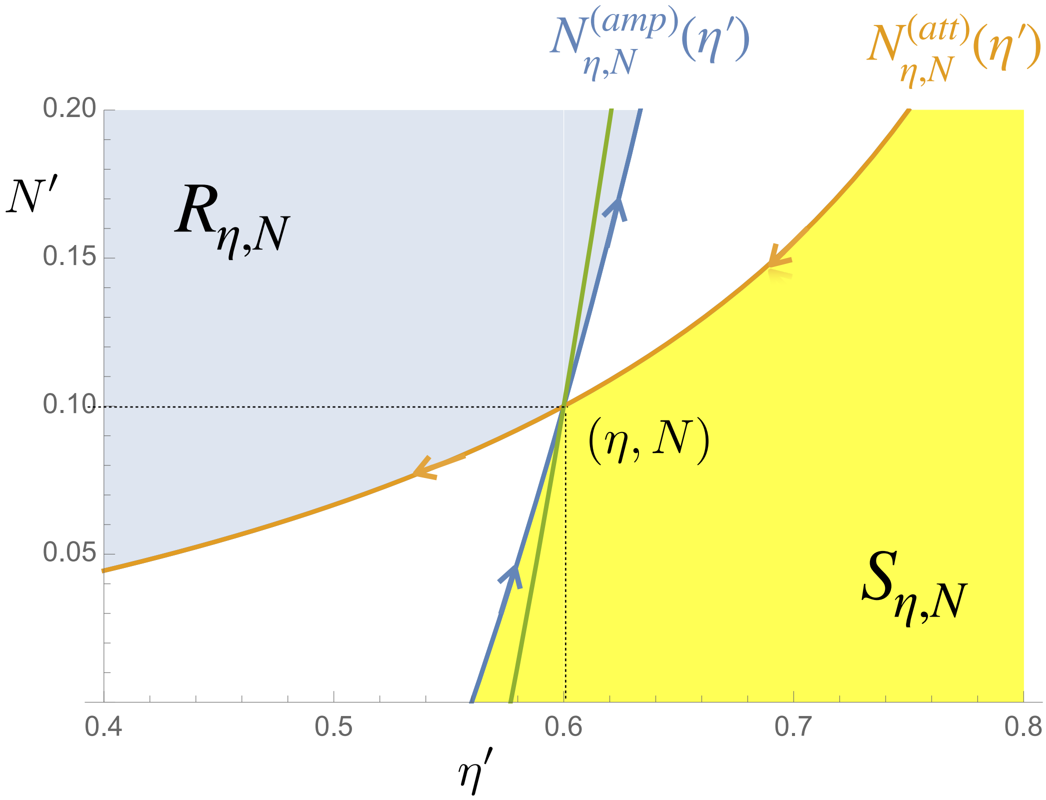

Figure 8.5: Given any point (η, N) the region $R_{\eta,N}$ represents the set of channels whose capacity must be smaller than or equal to $Q(\mathcal{E}_{\eta,N})$; similarly the region $S_{\eta,N}$ represents the set of channels whose capacity must be greater than or equal to $Q(\mathcal{E}_{\eta,N})$. Arrows in the picture show the direction where $Q(\mathcal{E}_{\eta,N})$ has to decrease (or at most remain constant). For the point in the white region our composition rules cannot be used to determine a specific capacity ordering with respect to $Q(\mathcal{E}_{\eta,N})$. The green line in the plot represent the point identified by the curve (η', N') with $N' = \frac{\eta'-\eta+\eta'(1-\eta)N}{\eta(1-\eta')}$ obtained by using the concatenation rule (8.29): as mentioned in the text these points are inside the regions $R_{\eta,N}$ and $S_{\eta,N}$; as for the point associated with the curve $(\eta', N^{amp}_{\eta,N}(\eta'))$ the capacity reduces when moving South-to-North. In the example we set $\eta = 0.6$, $N = 0.1$.

These functions still bound $Q(\mathcal{E}_{\eta,N})$, and potentially can improve $Q^{(+)}(\eta,N)$, $Q^{(-)}(\eta,N)$, i.e.

$$\bar{Q}^{(+)}(\eta,N) \geq Q(\mathcal{E}_{\eta,N}) \geq \bar{Q}^{(-)}(\eta,N) . \tag{8.49}$$

We say that an upper (lower) bound $Q^{(+)}(\eta,N)$ ($Q^{(-)}(\eta,N)$) is stable under concatenation if it coincide with its improved version $\bar{Q}^{(+)}(\eta,N)$ ($\bar{Q}^{(-)}(\eta,N)$).

Remark. *It is clear that good bounds must be stable (if not we can always define a new one that is stronger). In the supplementary materials we showed that $Q^{\rm att}_{\rm low}(\eta,N)$ is stable. However, for the other bounds the stability is not straightforward. In the next section we study the stability of $Q^{\rm att}_{\rm FKG}(\mathbf{C1})$ and $Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$.*

8.6 Question: are the bounds of Sec. 8.4 stable?

It is worth observing that the bounds derived in Sec. 8.4 are connected with the plane decomposition analyzed here. In particular we notice that $Q^{\rm att}_{\rm FKG}(\mathbf{C1})$ have being obtained by considering the points (η',N') on the curve $\mathcal{C}^{(amp,-)}_{\eta,N}$ (the one that delimit $S_{\eta,N}$ for $\eta' \leq \eta$), bounding their capacities (and hence $Q^{\rm att}_{\rm FKG}(\eta,N)$) via $Q^{\rm att}_{\rm FKG}(\eta',N')$ and then taking the minimum, i.e.

$$Q^{\rm att}_{\rm FKG}(\mathbf{C1}) = \min_{(\eta',N')\in\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\rm att}_{\rm FKG}(\eta',N') . \tag{8.50}$$

$Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$ on the other hand has been obtained by considering again the points of $\mathcal{C}^{(amp,-)}_{\eta,N}$ and using $Q^{\rm amp}_{\rm FKG}(g,M)$ to bound the capacity of the amplifier terms $\Phi_{g,M}$ that according to Eq. (8.29) are needed to move them to (η,N) (hence indirectly bounding $Q(\mathcal{E}_{\eta,N})$ as well), i.e.

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C1}) = \min_{(\eta',N')\in\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\rm amp}_{\rm FKG}(g,M) . \tag{8.51}$$

$Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ and $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ are defined analogously by using points of the curve $\mathcal{G}^{(amp,-)}_{\eta,N}$ that connects (η,N) via the concatenation rule that has reverse ordering with respect to (8.29),

$$Q^{\rm att}_{\rm FKG}(\mathbf{C2}) = \min_{(\eta',N')\in\mathcal{G}^{(amp,-)}_{\eta,N}} Q^{\rm att}_{\rm FKG}(\eta',N') , \tag{8.52}$$

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C2}) = \min_{(\eta',N')\in\mathcal{G}^{(amp,-)}_{\eta,N}} Q^{\rm amp}_{\rm FKG}(g,M) . \tag{8.53}$$

One can find a closed expression for $\mathcal{G}^{(amp,-)}_{\eta,N}$ as follows

$$\mathcal{G}^{(amp,-)}_{\eta,N} := \left\{ (\eta',N') : \eta' \leq \eta, N' \geq \frac{\eta'-\eta+\eta'(1-\eta)N}{\eta(1-\eta')} \right\} \tag{8.54}$$

(in Fig. 8.5 it is represented by the lowest part of the green curve).

From the above analysis it is clear that in principle none of the bounds $Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$, $Q^{\rm att}_{\rm FKG}(\mathbf{C1})$, $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$, and $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ are guaranteed to be stable. Indeed they have being obtained by only taking a minimization over a (tiny) portion of $\mathcal{S}_{\eta,N}$. There is hence a chance that their extension on $\mathcal{S}_{\eta,N}$ will give better results. The situation however is slightly more complex than what it seems at first view.

Consider fist the extensions of $Q^{\rm att}_{\rm FKG}(\mathbf{C1})$ and $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ which coincide by construction,

$$\bar{Q}^{\rm att}_{\rm FKG}(\mathbf{C1}) = \bar{Q}^{\rm att}_{\rm FKG}(\mathbf{C2}) = \min_{(\eta',N')\in S_{\eta,N}} Q^{\rm att}_{\rm FKG}(\eta',N') \; . \tag{8.55}$$

Now we remind that for fixed N', the function $Q^{\rm att}_{\rm FKG}(\eta',N')$ is monotonically decreasing in η'. Hence the minimum in Eq. (8.55) is attained on the left-most boundary of $S_{\eta,N}$, i.e. on the curves $\mathcal{C}^{(att,+)}_{\eta,N}$ and $\mathcal{C}^{(amp,-)}_{\eta,N}$. Therefore we can write

$$\begin{aligned} \bar{Q}^{\rm att}_{\rm FKG}(\mathbf{C1}) &= \min_{(\eta',N')\in \mathcal{C}^{(att,+)}_{\eta,N}\cup \mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\rm att}_{\rm FKG}(\eta',N') \\ &= \min\left\{ Q^{\rm att}_{\rm FKG}(\mathbf{C1}), \tilde{Q}^{\rm att}_{\rm FKG}(\mathbf{C1}) \right\} \; . \end{aligned} \tag{8.56}$$

where in the second passage we split the domain, use Eq. (8.50) and introduce the definition

$$\tilde{Q}^{\rm att}_{\rm FKG}(\mathbf{C1}) = \min_{(\eta',N')\in \mathcal{C}^{(att,+)}_{\eta,N}} Q^{\rm att}_{\rm FKG}(\eta',N') \; . \tag{8.57}$$

Now I strongly suspect (have not checked) that $Q^{\rm att}_{\rm FKG}(\eta',N')$ reaches it minimum on (η,N) (which is also included in $\mathcal{C}^{(amp,-)}_{\eta,N}$) so that the above expression reduces to $\bar{Q}^{\rm att}_{\rm FKG}(\mathbf{C1}) = Q^{\rm att}_{\rm FKG}(\mathbf{C1})$, i.e. there is no gain.

Here, we analyse the stability of $Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$ and $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$ in the region where the quantum capacity is potentially greater than zero $N \leq \frac{2\eta-1}{2(1-\eta)}$. In this regime, we combine Corollary 8.5.2 and Eq. 8.15, C.13 to write

$$\bar{Q}^{\rm amp}_{\rm FKG}(\mathbf{C1}) = \min_{(\eta',N')\in S_{\eta,N}} Q^{\rm amp}_{FKG}(\frac{(1-\eta')N'}{\eta'}) \tag{8.58}$$

$$\bar{Q}^{\rm amp}_{\rm FKG}(\mathbf{C2}) = \min_{(\eta',N')\in S_{\eta,N}} Q^{\rm amp}_{FKG}((1-\eta')N'). \tag{8.59}$$

We note that for $\kappa \leq \kappa_0$, $Q^{\rm amp}_{FKG}(\kappa)$ is decreasing in κ, which is indeed the case. Because, given that $N \leq \frac{2\eta-1}{2(1-\eta)}$ one can show $(1-\eta')N' \leq \frac{(1-\eta')N'}{\eta'} \leq \kappa_0$ for any $(\eta',N') \in S_{\eta,N}$. Therefore, to solve the minimization problems we should simply maximize $\frac{(1-\eta')N'}{\eta'}$ and

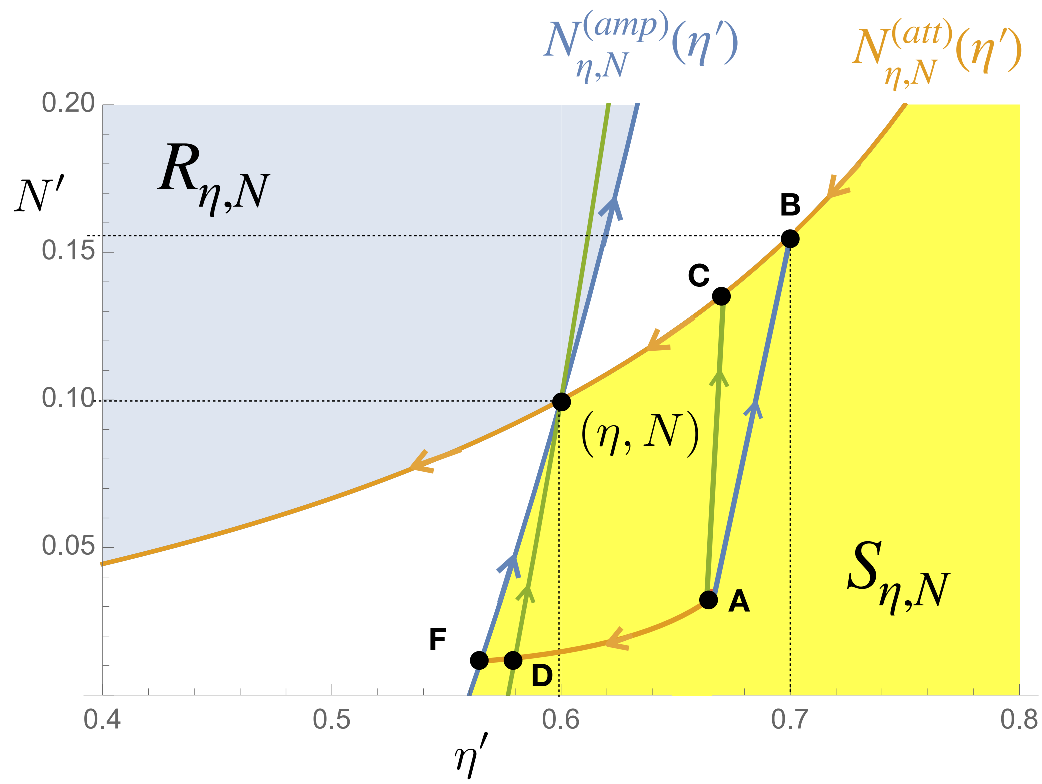

Figure 8.6: A generic point $A = (\eta', N')$ in the interior of $S_{\eta,N}$ can be moved to (η, N) via the action of one amplifier map Φ plus an extra attenuator $\mathcal{E}$. Depending on the ordering of the operations we can select different routes. For instance the routes $A \to D \to (\eta, N)$ and $A \to F \to (\eta, N)$ correspond to a transformation of the form $\mathcal{E} \circ \mathcal{E}_A \circ \Phi$ and $\Phi \circ \mathcal{E} \circ \mathcal{E}_A$ respectively.

$(1-\eta')N'$ which are increasing functions in N' for a fixed η'. Therefore, to find their maximum on $S_{\eta,N}$ we can reduce the maximizations to the borders of $S_{\eta,N}$, so

$$\bar{Q}^{\text{amp}}_{\text{FKG}}(\mathbf{C1}) := \min_{(\eta',N')\in\mathcal{C}^{(att,+)}_{\eta,N}\cup\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left(\frac{(1-\eta')N'}{\eta'}\right) \tag{8.60}$$

$$\bar{Q}^{\text{amp}}_{\text{FKG}}(\mathbf{C2}) := \min_{(\eta',N')\in\mathcal{C}^{(att,+)}_{\eta,N}\cup\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left((1-\eta')N'\right)\ . \tag{8.61}$$

For the minimizations on $\mathcal{C}^{(att,+)}$, using Eq. 8.21, we write

$$\frac{(1-\eta')N^{(att)}_{\eta,N}(\eta')}{\eta'} = \frac{(1-\eta)N}{\eta} \tag{8.62}$$

$$(1-\eta')N^{(att)}(\eta') = \frac{\eta'(1-\eta)N}{\eta}\ , \tag{8.63}$$

For the first equation, the optimization is trivial.
For the second one, $\eta'=1$ is where the function reaches its maximum, so

$$\begin{aligned} Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1}) &= \min_{(\eta',N')\in\mathcal{C}^{(att,+)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left(\frac{(1-\eta')N'}{\eta'}\right) \\ &= \min_{(\eta',N')\in\mathcal{C}^{(att,+)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left((1-\eta')N'\right)\ . \end{aligned} \tag{8.64}$$

The minimization on $\mathcal{C}^{(amp,+)}$ is also simple. Using Eq. 8.21 again, we can write

$$\frac{(1-\eta')N^{(amp)}_{\eta,N}(\eta')}{\eta'} = 1 - \frac{\eta-(1-\eta)N}{\eta'}\ , \tag{8.65}$$

$$(1-\eta')N^{(amp)}_{\eta,N}(\eta') = \eta' - (\eta-(1-\eta)N) \tag{8.66}$$

As $(\eta-(1-\eta)N)\geq 0$ (simply because $N\leq\frac{2\eta-1}{2(1-\eta)}$), both of the functions are increasing in η', therefore they reach their maximum for the maximum possible value of η' i.e. $\eta'=\eta$ (note that in $\mathcal{C}^{(amp,-)}$, we always have $\eta'\leq\eta$), and we get

$$\min_{(\eta',N')\in\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left(\frac{(1-\eta')N'}{\eta'}\right) = Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1}) \tag{8.67}$$

$$\min_{(\eta',N')\in\mathcal{C}^{(amp,-)}_{\eta,N}} Q^{\text{amp}}_{FKG}\left((1-\eta')N'\right) = Q^{\text{amp}}_{\text{FKG}}(\mathbf{C2})\,. \tag{8.68}$$

Putting everything together we get

$$\bar{Q}^{\text{amp}}_{\text{FKG}}(\mathbf{C1}) = \bar{Q}^{\text{amp}}_{\text{FKG}}(\mathbf{C2}) = Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1}). \tag{8.69}$$

This means that $Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1})$ is stable and using Corollary 8.5.2 we can improve $Q^{\text{amp}}_{\text{FKG}}(\mathbf{C1})$.

8.7 Conclusion

We have determined new upper bounds for the quantum and private capacity of thermal attenuator by studying the decomposition rules. The new bounds out perform the previous results for different values of the parameters of thermal attenuator. Also, we introduced a structure for the phase space of the parameters of thermal attenuator. This structure potentially can be used to improve any given lower or upper bound. A relevant problem could be applying this structure to improve the upper bounds in [Pir+17]. In addition, one could do a similar analysis for the thermal amplifier.

Chapter 9

Conclusions

In this thesis, we mainly focused on the long standing open problem of quantum Shannon theory, namely the estimation of the quantum capacities of quantum channels. We presented the previous bounds, and our contributions to the literature. Mostly, We made use of degradable extensions as the principal technique to do so. To design the degradable extensions, we introduced ancillary systems which give some information about the action of the original channels. In most cases, such ancillary systems can be interpreted as some non orthogonal quantum flags which make the extensions degradable.

In the thesis, after discussing some preliminaries in the first four chapters, we studied the impossibility of undoing a mixing process with some given side information, and found the optimal machines to do so, in Chapter 5. Then, in Chapter 6, we introduced an important technique, flagged channels, to design degradable extensions which is of a vast applicability. In Chapter 7, we generalized the flagged extension technique to Continuous variable systems, and bounded the capacities of some important Gaussian channels. Finally in Chapter 8, we improved the bounds for the capacities of Thermal attenuator found in Chapter 8 using information processing inequalities in their general form.
As the final remark, we recap the main results and possible future works.

9.1 Chapter 6: Degradable Flagged Extensions: Discrete Channels

We introduced a technique to design degradable extensions, flagged channels, of important qudit channels. Our technique is quite general, and we applied it to important qudit channels with unknown quantum capacity, namely Pauli channels and generalized amplitude damping, and improved the previous upper bounds on their quantum capacity. In the following we present the some possible future works

- Our degradable extension highly depends on the Kraus representation that we choose for the original channel. It would be interesting to use this degree of freedom i.e. choosing different Kraus representations, to improve the bounds.
- One can also design degradable extensions for many uses of the channel of interest. This could potentially result to a better bound, and bring us closer to the value of quantum capacity.

9.2 Chapter 7: Degradable Extension: Gaussian channels

We extended the technique introduced in Chapter 6 to Gaussian channels, and designed degradable extensions for important Gaussian channels, namely thermal attenuator, thermal amplifier, and additive Gaussian noise. By computing the quantum capacity of the degradable extensions, we managed to improve the previous upper bounds on the quantum capacity of the aforementioned channels. As some possible future work

- One can study the energy constrained quantum capacity and bound this quantity using the same techniques.
- Designing other degradable extensions can be always helpful to improve the bounds. For instance, our degradable extension of thermal attenuator has some degrees of freedom that can be used to improve the bound.

9.3 Chapter 8: Improving Bounds for Thermal Attenuator Using Decomposition Rules

We used decomposition rules in its most general form to improve the previous bounds on the quantum capacity of thermal attenuator. In addition, we showed that any bound on the quantum capacity should follow some certain symmetries, otherwise one can construct a better upper bound using decomposition rules. We propose some future works as follows

- The same analysis can be done for thermal amplifier and one may be able to improve the bounds for this channel too.
- One can also generalize the analysis to the energy constrained case, and find better bounds for the energy constrained quantum capacity.

Appendix A

Appendix of Optimal Subtracting Machine

Supplemental material is organised as following. First, we provide explicit derivation of the decomposition (5.16) of the main text. Then using (5.16) we derive the fidelity (5.20) of the main text. Third, we present an explicit derivation of Eq. (5.23) of the main text. Then we analyze the application of the decomposition (5.16) of the main text to the case where $n_1 = n_2 = 1$, and in the following section we do the same for the case $n_1 = 2, n_2 = 1$. Analytical optimisation is also done for the case $n_1 = 2, = \infty$. Then, we present the derivation of an upper bound for the average fidelity of the UQS realised via measurement and prepare strategies. Finally, we apply the method of Cirac et al. [CEM99] for case $n_1 = 2$ and arbitrary n_2.

A.1 Covariant Channel Characterisation

Here the calculations to derive the characterisation for covariant are presented. Introducing a Kraus decomposition for Λ in Eq.(5.14) of the main text we get

$$\Lambda_c[\cdots] = \sum_k \int d\mu_U \; U M_k U^{\dagger \otimes N} [\cdots] U^{\otimes N} M_k^{\dagger} U^{\dagger} \;, \tag{A.1}$$

with M_k the associated Kraus operators. Accordingly we can express the matrix element (5.16)

$$\begin{aligned} \left\langle \tfrac{1}{2}, s \right| \Lambda_c(|j,m,g\rangle \langle j',m',g'|) \left| \tfrac{1}{2}, s' \right\rangle = \quad & \sum_k \sum_{r,r'} \sum_{l,l'} \int d\mu_U D^{1/2}_{s,r}(U) M^{k,j,g}_{r,l} D^{j}_{l,m}(U^{\dagger}) \\ & \times D^{j'}_{m',l'}(U) M^{\dagger k,j',g'}_{l',r'} D^{1/2}_{r',s'}(U^{\dagger}) \;, \end{aligned} \tag{A.2}$$

where

$$D^j_{l,l'}(U) := \langle j,l,g| U^{\otimes N} |j,l',g\rangle \ , \qquad M^{k,j,g}_{r,l} := \langle \tfrac{1}{2}, r| M_k |j,l,g\rangle \ . \qquad \text{(A.3)}$$

We can write the multiplication of two Wigner matrices in the following form

$$\begin{aligned} D^{1/2}_{s,r}(U) D^j_{l,m}(U^\dagger) &= (-1)^{l-m} \langle \tfrac{1}{2}, s| U |\tfrac{1}{2}, r\rangle \langle j,-m,g| U^{\otimes N} |j,-l,g\rangle \\ &= (-1)^{l-m} \langle 1/2, s| \otimes \langle j,-m,g| U^{\otimes N+1} |1/2, r\rangle \otimes |j,-l,g\rangle \\ &= (-1)^{l-m} \sum_{j-\frac{1}{2}\leq q\leq j+\frac{1}{2}} C^{q \quad s-m}_{\frac{1}{2}\, s, j\, -m} C^{q \quad r-l}_{\frac{1}{2}\, r, j\, -l} D^q_{s-m,r-l}(U) \ , \qquad \text{(A.4)} \end{aligned}$$

where $C^{J \quad M}_{j\, m, j'\, m'} = \langle J, M| j\, m\rangle \otimes |j'\, m'\rangle$ are the Clebsch-Gordan coefficients. Exploiting this we can hence rewrite Eq. (A.2) in the following form

$$\begin{aligned} \langle \tfrac{1}{2}, s| \Lambda_c(|j,m,g\rangle \langle j',m',g'|) |\tfrac{1}{2}, s'\rangle &= \sum_k \sum_{r,r'} \sum_{l,l'} \sum_{q,q'} (-1)^{l-m+l'-m'} \int d\mu_U \quad C^{q \quad s-m}_{\frac{1}{2}\, s, j\, -m} C^{q \quad r-l}_{\frac{1}{2}\, r, j\, -l} \\ &\times D^q_{s-m,r-l}(U) M^{k,j,g}_{r,l} C^{q' \quad r'-l'}_{\frac{1}{2}\, r', j'\, -l'} C^{q' \quad s'-m'}_{\frac{1}{2}\, s', j'\, -m'} \\ &\times D^{q'}_{r'-l',s'-m'}(U^\dagger) M^{\dagger k,j',g'}_{l',r'} \ . \qquad \text{(A.5)} \end{aligned}$$

Remembering that following identity of Wigner matrices (Peter-Weyl theorem, see [Kna10])

$$\int d\mu_U\, D^j_{m,l}(U) D^{j'}_{m',l'}(U)^* = \frac{1}{2j+1} \delta_{j,j'} \delta_{m,m'} \delta_{l,l'} \qquad \text{(A.6)}$$

the integral in (A.5) can hence be simplified to

$$\begin{aligned} \langle \tfrac{1}{2}, s| \Lambda_c(|j,m,g\rangle \langle j',m',g'|) |\tfrac{1}{2}, s'\rangle &= \sum_k \sum_{r,r'} \sum_{l,l'} \sum_q \frac{(-1)^{l-m+l'-m'}}{2j+1} \delta_{s-m,s'-m'} \delta_{r-l,r'-l'} \\ &\times C^{q \quad s-m}_{\frac{1}{2}\, s, j\, -m} C^{q \quad s'-m'}_{\frac{1}{2}\, s', j'\, -m'} C^{q \quad r-l}_{\frac{1}{2}\, r, j\, -l} \\ &\times M^{k,j,g}_{r,l} C^{q \quad r'-l'}_{\frac{1}{2}\, r', j'\, -l'} M^{\dagger k,j',g'}_{l',r'} \ . \qquad \text{(A.7)} \end{aligned}$$

Introducing then the variable $p := r - l = r' - l'$, we can rewrite the above identity as

$$\begin{aligned} \langle 1/2, s| \Lambda_c(|j,m,g\rangle \langle j',m',g'|) |1/2, s'\rangle &= \sum_k \sum_{r,r'} \sum_p \sum_q \frac{(-1)^{r-m+r'-m'}}{2j+1} \delta_{s-m,s'-m'} \\ &\times C^{q \quad s-m}_{\frac{1}{2}\, s, j\, -m} C^{q \quad s'-m'}_{\frac{1}{2}\, s', j'\, -m'} C^{q \quad p}_{\frac{1}{2}\, r, j\, p-r} \\ &\times M^{k,j,g}_{r,r-p} C^{q \quad p}_{\frac{1}{2}\, r', j'\, p-r'} M^{\dagger k,j',g'}_{r'-p,r'} \ , \qquad \text{(A.8)} \end{aligned}$$

which, defining the row vectors $\mathbf{v}^j_{q,g}$ of components

$$\mathbf{v}^j_{q,g}(k,p) := \frac{1}{2j+1} \sum_r (-1)^r C^{q \quad p}_{\frac{1}{2}\, r, j\, p-r} M^{k,j,g}_{r,r-p} \ , \qquad \text{(A.9)}$$

and their associated scalar products

$$W^{j,j'}_{q,g,g'} := \mathbf{v}^{j}_{q,g} \cdot (\mathbf{v}^{j'}_{q,g'})^{\dagger} = \sum_{k,p} \mathbf{v}^{j}_{q,g}(k,p) \left[\mathbf{v}^{j'}_{q',g'}(k,p)\right]^{*} \ , \tag{A.10}$$

allows us to finally express Eq. (A.8) as in Eq. (5.16) of the main text

$$\left\langle \tfrac{1}{2}, s\right| \Lambda_c \left[|j,m,g\rangle\langle j',m',g'|\right] \left|\tfrac{1}{2}, s'\right\rangle = (-1)^{m-m'} \delta_{s-m,s'-m'} \sum_{q\in Q_{j,j'}} C^{q\ \ s-m}_{\frac{1}{2}\ s, j\ -m}\, C^{q\ \ s'-m'}_{\frac{1}{2}\ s', j'\ -m'}\ W^{j,j'}_{q,g,g'} \tag{A.11}$$

A.2 Fidelity calculation for arbitrary n_1, n_2 and numerical optimisation

Using Eq. (5.13) of the main text the average fidelity can be expressed as

$$F_{n_1,n_2}(\Lambda_c) = \langle\uparrow| \Lambda_c[\int d\mu_V \left(p\,|\uparrow\rangle\langle\uparrow| + (1-p)V\,|\uparrow\rangle\langle\uparrow|\,V^{\dagger}\right)^{\otimes n_1} \otimes \left(V\,|\uparrow\rangle\langle\uparrow|\,V^{\dagger}\right)^{\otimes n_2}]\,|\uparrow\rangle \ , \tag{A.12}$$

Knowing that Ω_{n_1,n_2} is invariant under any permutation on the first n_1 qubits, we can write

$$\begin{aligned} F_{n_1,n_2}(\Lambda_c) = \quad & \frac{1}{|S_{n_1}|} \langle\uparrow| \Lambda_c[\sum_{\sigma} \Pi_{\sigma} \int d\mu_V \left(p\,|\uparrow\rangle\langle\uparrow| + (1-p)V\,|\uparrow\rangle\langle\uparrow|\,V^{\dagger}\right)^{\otimes n_1} \\ & \otimes \left(V\,|\uparrow\rangle\langle\uparrow|\,V^{\dagger}\right)^{\otimes n_2} \Pi^{\dagger}_{\sigma}]\,|\uparrow\rangle \ , \end{aligned} \tag{A.13}$$

where Π_σ is a permutation on the first n_1 qubits, and σ runs over all the elements of the symmetric group S_{n_1}, and $|S_{n_1}|$ is the number of elements of symmetric group. Then we can write

$$F_{n_1,n_2}(\Lambda_c) = \frac{1}{|S_{n_1}|} \langle\uparrow| \Lambda_c[\sum_{k=0}^{n_1} \sum_{\sigma} \binom{n_1}{k} (1-p)^k p^{n_1-k} \Pi_\sigma\,|\uparrow\rangle\langle\uparrow|^{\otimes k} \otimes A_{N-k} \Pi^{\dagger}_{\sigma}]]\,|\uparrow\rangle \ , \tag{A.14}$$

where $A_k := \int d\mu_V [V\,|\uparrow\rangle\langle\uparrow|\,V^{\dagger}]^{\otimes k}$. Defining B_k, we carry on the calculation

$$\begin{aligned} B_k \ &:= \ |\uparrow\rangle\langle\uparrow|^{\otimes k} \otimes A_{N-k} \\ &= \sum_{m,m',s,s'} \frac{\delta_{m+s,m'+s'}}{N-k+1} C^{\frac{N-k}{2}\ \ m+s}_{\frac{N-k-n_2}{2}\ m,\ \frac{n_2}{2}\ s}\, C^{\frac{N-k}{2}\ \ m'+s'}_{\frac{N-k-n_2}{2}\ m',\ \frac{n_2}{2}\ s'}\, |\uparrow\rangle\langle\uparrow|^{\otimes k} \\ &\quad \otimes \left|\frac{N-k-n_2}{2}, m\right\rangle \left\langle\frac{N-k-n_2}{2}, m'\right| \otimes \left|\frac{n_2}{2}, s\right\rangle \left\langle\frac{n_2}{2}, s'\right| . \end{aligned} \tag{A.15}$$

Note that here we do not need to sum over any multiplicity index for the states $\left|\frac{N-k-n_2}{2}, m\right\rangle$ and $\left|\frac{n_2}{2}, s\right\rangle$, because A_{N-k} is supported on the completely symmetric subspace of $N-k$ qubits, therefore it is also supported on the tensor product of the completely symmetric subspaces of $N-k-n_2$ and n_2 qubits, which have multiplicity 1. Writing the first n_1 qubits in the total angular momentum basis we get

$$B_k = \sum_{m,s,m',s',j_1,j_1'} \frac{\delta_{m+s,m'+s'}}{N-k+1} C^{\frac{N-k}{2} \quad m+s}_{\frac{N-k-n_2}{2}\ m,\ \frac{n_2}{2}\ s} C^{\frac{N-k}{2} \quad m'+s'}_{\frac{N-k-n_2}{2}\ m',\ \frac{n_2}{2}\ s'} C^{j_1 \quad \frac{k}{2}+m}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m} C^{j_1' \quad \frac{k}{2}+m'}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m'} \left|j_1, \frac{k}{2}+m, k\right\rangle \left\langle j_1', \frac{k}{2}+m', k\right| \otimes \left|\frac{n_2}{2}, s\right\rangle \left\langle \frac{n_2}{2}, s'\right| \tag{A.16}$$

here the multiplicity index k indicates that we first wrote the k qubits in the total angular momentum basis then we summed it up with $\left|\frac{N-k-n_2}{2}, m\right\rangle \left\langle \frac{N-k-n_2}{2}, m\right|$. Schur's lemma implies

$$\frac{1}{|S_{n_1}|} \sum_\sigma \Pi_\sigma \left|j_1, m, k\right\rangle \left\langle j_1', m', k\right| \Pi_\sigma^\dagger = \sum_{g_{j_1}} \frac{1}{\#g_{j_1}} \left|j_1, m, g_{j_1}\right\rangle \left\langle j_1, m', g_{j_1}\right| \delta_{j_1,j_1'}, \tag{A.17}$$

where g_{j_1} is the index for the multiplicity of j_1 and runs over all the possible values for a certain j_1, and $\#g_{j_1} = \frac{(n_1)!(2j_1+1)}{(\frac{n_1-2j_1}{2})(\frac{n_1+2j_1}{2}+1)}$. Using Eq. (A.17) in Eq. (A.14) we get

$$\begin{aligned} F_{n_1,n_2}(\Lambda_c) &= \langle\uparrow| \Lambda_c \Big[\sum_{m,s,m',s',j_1,k,g_{j_1}} \frac{1}{\#g_{j_1}} \binom{n_1}{k} (1-p)^k p^{n_1-k} \frac{\delta_{m+s,m'+s'}}{N-k+1} C^{\frac{N-k}{2} \quad m+s}_{\frac{N-k-n_2}{2}\ m,\ \frac{n_2}{2}\ s} C^{\frac{N-k}{2} \quad m'+s'}_{\frac{N-k-n_2}{2}\ m',\ \frac{n_2}{2}\ s'} \\ &\quad C^{j_1 \quad \frac{k}{2}+m}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m} C^{j_1 \quad \frac{k}{2}+m'}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m'} \left|j_1, \frac{k}{2}+m, g_{j_1}\right\rangle \left\langle j_1, \frac{k}{2}+m', g_{j_1}\right| \otimes \left|\frac{n_2}{2}, s\right\rangle \left\langle \frac{n_2}{2}, s'\right| \Big] |\uparrow\rangle \\ &= \langle\uparrow| \Lambda_c \Big[\sum_{m,s,m',s',j_1,j,j',k,g_{j_1}} \frac{1}{\#g_{j_1}} \binom{n_1}{k} (1-p)^k p^{n_1-k} \frac{\delta_{m+s,m'+s'}}{N-k+1} \\ &\quad C^{\frac{N-k}{2} \quad m+s}_{\frac{N-k-n_2}{2}\ m,\ \frac{n_2}{2}\ s} C^{\frac{N-k}{2} \quad m'+s'}_{\frac{N-k-n_2}{2}\ m',\ \frac{n_2}{2}\ s'} \\ &\quad C^{j_1 \quad \frac{k}{2}+m}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m} C^{j_1 \quad \frac{k}{2}+m'}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m'} C^{j \quad \frac{k}{2}+m+s}_{j_1\ \frac{k}{2}+m,\ \frac{n_2}{2}\ s} C^{j' \quad \frac{k}{2}+m'+s'}_{j_1\ \frac{k}{2}+m',\ \frac{n_2}{2}\ s'} \\ &\quad \left|j, \frac{k}{2}+m+s, g_{j_1}\right\rangle \left\langle j', \frac{k}{2}+m'+s', g_{j_1}\right| \Big] |\uparrow\rangle\ . \end{aligned} \tag{A.18}$$

Using the Eq. (5.16) of the main text we get

$$\begin{aligned} F_{n_1,n_2}(\Lambda_c) &= \sum_{m,s,m',s',j_1,j,j',k,g_{j_1},q} \frac{1}{\#g_{j_1}} \binom{n_1}{k} (1-p)^k p^{n_1-k} \frac{\delta_{m+s,m'+s'}}{N-k+1} C^{\frac{N-k}{2} \quad m+s}_{\frac{N-k-n_2}{2}\ m,\ \frac{n_2}{2}\ s} \\ &\quad C^{\frac{N-k}{2} \quad m'+s'}_{\frac{N-k-n_2}{2}\ m',\ \frac{n_2}{2}\ s'} C^{j_1 \quad \frac{k}{2}+m}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m} C^{j_1 \quad \frac{k}{2}+m'}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\ m'} C^{j \quad \frac{k}{2}+m+s}_{j_1\ \frac{k}{2}+m,\ \frac{n_2}{2}\ s} C^{j' \quad \frac{k}{2}+m'+s'}_{j_1\ \frac{k}{2}+m',\ \frac{n_2}{2}\ s'} \\ &\quad C^{q \quad -\frac{k-1}{2}-m-s}_{\frac{1}{2}\frac{1}{2},\ j-\frac{k}{2}-m-s} C^{q \quad -\frac{k-1}{2}-m'-s'}_{\frac{1}{2}\frac{1}{2},\ j'-\frac{k}{2}-m'-s'} W^{j,j'}_{q,g_{j_1},g_{j_1}}\ . \end{aligned} \tag{A.19}$$

The dependence of the coefficients of $W^{j,j'}_{q,g_{j_1},g_{j_1}}$ on the multiplicity index g_{j_1} is only through j_1. So, we can define

$$C^{j,j'}_{q,j_1}(p) := \sum_{m,s,m',s',k} \binom{n_1}{k}(1-p)^k p^{n_1-k} \frac{\delta_{m+s,m'+s'}}{N-k+1} C^{\frac{N-k}{2}\quad m+s}_{\frac{N-k-n_2}{2}\, m,\ \frac{n_2}{2}\, s} C^{\frac{N-k}{2}\quad m'+s'}_{\frac{N-k-n_2}{2}\, m',\ \frac{n_2}{2}\, s'} \\ C^{j_1\quad \frac{k}{2}+m}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\, m} C^{j_1\quad \frac{k}{2}+m'}_{\frac{k}{2}\frac{k}{2},\ \frac{N-k-n_2}{2}\, m'} C^{j\quad \frac{k}{2}+m+s}_{j_1\, \frac{k}{2}+m,\ \frac{n_2}{2}\, s} C^{j'\quad \frac{k}{2}+m'+s'}_{j_1\, \frac{k}{2}+m',\ \frac{n_2}{2}\, s'} C^{q\quad -\frac{k-1}{2}-m-s}_{\frac{1}{2}\frac{1}{2},\ j-\frac{k}{2}-m-s} C^{q\quad -\frac{k-1}{2}-m'-s'}_{\frac{1}{2}\frac{1}{2},\ j'-\frac{k}{2}-m'-s'}, \tag{A.20}$$

and write the fidelity as

$$F_{n_1,n_2}(\Lambda_c) = \sum_{j,j',j_1,q} C^{j,j'}_{q,j_1}(p) \sum_{g_{j_1}} \frac{1}{\# g_{j_1}} W^{j,j'}_{q,g_{j_1},g_{j_1}}, \tag{A.21}$$

Because Ω_{n_1,n_2} is symmetric on the first n_1 qubits, we can always choose Λ_c to be symmetric on the first n_1 qubits, therefore

$$\Lambda_c[\rho] = \frac{1}{|S_{n_1}|} \sum_{\sigma} \Lambda_c[\Pi_\sigma \rho \Pi_\sigma^\dagger]. \tag{A.22}$$

Using (A.17) we derive

$$W^{j,j'}_{q,g_{j_1},g_{j_1}} = \frac{1}{\# g_{j_1}} \sum_{g'_{j_1}} W^{j,j'}_{q,g'_{j_1},g'_{j_1}}, \tag{A.23}$$

therefore

$$W^{j,j'}_{q,g_{j_1},g_{j_1}} = W^{j,j'}_{q,g'_{j_1},g'_{j_1}} \quad \forall g_{j_1}, g_{j'_1}. \tag{A.24}$$

so defining $W^{j,j'}_{q,j_1} := \frac{1}{\# g_{j_1}} \sum_{g_{j_1}} W^{j,j'}_{q,g_{j_1},g_{j_1}}$, then we get

$$F_{n_1,n_2}(\Lambda_c) = \sum_{j,j',j_1,q} C^{j,j'}_{q,j_1}(p) W^{j,j'}_{q,j_1}. \tag{A.25}$$

Now, the number of parameters i.e. $W^{j,j'}_{q,j_1}$, scale polynomially with n_1 and n_2 because the multiplicity index is fixed to be j_1 and the number of different j_1 is $\mathcal{O}(n_1)$. Without using the characterisation of covariant channels and writing Ω_{n_1,n_2} in the proper form, the number of parameters grows exponentially in n_1 and n_2. This exponential reduction of parameters makes the numerical optimisation feasible. In fact, this optimisation problem is exactly a semidefinite programming optimisation. To show this we first briefly review the semidefinite programming and then we define the parameters in the program.
A general semidefinite program can be defined as any mathematical program of the form [Sin96]

$$\max_{X \in \mathbb{S}^n} \quad F_{n_1,n_2}(X) = \mathrm{Tr}[C^\intercal X] \tag{A.26}$$
$$\text{subject to} \quad \mathrm{Tr}\left[D_k^\intercal X\right] \geq b_k, \quad k = 1, .., m, \quad \text{and} \quad X \geq 0$$

where $\mathbb{S}^n$ is the space of all real $n \times n$ matrices. C and D_k are $n \times n$ real matrices, and b_k are real numbers and $X \geq 0$ means that X is semidefinite.
In our problem, $C^{j,j'}_{q,j_1}(p)$ are the matrix elements of C which are all real since $C^{j,j'}_{q,j_1}(p)$ is the combination of the Clebsch-Gordan coefficients. Our constraints are equality constraints, each of which can be obtained from two inequalities. The matrix elements of X are $W^{j,j'}_{q,j_1}$, and the elements of D_k and b_k can be read from the coefficients in Eq. (5.23) of the main text.
To prove that our problem is a semidifinite program we should show that X is positive-semidefinite. X is positive-semidefinite if and only if there exists a set of vectors like $\{v_i\}$ such that $x_{m,n} = v_m^{\intercal}.v_n$. In the definition of $W^{j,j'}_{q,g,g'}$ in Eq. (A.10), we have

$$W^{j,j'}_{q,g_{j_1},g_{j_1}} := \mathbf{v}^{j}_{q,g_{j_1}} \cdot (\mathbf{v}^{j'}_{q,g_{j_1}})^{\dagger}\,, \tag{A.27}$$

and using Eq. (A.24) we get

$$W^{j,j'}_{q,j_1,j_1} := \mathbf{v}^{j}_{q,j_1} \cdot (\mathbf{v}^{j'}_{q,j_1})^{\dagger}\,. \tag{A.28}$$

So, $X \geq 0$ and our problem is a semidefinite program.
Note that in our maximisation problem the parameters in general can be complex numbers. However, the matrix elements of C are the contraction of Clebsch-Gordan coefficients which are all real, therefore without loss of generality we can assume that $W^{j,j'}_{q,j_1}$ are real.

A.3 Derivation of Eq. (4.23)

Here we give explicit derivation of the constraint 5.23 of the main text. The starting point to observe that by explicit substitution of Eq. (13) into Eq. (14) of the main text we get

$$\sum_{s=\pm\frac{1}{2}} \sum_{q} C^{q\ \ \ s-m}_{\frac{1}{2}\,s,j\,-m} C^{q\ \ \ s-m}_{\frac{1}{2}\,s,j'\,-m}\ W^{j,j'}_{q,g,g'} = \delta_{j,j'}\delta_{g,g'}\,. \tag{A.29}$$

Using then the following symmetry property of Clebsch-Gordan coefficients

$$C^{JM}_{j_1\,m_1,j_2\,m_2} = (-1)^{j_1-m_1}\sqrt{\tfrac{2J+1}{2j_2+1}}C^{j_2-m_2}_{j_1\,m_1,J\,-M}\,, \tag{A.30}$$

we can observe that

$$\sum_{s=\pm\frac{1}{2}} C^{q\ \ \ s-m}_{\frac{1}{2}\,s,j\,-m} C^{q\ \ \ s-m}_{\frac{1}{2}\,s,j'\,-m} = \sum_{s=\pm\frac{1}{2}} \frac{2q+1}{2j+1} C^{j\ \ \ m}_{\frac{1}{2}\,s,q\,m-s} C^{j'\ \ \ m}_{\frac{1}{2}\,s,q\,m-s} = \frac{2q+1}{2j+1}\langle j,m|\,\Pi_m\,|j'm\rangle = \frac{2q+1}{2j+1}\delta_{j,j'} \tag{A.31}$$

where Π_m is the projector on the the $j_z = m$ eigenspace. It follows hence that (A.29) is automatically fulfilled for $j \neq j'$, while for $j = j'$ instead it gives Eq. 5.23 of the main text

$$\tfrac{2+2j}{1+2j}\, W^{j,j}_{q,g,g'}\Big|_{q=j+\frac{1}{2}} + \tfrac{2j}{1+2j}\, W^{j,j}_{q,g,g'}\Big|_{q=j-\frac{1}{2}} = \delta_{g,g'}\ . \tag{A.32}$$

Using the definition of $W^{j,j'}_{q,j_1} := \frac{1}{\# g_{j_1}} \sum_{g_{j_1}} W^{j,j'}_{q,g_{j_1},g_{j_1}}$ and summing the equations (A.32) we get

$$\tfrac{2+2j}{(1+2j)}\, W^{j,j}_{q,j_1}\Big|_{q=j+\frac{1}{2}} + \tfrac{2j}{1+2j}\, W^{j,j}_{q,j_1}\Big|_{q=j-\frac{1}{2}} = 1\ . \tag{A.33}$$

A.4 Application of the formalism to the case $n_1 = n_2 = 1$

For $n_1 = n_2 = 1$, Eq. (5.13) of the main text explicitly yields

$$\Omega_{1,1} = (1-p)\left|\uparrow\right\rangle\left\langle\uparrow\right| \otimes I/2 + pA_2. \tag{A.34}$$

Notice that the term A_2 is invariant under rotations hence it gets mapped by Λ_c into a multiple of the identity operator: specifically noticing that $\mathrm{Tr}[A_2] = 1$ we have $\Lambda_c[A_2] = \int d\mu_U\ U\Lambda[A_2]U^\dagger = I/2$ which implies $\left\langle\uparrow\right| \Lambda_c\big[A_2\big] \left|\uparrow\right\rangle = 1/2$. On the contrary the first contribution to $\Omega_{1,1}$ admits the following decomposition

$$\left|\uparrow\right\rangle\left\langle\uparrow\right| \otimes I = |1,1\rangle\langle 1,1| + \frac{|1,0\rangle + |0,0\rangle}{\sqrt{2}}\frac{\langle 1,0| + \langle 0,0|}{\sqrt{2}}\ , \tag{A.35}$$

where without loss of generality we identified $\left|\uparrow\right\rangle$ with the vector $|\frac{1}{2},\frac{1}{2}\rangle$, and where in the r.h.s. appear states of the total angular momentum basis of two spin $\frac{1}{2}$ (no multiplicity being present). Using Eq. (5.16) of the main text and the table of Clebsch-Gordan coefficients we can then write

$$\begin{aligned}\left\langle\uparrow\right| \Lambda_c\big[\left|\uparrow\right\rangle\left\langle\uparrow\right| \otimes I\big]\left|\uparrow\right\rangle &= \frac{2}{3}\Big|\mathbf{v}^1_{3/2}\Big|^2 + \frac{5}{6}\Big|\mathbf{v}^1_{1/2}\Big|^2 + \frac{1}{2}\Big|\mathbf{v}^0_{1/2}\Big|^2 \\ &\quad + \frac{1}{\sqrt{3}}\,\mathrm{Re}\Big\{\mathbf{v}^0_{1/2}\cdot(\mathbf{v}^1_{1/2})^\dagger\Big\}\ ,\end{aligned} \tag{A.36}$$

where we dropped the index g since here is no multiplicity in total angular momentum basis of two qubits. Similarly the constraints (5.23) of the main text becomes

$$\frac{4}{3}\Big|\mathbf{v}^1_{3/2}\Big|^2 + \frac{2}{3}\Big|\mathbf{v}^1_{1/2}\Big|^2 = 1, \quad 2\Big|\mathbf{v}^0_{1/2}\Big|^2 = 1\ . \tag{A.37}$$

Exploiting this we observe that fidelity of $F_{1,1}(\Lambda)$ for a generic map must fulfil the constraint

$$\begin{aligned}F_{1,1}(\Lambda) &\le \frac{p}{2} + \frac{1-p}{2}\Big[\frac{2}{3}\Big|\mathbf{v}^1_{3/2}\Big|^2 + \frac{5}{6}\Big|\mathbf{v}^1_{1/2}\Big|^2 + \frac{1}{2}\Big|\mathbf{v}^0_{1/2}\Big|^2 \\ &\quad + \frac{1}{\sqrt{3}}\Big|\mathbf{v}^0_{1/2}\Big|\Big|\mathbf{v}^1_{1/2}\Big|\Big] \le 1 - p/2\ ,\end{aligned} \tag{A.38}$$

the first inequality being obtained by forcing $\mathbf{v}^0_{1/2}$ and $\mathbf{v}^1_{1/2}$ to be collinear, while the second following directly from (A.37). By comparing this with the lower bound $F^{(\max)}_{n_1,n_2} \geq 1 - p(d-1)/d$ discussed in the main text for the qubit case (i.e. $d = 2$) this allows us to recover the identity (5.10) of the main text, i.e.

$$F^{(\max)}_{1,1} = 1 - p/2 \,, \tag{A.39}$$

the bound being achived by employing the DN strategy.

A.5 Details of the Calculation for $n_1 = 2, n_2 = 1$

Here we present detailed calculation to derive Eq. (18) of the main text. Using the Eq. (A.19) we can write the fidelity as

$$\begin{aligned} F_{2,1}(\Lambda) \;=\; & \tfrac{p^2}{2} + \tfrac{5(1-p)(3+5p)W^{3/2,3/2}_{2,1}+(1-p)(33+23p)W^{3/2,3/2}_{1,1}}{72} + \tfrac{p(1-p)W^{1/2,1/2}_{0,0}+5p(1-p)W^{1/2,1/2}_{1,0}}{12} \\ +\tfrac{(1-p)(3+p)W^{3/2,1/2}_{1,1}}{9\sqrt{2}} \; & +\tfrac{(6-p)(1-p)W^{1/2,1/2}_{1,1}+(1-p)(6-5p)W^{1/2,1/2}_{0,1}}{36} \,, \end{aligned} \tag{A.40}$$

using the definition of $W^{j,j'}_{q,j_1} := \frac{1}{\# g_{j_1}} \sum_{g_{j_1}} W^{j,j'}_{q,g_{j_1},g_{j_1}}$ and the definition of $W^{j,j'}_{q,g,g'}$ in Eq. (A.10) we can write

$$\begin{aligned} F_{2,1}(\Lambda) \;=\; & \tfrac{p^2}{2} + \tfrac{5(1-p)(3+5p)\left|\mathbf{v}^{3/2}_{2,1}\right|^2+(1-p)(33+23p)\left|\mathbf{v}^{3/2}_{1,1}\right|^2}{72} + \tfrac{p(1-p)\left|\mathbf{v}^{1/2}_{0,2}\right|^2+5p(1-p)\left|\mathbf{v}^{1/2}_{1,2}\right|^2}{12} + \tfrac{(1-p)(3+p)\left|\mathbf{v}^{3/2}_{1,1}\right|\left|\mathbf{v}^{1/2}_{1,1}\right|}{9\sqrt{2}} \\ & +\tfrac{(6-p)(1-p)\left|\mathbf{v}^{1/2}_{1,1}\right|^2+(1-p)(6-5p)\left|\mathbf{v}^{1/2}_{0,1}\right|^2}{36} \,, \end{aligned} \tag{A.41}$$

with constraints:

$$\tfrac{5\left|\mathbf{v}^{3/2}_{2,1}\right|^2+3\left|\mathbf{v}^{3/2}_{1,1}\right|^2}{4} = 1 \,, \qquad \tfrac{3\left|\mathbf{v}^{1/2}_{1,g}\right|^2+\left|\mathbf{v}^{1/2}_{0,g}\right|^2}{2} = 1 \,, \tag{A.42}$$

where $g = 1, 2$. Using the constraints we eliminate $\left|\mathbf{v}^{3/2}_{2,1}\right|, \left|\mathbf{v}^{1/2}_{0,2}\right|, \left|\mathbf{v}^{1/2}_{0,1}\right|$, Eq. (A.41) becomes

$$F_{2,1}(\Lambda) = \tfrac{3-2p(1-p)}{6} + \tfrac{p(1-p)\left|\mathbf{v}^{1/2}_{1,2}\right|^2}{6} + \tfrac{(1-p)(3+p)\left|\mathbf{v}^{3/2}_{1,1}\right|^2}{9} + \tfrac{(1-p)(3+p)\left|\mathbf{v}^{3/2}_{1,1}\right|\left|\mathbf{v}^{1/2}_{1,1}\right|}{9\sqrt{2}} - \tfrac{(1-p)(6-7p)\left|\mathbf{v}^{1/2}_{1,1}\right|^2}{18} \tag{A.43}$$

The coefficients of $\left|\mathbf{v}^{1/2}_{1,2}\right|, \left|\mathbf{v}^{3/2}_{1,1}\right|$ are positive everywhere, so to maximise the fidelity we put their maximum values $\left|\mathbf{v}^{1/2}_{1,2}\right|^2 = \frac{2}{3}, \left|\mathbf{v}^{3/2}_{1,1}\right|^2 = \frac{4}{3}$, obtaining

$$F_{2,1}(\Lambda) = \tfrac{51-4p(7-p)}{54} + \tfrac{\sqrt{2}(1-p)(3+p)\left|\mathbf{v}^{1/2}_{1,1}\right|}{9\sqrt{3}} - \tfrac{(1-p)(6-7p)\left|\mathbf{v}^{1/2}_{1,1}\right|^2}{18} \,. \tag{A.44}$$

This last expression has to be maximise with respect to $\left|\mathbf{v}_{1,1}^{1/2}\right|$ considering that, according to the constraint (A.42) such variable has to belong to the interval $[0, \sqrt{2/3}]$. For the case $p < \frac{6}{7}$ we take the derivative and put it equal to zero obtaining

$$\left|\mathbf{v}_{1,1}^{1/2}\right| = \frac{\sqrt{2}(3+p)}{\sqrt{3}(6-7p)} , \tag{A.45}$$

which belongs to the allowed interval only when $p < 3/8$. Accordingly for these values of p we can use Eq. (A.45) obtaining

$$F_{2,1}^{(\max)} = \frac{51-4p(7-p)}{54} + \frac{(1-p)(3+p)^2}{27(6-7p)} . \tag{A.46}$$

For the case $1 > p > 3/8$ (which incidentally also includes $1 > p > 6/7$), instead the maximum for (A.43) is always maximised for the maximum allowed value of $\left|\mathbf{v}_{1,1}^{1/2}\right|$, i.e. $\left|\mathbf{v}_{1,1}^{1/2}\right| = \sqrt{2/3}$ yielding

$$F_{2,1}^{(\max)} = \frac{(1-p)(51+23p)}{54} + \frac{p(1-p)}{3} + \frac{p^2}{2}, \tag{A.47}$$

which together with (A.46) gives us (18) of the main text.

A.6 Case $n_1 = 2$, $n_2 = \infty$

As we argued in the text,

$$F_{n_1,\infty}^{(\max)} = \max_{\Lambda\in\mathrm{CPTP}} \int d\mu_U \langle\psi| \Lambda[\rho_{\mathrm{mix}}^{\otimes n_1}(p)] |\psi\rangle = \max_{\Lambda\in\mathrm{CPTP}} \int d\mu_U \langle\psi| \Lambda[((1-p)|\psi\rangle\langle\psi| + p|\phi\rangle\langle\phi|)^{\otimes 2}] |\psi\rangle , \tag{A.48}$$

This equality is consistent since $F_{n_1,\infty}^{(\max)}$ does not depend on $|\phi\rangle$ by virtue of the invariance property of the Haar measure, and therefore one can set $|\phi\rangle = |0\rangle$ without loss of generality. In this case the optimal Λ is not covariant, since it depends on $|0\rangle\langle 0|$, but we can still find the maximum fidelity through the standard Kraus representation of Λ. For $n_2 = 2$, there is no need to distinguish between equivalent representations and the matrix elements $M_{s,j,m}^{(k)}$ of a set of Kraus operators for Λ, M_k, satisfy

$$\left\langle \tfrac{1}{2}, s\right| \Lambda[|j,m\rangle\langle j',m'|] \left|\tfrac{1}{2}, s'\right\rangle = \sum_k M_{s,j,m}^{(k)} \overline{M_{s',j',m'}^{(k)}} \tag{A.49}$$

$$\sum_{s=-1/2}^{1/2} \left\langle \tfrac{1}{2}, s\right| \Lambda[|j,m\rangle\langle j',m'|] \left|\tfrac{1}{2}, s\right\rangle = \sum_{s=-1/2}^{1/2} \sum_k M_{s,j,m}^{(k)} \overline{M_{s,j',m'}^{(k)}} = \delta_{j,j'}\delta_{m,m'}. \tag{A.50}$$

The integral in (A.48) can be written as

$$\int d\mu_U \langle\psi| \Lambda[((1-p)|\psi\rangle\langle\psi| + p|0\rangle\langle 0|)^{\otimes 2}]|\psi\rangle =$$

$$= \sum_{s,s',l,m,l',m'} \int d\mu_U \left\langle \tfrac{1}{2}, s\right| D^{\frac{1}{2}}_{\frac{1}{2},s}(U^\dagger)\Lambda[\rho^{\otimes 2}_{\text{mix}}(p)_{l,m,l',m'} \left|\tfrac{1}{2}, l\right\rangle\left\langle\tfrac{1}{2}, m\right| \otimes \left|\tfrac{1}{2}, l'\right\rangle\left\langle\tfrac{1}{2}, m'\right|] D^{\frac{1}{2}}_{s',\frac{1}{2}}(U)\left|\tfrac{1}{2}, s'\right\rangle,$$

$$= \sum_{s,s',l,m,l',m'} \int d\mu_U \rho^{\otimes 2}_{\text{mix}}(p)_{l,m,l',m'} D^{\frac{1}{2}}_{\frac{1}{2},s}(U^\dagger) D^{\frac{1}{2}}_{s',\frac{1}{2}}(U)\left(\sum_{k,j,j'} M^{(k)}_{s,j,l+m}\overline{M^{(k)}_{s',j',l'+m'}} C^{j,l+m}_{\frac{1}{2},l,\frac{1}{2},m} C^{j,l'+m'}_{\frac{1}{2},l',\frac{1}{2},m'}\right), \tag{A.51}$$

where

$$\rho^{\otimes 2}_{\text{mix}}(p)_{l,m,l',m'} = \left(D^{\frac{1}{2}}_{l,\frac{1}{2}}(U) D^{\frac{1}{2}}_{\frac{1}{2},m}(U^\dagger) + \delta_{l,\frac{1}{2}}\delta_{m,\frac{1}{2}}\right)\left(D^{\frac{1}{2}}_{l',\frac{1}{2}}(U) D^{\frac{1}{2}}_{\frac{1}{2},m'}(U^\dagger) + \delta_{l',\frac{1}{2}}\delta_{m',\frac{1}{2}}\right). \tag{A.52}$$

After performing the integrations the result is

$$\int d\mu_U \langle\psi| \Lambda[((1-p)|\psi\rangle\langle\psi| + p|0\rangle\langle 0|)^{\otimes 2}]|\psi\rangle =$$

$$= \frac{p(1-p)}{3}\Sigma_k|M^{(k)}_{-\frac{1}{2},0,0}|^2 + \frac{p(1-p)}{6}\Sigma_k|M^{(k)}_{\frac{1}{2},0,0}|^2 + \frac{8(1-p)-5(1-p)^2}{12}\Sigma_k|M^{(k)}_{\frac{1}{2},1,1}|^2 +$$

$$+ \frac{4(1-p)-3(1-p)^2}{12}\Sigma_k|M^{(k)}_{-\frac{1}{2},1,1}|^2 + \frac{(1-p)^2}{4}\Sigma_k|M^{(k)}_{-\frac{1}{2},1,-1}|^2 + \frac{(1-p)^2}{12}\Sigma_k|M^{(k)}_{\frac{1}{2},1,-1}|^2 +$$

$$+ \frac{(1-p)(1+p)}{6\sqrt{2}}\Sigma_k|M^{(k)}_{-\frac{1}{2},1,0}|^2 + \frac{1-p}{6}\Sigma_k|M^{(k)}_{\frac{1}{2},1,0}|^2 + \frac{p^2}{2}$$

$$+ \frac{(1-p)^2}{6\sqrt{2}}\Sigma_k \operatorname{Re}[M^{(k)}_{\frac{1}{2},1,0}\overline{M^{(k)}_{-\frac{1}{2},1,-1}}] + \frac{(1-p)(1+p)}{6\sqrt{2}}\Sigma_k \operatorname{Re}[M^{(k)}_{-\frac{1}{2},1,0}\overline{M^{(k)}_{\frac{1}{2},1,1}}]. \tag{A.53}$$

Using the constraints (5.23) and the positivity and magnitude of the coefficients most of the optimal parameter choices can be found:

$$\Sigma_k|M^{(k)}_{-\frac{1}{2},0,0}|^2 = 1, \qquad \Sigma_k|M^{(k)}_{\frac{1}{2},0,0}|^2 = 0, \qquad \Sigma_k|M^{(k)}_{\frac{1}{2},1,1}|^2 = 1,$$

$$\Sigma_k|M^{(k)}_{-\frac{1}{2},1,1}|^2 = 0, \qquad \Sigma_k|M^{(k)}_{-\frac{1}{2},1,-1}|^2 = 1, \qquad \Sigma_k|M^{(k)}_{\frac{1}{2},1,-1}|^2 = 0.$$

Moreover, using the Cauchy-Schwartz inequality

$$|\operatorname{Re}[M^{(k)}_{\frac{1}{2},1,0}\overline{M^{(k)}_{-\frac{1}{2},1,-1}}]| \leq \sqrt{\sum_k |M^{(k)}_{\frac{1}{2},1,0}|^2}\sqrt{\sum_k |M^{(k)}_{-\frac{1}{2},1,-1}|^2} = \sqrt{\sum_k |M^{(k)}_{\frac{1}{2},1,0}|^2}$$

$$|\operatorname{Re}[M^{(k)}_{-\frac{1}{2},1,0}\overline{M^{(k)}_{\frac{1}{2},1,1}}]| \leq \sqrt{\sum_k |M^{(k)}_{-\frac{1}{2},1,0}|^2}\sqrt{\sum_k |M^{(k)}_{\frac{1}{2},1,1}|^2} = \sqrt{1-\sum_k |M^{(k)}_{\frac{1}{2},1,0}|^2}, \tag{A.54}$$

one is left with the maximisation of a function of the variable $t := \sqrt{\sum_k |M^{(k)}_{\frac{1}{2},1,0}|^2}$:

$$\frac{(1-p)(1+p)}{6\sqrt{2}}(1-t^2) + \frac{1-p}{6}t^2 + \frac{(1-p)^2}{6\sqrt{2}}t + \frac{(1-p)(1+p)}{6\sqrt{2}}\sqrt{1-t^2}\,. \tag{A.55}$$

The solution and the maximal value of the fidelity can be analytically determined, but they are quite cumbersome and we do not report them: instead we present the numerical plot in Fig. 5.2 of the main text.

A.7 Upper Bound on Measurement and Prepare Protocols

We have already observed that in the limit of large n_1 and n_2, MP protocols allows for optimal average fidelity. But what happens for finite number of copies? To answer this question we introduce an upper bound on the average fidelity attainable with MP protocols. Indeed, invoking once more the fact that for characterizing optimal performances one can restrict the analysis to transformations which are symmetric under the permutation of the first n_1 qubits. Using Eq. (A.14), the associated fidelity can be written as

$$F_{n_1,n_2}(\Lambda^{\mathrm{MP}}) := \sum_{k=0}^{n_1}\binom{n_1}{k}(1-p)^k p^{n_1-k}\int d\mu_U \langle\psi|\,\Lambda^{\mathrm{MP}}(|\psi\rangle\langle\psi|^{\otimes k}\otimes A_{N-k})\,|\psi\rangle\,, \tag{A.56}$$

where now Λ^{MP} is the optimal MP channel. Then, we can get the following upper bound by using an optimal MP for each independent part of the whole state

$$\begin{aligned} F_{n_1,n_2}(\Lambda^{\mathrm{MP}}) \;&\leq\; \sum_{k=0}^{n_1}\binom{n_1}{k}(1-p)^k p^{n_1-k} \\ &\times \int d\mu_U \langle\psi|\,\Lambda^{\mathrm{MP}}_k(|\psi\rangle\langle\psi|^{\otimes k}\otimes A_{N-k})\,|\psi\rangle\,, \end{aligned} \tag{A.57}$$

where Λ^{MP}_k is the optimal MP choice for $|\psi\rangle\langle\psi|^{\otimes k}$. Using the known result for tomography of pure states [MP95] we can then derive the following inequality

$$F_{n_1,n_2}(\Lambda^{\mathrm{MP}}) \leq \;\; \textstyle\sum_{k=0}^{n_1}\binom{n_1}{k}\frac{k+1}{k+2}(1-p)^k p^{n_1-k}, \tag{A.58}$$

where $\frac{k+1}{k+2}$ is the average fidelity in the optimal tomography of $k \geq 0$ copies of a pure state. Notice that the right-hand-side quantity does not depend explicitly on n_2, and that for $n_1 = 2$ reduces to the function (19) of the main text which we reported in Fig. 5.1.

A.8 Performance of the Cirac, Ekert, Macchiavello (CEM) protocol as a subtracting machine

Here we show that a direct application of the method of Ref. [CEM99] to solve our problem for $n_1 = 2$ and arbitrary n_2 leads to the same average fidelity as the DN strategy, being hence sub-optimal for our purposes.

The method presented in Ref. [CEM99] does not assume the possibility of operating on the noise signal, therefore the average fidelity one can achieve in this case does not depend on n_2. For case $n_1 = 2$, it consists of two steps first performing an orthogonal measurement on the system that discriminate the completely symmetric from the anti-symmetric subspace of two qubits, and then tracing out on of the qubits. Adopting this procedure from Eq. (5.4) of the main text we get

$$F^{\text{CEM}}_{n_1=2} = \int d\mu_U d\mu_V \langle\psi| \Lambda^{\text{CEM}}[\rho^{\otimes 2}_{\text{mix}}(p)] |\psi\rangle \tag{A.59}$$

$$= \int d\mu_U d\mu_V \langle\psi| \Lambda^{\text{CEM}}[(1-p)^2 |\psi\rangle\langle\psi|^{\otimes 2} + p^2 |\phi\rangle\langle\phi|^{\otimes 2} + p(1-p)(|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| + |\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi|)] |\psi\rangle \ . \tag{A.60}$$

Taking the integral on ϕ and using the fact that the method [CEM99] is also covariant we can carry on the calculation

$$\begin{aligned} F^{\text{CEM}}_{n_1=2} &= (1-p)^2 + \frac{p^2}{2} + \int d\mu_U \langle\psi| \Lambda^{\text{CEM}}[p(1-p)(|\psi\rangle\langle\psi| \otimes \frac{I}{2} + \frac{I}{2} \otimes |\psi\rangle\langle\psi|)] |\psi\rangle \\ &= (1-p)^2 + \frac{p^2}{2} + \langle 0| \Lambda^{\text{CEM}}[p(1-p)(|0\rangle\langle 0| \otimes \frac{I}{2} + \frac{I}{2} \otimes |0\rangle\langle 0|)] |0\rangle = 1 - \frac{p}{2} \end{aligned} \tag{A.61}$$

where in the last inequality we use the fact that, as anticipated, Λ^{CEM} consists in performing the measurements on the symmetric and antisymmetric subspace. We notice hence that $F^{\text{CEM}}_{n_1=2}$ exactly coincides with the fidelity one would get by simply adopting the DN strategy, i.e. $F^{\text{CEM}}_{n_1=2} = F^{\text{DN}}_{n_1,n_2}$ which is clearly not optimal in our case.

Appendix B

Appendix of degradable extension: Gaussian channels

This chapter is organized as follows. First, we prove that the flagged extension of Gaussian additive noise defined in Eq. 7.4 is actually Gaussian, then in the next next section we show that is degradable. In the final section, we calculate the coherent information of additive Gaussian and extended attenuator noise noise defined in Eq. 7.4 and 7.16 respectively

B.1 Proof of Gaussianity of flagged additive Gaussian noise

In this section we review the class of Gaussian channels known as classical mixing channels, then show that flagged additive Gaussian noise is a classical mixing channel.

For any $n \times n$ square matrix $Y \geq 0$ with eigenvalues $\lambda_1, ..., \lambda_n$, let us indicate the support of Y as $S(Y)$, $\det_+ Y = \prod_{i:\lambda_i > 0} \lambda_i$, and pseudoinverse of Y as $Y^{\ominus 1}$. Classical mixing channels have the form:

$$\Lambda_Y[\hat{\rho}] := \int_{S(Y)} \mathrm{d}\mathbf{r} \frac{e^{-\mathbf{r}^\mathsf{T} Y^{\ominus 1} \mathbf{r}}}{\sqrt{\pi}^{\dim S(Y)} \sqrt{\det_+ Y}} \hat{D}_\mathbf{r} \hat{\rho} \hat{D}_\mathbf{r}^\dagger \; . \tag{B.1}$$

Channels of this type are Gaussian and the action on the first and second moments is

$$\bar{\mathbf{r}} \xrightarrow{\Lambda_Y} \bar{\mathbf{r}}' = \bar{\mathbf{r}} \; , \qquad \boldsymbol{\sigma} \xrightarrow{\Lambda_Y} V' = \boldsymbol{\sigma} + Y \; . \tag{B.2}$$

By direct comparison with Eq. 7.4 of the main text it follows that the flagged additive Gaussian noise of Λ_β^e is a classical mixing channel applied to the state $\hat{\rho} \otimes |\beta/2\rangle\langle\beta/2| \otimes$

$|\beta/2\rangle\langle\beta/2|$ with the matrix Y equal to

$$Y = \begin{pmatrix} \frac{2}{\beta} & 0 & 0 & 0 & 0 & -\frac{1}{\beta} \\ 0 & \frac{2}{\beta} & 0 & \frac{1}{\beta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\beta} & 0 & \frac{1}{2\beta} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ -\frac{1}{\beta} & 0 & 0 & 0 & 0 & \frac{1}{2\beta} \end{pmatrix} , \tag{B.3}$$

and thus Gaussian.

B.2 Degradability of flagged additive noise channel

Here we prove the degradability of the channel Λ^e_β. We define the unitary operator $\hat{U}^{(x)} : L_2(\mathbb{R}^2) \to L_2(\mathbb{R}^2)$

$$\hat{U}^{(x)} : \psi(x_1, x_2) \to \psi(x_1, x_2 + x_1) , \tag{B.4}$$

and $\hat{U}^{(p)} : L_2(\mathbb{R}^2) \to L_2(\mathbb{R}^2)$

$$\hat{U}^{(p)} : \psi(x_1, x_2) \to \psi(x_1, x_2) e^{-ix_1 x_2} . \tag{B.5}$$

We define the pure states of two modes $|C_1\rangle$ and $|C_2\rangle$ with wave functions respectively

$$\begin{aligned} \psi_{x,\beta}(x_1, x_2) &= \sqrt{\frac{\beta}{2\pi}} e^{-\beta \frac{x_1^2}{4} - i\frac{x_1 x_2}{2} - \beta\frac{x_2^2}{4}} , \\ \psi_{p,\beta}(x_1, x_2) &= \sqrt{\frac{\beta}{2\pi}} e^{-\beta \frac{x_1^2}{4} + i\frac{x_1 x_2}{2} - \beta\frac{x_2^2}{4}} . \end{aligned} \tag{B.6}$$

We also note that the wave function of a displaced squeezed state $\hat{D}_{(0,x)} |\beta\rangle$ with $x \in \mathbb{R}$ is

$$\psi_{\beta,x}(x') = \sqrt{\frac{\beta}{\pi}} e^{-\beta\frac{x'^2}{2} - ix'x} . \tag{B.7}$$

Note hence that

$$\begin{aligned} &\langle\psi|_A \otimes \langle C_1|_{XP'} \otimes \langle C_2|_{PX'} \hat{U}^{(x)\dagger}_{XA} \hat{U}^{(p)\dagger}_{PA} [f(x_X, x_P)] = \\ &= \sqrt{\frac{\beta}{2\pi}} \int_{\mathbb{R}^2} \mathrm{d}x_{X'} \mathrm{d}x_{P'} \langle\psi| \hat{D}^\dagger_{(x_X,0)} \hat{D}^\dagger_{(0,x_P)} \langle\beta/2|_{P'} \hat{D}^\dagger_{(0,x_X/2)} \langle\beta/2|_{X'} \hat{D}^\dagger_{(0,-x_P/2)} e^{-\frac{\beta}{4}(x_X^2 + x_P^2)} f(x_X, x_P) . \end{aligned} \tag{B.8}$$

It follows that

$$\Lambda^e_\beta[|\psi\rangle\langle\psi|] := \mathrm{Tr}_{XP}[\hat{U}^{(p)}_{PA}\hat{U}^{(x)}_{XA}\,|\psi\rangle\langle\psi|_A \otimes |C_1\rangle\langle C_1|_{XP'} \otimes |C_2\rangle\langle C_2|_{PX'}\, U^{(x)}_{XA}{}^\dagger U^{(p)}_{PA}{}^\dagger]$$
$$= \frac{\beta}{2\pi}\int_{\mathbb{R}^2} \mathrm{d}x_X \mathrm{d}x_P e^{-\frac{\beta}{2}(x_X^2+x_P^2)}\hat{D}_{(x_X,x_P)}\hat{\rho}\hat{D}^\dagger_{(x_X,x_P)}$$
$$\otimes \hat{D}_{(0,-x_P/2)}\,|\beta/2\rangle\langle\beta/2|_{X'}\,\hat{D}^\dagger_{(0,-x_P/2)} \otimes \hat{D}_{(0,x_X/2)}\,|\beta/2\rangle\langle\beta/2|_{P'}\,\hat{D}^\dagger_{(0,x_X/2)}\ .$$

The wave function of $U^{(p)}_{P'A}U^{(x)}_{X'A}U^{(p)}_{PA}U^{(x)}_{XA}\,|\psi\rangle_A \otimes |C_1\rangle_{XP'} \otimes |C_2\rangle_{PX'}$ is

$$\sqrt{\frac{\beta}{2\pi}}e^{-\beta\frac{x_X^2}{4}-i\frac{x_X x_{P'}}{2}-\beta\frac{x_{P'}^2}{4}}e^{-\beta\frac{x_P^2}{4}+i\frac{x_P x_{X'}}{2}-\beta\frac{x_{X'}^2}{4}}\psi(x_A+x_X+x_{X'})e^{i(x_A-x_{X'})x_P+ix_Ax_{P'}} \tag{B.9}$$

$$= \sqrt{\frac{\beta}{2\pi}}e^{-\beta\frac{x_X^2}{4}-i\frac{x_X x_{P'}}{2}-\beta\frac{x_{X'}^2}{4}}e^{-\beta\frac{x_P^2}{4}-i\frac{x_P x_{X'}}{2}-\beta\frac{x_{P'}^2}{4}}\psi(x_A+x_X+x_{X'})e^{ix_A(x_P+x_{P'})}\ . \tag{B.10}$$

Since this wave function is symmetric under exchange $X \leftrightarrow X'$, $P \leftrightarrow P'$, defining the map

$$W_{X'P'A\to X'P'}[\hat{\rho}] := \mathrm{Tr}_A[\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{\rho}_{X'P'A}\hat{U}^{(x)}_{X'A}{}^\dagger\hat{U}^{(p)}_{P'A}{}^\dagger]\ , \tag{B.11}$$

we have that

$$W_{X'P'A\to X'P'} \circ \Lambda_{\beta\, A\to X'P'A}[\rho] = \mathrm{Tr}_{XPA}[\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}$$
$$\hat{\rho}_A \otimes |C_1\rangle\langle C_1|_{XP'} \otimes |C_2\rangle\langle C_2|_{PX'}\,(\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A})^\dagger]$$
$$= \mathrm{Tr}_{X'P'A}[\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{\rho}_A \otimes |C_1\rangle\langle C_1|_{XP'} \otimes |C_2\rangle\langle C_2|_{PX'}\,(\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A}\hat{U}^{(p)}_{P'A}\hat{U}^{(x)}_{X'A})^\dagger] = \Lambda^{e,c}_{\beta\ \ A\to XP}[\hat{\rho}_A]\ . \tag{B.12}$$

Thus $\Lambda^{e,c}_\beta$ is degradable.

B.3 Computing the Coherent information of extended channels

In this section, we calculate the coherent information of the flagged additive Gaussian noise Λ^e_β (see Eq. 7.4) and the extended thermal attenuator $\mathcal{E}^e_{\eta,N}$ (see Eq. 7.16). The von Neumann entropy of a Gaussian state can be computed from its covariance matrix $\boldsymbol{\sigma}$. In particular, we need to compute the symplectic eigenvalues $\nu_1,...,\nu_n$ of $\boldsymbol{\sigma}$. In particular, these eigenvalues can be obtained from the eigenvalues of the matrix $i\Omega\boldsymbol{\sigma}$, which correspond to $\nu_1,-\nu_1,...,\nu_n,-\nu_n$. The Von Neumann entropy of a state $\hat{\rho}$ with covariance matrix $\boldsymbol{\sigma}$ is then

$$S(\hat{\rho}) = \sum_{i=1}^n h(\nu_n)\ , \tag{B.13}$$

with

$$h(x) := \tfrac{x+1}{2}\log_2\left(\tfrac{x+1}{2}\right) - \tfrac{x-1}{2}\log_2\left(\tfrac{x-1}{2}\right) \ . \tag{B.14}$$

For flagged additive Gaussian noise channel Λ^e_β and extended thermal attenuator $\mathcal{E}^e_{\eta,N}$, gaussian states maximize the coherent information since the channels are degradable and admit a Gaussian degrading map, satisfying the conditions of Theorem 4.4.2. The degrading map is explicitly Gaussian for the extended thermal attenuator; in the case of the flagged additive Gaussian noise the degrading map we present in the next section is not explicitly Gaussian, but its complementary is Gaussian. Since any Gaussian channel admit a Stinespring representation with a Gaussian unitary, there exists a Gaussian dilation of the complementary of the degrading map. By the properties of the Stinespring representation, the Stinespring dilation of the degrading map is isometric to a Gaussian isometry, with the connecting isometry acting trivially on the systems associated with the output of the complementary of the degrading map. This is enough to apply Theorem 4.4.2. An explicit Gaussian degrading map will be presented elsewhere.

If in addition the channel is gauge-covariant, the maximization can be restricted to gauge-invariant states 4.4.2. In our case, both the thermal attenuator and the flagged additive noise satisfy a generalized gauge-covariance property. Defining the Gaussian unitary on one mode $\hat{R}(\theta)$ acting on $\hat{\mathbf{r}} = (\hat{x}, \hat{p})$ as the rotation matrix $R(\theta) := \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$

$$\hat{R}(\theta)\hat{\mathbf{r}}\hat{R}(\theta)^\dagger = R(\theta)\hat{\mathbf{r}}, \tag{B.15}$$

we have

$$\Lambda^e_\beta[\hat{R}(\theta)\hat{\rho}\hat{R}(\theta)^\dagger] = \hat{R}'(\theta)\Lambda^e_\beta[\hat{\rho}]\hat{R}'(\theta)^\dagger, \tag{B.16}$$

with $\hat{R}'(\theta)$ being a three mode Gaussian unitary acting on $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \hat{x}_3, \hat{p}_3)$ as

$$\hat{R}'(\theta)\hat{\mathbf{r}}\hat{R}'(\theta)^\dagger = R'(\theta)\hat{\mathbf{r}}, \tag{B.17}$$

with

$$
R'(\theta) := \begin{pmatrix} \cos\theta & \sin\theta & 0 & 0 & 0 & 0 \\ -\sin\theta & \cos\theta & 0 & 0 & 0 & 0 \\ 0 & 0 & \cos\theta & 0 & \sin\theta & 0 \\ 0 & 0 & 0 & \cos\theta & 0 & \sin\theta \\ 0 & 0 & -\sin\theta & 0 & \cos\theta & 0 \\ 0 & 0 & 0 & -\sin\theta & 0 & \cos\theta \end{pmatrix}. \tag{B.18}
$$

In a similar way,

$$
\mathcal{E}^e_{\eta,N}[\hat{R}(\theta)\hat{\rho}\hat{R}(\theta)^\dagger] = \hat{R}''(\theta)\mathcal{E}^e_{\eta,N}[\hat{\rho}]\hat{R}''(\theta)^\dagger, \tag{B.19}
$$

with $\hat{R}''(\theta)$ being a two mode Gaussian unitary acting on $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2)$ as

$$
\hat{R}''(\theta)\hat{\mathbf{r}}\hat{R}''(\theta)^\dagger = R''(\theta)\hat{\mathbf{r}}, \tag{B.20}
$$

with

$$
R''(\theta) := \begin{pmatrix} \cos\theta & \sin\theta & 0 & 0 \\ -\sin\theta & \cos\theta & 0 & 0 \\ 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & \sin\theta & \cos\theta \end{pmatrix}. \tag{B.21}
$$

Adapting the argument in 4.4.2 for gauge-covariant channels, Eq. (B.16),(B.19), together with the concavity of the coherent information of degradable channels, imply that the maximum of the coherent information is attained on gauge-invariant Gaussian states, which coincides with thermal states for channels with one mode as input. Moreover, since $\Lambda^e_\beta \circ \hat{D}_{\mathbf{s}} = \hat{D}_{\mathbf{s}} \circ \Lambda^e_\beta$ and $\mathcal{E}^e_{\eta,N}\hat{D}_{\mathbf{s}} = \hat{D}_{\sqrt{\eta}\mathbf{s}} \circ \mathcal{E}^e_{\eta,N}$, by concavity and unitarily invariance of the coherent information we have that higher energy thermal states have higher coherent information.

Thus, to compute the coherent information of the flagged additive noise we have to find the covariance matrix $\boldsymbol{\sigma}_M$ of $\Lambda^e_\beta[\hat{\rho}_M]$ and the covariance matrix $\boldsymbol{\sigma}'_M$ of $(\Lambda^e_\beta \otimes \mathcal{I})[|\rho_M\rangle\rangle\langle\langle\rho_M|]$ where $\hat{\rho}_M$ is the thermal state with average photon number M and $|\rho_M\rangle\rangle$ is its purification, which can be taken to be the two-mode squeezed state $|\tau\rangle$ (see Eq. 4.25).

We obtain

$$\boldsymbol{\sigma}_M = \begin{pmatrix} 2M+1+\frac{2}{\beta} & 0 & 0 & 0 & 0 & -\frac{1}{\beta} \\ 0 & 2M+1+\frac{2}{\beta} & 0 & \frac{1}{\beta} & 0 & 0 \\ 0 & 0 & \frac{2}{\beta} & 0 & 0 & 0 \\ 0 & \frac{1}{\beta} & 0 & \frac{\beta}{2}+\frac{1}{2\beta} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{2}{\beta} & 0 \\ -\frac{1}{\beta} & 0 & 0 & 0 & 0 & \frac{\beta}{2}+\frac{1}{2\beta} \end{pmatrix} \tag{B.22}$$

$$\boldsymbol{\sigma}'_M = \begin{pmatrix} 2M+1+\frac{2}{\beta} & 0 & 0 & 0 & 0 & -\frac{1}{\beta} & 2\sqrt{M(M+1)} & 0 \\ 0 & 2M+1+\frac{2}{\beta} & 0 & \frac{1}{\beta} & 0 & 0 & 0 & -2\sqrt{M(M+1)} \\ 0 & 0 & \frac{2}{\beta} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\beta} & 0 & \frac{\beta}{2}+\frac{1}{2\beta} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{2}{\beta} & 0 & 0 & 0 \\ -\frac{1}{\beta} & 0 & 0 & 0 & 0 & \frac{\beta}{2}+\frac{1}{2\beta} & 0 & 0 \\ 2\sqrt{M(M+1)} & 0 & 0 & 0 & 0 & 0 & 2M+1 & 0 \\ 0 & -2\sqrt{M(M+1)} & 0 & 0 & 0 & 0 & 0 & 2M+1 \end{pmatrix} . \tag{B.23}$$

The eigenvalues of $i\Omega\boldsymbol{\sigma}_M$ are

$$\pm 2M + O(1), \qquad \pm\frac{\sqrt{1+\beta^2}}{\beta} + O(1/M)\,, \qquad \pm\frac{\sqrt{1+\beta^2}}{\beta} + O(1/M)\,, \tag{B.24}$$

while the eigenvalues if $i\Omega\boldsymbol{\sigma}'_M$ are

$$\pm 2\frac{1}{\beta^{1/2}}\sqrt{M} + O(1), \qquad \pm 2\frac{1}{\beta^{1/2}}\sqrt{M} + O(1)\,, \qquad \pm 1\,, \qquad \pm 1\,. \tag{B.25}$$

Therefore we have

$$Q(\Lambda^e_\beta) = \lim_{M\to\infty} S(\Lambda^e_\beta[\rho_M]) - S((\Lambda^e_\beta \otimes \mathcal{I})[|\tau\rangle\langle\tau|_M]) = \log_2\beta - 1/\log 2 + 2h\left(\frac{\sqrt{1+\beta^2}}{\beta}\right) . \tag{B.26}$$

To compute the coherent information of the extended thermal attenuator $\mathcal{E}^e_{\eta,N}$ we have to find the covariance matrix $\boldsymbol{\sigma}_M$ of $\mathcal{E}^e_{\eta,N}[\hat{\rho}_M]$ and the covariance matrix $\boldsymbol{\sigma}'_M$ of the complementary channel $\mathcal{E}^{e,c}_{\eta,N}[\hat{\rho}_M] = \mathcal{E}^e_{1-\eta,N}[\hat{\rho}_M]$ where $\hat{\rho}_M$ is again the thermal state with average photon number M. We obtain

$$\boldsymbol{\sigma}_M = \begin{pmatrix} \eta(2M+1)+(1-\eta)\eta(2N+1) & 0 & (1-\eta)2\sqrt{N(N+1)} & 0 \\ 0 & \eta(2M+1)+(1-\eta)(2N+1) & 0 & -(1-\eta)2\sqrt{N(N+1)} \\ (1-\eta)2\sqrt{N(N+1)} & 0 & \eta+(1-\eta)(2N+1) & 0 \\ 0 & -(1-\eta)2\sqrt{N(N+1)} & 0 & \eta+(1-\eta)(2N+1) \end{pmatrix} . \tag{B.27}$$

while $\boldsymbol{\sigma}'_M$ is obtained from the above expression by exchanging $\eta \to 1-\eta$. The eigenvalues if $i\Omega\boldsymbol{\sigma}_M$ are hence

$$\pm\eta M + O(1), \qquad \pm(\eta + (1-\eta)(2N+1)) + O(1/M)\ , \tag{B.28}$$

while the eigenvalues if $i\Omega\boldsymbol{\sigma}'_M$ are

$$\pm(1-\eta)M + O(1), \qquad \pm((1-\eta) + \eta(2N+1)) + O(1/M)\ . \tag{B.29}$$

Therefore we have

$$\begin{aligned} Q(\mathcal{E}^e_{\eta,N}) &= \lim_{M\to\infty} S(\mathcal{E}^e_{\eta,N}[\hat\rho_M]) - S(\mathcal{E}^e_{1-\eta,N}[\hat\rho_M]) \\ &= -\log_2\left(\tfrac{\eta}{1-\eta}\right) + h(\eta + (1-\eta)(2N+1)) - h((1-\eta) + \eta(2N+1))\ . \end{aligned}$$

Appendix C

Appendix of degradable extension: Gaussian channels

This chapter is organized as follows. First, we present the calculations for the evaluation of $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ and $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$. Then, we apply the decomposition rules technique to the zero capacity region. Finally, we show that the lower bounds are stable under the symmetry imposed by the decomposition rules.

C.1 Evaluation of $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ and $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$

Evaluation of $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$*:–* It goes without mentioning that by construction this term is guaranteed to be not larger than $Q^{\rm att}_{\rm FKG}(\eta, N)$ (indeed $Q^{\rm att}_{\rm FKG}(\eta', N_1)$ reach this value on **C2** for $\eta' = \eta$ and $N_1 = N$). Observe now that the first equation of **C2** can be casted in the equivalent form

$$(g-1)(N_2+N_1+1) = (1-\eta)(N-N_1) \; , \qquad \text{(C.1)}$$

which shows that in order to guarantee that $g \geq 1$ imposes to focus only on the domain $N_1 \leq N$ (hence from now on we only focus on this regime). Notice also that expressing g in terms of η' we can rewrite the above constraint as

$$\eta' = \eta \frac{N_2+1+N_1}{N_2+1+\eta N_1+(1-\eta)N} = \eta\left(1-\frac{(1-\eta)(N-N_1)}{N_2+1+\eta N_1+(1-\eta)N}\right) \; , \qquad \text{(C.2)}$$

which by construction ensures that $\eta' \leq \eta$ (and $\eta' \geq 0$). Notice then that for fixed N the function $Q^{\rm att}_{\rm FKG}(\eta, N)$ is increasing in η and nullifies for $\eta = 1/2$ (being negative for $\eta < 1/2$ and positive otherwise). Therefore, for fixed $N_1 \leq N$, the minimum value of

$Q^{\rm att}_{\rm FKG}(\eta', N_1)$ on **C2** is always attained by using as N_2 the value that minimize η', i.e. $N_2 = 0$ (remember that we are bound to use $N_2 \geq 0$), obtaining

$$\eta'_{opt}(N_1) := \eta \frac{1+N_1}{1+\eta N_1 + (1-\eta)N} \ . \tag{C.3}$$

Hence we can now write

$$Q^{\rm att}_{\rm FKG}(\mathbf{C2}) := \min_{N_1 \in [0,N]} Q^{\rm att}_{\rm FKG}(\eta'_{opt}(N_1), N_1) \ . \tag{C.4}$$

This is a single letter formula that we can try to compute analytically. By plotting the function $Q^{\rm att}_{\rm FKG}(\eta'_{opt}(N_1), N_1)$ in terms of N_1 for fixed values of η and N we observe that it has two possible behaviours: either is increasing in N_1 (this happens for instance for high values of η) or it is decreasing (this happens typically for lower values of η). Accordingly we can conclude that the minimum over N_1 is obtained at the extreme of its domain, i.e either for $N_1 = N$ or for $N_1 = 0$. In the first case we get $\eta'_{opt}(N_1 = N) = \eta$ so that $Q^{\rm att}_{\rm FKG}(\eta'_{opt}(N_1), N_1)$ reduces to the old bound $Q^{\rm att}_{\rm FKG}(\eta, N)$. In the second case instead we get $\eta'_{opt}(N_1 = 0) = \eta/(1 + (1-\eta)N)$ which leads to

$$Q^{\rm att}_{\rm FKG}(\eta'_{opt}(N_1 = 0), N_1 = 0) = \bar{Q}^{\rm att}_{\rm FKG}(\eta, N) := \max\left\{0, \log_2 \frac{\eta}{(1-\eta)(N+1)}\right\} \ . \tag{C.5}$$

Accordingly we can claim

$$Q^{\rm att}_{\rm FKG}(\mathbf{C2}) := \min\left\{\bar{Q}^{\rm att}_{\rm FKG}(\eta, N), Q^{\rm att}_{\rm FKG}(\eta, N)\right\} \ . \tag{C.6}$$

It turns out that there are indeed values of η and N for which $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ is an improvement with respect to $Q^{\rm att}_{\rm FKG}(\eta, N)$ (and also with respect to PLOB). Unfortunately however $\bar{Q}^{\rm att}_{\rm FKG}(\eta, N)$ is always less performant than the one in RMG!! Observe also that from above expression it follows that $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ (and hence $Q(\mathcal{E}_{\eta,N})$) is identically null for

$$\frac{\eta}{(1-\eta)(N+1)} = 1 \quad \Longleftrightarrow \quad N = \frac{2\eta - 1}{1-\eta} \ , \tag{C.7}$$

(remember that on our analysis we can restrict ourselves to the case $\eta > 1/2$ – see footnote 1 in the previous pages). Exploiting then the fact that $Q(\mathcal{E}_{\eta,N})$ is not decreasing in η, this can also be used to show

$$Q(\mathcal{E}_{\eta,N}) = 0 \qquad \text{for } N \geq \tfrac{2\eta-1}{1-\eta} \ . \tag{C.8}$$

Remark: *the bound $\bar{Q}^{\rm att}_{\rm FKG}(\eta, N)$ is always less performant than the one in RMG!!! Therefore we can exclude that $Q^{\rm att}_{\rm FKG}(\mathbf{C2})$ does not buy nothing new to the analysis. In particular we notice that the zero capacity condition imposed by RMG reads*

$$Q(\mathcal{E}_{\eta,N}) = 0 \qquad \textit{for } N \geq \tfrac{2\eta-1}{2(1-\eta)} \ , \tag{C.9}$$

which implies (C.8) that is therefore a weaker result.

Evaluation of $Q^{\rm amp}_{\rm FKG}(\mathbf{C2})$*:–* As in the previous case we can restrict the analysis to $N_1 \in [0, N]$ and $\eta' \in [0, \eta]$ (the other regimes being incompatible with the constraint). From (C.10) we get

$$\begin{aligned} \kappa &= (g-1)N_2 = \frac{(1-\eta)(N-N_1)N_2}{N_2+N_1+1} \\ &= (1-\eta)(N-N_1)\left(1-\frac{N_1+1}{N_2+N_1+1}\right) , \end{aligned} \tag{C.10}$$

so that

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C2}) = \min_{\mathbf{C2}} Q^{\rm amp}_{\rm FKG}\left(\frac{(1-\eta)(N-N_1)N_2}{N_2+N_1+1}\right) . \tag{C.11}$$

Notice that for fixed η, N, κ is always upper bounded by

$$\kappa \le \kappa_{max} = (1-\eta)N , \tag{C.12}$$

a value that we can always attain setting $N_1 = 0$ and taking the limit $N_2 \to \infty$, $g \to 1$ while forcing $(g-1)N_2 = (1-\eta)N$.
Again for the regime in which the capacity is potentially positive i.e. $N \le \frac{2\eta-1}{2(1-\eta)}$, one can show that $(1-\eta)N < \kappa_0$. Therefore in this regime, $Q^{\rm amp}_{\rm FKG}$ reaches its minimum value in κ_{max} and we write

$$Q^{\rm amp}_{\rm FKG}(\mathbf{C2}) \;=\; Q^{\rm amp}_{\rm FKG}((1-\eta)N) \tag{C.13}$$

Remark: *this appears to be a good bound but we shall see that* $Q^{\rm amp}_{\rm FKG}(\mathbf{C1})$ *is an improvement of it.*

C.2 Zero capacity region

First of all given R an arbitrary region in the parameter space we define its extension $\bar{R}$ as the set

$$\bar{R} = \{(\eta', N') : \exists(\eta, N) \in R \quad \text{s.t.} \quad (\eta', N') \in R_{\eta,N}\} . \tag{C.14}$$

Of course since $(\eta, N) \in R_{\eta,N}$ it follows that $R \subseteq \bar{R}$; in case $\bar{R} = R$ we say that R is *stable.*

Now let R_0 a set of the parameter space where we know for sure that the capacity Q is zero:

$$Q(\mathcal{E}_{\eta,N}) = 0 \qquad \forall(\eta, N) \in R_0 \ . \tag{C.15}$$

Then by construction it follows that the capacity also nullifies on the extension of R_0, i.e.

$$Q(\mathcal{E}_{\eta,N}) = 0 \qquad \forall(\eta, N) \in \bar{R}_0 \ . \tag{C.16}$$

From the above definition we can then conclude that if $R_0^{\max}$ is the largest zero-capacity region of the problem, i.e. $Q(\mathcal{E}_{\eta,N}) = 0$, if and only if $(\eta, N) \in R_0^{\max}$, then $R_0^{\max}$ has to be stable (i.e. $R_0^{\max} = \bar{R}_0^{\max}$). In other words, a necessary condition for a set to be the largest zero-capacity region is to be stable; it turns out that the zero-capacity region identified by the RMG bound (i.e. the set $R_{0.5,0}^{(amp)}$) fulfils such condition: it is hence a good candidate for $R_0^{\max}$. Unfortunately this is not the only one: as a matter of fact another good candidate for $R_0^{\max}$ is the region one identifies if the q-capacity is not superadditive and Gaussian optimize. Suppose in fact that $Q(\mathcal{E}_{\eta,N})$ is not super-additive and it is optimized over Gaussian inputs. Then we can write

$$\begin{gathered} Q(\mathcal{E}_{\eta,N}) = Q_1^{(\mathrm{gaus})}(\mathcal{E}_{\eta,N}) := \\ \max\left\{0, \log_2(\frac{\eta}{1-\eta}) - h(2N+1)\right\} \ , \end{gathered} \tag{C.17}$$

with $Q_1^{(\mathrm{gaus})}(\mathcal{E}_{\eta,N})$ the maximal single-use coherent information computed on Gaussian inputs. Accordingly for $\eta \geq 0.5$ the zero-capacity region will be hence associated with points (η, N) such that

$$\log_2(\frac{\eta}{1-\eta}) \leq h(2N+1) \ , \tag{C.18}$$

that is the region with

$$\eta \leq \frac{1}{1 + e^{-h(2N+1)\log 2}} \ . \tag{C.19}$$

If this is correct then this region must be stable, i.e. for all (η, N) fullfiling (C.19) we must have

$$\eta' \leq \frac{1}{1 + e^{-h(2N'+1)\log 2}} \qquad \forall(\eta', N') \in R_{\eta,N} \ , \tag{C.20}$$

or equivalently we must have that the following equations holds true

$$\eta' \leq \frac{1}{1 + e^{-h(2N_{\eta,N}^{(att)}(\eta')+1)\log 2}} \ \forall(\eta', N') \in R_{\eta,N} \ , \tag{C.21}$$

$$\eta' \leq \frac{1}{1 + e^{-h(2N_{\eta,N}^{(amp)}(\eta')+1)\log 2}} \ \forall(\eta', N') \in R_{\eta,N} \ . \tag{C.22}$$

It turns out that these identities are indeed both satisfied.

C.3 The stability of the lower bounds

Analogous considerations apply to lower bounds as well. Remember that the quantum capacity is known for $N = 0$, i.e.

$$Q(\mathcal{E}_{\eta,0}) = Q_1(\mathcal{E}_{\eta,0}) = \max\left\{0, \log_2(\frac{\eta}{1-\eta})\right\} , \tag{C.23}$$

which for $\eta \geq 1/2$ is a monotonically increasing function. Remember also that for (η, N) generic we can write

$$Q(\mathcal{E}_{\eta,N}) \geq Q_{\text{low}}^{\text{att}}(\eta, N) := \max\left\{0, \log_2(\frac{\eta}{1-\eta}) - h(2N+1)\right\} . \tag{C.24}$$

Now for fixed η let us consider the point on the curve

$$\mathcal{C}_\eta := \left\{(\eta', N') : \eta' \geq \eta, N' = N_{\eta,N=0}^{(amp)}(\eta'))\right\} , \tag{C.25}$$

with

$$N_{\eta,0}^{(amp)}(\eta') := \frac{\eta' - \eta}{1 - \eta'} . \tag{C.26}$$

Using the monotonicity property of corollary 8.5.1 we can claim that

$$Q(\mathcal{E}_{\eta,0}) \geq Q(\mathcal{E}_{\eta',N'}) \geq Q_{\text{low}}^{\text{att}}(\eta', N') , \qquad \forall (\eta', N') \in \mathcal{C}_\eta , \tag{C.27}$$

where in the last inequality we employed (C.24). Unfortunately the above inequality doesn't buy you anything since it is always fulfilled.

Bibliography

[AC97] C. Adami and N. J. Cerf. "von Neumann capacity of noisy quantum channels". In: *Physical Review A* 56.5 (1997), pp. 3470–3483. DOI: 10.1103/PhysRevA.56.3470. arXiv: quant-ph/9609024 [quant-ph].

[App05] D. M. Appleby. "Symmetric informationally complete–positive operator valued measures and the extended Clifford group". In: *Journal of Mathematical Physics* 46.5 (2005), p. 052107. DOI: 10.1063/1.1896384. arXiv: quant-ph/0412001 [arXiv:quant-ph].

[AR+15] U. Alvarez-Rodriguez, M. Sanz, L. Lamata, and E. Solano. "The Forbidden Quantum Adder". In: *Scientific Reports* 5.1 (2015). DOI: 10.1038/srep11983.

[ARL14] Gerardo Adesso, Sammy Ragy, and Antony R. Lee. "Continuous Variable Quantum Information: Gaussian States and Beyond". In: *Open Systems and Information Dynamics* 21.01n02 (2014), p. 1440001. DOI: 10.1142/s1230161214400010.

[BB14a] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560 (2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

[BB14b] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theor. Comput. Sci.* 560.P1 (2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025. arXiv: arXiv:2003.06557.

[Ben+02] 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". In: *IEEE Transactions on Information Theory* 48.10 (2002), pp. 2637–2655. DOI: 10.1109/TIT.2002.802612. arXiv: quant-ph/0106052 [quant-ph].

[Ben+96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. "Mixed-state entanglement and quantum error correction". In: *Physical Review A* 54.5 (1996), pp. 3824–3851. DOI: 10.1103/PhysRevA.54.3824. arXiv: quant-ph/9604024 [quant-ph].

[Ben+99] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. "Entanglement-Assisted Classical Capacity of Noisy Quantum Channels". In: *Physical Review Letters* 83.15 (1999), pp. 3081–3084. DOI: `10.1103/PhysRevLett.83.3081`. arXiv: `quant-ph/9904023 [quant-ph]`.

[BH96] V. Buzek and M. Hillery. "Quantum copying: Beyond the no-cloning theorem". In: *Phys. Rev. A* 54 (3 1996), pp. 1844–1852. DOI: `10.1103/PhysRevA.54.1844`.

[Bia+17] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. "Quantum machine learning". In: *Nature* 549.7671 (2017), pp. 195–202. DOI: `10.1038/nature23474`.

[BKN00] H. Barnum, E. Knill, and M.A. Nielsen. "On quantum fidelities and channel capacities". In: *IEEE Transactions on Information Theory* 46.4 (2000), pp. 1317–1329. DOI: `10.1109/18.850671`. arXiv: `quant-ph/9809010 [quant-ph]`.

[BL20] Johannes Bausch and Felix Leditzky. "Quantum codes from neural networks". In: *New Journal of Physics* 22.2 (2020), p. 023005. DOI: `10.1088/1367-2630/ab6cdd`. arXiv: `1806.08781`.

[BL21] Johannes Bausch and Felix Leditzky. "Error Thresholds for Arbitrary Pauli Noise". In: *SIAM Journal on Computing* 50.4 (2021), pp. 1410–1460. DOI: `10.1137/20m1337375`.

[Boi+08] J.-C. Boileau, L. Sheridan, M. Laforest, and S. D. Bartlett. "Quantum reference frames and the classification of rotationally invariant maps". In: *Journal of Mathematical Physics* 49.3 (2008), p. 032105. DOI: `10.1063/1.2884583`.

[BRS07] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. "Reference frames, superselection rules, and quantum information". In: *Rev. Mod. Phys.* 79 (2 2007), pp. 555–609. DOI: `10.1103/RevModPhys.79.555`.

[Bru+98] Dagmar Bruß, David P. DiVincenzo, Artur Ekert, Christopher A. Fuchs, Chiara Macchiavello, and John A. Smolin. "Optimal universal and state-dependent quantum cloning". In: *Physical Review A* 57.4 (1998), pp. 2368–2378. DOI: `10.1103/PhysRevA.57.2368`. arXiv: `quant-ph/9705038 [quant-ph]`.

[CB08] Luca Chirolli and Guido Burkard. "Decoherence in solid-state qubits". In: *Advances in Physics* 57.3 (2008), pp. 225–285. DOI: `10.1080/00018730802218067`. arXiv: `0809.4716`.

[CD94] Carlton M. Caves and P. D. Drummond. "Quantum limits on bosonic communication rates". In: *Reviews of Modern Physics* 66.2 (1994), pp. 481–537. DOI: `10.1103/RevModPhys.66.481`.

[CEM99] J. I. Cirac, A. K. Ekert, and C. Macchiavello. "Optimal Purification of Single Qubits". In: *Phys. Rev. Lett.* 82 (21 1999), pp. 4344–4347. DOI: 10.1103/PhysRevLett.82.4344.

[Cer00] Nicolas J. Cerf. "Pauli Cloning of a Quantum Bit". In: *Physical Review Letters* 84.19 (2000), pp. 4497–4500. DOI: 10.1103/PhysRevLett.84.4497. arXiv: quant-ph/9803058 [quant-ph].

[CG06] Filippo Caruso and Vittorio Giovannetti. "Degradability of Bosonic Gaussian channels". In: *Physical Review A* 74.6 (2006), p. 062307. DOI: 10.1103/PhysRevA.74.062307. arXiv: quant-ph/0603257 [quant-ph].

[CG21a] Stefano Chessa and Vittorio Giovannetti. "Partially Coherent Direct Sum Channels". In: *Quantum* 5 (2021), p. 504. DOI: 10.22331/q-2021-07-15-504.

[CG21b] Stefano Chessa and Vittorio Giovannetti. "Quantum capacity analysis of multi-level amplitude damping channels". In: *Communications Physics* 4.1 (2021). DOI: 10.1038/s42005-021-00524-4.

[CGH06] F Caruso, V Giovannetti, and A S Holevo. "One-mode bosonic Gaussian channels: a full weak-degradability classification". In: *New Journal of Physics* 8.12 (2006), pp. 310–310. DOI: 10.1088/1367-2630/8/12/310. arXiv: quant-ph/0609013 [quant-ph].

[CRS08] Toby S. Cubitt, Mary Beth Ruskai, and Graeme Smith. "The structure of degradable quantum channels". In: *Journal of Mathematical Physics* 49.10 (2008), p. 102104. DOI: 10.1063/1.2953685. arXiv: 0802.1360.

[Cub+15] Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. "Unbounded number of channel uses may be required to detect quantum capacity". In: *Nature Communications* 6.1 (2015), p. 6739. DOI: 10.1038/ncomms7739. arXiv: 1408.5115.

[CWY04] N. Cai, A. Winter, and R. W. Yeung. "Quantum privacy and quantum wiretap channels". In: *Problems of Information Transmission* 40.4 (2004), pp. 318–336. DOI: 10.1007/s11122-005-0002-x.

[DB17] Vedran Dunjko and Hans J. Briegel. "Machine learning and artificial intelligence in the quantum domain". In: (2017). DOI: 10.48550/ARXIV.1709.02779.

[dBe13] Niel de Beaudrap. "A linearized stabilizer formalism for systems of finite dimension". In: *Quantum Information and Computation* 13.1-2 (2013), pp. 0073–0115. DOI: 10.26421/qic13.1-2-6. arXiv: 1102.3354.

[Dev05] Igor Devetak. "The Private Classical Capacity and Quantum Capacity of a Quantum Channel". In: *IEEE Transactions on Information Theory* 51.1 (2005), pp. 44–55. DOI: 10.1109/TIT.2004.839515. arXiv: quant-ph/0304127 [quant-ph].

[DHW04] Igor Devetak, Aram W. Harrow, and Andreas Winter. "A Family of Quantum Protocols". In: *Physical Review Letters* 93.23 (2004), p. 230504. DOI: 10.1103/PhysRevLett.93.230504. arXiv: quant-ph/0308044 [quant-ph].

[Die82] D. Dieks. "Communication by EPR devices". In: *Physics Letters A* 92.6 (1982), pp. 271–272. DOI: https://doi.org/10.1016/0375-9601(82)90084-6.

[DKK17] Mina Doosti, Farzad Kianvash, and Vahid Karimipour. "Universal superposition of orthogonal states". In: *Phys. Rev. A* 96 (5 2017), p. 052318. DOI: 10.1103/PhysRevA.96.052318.

[Dog+18] Shruti Dogra, George Thomas, Sibasish Ghosh, and Dieter Suter. "Superposing pure quantum states with partial prior information". In: *Phys. Rev. A* 97 (5 2018), p. 052330. DOI: 10.1103/PhysRevA.97.052330.

[DS05] I. Devetak and P. W. Shor. "The Capacity of a Quantum Channel for Simultaneous Transmission of Classical and Quantum Information". In: *Communications in Mathematical Physics* 256.2 (2005), pp. 287–303. DOI: 10.1007/s00220-005-1317-6. arXiv: quant-ph/0311131 [quant-ph].

[DSS98] David P. DiVincenzo, Peter W. Shor, and John A. Smolin. "Quantum-channel capacity of very noisy channels". In: *Physical Review A* 57.2 (1998), pp. 830–839. DOI: 10.1103/PhysRevA.57.830. arXiv: quant-ph/9706061 [quant-ph].

[ES15] David Elkouss and Sergii Strelchuk. "Superadditivity of Private Information for Any Number of Uses of the Channel". In: *Physical Review Letters* 115.4 (2015), p. 040501. DOI: 10.1103/PhysRevLett.115.040501. arXiv: 1502.05326.

[FH04] William Fulton and Joe Harris. *Representation theory: a first course.* Springer New York, NY, 2004.

[FKG20] Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Quantum Flags and New Bounds on the Quantum Capacity of the Depolarizing Channel". In: *Physical Review Letters* 125.2 (2020), p. 020503. DOI: 10.1103/PhysRevLett.125.020503. arXiv: 1911.01977.

[FKG21] Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. "Estimating Quantum and Private Capacities of Gaussian Channels via Degradable Extensions". In: *Phys. Rev. Lett.* 127 (21 2021), p. 210501. DOI: 10.1103/PhysRevLett.127.210501.

[FW08] Jesse Fern and K. Birgitta Whaley. "Lower bounds on the nonzero capacity of Pauli channels". In: *Physical Review A* 78.6 (2008), p. 062335. DOI: 10.1103/PhysRevA.78.062335. arXiv: 0708.1597.

[GB14] Michael Grant and Stephen Boyd. *CVX Matlab Software for Disciplined Convex Programming, version 2.1.* 2014.

[GE08] D. Gross and J. Eisert. "Quantum margulis expanders". In: *Quantum Information and Computation* 8.8-9 (2008), pp. 0722–0733. DOI: 10.26421/qic8.8-9-3. arXiv: 0710.0651.

[GF05] Vittorio Giovannetti and Rosario Fazio. "Information-capacity description of spin-chain correlations". In: *Physical Review A* 71.3 (2005), p. 032314. DOI: 10.1103/PhysRevA.71.032314. arXiv: quant-ph/0405110 [quant-ph].

[GHGP15] V. Giovannetti, A. S. Holevo, and R. García-Patrón. "A Solution of Gaussian Optimizer Conjecture for Quantum Channels". In: *Communications in Mathematical Physics* 334.3 (2015), pp. 1553–1571. DOI: 10.1007/s00220-014-2150-6. arXiv: arXiv:1312.2251.

[Gio+04] 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". In: *Physical Review Letters* 92.2 (2004), p. 027902. DOI: 10.1103/PhysRevLett.92.027902. arXiv: quant-ph/0308012 [quant-ph].

[Gio+14] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo. "Ultimate classical communication rates of quantum optical channels". In: *Nature Photonics* 8.10 (2014), pp. 796–800. DOI: 10.1038/nphoton.2014.216.

[GJL18a] Li Gao, Marius Junge, and Nicholas LaRacuente. "Capacity bounds via operator space methods". In: *Journal of Mathematical Physics* 59.12 (2018), p. 122202. DOI: 10.1063/1.5058692. arXiv: arXiv:1509.07294.

[GJL18b] Li Gao, Marius Junge, and Nicholas LaRacuente. "Capacity Estimates via Comparison with TRO Channels". In: *Communications in Mathematical Physics* 364.1 (2018), pp. 83–121. DOI: 10.1007/s00220-018-3249-y.

[GM97] N. Gisin and S. Massar. "Optimal Quantum Cloning Machines". In: *Phys. Rev. Lett.* 79 (11 1997), pp. 2153–2156. DOI: 10.1103/PhysRevLett.79.2153.

[GNW21] David Gross, Sepehr Nezami, and Michael Walter. "Schur–Weyl Duality for the Clifford Group with Applications: Property Testing, a Robust Hudson Theorem, and de Finetti Representations". In: *Communications in Mathematical Physics* 385.3 (2021), pp. 1325–1393. DOI: 10.1007/s00220-021-04118-7. arXiv: 1712.08628.

[GP+09] Raúl García-Patrón, Stefano Pirandola, Seth Lloyd, and Jeffrey H. Shapiro. "Reverse coherent information". In: *Physical Review Letters* 102.21 (2009). DOI: 10.1103/PhysRevLett.102.210501. arXiv: arXiv:0808.0210.

[Gro06] D. Gross. "Hudson's theorem for finite-dimensional quantum systems". In: *Journal of Mathematical Physics* 47.12 (2006), p. 122107. DOI: 10.1063/1.2393152. arXiv: quant-ph/0602001 [arXiv:quant-ph].

[GS08] Gilad Gour and Robert W Spekkens. "The resource theory of quantum reference frames: manipulations and monotones". In: *New Journal of Physics* 10.3 (2008), p. 033023. DOI: 10.1088/1367-2630/10/3/033023.

[GT07] Nicolas Gisin and Rob Thew. "Quantum communication". In: *Nature Photonics* 1.3 (2007), pp. 165–171. DOI: 10.1038/nphoton.2007.22.

[Has09] M. B. Hastings. "Superadditivity of communication capacity using entangled inputs". In: *Nature Physics* 5.4 (2009), pp. 255–257. DOI: 10.1038/nphys1224. arXiv: 0809.3972.

[Hay+21] Patrick Hayden, Sepehr Nezami, Sandu Popescu, and Grant Salton. "Error Correction of Quantum Reference Frame Information". In: *PRX Quantum* 2.1 (2021). DOI: 10.1103/prxquantum.2.010326.

[HG12] A. S. Holevo and V. Giovannetti. "Quantum channels and their entropic characteristics". In: *Reports on Progress in Physics* 75.4 (2012), p. 046001. DOI: 10.1088/0034-4885/75/4/046001.

[HHH98] Pawel Horodecki, Michal Horodecki, and Ryszard Horodecki. "General teleportation channel, singlet fraction and quasi-distillation". In: *Physical Review A - Atomic, Molecular, and Optical Physics* 60.3 (1998), pp. 1888–1898. arXiv: quant-ph/9807091 [quant-ph].

[Hol02] A. S. Holevo. *Remarks on the classical capacity of quantum channel.* 2002. DOI: 10.48550/ARXIV.QUANT-PH/0212025.

[Hol08] A. S. Holevo. "Entanglement-breaking channels in infinite dimensions". In: *Problems of Information Transmission* 44.3 (2008), pp. 171–184. DOI: 10.1134/S0032946008030010. arXiv: 0802.0235.

[Hol11] Alexander Holevo. *Probabilistic and Statistical Aspects of Quantum Theory.* Pisa: Edizioni della Normale, 2011. DOI: 10.1007/978-88-7642-378-9.

[Hol19] Alexander S. Holevo. *Quantum Systems, Channels, Information.* De Gruyter, 2019. DOI: 10.1515/9783110642490.

[Hol98] A. S. Holevo. "The capacity of the quantum channel with general signal states". In: *IEEE Transactions on Information Theory* 44.1 (1998), pp. 269–273. DOI: 10.1109/18.651037. arXiv: quant-ph/9611023 [quant-ph].

[Ipp+15] Matteo Ippoliti, Leonardo Mazza, Matteo Rizzi, and Vittorio Giovannetti. "Perturbative approach to continuous-time quantum error correction". In: *Physical Review A* 91.4 (2015). DOI: 10.1103/physreva.91.042322.

[KFG19] Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Optimal quantum subtracting machine". In: *Physical Review A* 99.5 (2019), p. 052319. DOI: 10.1103/PhysRevA.99.052319. arXiv: 1811.07187.

[KFG22] Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. "Bounding the quantum capacity with flagged extensions". In: *Quantum* 6 (2022), p. 647. DOI: 10.22331/q-2022-02-09-647.

[Kin02] Christopher King. "Additivity for unital qubit channels". In: *Journal of Mathematical Physics* 43.10 (2002), p. 4641. DOI: 10.1063/1.1500791. arXiv: quant-ph/0103156 [quant-ph].

[Kin03] Christopher King. "The capacity of the quantum depolarizing channel". In: *IEEE Transactions on Information Theory* 49.1 (2003), pp. 221–229. DOI: 10.1109/TIT.2002.806153. arXiv: quant-ph/0204172 [quant-ph].

[Kin+05] Christopher King, Keiji Matsumoto, Michael Nathanson, and Mary Beth Ruskai. "Properties of Conjugate Channels with Applications to Additivity and Multiplicativity". In: *Markov Process and Related Fields* 13 (2005), pp. 391–423. arXiv: quant-ph/0509126 [quant-ph].

[Kin06] Christopher King. "An application of the Lieb-Thirring inequality in quantum information theory". In: *XIVth International Congress on Mathematical Physics: Lisbon, 28 July - 2 August 2003*. WORLD SCIENTIFIC, 2006, pp. 486–490. DOI: 10.1142/9789812704016_0047. arXiv: quant-ph/0412046 [quant-ph].

[Kna10] Anthony W. Knapp. *Lie Groups Beyond an Introduction*. Birkhäuser Boston, MA, 2010.

[KSW20] Sumeet Khatri, Kunal Sharma, and Mark M. Wilde. "Information-theoretic aspects of the generalized amplitude-damping channel". In: *Physical Review A* 102.1 (2020), p. 012401. DOI: 10.1103/PhysRevA.102.012401. arXiv: 1903.07747.

[Lad+10] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. "Quantum computers". In: *Nature* 464.7285 (2010), pp. 45–53. DOI: 10.1038/nature08812.

[Lam+20] Ludovico Lami, Martin B. Plenio, Vittorio Giovannetti, and Alexander S. Holevo. "Bosonic Quantum Communication Across Arbitrarily High Loss Channels". In: *Physical Review Letters* 125.11 (2020), p. 110504. DOI: 10.1103/PhysRevLett.125.110504. arXiv: 2003.08895.

[LDS18] Felix Leditzky, Nilanjana Datta, and Graeme Smith. "Useful States and Entanglement Distillation". In: *IEEE Transactions on Information Theory*. Vol. 64. 7. 2018, pp. 4689–4708. DOI: 10.1109/TIT.2017.2776907. arXiv: 1701.03081.

[Led+22] Felix Leditzky, Debbie Leung, Vikesh Siddhu, Graeme Smith, and John A. Smolin. "The platypus of the quantum channel zoo". In: (2022). DOI: 10.48550/ARXIV.2202.08380.

[Li+09] Ke Li, Andreas Winter, Xubo Zou, and Guangcan Guo. "Private Capacity of Quantum Channels is Not Additive". In: *Physical Review Letters* 103.12 (2009), p. 120501. DOI: 10.1103/PhysRevLett.103.120501. arXiv: 0903.4308.

[Lim+19a] Youngrong Lim, Soojoon Lee, Jaewan Kim, and Kabgyun Jeong. "Upper bounds on the quantum capacity for a general attenuator and amplifier". In: *Physical Review A* 99.5 (2019), p. 052326. DOI: 10.1103/PhysRevA.99.052326. arXiv: 1903.04728.

[Lim+19b] Youngrong Lim, Ryuji Takagi, Gerardo Adesso, and Soojoon Lee. "Activation and superactivation of single-mode Gaussian quantum channels". In: *Physical Review A* 99.3 (2019), p. 032337. DOI: 10.1103/PhysRevA.99.032337. arXiv: 1901.03147.

[Lin75] Göran Lindblad. "Completely positive maps and entropy inequalities". In: *Communications in Mathematical Physics* 40.2 (1975), pp. 147–151. DOI: 10.1007/BF01609396.

[Llo97] Seth Lloyd. "Capacity of the noisy quantum channel". In: *Physical Review A* 55.3 (1997), pp. 1613–1622. DOI: 10.1103/PhysRevA.55.1613. arXiv: quant-ph/9604015 [quant-ph].

[LLS18a] Felix Leditzky, Debbie Leung, and Graeme Smith. "Dephrasure Channel and Superadditivity of Coherent Information". In: *Physical Review Letters* 121.16 (2018), p. 160501. DOI: 10.1103/PhysRevLett.121.160501. arXiv: 1806.08327.

[LLS18b] Felix Leditzky, Debbie Leung, and Graeme Smith. "Quantum and Private Capacities of Low-Noise Channels". In: *Phys. Rev. Lett.* 120 (16 2018), p. 160503. DOI: 10.1103/PhysRevLett.120.160503.

[LLS18c] Felix Leditzky, Debbie Leung, and Graeme Smith. "Quantum and Private Capacities of Low-Noise Channels". In: *Physical Review Letters* 120.16 (2018), p. 160503. DOI: 10.1103/PhysRevLett.120.160503. arXiv: 1705.04335.

[LR73a] Elliott H. Lieb and Mary Beth Ruskai. "A fundamental property of quantum-mechanical entropy". In: *Physical Review Letters* 30.10 (1973), pp. 434–436. DOI: 10.1103/PhysRevLett.30.434.

[LR73b] Elliott H. Lieb and Mary Beth Ruskai. "Proof of the strong subadditivity of quantum-mechanical entropy". In: *Journal of Mathematical Physics* 14.12 (1973), pp. 1938–1941. DOI: 10.1063/1.1666274.

[LS09] Debbie Leung and Graeme Smith. "Continuity of Quantum Channel Capacities". In: *Communications in Mathematical Physics* 292.1 (2009), pp. 201–215. DOI: 10.1007/s00220-009-0833-1. arXiv: 0810.4931.

[MAT10] MATLAB. *version 7.10.0 (R2010a)*. Natick, Massachusetts: The MathWorks Inc., 2010.

[MP95] S. Massar and S. Popescu. "Optimal Extraction of Information from Finite Quantum Ensembles". In: *Phys. Rev. Lett.* 74 (8 1995), pp. 1259–1263. DOI: 10.1103/PhysRevLett.74.1259.

[NAJ19] Kyungjoo Noh, Victor V. Albert, and Liang Jiang. "Quantum Capacity Bounds of Gaussian Thermal Loss Channels and Achievable Rates with Gottesman-Kitaev-Preskill Codes". In: *IEEE Transactions on Information Theory* 65.4 (2019), pp. 2563–2582. DOI: 10.1109/TIT.2018.2873764. arXiv: 1801.07271.

[NC02] Michael A. Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

[NC97] M. A. Nielsen and Isaac L. Chuang. "Programmable Quantum Gate Arrays". In: *Phys. Rev. Lett.* 79 (2 1997), pp. 321–324. DOI: 10.1103/PhysRevLett.79.321.

[NPJ20] Kyungjoo Noh, Stefano Pirandola, and Liang Jiang. "Enhanced energy-constrained quantum communication over bosonic Gaussian channels". In: *Nature Communications* 11.1 (2020), p. 457. DOI: 10.1038/s41467-020-14329-6. arXiv: 1811.06988.

[OMW22] Samad Khabbazi Oskouei, Stefano Mancini, and Andreas Winter. "Capacities of Gaussian Quantum Channels With Passive Environment Assistance". In: *IEEE Transactions on Information Theory* 68.1 (2022), pp. 339–358. DOI: 10.1109/tit.2021.3122150.

[Osz+16] Michal Oszmaniec, Andrzej Grudka, Michal Horodecki, and Antoni W'ojcik. "Creating a Superposition of Unknown Quantum States". In: *Phys. Rev. Lett.* 116 (11 2016), p. 110403. DOI: 10.1103/PhysRevLett.116.110403.

[Ouy14] Yingkai Ouyang. "Channel covariance, twirling, contraction, and some upper bounds on the quantum capacity". In: *Quantum Information and Computation* 14.11-12 (2014), pp. 917–936. DOI: 10.26421/qic14.11-12-2. arXiv: 1106.2337.

[PB00] Arun Kumar Pati and Samuel L. Braunstein. In: *Nature* 404.6774 (2000), pp. 164–165. DOI: 10.1038/35004532.

[PHH08] Marco Piani, Paweł Horodecki, and Ryszard Horodecki. "No-Local-Broadcasting Theorem for Multipartite Quantum Correlations". In: *Phys. Rev. Lett.* 100 (9 2008), p. 090502. DOI: 10.1103/PhysRevLett.100.090502.

[Pir+17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. "Fundamental limits of repeaterless quantum communications". In: *Nature Communications* 8.1 (2017), p. 15043. DOI: 10.1038/ncomms15043. arXiv: 1510.08863.

[Rai01] E. M. Rains. "A semidefinite program for distillable entanglement". In: *IEEE Transactions on Information Theory* 47.7 (2001), pp. 2921–2933. DOI: 10.1109/18.959270. arXiv: quant-ph/0008047 [quant-ph].

[Rai99] E. M. Rains. "Bound on distillable entanglement". In: *Physical Review A* 60.1 (1999), pp. 179–184. DOI: 10.1103/PhysRevA.60.179.

[RMG18] Matteo Rosati, Andrea Mari, and Vittorio Giovannetti. "Narrow bounds for the quantum capacity of thermal attenuators". In: *Nature Communications* 9.1 (2018), p. 4339. DOI: 10.1038/s41467-018-06848-0. arXiv: 1801.04731.

[Sca+02] Valerio Scarani, Mario Ziman, Peter Stelmachovic, Nicolas Gisin, and Vladimir Buz. "Thermalizing Quantum Machines: Dissipation and Entanglement". In: *Phys. Rev. Lett.* 88 (9 2002), p. 097905. DOI: 10.1103/PhysRevLett.88.097905.

[Sca+05] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acin. "Quantum cloning". In: *Rev. Mod. Phys.* 77 (4 2005), pp. 1225–1256. DOI: 10.1103/RevModPhys.77.1225.

[Sch95] Benjamin Schumacher. "Quantum coding". In: *Physical Review A* 51.4 (1995), pp. 2738–2747. DOI: 10.1103/PhysRevA.51.2738.

[Ser17] Alessio Serafini. *Quantum continuous variables: A primer of theoretical methods*. Boca Raton: CRC Press, 2017, pp. 1–349. DOI: 10.1201/9781315118727.

[SG21] Vikesh Siddhu and Robert B. Griffiths. "Positivity and Nonadditivity of Quantum Capacities Using Generalized Erasure Channels". In: *IEEE Transactions on Information Theory* 67.7 (2021), pp. 4533–4545. DOI: 10.1109/TIT.2021.3080819. arXiv: 2003.00583.

[Sha+18] Kunal Sharma, Mark M. Wilde, Sushovit Adhikari, and Masahiro Takeoka. "Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels". In: *New Journal of Physics* 20.6 (2018), p. 063025. DOI: 10.1088/1367-2630/aac11a. arXiv: 1708.07257.

[Sha48] C. E. Shannon. "A Mathematical Theory of Communication". In: *Bell System Technical Journal* 27.4 (1948), pp. 623–656. DOI: 10.1002/j.1538-7305.1948.tb00917.x.

[Shi06] M. E. Shirokov. "The Convex Closure of the Output Entropy of Infinite Dimensional Channels and the Additivity Problem". In: (2006). DOI: 10.48550/ARXIV.QUANT-PH/0608090.

[Sho02a] Peter W. Shor. "Additivity of the classical capacity of entanglement-breaking quantum channels". In: *Journal of Mathematical Physics* 43.9 (2002), pp. 4334–4340. DOI: 10.1063/1.1498000. arXiv: quant-ph/0201149 [quant-ph].

[Sho02b] Peter W. Shor. "The quantum channel capacity and coherent information". In: *lecture notes, MSRI Workshop on Quantum Computation (Quantum Information and Cryptography)*. 2002. DOI: www.msri.org/workshops/203/schedules/1181.

[Sho04] Peter W. Shor. "Equivalence of Additivity Questions in Quantum Information Theory". In: *Communications in Mathematical Physics* 246.3 (2004), pp. 473–473. DOI: 10.1007/s00220-004-1071-1.

[Sid20a] Vikesh Siddhu. *Leaking information to gain entanglement.* 2020. arXiv: 2011.15116.

[Sid20b] Vikesh Siddhu. *Log-singularities for studying capacities of quantum channels.* 2020. arXiv: 2003.10367.

[Sin96] In: *SIAM Rev.* 38.1 (1996). Ed. by R. Sincovec.

[Smi08] Graeme Smith. "Private classical capacity with a symmetric side channel and its application to quantum cryptography". In: *Physical Review A* 78.2 (2008), p. 022306. DOI: 10.1103/PhysRevA.78.022306. arXiv: 0705.3838.

[SRS08] Graeme Smith, Joseph M. Renes, and John A. Smolin. "Structured Codes Improve the Bennett-Brassard-84 Quantum Key Rate". In: *Physical Review Letters* 100.17 (2008), p. 170502. DOI: 10.1103/PhysRevLett.100.170502. arXiv: quant-ph/0607018 [quant-ph].

[SS07] Graeme Smith and John A. Smolin. "Degenerate Quantum Codes for Pauli Channels". In: *Physical Review Letters* 98.3 (2007), p. 030501. DOI: 10.1103/PhysRevLett.98.030501. arXiv: quant-ph/0604107 [quant-ph].

[SS08] Graeme Smith and John A. Smolin. "Additive extensions of a quantum channel". In: *2008 IEEE Information Theory Workshop.* IEEE, 2008, pp. 368–372. DOI: 10.1109/ITW.2008.4578688. arXiv: 0712.2471.

[SS96] Peter W. Shor and John A. Smolin. *Quantum Error-Correcting Codes Need Not Completely Reveal the Error Syndrome.* 1996. arXiv: quant-ph/9604006 [quant-ph].

[SSW08] Graeme Smith, John A. Smolin, and Andreas Winter. "The quantum capacity with symmetric side channels". In: *IEEE Transactions on Information Theory* 54.9 (2008), pp. 4208–4217. DOI: 10.1109/TIT.2008.928269. arXiv: quant-ph/0607039 [quant-ph].

[SSY11] Graeme Smith, John A. Smolin, and Jon Yard. "Quantum communication with Gaussian channels of zero quantum capacity". In: *Nature Photonics* 5.10 (2011), pp. 624–627. DOI: 10.1038/nphoton.2011.203. arXiv: 1102.4580.

[Sut+17] David Sutter, Volkher B. Scholz, Andreas Winter, and Renato Renner. "Approximate Degradable Quantum Channels". In: *IEEE Transactions on Information Theory* 63.12 (2017), pp. 7832–7844. DOI: 10.1109/TIT.2017.2754268. arXiv: 1412.0980.

[SW97] Benjamin Schumacher and Michael D. Westmoreland. "Sending classical information via noisy quantum channels". In: *Physical Review A* 56.1 (1997), pp. 131–138. DOI: 10.1103/PhysRevA.56.131. arXiv: quant-ph/9604023 [quant-ph].

[SY08] Graeme Smith and Jon Yard. "Quantum Communication with Zero-Capacity Channels". In: *Science* 321.5897 (2008), pp. 1812–1815. DOI: 10.1126/science.1162242. arXiv: 0807.4935.

[Wee+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, et al. "Gaussian quantum information". In: *Rev. Mod. Phys.* 84 (2 2012), pp. 621–669. DOI: 10.1103/RevModPhys.84.621.

[Wer01] R. F. Werner. "Quantum Information Theory - an Invitation". In: (2001). DOI: 10.48550/ARXIV.QUANT-PH/0101061.

[Wer98] R. F. Werner. "Optimal cloning of pure states". In: *Phys. Rev. A* 58 (3 1998), pp. 1827–1832. DOI: 10.1103/PhysRevA.58.1827.

[WFD19] Xin Wang, Kun Fang, and Runyao Duan. "Semidefinite Programming Converse Bounds for Quantum Communication". In: *IEEE Transactions on Information Theory* 65.4 (2019), pp. 2583–2592. DOI: 10.1109/TIT.2018.2874031. arXiv: 1709.00200.

[Wil17] Mark M. Wilde. *Quantum Information Theory*. Cambridge: Cambridge University Press, 2017, pp. 1–757. DOI: 10.1017/9781316809976.

[Wit14] Peter Wittek. *Quantum machine learning: what quantum computing means to data mining*. Academic Press, 2014.

[Wol18] Inc. Wolfram Research. *Mathematica*. Champaign, IL, 2018.

[Woo87] William K. Wootters. "A Wigner-function formulation of finite-state quantum mechanics". In: *Annals of Physics* 176.1 (1987). DOI: 10.1016/0003-4916(87)90176-X.

[WPG07] Michael M. Wolf and David Pérez-García. "Quantum capacities of channels with small environment". In: *Physical Review A* 75.1 (2007), p. 012303. DOI: 10.1103/PhysRevA.75.012303. arXiv: quant-ph/0607070 [quant-ph].

[WQ16] Mark M. Wilde and Haoyu Qi. "Energy-constrained private and quantum capacities of quantum channels". In: *IEEE Transactions on Information Theory* 64.12 (2016), pp. 7802–7827. DOI: 10.1109/TIT.2018.2854766. arXiv: 1609.01997.

[WTB17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. "Converse bounds for private communication over quantum channels". In: *IEEE Transactions on Information Theory* 63.3 (2017), pp. 1792–1817. DOI: 10.1109/TIT.2017.2648825. arXiv: 1602.08898.

[WW19] Xin Wang and Mark M. Wilde. "Resource theory of asymmetric distinguishability for quantum channels". In: *Physical Review Research* 1.3 (2019), p. 033169. DOI: 10.1103/PhysRevResearch.1.033169. arXiv: 1907.06306.

[WZ82] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". In: *Nature* 299.5886 (Oct. 1982), pp. 802–803. DOI: 10.1038/299802a0.

[YHD08] Jon Yard, Patrick Hayden, and Igor Devetak. "Capacity theorems for quantum multiple-access channels: classical-quantum and quantum-quantum capacity regions". In: *IEEE Transactions on Information Theory* 54.7 (2008), pp. 3091–3113. DOI: 10.1109/TIT.2008.924665. arXiv: quant-ph/0501045 [quant-ph].

[Yu+20] Shang Yu, Yu Meng, Raj B. Patel, Yi-Tao Wang, Zhi-Jin Ke, Wei Liu, et al. "Experimental Observation of Coherent-Information Superadditivity in a Dephrasure Channel". In: *Physical Review Letters* 125.6 (2020), p. 060502. DOI: 10.1103/PhysRevLett.125.060502. arXiv: 2003.13000.

[Zhu+19] Elton Yechao Zhu, Quntao Zhuang, Min Hsiu Hsieh, and Peter W. Shor. "Superadditivity in Trade-Off Capacities of Quantum Channels". In: *IEEE Transactions on Information Theory* 65.6 (2019), pp. 3973–3989. DOI: 10.1109/TIT.2018.2889082. arXiv: 1708.04314.

[ZZS17] Elton Yechao Zhu, Quntao Zhuang, and Peter W. Shor. "Superadditivity of the Classical Capacity with Limited Entanglement Assistance". In: *Physical Review Letters* 119.4 (2017), p. 040503. DOI: 10.1103/PhysRevLett.119.040503. arXiv: 1704.06955.