Louisiana State University

LSU Digital Commons

10-15-2018

Bipartite Quantum Interactions: Entangling and Information Processing Abilities

Siddhartha Das
Louisiana State University and Agricultural and Mechanical College

BIPARTITE QUANTUM INTERACTIONS:
ENTANGLING AND INFORMATION PROCESSING ABILITIES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Physics & Astronomy

by
Siddhartha Das
B.S. and M.S., Indian Institute of Science Education and Research Pune, 2014
December 2018

I dedicate this dissertation to my family members – sisters, Chetna Das and Hema Das, and parents, Ram Narayan Das and Kalpana Das. Their love, support, and sacrifices are immeasurable. They keep me going with a peaceful mind and content heart. In addition, I also dedicate this dissertation to all my teachers, in particular, Ishwari Shrestha and Akhilesh Kumar Das (Batul da). Their teachings and guidance still serve to shed light when I find myself lost.

Acknowledgments

Table of Contents

Abstract

The aim of this thesis is to advance the theory behind quantum information processing tasks, by deriving fundamental limits on bipartite quantum interactions and dynamics. A bipartite quantum interaction corresponds to an underlying Hamiltonian that governs the physical transformation of a two-body open quantum system. Under such an interaction, the physical transformation of a bipartite quantum system is considered in the presence of a bath, which may be inaccessible to an observer. The goal is to determine entangling abilities of such arbitrary bipartite quantum interactions. Doing so provides fundamental limitations on information processing tasks, including entanglement distillation and secret key generation, over a repeaterless bipartite quantum network. We also discuss limitations on the entropy change and its rate for dynamics of an open quantum system weakly interacting with the bath. We introduce a measure of non-unitarity to characterize the deviation of a doubly stochastic quantum process from a noiseless evolution.

Next, we introduce information processing tasks for secure read-out of digital information encoded in read-only memory devices against adversaries of varying capabilities. The task of reading a memory device involves the identification of an interaction process between probe system, which is in known state, and the memory device. Essentially, the information is stored in the choice of channels, which are noisy quantum processes in general and are chosen from a publicly known set. Hence, it becomes pertinent to securely read memory devices against scrutiny of an adversary. In particular, for a secure read-out task called private reading when a reader is under surveillance of a passive eavesdropper, we have determined upper bounds on its performance. We do so by leveraging the fact that private reading of digital information stored in a memory device can be understood as secret key agreement via a specific kind of bipartite quantum interaction.

1

Chapter 1   Exploring Informational Aspects of Quantum Interactions

1.1   Motivation

The beauty of nature is inexpressible. It is of fundamental interest to understand natural phenomena. All physical systems and processes are governed by the laws of nature. In this thesis, we limit our discussion to the domain in which the laws of nature are well described by *quantum* theory. Note that the classical theory emerges from the quantum theory as an approximation; i.e., the laws of classical mechanics can be obtained from the laws of quantum mechanics by making particular choices for a quantum process and the state of a quantum system [1, 2].

A physical system that is described by the laws of quantum mechanics is called a quantum system. The state of a quantum system has its complete physical description. A physical operation is quantum when evolution of a quantum system is feasible under its action. In general, the physical description contained in the state of a quantum system cannot be accounted for classical theory [1] [2]. While quantum effects are dominating in microscopic regime, these effects are largely unnoticeable (vanishing) in macroscopic regime.

With the inception of the idea that information is physical [10, 11], there has been wide interest in studying several physical phenomena and systems from an information-theoretic perspective. Information is associated with a physical respresentation. The information content of a physical system must be finite if the region of space and the energy is finite [11, 12]. From these observations, we can conclude that storage, processing, and transmission of information are all governed by physical laws.

The primary goal of this thesis is to explore informational aspects of bipartite quantum interactions and their capabilities to generate entanglement, an intriguing quantum phenomenon. A physical transformation of the state of a bipartite quantum system is effected by an underlying Hamiltonian. We are interested in the most general interaction such that a bipartite quantum system may be in contact with a bath, which is inaccessible to an observer. Bipartite quantum in-

---

[1]Entanglement, superposition, uncertainty relations, contextuality, and indeterminsim [3–9] are some of the interesting features of quantum theory.

teraction refers to an underlying Hamiltonian governing the physical evolution of an open bipartite system. Such an interaction models a non-trivial, elementary interaction in a many-body quantum system. This study is necessary also from the aspect of applications as a bipartite quantum interaction depicts a non-trivial, elementary model of a quantum network involving two parties.

In this age of technology and intelligence, it is of pertinent interest to also inspect information processing capabilities of quantum processes. In general, the laws of quantum theory allow us to push the abilities of processing and computing information beyond the limitations imposed by the classical information theory[2]. This provides us with ample opportunities to devise new information processing, communication, and computation protocols, e.g., quantum key distribution [16, 17], quantum teleportation [18, 19], quantum sensing [20], quantum algorithms for computational speed-up [21] etc.

Broadly speaking, quantum processes are variously referred to as quantum processes, quantum gates, quantum channels, or quantum operations[3]. Evolution of the state of a spin in an Ising model due to spin-spin interaction, a photon transmitted through an optical fiber, an electron interacting with electromagnetic field, or a quantum system decohering due to interaction with surrounding– all these quantum processes are also describable as quantum channels [21–23].

Note that a physical system itself can act as a quantum channel (process). This is because any physical system is capable of transforming the state of a quantum system. For examples, beamsplitter, spontaneous parametric down-conversion, optical fiber, etc. are physical systems that transform the state of incident photons. When I point a laser beam on a screen during my presentation, the state of incident photons would be different from that of the reflected ones. In this case, the screen is a quantum channel with photons as input and output system. This process is noisy as some photons may get absorbed by the screen and not all photons will be accessible to the audience who are observers here. As we will see later, these observations are crucial in devising communication protocols.

Let us now briefly discuss some of the key ideas – information content, quantum processes,

---

[2]There can be instances when there is no advantage provided by quantum theory over classical one [13–15].

[3]It should be clarified that all quantum channels are quantum processes; however, the converse is not true in general. Meaning and subtleties will be clear in Chapters 2 and 4.

entanglement, and information carriers – that led to this work. In the end, we provide an outline of this thesis by briefly discussing contents of the following chapters.

1.2 What is information?

Does a learner gain any knowledge if something obvious is stated to her? The answer is no. Obvious, isn't it?

Knowledge requires information. Information is related to a meaningful piece of data that can be of use to a learner. A piece of data is meaningful to the learner only if she is observant enough. Information content is understood in reference to an observer; in other words, information is observer-dependent. With gain in information, there is reduction in uncertainty about an associated event. The less favorable the occurrence of an outcome of the event is, the more information is learned upon its occurrence; the more favorable an outcome is, the less information is learned upon its occurrence. As an instance, consider that I attempt to defend my thesis in front of PhD committee members. Let us safely assume that the chance of my graduation is high given the trend. My friends will be less surprised and learn less information when the PhD committee gives a passing mark. Whereas, they will be more surprised and learn more information if I fail.

Claude E. Shannon was the first to give a qualitative description of what information is and how it can be transmitted amid noise [24]. The abstract nature of the (classical) information theory introduced by Shannon provided a unified framework to understand seemingly distinct modes of communications and information processing over classical systems. The subject area dealing with information associated to classical systems is called classical information theory. He introduced the notion of a bit as a unit of information, whose physical representation is with a classical system. Roughly speaking, a bit is a binary valued quantity in which values are orthogonal to each other, meaning that they are distinguishable. Occurrence of one value excludes the possible occurrence of the other. Conventionally, a bit is represented by a binary number that can be "0" or "1".

Consider an event, which is an information source, described by a random variable X with an associated discrete alphabet $\mathcal{X}$ of finite size, where $x \in \mathcal{X}$ is called a symbol. Each symbol x corresponds to an outcome of the event. The given random variable X can be represented by a classical register, and suppose that we only allow classical processes to occur. Let $p_X(x)$ be a

probability distribution for describing the outcomes of the event. One measure of the surprise of the symbol $x \in \mathscr{X}$ is

$$i(x) := -\log_2 p_X(x). \tag{1.1}$$

The quantity $i(x)$ is also called surprisal or information content of the symbol x. Formula (1.1) is motivated by desirable properties that a quantifier of information content should have (see [23, 25]). An observer will be infinitely surprised on an outcome of a symbol with no chance of occurrence, i.e., $p_X(x) = 0$. Consider an example of an event that corresponds to tossing of an unbiased coin with two sides– heads and tails. Upon a toss, if either heads or tails shows up then an observer learns one bit of information. The expected surprisal of an event is called its Shannon entropy:

$$S(X) := \mathbb{E}_X\{-\log_2 p_X(X)\} = -\sum_{x \in \mathscr{X}} p(x) \log_2 p(x). \tag{1.2}$$

Now suppose that information carriers are quantum systems. The state of a quantum system has its complete description. Quantum information is information associated to a quantum state. Analogous to the bit of classical information theory, a unit of quantum information is a qubit[4]. A qubit is a two-level quantum system that can be in a superposition state of $|0\rangle$ and $|1\rangle$, where $\{|0\rangle, |1\rangle\}$ form an orthonormal basis. A measure of the average information content of a quantum system is its von Neumann entropy (2.46) [28]. The mathematical framework of quantum mechanics from an information-theoretic perspective is discussed in the next chapter.

1.3 Quantum interactions and processes

Any physical process that operates on or transforms the state of a quantum system is called a quantum process. There is an underlying Hamiltonian that gives rise to such a process. In principle, the evolution of a closed quantum system A' is always given by a unitary transformation and underlying Hamiltonian acts just on A'. However, it is difficult to isolate a system from its surrounding, which leads to an unavoidable interaction with the bath E' (environment). It is often required to deal with a many-body quantum system, which is a difficult task. A simpler case of a many-body system is a two-body system. We call the Hamiltonian responsible for the interaction

---

[4]Interested readers may refer to [21, 23, 26, 27] for detailed discussions on quantum information.

between constituent quantum systems in a many-body system as multipartite quantum interaction. Bipartite unitary evolution is the simplest physical transformation considered on a many-body system.

Suppose that the system A' is uncorrelated to the bath E' before the action of Hamiltonian $\hat{H}_{A'E'}$. In general, $\hat{H}_{A'E'} = \hat{H}_{A'} + \hat{H}_{E'} + \hat{H}_{\text{int}}$, where $\hat{H}_{A'}$ and $\hat{H}_{E'}$ denote Hamiltonians acting on individual systems A' and E', respectively, and $\hat{H}_{\text{int}}$ denotes a Hamiltonian giving rise to a non-trivial interaction between A' and E'. Even though the evolution of the composite system $A' + E'$ is unitary, as $A' + E'$ is closed, transformation of the state of A' is noisy in general for an observer with no access to the bath. It is possible that after the action of the Hamiltonian, the degrees of freedom of the original system changes; i.e., an observer may have access to fewer or more degrees of freedom than A', even though the partial degrees of freedom of the bath system are inaccessible. The total degrees of freedom of composite system remains the same, since it is closed. Such noisy physical operations are also called *quantum channels* or (noisy) gates. A unitary operation is a particular quantum channel. Quantum channels are often called quantum "gates" in the discussion of quantum computation.

A Hamiltonian governing the evolution of an open two-body quantum system is called a bipartite quantum interaction. These interactions give rise to quantum processes that may change correlations between interacting systems if the interaction term present in the Hamiltonian is non-zero. As discussed previously, there is a need to inspect noisy processes involving two-body systems due to the unavoidable interaction between systems of interest and the bath. For an observer who has no access to the degrees of freedom of the bath, evolution process is noisy, i.e., non-unitary in general, and it is called a bipartite quantum channel. It should be noted that the degrees of freedom of the initial and final systems may change after the action of a bipartite channel.

In an information processing task, if pairs of input and output systems, (A', A) and (B', B) belong to two separate observers then a bipartite channel $\mathcal{N}_{A'B' \to AB}$ is called a bidirectional channel. A bidirectional channel $\mathcal{N}_{A'B' \to AB}$ provides the simplest form of a non-trivial network setting, as it allows for an interaction between two parties. Note that a point-to-point communication protocol, which is over a channel $\mathcal{N}_{A' \to B}$, is a special case of a communication protocol over a bidirectional channel $\mathcal{N}_{A'B' \to AB}$. A bidirectional quantum channel is an elementary, non-trivial example of a

quantum network.

1.4 Entanglement

We can sometimes be more certain about the joint state of a two-body quantum system AB than we can be about any one of its individual parts, A or B. These situations occur when a given two-body quantum system is in an entangled state [29]. A particular kind of entangled state is a "maximally entangled" state. As a system AB has two parts, A and B, measurements on its isolated parts A and B are physically possible. Such measurements are referred to as local measurements or operations. If AB is maximally entangled and we perform any local measurement of A or B, then we gain no information about the preparation of the state; instead we merely generate a random bit. A famous example of a maximally entangled state is the singlet state [30]. Entangled states are known to be a useful resource for different information processing tasks, e.g., quantum teleportation, unconditionally secure key distribution, randomness generation, etc.

Bipartite quantum interactions can generate correlations between two separated systems in such a way that the physical description cannot be given by local realistic, hidden variable theories. Two quantum systems need to be entangled for them to exhibit such non-local correlations. While non-local correlations between two quantum systems implies that they are entangled, the converse is not true in general. The state of a bipartite quantum system is said to be entangled when it cannot be described as a convex combination of the uncorrelated states, i.e., product states of the constituent systems. While entanglement can be uniquely defined in the case of bipartite systems, it gets complicated for multipartite systems. This is related to the fact that there is no unique way to describe non-local correlations among many-body quantum systems (see [7] and references therein).

We need quantum interactions to generate quantum correlations between separated systems. We can use these correlations to harvest information and perform computation or communication tasks that may not be achieved with classical processes and systems.

1.5 Information carriers

There are multiple ways to communicate and store a given message. We may use print and digital media for storage and communication of information. We may rely on our brain to store

information. Methods of information storage and transfer depend on the need and accessibility of media among the users. There are continuous efforts to increase information processing abilities of memory devices; we want to decrease the physical size of memory devices while increasing their storage capacity. As we are making advancements in information technology, there is great concern for privacy. At times, we need secure methods for processing or storage of information based on the ability of adversarial scrutiny.

We have been making use of a variety of physical sources for communication and storage of messages. For example, we can use light or sound signals to broadcast important messages to commuters for traffic control. A light signal is better as a traffic signal, as it can be seen by commuters at an appropriate place without getting disturbed by noise of vehicle horns. Sound signals with loud volume are used to alert about the type of emergency vehicles passing through roads amid a crowd. We can also use several distinguishable properties of a physical medium to communicate in different ways. Consider a known and most used medium of communication – sound. We pronounce words to communicate a message, change pitch or tone in order to indicate the level of urgency, and whisper for privacy against an eavesdropper.

We can also use quantum processes as information carriers by encoding a message into a sequence of quantum processes. The efficacy of such method would depend on how well can we distinguish between quantum processes that are usable for encoding. As an example, let us consider memory devices. At a fundamental level, we can always understand the storage of messages in memory devices to be in the form of quantum channels. The mechanism of reading of any memory device involves the transmission of a probe system, which is in a known state, and inspecting the transformation of its state after an interaction with the system used for encryption of a message. In principle, any quantum processes can be used for information storage and communication. The choice of quantum processes depends on the kind of quantum systems accessible by a reader. In order to build up secure information processing, we need to come up with a strategy that hides encoded messages in quantum processes against an adversary. While an authorized user can access a hidden message, the probability of an adversary being able to access a hidden message should be negligible.

Communication of messages over quantum processes, i.e., channels, is a topic of wide interest

[23, 27]; quantum states are used to encode a message and then are transmitted over a physical medium, which are modeled as some noisy quantum processes, e.g., bosonic Gaussian channels, depolarizing channels, etc. The primary idea behind such communication protocols depends on the discrimination of quantum states. These protocols allow for quick communication between distant parties.

The choice of information carrier as quantum states or processes depends on the need and interest of communicating parties. While mathematically there is a correspondence called the Choi–Jamiołkowski isomorphism between quantum processes and states, there are distinct differences from a physical perspective. If we want an information carrier to be robust against measurements and also to be long-lived, then we cannot encode a message in terms of quantum state in general. This is because quantum states are fragile against measurement and may decohere due to unavoidable interaction with surrounding. In such situations, we may instead want robust physical systems that can be described as quantum processes required for the task. Whereas, if we want our information carrier to be securely transmitted between points over a distance, we would encrypt the message in a quantum state and transmit it over a quantum channel. Subtle issues are discussed briefly in latter chapters.

1.6 Overview of thesis

In this section, we briefly review the main results developed and discussed in this thesis. In Chapter 2, we discuss the mathematical formulation of quantum mechanics, definitions of information measures, and important lemmas required to derive the main results discussed in latter chapters.

In Chapter 3, the main focus is on deriving fundamental limitations on entangling abilities of bipartite quantum interactions [31]. These bounds also provide limitations on the information processing abilities of a repeaterless bipartite quantum network. Entangling abilities of bipartite quantum interactions are relevant in a number of different areas of quantum physics, reaching from fundamental areas such as quantum thermodynamics and the theory of quantum measurements to other applications such as quantum computation, quantum key distribution, and other information processing protocols. A particular aspect of the study of bipartite interactions is concerned with

entanglement that can be created from such interactions. In this chapter, we discuss two basic building blocks of bipartite quantum protocols, namely, the generation of maximally entangled states and secret key via bipartite quantum interactions. In particular, we provide a non-trivial, efficiently computable upper bound on the positive-partial-transpose-assisted (PPT-assisted) entanglement distillation capacity of bidirectional quantum channel, thus addressing a question that has been open since 2002. In addition, we provide an upper bound on the private capacity of bidirectional quantum channels assisted by local operations and classical communication (LOCC).

In Chapter 4, we discuss limitations on quantum dynamics based on entropy change [32]. It is well known in the realm of quantum mechanics and information theory that the entropy is non-decreasing for the class of doubly stochastic physical processes, also called unital processes. However, in general, the entropy does not exhibit monotonic behavior. This has restricted the use of entropy change in characterizing evolution processes. Recently, a lower bound on the entropy change was provided in [33]. We explore the limit that this bound places on the physical evolution of a quantum system and discuss how these limits can be used as witnesses to characterize quantum dynamics. In particular, we derive a lower limit on the rate of entropy change for memoryless quantum dynamics, and we argue that it provides a witness of non-unitality; i.e., violation of the bound would be possible only if the dynamics are non-unital. This limit on the rate of entropy change leads to definitions of several witnesses for testing memory effects in quantum dynamics. Furthermore, from the aforementioned lower bound on entropy change, we obtain a measure of non-unitarity for unital evolutions.

In Chapter 5, we discuss a general protocol for quantum reading and discuss bounds on the reading capacities [34]. Quantum reading refers to the task of reading out classical information stored in a read-only memory device. In any such protocol, the transmitter and receiver are in the same physical location, and the goal of such a protocol is to use these devices, coupled with a quantum strategy, to read out as much information as possible from a memory device, such as a CD or DVD. As a consequence of the physical setup of quantum reading, the most natural and general definition for quantum reading capacity should allow for an adaptive operation after each call to the channel, and this is how quantum reading capacity is defined in this chapter. We also derive several bounds on quantum reading capacity, and we introduce an environment-parametrized

memory cell, delivering second-order and strong converse bounds for its quantum reading capacity. We calculate the quantum reading capacities for some exemplary memory cells, including a thermal memory cell, a qudit erasure memory cell, and a qudit depolarizing memory cell. We finally discuss an explicit example to illustrate the advantage of using an adaptive strategy in the context of zero-error quantum reading capacity.

In Chapter 6, we introduce a protocol for the private reading of memory devices against an eavesdropper [31]. We can use this protocol for secret key agreement between two authorized parties where secret key is encoded in a memory device. The goal is to protect from the leakage of the secret key to an eavesdropper who is spying on the reader. We notice that private reading can be understood as a particular kind of secret-key-agreement protocol that employs a particular kind of bipartite interaction. We make use of this observation to derive upper bounds on private reading capacities of memory devices.

In Chapter 7, we introduce protocols for the secure retrieval of digital information stored in a memory device under different adversarial situations. We refer to such protocols as secure reading. Information in memory devices is encoded in terms of quantum channels selected from a particular set called a memory cell. We allow the encoder and the intended reader to share secret keys prior to the reading task is carried out. We also consider a toy model in which a message is encoded in unitary gates and show the advantage of an authorized reader who has key against an unauthorized user with no key. For more general secure reading protocol, we consider a passive adversary who has complete access to the environment, and a semi-passive adversary who can access the memory device. To illustrate these protocols, we discuss examples for the secure reading of memory devices encoded with a binary memory cell consisting of amplitude damping channels or depolarizing channels. We also briefly discuss application of a secure reading protocol for a threat level identification scheme, which is inspired by IFF: identification, friend or foe.

Chapter 2   Quantum Systems, Physical Processes, and Information Measures

In this chapter, we take an information-theoretic approach to review some of the basic concepts of quantum mechanics. We start by introducing standard notations, definitions, and important lemmas that are required for the derivation and discussions of results introduced in latter sections and chapters. We discuss the mathematical representation of the state of a quantum system and physical quantum processes, particular set of states, structure of physical processes obeying certain symmetries, measures to quantify information content in a quantum system, and the notion of bipartite entanglement measures. Finally, in Section 2.8.1[1], we present results on the approximate normalization of two different entanglement measures– entropy of entanglement [35] and squashed entanglement [36].

2.1   Bounded operators and super-operators

In this review, the discussion is focused on finite–dimensional Hilbert spaces. See Section 4.1 for discussion on infinite–dimensional Hilbert spaces.

Let $\mathscr{B}(\mathcal{H})$ denote the algebra of bounded operators acting on a Hilbert space $\mathcal{H}$, with $\mathbb{1}_\mathcal{H} \in \mathscr{B}(\mathcal{H})$ denoting the identity operator and id denoting the identity super-operator[2]. Let $\dim(\mathcal{H})$ denote the dimension of Hilbert space $\mathcal{H}$ [3]. $\mathscr{B}(\mathcal{H})$ also denotes the set of all trace-class operators acting on the Hilbert space $\mathcal{H}$, since $\mathcal{H}$ is finite-dimensional.

The Hilbert space of a system A is denoted by $\mathcal{H}_A$ and the Hilbert space of a composite system consisting of systems A and B is given by the tensor product $\mathcal{H}_{AB} := \mathcal{H} \otimes \mathcal{H}_B$. The notation $A^n := A_1 A_2 \cdots A_n$ indicates a composite system consisting of n subsystems A, each of which is isomorphic to the Hilbert space $\mathcal{H}_A$; i.e., for all $i \in [n]$, $A_i \simeq A$, where $[n] := \{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$. Let us denote the set of all orthonormal bases of the Hilbert space $\mathcal{H}$ as $\mathrm{ONB}(\mathcal{H})$.

The subset of $\mathcal{B}(\mathcal{H})$ containing all positive semi-definite operators is denoted by $\mathscr{B}_+(\mathcal{H})$. We

---

[1]Section 2.8.1 is entirely based on an unpublished work done in collaboration with Mark M. Wilde.

[2]A super-operator is a linear map that acts on an operator.

[3]Note that $\dim(\mathcal{H})$ is equal to $+\infty$ in the case that $\mathcal{H}$ is a separable, infinite-dimensional Hilbert space.

write $C \geq 0$ to indicate that $C \in \mathscr{B}_+(\mathcal{H})$, and $C \geq D$ indicates $C - D \in \mathscr{B}_+(\mathcal{H})$.

A super-operator $\mathcal{M}_{A \to B}$ denotes a linear map $\mathcal{M} : \mathscr{B}(\mathcal{H}_A) \to \mathscr{B}(\mathcal{H}_B)$ that maps elements in $\mathscr{B}(\mathcal{H}_A)$ to elements in $\mathscr{B}(\mathcal{H}_B)$. The adjoint $\mathcal{M}^\dagger : \mathscr{B}(\mathcal{H}_B) \to \mathscr{B}(\mathcal{H}_A)$ of a linear map $\mathcal{M} : \mathscr{B}(\mathcal{H}_A) \to \mathscr{B}(\mathcal{H}_B)$ is the unique linear map that satisfies

$$\langle Y_B, \mathcal{M}(X_A) \rangle = \langle \mathcal{M}^\dagger(Y_B), X_A \rangle, \qquad \forall\ X_A \in \mathscr{B}(\mathcal{H}_A), Y_B \in \mathscr{B}(\mathcal{H}_B) \tag{2.1}$$

where $\langle C, D \rangle = \mathrm{Tr}\{C^\dagger D\}$ is the Hilbert-Schmidt inner product. An isometry $U : \mathcal{H} \to \mathcal{H}'$ is a linear map such that $U^\dagger U = \mathbb{1}_\mathcal{H}$ and $UU^\dagger = \Pi_{\mathcal{H}'}$, where $\Pi_{\mathcal{H}'}$ is a projection onto a subspace of the Hilbert space $\mathcal{H}'$.

A super-operator $\mathcal{M}_{A \to B} : \mathscr{B}(\mathcal{H}_A) \to \mathscr{B}(\mathcal{H}_B)$ is called positive if it maps elements of $\mathscr{B}_+(\mathcal{H}_A)$ to elements of $\mathscr{B}_+(\mathcal{H}_B)$ and completely positive if $\mathrm{id}_R \otimes \mathcal{M}_{A \to B}$ is positive for a Hilbert space $\mathcal{H}_R$ of any dimension, where id_R is the identity super-operator acting on $\mathscr{B}(\mathcal{H}_R)$. A positive map $\mathcal{M}_{A \to B} : \mathscr{B}_+(\mathcal{H}_A) \to \mathscr{B}_+(\mathcal{H}_B)$ is called trace non-increasing if $\mathrm{Tr}\{\mathcal{M}_{A \to B}(\sigma_A)\} \leq \mathrm{Tr}\{\sigma_A\}$ for all $\sigma_A \in \mathscr{B}_+(\mathcal{H}_A)$, and it is called trace-preserving if $\mathrm{Tr}\{\mathcal{M}_{A \to B}(\sigma_A)\} = \mathrm{Tr}\{\sigma_A\}$ for all $\sigma_A \in \mathscr{B}_+(\mathcal{H}_A)$. When confusion does not arise, we omit identity operators in expressions involving multiple tensor factors, so that, for example, $\mathcal{M}_{A \to B}(\rho_{RA})$ is understood to mean $\mathrm{id}_R \otimes \mathcal{M}_{A \to B}(\rho_{RA})$.

A linear map $\mathcal{M}_{A \to B} : \mathscr{B}(\mathcal{H}_A) \to \mathscr{B}(\mathcal{H}_B)$ is called sub-unital if $\mathcal{M}_{A \to B}(\mathbb{1}_A) \leq \mathbb{1}_B$, unital if $\mathcal{M}_{A \to B}(\mathbb{1}_A) = \mathbb{1}_B$, and super-unital if $\mathcal{M}_{A \to B}(\mathbb{1}_A) > \mathbb{1}_B$. Note that it is possible for a linear map to be neither unital, sub-unital, nor super-unital. A positive trace-preserving map can be sub-unital only if the dimension of the output Hilbert space is greater than or equal to the dimension of the input Hilbert space. A positive trace-preserving map can be super-unital only if the dimension of the output Hilbert space is less than the dimension of the input Hilbert space. Positive trace-preserving maps between two finite-dimensional Hilbert spaces of the same dimension that are sub-unital are also unital.

2.2 Operator-valued functions and norms

Let A be a self-adjoint operator acting on a Hilbert space $\mathcal{H}$. The support $\mathrm{supp}(A)$ of A is the span of the eigenvectors of A corresponding to its non-zero eigenvalues, and the kernel of A is the span of the eigenvectors of A corresponding to its zero eigenvalues. There exists a spectral

decomposition of A:

$$A = \sum_k \lambda_k \left| k \right\rangle\!\left\langle k \right|, \tag{2.2}$$

where $\{\lambda_k\}_k$ are the eigenvalues corresponding to an orthonormal basis of eigenvectors $\{\left| k \right\rangle\}_k$ of A. The projection $\Pi(A)$ onto $\mathrm{supp}(A)$ is then

$$\Pi(A) = \sum_{k:\lambda_k \neq 0} \left| k \right\rangle\!\left\langle k \right|. \tag{2.3}$$

Let $\mathrm{rank}(A)$ denote the rank of A. If A is positive definite, i.e., $A > 0$, then $\mathrm{rank}(A) = \dim(\mathcal{H})$, $\Pi(A) = \mathbb{1}_{\mathcal{H}}$, and we say that the rank of A is full. If f is a real-valued function with domain $\mathrm{Dom}(f)$, then $f(A)$ is defined as

$$f(A) = \sum_{k:\lambda_k \in \mathrm{Dom}(f)} f(\lambda_k) \left| k \right\rangle\!\left\langle k \right|. \tag{2.4}$$

The Schatten p-norm of an operator $A \in \mathscr{B}(\mathcal{H})$ is defined as

$$\|A\|_p \equiv \left(\mathrm{Tr}\left\{|A|^p\right\}\right)^{\frac{1}{p}}, \tag{2.5}$$

where $|A| \equiv \sqrt{A^\dagger A}$ and $p \in [1, \infty)$. If $\{\sigma_i(A)\}_i$ are the singular values of A, then

$$\|A\|_p = \left[\sum_i \sigma_i(A)^p\right]^{\frac{1}{p}}. \tag{2.6}$$

$\|A\|_\infty := \lim_{p \to \infty} \|A\|_p$ is the largest singular value of A. Let $\mathscr{B}_p(\mathcal{H})$ be the subset of $\mathscr{B}(\mathcal{H})$ consisting of operators with finite Schatten p-norm. The Schatten p-norms are unitarily invariant norms.

Lemma 2.1 (Hölder's inequality [37–39]) *For all $A \in \mathscr{B}_p(\mathcal{H})$, $B \in \mathscr{B}_q(\mathcal{H})$, and $p, q \in [1, \infty]$ such that $\frac{1}{p} + \frac{1}{q} = 1$, it holds that*

$$|\langle A, B \rangle| = \left|\mathrm{Tr}\left\{A^\dagger B\right\}\right| \leq \|A\|_p \|B\|_q. \tag{2.7}$$

The following lemma can be found in [40, Corollary 5.2].

Lemma 2.2 Let $\mathcal{M} : \mathcal{B}_+(\mathcal{H}_A) \to \mathcal{B}_+(\mathcal{H}_B)$ be a linear, positive, and sub-unital map. Then, for all $\sigma_A \in \mathcal{B}_+(\mathcal{H}_A)$ it holds that

$$\mathcal{M}_{A \to B}(\log(\sigma_A)) \leq \log(\mathcal{M}_{A \to B}(\sigma_A)). \tag{2.8}$$

2.2.1 Derivatives of operator-valued functions

Here we recall [39, Theorem V.3.3].

If f is a continuously differentiable function on an open neighbourhood of the spectrum of some self-adjoint operator A, then its derivative $Df(A)$ at A is a linear superoperator and its action on an operator H is given by

$$Df(A)(H) = \sum_{\lambda, \eta} f^{[1]}(\lambda, \eta) P_A(\lambda) H P_A(\eta), \tag{2.9}$$

where $A = \sum_\lambda \lambda P_A(\lambda)$ is the spectral decomposition of A and $f^{[1]}$ is the first divided difference function.

If $t \mapsto A(t) \in \mathscr{B}_+(\mathcal{H})$ is a continuously differentiable function on an open interval in $\mathbb{R}$, with derivative $A' := \frac{\mathrm{d}A}{\mathrm{d}t}$, then

$$f'(A(t)) := \frac{\mathrm{d}}{\mathrm{d}t} f(A(t)) = Df(A)(A'(t)) = \sum_{\lambda, \eta} f^{[1]}(\lambda, \eta) P_{A(t)}(\lambda) A'(t) P_{A(t)}(\eta). \tag{2.10}$$

In particular, (2.10) implies the following:

$$\frac{\mathrm{d}}{\mathrm{d}t} \mathrm{Tr}\{f(A(t))\} = \mathrm{Tr}\{f'(A(t)) A'(t)\}, \tag{2.11}$$

$$\mathrm{Tr}\{B(t) f'(A(t))\} = \mathrm{Tr}\{B(t) f'(A(t)) A'(t)\}, \tag{2.12}$$

where $B(t)$ is assumed to commute with $A(t)$.

2.3 Quantum states and channels

The state of a quantum system A is represented by a density operator ρ_A, which is a positive semi-definite operator with unit trace. Let $\mathscr{D}(\mathcal{H}_A)$ denote the set of density operators, i.e., all

elements $\rho_A \in \mathscr{B}_+(\mathcal{H}_A)$ such that $\mathrm{Tr}\{\rho_A\} = 1$. The density operator of a composite system AB is defined as $\rho_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$, and the partial trace over A gives the reduced density operator for the system B, i.e., $\mathrm{Tr}_A\{\rho_{AB}\} = \rho_B$ such that $\rho_B \in \mathscr{D}(\mathcal{H}_B)$. A pure state ψ_A of a system A is a rank-one density operator in $\mathscr{D}(\mathcal{H}_A)$, and we write it as $\psi_A = |\psi\rangle\!\langle\psi|_A$ for a unit vector $|\psi\rangle_A \in \mathcal{H}_A$. A purification of a density operator ρ_A is a pure state ψ_{AE}^ρ such that $\mathrm{Tr}_E\{\psi_{AE}^\rho\} = \rho_A$, where E is called the purifying system. The maximally mixed state is denoted by $\pi_A := \mathbb{1}_A/|A| \in \mathcal{D}(\mathcal{H}_A)$.

It is known that there exists a Schmidt decomposition for any bipartite quantum system in a pure state. It means that any pure state $\psi_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$ can be expressed as

$$|\psi\rangle_{AB} = \sum_{i=0}^{d-1} \sqrt{p_i}|i\rangle_A|i\rangle_B, \tag{2.13}$$

such that $\{|i\rangle_A\}_i \in \mathrm{ONB}(\mathcal{H}_A)$, $\{|i\rangle_B\}_i \in \mathrm{ONB}(\mathcal{H}_B)$, $\sum_{i=0}^{d-1} p_i = 1$, and for all $i:\ 0 \le p_i \le 1$, where $d = \min\{|A|, |B|\}$.

Let $U_{A'E' \to AE}^{\hat{H}}$ be a unitary associated to a Hamiltonian $\hat{H}$, which governs the underlying interaction between an input subsystem A' and a bath E', to produce an output subsystem A for the observer and E for the bath. In general, the individual input systems A' and E' and the output systems A and E can have different dimensions. At an initial time, in the absence of an interaction Hamiltonian $\hat{H}$, the bath is in a fixed state $\tau_{E'}$ and the system A' has no correlation with the bath; i.e., the state of the composite system $A'E'$ is of the form $\omega_{A'} \otimes \tau_{E'}$, where $\omega_{A'E'}$ is the joint state of the systems A' and E'. Under the action of the interaction Hamiltonian $\hat{H}$, the state of the composite system transforms as

$$\rho_{AE} = U^{\hat{H}}(\omega_{A'} \otimes \tau_{E'})(U^{\hat{H}})^\dagger. \tag{2.14}$$

In the above interaction process, since the system E in (2.14) is inaccessible, the evolution of the system of interest is noisy in general. The noisy evolution of the system A' under the action of the interaction Hamiltonian $\hat{H}$ is represented by a completely positive, trace-preserving (CPTP)

map [41], called a quantum channel:

$$\mathcal{M}_{A'\to A}(\omega_{A'}) = \mathrm{Tr}_E\{U^{\hat{H}}(\omega_{A'} \otimes \tau_{E'})(U^{\hat{H}})^\dagger\}, \tag{2.15}$$

where system E represents inaccessible degrees of freedom. In particular, when the Hamiltonian $\hat{H}$ is such that there is no interaction between the system A' and the bath E', and $A' \simeq A$, then $\mathcal{M}$ corresponds to a unitary evolution, i.e., $\mathcal{M}(\cdot) = \mathcal{U}^{\hat{H}}(\cdot) := U^{\hat{H}}_{A'\to A}(\cdot)(U^{\hat{H}}_{A'\to A})^\dagger$. The weakly complementary channel $\widehat{\mathcal{M}}_{A'\to E}$ is given by

$$\widehat{\mathcal{M}}_{A'\to E}(\omega_{A'}) = \mathrm{Tr}_B\{U^{\hat{H}}(\omega_{A'} \otimes \tau_{E'})(U^{\hat{H}})^\dagger\}. \tag{2.16}$$

If we suppose that the state $\tau_{E'}$ of a bath system E' is pure, then $\widehat{\mathcal{M}}_{A'\to E}$ is called the complementary channel of $\mathcal{M}_{A'\to E}$.

A completely positive, trace non-increasing map is called a quantum sub-operation.

A CPTP map $\mathcal{N}_{A'B'\to AB} : \mathcal{B}_+(\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}) \to \mathcal{B}_+(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called a bipartite channel. A bipartite channel $\mathcal{N}_{A'B'\to AB}$ is also called bidirectional channel in the setting of communication protocols when pairs (A', A) and (B', B) of quantum systems are held by two spatially separated parties.

A memory cell $\{\mathcal{M}^x\}_{x\in\mathscr{X}}$ is defined to be a set of quantum channels $\mathcal{M}^x$, for all $x \in \mathscr{X}$, where $\mathscr{X}$ is an alphabet, and $\mathcal{M}^x : \mathcal{B}_+(\mathcal{H}_{A'}) \to \mathcal{B}_+(\mathcal{H}_A)$ for all $x \in \mathscr{X}$.

A quantum instrument is a collection $\{\mathcal{M}^x_{A'\to A}\}_{x\in\mathscr{X}}$ of quantum sub-operations, such that the sum map $\sum_x \mathcal{M}^x$ is a quantum channel. The action of a quantum instrument on an input operator $\rho_{A'}$ can be described in terms of the following quantum channel:

$$\rho_{A'} \mapsto \sum_{x\in\mathscr{X}} \mathcal{M}^x_{A'\to A}(\rho_A) \otimes |x\rangle\langle x|_X, \tag{2.17}$$

where $\{|x\rangle_X\}_x \in \mathrm{ONB}(\mathcal{H}_X)$ and X denotes a (classical) register that stores the classical output of the instrument.

The Choi–Jamiołkowski isomorphism represents a well known duality between channels and states. Let $\mathcal{M}_{A'\to A}$ be a quantum channel, and let $|\Upsilon\rangle_{R:A'}$ denote the following maximally entangled

vector:

$$|\Upsilon\rangle_{R:A'} := \sum_i |i\rangle_R |i\rangle_{A'}, \qquad (2.18)$$

where $|R| = |A'|$, and $\{|i\rangle_R\}_i \in \mathrm{ONB}(\mathcal{H}_R)$ and $\{|i\rangle_{A'}\}_i \in \mathrm{ONB}(\mathcal{H}_{A'})$ are fixed orthonormal bases, and $R : A'$ denotes a bipartite cut. Let us extend this notation to multiple parties with a given bipartite cut as

$$|\Upsilon\rangle_{R_A R_B : A' B'} := |\Upsilon\rangle_{R'_A : A'} \otimes |\Upsilon\rangle_{R_B : B'}. \qquad (2.19)$$

A maximally entangled state $\Phi_{RA'}$ is defined for a bipartite system $R : A'$ as

$$\Phi_{RA'} = \frac{1}{|A'|} |\Upsilon\rangle\langle\Upsilon|_{RA'}. \qquad (2.20)$$

The Choi operator for a channel $\mathcal{M}_{A' \to A}$ is defined as

$$J_{RA}^{\mathcal{M}} = (\mathrm{id}_R \otimes \mathcal{M}_{A' \to A}) \left(|\Upsilon\rangle\langle\Upsilon|_{RA'} \right), \qquad (2.21)$$

where id_R denotes the identity map on R. For $A' \simeq A$, the following identity holds

$$\langle\Upsilon|(\rho_{R_A A'} \otimes J_{RA}^{\mathcal{M}})|\Upsilon\rangle_{A':R} = \mathcal{M}_{A' \to A}(\rho_{R_A A'}), \qquad (2.22)$$

where $A' \simeq A$. The above identity can be understood in terms of a post-selected variant [42] of the quantum teleportation protocol [18]. Another identity that holds is

$$\langle\Upsilon|(Q_{R_A R} \otimes \mathbb{1}_A)|\Upsilon\rangle_{R:A} = \mathrm{Tr}_R\{Q_{R_A R}\}, \qquad (2.23)$$

for an operator $Q_{R_A R} \in \mathcal{B}(\mathcal{H}_{R_A} \otimes \mathcal{H}_R)$.

2.3.1   Separable and PPT: states and channels

For a fixed basis $\{|i\rangle_B\}_{i\in\mathscr{I}} \in \mathrm{ONB}(\mathcal{H}_B)$, the partial transpose T_B on the composite system AB is the following map:

$$(\mathrm{id}_A \otimes \mathrm{T}_B)\,(Q_{AB}) = \sum_{i,j\in\mathscr{I}} (\mathbb{1}_A \otimes |i\rangle\langle j|_B)\, Q_{AB}\, (\mathbb{1}_A \otimes |i\rangle\langle j|_B), \tag{2.24}$$

where $Q_{AB} \in \mathscr{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Note that the partial transpose is self-adjoint, i.e., $\mathrm{T}_B = \mathrm{T}_B^{\dagger}$ and is also involutory:

$$\mathrm{T}_B \circ \mathrm{T}_B = \mathbb{1}_B. \tag{2.25}$$

The following identity also holds:

$$\mathrm{T}_R(|\Upsilon\rangle\langle\Upsilon|_{RA}) = \mathrm{T}_A(|\Upsilon\rangle\langle\Upsilon|_{RA}). \tag{2.26}$$

Let $\mathrm{SEP}(A\!:\!B)$ denote the set of all separable states $\sigma_{AB} \in \mathscr{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, which are states that can be written as

$$\sigma_{AB} = \sum_{x\in\mathscr{X}} p_X(x)\omega_A^x \otimes \tau_B^x, \tag{2.27}$$

where $p_X(x)$ denotes a probability distribution corresponding to a random variable X associated with an alphabet $\mathscr{X}$, $\omega_A^x \in \mathscr{D}(\mathcal{H}_A)$, and $\tau_B^x \in \mathscr{D}(\mathcal{H}_B)$ for all $x \in \mathscr{X}$. This set is closed under the action of the partial transpose maps T_A and T_B [43,44]. Generalizing the set of separable states, we can define the set $\mathrm{PPT}(A\!:\!B)$ of all bipartite states $\rho_{AB} \in \mathscr{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ that remain positive after the action of the partial transpose T_B. A state $\rho_{AB} \in \mathrm{PPT}(A\!:\!B)$ is also called a PPT (positive under partial transpose) state. If a state is not PPT then it is called NPT (non-positive under partial transpose). We can define an even more general set of positive semi-definite operators [45] as follows:

$$\mathrm{PPT}'(A\!:\!B) := \{\sigma_{AB}:\ \sigma_{AB} \geq 0 \wedge \|\mathrm{T}_B(\sigma_{AB})\|_1 \leq 1\}. \tag{2.28}$$

We then have the containments $\mathrm{SEP} \subsetneq \mathrm{PPT} \subsetneq \mathrm{PPT}'$.

Lemma 2.3 ([46]) *For any $\sigma_{AB} \in \text{PPT}'(A:B)$, the following inequality holds*

$$\text{Tr}\{\Phi_{AB}\sigma_{AB}\} \leq \frac{1}{M},$$

(2.29)

where Φ_{AB} is a maximally entangled state of Schmidt rank M, i.e., $|A| = |B| = M$.

A bipartite quantum channel $\mathcal{P}_{A'B' \to AB}$ is a PPT-preserving channel if the map $\text{T}_B \circ \mathcal{P}_{A'B' \to AB} \circ \text{T}_{B'}$ is a quantum channel [46, 47]. A bipartite quantum channel $\mathcal{P}_{A'B' \to AB}$ is PPT-preserving if and only if its Choi state is a PPT state [47], i.e., $\frac{J^{\mathcal{P}}_{R_A R_B:AB}}{|R_A R_B|} \in \text{PPT}(R_A A: BR_B)$, where

$$\frac{J^{\mathcal{P}}_{R_A R_B:AB}}{|R_A R_B|} = \mathcal{P}_{A'B' \to AB}(\Phi_{R_A A'} \otimes \Phi_{B' R_B}).$$

(2.30)

A bipartite quantum channel $\mathcal{S}_{A'B' \to AB}$ is a separable channel if and only if its Choi state is a separable state [48], i.e, $\frac{J^{\mathcal{S}}_{R_A R_B:AB}}{|R_A R_B|} \in \text{SEP}(R_A A: BR_B)$, where

$$\frac{J^{\mathcal{S}}_{R_A R_B:AB}}{|R_A R_B|} = \mathcal{S}_{A'B' \to AB}(\Phi_{R_A A'} \otimes \Phi_{B' R_B}).$$

(2.31)

A 1W-LOCC (one-way local operations and classical communication) channel is a separable super-operator

$$\mathcal{L}^{\to}_{A'B' \to AB} = \sum_{y \in \mathscr{Y}} \mathcal{E}^y_{A' \to A} \otimes \mathcal{F}^y_{B' \to B},$$

(2.32)

where $\mathscr{Y}$ is an alphabet, $\{\mathcal{E}^y_{A \to A'}\}_{y \in \mathscr{Y}}$ is a set of CP maps such that the sum map $\sum_{y \in \mathscr{Y}} \mathcal{E}^y_{A \to A'}$ is trace preserving, while $\{\mathcal{F}^y_{B \to B'}\}_{y \in \mathscr{Y}}$ is a set of quantum channels. Whereas, an LOCC (local communication and classical operations) channels $\mathcal{L}_{AB \to A'B'}$ takes the form in (2.32) such that $\{\mathcal{E}^y_{A \to A'}\}_{y \in \mathscr{Y}}$ and $\{\mathcal{F}^y_{B \to B'}\}_{y \in \mathscr{Y}}$ are sets of completely positive (CP) maps such that $\mathcal{L}_{AB \to A'B'}$ is trace preserving. Thus, the LOCC channels are also separable super-operators, but the converse is not true. Note that any 1W-LOCC channel is also an LOCC channel and all LOCC channels are PPT-preserving.

2.4 Channels with symmetry

Consider a finite group $\mathscr{G}$ of size $|G|$. For every $g \in \mathscr{G}$, let $g \to U_A(g)$ and $g \to V_B(g)$ be projective unitary representations of g acting on the input space $\mathcal{H}_A$ and the output space $\mathcal{H}_B$ of a quantum channel $\mathcal{M}_{A \to B}$, respectively. A quantum channel $\mathcal{M}_{A \to B}$ is covariant with respect to these representations if the following relation is satisfied [27, 49]:

$$\forall \rho_A \in \mathscr{D}(\mathcal{H}_A) \text{ and } \forall g \in \mathscr{G}, \ \mathcal{M}_{A \to B}\left(U_A(g)\rho_A U_A^\dagger(g)\right) = V_B(g)\mathcal{M}_{A \to B}(\rho_A)V_B^\dagger(g). \tag{2.33}$$

Definition 2.1 (Covariant channel [27]) *A quantum channel is covariant if it is covariant with respect to a group $\mathscr{G}$ which has a representation $U(g)$, for all $g \in \mathscr{G}$, on $\mathcal{H}_A$ that is a unitary one-design; i.e., the map $\frac{1}{|G|}\sum_{g \in \mathscr{G}} U(g)(\cdot)U^\dagger(g)$ always outputs the maximally mixed state for all input states.*

For an isometric channel $\mathcal{U}_{A \to BE}^{\mathcal{M}}$ extending the covariant channel $\mathcal{M}_{A \to B}$ defined above, there exists a unitary representation $W_E(g)$ acting on the environment Hilbert space $\mathcal{H}_E$ [27], such that for all $g \in \mathscr{G}$,

$$\mathcal{U}_{A \to BE}^{\mathcal{M}}\left(U_A(g)\rho_A U_A^\dagger(g)\right) = (V_B(g) \otimes W_E(g))\left(\mathcal{U}_{A \to BE}^{\mathcal{M}}(\rho_A)\right)\left(V_B^\dagger(g) \otimes W_E^\dagger(g)\right). \tag{2.34}$$

We can restate this as the following lemma:

Lemma 2.4 ([27]) *Suppose that a channel $\mathcal{M}_{A \to B}$ is covariant with respect to a group $\mathscr{G}$. For an isometric extension $U_{A \to BE}^{\mathcal{M}}$ of $\mathcal{M}_{A \to B}$, there is a set of unitaries $\{W_E^g\}_{g \in \mathscr{G}}$ such that the following covariance holds for all $g \in \mathscr{G}$:*

$$U_{A \to BE}^{\mathcal{M}}U_A^g = (V_B^g \otimes W_E^g)\, U_{A \to BE}^{\mathcal{M}}. \tag{2.35}$$

Proof. For convenience, we discuss a proof of this lemma presented in [31, Appendix A].

Given is a group $\mathscr{G}$ and a quantum channel $\mathcal{M}_{A \to B}$ that is covariant in the following sense:

$$\mathcal{M}_{A \to B}(U_A^g \rho_A U_A^{g\dagger}) = V_B^g \mathcal{M}_{A \to B}(\rho_A)V_B^{g\dagger}, \tag{2.36}$$

21

for a set of unitaries $\{U_A^g\}_{g \in \mathcal{G}}$ and $\{V_B^g\}_{g \in \mathcal{G}}$.

Let a Kraus representation of $\mathcal{M}_{A \to B}$ be given as

$$\mathcal{M}_{A \to B}(\rho_A) = \sum_j L^j \rho_A L^{j\dagger}. \tag{2.37}$$

We can rewrite (2.36) as

$$V_B^{g\dagger} \mathcal{M}_{A \to B}(U_A^g \rho_A U_A^{g\dagger}) V_B^g = \mathcal{M}_{A \to B}(\rho_A), \tag{2.38}$$

which means that for all g, the following equality holds

$$\sum_j L^j \rho_A L^{j\dagger} = \sum_j V_B^{g\dagger} L^j U_A^g \rho_A \left(V_B^{g\dagger} L^j U_A^g\right)^\dagger. \tag{2.39}$$

Thus, the channel has two different Kraus representations $\{L^j\}_j$ and $\{V_B^{g\dagger} L^j U_A^g\}_j$, and these are necessarily related by a unitary with matrix elements w_{jk}^g [23, 26]:

$$V_B^{g\dagger} L^j U_A^g = \sum_k w_{jk}^g L^k. \tag{2.40}$$

A canonical isometric extension $U_{A \to BE}^{\mathcal{M}}$ of $\mathcal{M}_{A \to B}$ is given as

$$U_{A \to BE}^{\mathcal{M}} = \sum_j L^j \otimes |j\rangle_E, \tag{2.41}$$

where $\{|j\rangle_E\}_j$ is an orthonormal basis. Defining W_E^g as the following unitary

$$W_E^g |k\rangle_E = \sum_j w_{jk}^g |j\rangle_E, \tag{2.42}$$

where the states $|k\rangle_E$ are chosen from $\{|j\rangle_E\}_j$, consider that

$$U_{A \to BE}^{\mathcal{M}} U_A^g = \sum_j L^j U_A^g \otimes |j\rangle_E = \sum_j V_B^g V_B^{g\dagger} L^j U_A^g \otimes |j\rangle_E = \sum_j V_B^g \left[\sum_k w_{jk}^g L^k\right] \otimes |j\rangle_E$$

$$= V_B^g \sum_k L^k \otimes \sum_j w_{jk}^g |j\rangle_E = V_B^g \sum_k L^k \otimes W_E^g |k\rangle_E = (V_B^g \otimes W_E^g) U_{A \to BE}^{\mathcal{M}}. \tag{2.43}$$

This concludes the proof. ∎

Definition 2.2 (Teleportation-simulable [50, 51]) *A channel $\mathcal{M}_{A \to B}$ is teleportation-simulable with an associated resource state if for all $\rho_A \in \mathscr{D}(\mathcal{H}_A)$ there exists a resource state $\omega_{R_A B} \in \mathscr{D}(\mathcal{H}_{R_A B})$ such that*

$$\mathcal{M}_{A \to B}(\rho_A) = \mathcal{L}_{R_A AB \to B}(\rho_A \otimes \omega_{R_A B}), \tag{2.44}$$

where $\mathcal{L}_{R_A AB \to B}$ is an LOCC channel acting on $R_A A:B$. A particular example of an LOCC channel could be a generalized teleportation protocol [52].

One can find the defining equation (2.44) explicitly stated as [51, Eq. (11)]. All covariant channels, as given in Definition 2.1, are teleportation-simulable with respect to a resource state $\mathcal{M}_{A \to B}(\Phi_{R_A A})$ [53].

Definition 2.3 (PPT-simulable [54]) *A channel $\mathcal{M}_{A \to B}$ is PPT-simulable with an associated resource state if for all $\rho_A \in \mathscr{D}(\mathcal{H}_A)$ there exists a resource state $\omega_{R_A B} \in \mathscr{D}(\mathcal{H}_{R_A B})$ such that*

$$\mathcal{M}_{A \to B}(\rho_A) = \mathcal{P}_{R_A AB \to B}(\rho_A \otimes \omega_{R_A B}), \tag{2.45}$$

where $\mathcal{P}_{L_A AB \to B}$ is a PPT-preserving channel acting on $R_A A:B$, where the transposition map is with respect to the system B.

Definition 2.4 (Jointly covariant memory cell [34]) *A set $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{M}^x_{A \to B}\}_{x \in \mathscr{X}}$ of quantum channels is jointly covariant if there exists a group $\mathscr{G}$ such that for all $x \in \mathscr{X}$, the channel $\mathcal{M}^x$ is a covariant channel with respect to the group $\mathscr{G}$ (cf., Definition 2.1).*

Remark 2.1 ([34]) *Any jointly covariant memory cell $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{M}^x_{A \to B}\}_{x \in \mathscr{X}}$ is jointly teleportation-simulable with respect to the set $\{\mathcal{M}^x_{A \to B}(\Phi_{R_A A})\}_{x \in \mathscr{X}}$ of resource states.*

2.5 Entropies and information

The von Neumann entropy of a density operator ρ_A is defined as [28]

$$S(A)_\rho := S(\rho_A) = -\operatorname{Tr}\{\rho_A \log_2 \rho_A\}. \tag{2.46}$$

The conditional quantum entropy $S(A|B)_\rho$ of a density operator ρ_{AB} of a composite system AB is defined as

$$S(A|B)_\rho := S(AB)_\rho - S(B)_\rho. \tag{2.47}$$

The coherent information $I(A\rangle B)_\rho$ of a density operator ρ_{AB} is defined as [55]

$$I(A\rangle B)_\rho := -S(A|B)_\rho = S(B)_\rho - S(AB)_\rho. \tag{2.48}$$

The quantum relative entropy of two quantum states is a measure of their distinguishability. For $\rho \in \mathscr{D}(\mathcal{H})$ and $\sigma \in \mathscr{B}_+(\mathcal{H})$, it is defined as [56]

$$D(\rho\|\sigma) := \begin{cases} \mathrm{Tr}\{\rho[\log_2 \rho - \log_2 \sigma]\}, & \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ +\infty, & \text{otherwise.} \end{cases} \tag{2.49}$$

The quantum relative entropy is non-increasing under the action of positive trace-preserving maps [57], which is the statement that $D(\rho\|\sigma) \geq D(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$ for any two density operators ρ and σ and a positive trace-preserving map $\mathcal{M}$ (this inequality applies to quantum channels as well [58], since every completely positive map is also a positive map by definition).

The quantum mutual information $I(A;B)_\rho$ is a measure of correlation between quantum systems A and B in the state ρ_{AB}. It is defined as

$$I(A;B)_\rho := \inf_{\sigma_A \in \mathscr{D}(\mathcal{H}_A)} D(\rho_{AB}\|\rho_A \otimes \sigma_B) = S(A)_\rho + S(B)_\rho - S(AB)_\rho. \tag{2.50}$$

The conditional quantum mutual information $I(A;B|C)_\rho$ of a tripartite density operator ρ_{ABC} is defined as

$$I(A;B|C)_\rho := S(A|C)_\rho + S(B|C)_\rho - S(AB|C)_\rho. \tag{2.51}$$

It is known that quantum entropy, quantum mutual information, and conditional quantum mutual information are all non-negative quantities (see [59, 60]).

The following AFW inequality gives uniform continuity bounds for conditional entropy:

Lemma 2.5 ([61, 62]) *Let $\rho_{AB}, \sigma_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$. Suppose that $\frac{1}{2}\|\rho_{AB} - \sigma_{AB}\|_1 \leq \varepsilon$, where $\varepsilon \in [0, 1]$. Then*

$$|S(A|B)_\rho - S(A|B)_\sigma| \leq 2\varepsilon \log_2 \dim(\mathcal{H}_A) + (1 + \varepsilon) h_2 \left(\frac{\varepsilon}{1 + \varepsilon} \right), \tag{2.52}$$

where $h_2(\varepsilon)$ denotes binary entropy function:

$$h_2(\varepsilon) := -\varepsilon \log_2 \varepsilon - (1 - \varepsilon) \log_2(1 - \varepsilon). \tag{2.53}$$

If system B is a classical register X such that ρ_{XA} and σ_{XA} are classical-quantum (cq) states of the following form:

$$\rho_{XA} = \sum_{x \in \mathcal{X}} p_X(x)|x\rangle\langle x|_X \otimes \rho_A^x, \quad \sigma_{XA} = \sum_{x \in \mathcal{X}} q_X(x)|x\rangle\langle x|_X \otimes \sigma_A^x, \tag{2.54}$$

where $\{|x\rangle_X\}_{x \in \mathcal{X}} \in \mathrm{ONB}(\mathcal{H}_X)$ and $\forall x \in \mathcal{X}: \rho_A^x, \sigma_A^x \in \mathcal{D}(\mathcal{H}_A)$, then

$$|S(X|A)_\rho - S(X|A)_\sigma| \leq \varepsilon \log_2 \dim(\mathcal{H}_X) + g(\varepsilon), \tag{2.55}$$

$$|S(A|X)_\rho - S(A|X)_\sigma| \leq \varepsilon \log_2 \dim(\mathcal{H}_A) + g(\varepsilon). \tag{2.56}$$

2.6 Generalized divergences

A quantity is called a generalized divergence [63, 64] if it satisfies the following monotonicity (data-processing) inequality for all density operators $\rho \in \mathscr{D}(\mathcal{H}')$ and $\sigma \in \mathscr{D}(\mathcal{H}')$ and quantum channels $\mathcal{M} : \mathscr{B}_+(\mathcal{H}') \to \mathscr{B}_+(\mathcal{H})$:

$$\mathbf{D}(\rho\|\sigma) \geq \mathbf{D}(\mathcal{M}(\rho)\|\mathcal{M}(\sigma)). \tag{2.57}$$

As a direct consequence of the above inequality, any generalized divergence satisfies the following two properties for an isometry U and a state τ [65]:

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(U\rho U^\dagger\|U\sigma U^\dagger), \tag{2.58}$$

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(\rho \otimes \tau\|\sigma \otimes \tau). \tag{2.59}$$

One can define a generalized mutual information for a quantum state ρ_{AB} as

$$I_{\mathbf{D}}(A;B)_\rho := \inf_{\sigma_B \in \mathscr{D}(\mathcal{H}_B)} \mathbf{D}(\rho_{AB}\|\rho_A \otimes \sigma_B). \tag{2.60}$$

The sandwiched Rényi relative entropy [65,66] is denoted as $\widetilde{D}_\alpha(\rho\|\sigma)$ and defined for $\rho \in \mathscr{D}(\mathcal{H})$, $\sigma \in \mathscr{B}_+(\mathcal{H})$, and $\forall \alpha \in (0,1) \cup (1,\infty)$ as

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1} \log_2 \operatorname{Tr}\left\{\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right\}, \tag{2.61}$$

but it is set to $+\infty$ for $\alpha \in (1,\infty)$ if $\operatorname{supp}(\rho) \nsubseteq \operatorname{supp}(\sigma)$. The sandwiched Rényi relative entropy obeys the following "monotonicity in α" inequality [66]:

$$\widetilde{D}_\alpha(\rho\|\sigma) \leq \widetilde{D}_\beta(\rho\|\sigma) \text{ if } \alpha \leq \beta, \text{ for } \alpha, \beta \in (0,1) \cup (1,\infty). \tag{2.62}$$

The following lemma states that the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ is a particular generalized divergence for certain values of α.

Lemma 2.6 ([67, 68]) *Let $\mathcal{M}_{A'\to A}$ be a quantum channel and let $\rho_{A'} \in \mathscr{D}(\mathcal{H}_{A'})$ and $\sigma_{A'} \in \mathscr{B}_+(\mathcal{H}_{A'})$. Then,*

$$\widetilde{D}_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\mathcal{M}(\rho)\|\mathcal{M}(\sigma)), \ \forall \alpha \in [1/2, 1) \cup (1,\infty). \tag{2.63}$$

In the limit $\alpha \to 1$, the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ converges to the quantum relative entropy [65, 66]:

$$\lim_{\alpha\to 1} \widetilde{D}_\alpha(\rho\|\sigma) := D_1(\rho\|\sigma) = D(\rho\|\sigma). \tag{2.64}$$

In the limit $\alpha \to \infty$, the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ converges to the max-relative entropy [66], which is defined as [69, 70]

$$D_{\max}(\rho\|\sigma) = \inf\{\lambda : \ \rho \leq 2^\lambda \sigma\}, \tag{2.65}$$

and if $\operatorname{supp}(\rho) \nsubseteq \operatorname{supp}(\sigma)$ then $D_{\max}(\rho\|\sigma) = \infty$.

The sandwiched Rényi mutual information $\widetilde{I}_\alpha(R; B)_\rho$ is defined as [68, 71]

$$\widetilde{I}_\alpha(R; B)_\rho := \min_{\sigma_B} \widetilde{D}_\alpha(\rho_{RB} \| \rho_R \otimes \sigma_B). \tag{2.66}$$

Another generalized divergence is the ε-hypothesis-testing divergence [72, 73], defined as

$$D_h^\varepsilon(\rho \| \sigma) := -\log_2 \inf_\Lambda \{ \mathrm{Tr}\{\Lambda \sigma\} : \ 0 \leq \Lambda \leq \mathbb{1} \wedge \mathrm{Tr}\{\Lambda \rho\} \geq 1 - \varepsilon \}, \tag{2.67}$$

for $\varepsilon \in [0, 1]$, $\rho \in \mathscr{D}(\mathcal{H})$, and $\sigma \in \mathscr{B}_+(\mathcal{H})$.

The following lemma follows directly from the statement of [74, Theorem III.1].

Lemma 2.7 ([74]) *Let $\rho_A \in \mathscr{D}(\mathcal{H}_A)$, and positive semidefinite operators $\sigma \in \mathscr{B}_+(\mathcal{H}_B), \sigma' \in \mathscr{B}_+(\mathcal{H}_A)$, the following inequality holds for any positive trace-preserving map $\mathcal{M}_{A \to B}$*

$$D_{\max}(\mathcal{M}(\rho) \| \sigma) \leq D_{\max}(\rho \| \sigma') + D_{\max}(\mathcal{M}(\sigma') \| \sigma). \tag{2.68}$$

Some other examples of generalized divergences are the trace distance and the fidelity. The trace distance between two density operators $\rho, \sigma \in \mathscr{D}(\mathcal{H})$ is equal to $\|\rho - \sigma\|_1$, where $\|T\|_1 = \mathrm{Tr}\{\sqrt{T^\dagger T}\}$. The fidelity of $\tau, \sigma \in \mathcal{B}_+(\mathcal{H})$, which is defined as $F(\tau, \sigma) = \|\sqrt{\tau}\sqrt{\sigma}\|_1^2$ [75], is also a generalized divergence.

Lemma 2.8 (Uhlmann's theorem [75]) *The following two expressions for fidelity between two states ρ_A and σ_A are equal:*

$$F(\rho_A, \sigma_A) = \max_U |\langle \varphi^\rho |_{RA} U_R \otimes \mathbb{1}_A |\varphi_{RA}^\sigma \rangle|^2 = \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2, \tag{2.69}$$

where U_R is a unitary operator and φ_{RA}^ω denotes purification of any $\omega_A \in \mathcal{D}(\mathcal{H}_{RA})$.

The following well known lemma establishes relations between fidelity and trace distance.

Lemma 2.9 ([76]) *For any two density operators $\rho, \sigma \in \mathscr{D}(\mathcal{H})$, the following bounds hold*

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)}. \tag{2.70}$$

Another well known lemma that establishes relation between the relative entropy and trace distance is as follows.

Lemma 2.10 (Pinsker's inequality [77]) *For any two density operators $\rho, \sigma \in \mathscr{D}(\mathcal{H})$, following bounds hold*

$$D(\rho \| \sigma) \geq \frac{1}{2 \ln 2} \| \rho - \sigma \|_1^2, \tag{2.71}$$

where $\ln$ *denotes natural logarithm.*

2.7   Private states and privacy test

Private states [78, 79] are an essential notion in any discussion of secret key distillation in quantum information, and we review their basics here.

A tripartite key state $\gamma_{K_A K_B E}$ contains $\log_2 |K|$ bits of secret key, shared between systems K_A and K_B and protected from an eavesdropper possessing system E, if there exists a state $\sigma_E \in \mathscr{D}(\mathcal{H}_E)$ and a projective measurement channel $\mathcal{M}(\cdot) = \sum_i |i\rangle\langle i| (\cdot) |i\rangle\langle i|$, where $\{|i\rangle\}_i \in \text{ONB}$, such that

$$(\mathcal{M}_{K_A} \otimes \mathcal{M}_{K_B}) (\gamma_{K_A K_B E}) = \frac{1}{|K|} \sum_{i=0}^{K-1} |i\rangle\langle i|_{K_A} \otimes |i\rangle\langle i|_{K_B} \otimes \sigma_E. \tag{2.72}$$

The systems K_A and K_B are maximally classically correlated, and the key value is uniformly random and independent of the system E.

A bipartite private state $\gamma_{S_A K_A K_B S_B}$ containing $\log_2 |K|$ bits of secret key has the following form:

$$\gamma_{S_A K_A K_B S_B} := U_{S_A K_A K_B S_B}^t (\Phi_{K_A K_B} \otimes \theta_{R_A R_B}) (U_{S_A K_A K_B S_B}^t)^\dagger, \tag{2.73}$$

where $\Phi_{K_A K_B}$ is a maximally entangled state of Schmidt rank $|K|$, $U_{S_A K_A K_B S_B}^t$ is a "twisting" unitary of the form

$$U_{S_A K_A K_B S_B}^t := \sum_{i,j=0}^{K-1} |i\rangle\langle i|_{K_A} \otimes |j\rangle\langle j|_{K_B} \otimes U_{S_A S_B}^{ij}, \tag{2.74}$$

with each $U_{S_A S_B}^{ij}$ a unitary, and $\theta_{S_A S_B}$ is a state. The systems S_A, S_B are called " shield" systems because they, along with the twisting unitary, can help to protect the key in systems K_A and K_B from any party possessing a purification of $\gamma_{S_A K_A K_B S_B}$.

Bipartite private states and tripartite key states are equivalent [78, 79]. That is, for $\gamma_{S_A K_A K_B S_B}$ a bipartite private state and $\gamma_{S_A K_A K_B S_B E} \in \mathcal{H}_{S_A} \otimes \mathcal{H}_{K_A} \otimes \mathcal{H}_{K_B} \otimes \mathcal{H}_{S_B} \otimes \mathcal{E}$ some purification of it, $\gamma_{K_A K_B E}$ is a tripartite key state. Conversely, for any tripartite key state $\gamma_{K_A K_B E}$ and any purification $\gamma_{S_A K_A K_B S_B E}$ of it, $\gamma_{S_A K_A K_B S_B}$ is a bipartite private state.

A state $\rho_{K_A K_B E}$ is an ε-approximate tripartite key state if there exists a tripartite key state $\gamma_{K_A K_B E}$ such that

$$F(\rho_{K_A K_B E}, \gamma_{K_A K_B E}) \geq 1 - \varepsilon, \tag{2.75}$$

where $\varepsilon \in [0, 1]$. Similarly, a state $\rho_{S_A K_A K_B S_B}$ is an ε-approximate bipartite private state if there exists a bipartite private state $\gamma_{S_A K_A K_B S_B}$ such that

$$F(\rho_{S_A K_A K_B S_B E}, \gamma_{S_A K_A K_B S_B E}) \geq 1 - \varepsilon. \tag{2.76}$$

If $\rho_{S_A K_A K_B S_B}$ is an ε-approximate bipartite key state with K key values, then Alice and Bob hold an ε-approximate tripartite key state with $|K|$ key values, and the converse is true as well [78, 79].

A privacy test corresponding to $\gamma_{S_A K_A K_B S_B}$ (a γ-privacy test) is defined as the following dichotomic measurement [80]:

$$\{\Pi^\gamma_{S_A K_A K_B S_B}, \mathbb{1}_{S_A K_A K_B S_B} - \Pi^\gamma_{S_A K_A K_B S_B}\}, \tag{2.77}$$

where

$$\Pi^\gamma_{S_A K_A K_B S_B} := U^t_{S_A K_A K_B S_B}(\Phi_{K_A K_B} \otimes \mathbb{1}_{S_A S_B})(U^t_{S_A K_A K_B S_B})^\dagger, \tag{2.78}$$

$\mathbb{1}_{S_A S_B} \in \mathcal{B}_+(\mathcal{H}_{S_A S_B})$ is the identity operator, and $U^t_{S_A K_A K_B S_B}$ is the twisting unitary discussed earlier. Let $\varepsilon \in [0, 1]$ and $\rho_{S_A K_A K_B S_B}$ be an ε-approximate bipartite private state. The probability for $\rho_{S_A K_A K_B S_B}$ to pass the γ-privacy test is never smaller than $1 - \varepsilon$ [80]:

$$\mathrm{Tr}\{\Pi^\gamma_{S_A K_A K_B S_B}\rho_{S_A K_A K_B S_B}\} \geq 1 - \varepsilon. \tag{2.79}$$

For a state $\sigma_{S_A K_A K_B S_B} \in \mathrm{SEP}(S_A K_A : K_B S_B)$, the probability of passing any γ-privacy test is never

greater than $\frac{1}{|K|}$ [79]:

$$\mathrm{Tr}\{\Pi^{\gamma}_{S_A K_A K_B S_B} \sigma_{S_A K_A K_B S_B}\} \leq \frac{1}{|K|}, \tag{2.80}$$

where $|K|$ is the number of values that the secret key can take (i.e., $|K| = \dim(\mathcal{H}_{K_A}) = \dim(\mathcal{H}_{K_B})$). These two inequalities are foundational for some of the converse bounds established in this thesis, as was the case in [79, 80].

2.8 Entanglement measures

Let $\mathrm{Ent}(A; B)_{\rho}$ denote an entanglement measure [81] that is evaluated for a bipartite state ρ_{AB}. The basic property of an entanglement measure is that it should be an LOCC monotone [81], i.e., non-increasing under the action of an LOCC channel.

Entanglement distillation from a bipartite state ρ_{AB} is the task of distilling a maximally entangled state Φ_{AB} of Schmidt rank $|M|$ from (asymptotically) large number of independent and identically distributed copies of ρ_{AB}, i.e., $\rho_{AB}^{\otimes n}$ for $n \to \infty$ via standard LOCC distillation protocols [82, 83]. A state ρ_{AB} is entanglement distillable if $\mathrm{Tr}\{\Phi_{AB} \rho_{AB}\} \geq \frac{1}{|M|}$ [82, 83].

There are different entanglement measures based on characteristic properties of entangled states. These properties are associated to the ability of how useful these entangled states are for specific information processing tasks, such as entanglement and secret-key distillation. It is known that all entangled states are useful for distilling secret key. However, there exists class of entangled states called bound entangled states that are not entanglement distillable.

Given such an entanglement measure $\mathrm{Ent}(A; B)_{\rho}$, one can define the entanglement $\mathrm{Ent}(\mathcal{M})$ of a channel $\mathcal{M}_{A \to B}$ in terms of it by optimizing over all pure, bipartite states that can be input to the channel:

$$\mathrm{Ent}(\mathcal{M}) = \sup_{\psi_{RA}} \mathrm{Ent}(R; B)_{\omega}, \tag{2.81}$$

where $\omega_{RB} = \mathcal{M}_{A \to B}(\psi_{RA})$. Due to the properties of an entanglement measure and the well known Schmidt decomposition theorem, it suffices to optimize over pure states ψ_{RA} such that $R \simeq A$ (i.e., one does not achieve a higher value of $\mathrm{Ent}(\mathcal{M})$ by optimizing over mixed states with unbounded reference system R). In an information-theoretic setting, the entanglement $\mathrm{Ent}(\mathcal{M})$ of a channel $\mathcal{M}$ characterizes the amount of entanglement that a sender A and receiver B can generate by using the channel if they do not share entanglement prior to its use.

30

Alternatively, one can consider the amortized entanglement $\text{Ent}_A(\mathcal{M})$, also called the entangling power, of a channel $\mathcal{M}_{A \to B}$ as the following optimization [54, 84] (see also [74, 85–87]):

$$\text{Ent}_A(\mathcal{M}) := \sup_{\rho_{R_A A R_B}} \left[\text{Ent}(R_A; B R_B)_\tau - \text{Ent}(R_A A; R_B)_\rho \right], \tag{2.82}$$

where $\tau_{R_A B R_B} = \mathcal{M}_{A \to B}(\rho_{R_A A R_B})$ and $\rho_{R_A A R_B} \in \mathscr{D}(\mathcal{H}_{R_A A R_B})$. The supremum is with respect to all states $\rho_{R_A A R_B}$ and the systems R_A, R_B are finite-dimensional but could be arbitrarily large. Thus, in general, $\text{Ent}_A(\mathcal{M})$ need not be computable. The amortized entanglement quantifies the net amount of entanglement that can be generated by using the channel $\mathcal{M}_{A \to B}$, if the sender and the receiver are allowed to begin with some initial entanglement in the form of the state $\rho_{R_A A R_B}$. That is, $\text{Ent}(R_A A; R_B)_\rho$ quantifies the entanglement of the initial state $\rho_{R_A A R_B}$, and $\text{Ent}(R_A; B R_B)_\tau$ quantifies the entanglement of the final state produced after the action of the channel.

Recently, it was shown in [54], connected to related developments in [34, 74, 84–86], that the amortized entanglement of a point-to-point channel $\mathcal{M}_{A \to B}$ serves as an upper bound on the entanglement of the final state, say ω_{AB}, generated at the end of an LOCC- or PPT-assisted quantum communication protocol that uses $\mathcal{M}_{A \to B}$ n times:

$$\text{Ent}(A; B)_\omega \leq n \, \text{Ent}_A(\mathcal{M}). \tag{2.83}$$

Thus, the physical question of determining meaningful upper bounds on the LOCC- or PPT-assisted capacities of point-to-point channel $\mathcal{M}$ is equivalent to the mathematical question of whether amortization can enhance the entanglement of a given channel, i.e., whether the following equality holds for a given entanglement measure Ent:

$$\text{Ent}_A(\mathcal{M}) \overset{?}{=} \text{Ent}(\mathcal{M}). \tag{2.84}$$

The Rains relative entropy of a state ρ_{AB} is defined as [45, 47]

$$R(A; B)_\rho := \min_{\sigma_{AB} \in \text{PPT}'(A:B)} D(\rho_{AB} \| \sigma_{AB}), \tag{2.85}$$

and it is monotone non-increasing under the action of a PPT-preserving quantum channel $\mathcal{P}_{A'B'\to AB}$, i.e.,

$$R(A';B')_\rho \geq R(A;B)_\omega, \tag{2.86}$$

where $\omega_{AB} = \mathcal{P}_{A'B'\to AB}(\rho_{A'B'})$. The sandwiched Rains relative entropy of a state ρ_{AB} is defined as follows [88]:

$$\widetilde{R}_\alpha(A;B)_\rho := \min_{\sigma_{AB}\in\text{PPT}'(A:B)} \widetilde{D}_\alpha(\rho_{AB}\|\sigma_{AB}). \tag{2.87}$$

The max-Rains relative entropy of a state ρ_{AB} is defined as [89]

$$R_{\max}(A;B)_\rho := \min_{\sigma_{AB}\in\text{PPT}'(A:B)} D_{\max}(\rho_{AB}\|\sigma_{AB}). \tag{2.88}$$

The max-Rains information of a quantum channel $\mathcal{M}_{A\to B}$ is defined as [90]

$$R_{\max}(\mathcal{M}) := \max_{\phi_{RA}} R_{\max}(R;B)_\omega, \tag{2.89}$$

where $\omega_{RB} = \mathcal{M}_{A\to B}(\phi_{RA})$ and ϕ_{RA} is a pure state, with $\dim(\mathcal{H}_R) = \dim(\mathcal{H}_A)$. The amortized max-Rains information of a channel $\mathcal{M}_{A\to B}$, denoted as $R_{\max,A}(\mathcal{M})$, is defined by replacing Ent in (2.82) with the max-Rains relative entropy $R_{\max}$ [91]. It was shown in [91] that amortization does not enhance the max-Rains information of an arbitrary point-to-point channel, i.e.,

$$R_{\max,A}(\mathcal{M}) = R_{\max}(\mathcal{M}). \tag{2.90}$$

Recently, in [92, Eq. (8)] (see also [90]), the max-Rains relative entropy of a state ρ_{AB} was expressed as

$$R_{\max}(A;B)_\rho = \log_2 W(A;B)_\rho, \tag{2.91}$$

where $W(A; B)_\rho$ is the solution to the following semi-definite program:

$$\text{minimize} \quad \text{Tr}\{C_{AB} + D_{AB}\}$$

$$\text{subject to} \quad C_{AB}, D_{AB} \geq 0,$$

$$\text{T}_B(C_{AB} - D_{AB}) \geq \rho_{AB}. \tag{2.92}$$

Similarly, in [90, Eq. (21)], the max-Rains information of a quantum channel $\mathcal{M}_{A \rightarrow B}$ was expressed as

$$R_{\max}(\mathcal{M}) = \log \Gamma(\mathcal{M}), \tag{2.93}$$

where $\Gamma(\mathcal{M})$ is the solution to the following semi-definite program (SDP):

$$\text{minimize} \quad \|\text{Tr}_B\{V_{RB} + Y_{RB}\}\|_\infty$$

$$\text{subject to} \quad Y_{RB}, V_{RB} \geq 0,$$

$$\text{T}_B(V_{RB} - Y_{RB}) \geq J_{RB}^{\mathcal{M}}. \tag{2.94}$$

The sandwiched relative entropy of entanglement of a bipartite state ρ_{AB} is defined as [80]

$$\widetilde{E}_\alpha(A; B)_\rho := \min_{\sigma_{AB} \in \text{SEP}(A:B)} \widetilde{D}_\alpha(\rho_{AB} \| \sigma_{AB}). \tag{2.95}$$

In the limit $\alpha \rightarrow 1$, $\widetilde{E}_\alpha(A; B)_\rho$ converges to the relative entropy of entanglement [93], i.e.,

$$\lim_{\alpha \rightarrow 1} \widetilde{E}_\alpha(A; B)_\rho = E(A; B)_\rho := \min_{\sigma_{AB} \in \text{SEP}(A:B)} D(\rho_{AB} \| \sigma_{AB}). \tag{2.96}$$

The max-relative entropy of entanglement [69, 70] is defined for a bipartite state ρ_{AB} as

$$E_{\max}(A; B)_\rho := \min_{\sigma_{AB} \in \text{SEP}(A:B)} D_{\max}(\rho_{AB} \| \sigma_{AB}). \tag{2.97}$$

The max-relative entropy of entanglement $E_{\max}(\mathcal{M})$ of a channel $\mathcal{M}_{A \rightarrow B}$ is defined as in (2.81), by replacing Ent with $E_{\max}$ [74]. It was shown in [74] that amortization does not increase max-relative

entropy of entanglement of a channel $\mathcal{M}_{A \to B}$, i.e.,

$$E_{\mathrm{max},A}(\mathcal{M}) = E_{\mathrm{max}}(\mathcal{M}). \tag{2.98}$$

The squashed entanglement of a state $\rho_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$ is defined as [36] (see also [94, 95]):

$$E_{\mathrm{sq}}(A;B)_{\rho} = \frac{1}{2} \inf_{\omega_{ABE}} \left\{ I(A;B|E)_{\omega} : \mathrm{Tr}_E\{\omega_{ABE}\} = \rho_{AB} \wedge \omega_{ABE} \in \mathcal{D}\left(\mathcal{H}_{ABE}\right) \right\}. \tag{2.99}$$

In general, the system E is finite-dimensional, but can be arbitrarily large. We can directly infer from the above definition that $E_{\mathrm{sq}}(B;A)_{\rho} = E_{\mathrm{sq}}(A;B)_{\rho}$ for any $\rho_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$. We can similarly define the squashed entanglement $E_{\mathrm{sq}}(\mathcal{M})$ of a channel $\mathcal{M}_{A \to B}$ [96], and it is known that amortization does not increase the squashed entanglement of a channel [96]:

$$E_{\mathrm{sq},A}(\mathcal{M}) = E_{\mathrm{sq}}(\mathcal{M}). \tag{2.100}$$

2.8.1 Approximate normalization of entanglement measures

Now we briefly discuss normalization properties of some entanglement measures, namely, entropy of entanglement [35] and squashed entanglement [36][4].

Squashed Entanglement

We know that squashed entanglement obeys the normalization property; i.e., it is equal to $\log_2 d$ for a maximally entangled state Φ_{AB} of Schmidt rank d [36]. Due to the continuity of squashed entanglement [61], we even know that if the state ρ_{AB} is approximately close to a maximally entangled state Φ_{AB}, then the squashed entanglement is near to $\log_2 d$ (see also [36, Remark 11]). In particular,

$$\frac{1}{2} \|\rho_{AB} - \Phi_{AB}\|_1 \le \varepsilon \tag{2.101}$$

---

[4]This section is based on an unpublished work with Mark M. Wilde.

implies that [61, 62, 97]

$$\left| E_{\mathrm{sq}}\left(A;B\right)_{\rho} - E_{\mathrm{sq}}\left(A;B\right)_{\Phi} \right| \leq \sqrt{2\varepsilon}\log_2 d + (1 + \sqrt{2\varepsilon})h_2\left(\frac{\sqrt{2\varepsilon}}{1 + \sqrt{2\varepsilon}}\right), \qquad (2.102)$$

where d is Schmidt rank of Φ_{AB} and $h_2(\cdot)$ is defined in (2.53). From (2.102), we get

$$E_{\mathrm{sq}}\left(A;B\right)_{\rho} \geq (1 - \sqrt{2\varepsilon})\log_2 d - (1 + \sqrt{2\varepsilon})h_2\left(\frac{\sqrt{2\varepsilon}}{1 + \sqrt{2\varepsilon}}\right). \qquad (2.103)$$

Our statement here is about the converse situation. We show that

$$E_{\mathrm{sq}}\left(A;B\right)_{\rho} \geq \log_2 |A|\left(1 - \varepsilon\right) \qquad (2.104)$$

implies that the state ρ_{AB} is near to a maximally entangled state. More precisely, we prove the following proposition.

Proposition 2.1 *Suppose that $\rho_{AB} \in \mathscr{D}(\mathcal{H}_{AB})$ and that*

$$E_{sq}\left(A;B\right)_{\rho} \geq \log_2 |A|\left(1 - \varepsilon\right), \qquad (2.105)$$

for some $\varepsilon \in (0, 1)$. Then ρ_{AB} is close to Φ_{AB} up to some local unitary U_B:

$$\frac{1}{2}\left\| \rho_{AB} - U_B\Phi_{AB}U_B^{\dagger} \right\|_1 \leq (2\sqrt{\varepsilon \ln |A|})^{1/2}. \qquad (2.106)$$

Proof. Let us consider

$$E_{\mathrm{sq}}\left(A;B\right)_{\rho} \geq \log_2 |A|\left(1 - \varepsilon\right). \qquad (2.107)$$

Then

$$\frac{1}{2}I\left(A;B\right)_{\rho} \geq E_{\mathrm{sq}}\left(A;B\right)_{\rho} \geq \log_2 |A|\left(1 - \varepsilon\right). \qquad (2.108)$$

35

Let ψ_{ABE} be a purification of ρ_{AB}. Then

$$2\log_2 |A| \, (1 - \varepsilon) \leq I(A; B)_\rho \tag{2.109}$$

$$= S(A)_\rho - S(A|B)_\rho \tag{2.110}$$

$$= S(A)_\rho + S(A|E)_\psi. \tag{2.111}$$

From (2.111), we get

$$2\varepsilon \log_2 |A| \geq -S(A|E) + \log_2 |A| + \log_2 |A| - S(A) \tag{2.112}$$

$$\geq D\left(\psi_{AE}\|\pi_A \otimes \psi_E\right) \tag{2.113}$$

$$\geq \frac{1}{2\ln 2} \left\|\psi_{AE} - \pi_A \otimes \psi_E\right\|_1^2, \tag{2.114}$$

where $\pi_A = \frac{\mathbb{I}}{|A|}$ is the maximally mixed state. We have

$$\left\|\psi_{AE} - \pi_A \otimes \psi_E\right\|_1 \leq 2\sqrt{\varepsilon \ln |A|}, \tag{2.115}$$

which implies (see Lemma 2.9)

$$F(\psi_{AE}, \pi_A \otimes \psi_E) \geq 1 - 2\sqrt{\varepsilon \ln |A|}. \tag{2.116}$$

Invoking Ulhmann's theorem and then monotonicity of the fidelity under partial trace, we can conclude that there exists some local unitary operator U_B such that

$$F(\rho_{AB}, U_{AB}\Phi_{AB}U_{AB}^\dagger) \geq 1 - 2\sqrt{\varepsilon \ln |A|}. \tag{2.117}$$

Using (2.117) in Lemma 2.9, we get

$$\left\|\rho_{AB} - U_{AB}\Phi_B U_B^\dagger\right\|_1 \leq 2\sqrt{2\sqrt{\varepsilon \ln |A|}}. \tag{2.118}$$

This completes the proof. ∎

Entropy of Entanglement

Proposition 2.2 *Suppose that ψ_{AB} is a pure state and that*

$$S(A)_\psi \geq (1 - \varepsilon) \log_2 |A|, \tag{2.119}$$

for some $\varepsilon \in (0, 1)$. Then there exists a unitary operator U_B such that

$$\frac{1}{2} \left\| U_B \psi_{AB} U_B^\dagger - \Phi_{AB} \right\|_1 \leq (2\varepsilon \ln |A|)^{1/4}. \tag{2.120}$$

Proof. Consider that our inequality is the same as

$$S(A)_\psi - (1 - \varepsilon) \log_2 |A| \geq 0. \tag{2.121}$$

We find that

$$S(A)_\psi - (1 - \varepsilon) \log_2 |A| = S(A)_\psi - \log_2 |A| + \varepsilon \log_2 |A| \tag{2.122}$$

$$= -D(\psi_A \| \pi_A) + \varepsilon \log_2 |A| \tag{2.123}$$

By assuming (2.119), we find that

$$\varepsilon \log_2 |A| \geq D(\psi_A \| \pi_A) \geq \frac{1}{2 \ln 2} \| \psi_A - \pi_A \|_1^2. \tag{2.124}$$

By an application of Uhlmann's theorem and Lemma 2.9, we recover the statement of the theorem.

∎

Chapter 3 Fundamental Limits on Entangling Abilities of Bipartite Quantum Interactions

A bipartite quantum interaction is an underlying Hamiltonian that governs the physical evolution of an open bipartite quantum system. In general, any two-body quantum system of interest can be in contact with a bath, and part of the composite system may be inaccessible to observers possessing these systems. As contact with the surrounding (bath) is unavoidable, the study of bipartite quantum interactions is pertinent. Depending on the kind of bipartite interaction and the input states, entanglement can be created, destroyed, or changed between two quantum systems [81, 98]. As entanglement is one of the fundamental and intriguing quantum phenomena [29, 30], determining the entangling abilities of bipartite quantum interactions is important. These bounds imply fundamental limitations on information processing capabilities over a repeaterless bipartite quantum network. Non-trivial bounds on the entangling abilities can also serve as the benchmarks for the efficiency testing of bipartite quantum gates in Noisy Intermediate-Scale Quantum (NISQ) processors [99] (cf. [100]).

It is known from quantum mechanics that a closed system evolves according to a unitary transformation [1, 2]. Let $U^{\hat{H}}_{A'B'E' \to ABE}$ be a unitary associated to an underlying Hamiltonian $\hat{H}$, which governs the physical evolution of the input subsystems A' and B' in the presence of a bath E', to produce output subsystems A and B for the observers and E for the bath. In general, the individual input systems A', B', and E' and the respective output systems A, B, and E can have different dimensions. Initially, in the absence of an interaction Hamiltonian $\hat{H}$, the bath is taken to be in a pure state and the systems of interest have no correlation with the bath; i.e., the state of the composite system $A'B'E'$ is of the form $\omega_{A'B'} \otimes \tau_{E'}$, for some fixed state $\tau_{E'}$ of the bath. Under the action of the Hamiltonian $\hat{H}$, the state of the composite system transforms as

$$\rho_{ABE} = U^{\hat{H}}(\omega_{A'B'} \otimes \tau_{E'})(U^{\hat{H}})^{\dagger}. \tag{3.1}$$

Since the system E in (3.1) is inaccessible, the evolution of the systems of interest is noisy in general.

Most of this chapter is based on [31], a joint work with Stefan Bäuml and Mark M. Wilde.

The noisy evolution of the bipartite system $A'B'$ under the action of the interaction Hamiltonian $\hat{H}$ is represented by a completely positive, trace-preserving (CPTP) map [41], called a bipartite quantum channel:

$$\mathcal{N}^{\hat{H}}_{A'B'\to AB}(\omega_{A'B'}) = \text{Tr}_E\{U^{\hat{H}}(\omega_{A'B'} \otimes \tau_{E'})(U^{\hat{H}})^\dagger\}, \qquad (3.2)$$

where system E represents inaccessible degrees of freedom. In particular, when the Hamiltonian $\hat{H}$ is such that there is no interaction between the composite system $A'B'$ and the bath E', and $A'B' \simeq AB$, then $\mathcal{N}^{\hat{H}}$ corresponds to a bipartite unitary, i.e., $\mathcal{N}^{\hat{H}}(\cdot) = U^{\hat{H}}_{A'B'\to AB}(\cdot)(U^{\hat{H}}_{A'B'\to AB})^\dagger$.

In the setting of an information processing task, when two spatially separated observers have access to different pair of quantum systems, (A', A) or (B', B), then a bipartite channel $\mathcal{N}_{A'B'\to AB}$ is also called *bidirectional channel*.

In this chapter, we focus on two different information-processing tasks relevant for bipartite quantum interactions, the first being entanglement distillation [46, 101, 102] and the second secret key agreement [78, 79, 103, 104]. Entanglement distillation is the task of generating a maximally entangled state, such as the singlet state, when two separated quantum systems undergo a bipartite interaction. Whereas, secret key agreement is the task of extracting maximal classical correlation between two separated systems, such that it is independent of the state of the bath system, which an eavesdropper could possess.

In an information-theoretic setting, a bipartite interaction between classical systems was first considered in [105] in the context of communication; therein, a bipartite interaction was called a two-way communication channel. In the quantum domain, bipartite unitaries have been widely considered in the context of their entangling ability, applications for interactive communication tasks, and the simulation of bipartite Hamiltonians in distributed quantum computation [21, 48, 84, 106–113] (see also Section 3.1). These unitaries form the simplest model of non-trivial interactions in many-body quantum systems and have been used as a model of scrambling in the context of quantum chaotic systems [114–116], as well as for the internal dynamics of a black hole [117] in the context of the information-loss paradox [118]. More generally, [119] developed the model of a bipartite interaction or two-way quantum communication channel. Bounds on the rate of entanglement generation in open quantum systems undergoing time evolution have also been discussed for particular classes

of quantum dynamics [32, 120].

The maximum rate at which a particular task can be accomplished by allowing the use of a bipartite interaction a large number of times, is equal to the capacity of the interaction for the task. The entanglement generating capacity quantifies the maximum rate of entanglement that can be generated from a bipartite interaction. Various capacities of a general bipartite unitary evolution were formalized in [84]. Later, various capacities of a general two-way channel were discussed in [119]. The entanglement generating capacities or entangling power of bipartite unitaries for different communication protocols have been widely discussed in the literature [84,85,107,121–123]. Also, prior to the work of [31], it was an open question to find a non-trivial, computationally efficient upper bound on the entanglement generating capacity of a bipartite quantum interaction.

In this chapter, we determine bounds on the capacities of bipartite interactions for entanglement generation and secret key agreement. The organization of this chapter is as follows. In Section 3.2, we derive a strong converse upper bound on the rate at which entanglement can be distilled from a bipartite quantum interaction. This bound is given by an information quantity introduced in [31, Section 3.1], called the bidirectional max-Rains information $R_{\max}^{2\to2}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$. The bidirectional max-Rains information is the solution to a semi-definite program and is thus efficiently computable. In Section 3.3, we derive a strong converse upper bound on the rate at which a secret key can be distilled from a bipartite quantum interaction. This bound is given by a related information quantity introduced in [31, Section 4.1], called the bidirectional max-relative entropy of entanglement $E_{\max}^{2\to2}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$. In Section 3.4, we derive upper bounds on the entanglement generation and secret key agreement capacities of bidirectional PPT- and teleportation-simulable channels, respectively. Our upper bounds on the capacities of such channels depend only on the entanglement of the resource states with which these bidirectional channels can be simulated.

3.1 Bipartite interactions and controlled unitaries

Let us consider a bipartite quantum interaction between systems X' and B', generated by a Hamiltonian $\hat{H}_{X'B'E'}$, where E' is a bath system. Suppose that the Hamiltonian is time independent,

having the following form:

$$\hat{H}_{X'B'E'} := \sum_{x \in \mathcal{X}} |x\rangle\langle x|_{X'} \otimes \hat{H}^x_{B'E'}, \tag{3.3}$$

where $\{|x\rangle\}_{x \in \mathcal{X}} \in \mathrm{ONB}(\mathcal{H}_{X'})$ and $\hat{H}^x_{B'E'}$ is a Hamiltonian for the composite system $B'E'$. Then, the evolution of the composite system $X'B'E'$ is given by the following controlled unitary:

$$U_{\hat{H}}(t) := \sum_{x \in \mathcal{X}} |x\rangle\langle x|_{X'} \otimes \exp\left(-\frac{\iota}{\hbar}\hat{H}^x_{B'E'}t\right), \tag{3.4}$$

where t denotes time. Suppose that the systems B' and E' are not correlated before the action of Hamiltonian $\hat{H}^x_{B'E'}$ for each $x \in \mathcal{X}$. Then, the evolution of the system B' under the interaction $\hat{H}^x_{B'E'}$ is given by a quantum channel $\mathcal{M}^x_{B'\to B}$ for all x.

For some distributed quantum computing and information processing tasks where the controlling system X and input system B' are jointly accessible, the following bidirectional channel is relevant:

$$\mathcal{N}_{X'B'\to XB}(\cdot) := \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes \mathcal{M}^x_{B'\to B}\left(\langle x|(\cdot)|x\rangle_{X'}\right). \tag{3.5}$$

In the above, X' is a controlling system that determines which evolution from the set $\{\mathcal{M}^x\}_{x \in \mathcal{X}}$ takes place on input system B'. In particular, when X' and B' are spatially separated and the input state for the system $X'B'$ are considered to be in a product state, the noisy evolution for such constrained interaction is given by the following bidirectional channel:

$$\mathcal{N}_{X'B'\to XB}(\sigma_{X'} \otimes \rho_{B'}) := \sum_{x \in \mathcal{X}} \langle x|\sigma_{X'}|x\rangle_{X'} |x\rangle\langle x|_X \otimes \mathcal{M}^x_{B'\to B}(\rho_{B'}). \tag{3.6}$$

3.2 Entanglement distillation from bipartite quantum interactions

In this section, we define the bidirectional max-Rains information $R^{2\to2}_{\max}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$ and show that it is not enhanced by amortization. We also prove that $R^{2\to2}_{\max}(\mathcal{N})$ is an upper bound on the amount of entanglement that can be distilled from a bidirectional channel $\mathcal{N}$. We do so by adapting to the bidirectional setting, the result from [54] and recent techniques developed in [74, 87, 91] for point-to-point quantum communication protocols.
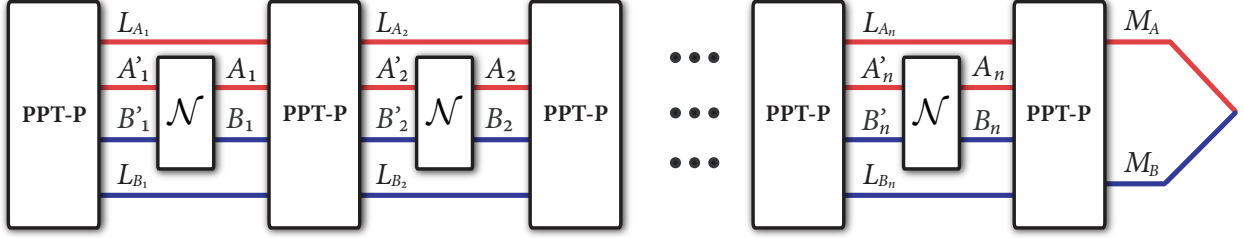
Figure 3.1. A protocol for PPT-assisted bidirectional quantum communication that uses a bidirectional quantum channel $\mathcal{N}$ n times. Every channel use is interleaved by a PPT-preserving (PPT-P) channel. The goal of such a protocol is to produce an approximate maximally entangled state in the systems M_A and M_B, where Alice possesses system M_A and Bob system M_B.

3.2.1   Bidirectional max-Rains information

The following definition generalizes the max-Rains information from (2.89), (2.93), and (2.94) to the bidirectional setting:

Definition 3.1 (Bidirectional max-Rains information) *The bidirectional max-Rains information of a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ is defined as*

$$R_{\max}^{2\to2}(\mathcal{N}) := \log \Gamma^{2\to2}(\mathcal{N}), \tag{3.7}$$

where $\Gamma^{2\to2}(\mathcal{N})$ is the solution to the following semi-definite program:

$$\text{minimize} \quad \|\text{Tr}_{AB}\{V_{L_A ABL_B} + Y_{L_A ABL_B}\}\|_\infty$$
$$\text{subject to} \quad V_{L_A ABL_B}, Y_{L_A ABL_B} \geq 0,$$
$$\text{T}_{BL_B}(V_{L_A ABL_B} - Y_{L_A ABL_B}) \geq J^{\mathcal{N}}_{L_A ABL_B}, \tag{3.8}$$

where $J^{\mathcal{N}}_{L_A ABL_B}$ denotes the Choi operator of the bidirectional channel $\mathcal{N}$, such that $L_A \simeq A'$, and $L_B \simeq B'$.

Remark 3.1 *By employing the Lagrange multiplier method, the bidirectional max-Rains information of a bidirectional channel $\mathcal{N}_{A'B'\to AB}$ can also be expressed as*

$$R_{\max}^{2\to2}(\mathcal{N}) = \log \Gamma^{2\to2}(\mathcal{N}), \tag{3.9}$$

where $\Gamma^{2\to2}(\mathcal{N})$ *is solution to the following semi-definite program (SDP):*

$$\text{maximize} \quad \text{Tr}\{J^{\mathcal{N}}_{L_A ABL_B} X_{L_A ABL_B}\}$$

$$\text{subject to} \quad X_{L_A ABL_B}, \rho_{L_A L_B} \geq 0,$$

$$\text{Tr}\{\rho_{L_A L_B}\} = 1, \quad -\rho_{L_A L_B} \otimes \mathbb{1}_{AB} \leq \text{T}_{BL_B}(X_{L_A ABL_B}) \leq \rho_{L_A L_B} \otimes \mathbb{1}_{AB}, \quad (3.10)$$

such that $L_A \simeq A'$, *and* $L_B \simeq B'$. *Strong duality holds by employing Slater's condition [26] (see also [92]). Thus, as indicated above, the optimal values of the primal and dual semi-definite programs, i.e., (3.10) and (3.8), respectively, are equal.*

The following proposition constitutes one of our main technical results, and an immediate corollary of it is that amortization does not enhance the bidirectional max-Rains information of a bidirectional quantum channel.

Proposition 3.1 (Amortization ineq. for bidirectional max-Rains info.) *Let* $\rho_{L_A A' B' L_B}$ *be an arbitrary state and let* $\mathcal{N}_{A'B'\to AB}$ *be a bidirectional channel. Then*

$$R_{\max}(L_A A; BL_B)_\omega \leq R_{\max}(L_A A'; B'L_B)_\rho + R^{2\to2}_{\max}(\mathcal{N}), \quad (3.11)$$

where $\omega_{L_A ABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$ *and* $R^{2\to2}_{\max}(\mathcal{N})$ *is the bidirectional max-Rains information of* $\mathcal{N}_{A'B'\to AB}$.

Proof. We adapt the proof steps of [91, Proposition 1] to the bidirectional setting. By removing logarithms and applying (2.91) and (3.7), the desired inequality is equivalent to the following

$$W(L_A A; BL_B)_\omega \leq W(L_A A'; B'L_B)_\rho \cdot \Gamma^{2\to2}(\mathcal{N}), \quad (3.12)$$

and so we aim to prove this one. Exploiting the identity in (2.92), we find that

$$W(L_A A'; B'L_B)_\rho = \min \text{Tr}\{C_{L_A A'B'L_B} + D_{L_A A'B'L_B}\}, \quad (3.13)$$

43

subject to the constraints

$$C_{L_A A' B' L_B}, D_{L_A A' B' L_B} \geq 0, \tag{3.14}$$

$$T_{B' L_B}(C_{L_A A' B' L_B} - D_{L_A A' B' L_B}) \geq \rho_{L_A A' B' L_B}, \tag{3.15}$$

while the definition in (3.8) gives that

$$\Gamma^{2 \to 2}(\mathcal{N}) = \min \|\text{Tr}_{AB}\{V_{R_A A B R_B} + Y_{R_A A B R_B}\}\|_\infty, \tag{3.16}$$

subject to the constraints

$$V_{R_A A B R_B}, Y_{R_A A B R_B} \geq 0, \tag{3.17}$$

$$T_{B R_B}(V_{R_A A B R_B} - Y_{R_A A B R_B}) \geq J^{\mathcal{N}}_{R_A A B R_B}. \tag{3.18}$$

The identity in (2.92) implies that the left-hand side of (3.12) is equal to

$$W(L_A A; B L_B)_\omega = \min \text{Tr}\{E_{L_A A B L_B} + F_{L_A A B L_B}\}, \tag{3.19}$$

subject to the constraints

$$E_{L_A A B L_B}, F_{L_A A B L_B} \geq 0, \tag{3.20}$$

$$\mathcal{N}_{A' B' \to AB}(\rho_{L_A A' B' L_B}) \leq T_{B L_B}(E_{L_A A B L_B} - F_{L_A A B L_B}). \tag{3.21}$$

Once we have these SDP formulations, we can now show that the inequality in (3.12) holds by making appropriate choices for $E_{L_A A B L_B}, F_{L_A A B L_B}$. Let $C_{L_A A' B' L_B}$ and $D_{L_A A' B' L_B}$ be optimal for $W(L_A A'; B' L_B)_\rho$, and let $V_{L_A A B L_B}$ and $Y_{L_A A B L_B}$ be optimal for $\Gamma^{2 \to 2}(\mathcal{N})$. Let $|\Upsilon\rangle_{R_A R_B : A' B'}$ be the maximally entangled vector. Choose

$$E_{L_A A B L_B} = \langle \Upsilon|_{R_A R_B : A' B'} C_{L_A A' B' L_B} \otimes V_{R_A A B R_B} + D_{L_A A' B' L_B} \otimes Y_{L_A A B L_B} |\Upsilon\rangle_{R_A R_B : A' B'} \tag{3.22}$$

$$F_{L_A A B L_B} = \langle \Upsilon|_{R_A R_B : A' B'} C_{L_A A' B' L_B} \otimes Y_{R_A A B R_B} + D_{L_A A' B' L_B} \otimes V_{R_A A B R_B} |\Upsilon\rangle_{R_A R_B : A' B'}. \tag{3.23}$$

The above choices can be thought of as bidirectional generalizations of those made in the proof of [91, Proposition 1] (see also [90, Proposition 6]), and they can be understood roughly via (2.22) as a post-selected teleportation of the optimal operators of $W(L_A A'; B' L_B)_\rho$ through the optimal operators of $\Gamma^{2\to 2}(\mathcal{N})$, with the optimal operators of $W(L_A A'; B' L_B)_\rho$ being in correspondence with the Choi operator $J^{\mathcal{N}}_{R_A ABR_B}$ through (3.18). Then, we have, $E_{L_A ABL_B}, F_{L_A ABL_B} \geq 0$, because

$$C_{L_A A' B' L_B}, D_{L_A A' B' L_B}, Y_{R_A ABR_B}, V_{R_A ABR_B} \geq 0. \tag{3.24}$$

Also, consider that

$$E_{L_A ABL_B} - F_{L_A ABL_B}$$
$$= \langle \Upsilon |_{R_A R_B : A'B'} (C_{L_A A'B'L_B} - D_{L_A A'B'L_B}) \otimes (V_{R_A ABR_B} - Y_{R_A ABR_B}) |\Upsilon\rangle_{R_A R_B : A'B'} \tag{3.25}$$
$$= \mathrm{Tr}_{R_A A'B'R_B}\{|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} (C_{L_A A'B'L_B} - D_{L_A A'B'L_B}) \otimes (V_{R_A ABR_B} - Y_{R_A ABR_B})\}. \tag{3.26}$$

Then, using the abbreviations $E' := E_{L_A ABL_B}$, $F' := F_{L_A ABL_B}$, $C' := C_{L_A A'B'L_B}$, $D' := D_{L_A A'B'L_B}$, $V' := V_{R_A ABR_B}$, and $Y' := Y_{R_A ABR_B}$, we have

$$\mathrm{T}_{BL_B}(E' - F') = \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{R_A A'B'R_B}\{|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} (C' - D') \otimes (V' - Y')\}\right] \tag{3.27}$$
$$= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{R_A A'B'R_B}\{|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} (C' - D') \otimes (\mathrm{T}_{R_B} \circ \mathrm{T}_{R_B})(V' - Y')\}\right] \tag{3.28}$$
$$= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{R_A A'B'R_B}\{\mathrm{T}_{R_B}|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} (C' - D') \otimes \mathrm{T}_{R_B}(V' - Y')\}\right] \tag{3.29}$$
$$= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{R_A A'B'R_B}\{|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} \mathrm{T}_{B'}(C' - D') \otimes \mathrm{T}_{R_B}(V' - Y')\}\right] \tag{3.30}$$
$$= \mathrm{Tr}_{R_A A'B'R_B}\{|\Upsilon\rangle\langle\Upsilon|_{R_A R_B : A'B'} \mathrm{T}_{B'L_B}(C' - D') \otimes \mathrm{T}_{BR_B}(V' - Y')\} \tag{3.31}$$
$$\geq \langle \Upsilon |_{R_A R_B : AB}\, \rho_{L_A A'B'L_B} \otimes J^{\mathcal{N}}_{R_A ABR_B} |\Upsilon\rangle_{R_A R_B : AB} \tag{3.32}$$
$$= \mathcal{N}_{A'B' \to AB}(\rho_{L_A A'B'L_B}). \tag{3.33}$$

In the above, we employed properties of the partial transpose reviewed in (2.24)–(2.26). Now,

consider that

$$\text{Tr}\{E_{L_A ABL_B} + F_{L_A ABL_B}\}$$

$$= \text{Tr}\{\langle \Upsilon|_{R_A R_B : A'B'} (C_{L_A A'B'L_B} + D_{L_A A'B'L_B}) \otimes (V_{R_A ABR_B} + Y_{R_A ABR_B}) |\Upsilon\rangle_{R_A R_B : A'B'}\} \tag{3.34}$$

$$= \text{Tr}\{(C_{L_A A'B'L_B} + D_{L_A A'B'L_B}) T_{A'B'} (V_{A'ABB'} + Y_{A'ABB'})\} \tag{3.35}$$

$$= \text{Tr}\{(C_{L_A A'B'L_B} + D_{L_A A'B'L_B}) T_{A'B'} (\text{Tr}_{AB}\{V_{A'ABB'} + Y_{A'ABB'}\})\} \tag{3.36}$$

$$\leq \text{Tr}\{(C_{L_A A'B'L_B} + D_{L_A A'B'L_B})\} \| T_{A'B'} (\text{Tr}_{AB}\{V_{A'ABB'} + Y_{A'ABB'}\}) \|_\infty \tag{3.37}$$

$$= \text{Tr}\{(C_{L_A A'B'L_B} + D_{L_A A'B'L_B})\} \| \text{Tr}_{AB}\{V_{A'ABB'} + Y_{A'ABB'}\} \|_\infty \tag{3.38}$$

$$= W(L_A A'; B'L_B)_\rho \cdot \Gamma^{2\to2}(\mathcal{N}). \tag{3.39}$$

The inequality is a consequence of Hölder's inequality [39]. The final equality follows because the spectrum of a positive semi-definite operator is invariant under the action of a full transpose (note, in this case, $\text{T}_{A'B'}$ is the full transpose as it acts on reduced positive semi-definite operators $V_{A'B'}$ and $Y_{A'B'}$).

Therefore, we can infer that our choices of $E_{L_A ABL_B}, F_{L_A ABL_B}$ are feasible for $W(L_A A; BL_B)_\omega$. Since $W(L_A A; BL_B)_\omega$ involves a minimization over all $E_{L_A ABL_B}, F_{L_A ABL_B}$ satisfying (3.20) and (3.21), this concludes our proof of (3.12). ∎

An immediate corollary of Proposition 3.1 is the following:

Corollary 3.1 *Amortization does not enhance the bidirectional max-Rains information of a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$; i.e., the following inequality holds*

$$R^{2\to2}_{\max,A}(\mathcal{N}) \leq R^{2\to2}_{\max}(\mathcal{N}), \tag{3.40}$$

where $R^{2\to2}_{\max,A}(\mathcal{N})$ is a measure of the entangling power of a bidirectional channel $\mathcal{N}$, i.e.,

$$R^{2\to2}_{\max,A}(\mathcal{N}) := \sup_{\rho_{L_A A'B'L_B} \in \mathscr{D}(\mathcal{H}_{L_A A'B'L_B})} [R_{\max}(L_A A; BL_B)_\sigma - R_{\max}(L_A A'; B'L_B)_\rho], \tag{3.41}$$

and $\sigma_{L_A ABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$, where L_A and L_B can be arbitrarily large.

Proof. The inequality $R^{2\to2}_{\max,A}(\mathcal{N}) \leq R^{2\to2}_{\max}(\mathcal{N})$ is an immediate consequence of Proposition 3.1. Let $\rho_{L_A A' B' L_B}$ denote an arbitrary input state. Then from Proposition 3.1

$$R_{\max}(L_A A; B L_B)_\omega - R_{\max}(L_A A'; B' L_B)_\rho \leq R^{2\to2}_{\max}(\mathcal{N}), \tag{3.42}$$

where $\omega_{L_A A B L_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_A A' B' L_B})$. As the inequality holds for any state $\rho_{L_A A' B' L_B}$, we conclude that $R^{2\to2}_{\max,A}(\mathcal{N}) \leq R^{2\to2}_{\max}(\mathcal{N})$. ∎

See Appendix B for some examples where the bidirectional max-Rains information of some channels are numerically evaluated.

3.2.2 Application to entanglement generation

In this section, we discuss the implication of Proposition 3.1 for PPT-assisted entanglement generation from a bidirectional channel[1]. Suppose that two parties Alice and Bob are connected by a bipartite quantum interaction. Suppose that the systems that Alice and Bob hold are A' and B', respectively. The bipartite quantum interaction between them is represented by a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$, where output systems A and B are in possession of Alice and Bob, respectively. This kind of protocol was considered in [84] when there is LOCC assistance.

Protocol for PPT-assisted entanglement generation

We now discuss PPT-assisted entanglement generation protocols that make use of a bidirectional quantum channel. We do so by generalizing the point-to-point communication protocol discussed in [54] to the bidirectional setting.

In a PPT-assisted bidirectional protocol, as depicted in Figure 3.1, Alice and Bob are spatially separated and they are allowed to undergo a bipartite quantum interaction $\mathcal{N}_{A'B'\to AB}$, where for a fixed basis $\{|i\rangle_B |j\rangle_{L_B}\}_{i,j}$, the partial transposition T_{BL_B} is considered on systems associated to Bob. Alice holds systems labeled by A', A whereas Bob holds B', B. They begin by per-

---

[1]It is an open question whether or not NPT (non-positive under partial transpose) bound entangled states exist. However, it is known that all bipartite quantum states that are non-positive under partial transpose are distillable via some PPT-preserving channels [124]. Therefore, in the standard case, the free operations allowed for the task of entanglement distillation are LOCC channels.

forming a PPT-preserving channel $\mathcal{P}^{(1)}_{\emptyset \to L_{A_1} A_1' B_1' L_{B_1}}$, which leads to a PPT state $\rho^{(1)}_{L_{A_1} A_1' B_1' L_{B_1}}$, where L_{A_1}, L_{B_1} are finite-dimensional systems of arbitrary size and A_1', B_1' are input systems to the first channel use. Alice and Bob send systems A_1' and B_1', respectively, through the first channel use, which yields the output state $\sigma^{(1)}_{L_{A_1} A_1 B_1 L_{B_1}} := \mathcal{N}_{A_1' B_1' \to A_1 B_1}(\rho^{(1)}_{L_{A_1} A_1' B_1' L_{B_1}})$. Alice and Bob then perform the PPT-preserving channel $\mathcal{P}^{(2)}_{L_{A_1} A_1 B_1 L_{B_1} \to L_{A_2} A_2' B_2' L_{B_2}}$, which leads to the state $\rho^{(2)}_{L_{A_2} A_2' B_2' L_{B_2}} :=$ $\mathcal{P}^{(2)}_{L_{A_1} A_1 B_1 L_{B_1} \to L_{A_2} A_2' B_2' L_{B_2}}(\sigma^{(1)}_{L_{A_1} A_1 B_1 L_{B_1}})$. Both parties then send systems A_2', B_2' through the second channel use $\mathcal{N}_{A_2' B_2' \to A_2 B_2}$, which yields the state $\sigma^{(2)}_{L_{A_2} A_2 B_2 L_{B_2}} := \mathcal{N}_{A_2' B_2' \to A_2 B_2}(\rho^{(2)}_{L_{A_2} A_2' B_2' L_{B_2}})$. They iterate this process such that the protocol makes use of the channel n times. In general, we have the following states for the ith use, for $i \in \{2, 3, \ldots, n\}$:

$$\rho^{(i)}_{L_{A_i} A_i' B_i' L_{B_i}} := \mathcal{P}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A_i' B_i' L_{B_i}}(\sigma^{(i-1)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}}}), \qquad (3.43)$$

$$\sigma^{(i)}_{L_{A_i} A_i B_i L_{B_i}} := \mathcal{N}_{A_i' B_i' \to A_i B_i}(\rho^{(i)}_{L_{A_i} A_i' B_i' L_{B_i}}), \qquad (3.44)$$

where $\mathcal{P}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A_i' B_i' L_{B_i}}$ is a PPT-preserving channel, with the partial transposition acting on systems $B_{i-1}, L_{B_{i-1}}$ associated to Bob. In the final step of the protocol, a PPT-preserving channel $\mathcal{P}^{(n+1)}_{L_{A_n} A_n B_n L_{B_n} \to M_A M_B}$ is applied, that generates the final state:

$$\omega_{M_A M_B} := \mathcal{P}^{(n+1)}_{L_{A_n} A_n B_n L_{B_n} \to M_A M_B}(\sigma^{(n)}_{L_{A_n} A_n' B_n' L_{B_n}}), \qquad (3.45)$$

where M_A and M_B are held by Alice and Bob, respectively.

The goal of the protocol is for Alice and Bob to distill entanglement in the end; i.e., the final state $\omega_{M_A M_B}$ should be close to a maximally entangled state $\Phi_{M_A M_B}$. For a fixed n, $|M| \in \mathbb{N}$, $\varepsilon \in [0, 1]$, the original protocol is an (n, Q, ε) protocol if the channel is used n times as discussed above, $|M_A| = |M_B| = |M|$, $Q := \frac{1}{n} \log_2 |M|$, and if

$$F(\omega_{M_A M_B}, \Phi_{M_A M_B}) = \langle \Phi |_{M_A M_B} \omega_{M_A M_B} |\Phi\rangle_{AB} \qquad (3.46)$$

$$\geq 1 - \varepsilon, \qquad (3.47)$$

where $\Phi_{M_A M_B}$ is the maximally entangled state. A rate Q is said to be achievable for PPT-

assisted entanglement generation if for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n, there exists an $(n, Q - \delta, \varepsilon)$ protocol. The PPT-assisted entanglement generation capacity of a bidirectional channel $\mathcal{N}$, denoted as $Q_{\text{PPT}}^{2 \to 2}(\mathcal{N})$, is equal to the supremum of all achievable rates. Whereas, a rate Q is a strong converse rate for PPT-assisted entanglement generation if for all $\varepsilon \in [0, 1)$, $\delta > 0$, and sufficiently large n, there does not exist an $(n, Q + \delta, \varepsilon)$ protocol. The strong converse PPT-assisted entanglement generation $\widetilde{Q}_{\text{PPT}}^{2 \to 2}(\mathcal{N})$ is equal to the infimum of all strong converse rates. A bidirectional channel $\mathcal{N}$ is said to obey the strong converse property for PPT-assisted entanglement generation if $Q_{\text{PPT}}^{2 \to 2}(\mathcal{N}) = \widetilde{Q}_{\text{PPT}}^{2 \to 2}(\mathcal{N})$.

Note that every LOCC channel is a PPT-preserving channel. Given this, the well-known fact that teleportation [18] is an LOCC channel, and PPT-preserving channels are allowed for free in the above protocol, there is no difference between an (n, Q, ε) entanglement generation protocol and an (n, Q, ε) quantum communication protocol. Thus, all of the capacities for entanglement generation are equal to those for quantum communication.

Also, we can consider the whole development discussed above for LOCC-assisted bidirectional quantum communication instead of more general PPT-assisted bidirectional quantum communication. All the notions discussed above follow when we restrict the class of assisting PPT-preserving channels allowed to be LOCC channels. It follows that the LOCC-assisted bidirectional quantum capacity $Q_{\text{LOCC}}^{2 \to 2}(\mathcal{N})$ and the strong converse LOCC-assisted quantum capacity $\widetilde{Q}_{\text{LOCC}}^{2 \to 2}(\mathcal{N})$ are bounded from above as

$$Q_{\text{LOCC}}^{2 \to 2}(\mathcal{N}) \leq Q_{\text{PPT}}^{2 \to 2}(\mathcal{N}), \tag{3.48}$$

$$\widetilde{Q}_{\text{LOCC}}^{2 \to 2}(\mathcal{N}) \leq \widetilde{Q}_{\text{PPT}}^{2 \to 2}(\mathcal{N}). \tag{3.49}$$

Also, the capacities of bidirectional quantum communication protocols without any assistance are always less than or equal to the LOCC-assisted bidirectional quantum capacities.

The following lemma will be useful in deriving upper bounds on the bidirectional quantum capacities in the forthcoming sections, and it represents a generalization of the amortization idea to the bidirectional setting (see [84] in this context).

Lemma 3.1 *Let* $\text{Ent}_{\text{PPT}}(A; B)_\rho$ *be a bipartite entanglement measure for an arbitrary bipartite state*

ρ_{AB}. *Suppose that* $\mathrm{Ent}_{\mathrm{PPT}}(A;B)_\rho$ *vanishes for all* $\rho_{AB} \in \mathrm{PPT}(A:B)$ *and is monotone non-increasing under PPT-preserving channels. Consider an* (n, M, ε) *protocol for PPT-assisted entanglement generation over a bidirectional quantum channel* $\mathcal{N}_{A'B' \to AB}$, *as described in Section 3.2.2. Then, the following bound holds:*

$$\mathrm{Ent}_{\mathrm{PPT}}(M_A; M_B)_\omega \leq n\, \mathrm{Ent}_{\mathrm{PPT},A}(\mathcal{N}), \tag{3.50}$$

where $\mathrm{Ent}_{\mathrm{PPT},A}(\mathcal{N})$ *is the amortized entanglement of a bidirectional channel* $\mathcal{N}$, *i.e.,*

$$\mathrm{Ent}_{\mathrm{PPT},A}(\mathcal{N}) \coloneqq \sup_{\rho_{L_A A' B' L_B} \in \mathscr{D}(\mathcal{H}_{L_A A' B' L_B})} \left[\mathrm{Ent}_{\mathrm{PPT}}(L_A A; B L_B)_\sigma - \mathrm{Ent}_{\mathrm{PPT}}(L_A A'; B' L_B)_\rho \right], \tag{3.51}$$

such that $\sigma_{L_A A B L_B} \coloneqq \mathcal{N}_{A'B' \to AB}(\rho_{L_A A' B' L_B})$.

Proof. From the discussion above, as $\mathrm{Ent}_{\mathrm{PPT}}$ is monotonically non-increasing under the action of PPT-preserving channels, we get that

$$\mathrm{Ent}_{\mathrm{PPT}}(M_A; M_B)_\omega \leq \mathrm{Ent}_{\mathrm{PPT}}(L_{A_n} A_n; B_n L_{B_n})_{\sigma^{(n)}} \tag{3.52}$$

$$= \mathrm{Ent}_{\mathrm{PPT}}(L_{A_n} A_n; B_n L_{B_n})_{\sigma^{(n)}} - \mathrm{Ent}_{\mathrm{PPT}}(L_{A_1} A_1'; B_1' L_{B_1})_{\rho^{(1)}} \tag{3.53}$$

$$= \mathrm{Ent}_{\mathrm{PPT}}(L_{A_n} A_n; B_n L_{B_n})_{\sigma^{(n)}}$$
$$+ \left[\sum_{i=2}^{n} \mathrm{Ent}_{\mathrm{PPT}}(L_{A_i} A_i'; B_i' L_{B_i})_{\rho^{(i)}} - \mathrm{Ent}_{\mathrm{PPT}}(L_{A_i} A_i'; B_i' L_{B_i})_{\rho^{(i)}} \right]$$
$$- \mathrm{Ent}_{\mathrm{PPT}}(L_{A_1} A_1'; B_1' L_{B_1})_{\rho^{(1)}} \tag{3.54}$$

$$\leq \sum_{i=1}^{n} \left[\mathrm{Ent}_{\mathrm{PPT}}(L_{A_i} A_i; B_i L_{B_i})_{\sigma^{(i)}} - \mathrm{Ent}_{\mathrm{PPT}}(L_{A_i} A_i'; B_i' L_{B_i})_{\rho^{(i)}} \right] \tag{3.55}$$

$$\leq n\, \mathrm{Ent}_{\mathrm{PPT},A}(\mathcal{N}). \tag{3.56}$$

The first equality follows because $\rho^{(1)}_{L_{A_1} A_1' B_1' L_{B_1}}$ is a PPT state with vanishing $\mathrm{Ent}_{\mathrm{PPT}}$. The second equality follows trivially because we add and subtract the same terms. The second inequality follows because $\mathrm{Ent}_{\mathrm{PPT}}(L_{A_i} A_i'; B_i' L_{B_i})_{\rho^{(i)}} \leq \mathrm{Ent}_{\mathrm{PPT}}(L_{A_{i-1}} A_{i-1}; B_{i-1} L_{B_{i-1}})_{\sigma^{(i-1)}}$ for all $i \in \{2, 3, \ldots, n\}$, due to monotonicity of $\mathrm{Ent}_{\mathrm{PPT}}$ with respect to PPT-preserving channels. The final inequality follows

by applying the definition in (3.51) to each summand. ∎

Strong converse rate for PPT-assisted entanglement generation

We now establish the following upper bound on the entanglement generation rate Q (qubits per channel use) of any (n, Q, ε) PPT-assisted protocol:

Theorem 3.1 *For a fixed n, $|M| \in \mathbb{N}$, $\varepsilon \in (0, 1)$, the following bound holds for an (n, Q, ε) protocol for PPT-assisted entanglement generation over a bidirectional quantum channel $\mathcal{N}$:*

$$Q \leq R_{\max}^{2 \to 2}(\mathcal{N}) + \frac{1}{n} \log_2 \left(\frac{1}{1 - \varepsilon} \right) \tag{3.57}$$

such that $Q = \frac{1}{n} \log_2 |M|$.

Proof. From earlier discussion, we have that

$$\mathrm{Tr}\{\Phi_{M_A M_B} \omega_{M_A M_B}\} \geq 1 - \varepsilon, \tag{3.58}$$

while [46, Lemma 2] implies that

$$\forall \sigma_{M_A M_B} \in \mathrm{PPT}'(M_A : M_B), \ \mathrm{Tr}\{\Phi_{M_A M_B} \sigma_{M_A M_B}\} \leq \frac{1}{|M|}. \tag{3.59}$$

Under an "entanglement test", which is a measurement with POVM $\{\Phi_{M_A M_B}, \mathbb{1}_{M_A M_B} - \Phi_{M_A M_B}\}$, and applying the data processing inequality for the max-relative entropy, we find that

$$R_{\max}(M_A; M_B)_\omega \geq \log_2[(1 - \varepsilon)|M|]. \tag{3.60}$$

Applying Lemma 3.1 and Proposition 3.1, we get that

$$R_{\max}(M_A; M_B)_\omega \leq n R_{\max}^{2 \to 2}(\mathcal{N}). \tag{3.61}$$

Combining (3.60) and (3.61), we get the desired inequality (3.57). ∎

Remark 3.2 *The bound in* (3.57) *can also be rewritten as*

$$1 - \varepsilon \leq 2^{-n[Q - R_{\max}^{2 \to 2}(\mathcal{N})]}. \tag{3.62}$$

Thus, if the bidirectional communication rate Q is strictly larger than the bidirectional max-Rains information $\mathcal{R}_{\max}^{2 \to 2}(\mathcal{N})$, then the fidelity of the transmission $(1 - \varepsilon)$ decays exponentially fast to zero in the number n of channel uses.

An immediate corollary of the above remark is the following strong converse statement:

Corollary 3.2 *The strong converse PPT-assisted bidirectional quantum capacity of a bidirectional channel $\mathcal{N}$ is bounded from above by its bidirectional max-Rains information:*

$$\widetilde{Q}_{\mathrm{PPT}}^{2 \to 2}(\mathcal{N}) \leq R_{\max}^{2 \to 2}(\mathcal{N}). \tag{3.63}$$

3.3 Secret key distillation from bipartite quantum interactions

In this section, we define the bidirectional max-relative entropy of entanglement $E_{\max}^{2 \to 2}(\mathcal{N})$. The main goal of this section is to derive an upper bound on the rate at which secret key can be distilled from a bipartite quantum interaction. In deriving this bound, we consider private communication protocols over bidirectional quantum channels, and we make use of recent techniques developed in quantum information theory for point-to-point private communication protocols [54, 74, 79, 80].

3.3.1 Bidirectional generalized divergence of entanglement

We define divergence based measures to quantify the ability of distilling secret key from a bipartite quantum channel.

Definition 3.2 *The generalized divergence of entanglement from a bidirectional channel $\mathcal{N}_{A'B' \to AB}$ is defined as*

$$\boldsymbol{E}_D^{2 \to 2}(\mathcal{N}) = \sup_{\rho \in \mathrm{SEP}(L_A A' : B' L_B)} \boldsymbol{E}(L_A A; B L_B)_\omega, \tag{3.64}$$

where $\boldsymbol{E}(L_A A; B L_B)_\omega$ is a generalized divergence of entanglement of the state

$$\omega_{L_A A B L_B} := \mathcal{N}_{A'B' \to AB}(\rho_{L_A A' B' L_B}), \tag{3.65}$$

with L_A and L_B being arbitrarily large,

$$\boldsymbol{E}(\hat{A}; \hat{B})_\tau := \inf_{\sigma_{\hat{A}\hat{B}} \in \mathrm{SEP}(\hat{A}:\hat{B})} \boldsymbol{D}(\tau_{\hat{A}\hat{B}} \| \sigma_{\hat{A}\hat{B}}). \tag{3.66}$$

The following definition generalizes a channel's max-relative entropy of entanglement from [74] to the bidirectional setting, which we get after substituting generalized divergence $\boldsymbol{D}$ in (3.66) with the max-relative entropy $D_{\max}$:

Definition 3.3 (Bidirectional max-relative entropy of entanglement) *The bidirectional max-relative entropy of entanglement of a bidirectional channel $\mathcal{N}_{A'B' \to AB}$ is defined as*

$$E_{\max}^{2\to2}(\mathcal{N}) = \max_{\psi_{L_A A'} \otimes \varphi_{B'L_B}} E_{\max}(L_A A; B L_B)_\omega, \tag{3.67}$$

where $\omega_{L_A A B L_B} := \mathcal{N}_{A'B' \to AB}(\psi_{L_A A'} \otimes \varphi_{B'L_B})$, and $\psi_{L_A A'} \otimes \varphi_{B'L_B} \in \mathrm{SEP}(L_A A' : B' L_B)$ is a pure tensor-product state such that $L_A \simeq A'$, and $L_B \simeq B'$.

Remark 3.3 *Note that we could define $E_{\max}^{2\to2}(\mathcal{N})$ to have an optimization over separable input states $\rho_{L_A A' B' L_B} \in \mathrm{SEP}(L_A A' : B' L_B)$ with finite-dimensional, but arbitrarily large auxiliary systems L_A and L_B. However, the quasi-convexity of the max-relative entropy of entanglement [69, 70] and the Schmidt decomposition theorem guarantee that it suffices to restrict the optimization to be as stated in Definition 3.3.*

Analogous to definition of the bidirectional max-relative entropy of entanglement aforementioned, definition of the bidirectional relative entropy of entanglement $E_D^{2\to2}(\mathcal{N})$ of an arbitrary bidirectional channel $\mathcal{N}$ is obtained by substituting generalized divergence in (3.66) with the relative entropy.

Remark 3.4 *The bidirectional max-relative entropy of entanglement and the bidirectional relative entropy of entanglement of a bidirectional channel $\mathcal{N}_{A'B'\to AB}$ are both zero if and only if $\mathcal{N}_{A'B'\to AB}$ is a separable channel.*

Proposition 3.2 (Amortization ineq. for bidirectional max-relative entropy) *Let $\rho_{L_A A'B'L_B}$ be an arbitrary state and let $\mathcal{N}_{A'B'\to AB}$ be a bidirectional channel. Then*

$$E_{\max}(L_A A; BL_B)_\omega \le E_{\max}(L_A A'; B'L_B)_\rho + E_{\max}^{2\to2}(\mathcal{N}), \tag{3.68}$$

where $\omega_{L_A ABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$ and $E_{\max}^{2\to2}(\mathcal{N})$ is the bidirectional max-relative entropy of entanglement of $\mathcal{N}_{A'B'\to AB}$.

Proof. Let us consider states $\sigma'_{L_A A'B'L_B} \in \mathrm{SEP}(L_A A' : B'L_B)$ and $\sigma_{L_A ABL_B} \in \mathrm{SEP}(L_A A : BL_B)$, where L_A and L_B are finite-dimensional, but arbitrarily large. With respect to the bipartite cut $L_A A : BL_B$, the following inequality holds

$$E_{\max}(L_A A; BL_B)_\omega \le D_{\max}(\mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})\|\sigma_{L_A ABL_B}). \tag{3.69}$$

Applying the data-processed triangle inequality [74, Theorem III.1], we find that

$$D_{\max}(\mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})\|\sigma_{L_A ABL_B})$$
$$\le D_{\max}(\rho_{L_A A'B'L_B}\|\sigma'_{L_A A'B'L_B}) + D_{\max}(\mathcal{N}_{A'B'\to AB}(\sigma'_{L_A A'B'L_B})\|\sigma_{L_A ABL_B}). \tag{3.70}$$

Since $\sigma'_{L_A A'B'L_B}$ and $\sigma_{L_A ABL_B}$ are arbitrary separable states, we arrive at

$$E_{\max}(L_A A; BL_B)_\omega \le E_{\max}(L_A A'; B'L_B)_\rho + E_{\max}(\mathcal{N}_{A'B'\to AB}(\sigma'_{L_A A'B'L_B})), \tag{3.71}$$

where $\omega_{L_A ABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$. This implies the desired inequality after applying the observation in Remark 3.3, given that $\sigma'_{L_A A'B'L_B} \in \mathrm{SEP}(L_A A' : B'L_B)$. ∎

An immediate consequence of Proposition 3.2 is the following corollary:

Corollary 3.3 *Amortization does not enhance the bidirectional max-relative entropy of entanglement of a bidirectional quantum channel $\mathcal{N}_{A'B' \to AB}$; and the following equality holds:*

$$E_{\max,A}^{2 \to 2}(\mathcal{N}) = E_{\max}^{2 \to 2}(\mathcal{N}), \tag{3.72}$$

where $E_{\max,A}^{2 \to 2}(\mathcal{N})$ is the amortized entanglement of a bidirectional channel $\mathcal{N}$, i.e.,

$$E_{\max,A}^{2 \to 2}(\mathcal{N}) := \sup_{\rho_{L_A A'B'L_B} \in \mathscr{D}(\mathcal{H}_{L_A A'B'L_B})} \left[E_{\max}(L_A A; BL_B)_\sigma - E_{\max}(L_A A'; B'L_B)_\rho \right], \tag{3.73}$$

and $\sigma_{L_A ABL_B} := \mathcal{N}_{A'B' \to AB}(\rho_{L_A A'B'L_B})$ where L_A and L_B can be arbitrary large.

Proof. The inequality $E_{\max,A}^{2 \to 2}(\mathcal{N}) \geq E_{\max}^{2 \to 2}(\mathcal{N})$ always holds. The other inequality $E_{\max,A}^{2 \to 2}(\mathcal{N}) \leq E_{\max}^{2 \to 2}(\mathcal{N})$ is an immediate consequence of Proposition 3.2 (the argument is similar to that given in the proof of Corollary 3.1). ∎

3.3.2 Application to secret key generation

Protocol for LOCC-assisted secret key generation

We first discuss an LOCC-assisted secret key generation protocol that employs a bidirectional quantum channel.

In an LOCC-assisted secret key generation protocol, Alice and Bob are spatially separated and they are allowed to make use of a bipartite quantum interaction $\mathcal{N}_{A'B' \to AB}$, where the bipartite cut is considered between systems associated to Alice and Bob, $L_A A : L_B B$. Let $\mathcal{U}_{A'B' \to ABE}^{\mathcal{N}}$ be an isometric channel extending $\mathcal{N}_{A'B' \to AB}$:

$$\mathcal{U}_{A'B' \to ABE}^{\mathcal{N}}(\cdot) = U_{A'B' \to ABE}^{\mathcal{N}}(\cdot) \left(U_{A'B' \to ABE}^{\mathcal{N}} \right)^\dagger, \tag{3.74}$$

where $U_{A'B' \to ABE}^{\mathcal{N}}$ is an isometric extension of $\mathcal{N}_{A'B' \to AB}$. Let us assume that the eavesdropper Eve has access to the system E, also referred to as the environment, as well as a coherent copy of the classical communication exchanged between Alice and Bob. One could also consider a weaker assumption, in which the eavesdropper has access to only part of $E = E'E''$.

Alice and Bob begin by performing an LOCC channel $\mathcal{L}^{(1)}_{\emptyset \to L_{A_1} A'_1 B'_1 L_{B_1}}$, which leads to a state $\rho^{(1)}_{L_{A_1} A'_1 B'_1 L_{B_1}} \in \mathrm{SEP}(L_{A_1} A'_1 : B'_1 L_{B_1})$, where L_{A_1}, L_{B_1} are finite-dimensional systems of arbitrary size and A'_1, B'_1 are input systems to the first channel use. Alice and Bob send systems A'_1 and B'_1, respectively, through the first channel use, that outputs the state $\sigma^{(1)}_{L_{A_1} A_1 B_1 L_{B_1}} := \mathcal{N}_{A'_1 B'_1 \to A_1 B_1}(\rho^{(1)}_{L_{A_1} A'_1 B'_1 L_{B_1}})$. They then perform the LOCC channel $\mathcal{L}^{(2)}_{L_{A_1} A_1 B_1 L_{B_1} \to L_{A_2} A'_2 B'_2 L_{B_2}}$, which leads to the state $\rho^{(2)}_{L_{A_2} A'_2 B'_2 L_{B_2}} := \mathcal{L}^{(2)}_{L_{A_1} A_1 B_1 L_{B_1} \to L_{A_2} A'_2 B'_2 L_{B_2}}(\sigma^{(1)}_{L_{A_1} A_1 B_1 L_{B_1}})$. Both parties then send systems A'_2, B'_2 through the second channel use $\mathcal{N}_{A'_2 B'_2 \to A_2 B_2}$, which yields the state $\sigma^{(2)}_{L_{A_2} A_2 B_2 L_{B_2}} := \mathcal{N}_{A'_2 B'_2 \to A_2 B_2}(\rho^{(2)}_{L_{A_2} A'_2 B'_2 L_{B_2}})$. They iterate the process such that the protocol uses the channel n times. In general, we have the following states for the ith channel use, for $i \in [n]$:

$$\rho^{(i)}_{L_{A_i} A'_i B'_i L_{B_i}} := \mathcal{L}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A'_i B'_i L_{B_i}}(\sigma^{(i-1)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}}}), \qquad (3.75)$$

$$\sigma^{(i)}_{L_{A_i} A_i B_i L_{B_i}} := \mathcal{N}_{A'_i B'_i \to A_i B_i}(\rho^{(i)}_{L_{A_i} A'_i B'_i L_{B_i}}), \qquad (3.76)$$

where $\mathcal{L}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A'_i B'_i L_{B_i}}$ is an LOCC channel corresponding to the bipartite cut $L_{A_{i-1}} A_{i-1} : B_{i-1} L_{B_{i-1}}$. In the final step of the protocol, an LOCC channel $\mathcal{L}^{(n+1)}_{L_{A_n} A_n B_n L_{B_n} \to K_A K_B}$ is applied, which generates the final state:

$$\omega_{K_A K_B} := \mathcal{L}^{(n+1)}_{L_{A_n} A'_n B'_n L_{B_n} \to K_A K_B}(\sigma^{(n)}_{L_{A_n} A'_n B'_n L_{B_n}}), \qquad (3.77)$$

where the key systems K_A and K_B are held by Alice and Bob, respectively.

The goal of the protocol is for Alice and Bob to distill a secret key state, such that the systems K_A and K_B are maximally classical correlated and in tensor product with all of the systems that Eve possesses (see Section 2.7 for a review of tripartite secret key states).

Purifying an LOCC-assisted secret key agreement protocol

As observed in [78,79] and reviewed in Section 2.7, any protocol of the above form can be purified in the following sense.

The initial state $\rho^{(1)}_{L_{A_1} A_1' B_1' L_{B_1}} \in \mathrm{SEP}(L_{A_1} A_1' : B_1' L_{B_1})$ is of the following form:

$$\rho^{(1)}_{L_{A_1} A_1' B_1' L_{B_1}} := \sum_{y_1} p_{Y_1}(y_1) \tau^{y_1}_{L_{A_1} A_1'} \otimes \varsigma^{y_1}_{L_{B_1} B_1'}. \tag{3.78}$$

The classical random variable Y_1 corresponds to a message exchanged between Alice and Bob to establish this state. It can be purified in the following way:

$$|\psi^{(1)}\rangle_{Y_1 S_{A_1} L_{A_1} A_1' B_1' L_{B_1} S_{B_1}} := \sum_{y_1} \sqrt{p_{Y_1}(y_1)} \, |y_1\rangle_{Y_1} \otimes |\tau^{y_1}\rangle_{S_{A_1} L_{A_1} A_1'} \otimes |\varsigma^{y_1}\rangle_{S_{B_1} L_{B_1} B_1'}, \tag{3.79}$$

where S_{A_1} and S_{B_1} are local "shield" systems that in principle could be held by Alice and Bob, respectively, $|\tau^{y_1}\rangle_{S_{A_1} L_{A_1} A_1'}$ and $|\varsigma^{y_1}\rangle_{S_{B_1} L_{B_1} B_1'}$ purify $\tau^{y_1}_{L_{A_1} A_1'}$ and $\varsigma^{y_1}_{L_{B_1} B_1'}$, respectively, and Eve possesses system Y_1, which contains a coherent classical copy of the classical data exchanged between Alice and Bob. Each LOCC channel $\mathcal{L}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A_i' B_i' L_{B_i}}$ can be written in the following form [26], for all $i \in \{2, 3, \ldots, n\}$:

$$\mathcal{L}^{(i)}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to L_{A_i} A_i' B_i' L_{B_i}} := \sum_{y_i} \mathcal{E}^{y_i}_{L_{A_{i-1}} A_{i-1} \to L_{A_i} A_i'} \otimes \mathcal{F}^{y_i}_{B_{i-1} L_{B_{i-1}} \to B_i' L_{B_i}}, \tag{3.80}$$

where $\{\mathcal{E}^{y_i}_{L_{A_{i-1}} A_{i-1} \to L_{A_i} A_i'}\}_{y_i}$ and $\{\mathcal{F}^{y_i}_{B_{i-1} L_{B_{i-1}} \to B_i' L_{B_i}}\}_{y_i}$ are collections of completely positive, trace non-increasing maps such that the map in (3.80) is trace preserving. Such an LOCC channel can be purified to an isometry in the following way:

$$U^{\mathcal{L}^{(i)}}_{L_{A_{i-1}} A_{i-1} B_{i-1} L_{B_{i-1}} \to Y_i S_{A_i} L_{A_i} A_i' B_i' L_{B_i} S_{B_i}} := \sum_{y_i} |y_i\rangle_{Y_i} \otimes U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}} A_{i-1} \to S_{A_i} L_{A_i} A_i'} \otimes U^{\mathcal{F}^{y_i}}_{B_{i-1} L_{B_{i-1}} \to B_i' L_{B_i} S_{B_i}}, \tag{3.81}$$

where $\{U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}} A_{i-1} \to S_{A_i} L_{A_i} A_i'}\}_{y_i}$ and $\{U^{\mathcal{F}^{y_i}}_{B_{i-1} L_{B_{i-1}} \to B_i' L_{B_i} S_{B_i}}\}_{y_i}$ are collections of linear operators (each of which is a contraction, i.e., $\left\| U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}} A_{i-1} \to S_{A_i} L_{A_i} A_i'} \right\|_\infty, \left\| U^{\mathcal{F}^{y_i}}_{B_{i-1} L_{B_{i-1}} \to B_i' L_{B_i} S_{B_i}} \right\|_\infty \leq 1$ for all y_i) such that the linear operator $U^{\mathcal{L}^{(i)}}$ in (3.81) is an isometry, the system Y_i being held by Eve. The final LOCC channel can be written similarly as

$$\mathcal{L}^{(n+1)}_{L_{A_n} A_n' B_n' L_{B_n} \to K_A K_B} := \sum_{y_{n+1}} \mathcal{E}^{y_{n+1}}_{L_{A_n} A_n \to K_A} \otimes \mathcal{F}^{y_{n+1}}_{B_n L_{B_n} \to K_B}, \tag{3.82}$$

and it can be purified to an isometry similarly as

$$U^{\mathcal{L}^{(n+1)}}_{L_{A_n} A_n B_n L_{B_n} \to Y_{n+1} S_{A_{n+1}} K_A K_B S_{B_{n+1}}} := \sum_{y_{n+1}} |y_{n+1}\rangle_{Y_{n+1}} \otimes U^{\mathcal{E}^{y_{n+1}}}_{L_{A_n} A_n \to S_{A_{n+1}} K_A} \otimes U^{\mathcal{F}^{y_{n+1}}}_{K_B S_{B_{n+1}}}. \tag{3.83}$$

Furthermore, each channel use $\mathcal{N}_{A_i' B_i' \to A_i B_i}$, for all $i \in \{1, 2, \ldots, n\}$, is purified by an isometry $U^{\mathcal{N}}_{A_i' B_i' \to A_i B_i E_i}$, such that Eve possesses the environment system E_i.

At the end of the purified protocol, Alice possesses the key system K_A and the shield systems $S_A := S_{A_1} S_{A_2} \cdots S_{A_{n+1}}$, Bob possesses the key system K_B and the shield systems $S_B := S_{B_1} S_{B_2} \cdots S_{B_{n+1}}$, and Eve possesses the environment systems $E^n := E_1 E_2 \cdots E_n$ as well as the coherent copies $Y^{n+1} := Y_1 Y_2 \cdots Y_{n+1}$ of the classical data exchanged between Alice and Bob. The state at the end of the protocol is a pure state $\omega_{Y^{n+1} S_A K_A K_B S_B E^n}$.

For a fixed n, $|K| \in \mathbb{N}$, $\varepsilon \in [0, 1]$, the original protocol is an (n, K, ε) protocol if the channel is used n times as discussed above, $|K_A| = |K_B| = |K|$, and if

$$F(\omega_{S_A K_A K_B S_B}, \gamma_{S_A K_A K_B S_B}) \geq 1 - \varepsilon, \tag{3.84}$$

where $\gamma_{S_A K_A K_B S_B}$ is a bipartite private state. A rate P is said to be achievable for LOCC-assisted secret key agreement if for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n, there exists an $(n, P - \delta, \varepsilon)$ protocol. The LOCC-assisted secret-key-agreement capacity of a bidirectional channel $\mathcal{N}$, denoted as $P^{2 \to 2}_{\text{LOCC}}(\mathcal{N})$, is equal to the supremum of all achievable rates. Whereas, a rate R is a strong converse rate for LOCC-assisted secret key agreement if for all $\varepsilon \in [0, 1)$, $\delta > 0$, and sufficiently large n, there does not exist an $(n, R + \delta, \varepsilon)$ protocol. The strong converse LOCC-assisted secret-key-agreement capacity $\widetilde{P}^{2 \to 2}_{\text{LOCC}}(\mathcal{N})$ is equal to the infimum of all strong converse rates. A bidirectional channel $\mathcal{N}$ is said to obey the strong converse property for LOCC-assisted secret key agreement if $P^{2 \to 2}_{\text{LOCC}}(\mathcal{N}) = \widetilde{P}^{2 \to 2}_{\text{LOCC}}(\mathcal{N})$.

Note that the identity channel corresponding to no assistance is an LOCC channel. Therefore, we can also consider the whole development discussed above for bidirectional private communication without any assistance or feedback instead of LOCC-assisted communication. All the notions discussed above follow when we exempt the employment of any non-trivial LOCC-assistance. It

follows that, unassisted bidirectional private capacity $P_{\text{n-a}}^{2\to2}(\mathcal{N})$ and the strong converse unassisted bidirectional private capacity $\widetilde{P}_{\text{n-a}}^{2\to2}(\mathcal{N})$ are bounded from above as

$$P_{\text{n-a}}^{2\to2}(\mathcal{N}) \le P_{\text{LOCC}}^{2\to2}(\mathcal{N}), \tag{3.85}$$

$$\widetilde{P}_{\text{n-a}}^{2\to2}(\mathcal{N}) \le \widetilde{P}_{\text{LOCC}}^{2\to2}(\mathcal{N}). \tag{3.86}$$

The following lemma will be useful in deriving upper bounds on the bidirectional secret-key-agreement capacity of a bidirectional channel. Its proof is very similar to the proof of Lemma 3.1, and so we omit it.

Lemma 3.2 *Let* $\text{Ent}_{\text{LOCC}}(A; B)_\rho$ *be a bipartite entanglement measure for an arbitrary bipartite state* ρ_{AB}*. Suppose that* $\text{Ent}_{\text{LOCC}}(A; B)_\rho$ *vanishes for all* $\rho_{AB} \in \text{SEP}(A : B)$ *and is monotone non-increasing under LOCC channels. Consider an* (n, K, ε) *protocol for LOCC-assisted secret key agreement over a bidirectional quantum channel* $\mathcal{N}_{A'B'\to AB}$ *as described in Section 3.3.2. Then the following bound holds:*

$$\text{Ent}_{\text{LOCC}}(S_A K_A; K_B S_B)_\omega \le n\,\text{Ent}_{\text{LOCC},A}(\mathcal{N}), \tag{3.87}$$

where $\text{Ent}_{\text{LOCC},A}(\mathcal{N})$ *is the amortized entanglement of a bidirectional channel* $\mathcal{N}$*, i.e.,*

$$\text{Ent}_{\text{LOCC},A}(\mathcal{N}) := \sup_{\rho_{L_A A'B'L_B} \in \mathscr{D}(\mathcal{H}_{L_A A'B'L_B})} \left[\text{Ent}_{\text{LOCC}}(L_A A; BL_B)_\sigma - \text{Ent}_{\text{LOCC}}(L_A A'; B'L_B)_\rho\right], \tag{3.88}$$

and $\sigma_{L_A ABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$.

Strong converse rate for LOCC-assisted secret key agreement

We now prove the following upper bound on the bidirectional secret key agreement rate $P = \frac{1}{n}\log_2|K|$ (secret bits per channel use) of any (n, P, ε) LOCC-assisted secret-key-agreement protocol over a bidirectional channel $\mathcal{N}$:

Theorem 3.2 *For a fixed* n*,* $|K| \in \mathbb{N}$*,* $\varepsilon \in (0, 1)$*, the following bound holds for an* (n, P, ε) *protocol*

for LOCC-assisted secret key agreement over a bidirectional quantum channel $\mathcal{N}$:

$$\frac{1}{n} \log_2 K \leq E_{\max}^{2\to2}(\mathcal{N}) + \frac{1}{n} \log_2 \left(\frac{1}{1-\varepsilon} \right), \tag{3.89}$$

such that $P = \frac{1}{n} \log_2 |K|$.

Proof. From Section 3.3.2, the following inequality holds for an $(n, |K|, \varepsilon)$ protocol:

$$F(\omega_{S_A K_A K_B S_B}, \gamma_{S_A K_A K_B S_B}) \geq 1 - \varepsilon, \tag{3.90}$$

for some bipartite private state $\gamma_{S_A K_A K_B S_B}$ with key dimension $|K|$. From Section 2.7, $\omega_{S_A K_A K_B S_B}$ passes a γ-privacy test with probability at least $1-\varepsilon$, whereas any $\tau_{S_A K_A K_B S_B} \in \text{SEP}(S_A K_A : K_B S_B)$ does not pass with probability greater than $\frac{1}{|K|}$ [79]. Making use of the discussion in [74, Sections III & IV] (i.e., from the monotonicity of the max-relative entropy of entanglement under the γ-privacy test), it can be concluded that

$$\log_2 |K| \leq E_{\max}(S_A K_A; K_B S_B)_\omega + \log_2 \left(\frac{1}{1-\varepsilon} \right). \tag{3.91}$$

Applying Lemma 3.2 and Corollary 3.3, we get that

$$E_{\max}(S_A K_A; K_B S_B)_\omega \leq n E_{\max}^{2\to2}(\mathcal{N}). \tag{3.92}$$

Combining (3.91) and (3.92), we get the desired inequality in (3.89). ∎

Remark 3.5 *Note that Theorem 3.2 applies in the case that the bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is an infinite-dimensional bipartite channel, taking input density operators acting on a separable Hilbert space to output density operators acting on a separable Hilbert space. We arrive at this conclusion because the max-relative entropy is well defined for infinite-dimensional states.*

Remark 3.6 *The bound in (3.89) can also be rewritten as*

$$1 - \varepsilon \leq 2^{-n[P - E_{\max}^{2\to2}(\mathcal{N})]}. \tag{3.93}$$

Thus, if the bidirectional secret-key-agreement rate P is strictly larger than the bidirectional max-relative entropy of entanglement $\mathcal{E}_{\max}^{2\to2}(\mathcal{N})$, then the reliability and security of the transmission $(1-\varepsilon)$ decays exponentially fast to zero in the number n of channel uses.

An immediate corollary of the above remark is the following strong converse statement:

Corollary 3.4 *The strong converse LOCC-assisted bidirectional secret-key-agreement capacity of a bidirectional channel $\mathcal{N}$ is bounded from above by its bidirectional max-relative entropy of entanglement:*

$$\widetilde{P}_{\mathrm{LOCC}}^{2\to2}(\mathcal{N}) \leq E_{\max}^{2\to2}(\mathcal{N}). \tag{3.94}$$

3.4 Entangling abilities of symmetric interactions

Interactions obeying particular symmetries have played an important role in several quantum information processing tasks in the context of quantum communication protocols [49–51], quantum computing and quantum metrology [125–127], and resource theories [128, 129], etc.

In this section, we define bidirectional PPT- and teleportation-simulable channels by adapting the definitions of point-to-point PPT- and LOCC-simulable channels [50, 51, 54] to the bidirectional setting. Then, we derive upper bounds on the entanglement and secret-key-agreement capacities for communication protocols that employ bidirectional PPT- and teleportation-simulable channels, respectively. These bounds are generally tighter than those given in the previous section, because they exploit the symmetry inherent in bidirectional PPT- and teleportation-simulable channels.

Definition 3.4 (Bidirectional PPT-simulable) *A bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is PPT-simulable with an associated resource state $\theta_{\hat{S}_A\hat{S}_B} \in \mathscr{D}\left(\mathcal{H}_{\hat{S}_A\hat{S}_B}\right)$ if for all input states $\rho_{A'B'} \in \mathscr{D}\left(\mathcal{H}_{A'B'}\right)$ the following equality holds*

$$\mathcal{N}_{A'B'\to AB}\left(\rho_{A'B'}\right) = \mathcal{P}_{\hat{S}_A A'B'\hat{S}_B\to AB}\left(\rho_{A'B'} \otimes \theta_{\hat{S}_A\hat{S}_B}\right), \tag{3.95}$$

with $\mathcal{P}_{\hat{S}_A A'B'\hat{S}_B\to AB}$ being a PPT-preserving channel acting on $\hat{S}_A A':B'\hat{S}_B$, where the partial transposition acts on the composite system $B'\hat{S}_B$.

The following definition was given in [130] for the special case of bipartite unitary channels:

Definition 3.5 (Bidirectional teleportation-simulable) *A bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is teleportation-simulable with associated resource state $\theta_{\hat{S}_A\hat{S}_B} \in \mathscr{D}\left(\mathcal{H}_{\hat{S}_A\hat{S}_B}\right)$ if for all input states $\rho_{A'B'} \in \mathscr{D}\left(\mathcal{H}_{A'B'}\right)$ the following equality holds*

$$\mathcal{N}_{A'B'\to AB}\left(\rho_{A'B'}\right) = \mathcal{L}_{\hat{S}_AA'B'\hat{S}_B\to AB}\left(\rho_{A'B'} \otimes \theta_{\hat{S}_A\hat{S}_B}\right), \tag{3.96}$$

where $\mathcal{L}_{\hat{S}_AA'B'\hat{S}_B\to AB}$ is an LOCC channel acting on $\hat{S}_AA' : B'\hat{S}_B$.

Let $\mathscr{G}$ and $\mathscr{H}$ be finite groups of sizes $|G|$ and $|H|$, respectively. For $g \in \mathscr{G}$ and $h \in \mathscr{H}$, let $g \to U_{A'}(g)$ and $h \to V_{B'}(h)$ be unitary representations. Also, let $(g,h) \to W_A(g,h)$ and $(g,h) \to T_B(g,h)$ be unitary representations. A bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ is *bicovariant* with respect to these representations if the following relation holds for all input density operators $\rho_{A'B'}$ and group elements $g \in \mathscr{G}$ and $h \in \mathscr{H}$:

$$\mathcal{N}_{A'B'\to AB}((\mathcal{U}_{A'}(g) \otimes \mathcal{V}_{B'}(h))(\rho_{A'B'})) = (\mathcal{W}_A(g,h) \otimes \mathcal{T}_B(g,h))(\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})), \tag{3.97}$$

where $\mathcal{U}(g)(\cdot) := U(g)(\cdot)(U(g))^\dagger$, $\mathcal{V}(h)(\cdot) := V(h)(\cdot)(V(h))^\dagger$, $\mathcal{T}(g,h)(\cdot) := T(g,h)(\cdot)(T(g,h))^\dagger$, and $\mathcal{W}(g,h)(\cdot) := W(g,h)(\cdot)(W(g,h))^\dagger$ are unitary channels associated with respective unitary operators.

Definition 3.6 (Bicovariant channel) *A bidirectional channel is called bicovariant if it is bicovariant with respect to groups that have representations as unitary one-designs, i.e., for all $\rho_{A'} \in \mathscr{D}(\mathcal{H}_{A'})$ and $\rho_{B'} \in \mathscr{D}(\mathcal{H}_{B'})$,*

$$\frac{1}{|G|}\sum_g \mathcal{U}_{A'}(g)(\rho_{A'}) = \pi_{A'} \text{ and } \frac{1}{|H|}\sum_h \mathcal{V}_{B'}(h)(\rho_{B'}) = \pi_{B'}, \tag{3.98}$$

where $\pi_{A'}$ and $\pi_{B'}$ are maximally mixed states.

An example of a bidirectional channel that is bicovariant is the controlled-NOT (CNOT) gate

[106], for which we have the following covariances [131, 132]:

$$\text{CNOT}(X \otimes \mathbb{1}) = (X \otimes X)\text{CNOT}, \tag{3.99}$$

$$\text{CNOT}(Z \otimes \mathbb{1}) = (Z \otimes \mathbb{1})\text{CNOT}, \tag{3.100}$$

$$\text{CNOT}(Y \otimes \mathbb{1}) = (Y \otimes X)\text{CNOT}, \tag{3.101}$$

$$\text{CNOT}(\mathbb{1} \otimes X) = (\mathbb{1} \otimes X)\text{CNOT}, \tag{3.102}$$

$$\text{CNOT}(\mathbb{1} \otimes Z) = (Z \otimes Z)\text{CNOT}, \tag{3.103}$$

$$\text{CNOT}(\mathbb{1} \otimes Y) = (Z \otimes Y)\text{CNOT}, \tag{3.104}$$

where $\{\mathbb{1}, X, Y, Z\}$ is the Pauli group with the identity element $\mathbb{1}$. A more general example of a bicovariant channel is one that applies a CNOT with some probability and, with the complementary probability, replaces the input with the maximally mixed state.

In [132], the prominent idea of gate teleportation was developed, wherein one can generate the Choi state for the CNOT gate by sending in shares of maximally entangled states and then simulate the CNOT gate's action on any input state by using teleportation through the Choi state (see also [133] for earlier related developments). This idea generalized the notion of teleportation simulation of channels [50, 51] from the single-sender single-receiver setting to the bidirectional setting. After these developments, [48, 134] generalized the idea of gate teleportation to bipartite quantum channels that are not necessarily unitary channels.

The following result slightly generalizes the developments in [48, 132, 134]:

Proposition 3.3 *If a bidirectional channel* $\mathcal{N}_{A'B' \to AB}$ *is bicovariant, Definition 3.6, then it is teleportation-simulable with a resource state* $\theta_{L_A AB L_B} = \mathcal{N}_{A'B' \to AB}(\Phi_{L_A A'} \otimes \Phi_{B'L_B})$.

Proof. Let $\mathcal{N}_{A'B' \to AB}$ be a bidirectional quantum channel. Given $\mathscr{G}$ and $\mathscr{H}$ are groups with unitary representations $g \to \mathcal{U}_{A'}(g)$ and $h \to \mathcal{V}_{B'}(h)$ and $(g, h) \to W_A(g, h)$ and $(g, h) \to T_B(g, h)$, such that

$$\frac{1}{|G|} \sum_g \mathcal{U}_{A'}(g)(X_{A'}) = \text{Tr}\{X_{A'}\}\pi_{A'}, \tag{3.105}$$

$$\frac{1}{|H|} \sum_h \mathcal{V}_{B'}(h)(Y_{B'}) = \text{Tr}\{Y_{B'}\}\pi_{B'}, \tag{3.106}$$

63

$$\mathcal{N}_{A'B'\to AB}((\mathcal{U}_{A'}(g)\otimes\mathcal{V}_{B'}(h))(\rho_{A'B'})) = (\mathcal{W}_A(g,h)\otimes\mathcal{T}_B(g,h))(\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})), \tag{3.107}$$

where $X_{A'}\in\mathcal{B}(\mathcal{H}_{A'})$, $Y_{B'}\in\mathcal{B}(\mathcal{H}_{B'})$, and π denotes the maximally mixed state. Consider that

$$\frac{1}{|G|}\sum_g \mathcal{U}_{A''}(g)(\Phi_{A''A'}) = \pi_{A''}\otimes\pi_{A'}, \tag{3.108}$$

where Φ denotes a maximally entangled state and A'' is a system isomorphic to A'. Similarly,

$$\frac{1}{|H|}\sum_h \mathcal{V}_{B''}(h)(\Phi_{B''B'}) = \pi_{B''}\otimes\pi_{B'}. \tag{3.109}$$

Note that in order for $\{U_{A'}^g\}$ to satisfy (3.105), it is necessary that $|A'|^2 \leq |G|$ [135]. Similarly, it is necessary that $|B'|^2 \leq |H|$. Consider the POVM $\{E_{A''L_A}^g\}_g$, with each element $E_{A''L_A}^g$ defined as

$$E_{A''L_A}^g := \frac{|A'|^2}{|G|}U_{A''}^g\Phi_{A''L_A}\left(U_{A''}^g\right)^\dagger. \tag{3.110}$$

It follows from the fact that $|A'|^2 \leq |G|$ and (3.108) that $\{E_{A''L_A}^g\}_g$ is a valid POVM. Similarly, let us fine the POVM $\{F_{B''L_B}^h\}_h$ as

$$F_{B''L_B}^h := \frac{|B'|^2}{|H|}V_{B''}^h\Phi_{B''L_B}\left(V_{B''}^h\right)^\dagger. \tag{3.111}$$

The simulation of the channel $\mathcal{N}_{A'B'\to AB}$ via teleportation begins with a state $\rho_{A''B''}$ and a shared resource $\theta_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'}\otimes\Phi_{B'L_B})$. The desired outcome is for the receivers to receive the state $\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})$ and for the protocol to work independently of the input state $\rho_{A'B'}$. The first step is for the senders to locally perform the measurement $\{E_{A''L_A}^g\otimes F_{B''L_B}^h\}_{g,h}$ and then send the outcomes g and h to the receivers. Based on the outcomes g and h, the receivers then perform $W_A^{g,h}$ and $T_B^{g,h}$. The following analysis demonstrates that this protocol works, by simplifying the

form of the post-measurement state:

$$|G|\,|H|\,\mathrm{Tr}_{A''L_AB''L_B}\{(E^g_{A''L_A} \otimes F^h_{B''L_B})(\rho_{A''B''} \otimes \theta_{L_AABL_B})\}$$

$$= |A'|^2\,|B'|^2\,\mathrm{Tr}_{A''L_AB''L_B}\{[U^g_{A''}\Phi_{A''L_A}(U^g_{A''})^\dagger \otimes V^h_{B''}\Phi_{B''L_B}(V^h_{B''})^\dagger](\rho_{A''B''} \otimes \theta_{L_AABL_B})\} \qquad (3.112)$$

$$= |A'|^2\,|B'|^2\,\langle\Phi|_{A''L_A} \otimes \langle\Phi|_{B''L_B}(U^g_{A''} \otimes V^h_{B''})^\dagger(\rho_{A''B''} \otimes \theta_{L_AABL_B})(U^g_{A''} \otimes V^h_{B''})|\Phi\rangle_{A''L_A} \otimes |\Phi\rangle_{B''L_B}$$

$$(3.113)$$

$$= |A'|^2\,|B'|^2\,\langle\Phi|_{A''L_A} \otimes \langle\Phi|_{B''L_B}\left[(U^g_{A''} \otimes V^h_{B''})^\dagger\rho_{A''B''}(U^g_{A''} \otimes V^h_{B''})\right]$$

$$\otimes\,\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'} \otimes \Phi_{B'L_B}))|\Phi\rangle_{A''L_A} \otimes |\Phi\rangle_{B''L_B} \qquad (3.114)$$

$$= |A'|^2\,|B'|^2\,\langle\Phi|_{A''L_A} \otimes \langle\Phi|_{B''L_B}\left[(U^g_{L_A} \otimes V^h_{L_B})^\dagger\rho_{L_AL_B}(U^g_{L_A} \otimes V^h_{L_B})\right]^*$$

$$\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'} \otimes \Phi_{B'L_B}))|\Phi\rangle_{A''L_A} \otimes |\Phi\rangle_{B''L_B}. \qquad (3.115)$$

The first three equalities follow by substitution and some rewriting. The fourth equality follows from the fact that

$$\langle\Phi|_{A'A}M_{A'} = \langle\Phi|_{A'A}M^*_A \qquad (3.116)$$

for any operator M and where $*$ denotes the complex conjugate, taken with respect to the basis in which $|\Phi\rangle_{A'A}$ is defined. Continuing, we have that

$$(3.115) = |A'|\,|B'|\,\mathrm{Tr}_{L_AL_B}\left\{\left[(U^g_{L_A} \otimes V^h_{L_B})^\dagger\rho_{L_AL_B}(U^g_{L_A} \otimes V^h_{L_B})\right]^*\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'} \otimes \Phi_{B'L_B}))\right\}$$

$$(3.117)$$

$$= |A'|\,|B'|\,\mathrm{Tr}_{L_AL_B}\left\{\mathcal{N}_{A'B'\to AB}\left(\left[(U^g_{A'} \otimes V^h_{B'})^\dagger\rho_{A'B'}(U^g_{A'} \otimes V^h_{B'})\right]^\dagger(\Phi_{L_AA'} \otimes \Phi_{B'L_B})\right)\right\}$$

$$(3.118)$$

$$= \mathcal{N}_{A'B'\to AB}\left(\left[(U^g_{A'} \otimes V^h_{B'})^\dagger\rho_{A'B'}(U^g_{A'} \otimes V^h_{B'})\right]^\dagger\right) \qquad (3.119)$$

$$= \mathcal{N}_{A'B'\to AB}\left((U^g_{A'} \otimes V^h_{B'})^\dagger\rho_{A'B'}(U^g_{A'} \otimes V^h_{B'})\right) \qquad (3.120)$$

$$= \left(W^{g,h}_A \otimes T^{g,h}_B\right)^\dagger\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})\left(W^{g,h}_A \otimes T^{g,h}_B\right) \qquad (3.121)$$

The first equality follows because $|A|\,\langle\Phi|_{A'A}(\mathbb{1}_{A'} \otimes M_{AB})|\Phi\rangle_{A'A} = \mathrm{Tr}_A\{M_{AB}\}$ for any operator M_{AB}. The second equality follows by applying the conjugate transpose of (3.116). The final

equality follows from the covariance property of the channel.

Thus, if the receivers finally perform the unitaries $W_A^{g,h} \otimes T_B^{g,h}$ upon receiving g and h via a classical channel from the senders, then the output of the protocol is $\mathcal{N}_{A'B' \to AB}(\rho_{A'B'})$, so that this protocol simulates the action of the channel $\mathcal{N}$ on the state ρ. ∎

We now establish an upper bound on the entanglement generation rate of any (n, M, ε) PPT-assisted protocol that employs a bidirectional PPT-simulable channel.

Theorem 3.3 *For a fixed n, $|M| \in \mathbb{N}$, $\varepsilon \in (0,1)$, the following strong converse bound holds for an (n, Q, ε) protocol for PPT-assisted entanglement generation over a bidirectional PPT-simulable quantum channel $\mathcal{N}$ with an associated resource state $\theta_{\hat{S}_A \hat{S}_B}$, Definition 3.4,*

$$\forall \alpha > 1, \quad Q \leq \widetilde{R}_\alpha(\hat{S}_A; \hat{S}_B)_\theta + \frac{\alpha}{n(\alpha - 1)} \log_2\left(\frac{1}{1 - \varepsilon}\right) \tag{3.122}$$

such that $Q = \frac{1}{n} \log_2 |M|$, where $\widetilde{R}_\alpha(\hat{S}_A; \hat{S}_B)_\theta$ is the sandwiched Rains information (2.87) of the state $\theta_{\hat{S}_A \hat{S}_B}$.

Proof. The first few steps are similar to those in the proof of Theorem 3.1. From Section 3.2.2, we have that

$$\text{Tr}\{\Phi_{M_A M_B} \omega_{M_A M_B}\} \geq 1 - \varepsilon, \tag{3.123}$$

while [46, Lemma 2] implies that

$$\forall \sigma_{M_A M_B} \in \text{PPT}'(M_A : M_B), \ \text{Tr}\{\Phi_{M_A M_B} \sigma_{M_A M_B}\} \leq \frac{1}{|M|}. \tag{3.124}$$

Under an "entanglement test", which is a measurement with POVM $\{\Phi_{M_A M_B}, \mathbb{1}_{M_A M_B} - \Phi_{M_A M_B}\}$, and applying the data processing inequality for the sandwiched Rényi relative entropy, we find that, for all $\alpha > 1$,

$$\log_2 |M| \leq \widetilde{R}_\alpha(M_A; M_B)_\omega + \frac{\alpha}{\alpha - 1} \log_2\left(\frac{1}{1 - \varepsilon}\right). \tag{3.125}$$

The sandwiched Rains relative entropy is monotonically non-increasing under the action of PPT-

preserving channels and vanishing for a PPT state. Applying Lemma 3.1, we find that

$$\widetilde{R}_\alpha(M_A; M_B)_\omega \le n \sup_{\rho_{L_A A' B' L_B}} \left[\widetilde{R}_\alpha(L_A A; B L_B)_{\mathcal{N}(\rho)} - \widetilde{R}_\alpha(L_A A'; B' L_B)_\rho \right]. \qquad (3.126)$$

As stated in Definition 3.4, a PPT-simulable bidirectional channel $\mathcal{N}_{A'B'\to AB}$ with an associated resource state $\theta_{\hat{S}_A \hat{S}_B}$ is such that, for any input state $\rho'_{A'B'}$,

$$\mathcal{N}_{A'B'\to AB}\left(\rho'_{A'B'}\right) = \mathcal{P}_{\hat{S}_A A' B' \hat{S}_B \to AB}\left(\rho'_{A'B'} \otimes \theta_{\hat{S}_A \hat{S}_B}\right). \qquad (3.127)$$

Then, for any input state $\omega'_{L_A A' B' L_B}$,

$$\widetilde{R}_\alpha(L_A A; B L_B)_{\mathcal{P}(\omega'\otimes\theta)} - \widetilde{R}_\alpha(L_A A'; B' L_B)_{\omega'}$$

$$\le \widetilde{R}_\alpha(L_A \hat{S}_A A'; B' \hat{S}_B L_B)_{\omega'\otimes\theta} - \widetilde{R}_\alpha(L_A A'; B' L_B)_{\omega'} \qquad (3.128)$$

$$\le \widetilde{R}_\alpha(L_A A'; B' L_B)_{\omega'} + \widetilde{R}_\alpha(\hat{S}_A; \hat{S}_B)_\theta - \widetilde{R}_\alpha(L_A A'; B' L_B)_{\omega'} \qquad (3.129)$$

$$= \widetilde{R}_\alpha(\hat{S}_A; \hat{S}_B)_\theta. \qquad (3.130)$$

The first inequality follows from monotonicity of $\widetilde{R}_\alpha$ with respect to PPT-preserving channels. The second inequality follows because $\widetilde{R}_\alpha$ is sub-additive with respect to tensor-product states.

Applying the bound in (3.130) to (3.126), we find that

$$\widetilde{R}_\alpha(M_A; M_B)_\omega \le n \widetilde{R}_\alpha(\hat{S}_A; \hat{S}_B)_\theta. \qquad (3.131)$$

Combining (3.125) and (3.131), we get the desired inequality in (3.122). ∎

Now we establish an upper bound on the secret key rate of an $(n, |K|, \varepsilon)$ secret-key-agreement protocol that employs a bidirectional teleportation-simulable channel.

Theorem 3.4 *For a fixed n, $|K| \in \mathbb{N}$, $\varepsilon \in (0, 1)$, the following strong converse bound holds for an (n, P, ε) protocol for secret key agreement over a bidirectional teleportation-simulable quantum*

channel $\mathcal{N}$ *with an associated resource state* $\theta_{\hat{S}_A\hat{S}_B}$:

$$\forall \alpha > 1, \quad P \leq \widetilde{E}_\alpha(\hat{S}_A; \hat{S}_B)_\theta + \frac{\alpha}{n(\alpha - 1)} \log_2\left(\frac{1}{1-\varepsilon}\right) \tag{3.132}$$

such that $P = \frac{1}{n}\log_2|K|$, *where* $\widetilde{E}_\alpha(\hat{S}_A; \hat{S}_B)_\theta$ *is the sandwiched relative entropy of entanglement* (2.95) *of the state* $\theta_{\hat{S}\hat{S}_B}$.

Proof. As stated in Definition 3.4, a bidirectional teleportation-simulable channel $\mathcal{N}_{A'B'\to AB}$ is such that, for any input state $\rho'_{A'B'}$,

$$\mathcal{N}_{A'B'\to AB}\left(\rho'_{A'B'}\right) = \mathcal{L}_{\hat{S}_A A'B'\hat{S}_B\to AB}\left(\rho'_{A'B'}\otimes\theta_{\hat{S}_A\hat{S}_B}\right). \tag{3.133}$$

Then, for any input state $\omega'_{L_A A'B'L_B}$,

$$\widetilde{E}_\alpha(L_A A; B L_B)_{\mathcal{L}(\omega'\otimes\theta)} - \widetilde{E}_\alpha(L_A A'; B' L_B)_{\omega'}$$

$$\leq \widetilde{E}_\alpha(L_A \hat{S}_A A'; B'\hat{S}_B L_B)_{\omega'\otimes\theta} - \widetilde{E}_\alpha(L_A A'; B' L_B)_{\omega'} \tag{3.134}$$

$$\leq \widetilde{E}_\alpha(L_A A'; B' L_B)_{\omega'} + \widetilde{E}_\alpha(\hat{S}_A; \hat{S}_B)_\theta - \widetilde{E}_\alpha(L_A A'; B' L_B)_{\omega'} \tag{3.135}$$

$$= \widetilde{E}_\alpha(\hat{S}_A; \hat{S}_B)_\theta. \tag{3.136}$$

The first inequality follows from monotonicity of $\widetilde{E}_\alpha$ with respect to LOCC channels. The second inequality follows because $\widetilde{E}_\alpha$ is sub-additive.

From Section 3.3.2, the following inequality holds for an (n, P, ε) protocol:

$$F(\omega_{S_A K_A K_B S_B}, \gamma_{S_A K_A K_B S_B}) \geq 1 - \varepsilon, \tag{3.137}$$

for some bipartite private state $\gamma_{S_A K_A K_B S_B}$ with key dimension $|K|$. From Section 2.7, $\omega_{S_A K_A K_B S_B}$ passes a γ-privacy test with probability at least $1-\varepsilon$, whereas any $\tau_{S_A K_A K_B S_B} \in \text{SEP}(S_A K_A : K_B S_B)$ does not pass with probability greater than $\frac{1}{|K|}$ [79]. Making use of the results in [80, Section 5.2],

we conclude that

$$\log_2 |K| \leq \widetilde{E}_\alpha(S_A K_A; K_B S_B)_\omega + \frac{\alpha}{\alpha - 1} \log_2\left(\frac{1}{1 - \varepsilon}\right). \tag{3.138}$$

Now we can follow steps similar to those in the proof of Theorem 3.3 in order to arrive at (3.132).
∎

We can also establish the following weak converse bounds, by combining the above approach with that in [54, Section 3.5]:

Remark 3.7 *The following weak converse bound holds for an (n, Q, ε) PPT-assisted bidirectional quantum communication protocol (Section 3.2.2) that employs a bidirectional PPT-simulable quantum channel $\mathcal{N}$ with an associated resource state $\theta_{\hat{S}_A \hat{S}_B}$*

$$(1 - \varepsilon)Q \leq R(\hat{S}_A; \hat{S}_B)_\theta + \frac{1}{n} h_2(\varepsilon), \tag{3.139}$$

where $R(\hat{S}_A; \hat{S}_B)_\theta$ is defined in (2.85) and $h_2(\varepsilon) := -\varepsilon \log_2 \varepsilon - (1 - \varepsilon) \log_2(1 - \varepsilon)$.

Remark 3.8 *The following weak converse bound holds for an (n, P, ε) LOCC-assisted bidirectional secret key agreement protocol (see Section 3.3.2) that employs a bidirectional teleportation-simulable quantum channel $\mathcal{N}_{A'B' \to AB}$ with an associated resource state $\theta_{\hat{S}_A \hat{S}_B}$*

$$(1 - \varepsilon)P \leq E(\hat{S}_A; \hat{S}_B)_\theta + \frac{1}{n} h_2(\varepsilon), \tag{3.140}$$

where $E(\hat{S}_A; \hat{S}_B)_\theta$ is defined in (2.96).

Since every LOCC channel $\mathcal{L}_{\hat{S}_A A' B' \hat{S}_B \to AB}$ acting with respect to the bipartite cut $\hat{S}_A A' : B' \hat{S}_B$ is also a PPT-preserving channel with the partial transposition action on $B' \hat{S}_B$, it follows that bidirectional teleportation-simulable channels are also bidirectional PPT-simulable channels. Based on Proposition 3.3, Theorem 3.3, Theorem 3.4, and the limits $n \to \infty$ and then $\alpha \to 1$ (in this order),[2] we can then conclude the following strong converse bounds:

---

[2]One could also set $\alpha = 1 + 1/\sqrt{n}$ and then take the limit $n \to \infty$.

Corollary 3.5 *If a bidirectional quantum channel $\mathcal{N}$ is bicovariant (Definition 3.6), then*

$$\widetilde{Q}_{\mathrm{PPT}}^{2\to2}(\mathcal{N}) \le R(L_A A; B L_B)_\theta, \tag{3.141}$$

$$\widetilde{P}_{\mathrm{LOCC}}^{2\to2}(\mathcal{N}) \le E(L_A A; B L_B)_\theta, \tag{3.142}$$

where $\theta_{L_A A B L_B} = \mathcal{N}_{A'B'\to AB}(\Phi_{L_A A'} \otimes \Phi_{B'L_B})$, and $\widetilde{Q}_{\mathrm{PPT}}^{2\to2}(\mathcal{N})$ and $\widetilde{P}_{\mathrm{LOCC}}^{2\to2}(\mathcal{N})$ denote the strong converse PPT-assisted bidirectional quantum capacity and strong converse LOCC-assisted bidirectional secret-key-agreement capacity, respectively, of a bidirectional channel $\mathcal{N}$.

3.5 Conclusion

In this chapter, we mainly focused on two different information processing tasks: entanglement distillation and secret key distillation using bipartite quantum interactions or bidirectional channels. We determined several bounds on the entanglement and secret-key-agreement capacities of bipartite quantum interactions. In deriving these bounds, we described communication protocols in the bidirectional setting, related to those discussed in [84] and which generalize related point-to-point communication protocols. We defined an entanglement measure called the bidirectional max-Rains information of a bidirectional channel and showed that it is a strong converse upper bound on the PPT-assisted quantum capacity of the given bidirectional channel. We also defined a related entanglement measure called the bidirectional max-relative entropy of entanglement and showed that it is a strong converse bound on the LOCC-assisted secret-key-agreement capacity of a given bidirectional channel. When the bidirectional channels are either teleportation- or PPT-simulable, the upper bounds on the bidirectional quantum and bidirectional secret-key-agreement capacities depend only on the entanglement of an underlying resource state. If a bidirectional channel is bicovariant, then the underlying resource state can be taken to be the Choi state of the bidirectional channel.

Chapter 4 Fundamental Limits on Quantum Dynamics Based on Entropy Change

Entropy is a fundamental quantity that is of wide interest in physics and information theory [24, 28, 136, 137]. Many natural phenomena are described according to laws based on entropy, like the second law of thermodynamics [138–140], entropic uncertainty relations in quantum mechanics and information theory [9, 141–144], and area laws in black holes and condensed matter physics [35, 145–147].

No quantum system can be perfectly isolated from its environment. The interaction of a system with its environment generates correlations between the system and the environment. In realistic situations, instead of isolated systems, we must deal with open quantum systems, that is, systems whose environment is not under the control of the observer. The interaction between the system and the environment can cause a loss of information as a result of decoherence, dissipation, or decay phenomena [22, 148, 149]. The rate of entropy change quantifies the flow of information between the system and its environment.

In this chapter, we focus on the von Neumann entropy, which is defined for a system in the state ρ as $S(\rho) := -\operatorname{Tr}\{\rho \log \rho\}^1$, and from here onwards we refer to it as the entropy. The entropy is monotonically non-decreasing under doubly-stochastic, also called unital, physical evolutions [150, 151]. This has restricted the use of entropy change in the characterization of quantum dynamics only to unital dynamics [152–155]. Recently, [33] gave a lower bound on the entropy change for any positive trace-preserving map. Lower bounds on the entropy change have also been discussed in [152, 155–157] for certain classes of time evolution. Natural questions that arise are as follows: what are the limits placed by the bound[2] on the entropy change on the dynamics of a system, and can it be used to characterize evolution processes?

Most of this chapter is reproduced from [Siddhartha Das, Sumeet Khatri, George Siopsis, and Mark M. Wilde. *Journal of Mathematical Physics*, 59(1):012205, (2018)], with the permission of AIP Publishing (see Appendix D).

[1]In this chapter, we particularly use natural logarithm in the definition of the entropy and the relative entropy.

[2]Specifically, we consider the bound in [33, Theorem 1] as it holds for arbitrary evolution of both finite- and infinite-dimensional systems.

We delve into these questions, at first, by inspecting another pertinent question: at what rate does the entropy of a quantum system change? Although the answer is known for Markovian one-parameter semigroup dynamics of a finite-dimensional system with full-rank states [158], the answer in full generality has not yet been given. In [159], the result of [158] was extended to infinite-dimensional systems with full-rank states undergoing Markovian one-parameter semigroup dynamics (cf., [160]). We now prove that the formula derived in [158] holds not only for finite-dimensional quantum systems undergoing Markovian one-parameter semigroup dynamics, but also for arbitrary dynamics of both finite- and infinite-dimensional systems with states of arbitrary rank. We then derive a lower bound on the rate of entropy change for any memoryless quantum evolution, also called a quantum Markov process. This lower bound is a witness of non-unitality in quantum Markov processes. Interestingly, this lower bound also helps us to derive witnesses for the presence of memory effects, i.e., non-Markovianity, in quantum dynamics. We compare one of our witnesses to the well-known Breuer-Laine-Piilo (BLP) measure [161] of non-Markovianity for two common examples. As it turns out, in one of the examples, our witness detects non-Markovianity even when the BLP measure does not, while for the other example our measure agrees with the BLP measure. We also provide bounds on the entropy change of a system. These bounds are witnesses of how non-unitary an evolution process is. We use one of these witnesses to propose a measure of non-unitarity for unital evolutions and discuss some of its properties.

The organization of the chapter is as follows. In Section 4.1, we introduce some definitions and facts for continuous variable systems that are not covered in Chapter 2. In Section 4.2, we discuss the explicit form (Theorem 4.1) for the rate of entropy change of a system in any state undergoing arbitrary time evolution. In Section 4.3, we briefly review quantum Markov processes. We state Theorem 4.2, which provides a lower limit on the rate of entropy change for quantum Markov processes. We show that this lower limit provides a witness of non-unitality. We also discuss the implications of the lower limit on the rate of entropy change in the context of bosonic Gaussian dynamics (Section 4.3.1). In Section 4.4, based on the necessary conditions for the Markovianity of quantum processes as stated in Theorem 4.2, we define some witnesses of non-Markovianity and also a couple of measures of non-Markovianity based on these witnesses. We apply these witnesses to two common examples of non-Markovian dynamics (Section 4.4.1 and Section 4.4.1) and illustrate

that they can detect non-Markovianity. In Section 4.4.1, we consider an example of a non-unital quantum non-Markov process whose non-Markovianity goes undetected by the BLP measure while it is detected by our witness. In Section 4.5, we derive an upper bound on entropy change for unital evolutions. We also show the monotonic behavior of the entropy for a wider class of operations than previously known. In Section 4.6, we define a measure of non-unitarity for any unital evolution. We also discuss properties of the measure of non-unitarity.

4.1 Preliminaries

In this section, we add few more standard notations, definitions, and facts to the discussion in Chapter 2 because of subtleties that come when dealing with continuous variable systems, which are associated to separable, infinite-dimensional Hilbert spaces.

The dimension $\dim(\mathcal{H})$ of the Hilbert space $\mathcal{H}$ is equal to $+\infty$ in the case that $\mathcal{H}$ is a separable, infinite-dimensional Hilbert space. The subset of $\mathscr{B}(\mathcal{H})$ containing all trace-class operators is denoted by $\mathscr{B}_1(\mathcal{H})$. Let $\mathcal{B}_1^+(\mathcal{H}) := \mathcal{B}_+(\mathcal{H}) \cap \mathcal{B}_1(\mathcal{H})$.

The adjoint $\mathcal{M}^\dagger : \mathscr{B}(\mathcal{H}_B) \to \mathscr{B}(\mathcal{H}_A)$ of a linear map $\mathcal{M} : \mathscr{B}_1(\mathcal{H}_A) \to \mathscr{B}_1(\mathcal{H}_B)$ is the unique linear map that satisfies

$$\forall \, X_A \in \mathscr{B}_1(\mathcal{H}_A), Y_B \in \mathscr{B}(\mathcal{H}_B): \quad \langle Y_B, \mathcal{N}(X_A) \rangle = \langle \mathcal{N}^\dagger(Y_B), X_A \rangle, \tag{4.1}$$

where $\langle C, D \rangle = \mathrm{Tr}\{C^\dagger D\}$ is the Hilbert-Schmidt inner product.

The von Neumann entropy of a state ρ_A of a quantum system A is defined as

$$S(A)_\rho := S(\rho_A) = -\mathrm{Tr}\{\rho_A \log \rho_A\}, \tag{4.2}$$

where $\log$ denotes the natural logarithm. In general, the state of an infinite-dimensional quantum system need not have finite entropy [162]. For any finite-dimensional system A, the entropy is upper-bounded by $\log |A|$.

The quantum relative entropy of any two density operators $\rho, \sigma \in \mathscr{D}(\mathcal{H})$ is defined as [56,163,164]

$$D(\rho \| \sigma) = \sum_{i,j} |\langle \phi_i | \psi_j \rangle|^2 \left[p(i) \log \left(\frac{p(i)}{q(j)} \right) \right], \tag{4.3}$$

73

where $\rho = \sum_i p(i) |\phi_i\rangle \langle \phi_i|$ and $\sigma = \sum_j q(j) |\psi_j\rangle \langle \psi_j|$ are spectral decompositions of ρ and σ, respectively, with both $\{|\phi_i\rangle\}_i, \{|\psi_j\rangle\}_j \in \mathrm{ONB}(\mathcal{H})$ (cf. (2.49)). From the above definition, it is clear that $D(\rho\|\sigma) = +\infty$ if $\mathrm{supp}(\rho) \nsubseteq \mathrm{supp}(\sigma)$.

For any two positive semi-definite operators $\rho, \sigma \in \mathscr{B}_1^+(\mathcal{H})$, $D(\rho\|\sigma) \geq 0$ if $\mathrm{Tr}\{\rho\} \geq \mathrm{Tr}\{\sigma\}$, $D(\rho\|\sigma) = 0$ if and only if $\rho = \sigma$, and $D(\rho\|\sigma) < 0$ if $\rho < \sigma$. The quantum relative entropy is non-increasing under the action of positive trace-preserving maps [57], that is, $D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$ for any two density operators $\rho, \sigma \in \mathscr{D}(\mathcal{H})$ and positive trace-preserving map $\mathcal{N} : \mathscr{B}_+^1(\mathcal{H}) \to \mathscr{B}_+^1(\mathcal{H}')$.

We now define entropy change, which is the main focus of this chapter.

Definition 4.1 (Entropy change) *Let $\mathcal{N} : \mathscr{B}_1^+(\mathcal{H}) \to \mathscr{B}_1^+(\mathcal{H}')$ be a positive trace-non-increasing map. The entropy change $\Delta S(\rho, \mathcal{N})$ of a system in the state $\rho \in \mathscr{D}(\mathcal{H})$ under the action of $\mathcal{N}$ is defined as*

$$\Delta S(\rho, \mathcal{N}) := S(\mathcal{N}(\rho)) - S(\rho) \tag{4.4}$$

whenever $S(\rho)$ and $S(\mathcal{N}(\rho))$ are finite.

It should be noted that $\mathcal{N}(\rho)$ is a sub-normalized state, i.e., $\mathrm{Tr}\{\mathcal{N}(\rho)\} \leq 1$, if $\mathcal{N}$ is a positive trace-non-increasing map.

It is well known that the entropy change $\Delta S(\rho, \mathcal{N})$ of ρ is non-negative, i.e., the entropy is non-decreasing, under the action of a positive, sub-unital, and trace-preserving map $\mathcal{N}$ [150, 151] (see also [33, Section III], [165, Theorem 4.2.2]). Recently, a refined statement of this result was made in [33], which is the following:

Lemma 4.1 (Lower bound on entropy change) *Let $\mathcal{N} : \mathscr{B}_1^+(\mathcal{H}) \to \mathscr{B}_1^+(\mathcal{H}')$ be a positive, trace-preserving map. Then, for all $\rho \in \mathcal{D}(\mathcal{H})$,*

$$\Delta S(\rho, \mathcal{N}) \geq D\left(\rho \,\|\, \mathcal{N}^\dagger \circ \mathcal{N}(\rho)\right). \tag{4.5}$$

Proof. Using the definition (4.1) of the adjoint, we obtain

$$\Delta S(\rho, \mathcal{N}) = S(\mathcal{N}(\rho)) - S(\rho) = \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\{\mathcal{N}(\rho) \log \mathcal{N}(\rho)\} \tag{4.6}$$

Then

$$\Delta S(\rho, \mathcal{N}) = \text{Tr}\{\rho \log \rho\} - \text{Tr}\left\{\rho \mathcal{N}^\dagger \left(\log \mathcal{N}(\rho)\right)\right\}$$

$$\geq \text{Tr}\{\rho \log \rho\} - \text{Tr}\left\{\rho \log\left[\mathcal{N}^\dagger \circ \mathcal{N}(\rho)\right]\right\}$$

$$= D\left(\rho \,\|\, \mathcal{N}^\dagger \circ \mathcal{N}(\rho)\right). \tag{4.7}$$

The inequality follows from Lemma 2.2 applied to $\mathcal{N}^\dagger$, which is positive and sub-unital since $\mathcal{N}$ is positive and trace non-increasing. ∎

Lemma 4.1 gives a tight lower bound on the entropy change. As an example of a map saturating the inequality (4.5), let us take the partial trace $\mathcal{N}_{AB \to B} = \text{Tr}_A$, which is a quantum channel that corresponds to discarding system A from the composite system AB. Its adjoint is $\mathcal{N}^\dagger(\rho_B) = \mathbb{1}_A \otimes \rho_B$. Then, one notices that $S\left(\mathcal{N}(\rho_{AB})\right) - S\left(\rho_{AB}\right) = S(\rho_B) - S(\rho_{AB}) = D\left(\rho_{AB} \| \mathbb{1}_A \otimes \rho_B\right) = D\left(\rho_{AB} \,\|\, \mathcal{N}^\dagger \circ \mathcal{N}(\rho_{AB})\right)$.

4.2 Quantum dynamics and the rate of entropy change

In general, physical systems are dynamical and undergo evolution processes with time. An evolution process for an isolated and closed system is unitary. However, no quantum system can remain isolated from its environment. There is always an interaction between a system and its environment. The joint evolution of the system and environment is considered to be a unitary operation whereas the local evolution of the system alone can be non-unitary. This non-unitarity causes a flow of information between the system and the environment, which can change the entropy of the system.

For any dynamical system with associated Hilbert space $\mathcal{H}$, the state of the system depends on time. The time evolution of the state ρ_t of the system at an instant t is determined by $\frac{d\rho_t}{dt}$ when it is well defined[3]. The state ρ_T at some later time $t = T$ is determined by the initial state ρ_0, the evolution process, and the time duration of the evolution. Since the time evolution is a physical process, the following condition holds for all t:

$$\text{Tr}\{\dot{\rho}_t\} = 0, \tag{4.8}$$

_____

[3]By this, we mean that each matrix element of ρ_t is differentiable with respect to t.

where $\dot{\rho}_t := \frac{\mathrm{d}\rho_t}{\mathrm{d}t}$.

It is known from [158, 166] that for any finite-dimensional system the following formula for the rate of entropy change holds for any state ρ_t whose kernel remains the same at all times and whose support Π_t is differentiable:

$$\frac{\mathrm{d}}{\mathrm{d}t}S(\rho_t) = -\operatorname{Tr}\left\{\dot{\rho}_t \log \rho_t\right\}. \tag{4.9}$$

The above formula has also been applied to infinite-dimensional systems for Gaussian states evolving under a quantum diffusion semigroup [159, 160] whose kernels do not change in time.

Here, we derive the formula (4.9) for states ρ_t having fewer restrictions, which generalizes the statements from [158, 166]. In particular, we show that the formula (4.9) can be applied to quantum dynamical processes in which the kernel of the state changes with time, which can happen because the state has time-dependent support.

Theorem 4.1 *For any quantum dynamical process with* $\dim(\mathcal{H}) < +\infty$, *the rate of entropy change is given by*

$$\frac{\mathrm{d}}{\mathrm{d}t}S(\rho_t) = -\operatorname{Tr}\left\{\dot{\rho}_t \log \rho_t\right\}, \tag{4.10}$$

whenever $\dot{\rho}_t$ *is well defined. The above formula also holds when* $\dim(\mathcal{H}) = +\infty$ *if* $\dot{\rho}_t \log \rho_t$ *is trace-class and the sum of the time derivative of the eigenvalues of* ρ_t *is uniformly convergent[4] on some neighborhood of* t, *however small.*

Proof. Let $\operatorname{Spec}(\rho_t)$ be the set of all eigenvalues of $\rho_t \in \mathscr{D}(\mathcal{H})$, including those in its kernel. Let

$$\rho_t = \sum_{\lambda(t) \in \operatorname{Spec}(\rho_t)} \lambda(t) P_\lambda(t) \tag{4.11}$$

be a spectral decomposition of ρ_t, where the sum of the projections $P_\lambda(t)$ corresponding to $\lambda(t)$ is

$$\sum_{\lambda(t) \in \operatorname{Spec}(\rho_t)} P_\lambda(t) = \mathbb{1}_{\mathcal{H}}. \tag{4.12}$$

The following assumptions suffice to arrive at the statement of the theorem when $\dim(\mathcal{H}) = +\infty$. We assume that $\dot{\rho}_t$ is well defined. We further assume that $\sum_{\lambda(t) \in \operatorname{Spec}(\rho_t)} \dot{\lambda}(t)$ is uniformly con-

---

[4]Uniform convergence is defined as stated in [167, Definition 7.7].

vergent on some neighborhood of t, and $\dot{\rho}_t \log \rho_t$ is trace-class. Note that when $\dim(\mathcal{H}) < +\infty$, $\sum_{\lambda(t) \in \mathrm{Spec}(\rho_t)} \dot{\lambda}(t)$ and $\dot{\rho}_t \log \rho_t$ are always uniformly convergent and trace-class, respectively.

Now, let us define the function $s : [0, \infty) \times (-1, \infty) \to (0, \infty)$ by

$$s(t, h) := \mathrm{Tr}\{\rho_t^{1+h}\} = \sum_{\lambda(t) \in \mathrm{Spec}(\rho_t)} \lambda(t)^{1+h}. \tag{4.13}$$

Noting that $\frac{\mathrm{d}}{\mathrm{d}x} a^x = a^x \log a$ for all $a > 0$ and $x \in \mathbb{R}$, we get

$$\frac{\mathrm{d}}{\mathrm{d}h} \rho_t^{h+1} = \rho_t^{h+1} \log \rho_t. \tag{4.14}$$

Applying (2.11) in Section 2.2.1, we find that

$$\frac{\mathrm{d}}{\mathrm{d}t} s(t, h) = \frac{\mathrm{d}}{\mathrm{d}t} \mathrm{Tr}\{\rho_t^{h+1}\} = (h + 1) \mathrm{Tr}\{\rho_t^h \dot{\rho}_t\}, \tag{4.15}$$

$$\frac{\mathrm{d}}{\mathrm{d}h} s(t, h) = \frac{\mathrm{d}}{\mathrm{d}h} \mathrm{Tr}\{\rho_t^{h+1}\} = \mathrm{Tr}\{\rho_t^{h+1} \log \rho_t\}. \tag{4.16}$$

Then the entropy is

$$S(\rho_t) = -\left. \frac{\mathrm{d}}{\mathrm{d}h} s(t, h) \right|_{h=0} = -\mathrm{Tr}\{\rho_t \log \rho_t\} = -\sum_{\lambda(t) \in \mathrm{Spec}(\rho_t)} \lambda(t) \log \lambda(t), \tag{4.17}$$

where by definition $0 \log 0 = 0$.

Note that ρ_t^h is an infinitely differentiable function of h, i.e., a smooth function of h, and a differentiable function of t for all t, h. Also, the trace is a continuous function. Since $\frac{\mathrm{d}}{\mathrm{d}h} \frac{\mathrm{d}}{\mathrm{d}t} s(t, h)$ exists and is continuous for all $(t, h) \in [0, \infty) \times (-1, \infty)$, the following exchange of derivatives holds for all $(t, h) \in (0, \infty) \times (-1, \infty)$:

$$\frac{\mathrm{d}}{\mathrm{d}h} \left[\frac{\mathrm{d}}{\mathrm{d}t} s(t, h) \right] = \frac{\mathrm{d}}{\mathrm{d}t} \left[\frac{\mathrm{d}}{\mathrm{d}h} s(t, h) \right]. \tag{4.18}$$

This implies that

$$\left. \frac{\mathrm{d}}{\mathrm{d}h} \left[\frac{\mathrm{d}}{\mathrm{d}t} s(t, h) \right] \right|_{h=0} = \frac{\mathrm{d}}{\mathrm{d}t} \left[\left. \frac{\mathrm{d}}{\mathrm{d}h} s(t, h) \right|_{h=0} \right] \tag{4.19}$$

From (4.15), we notice that $\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)$ is a smooth function of h. Therefore, the Taylor series expansion of this function in the neighborhood of $h = 0$ is

$$\frac{\mathrm{d}}{\mathrm{d}t}s(t,h) = \left.\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)\right|_{h=0} + \left.\frac{\mathrm{d}}{\mathrm{d}h}\left[\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)\right]\right|_{h=0} h + O(h^2). \tag{4.20}$$

From (4.13), we find:

$$\left.\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)\right|_{h=0} = \left.\frac{\mathrm{d}}{\mathrm{d}t}\left[\sum_{\lambda(t)\in\mathrm{Spec}(\rho_t)}\lambda(t)^{1+h}\right]\right|_{h=0} = \sum_{\lambda(t)\in\mathrm{Spec}(\rho_t)}\left.\frac{\mathrm{d}}{\mathrm{d}t}\left[\lambda(t)^{1+h}\right]\right|_{h=0} \tag{4.21}$$

$$= \sum_{\lambda(t)\in\mathrm{Spec}(\rho_t)}\left[(1+h)\lambda(t)^h\dot{\lambda}(t)\right]_{h=0} \tag{4.22}$$

$$= \sum_{\lambda(t)\neq 0}\dot{\lambda}(t). \tag{4.23}$$

The second equality follows from [167, Theorem 7.17] due to the uniform convergence of $\sum_{\lambda(t)\in\mathrm{Spec}(\rho_t)}\dot{\lambda}(t)$ on some neighborhood of t. To obtain the last equality, we use the following fact: since $\lambda(t) \geq 0$ for all t and $\lambda(t)$ is differentiable, if $\lambda(t^*) = 0$ for some time $t = t^* \in (0,\infty)$, then $\dot{\lambda}(t^*) = 0$. From (4.15) and (4.23), we obtain

$$\mathrm{Tr}\{\Pi_t\dot{\rho}_t\} = \sum_{\lambda(t)\neq 0}\dot{\lambda}(t) = \frac{\mathrm{d}}{\mathrm{d}t}\sum_{\lambda(t)\neq 0}\lambda(t) = \frac{\mathrm{d}}{\mathrm{d}t}\mathrm{Tr}\{\rho_t\} = 0, \tag{4.24}$$

where Π_t is the projection onto the support of ρ_t. The second equality holds because $\dot{\lambda}(t^*) = 0$ whenever $\lambda(t^*) = 0$ for all $\lambda(t^*) \in \mathrm{Spec}(\rho_{t^*})$ and all $t^* \in (0,\infty)$.

Employing (2.12), we find that

$$\frac{\mathrm{d}}{\mathrm{d}h}\left[\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)\right] = \frac{\mathrm{d}}{\mathrm{d}h}\left[(h+1)\,\mathrm{Tr}\{\rho_t^h\dot{\rho}_t\}\right] \tag{4.25}$$

$$= \mathrm{Tr}\{\rho_t^h\dot{\rho}_t\} + (h+1)\,\mathrm{Tr}\left\{\left[\rho_t^h\log\rho_t\right]\dot{\rho}_t\right\}. \tag{4.26}$$

Therefore,

$$-\frac{\mathrm{d}}{\mathrm{d}t}S(\rho_t) = \frac{\mathrm{d}}{\mathrm{d}t}\left[\frac{\mathrm{d}}{\mathrm{d}h}s(t,h)\Big|_{h=0}\right] \tag{4.27}$$

$$= \frac{\mathrm{d}}{\mathrm{d}h}\left[\frac{\mathrm{d}}{\mathrm{d}t}s(t,h)\right]\Big|_{h=0} \tag{4.28}$$

$$= \mathrm{Tr}\{\Pi_t\dot{\rho}_t\} + \mathrm{Tr}\left\{\dot{\rho}_t\Pi_t\log\rho_t\right\} \tag{4.29}$$

$$= \mathrm{Tr}\{\dot{\rho}_t\log\rho_t\}, \tag{4.30}$$

where to obtain the last equality we used (4.24) and the fact that $\log\rho_t$ is defined on $\mathrm{supp}(\rho_t)$. This concludes the proof. ∎

As an immediate application of Theorem 4.1, consider a closed system consisting of a system of interest A and a bath (environment) system E in a pure state ψ_{AE}, for which the time evolution is given by a bipartite unitary U_{AE}, a special case of bipartite quantum interactions (Chapter 3). Under unitary evolution, the entropy of the composite system AE does not change. Also, for a pure state, the entropy of the composite system is zero, and $S(\rho_A) = S(\rho_E)$, where ρ_A and ρ_E are the reduced states of the systems A and E, respectively. Now, it is often of interest to determine the amount of entanglement in the reduced state ρ_A of the system A. Several measures of entanglement have been proposed [63], among which the entanglement of formation [50,168], the distillable entanglement [50,102], and the relative entropy of entanglement [93,169] all reduce to the entropy $S(\rho_A)$ of the system A in the case of a closed bipartite system [170]. Thus, in this case, the rate of entropy change of the system A is equal to the rate of entanglement change (with respect to the aforementioned entanglement measures) caused by unitary time evolution of the pure state of the composite system, and Theorem 4.1 provides a general expression for this rate of entanglement change.

In Appendix C, we discuss how (4.10) generalizes the development in [158, 166]. We consider examples of dynamical processes in which the support and/or the rank of the state change with time, but the formula (4.10) is still applicable according to the above theorem.

4.3 Open quantum system and Markovian dynamics

The dynamics of an open quantum system can be categorized into two broad classes, quantum Markov processes and quantum non-Markov processes, based on whether the evolution process exhibits memoryless behavior or has memory effects.

Here, we consider the dynamics of an open quantum system in the time interval $I = [t_1, t_2) \subset \mathbb{R}$ for $t_1 < t_2$. We assume that the state $\rho_t \in \mathscr{D}(\mathcal{H})$ of the system at time $t \in I$ satisfies the following differential master equation:

$$\dot{\rho}_t = \mathcal{L}_t(\rho_t) \quad \forall\, t \in I, \tag{4.31}$$

where $\mathcal{L}_t$ is called the generator [171], or Liouvillian, of the dynamics and can in general be time-dependent [172]. A state ρ_{eq} is called a fixed point, or invariant state of the dynamics, if $\dot{\rho}_{\mathrm{eq}} = 0$, or

$$\mathcal{L}_t(\rho_{\mathrm{eq}}) = 0 \quad \forall\, t \in I. \tag{4.32}$$

In general, the evolution of systems governed by the master equation (4.31) is given by the two-parameter family $\{\mathcal{M}_{t,s}\}_{t,s\in I}$ of maps $\mathcal{M}_{t,s} : \mathscr{B}(\mathcal{H}) \to \mathscr{B}(\mathcal{H})$ defined by [22]

$$\mathcal{M}_{t,s} = \mathcal{T}\exp\left[\int_s^t \mathcal{L}_\tau \, \mathrm{d}\tau\right] \quad \forall\, s, t \in I, \ s \leq t, \quad \mathcal{M}_{t,t} = \mathrm{id} \quad \forall\, t \in I, \tag{4.33}$$

where $\mathcal{T}$ is the time-ordering operator, so that the state ρ_t of the system at time t is obtained from the state of the system at time $s \leq t$ as $\rho_t = \mathcal{M}_{t,s}(\rho_s)$. The maps $\{\mathcal{M}_{t,s}\}_{t\geq s}$ satisfy the following composition law:

$$\forall\, s \leq r \leq t: \quad \mathcal{M}_{t,s} = \mathcal{M}_{t,r} \circ \mathcal{M}_{r,s}, \tag{4.34}$$

$$\forall\, t \in I: \quad \mathcal{M}_{t,t} = \mathrm{id}, \tag{4.35}$$

and in terms of these maps the generator $\mathcal{L}_t$ is given by

$$\mathcal{L}_t = \lim_{\varepsilon \to 0^+} \frac{\mathcal{M}_{t+\varepsilon,t} - \mathrm{id}}{\varepsilon}. \tag{4.36}$$

For the maps $\{\mathcal{M}_{t,s}\}_{t\geq s}$ to represent physical evolution, they must be trace-preserving. This implies

that for all $\rho \in \mathscr{D}(\mathcal{H})$ the generator $\mathcal{L}_t$ has to satisfy

$$\mathrm{Tr}\left[\mathcal{L}_t(\rho)\right] = 0 \quad \forall\, t \in I. \tag{4.37}$$

When the intermediate maps $\mathcal{M}_{t,r}$ and $\mathcal{M}_{r,s}$ are positive and trace-preserving for all $s \leq r \leq t$, the condition (4.34) is called P-divisibility. If the intermediate maps $\mathcal{M}_{t,r}$ and $\mathcal{M}_{r,s}$ are CPTP (i.e., quantum channels) for all $s \leq r \leq t$, the condition (4.34) is called CP-divisibility [173, 174]. Based on the notion of CP-divisibility, we consider the following definition of a quantum Markov process, which was introduced in [175].

Definition 4.2 (Quantum Markov process) *The dynamics of a system in a time interval I are called a quantum Markov process when they are governed by (4.31) and they are CP-divisible (i.e., the intermediate maps in (4.34) are CPTP).*

An important fact is that the dynamics governed by the master equation (4.31) are CP-divisible (hence Markovian) if and only if the generator $\mathcal{L}_t$ of the dynamics has the Lindblad form

$$\mathcal{L}_t(\rho) = -\iota[H(t), \rho] + \sum_i \gamma_i(t)\left[A_i(t)\rho A_i^\dagger(t) - \frac{1}{2}\left\{A_i^\dagger(t)A_i(t), \rho\right\}\right], \tag{4.38}$$

with $H(t)$ a self-adjoint operator and $\gamma_i(t) \geq 0$ for all i and for all $t \in I$. The operators $A_i(t)$ are called Lindblad operators. In the time-independent case, this result was independently obtained by Gorini *et al.* [176] for finite-dimensional systems and by Lindblad [177] for infinite-dimensional systems. For a proof of this result in the time-dependent scenario, see [22, 154]. In finite dimensions, necessary and sufficient conditions for $\mathcal{L}_t$ to be written in Lindblad form have been given in [178]. It should be noted that in general, for some physical processes, $\gamma_i(t)$ can be temporarily negative for some i and the overall evolution still CPTP [179, 180].

Given the generator $\mathcal{L}_t$ of the dynamics (4.31) and the corresponding positive trace-preserving maps $\{\mathcal{M}_{s,t}\}_{s,t \in I}$, it holds that the adjoint maps $\{\mathcal{M}_{s,t}^\dagger\}_{s,t \in I}$ are positive and unital. Furthermore, the adjoint maps $\{\mathcal{M}_{s,t}^\dagger\}_{s,t \in I}$ are generated by $\mathcal{L}_t^\dagger$, where $\mathcal{L}_t^\dagger$ is the adjoint of $\mathcal{L}_t$. The Lindblad form

(4.38) of the generator $\mathcal{L}_t^\dagger$ is

$$\mathcal{L}_t^\dagger(X) = \iota[H(t), X] + \sum_i \gamma_i(t) \left(A_i^\dagger(t) X A_i(t) - \frac{1}{2} \left\{ X, A_i^\dagger(t) A_i(t) \right\} \right) \quad \forall X \in \mathscr{B}(\mathcal{H}). \tag{4.39}$$

Now, let us consider the rate of entropy change $\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t)$ of a system in state ρ_t at time t evolving under dynamics with Liouvillian $\mathcal{L}_t$. Theorem 4.1 implies the following equality:

$$\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t) = -\operatorname{Tr}\left\{ \mathcal{L}_t(\rho_t) \log \rho_t \right\} \quad \forall\, t \in I. \tag{4.40}$$

We now derive a limitation on the rate of entropy change of quantum Markov processes using the lower bound in Lemma 4.1 on entropy change.

Theorem 4.2 (Lower limit on the rate of entropy change) *The rate of entropy change of any quantum Markov process (Definition 4.2) is lower bounded as*

$$\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t) \geq -\lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\varepsilon} \operatorname{Tr}\left\{ \Pi_t \left((\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t) \right) \right\} = -\operatorname{Tr}\left\{ \Pi_t \mathcal{L}_t^\dagger(\rho_t) \right\}, \tag{4.41}$$

where Π_t is the projection onto the support of the state ρ_t of a system. In general, (4.41) also holds for dynamics that obey (4.31) and are P-divisible.

Proof. First, since the system is governed by (4.31), so $\rho_{t+\varepsilon} = \mathcal{M}_{t+\varepsilon,t}(\rho_t)$ for any $\varepsilon > 0$. Also, since $\mathcal{M}_{t+\varepsilon,t}$ is CPTP (hence positive and trace-preserving), we can apply Lemma 4.1 to get the following inequality

$$S(\mathcal{M}_{t+\varepsilon,t}(\rho_t)) - S(\rho_t) \geq D\left(\rho_t \,\middle\|\, (\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t) \right) \tag{4.42}$$

Therefore, by definition of the derivative, we obtain

$$\frac{\mathrm{d}}{\mathrm{d}\,t}S(\rho_t) = \lim_{\varepsilon\to 0^+} \frac{S(\rho_{t+\varepsilon}) - S(\rho_t)}{\varepsilon} \tag{4.43}$$

$$\geq \lim_{\varepsilon\to 0^+} \frac{1}{\varepsilon} D\left(\rho_t \,\Big\|\, (\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right) \tag{4.44}$$

$$= \lim_{\varepsilon\to 0^+} \frac{-S(\rho_t) - \mathrm{Tr}\left\{\rho_t \log\left[(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right]\right\}}{\varepsilon} \tag{4.45}$$

$$= -\lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\rho_t \log\left[(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right]\right\} \tag{4.46}$$

$$= -\lim_{\varepsilon\to 0^+} \mathrm{Tr}\left\{\rho_t \frac{\mathrm{d}\left(\log\left[(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right]\right)}{\mathrm{d}\,\varepsilon}\right\} \tag{4.47}$$

$$= -\lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\Pi_t \,(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right\}, \tag{4.48}$$

where we used the definition of the derivative to get (4.46) from (4.45). From Section 2.2.1, and noting that $\lim_{\varepsilon\to 0} (\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t) = \rho_t$, we arrive at (4.48). Then, using the definition of the adjoint and the master equation (4.31), we get

$$-\lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\Pi_t \,(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right\}$$

$$= -\lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\mathcal{M}_{t+\varepsilon,t}(\Pi_t)\mathcal{M}_{t+\varepsilon,t}(\rho_t)\right\} \tag{4.49}$$

$$= -\lim_{\varepsilon\to 0^+} \mathrm{Tr}\left\{\frac{\mathrm{d}}{\mathrm{d}\,\varepsilon}\left(\mathcal{M}_{t+\varepsilon,t}(\Pi_t)\mathcal{M}_{t+\varepsilon,t}(\rho_t)\right)\right\} \tag{4.50}$$

$$= -\lim_{\varepsilon\to 0^+} \mathrm{Tr}\left\{\left(\frac{\mathrm{d}}{\mathrm{d}\,\varepsilon}\mathcal{M}_{t+\varepsilon,t}(\Pi_t)\right)\mathcal{M}_{t+\varepsilon,t}(\rho_t) + \mathcal{M}_{t+\varepsilon,t}(\Pi_t)\left(\frac{\mathrm{d}}{\mathrm{d}\,\varepsilon}\mathcal{M}_{t+\varepsilon,t}(\rho_t)\right)\right\}. \tag{4.51}$$

Employing (4.36) and the fact that $\mathcal{M}_{t,t} = \mathrm{id}$ for all $t \in I$, we get

$$\mathcal{L}_t = \lim_{\varepsilon\to 0^+} \frac{\mathcal{M}_{t+\varepsilon,t} - \mathrm{id}}{\varepsilon} = \lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon}\mathcal{M}_{t+\varepsilon,t}. \tag{4.52}$$

Therefore,

$$-\lim_{\varepsilon\to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\Pi_t \,(\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right\} = -\mathrm{Tr}\left\{\mathcal{L}_t(\Pi_t)\rho_t + \Pi_t\mathcal{L}_t(\rho_t)\right\} \tag{4.53}$$

$$= -\mathrm{Tr}\left\{\Pi_t\mathcal{L}_t^\dagger(\rho_t)\right\}, \tag{4.54}$$

where we used the fact (4.24) that $\text{Tr}\{\Pi_t \mathcal{L}_t(\rho_t)\} = \text{Tr}\{\Pi_t \dot{\rho}_t\} = 0$. ∎

Quantum dynamics obeying (4.31) are unital in a time interval I if $\mathcal{L}_t(\mathbb{1}) = 0$ for all $t \in I$, which implies that $\text{Tr}\{\Pi_t \mathcal{L}_t^\dagger(\rho_t)\} = 0$ for any initial state ρ_0 and for all $t \in I$. The deviation of $\text{Tr}\{\Pi_t \mathcal{L}_t^\dagger(\rho_t)\}$ from zero is therefore a *witness of non-unitality* at time t.

Remark 4.1 *When $\rho_t > 0$, the rate of entropy change of any quantum Markov process is lower bounded as*

$$\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t) \geq -\lim_{\varepsilon \to 0} \frac{\mathrm{d}}{\mathrm{d}\varepsilon} \text{Tr}\left\{ (\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t) \right\} = -\text{Tr}\left\{ \mathcal{L}_t^\dagger(\rho_t) \right\}. \tag{4.55}$$

Given a quantum Markov process and a state described by a density operator $\rho_t > 0$ that is not a fixed (invariant) state of the dynamics, we can make the following statements for $t \in I$ and for all $\varepsilon > 0$ such that $[t, t+\varepsilon) \subset I$:

(i) If $\mathcal{M}_{t+\varepsilon,t}$ is strictly sub-unital, i.e., $\mathcal{M}_{t+\varepsilon,t}(\mathbb{1}) < \mathbb{1}$, then its adjoint is trace non-increasing, which means that $\text{Tr}\{\mathcal{L}_t^\dagger(\rho_t)\} < 0$. This implies that the rate of entropy change is strictly positive for strictly sub-unital Markovian dynamics.

(ii) If $\mathcal{M}_{t+\varepsilon,t}$ is unital, i.e., $\mathcal{M}_{t+\varepsilon,t}(\mathbb{1}) = \mathbb{1}$, then its adjoint is trace-preserving, which means that $\text{Tr}\{\mathcal{L}_t^\dagger(\rho_t)\} = 0$. This implies that the rate of entropy change is non-negative for unital Markovian dynamics.

(iii) If $\mathcal{M}_{t+\varepsilon,t}$ is strictly super-unital, i.e., $\mathcal{M}_{t+\varepsilon,\varepsilon}(\mathbb{1}) > \mathbb{1}$, then its adjoint is trace-increasing, which means that $\text{Tr}\{\mathcal{L}_t^\dagger(\rho_t)\} > 0$. This implies that it is possible for the rate of entropy change to be negative for strictly super-unital Markovian dynamics.

Using the Lindblad form of $\mathcal{L}_t^\dagger$ in (4.39), we find that

$$\text{Tr}\{\mathcal{L}_t^\dagger(\rho_t)\} = \sum_i \gamma_i(t) \left\langle \left[A_i(t), A_i^\dagger(t) \right] \right\rangle_{\rho_t} \tag{4.56}$$

where $\langle A \rangle_\rho = \text{Tr}\{A\rho\}$. Using this expression, the lower bound on the rate of entropy change for quantum Markov processes when the state $\rho_t > 0$ is

$$\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t) \geq \sum_i \gamma_i(t) \left\langle \left[A_i^\dagger(t), A_i(t) \right] \right\rangle_{\rho_t}. \tag{4.57}$$

The inequality (4.57) was first derived in [181] and recently discussed in [182].

When the generator $\mathcal{L}_t \equiv \mathcal{L}$ is time-independent and $I = [0, \infty)$, it holds that the time evolution from time $s \in I$ to time $t \in I$ is determined merely by the time difference $t - s$, that is, $\mathcal{M}_{t,s} = \mathcal{M}_{t-s,0}$ for all $t \geq s$. The evolution of the system is then determined by a one-parameter semi-group. Let $\mathcal{M}_t := \mathcal{M}_{t,0}$ for all $t \geq 0$.

Remark 4.2 *If the dynamics of a system are unital and can be represented by a one-parameter semi-group $\{\mathcal{M}_t\}_{t \geq 0}$ of quantum channels such that the generator $\mathcal{L}$ is self-adjoint, then for $\rho_0 > 0$,*

$$-\operatorname{Tr}\{\rho_0 \log \rho_{2t}\} \leq S(\rho_t) \leq -\operatorname{Tr}\{\rho_{2t} \log \rho_0\}. \tag{4.58}$$

This follows from Lemma 2.2, (4.1), and the fact that $\mathcal{M}_t^\dagger = \mathcal{M}_t$. In particular,

$$S(\rho_t) = S(\mathcal{M}_t(\rho_0)) = -\operatorname{Tr}\{\mathcal{M}_t(\rho_0) \log \mathcal{M}_t(\rho_0)\} \leq -\operatorname{Tr}\{\mathcal{M}_t(\rho_0)\mathcal{M}_t(\log \rho_0)\} \tag{4.59}$$

$$= -\operatorname{Tr}\{\mathcal{M}_t^\dagger \circ \mathcal{M}_t(\rho_0) \log \rho_0\} \tag{4.60}$$

$$= -\operatorname{Tr}\{\rho_{2t} \log \rho_0\}. \tag{4.61}$$

Similarly,

$$S(\rho_t) = S(\mathcal{M}_t(\rho_0)) = -\operatorname{Tr}\{\mathcal{M}_t(\rho_0) \log \mathcal{M}_t(\rho_0)\} = -\operatorname{Tr}\{\rho_0 \mathcal{M}_t^\dagger(\log \mathcal{M}_t(\rho_0))\} \tag{4.62}$$

$$\geq -\operatorname{Tr}\{\rho_0 \log\left(\mathcal{M}_t^\dagger \circ \mathcal{M}_t(\rho_0)\right)\} \tag{4.63}$$

$$= -\operatorname{Tr}\{\rho_0 \log \rho_{2t}\}. \tag{4.64}$$

Remark 4.3 *If the dynamics of a system are unital and can be represented by a one-parameter semi-group $\{\mathcal{M}_t\}_{t \geq 0}$ of quantum channels such that the generator $\mathcal{L}$ is self-adjoint, then the entropy change is lower bounded as*

$$S(\rho_t) - S(\rho_0) \geq D(\rho_0 \| \rho_{2t}). \tag{4.65}$$

This follows using Lemma 4.1. Under certain assumptions, when the dynamics of a system are described by Davies maps [183], the same lower bound (4.65) holds for the entropy change [156].

From the above remark, notice that the entropy change in a time interval $[0, t]$ is lower bounded by the relative entropy between the initial state ρ_0 and the evolved state ρ_{2t} after time $2t$. In the context of information theory, the relative entropy has an operational meaning as the optimal type-II error exponent (in the asymptotic limit) in asymmetric quantum hypothesis testing [184, 185]. The entropy change in the time interval $[0, t]$ is thus an upper bound on the optimal type-II error exponent, where ρ_0 is the null hypothesis and ρ_{2t} is the alternate hypothesis.

Remark 4.4 *Consider evolution of an open bipartite quantum system AB given by two-parameter family $\{\mathcal{M}_{t,s}\}_{t,s \in I}$ of maps $\mathcal{M}_{t,s} : \mathscr{B}(\mathcal{H}) \to \mathscr{B}(\mathcal{H})$, where $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, as defined in (4.33). Furthermore, assume that the dynamics are CP-divisible, meaning that the intermediate maps $\mathcal{M}_{t,r}$ and $\mathcal{M}_{r,s}$ are CPTP for all $s \leq r \leq t$. In other words, we are assuming that the dynamics of the given bipartite system is a quantum Markov process. Note that entangling abilities of such bipartite interactions are limited by the bounds derived in Chapters 3 (see also [186] in the context of an open quantum system).*

4.3.1 Bosonic Gaussian dynamics

Here we consider Gaussian dynamics that can be represented by the one-parameter family $\{\mathcal{G}_t\}_{t \geq 0}$ of phase-insensitive bosonic Gaussian channels $\mathcal{G}_t$ (cf. [187]). It is known that all phase-insensitive gauge-covariant single-mode bosonic Gaussian channels form a one-parameter semi-group [188]. The Liouvillian for such Gaussian dynamics is time-independent and has the following form:

$$\mathcal{L} = \gamma_+ \mathcal{L}_+ + \gamma_- \mathcal{L}_-, \tag{4.66}$$

where

$$\mathcal{L}_+(\rho) = \hat{a}^\dagger \rho \hat{a} - \frac{1}{2}\left\{\hat{a}\hat{a}^\dagger, \rho\right\}, \tag{4.67}$$

$$\mathcal{L}_-(\rho) = \hat{a} \rho \hat{a}^\dagger - \frac{1}{2}\left\{\hat{a}^\dagger \hat{a}, \rho\right\}, \tag{4.68}$$

$\hat{a}$ is the field-mode annihilation operator of the system, and the following commutation relation holds for bosonic systems:

$$[\hat{a}, \hat{a}^\dagger] = \mathbb{1}. \tag{4.69}$$

The state ρ_t of the system at time t is

$$\rho_t = \mathcal{G}_t(\rho_0) = e^{t\mathcal{L}}(\rho_0). \tag{4.70}$$

The thermal state $\rho_{\mathrm{th}}(N)$ with mean photon number N is defined as

$$\rho_{\mathrm{th}}(N) := \frac{1}{N+1} \sum_{n=0}^{\infty} \left(\frac{N}{N+1}\right)^n |n\rangle\langle n|, \tag{4.71}$$

where $N \geq 0$ and $\{|n\rangle\}_{n \geq 0}$ is the orthonormal, photonic number-state basis. Using (4.56), we get

$$-\operatorname{Tr}\{\mathcal{L}^\dagger(\rho_t)\} = -\gamma_+ \left\langle [\hat{a}^\dagger, \hat{a}] \right\rangle_{\rho_t} - \gamma_- \left\langle [\hat{a}, \hat{a}^\dagger] \right\rangle_{\rho_t} \tag{4.72}$$

$$= \gamma_+ - \gamma_- . \tag{4.73}$$

Therefore, by Remark 4.1, if $\rho_t > 0$, then

$$\frac{\mathrm{d}\, S(\mathcal{G}_t(\rho_0))}{\mathrm{d}\, t} \geq \gamma_+ - \gamma_- . \tag{4.74}$$

The lower bound $\gamma_+ - \gamma_-$ is a witness of non-unitality. It is positive for strictly sub-unital, zero for unital, and negative for strictly super-unital dynamics. For example, when the dynamics are represented by a family $\{\mathcal{A}_t\}_{t \geq 0}$ of noisy amplifier channels $\mathcal{A}_t$ with thermal noise $\rho_{\mathrm{th}}(N)$, then $\gamma_+ = N + 1$ and $\gamma_- = N$, which implies that the dynamics are strictly sub-unital. When the dynamics are represented by a family $\{\mathcal{B}_t\}_{t \geq 0}$ of lossy channels $\mathcal{B}_t$ (i.e., beamsplitters) with thermal noise $\rho_{\mathrm{th}}(N)$, then $\gamma_+ = N$, $\gamma_- = N + 1$, which implies that the dynamics are strictly super-unital. When the dynamics are represented by a family $\{\mathcal{C}_t\}_{t \geq 0}$ of additive Gaussian noise channels $\mathcal{C}_t$, then $\gamma_+ = \gamma_-$, which implies that the dynamics are unital.

4.4 Quantum non-Markovian processes

Dynamics of a quantum system that are not a quantum Markov process as stated in Definition 4.2 are called a quantum non-Markov process. Among these two classes of quantum dynamics, non-Markov processes are not well understood and have attracted increased focus over the past decade. Some examples of applications of quantum Markov processes are in the fields of quantum optics, semiconductors in condensed matter physics, the quantum mechanical description of Brownian motion, whereas some examples where quantum non-Markov processes have been applied are in the study of a damped harmonic oscillator, or a damped driven two-level atom [22, 148, 149].

There can be several tests derived from the properties of quantum Markov processes, the satisfaction of which gives witnesses of non-Markovianity. Based on Theorem 4.2, we mention here a few tests that will always fail for a quantum Markov process. Passing of these tests guarantees that the dynamics are non-Markovian.

An immediate consequence of Theorem 4.2 is that only a quantum non-Markov process can pass any of the following tests:

(a)
$$\frac{\mathrm{d}}{\mathrm{d}\,t}S(\rho_t) + \lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \operatorname{Tr}\left\{\Pi_t \left((\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right)\right\} < 0. \tag{4.75}$$

(b)
$$\frac{\mathrm{d}}{\mathrm{d}\,t}S(\rho_t) + \operatorname{Tr}\left\{\Pi_t \mathcal{L}_t^\dagger(\rho_t)\right\} < 0. \tag{4.76}$$

(c)
$$\lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \operatorname{Tr}\left\{\Pi_t \left((\mathcal{M}_{t+\varepsilon,t})^\dagger \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right)\right\} \neq \operatorname{Tr}\left\{\Pi_t \mathcal{L}_t^\dagger(\rho_t)\right\}. \tag{4.77}$$

If the dynamics of the system satisfy any of the above tests, then the process is non-Markovian. Based on the description of the dynamics and the state of the system, one can choose which test to apply. In the case of unital dynamics, (4.75) and (4.76) reduce to $\frac{\mathrm{d}}{\mathrm{d}\,t}S(\rho_t) < 0$. The observation that the negativity of the rate of entropy change is a witness of non-Markovianity for random unitary processes, which are a particular kind of unital processes, was made in [189].

Based on the above witnesses of non-Markovianity, we can introduce different measures of non-

Markovianity for physical processes. Here, we define two measures of non-Markovianity that are based on the channel and generator representation of the dynamics of the system:

1.

$$\mathsf{C}_{\mathrm{M}}(\mathcal{L}) := \max_{\rho_0} \ \sum_{\substack{t: \\ \frac{\mathrm{d}\,S(\rho_t)}{\mathrm{d}\,t} + \mathrm{Tr}\left\{\Pi_t \mathcal{L}_t^{\dagger}(\rho_t)\right\} < 0}} \left| \frac{\mathrm{d}\,S(\rho_t)}{\mathrm{d}\,t} + \mathrm{Tr}\left\{\Pi_t \mathcal{L}_t^{\dagger}(\rho_t)\right\} \right|. \tag{4.78}$$

2.

$$\mathsf{C}_{\mathrm{M}}(\mathcal{M}) := \max_{\rho_0} \ \sum_{t: f(t) < 0} |f(t)|, \tag{4.79}$$

where

$$f(t) := \frac{\mathrm{d}}{\mathrm{d}\,t} S(\rho_t) + \lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\,\varepsilon} \mathrm{Tr}\left\{\Pi_t \left((\mathcal{M}_{t+\varepsilon,t})^{\dagger} \circ \mathcal{M}_{t+\varepsilon,t}(\rho_t)\right)\right\}. \tag{4.80}$$

In the case of unital dynamics, the above measures are equal. It should be noted that the above measures of non-Markovianity are not faithful. This is due to the fact that the statements in Theorem 4.2 do not provide sufficient conditions for the evolution to be a quantum Markov process. In other words, if the measure C_{M} (4.78) is non-zero, then the dynamics are non-Markovian, but if it is equal to zero, then that does not in general imply that the dynamics are Markovian.

4.4.1 Examples

In this section, we consider two common examples of quantum non-Markov processes: pure decoherence of a qubit system (Section 4.4.1) and a generalized amplitude damping channel (Section 4.4.1). In order to characterize quantum dynamics, several witnesses of non-Markovianity and measures of non-Markovianity based on these witnesses have been proposed [161, 175, 178, 180, 189–197]. Many of these measures are based on the fact that certain quantities are monotone under Markovian dynamics, such as the trace distance between states [161], entanglement measures [175, 191, 192], Fisher information and Bures distance [190, 193, 194], and the volume of states [195]. Among these measures, the one proposed in [175] based on the Choi representation of dynamics is both necessary and sufficient. The measure proposed in [180] is also necessary and sufficient and is based on the values of the decay rates $\gamma_i(t)$ appearing in the Lindblad form (4.38) of the Liouvillian of the dynamics.

Here, we compare our measures of non-Markovianity with the widely-considered Breuer-Laine-Piilo (BLP) measure of non-Markovianity [161]. This is a measure of non-Markovianity defined using the trace distance and is based on the fact that the trace distance is monotonically non-increasing under quantum channels. Breuer et al. [161] in 2009 defined Markovianity using CP-divisibility. BLP measure uses the trace distance and exploits the fact that it is monotonically non-increasing under quantum channels. Violation of this monotonicity is thus an indication of non-Markovianity. Specifically, for a given set $\{\mathcal{M}_{t,s}\}_{s,t\geq0}$ of completely positive and trace-preserving maps, their measure is

$$N = \max_{\rho_1(0),\rho_2(0)} \int_{\sigma>0} \sigma(t,\rho_1(0),\rho_2(0)) \ \mathrm{d}\,t, \tag{4.81}$$

where $\sigma(t,\rho_1(0),\rho_2(0)) = \frac{\mathrm{d}}{\mathrm{d}\,t}\frac{1}{2}\|\rho_1(t)-\rho_2(t)\|_1$ and $\rho_1(t) = \mathcal{M}_{t,0}\rho_1(0)$, $\rho_2(t) = \mathcal{M}_{t,0}\rho_2(0)$.

Our measure agrees with the BLP measure in the case of pure decoherence of a qubit. In the case of the generalized amplitude damping channel, our witness is able to detect non-Markovianity even when the BLP measure does not.

Pure decoherence of a qubit system

Consider a two-level system with ground state $|-\rangle$ and excited state $|+\rangle$. This qubit system is allowed to interact with a bosonic environment that is a reservoir of field modes. The time evolution of the qubit system is given by

$$\frac{\mathrm{d}\,\rho_t}{\mathrm{d}\,t} = -\iota[H(t),\rho_t] + \gamma(t)\left[\sigma_-\rho_t\sigma_+ - \frac{1}{2}\{\sigma_+\sigma_-,\rho_t\}\right], \tag{4.82}$$

where $\sigma_+ = |+\rangle\langle-|$, $\sigma_- = |-\rangle\langle+|$ and $t \geq 0$. If $H(t) = 0$, then the system undergoes pure decoherence and the Liouvillian reduces to

$$\mathcal{L}_t(\rho_t) = \frac{\gamma(t)}{2}\left(\sigma_z\rho_t\sigma_z - \rho_t\right), \tag{4.83}$$

where $\sigma_z = [\sigma_+,\sigma_-]$. The decoherence rate is given by $\gamma(t)$, and it can be determined by the spectral density of the reservoir [161].

We can verify that $\mathrm{Tr}\{\Pi_t\mathcal{L}_t^\dagger(\rho_t)\} = 0$ for all $t \geq 0$ and any initial state ρ_0. This implies that the

dynamics are unital for all $t \geq 0$. In this case, for $t > 0$, our witness (4.76) reduces to $\frac{\mathrm{d}}{\mathrm{d}t}S(\rho_t) < 0$. For qubit systems undergoing the given unital evolution, it holds that $\rho_t > 0$ for all $t > 0$, and thus for $t > 0$ our measures (4.78) and (4.79) are equal and reduce to the measure in [196, Eq. (15)], which was based on the fact that the rate of entropy change is non-negative for unital quantum channels. As stated therein, these measures of non-Markovianity are positive and agree with those obtained by the BLP measure [161, Eq. (11)].

Generalized amplitude damping channel

In this example, we consider non-unital dynamics that can be represented as a family of generalized amplitude damping channels $\{\mathcal{M}_t\}_{t \geq 0}$ on a two-level system [194]. These channels have Kraus operators [198]

$$
\begin{aligned}
M_t^1 &= \sqrt{p_t} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\eta_t} \end{pmatrix} \\
M_t^2 &= \sqrt{p_t} \begin{pmatrix} 0 & \sqrt{1-\eta_t} \\ 0 & 0 \end{pmatrix} \\
M_t^3 &= \sqrt{1-p_t} \begin{pmatrix} \sqrt{\eta_t} & 0 \\ 0 & 1 \end{pmatrix} \\
M_t^4 &= \sqrt{1-p_t} \begin{pmatrix} 0 & 0 \\ \sqrt{1-\eta_t} & 0 \end{pmatrix},
\end{aligned}
\tag{4.84}
$$

where $p_t = \cos^2(\omega t)$, $\omega \in \mathbb{R}$, and $\eta_t = e^{-t}$. Then, for all $t \geq 0$, $\mathcal{M}_t(\rho) = \sum_{i=1}^4 M_t^i \rho (M_t^i)^\dagger$. $\mathcal{M}_t$ is unital if and only if $p_t = \frac{1}{2}$ or $\eta_t = 1$. When $\eta_t = 1$, $\mathcal{M}_t = \mathrm{id}$ for all ω.

It was shown in [194] that the BLP measure [161] does not capture the non-Markovianity of the dynamics given by (4.84).

Let the initial state ρ_0 be maximally mixed, that is, $\rho_0 = \frac{1}{2}\mathbb{1}$. The evolution of this state under $\mathcal{M}_t$ is then

$$
\rho_t := \mathcal{M}_t(\rho_0) = \frac{1}{2} \begin{pmatrix} 1 + W_t & 0 \\ 0 & 1 - W_t \end{pmatrix},
\tag{4.85}
$$

where $W_t = (2p_t - 1)(1 - \eta_t) = \cos(2\omega t)(1 - e^{-t})$. Note that $\rho_t > 0$ for all $t \geq 0$. The evolution of

91

these states for an $\varepsilon > 0$ time interval is

$$\rho_{t+\varepsilon} = \mathcal{M}_\varepsilon(\rho_t) = \frac{1}{2} \begin{pmatrix} 1 + W_\varepsilon + \eta_\varepsilon W_t & 0 \\ 0 & 1 - W_\varepsilon - \eta_\varepsilon W_t \end{pmatrix} \tag{4.86}$$

To check whether or not the given dynamics are non-Markovian, we apply the test in (4.75). First, we evaluate

$$\mathcal{M}_\varepsilon^\dagger \circ \mathcal{M}_\varepsilon(\rho_t) = \frac{1}{2} \begin{pmatrix} a_t & 0 \\ 0 & b_t \end{pmatrix}, \tag{4.87}$$

where

$$a_t := p_t(1 + W_\varepsilon + \eta_\varepsilon W_t) + (1 - p_t)\eta_t(1 + W_\varepsilon + \eta_\varepsilon W_t) + (1 - p_t)(1 - \eta_t)(1 - W_\varepsilon + \eta_\varepsilon W_t) \tag{4.88}$$

$$b_t := p_t\eta_t(1 - W_\varepsilon + \eta_\varepsilon W_t) + p_t(1 - \eta_t)(1 + W_\varepsilon + \eta_\varepsilon W_t) + (1 - p_t)(1 - W_\varepsilon + \eta_\varepsilon W_t). \tag{4.89}$$

Then,

$$\lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\varepsilon} \mathrm{Tr}\left\{ \mathcal{M}_\varepsilon^\dagger \circ \mathcal{M}_\varepsilon(\rho_t) \right\} = W_t. \tag{4.90}$$

We note that the deviation of W_t from zero is a witness of non-unitality. For a unital process, for any initial state ρ_0 and for all time t, we have $\lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\varepsilon} \mathrm{Tr}\left\{ \Pi_t \mathcal{M}_\varepsilon^\dagger \circ \mathcal{M}_\varepsilon(\rho_t) \right\} = 0$. For a non-unital process, there will exist some initial state such that for some time t, $\lim_{\varepsilon \to 0^+} \frac{\mathrm{d}}{\mathrm{d}\varepsilon} \mathrm{Tr}\left\{ \Pi_t \mathcal{M}_\varepsilon^\dagger \circ \mathcal{M}_\varepsilon(\rho_t) \right\} \neq 0$. Next, we evaluate the entropy of the state ρ_t to be

$$S(\rho_t) = -\frac{1}{2}\left[(1 + W_t)\log\left(\frac{1 + W_t}{2}\right) + (1 - W_t)\log\left(\frac{1 - W_t}{2}\right) \right]. \tag{4.91}$$

This implies that the rate of entropy change is:

$$\frac{\mathrm{d}\,S(\rho_t)}{\mathrm{d}\,t} = -\frac{1}{2}\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t}\log\left[\frac{1 + W_t}{2}\right] + \frac{1}{2}\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t}\log\left[\frac{1 - W_t}{2}\right] \tag{4.92}$$

$$= \frac{1}{2}\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t}\log\left[\frac{1 - W_t}{1 + W_t}\right], \tag{4.93}$$
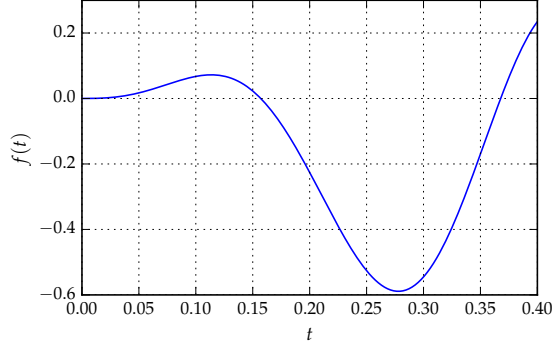
Figure 4.1. Negative values of f, as given in (4.95), indicate non-Markovianity for $\omega = 5$.

where

$$\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t} = -2\omega \sin(2\omega t)(1 - e^{-t}) + \cos(2\omega t)e^{-t}. \tag{4.94}$$

Therefore, the test in (4.75) reduces to

$$f(t) = -\frac{1}{2}\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t}\log\left[\frac{1 + W_t}{2}\right] + \frac{1}{2}\frac{\mathrm{d}\,W_t}{\mathrm{d}\,t}\log\left[\frac{1 - W_t}{2}\right] + W_t < 0, \tag{4.95}$$

where f is defined in (4.80). For values of ω such that the dynamics are non-unital, we find that f can be negative in several time intervals; for example, see Fig. 4.1 for the case $\omega = 5$.

4.5 Bounds on entropy change

In this section, we derive bounds on how much the entropy of a system can change as a function of the initial state of the system and the evolution it undergoes.

Lemma 4.2 *Let* $\mathcal{M} : \mathscr{B}_1^+(\mathcal{H}) \to \mathscr{B}_1^+(\mathcal{H}')$ *be a positive, trace-non-increasing map. Then, for all* $\rho \in \mathscr{D}(\mathcal{H})$ *such that* $\mathcal{M}(\rho) > 0$,

$$\Delta S(\rho, \mathcal{M}) \geq D\left(\rho \,\|\, \mathcal{M}^\dagger \circ \mathcal{M}\,(\rho)\right). \tag{4.96}$$

Proof. Using the definition (4.1) of the adjoint, one obtains

$$\Delta S(\rho, \mathcal{M}) = S(\mathcal{M}(\rho)) - S(\rho) = \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\left\{\mathcal{M}(\rho) \log \mathcal{M}(\rho)\right\}$$

$$= \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\left\{\rho \mathcal{M}^\dagger \left(\log \mathcal{M}(\rho)\right)\right\}$$

$$\geq \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\left\{\rho \log\left[\mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right]\right\}$$

$$= D\left(\rho \,\|\, \mathcal{M}^\dagger \circ \mathcal{M}\left(\rho\right)\right). \tag{4.97}$$

The inequality follows from Lemma 2.2 applied to $\mathcal{M}^\dagger$, which is positive and sub-unital since $\mathcal{M}$ is positive and trace non-increasing. $\blacksquare$

Note that for a quantum channel $\mathcal{M}$, $\Delta S(\rho, \mathcal{M}) = 0$ for all ρ if and only if $\rho = \mathcal{M}^\dagger \circ \mathcal{M}(\rho)$, which is true if and only if $\mathcal{M}$ is a unitary operation [199, Theorem 2.1], [22, Theorem 3.4.1]. We use this fact to provide a measure of non-unitarity in Section 4.6.

As an application of the lower bound in Lemma 4.1, let us suppose that a quantum channel $\mathcal{E}_{A \to B}$ can be simulated as follows

$$\forall \, \rho_A \in \mathscr{D}(\mathcal{H}_A): \; \mathcal{E}_{A \to B}(\rho_A) = \mathcal{F}_{AC \to B}(\rho_A \otimes \theta_C), \tag{4.98}$$

for a fixed (interaction) channel $\mathcal{F}_{AC \to B}$ and a fixed ancillary state θ_C. By applying Lemma 4.1 to $\mathcal{F}$ and the state $\rho_A \otimes \theta_C$, we obtain

$$\Delta S(\rho_A, \mathcal{E}) = S\left(\mathcal{F}(\rho_A \otimes \theta_C)\right) - S\left(\rho_A\right) \tag{4.99}$$

$$\geq S\left(\rho_A \otimes \theta_C\right) - S\left(\rho_A\right) + D\left(\rho_A \otimes \theta_C \,\|\, \mathcal{F}^\dagger \circ \mathcal{F}(\rho_A \otimes \theta_C)\right) \tag{4.100}$$

$$= S\left(\theta_C\right) + D\left(\rho_A \otimes \theta_C \,\|\, \mathcal{F}^\dagger \circ \mathcal{F}(\rho_A \otimes \theta_C)\right). \tag{4.101}$$

Equality holds, i.e., $\Delta S(\rho, \mathcal{E}) = S\left(\theta_C\right)$, if and only if the interaction channel $\mathcal{F}$ is a unitary interaction. If $\mathcal{F}$ is a sub-unital channel, then $\Delta S(\rho, \mathcal{E}) \geq S\left(\theta_C\right)$ because the relative entropy term is non-negative. This result is of relevance in the context of quantum channels obeying certain symmetries (see Section 2.4).

Lemma 4.3 *Let $\mathcal{M} : \mathscr{B}_+(\mathcal{H}) \to \mathscr{B}_+(\mathcal{H}')$ be a sub-unital channel. Then, for all $\rho \in \mathscr{D}(\mathcal{H})$ such that $\rho > 0$,*

$$\Delta S(\rho, \mathcal{M}) \leq \mathrm{Tr}\left\{\left[\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right] \log \rho\right\}. \tag{4.102}$$

This also holds for any positive sub-unital map satisfying the above conditions.

Proof. By applying Lemma 2.2 to $\mathcal{M}$, we get

$$\Delta S(\rho, \mathcal{M}) = \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\left\{\mathcal{M}(\rho) \log \mathcal{M}(\rho)\right\}$$

$$\leq \mathrm{Tr}\{\rho \log \rho\} - \mathrm{Tr}\left\{\mathcal{M}(\rho) \mathcal{M}(\log \rho)\right\}$$

$$= \mathrm{Tr}\left\{\left[\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right] \log \rho\right\}. \tag{4.103}$$

This concludes the proof. ∎

By applying Hölder's inequality (Lemma 2.1) to this upper bound, we obtain the following.

Corollary 4.1 *Let $\mathcal{M} : \mathscr{B}_+(\mathcal{H}) \to \mathscr{B}_+(\mathcal{H}')$ be a sub-unital channel. Then, for all $\rho \in \mathscr{D}(\mathcal{H})$ such that $\rho > 0$,*

$$\Delta S(\rho, \mathcal{M}) \leq \left\|\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right\|_1 \|\log \rho\|_\infty. \tag{4.104}$$

Now, assume $\mathcal{M}$ to be a sub-unital quantum sub-operation, then as a consequence of Lemma 4.1 and Corollary 4.1, we have, for all states $\rho > 0$ such that $\mathcal{M}(\rho) > 0$ and the entropies $S(\rho)$ and $S(\mathcal{M}(\rho))$ are finite,

$$D\left(\rho \,\|\, \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right) \leq S(\mathcal{M}(\rho)) - S(\rho) \leq \left\|\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right\|_1 \|\log \rho\|_\infty. \tag{4.105}$$

It is interesting to note that (4.105) implies

$$\left\|\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right\|_1 \geq \frac{1}{\|\log \rho\|_\infty} D\left(\rho \,\|\, \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right) \tag{4.106}$$

for a sub-unital quantum sub-operation $\mathcal{M}$ and a state $\rho > 0$ such that $\mathcal{M}(\rho) > 0$. This inequality
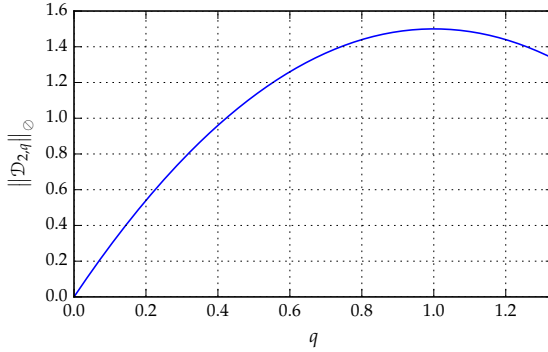
Figure 4.2. The measure $\|\mathcal{D}_{2,q}\|_{\oslash}$ of non-unitarity for the qubit depolarizing channel $\mathcal{D}_{2,q}$ as a function of the parameter $q \in \left[0, \frac{4}{3}\right]$.

has the reverse form of Pinsker's inequality [200], which in this case is

$$D\left(\rho \,\|\, \mathcal{M}^\dagger \circ \mathcal{M}\left(\rho\right)\right) \geq \frac{1}{2}\left\|\rho - \mathcal{M}^\dagger \circ \mathcal{M}(\rho)\right\|_1^2. \tag{4.107}$$

In general, the relationship between relative entropy and different distance measures, including trace distance, has been studied in [201–203].

4.6 Measure of non-unitarity

In this section, we introduce a measure of non-unitarity for any unital quantum channel that is inspired by the discussion at the end of Section 4.5. A measure of unitarity for channels $\mathcal{M}$: $\mathscr{D}(\mathcal{H}_A) \to \mathscr{D}(\mathcal{H}_A)$, where $\mathcal{H}_A$ is finite-dimensional, was defined in [204]. A related measure for non-isometricity for sub-unital channels was introduced in [33]. A measure of non-unitarity for a unital channel is a quantity that gives the distinguishability between a given unital channel with respect to any unitary operation. It quantifies the deviation of a given unital evolution from a unitary evolution. These measures are relevant in the context of cryptographic applications [205, 206] and randomized benchmarking [204].

It is known that any unitary evolution is reversible. The adjoint of a unitary operator is also a unitary operator, and a unitary operator and its adjoint are the inverse of each other. These are the distinct properties of any unitary operation. Let $U_{A \to B}$ denote a unitary operator, where $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B)$. Then a necessary condition for the unitarity of $U_{A \to B}$ is that $(U_{A \to B})^\dagger U_{A \to B} = \mathbb{1}_A$. The

unitary evolution $\mathcal{U}_{A \to B}$ of a quantum state ρ_A is given by

$$\mathcal{U}_{A \to B}(\rho_A) = U_{A \to B}(\rho_A)(U_{A \to B})^\dagger. \tag{4.108}$$

From the reversibility property of a unitary evolution, it holds that $(\mathcal{U}_{A \to B})^\dagger \circ \mathcal{U}_{A \to B} = \mathrm{id}_A$. It is clear that $(\mathcal{U}_{A \to B})^\dagger$ is also a unitary evolution, and $(\mathcal{U}_{A \to B})^\dagger$ and $\mathcal{U}_{A \to B}$ are the inverse of each other.

Contingent upon the above observation, it is to be noted that a measure of non-unitarity for a unital channel $\mathcal{M}_{A \to B}$ should quantify the deviation of $(\mathcal{M}_{A \to B})^\dagger \circ \mathcal{M}_{A \to B}$ from id_A and is desired to be a non-negative quantity. We make use of the trace distance, which gives a distinguishability measure between two positive semi-definite operators and appears in the upper bound[5] on entropy change for a unital channel (Section 4.5), to define a measure of non-unitarity for a unital channel called the diamond norm of non-unitarity.

Definition 4.3 (Diamond norm of non-unitarity) *The diamond norm of non-unitarity of a unital channel $\mathcal{M}_{A \to B}$ is a measure that quantifies the deviation of a given unital evolution from a unitary evolution and is defined as*

$$\|\mathcal{M}\|_\oslash = \left\| \mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{M} \right\|_\diamond, \tag{4.109}$$

where the diamond norm $\|\cdot\|_\diamond$ [207] of a Hermiticity-preserving map $\mathcal{M}$ is defined as

$$\|\mathcal{M}\|_\diamond = \max_{\rho_{RA} \in \mathscr{D}(\mathcal{H}_{RA})} \left\| (\mathrm{id} \otimes \mathcal{M})(\rho_{RA}) \right\|_1. \tag{4.110}$$

In other words,

$$\|\mathcal{M}\|_\oslash = \max_{\rho_{RA} \in \mathscr{D}(\mathcal{H}_{RA})} \left\| (\mathrm{id} \otimes (\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{M}))(\rho_{RA}) \right\|_1. \tag{4.111}$$

The diamond norm of non-unitarity of any unital channel $\mathcal{M}$ has the following properties:

1. $\|\mathcal{M}\|_\oslash \geq 0$.

2. $\|\mathcal{M}\|_\oslash = 0$ if and only if $\mathcal{M}^\dagger \circ \mathcal{M} = \mathrm{id}$, i.e., the unital channel $\mathcal{M}$ is unitary.

---

[5]Notice that the lower bound on the entropy change can also be used to arrive at the measure in terms of trace distance by employing Pinsker's inequality (4.107).

3. In (4.111), it suffices to take ρ_{RA} to be rank one and to let $\dim(\mathcal{H}_R) = \dim(\mathcal{H}_A)$.

4. $\|\mathcal{M}\|_\oslash \leq 2$.

Noticing that $\mathcal{M}^\dagger \circ \mathcal{M} : \mathscr{D}(\mathcal{H}_A) \to \mathscr{D}(\mathcal{H}_A)$ is a quantum channel, properties 1, 3, and 4 are direct consequences of the properties of the diamond norm [26]. For property 3, the reference system R has to be comparable with the channel input system A, following from the Schmidt decomposition. So $\mathcal{H}_R$ should be countably infinite if $\mathcal{H}_A$ is. Property 2 follows from [199, Theorem 2.1], [22, Theorem 3.4.1].

The diamond norm has an operational interpretation in terms of channel discrimination [23, 26] (see also [208, 209] for state discrimination). Specifically, the optimal success probability $p_{\mathrm{succ}}(\mathcal{M}_1, \mathcal{M}_2)$ of distinguishing between two channels $\mathcal{M}_1$ and $\mathcal{M}_2$ is

$$p_{\mathrm{succ}}(\mathcal{M}_1, \mathcal{M}_2) := \frac{1}{2}\left(1 + \frac{1}{2}\|\mathcal{M}_1 - \mathcal{M}_2\|_\diamond\right). \tag{4.112}$$

It follows that the optimal success probability of distinguishing between the identity channel and $\mathcal{M}^\dagger \circ \mathcal{M}$ is

$$p_{\mathrm{succ}}(\mathrm{id}, \mathcal{M}^\dagger \circ \mathcal{M}) = \frac{1}{2}\left(1 + \frac{1}{2}\|\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{M}\|_\diamond\right) \tag{4.113}$$

$$= \frac{1}{2}\left(1 + \frac{1}{2}\|\mathcal{M}\|_\oslash\right). \tag{4.114}$$

Proposition 4.1 *Let* $\mathcal{M} : \mathscr{D}(\mathcal{H}) \to \mathscr{D}(\mathcal{H})$ *be a unital channel. If there exists a unitary operator* $U \in \mathscr{B}(\mathcal{H})$ *such that*

$$\|\mathcal{M} - \mathcal{U}\|_\diamond \leq \delta, \tag{4.115}$$

where $\mathcal{U} : \mathscr{D}(\mathcal{H}) \to \mathscr{D}(\mathcal{H})$ *is the unitary evolution* (4.108) *associated with* U, *then* $\|\mathcal{M}\|_\oslash \leq \sqrt{2\delta} + \delta$.

Proof. The following relations hold

$$\left\|\text{id} - \mathcal{M}^\dagger \circ \mathcal{M}\right\|_\diamond = \left\|\text{id} - \mathcal{M}^\dagger \circ \mathcal{U} + \mathcal{M}^\dagger \circ \mathcal{U} - \mathcal{M}^\dagger \circ \mathcal{M}\right\|_\diamond \tag{4.116}$$

$$\leq \left\|\text{id} - \mathcal{M}^\dagger \circ \mathcal{U}\right\|_\diamond + \left\|\mathcal{M}^\dagger \circ (\mathcal{U} - \mathcal{M})\right\|_\diamond \tag{4.117}$$

$$\leq \left\|\text{id} - \mathcal{M}^\dagger \circ \mathcal{U}\right\|_\diamond + \delta. \tag{4.118}$$

To obtain these inequalities, we have used the following properties of the diamond norm [26]:

1. Triangle inequality: $\|\mathcal{M}_1 + \mathcal{M}_2\|_\diamond \leq \|\mathcal{M}_1\|_\diamond + \|\mathcal{M}_2\|_\diamond$.

2. Sub-multiplicativity: $\|\mathcal{M}_1 \circ \mathcal{M}_2\|_\diamond \leq \|\mathcal{M}_1\|_\diamond \|\mathcal{M}_2\|_\diamond$.

3. For all channels $\mathcal{M}$, $\|\mathcal{M}\|_\diamond = 1$.

In particular, to use the third fact, we notice that $\mathcal{M}^\dagger$ is a channel since $\mathcal{M}$ is unital. We have also made use of an assumption that $\|\mathcal{U} - \mathcal{M}\|_\diamond \leq \delta$.

Now, from the assumption $\|\mathcal{U} - \mathcal{M}\|_\diamond \leq \delta$, it follows by unitary invariance of the diamond norm that

$$\left\|\text{id} - \mathcal{U}^\dagger \circ \mathcal{M}\right\|_\diamond \leq \delta. \tag{4.119}$$

By the operational interpretation of the diamond distance, this means that the success probability of distinguishing the channel $\mathcal{U}^\dagger \circ \mathcal{M}$ from the identity channel, using any scheme whatsoever, cannot exceed $p_{\text{succ}}(\text{id}, \mathcal{U}^\dagger \circ \mathcal{M})$ as defined in (4.112). In other words, the success probability cannot exceed $\frac{1}{2}\left(1 + \frac{1}{2}\delta\right)$. One such scheme is to send in a bipartite state $|\psi\rangle_{RA}$ on a reference system R and the system A on which the channel acts and perform the measurement defined by the positive operator-valued measure (POVM) $\{|\psi\rangle\langle\psi|_{RA}, \mathbb{1}_{RA} - |\psi\rangle\langle\psi|_{RA}\}$. If the outcome of the measurement is $|\psi\rangle\langle\psi|_{RA}$, then one guesses that the channel is the identity channel, and if the outcome of the measurement is $\mathbb{1}_{RA} - |\psi\rangle\langle\psi|_{RA}$ then one guesses that the channel is $\mathcal{U}^\dagger \circ \mathcal{M}$. The success probability of this scheme is

$$\frac{1}{2}\left[\text{Tr}\{|\psi\rangle\langle\psi|_{RA}\,\text{id}_{RA}(|\psi\rangle\langle\psi|_{RA})\} + \text{Tr}\{(\mathbb{1}_{RA} - |\psi\rangle\langle\psi|_{RA})\left[\text{id}_R \otimes(\mathcal{U}^\dagger \circ \mathcal{M})_A\right](|\psi\rangle\langle\psi|_{RA})\}\right]$$

$$= \frac{1}{2}\left[2 - \langle\psi|_{RA}\left[\text{id}_R \otimes(\mathcal{U}^\dagger \circ \mathcal{M})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA}\right]. \tag{4.120}$$

By employing the above, we get

$$\frac{1}{2}\left[2 - \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{U}^\dagger \circ \mathcal{M})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA}\right] \leq \frac{1}{2}\left(1 + \frac{1}{2}\delta\right) \tag{4.121}$$

$$\Leftrightarrow \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{U}^\dagger \circ \mathcal{M})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA} \geq 1 - \frac{1}{2}\delta. \tag{4.122}$$

By employing the definition of the channel adjoint, we find that

$$\langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{U}^\dagger \circ \mathcal{M})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA}$$
$$= \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA} \geq 1 - \frac{1}{2}\delta. \tag{4.123}$$

This holds for all input states, so we can conclude that the following inequality holds:

$$\min_{\psi_{RA}} \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA} \geq 1 - \frac{1}{2}\delta. \tag{4.124}$$

Now, by the definition (4.110) of the diamond norm, and the fact that it suffices to take the maximization in the definition of the diamond norm over only pure states, we have

$$\left\|\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{U}\right\|_\diamond = \max_{\psi_{RA}}\left\|\left[\mathrm{id}_R \otimes(\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\right\|_1. \tag{4.125}$$

By the Fuchs-van de Graaf inequality [76], we obtain

$$\left\|\left[\mathrm{id}_R \otimes(\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\right\|_1 \tag{4.126}$$
$$= \left\||\psi\rangle\langle\psi|_{RA} - \left[\mathrm{id}_R \otimes(\mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\right\|_1 \tag{4.127}$$
$$\leq 2\sqrt{1 - \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA}}. \tag{4.128}$$

It follows that

$$\left\|\mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{U}\right\|_\diamond \leq 2\sqrt{1 - \min_{\psi_{RA}} \langle\psi|_{RA}\left[\mathrm{id}_R \otimes(\mathcal{M}^\dagger \circ \mathcal{U})_A\right](|\psi\rangle\langle\psi|_{RA})\,|\psi\rangle_{RA}}. \tag{4.129}$$

Using (4.124), we therefore obtain

$$\left\| \mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{U} \right\|_\diamond \leq 2\sqrt{\frac{1}{2}\delta} = \sqrt{2\delta}. \tag{4.130}$$

Finally, from (4.118) we arrive at

$$\left\| \mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{M} \right\|_\diamond \leq \sqrt{2\delta} + \delta, \tag{4.131}$$

as required. ∎

We can also make qualitative argument for the converse statement to suggest that if the diamond norm of non-unitarity $\|M\|_\oslash$ of a unital channel $\mathcal{M}$ is less than δ, then $\mathcal{M}$ is close to some unitary evolution (channel) for small δ [6]. Consider that $\left\| \mathrm{id} - \mathcal{M}^\dagger \circ \mathcal{M} \right\|_\diamond \leq \delta$. Then, using tools of channel discrimination in the same way as in the proof of Proposition 4.1, we obtain

$$\forall \ |\psi\rangle_{RA} : \ \mathrm{Tr}\left[|\psi\rangle\langle\psi|_{RA} \, (\mathrm{id}_R \otimes \mathcal{M}^\dagger \circ \mathcal{M})(|\psi\rangle\langle\psi|_{RA}) \right] \geq 1 - \frac{1}{2}\delta, \tag{4.132}$$

which implies that

$$\mathrm{Tr}\left[(\mathrm{id}_R \otimes \mathcal{M})(|\psi\rangle\langle\psi|_{RA})^2 \right] \geq 1 - \frac{1}{2}\delta. \tag{4.133}$$

We know that $\mathrm{Tr}\{\rho^2\} = 1$ for a density operator ρ if and only if it is a pure state, and any deviation of $\mathrm{Tr}\{\rho^2\}$ from unit shows how mixed the state is. Hence, the above inequality (4.133) implies that less noise is introduced in the system A if the unital channel is close to some unitary process.

We now quantify the non-unitarity of the qudit depolarizing channel $\mathcal{D}_{d,q}$ defined as [210]

$$\mathcal{D}_{d,q}(\rho) = (1-q)\rho + q\frac{1}{d}\mathbb{1} \quad \forall \rho \in \mathscr{D}(\mathcal{H}_A), \tag{4.134}$$

where $\dim(\mathcal{H}_A) = d$ and $q \in \left[0, \frac{d^2}{d^2-1}\right]$. The input state ρ remains invariant with probability $1 - \left(1 - \frac{1}{d^2}\right)q$ under the action of $\mathcal{D}_{d,q}$.

---

[6] A concrete proof of the converse statement of Proposition 4.1 has been derived in an unpublished work with Sumeet Khatri, Mark M. Wilde, and Elton Y. Zhu.

Proposition 4.2 *For the depolarizing channel $\mathcal{D}_{d,q}$, the diamond norm of non-unitarity is*

$$\|\mathcal{D}_{d,q}\|_\oslash = 2q(2-q)\left(1 - \frac{1}{d^2}\right). \tag{4.135}$$

Proof. The result follows directly from [211, Section V.A], but here we provide an alternative proof argument that holds for more general classes of channels.

The depolarizing channel is self-adjoint, that is, $\mathcal{D}_{d,q}^\dagger = \mathcal{D}_{d,q}$ for all q, which means that $\mathcal{D}_{d,q}^\dagger \circ \mathcal{D}_{d,q} = \mathcal{D}_{d,q}^2 = \mathcal{D}_{d,2q-q^2}$. Therefore,

$$\|\mathcal{D}_{d,q}\|_\oslash = \left\|\mathrm{id} - \mathcal{D}_{d,q}^2\right\|_\diamond = \left|2q - q^2\right| \max_{\psi_{A'A}} \left\|\psi_{A'A} - \psi_{A'} \otimes \frac{\mathbb{1}}{d}\right\|_1, \tag{4.136}$$

where $\psi_{A'A} = |\psi\rangle\langle\psi|_{A'A}$ is a pure state and $\dim(\mathcal{H}_{A'}) = \dim(\mathcal{H}_A) = d$.

The identity channel and the depolarizing channel are jointly teleportation-simulable [34, Definition 6] with respect to resource states, which in this case are the respective Choi states (because these channels are also jointly covariant (Definition 2.4, also see [34, Definitions 7 & 12]). It is known that the trace distance is monotonically non-increasing under the action of a quantum channel. Therefore, we can conclude from the form [34, Eq. (3.2)] of the action of jointly teleportation-simulable channels that the diamond norm between any two jointly teleportation-simulable channels is upper bounded by the trace distance between the associated resource states.

Since $\dim(\mathcal{H}_A)$ is finite, the maximally entangled state $|\Phi\rangle_{A'A} := \frac{1}{\sqrt{d}}\sum_{i=1}^d |i\rangle |i\rangle$, where $\{|i\rangle\}_{i=1}^d \in \mathrm{ONB}(\mathcal{H}_A)$, is an optimal state in (4.136). It is known that

$$\frac{\mathbb{1}}{d} \otimes \frac{\mathbb{1}}{d} = \frac{1}{d^2}\sum_{x=0}^{d^2-1} \sigma_A^x \Phi_{A'A} \sigma_A^x, \tag{4.137}$$

where $\{\sigma_A^x \Phi_{A'A} \sigma_A^x\}_{x=0}^{d^2-1} \in \mathrm{ONB}(\mathcal{H}_{A'A})$ and $\{\sigma^x\}_{x=0}^{d^2-1}$ forms the Heisenberg-Weyl group (see Ap-

pendix A). We denote the identity element in $\{\sigma^x\}_{x=0}^{d^2-1}$ by σ^0. Using this, we get

$$\|\mathcal{D}_{d,q}\|_\oslash = (2q - q^2) \left\|\Phi_{A'A} - \frac{\mathbb{1}}{d} \otimes \frac{\mathbb{1}}{d}\right\|_1 \tag{4.138}$$

$$= (2q - q^2) \left\|\left(1 - \frac{1}{d^2}\right)\Phi_{A'A} - \frac{1}{d^2}\sum_{x=1}^{d^2-1}\sigma_A^x\Phi_{A'A}\sigma_A^x\right\|_1 \tag{4.139}$$

$$= (2q - q^2) \left[\left(1 - \frac{1}{d^2}\right) + \frac{d^2 - 1}{d^2}\right] \tag{4.140}$$

$$= 2q(2 - q)\left(1 - \frac{1}{d^2}\right). \tag{4.141}$$

Hence, we can conclude that $\|\mathcal{D}_{d,q}\|_\oslash = 2q(2 - q)\left(1 - \frac{1}{d^2}\right)$. See Fig. 4.2 for a plot of $\|\mathcal{D}_{2,q}\|_\oslash$ as a function of q. ∎

4.7 Conclusion

In this chapter, we discussed the rate of entropy change of a system undergoing time evolution for arbitrary states and proved that the formula derived in [158] holds for both finite- and infinite-dimensional systems undergoing arbitrary dynamics with states of arbitrary rank. We derived a lower limit on the rate of entropy change for anarbitrary quantum Markov process. We discussed the implications of this lower limit in the context of bosonic Gaussian dynamics. From this lower limit, we also obtained several witnesses of non-Markovianity, which we used in two common examples of non-Markovian dynamics. Interestingly, our witness turned out to be useful in detecting non-Markovianity for given non-unital process, which could not be detected using BLP measure. We generalized the class of operations for which the entropy exhibits monotonic behavior. We also defined a measure of non-unitarity based on bounds on the entropy change, discussed its properties, and evaluated it for the depolarizing channel.

Chapter 5   Reading of Memory Devices: General Protocol and Bounds

One of the primary goals of quantum information theory is to identify limitations on information processing when constrained by the laws of quantum mechanics. In general, quantum information theory uses tools that are universally applicable to the processing of arbitrary quantum systems, which include quantum optical systems, superconducting systems, trapped ions, etc. [21]. The abstract approach to quantum information allows us to explore how to use the principles of quantum mechanics for communication or computation tasks, some of which would not be possible without quantum mechanics.

In [109], a communication protocol was introduced in which a classical message is encoded in a set of unitary operations, and later on, one can read out the information stored in the unitary operations by calling them. Over a decade after [109] was published, this communication model was generalized and studied under the name "quantum reading" in [212], and it was applied to the setting of an optical read-only memory device. An optical read-only memory device is one of the prototypical examples of quantum reading, and for this reason, quantum reading had been mainly considered in the context of optical realizations like CD-ROMs and DVDs [212–216]. In this case, classical bits are encoded in the reflectivity and phase of memory cells, which can be modeled as a collection of pure-loss bosonic channels. More generally and abstractly, a memory cell is a collection of quantum channels, from which an encoder can select to form codewords for the encoding of a classical message. Each quantum channel in a codeword, representing one part of the stored information, is read only once. In subsequent works [213, 217], the model was extended to a memory cell consisting of arbitrary quantum channels. In a quantum reading strategy, one exploits entangled states and collective measurements to help read out a classical message stored in a read-only memory device. In many cases, one can achieve performance better than what can be achieved when using a classical strategy [212].

Some early developments in quantum reading [212] were based on a direct application of developments in quantum channel discrimination [207, 218–225]. However, the past few years have seen

---

This chapter is entirely based on [34], a joint work with Mark M. Wilde.

some progress in quantum reading: there have been developments in defining protocols for quantum reading (including limited definitions of reading capacity and zero-error reading capacity), giving upper bounds on the rates for classical information readout, achievable rates for memory cells consisting of a particular class of bosonic channels, and details of a quantum measurement that can achieve non-trivial rates for memory cells consisting of a certain class of bosonic channels [212–217]. The information-theoretic study of quantum reading is based on considerations coming from quantum Shannon theory, and the most abstract and general way to define the encoding of a classical message in a quantum reading protocol is as mentioned above, a sequence of quantum channels chosen from a given memory cell.

Hitherto, all prior works on quantum reading considered decoding protocols of the following form: A reader possessing a transmitter system entangled with an idler system sends the transmitter system through the coded sequence of quantum channels. Finally, the reader decodes the message by performing a collective measurement on the joint state of the output system and the idler system.

However, the above approach neglects an important consideration: *in a quantum reading protocol, the transmitter and receiver are in the same physical location.* We can thus refer to both devices as a single device called a transceiver. As a consequence of this physical setup, the most general and natural definition for quantum reading capacity should allow for the transceiver to perform an adaptive operation after each call to the memory, and this is how quantum reading capacity was defined in [34].

In general, an adaptive strategy can have a significant advantage over a non-adaptive strategy in the context of quantum channel discrimination [224]. Furthermore, a quantum channel discrimination protocol employing a non-adaptive strategy is a special case of one that uses an adaptive strategy. Since quantum reading bears close connections to quantum channel discrimination, we suspect that adaptive operations could help to increase quantum reading capacity in some cases, and this is one contribution of [34].

It is to be noted that the physical setup of quantum reading is rather different from that considered in a typical communication problem, in which the sender and receiver are in different physical locations. In this latter case, allowing for adaptive operations represents a different physical model and is thus considered as a different kind of capacity, typically called a feedback-assisted

capacity. However, as advocated above, the physical setup of quantum reading necessitates that there should be no such distinction between capacities: the quantum reading capacity should be defined as it is here, in such a way as to allow for adaptive operations.

Another point of concern with prior work on quantum reading is as follows: so far, all bounds on the quantum reading rate have been derived in the usual setting of quantum Shannon theory, in which the number of uses of the channels tends to infinity (also called the i.i.d. setting, where i.i.d. stands for "independent and identically distributed"). However, it is important for practical purposes to determine rates for quantum reading in the non-asymptotic scenario, i.e., for a finite number of quantum channel uses and a given error probability for decoding. The information-theoretic analysis in the non-asymptotic case is motivated by the fact that in practical scenarios, we have only finite resources at our disposal [17, 226, 227].

The main focus of this chapter is to address some of the concerns mentioned above by giving the most general and natural definition for a quantum reading protocol and quantum reading capacity. We also establish bounds on the rates of quantum reading for wider classes of memory cells in both the asymptotic and non-asymptotic cases. First, we define a quantum reading protocol and quantum reading capacity in the most general setting possible by allowing for adaptive strategies. We give weak-converse, single-letter bounds on the rates of quantum reading protocols that employ either adaptive or non-adaptive strategies for arbitrary memory cells. We also introduce a particular class of memory cell, which we call an *environment-parametrized* (see Section 5.1 for definitions), for which stronger statements can be made for the rates and capacities in the non-asymptotic situation of a finite number of uses of the channels. It should be noted that a particular kind of environment-parametrized memory cell consists of a collection of channels that are jointly teleportation simulable. Many channels of interest obey these symmetries: some examples are erasure, dephasing, thermal, noisy amplifier, and Pauli channels [50, 80, 125, 126, 228–230]. Here we determine strong converse and second-order bounds on the quantum reading capacities of environment-parametrized memory cells. Based on an example from [224, Section 3], we show in Section 5.5 that there exists a memory cell for which its zero-error reading capacity with adaptive operations is at least $\frac{1}{2}$, but its zero-error reading capacity without adaptive operations is equal to zero. This example emphasizes how reading capacity should be defined in such a way as to allow for adaptive operations, as stressed in

this chapter.

The organization of this chapter is as follows. In Section 5.1, we briefly review the set up of quantum reading protocol as a particular instance of communication protocol over bipartite quantum interaction. We then introduce two of the aforementioned classes of memory cells. In Section 5.2, we define a quantum reading protocol and quantum reading capacity in the most general and natural way. Section 5.3 contains main results, which were briefly summarized in the previous paragraph. In Section 5.4, we calculate quantum reading capacities for a thermal memory cell and for a class of jointly covariant memory cells, including a qudit erasure memory cell and a qudit depolarizing memory cell. In Section 5.5, we provide an example to illustrate the advantage of adaptive operations over non-adaptive operations in the context of zero-error quantum reading capacity. In the final section of the chapter, we conclude and shed some light on possible future work.

5.1 Memory cells with symmetry

In this section, we first review controlled channels as a particular instance of bipartite quantum interactions. This observation leads to the realization that a (quantum) reading protocol is a particular instance of information processing or communication task that uses bipartite quantum interactions of specific forms. Next, we define a broad class of memory cell called environment-parametrized memory cell that is a set of quantum channels obeying certain symmetries.

Throughout this chapter, let $\mathscr{X}$ denote an alphabet of size $|X|$, where $|X|$ is finite.

5.1.1 Bipartite interaction and quantum reading

Consider a bipartite quantum interaction between systems X' and B', generated by a Hamiltonian $\hat{H}_{X'B'E'}$, where E' is a bath system, as given by (3.3).

For some distributed quantum computing and information processing tasks where the controlling system (register) X and input system B' are jointly accessible, the following bidirectional channel is relevant:

$$\mathcal{B}_{X'B'\to XB}(\cdot) := \sum_{x\in\mathscr{X}} |x\rangle\langle x|_X \otimes \mathcal{N}^x_{B'\to B}\left(\langle x|(\cdot)|x\rangle_{X'}\right). \tag{5.1}$$

In the above, X' is a controlling system that determines which evolution from the set $\{\mathcal{N}^x\}_{x\in\mathscr{X}}$

takes place on input system B'. In particular, when X' and B' are spatially separated and the input states for the system $X'B'$ are considered to be in product state, the noisy evolution for such constrained interactions is given by the following bidirectional channel:

$$\mathcal{B}_{X'B'\to XB}(\sigma_{X'} \otimes \rho_{B'}) := \sum_{x\in\mathcal{X}} \langle x| \sigma_{X'} |x\rangle_{X'} |x\rangle\langle x|_X \otimes \mathcal{N}^x_{B'\to B}(\rho_{B'}). \tag{5.2}$$

This kind of bipartite interaction is in one-to-one correspondence with the notion of a memory cell from the context of quantum reading [109,212]. There, a memory cell is a collection $\{\mathcal{N}^x_{B'\to B}\}_{x\in\mathcal{X}}$ of quantum channels. One party chooses which channel is applied to another party's input system B' by selecting a classical letter $x \in \mathcal{X}$. Clearly, the description in (5.1) is a fully quantum description of this process, and thus one notices that quantum reading can be understood as the use of a particular kind of bipartite interaction.

5.1.2 Environment-parametrized memory cells

A collection of channels $\{\mathcal{E}^x_{B'\to B}\}_{x\in\mathcal{X}}$ is called environment-parametrized if there exists a set of ancillary states $\{\theta^x_E\}_{x\in\mathcal{X}}$, and $\mathcal{F}_{B'E\to B}$ a quantum channel, called an interaction channel, such that $\mathcal{E}^x_{B'\to B}$ can be realized as follows:

$$\mathcal{E}^x_{B'\to B}(X_{B'}) := \mathcal{F}_{B'E\to B}(X_{B'} \otimes \theta^x_E), \tag{5.3}$$

for all $X_{B'} \in \mathcal{B}_1(\mathcal{H}_{B'})$. This notion is related to the notion of programmable channels, used in the context of quantum computation [125] (see Section 2.4).

Remark 5.1 *We notice from Definition 2.2 that a teleportation-simulable channel is a particular kind of environment-parametrized channel in which a resource state ω_{RB} is the ancillary state and LOCC channel $\mathcal{L}_{RB'B\to B}$ is the interaction channel.*

We now define a broad class of sets of quantum channels that we call environment-parametrized memory cells, and we discuss two classes of sets of quantum channels that are particular kinds of environment-parametrized memory cells.

Definition 5.1 (Environment-parametrized memory cell) *A set $\mathscr{E}_{\mathscr{X}} = \{\mathcal{N}^x_{B'\to B}\}_{x\in\mathscr{X}}$ of quantum channels is an environment-parametrized memory cell if there exists a set $\{\theta^x_E\}_{x\in\mathscr{X}}$ of ancillary states and a fixed interaction channel $\mathcal{F}_{B'E\to B}$ such that for all input states $\rho_{B'}$ and $\forall x \in \mathscr{X}$*

$$\mathcal{N}^x_{B'\to B}(\rho_{B'}) = \mathcal{F}_{B'E\to B}(\rho_{B'} \otimes \theta^x_E). \tag{5.4}$$

Definition 5.2 (Jointly teleportation-simulable memory cell) *A set $\mathscr{T}_{\mathscr{X}} = \{\mathcal{T}^x_{B'\to B}\}_{x\in\mathscr{X}}$ of quantum channels is a jointly teleportation-simulable memory cell if there exists a set $\{\omega^x_{RB}\}_{x\in\mathscr{X}}$ of resource states and an LOCC channel $\mathcal{L}_{B'RB\to B}$ such that, for all input states $\rho_{B'}$ and $\forall x \in \mathscr{X}$*

$$\mathcal{T}^x_{B'\to B}(\rho_{B'}) = \mathcal{L}_{B'RB\to B}(\rho_{B'} \otimes \omega^x_{RB}), \tag{5.5}$$

where the LOCC channel input is with respect to the bipartition $RB':B$.

Definition 5.3 (Jointly covariant memory cell) *A set $\mathscr{T}_{\mathscr{X}} = \{\mathcal{T}^x_{B'\to B}\}_{x\in\mathscr{X}}$ of quantum channels is jointly covariant if there exists a group $\mathscr{G}$ such that for all $x \in \mathscr{X}$, the channel $\mathcal{T}^x$ is a covariant channel with respect to the group $\mathscr{G}$ (Definition 2.1).*

Proposition 5.1 *Any jointly covariant memory cell $\mathscr{T}_{\mathscr{X}} = \{\mathcal{T}^x_{B'\to B}\}_{x\in\mathscr{X}}$ is jointly teleportation-simulable with respect to a set $\{\mathcal{T}^x_{B'\to B}(\Phi_{RB'})\}_{x\in\mathscr{X}}$ of resource states.*

Proof. For a jointly covariant memory cell with respect to a group $\mathscr{G}$, all the channels $\mathcal{T}^x_{B'\to B}$ are jointly teleportation-simulable with respect to the resource states $\mathcal{T}^x_{B'\to B}(\Phi_{RB'})$, which are respective Choi states, by using a fixed POVM $\{E^g_{B''R}\}_{g\in\mathscr{G}}$, similar to that defined in [80, Equation (A.4), Appendix A]. See [80, Appendix A] for an explicit proof. ∎

Remark 5.2 *Any jointly teleportation-simulable memory cell is environment-parametrized, an observation that is a direct consequence of definitions. This implies that all jointly covariant memory cells are also environment-parametrized.*

5.2 Quantum reading protocols and quantum reading capacity

In a quantum reading protocol, we consider an encoder and a reader (transceiver). An encoder is one who encodes a message onto a physical memory device that is delivered to Bob, a receiver,
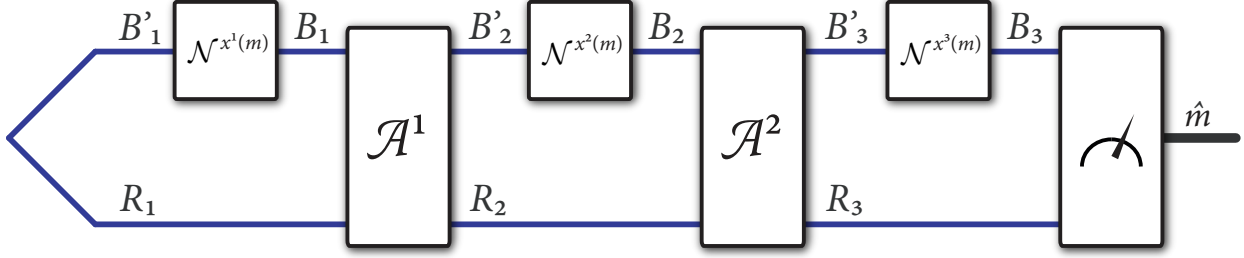
Figure 5.1. The figure depicts a quantum reading protocol that calls a memory cell three times to decode the message m as $\hat{m}$. See the discussion in Section 5.2 for a detailed description of a quantum reading protocol.

whose task it is to read the message. Bob is also referred to as the reader. The quantum reading task comprises the estimation of a message encoded in the form of a sequence of quantum channels chosen from a given set $\{\mathcal{N}^x_{B'\to B}\}_{x\in\mathcal{X}}$ of quantum channels called a memory cell, where $\mathcal{X}$ is a finite alphabet. In the most general setting considered here, the reader can use an adaptive strategy for quantum reading.

Both the encoder and the reader agree upon a memory cell $\mathscr{S}_{\mathcal{X}} = \{\mathcal{N}^x_{B'\to B}\}_{x\in\mathcal{X}}$ before executing the reading protocol. Consider a classical message set $\mathcal{M} = \{1, 2, \ldots, |M|\}$, and let M be an associated system denoting a classical register for the message. The encoder encodes a message $m \in \mathcal{M}$ using a sequence $x^n(m) = (x_1(m), x_2(m), \ldots, x_n(m))$ of length n, where $x_i(m) \in \mathcal{X}$ for all $i \in \{1, 2, \ldots, n\}$. Each sequence identifies with a corresponding codeword formed from quantum channels chosen from the memory cell $\mathscr{S}_{\mathcal{X}}$:

$$\left(\mathcal{N}^{x_1(m)}_{B'_1\to B_1}, \mathcal{N}^{x_2(m)}_{B'_2\to B_2}, \ldots, \mathcal{N}^{x_n(m)}_{B'_n\to B_n}\right). \tag{5.6}$$

Each quantum channel in a codeword, each of which represents one part of the stored information, is only read once.

An adaptive decoding strategy $\mathcal{J}_{\mathscr{S}_{\mathcal{X}}}$ makes n calls to the memory cell $\mathscr{S}_{\mathcal{X}}$. It is specified in terms of a transmitter state $\rho_{R_1 B'_1}$, a set of adaptive, interleaved channels $\{\mathcal{A}^i_{R_i B_i \to R_{i+1} B'_{i+1}}\}_{i=1}^{n-1}$, and a final quantum measurement $\{\Lambda^{\hat{m}}_{R_n B_n}\}_{\hat{m}\in\mathcal{M}}$ that outputs an estimate $\hat{m}$ of the message m.

The strategy begins with Bob preparing the input state $\rho_{R_1 B_1'}$ and sending the B_1' system into the channel $\mathcal{N}_{B_1' \to B_1}^{x_1(m)}$. The channel outputs the system B_1, which is available to Bob. She adjoins the system B_1 to the system R_1 and applies the channel $\mathcal{A}_{R_1 B_1 \to R_2 B_2'}^1$. The channel $\mathcal{A}_{R_i B_i \to R_{i+1} B_{i+1}'}^i$ is called adaptive because it can take an action conditioned on the information in the system B_i, which itself might contain partial information about the message m. Then, he sends the system B_2' into the second use of the channel $\mathcal{N}_{B_2' \to B_2}^{x_2(m)}$, which outputs a system B_2. The process of successively using the channels interleaved by the adaptive channels continues $n - 2$ more times, which results in the final output systems R_n and B_n with Bob. Next, he performs a measurement $\{\Lambda_{R_n B_n}^{\hat{m}}\}_{\hat{m} \in \mathcal{M}}$ on the output state $\rho_{R_n B_n}$, and the measurement outputs an estimate $\hat{m}$ of the original message m. See Figure 5.1 for a depiction of a quantum reading protocol.

It is apparent that a non-adaptive strategy is a special case of an adaptive strategy in which the reader does not perform any adaptive channels and instead uses $\rho_{RB'^n}$ as the transmitter state with each B_i' system passing through the corresponding channel $\mathcal{N}_{B_i' \to B_i}^{x_i(m)}$ and R being an idler system. The final step in such a non-adaptive strategy is to perform a decoding measurement on the joint system RB^n.

As we argued previously, it is natural to consider the use of an adaptive strategy for a quantum reading protocol because the channel input and output systems are in the same physical location. In a quantum reading protocol, the reader assumes the role of both the transmitter and receiver.

Definition 5.4 (Quantum reading protocol) *An (n, R, ε) quantum reading protocol for a memory cell $\mathscr{S}_{\mathcal{X}}$ is defined by an encoding map $\mathcal{E}_{\mathrm{enc}} : \mathcal{M} \to \mathcal{X}^{\times n}$ and an adaptive strategy $\mathcal{J}_{\mathscr{S}_{\mathcal{X}}}$ with measurement $\{\Lambda_{R_n B_n}^{\hat{m}}\}_{\hat{m} \in \mathcal{M}}$. The protocol is such that the average success probability is at least $1 - \varepsilon$, where $\varepsilon \in (0, 1)$:*

$$1 - \varepsilon \leq 1 - p_{\mathrm{err}} :=$$
$$\frac{1}{|M|} \sum_m \mathrm{Tr} \left\{ \Lambda_{R_n B_n}^{(m)} \left(\mathcal{N}_{B_n' \to B_n}^{x_n(m)} \circ \mathcal{A}_{R_{n-1} B_{n-1} \to R_n B_n'}^{n-1} \circ \cdots \circ \mathcal{A}_{R_1 B_1 \to R_2 B_2'}^1 \circ \mathcal{N}_{B_1' \to B_1}^{x_1(m)} \right) (\rho_{R_1 B_1'}) \right\}. \quad (5.7)$$

The rate R of a given (n, R, ε) quantum reading protocol is equal to the number of bits read per

channel use:

$$R := \frac{1}{n} \log_2 |M|. \tag{5.8}$$

To arrive at a definition of quantum reading capacity, we demand that there exists a sequence of reading protocols, indexed by n, for which the error probability $p_{\text{err}} \to 0$ as $n \to \infty$ at a fixed rate R.

Definition 5.5 (Achievable rate) *A rate R is called achievable if $\forall \varepsilon \in (0, 1)$, $\delta > 0$, and sufficiently large n, there exists an $(n, R - \delta, \varepsilon)$ code.*

Definition 5.6 (Quantum reading capacity) *The quantum reading capacity $\mathcal{C}(\mathscr{S}_{\mathscr{X}})$ of a memory cell $\mathscr{S}_{\mathscr{X}}$ is defined as the supremum of all achievable rates R.*

5.3 Fundamental limits on quantum reading capacities

In this section, we establish second-order and strong converse bounds for any environment-parametrized memory cell. We also establish general weak converse (upper) bounds on various reading capacities.

5.3.1 Converse bounds for environment-parametrized memory cells

In this section, we derive upper bounds on the performance of quantum reading of environment-parametrized memory cells.

To begin with, let us consider an (n, R, ε) quantum reading protocol of an environment-parametrized memory cell $\mathscr{E}_{\mathscr{X}} = \{\mathcal{N}^x\}_{x \in \mathscr{X}}$ (Definition 5.1). The structure of reading protocols involving adaptive channels simplifies immensely for memory cells that are teleportation-simulable and more generally environment-parametrized. This is a direct consequence of the symmetry obeyed by the channels in the cell. For such memory cells, a quantum reading protocol can be simulated by one in which every channel use is replaced by the encoder preparing the ancillary state $\theta_E^{x_i(m)}$ from (5.4) and then interacting the channel input with the interaction channel $\mathcal{F}_{B'E \to B}$. Critically, each interaction channel $\mathcal{F}_{B'E \to B}$ is independent of the message $m \in \mathscr{M}$. Let

$$\theta_{E^n}^{x^n(m)} := \bigotimes_{i=1}^{n} \theta_E^{x_i(m)} \tag{5.9}$$
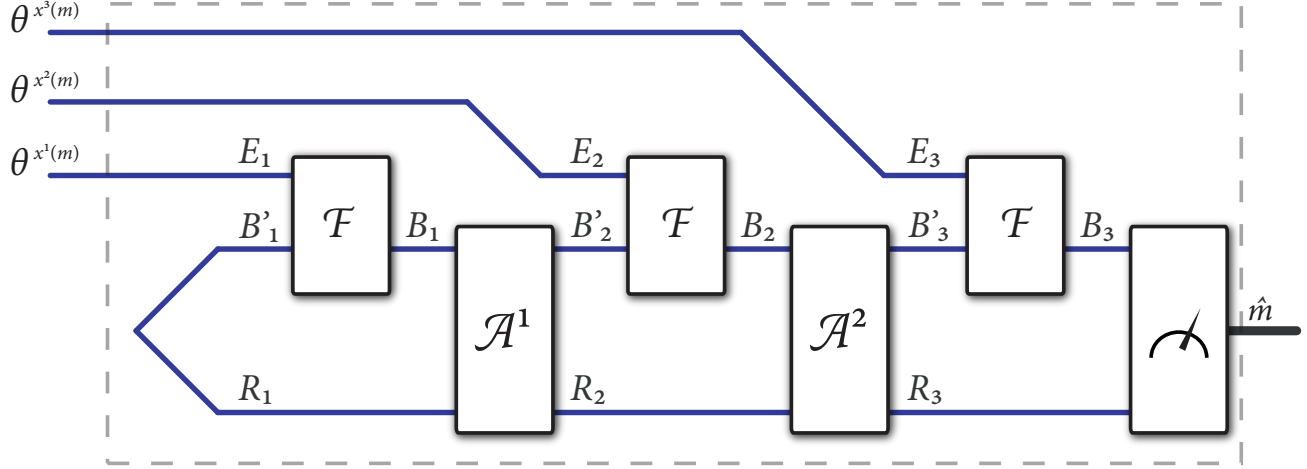
Figure 5.2. The figure depicts how a quantum reading protocol of an environment-parametrized memory cell can be rewritten as a protocol that tries to decode the message m from the ancillary states $\theta_{E^n}^{x^n(m)}$. All of the operations inside the dashed lines can be understood as a measurement on the states $\theta_{E^n}^{x^n(m)}$.

denote the ancillary state needed for the simulation of all n of the channel uses in the quantum reading protocol. This leads to the translation of a general quantum reading protocol to one in which all of the rounds of adaptive channels can be delayed until the very end of the protocol, such that the resulting protocol is a non-adaptive quantum reading protocol.

The following proposition, holding for any environment-parametrized memory cell, is a direct consequence of observations made in [50, Section V], [51], [228, Theorem 14 & Remark 11], and [127]. We thus omit a detailed proof, but Figure 5.2 clarifies the main idea: any quantum reading protocol of an environment-parametrized memory cell can be rewritten as in Figure 5.2. Inspecting the figure, one can notice that the protocol can be understood as a non-adaptive decoding of the ancillary states $\theta_{E^n}^{x^n(m)}$, with the decoding measurement constrained to contain the interaction channel $\mathcal{F}_{B'E\to B}$ interleaved between arbitrary adaptive channels. Thus, Proposition 5.2 establishes that an adaptive strategy used for decoding an environment-parametrized memory cell can be reduced to a particular non-adaptive decoding of the ancillary states $\theta_{E^n}^{x^n(m)}$.

Proposition 5.2 (Adaptive-to-non-adaptive reduction) *Let $\mathscr{E}_{\mathscr{X}} = \{\mathcal{N}_{B'\to B}^x\}_{x\in\mathscr{X}}$ be an environment-parametrized memory cell with an associated set of ancillary states $\{\theta_E^x\}_{x\in\mathscr{X}}$ and a fixed interaction channel $\mathcal{F}_{B'E\to B}$, as given in Definition 5.1. Then any quantum reading protocol as stated in Defini-*

tion 5.4, which uses an adaptive strategy $\mathcal{J}_{\mathscr{E}_{\mathscr{X}}}$, *can be simulated as a non-adaptive quantum reading protocol, in the following sense:*

$$\text{Tr}\left\{\Lambda^{\hat{m}}_{E_n B_n}\left(\mathcal{N}^{x_n(m)}_{B'_n \to B_n} \circ \mathcal{A}^{n-1}_{E_{n-1}B_{n-1}\to E_n B'_n} \circ \cdots \circ \mathcal{A}^1_{E_1 B_1 \to E_2 B'_2} \circ \mathcal{N}^{x_1(m)}_{B'_1 \to B_1}\right)\left(\rho_{E_1 B'_1}\right)\right\}$$
$$= \text{Tr}\left\{\Gamma^{\hat{m}}_{E^n}\left(\bigotimes_{i=1}^n \theta^{x_i(m)}_E\right)\right\}, \quad (5.10)$$

for some POVM $\{\Gamma^{\hat{m}}_{E^n}\}_{\hat{m}\in\mathscr{M}}$ *that depends on* $\mathcal{J}_{\mathscr{E}_{\mathscr{X}}}$.

Using the observation in Proposition 5.2, we now show how to arrive at upper bounds on the performance of any reading protocol that uses an environment-parametrized memory cell.

Our proof strategy is to employ a generalized divergence to make a comparison between the states involved in the actual reading protocol and one in which the memory cell is fixed as $\hat{\mathscr{E}} := \{\mathcal{P}_{B' \to B}\}$, containing only a single channel with environment state $\hat{\theta}_E$ and interaction channel $\mathcal{F}_{B'E \to B}$. The latter reading protocol contains no information about the message m. Observe that the augmented memory cell $\{\mathscr{E}_{\mathscr{X}}, \hat{\mathscr{E}}\}$ is environment-parametrized.

One of the main steps that we use in our proof is as follows. Consider the following states:

$$\sigma_{M\hat{M}} = \sum_{m\in\mathscr{M},\hat{m}\in\mathscr{M}} \frac{1}{|M|} |m\rangle\langle m|_M \otimes p_{\hat{M}|M}(\hat{m}|m) |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}, \quad (5.11)$$

$$\tau_{M\hat{M}} = \sum_{m\in\mathscr{M}} \frac{1}{|M|} |m\rangle\langle m|_M \otimes \hat{\tau}_{\hat{M}}, \quad (5.12)$$

where $p_{\hat{M}|M}(\hat{m}|m)$ is a distribution that results after the final decoding step of an (n, R, ε) quantum reading protocol, while $\hat{\tau}_{\hat{M}}$ is a fixed state. By applying the comparator test $\{\Pi_{M\hat{M}}, \mathbb{1}_{M\hat{M}} - \Pi_{M\hat{M}}\}$, defined by

$$\Pi_{M\hat{M}} := \sum_m |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{\hat{M}}, \quad (5.13)$$

and using definitions, we arrive at the following inequalities that hold for an arbitrary (n, R, ε) quantum reading protocol:

$$\text{Tr}\{\Pi_{M\hat{M}}\sigma_{M\hat{M}}\} \geq 1 - \varepsilon, \quad \text{Tr}\{\Pi_{M\hat{M}}\tau_{M\hat{M}}\} = \frac{1}{|M|}. \quad (5.14)$$

Then by applying the definition of the ε-hypothesis-testing divergence, we arrive at the following bound, which is a critical first step to establish second-order and strong converse bounds:

$$D_h^\varepsilon(\sigma_{M\hat{M}}\|\tau_{M\hat{M}}) \geq \log_2 |M|. \tag{5.15}$$

In the converse proof that follows, the main idea for arriving at an upper bound on performance is to make a comparison between the case in which the message m is encoded in a sequence of quantum channels and the case in which it is not.

Second-order asymptotics and strong converse

In this section, we derive second-order asymptotics and strong converse bounds for environment-parametrized memory cells. We begin by deriving a relation between the quantum reading rate and the hypothesis testing divergence.

Lemma 5.1 *The following bound holds for an (n, R, ε) reading protocol that uses an environment-parametrized memory cell (Definition 5.1):*

$$\log_2 |M| = nR \leq$$

$$\sup_{p_{X^n}} \inf_{\hat{\theta}} D_h^\varepsilon\left(\sum_{x^n \in \mathcal{X}^n} p_{X^n}(x^n) \, |x^n\rangle\langle x^n|_{X^n} \otimes \theta_{E^n}^{x^n} \, \middle\| \, \sum_{x^n \in \mathcal{X}^n} p_{X^n}(x^n) \, |x^n\rangle\langle x^n|_{X^n} \otimes \hat{\theta}_E^{\otimes n}\right). \tag{5.16}$$

Proof. Proof begins by applying the observation from Proposition 5.2, which allows reduction of any adaptive protocol to a non-adaptive one. If the encoder chooses the message m uniformly at random and places it in a system M, the output state in (5.11) after Bob's decoding measurement in the actual protocol is

$$\sigma_{M\hat{M}} = \sum_{m,\hat{m}} \frac{1}{|M|} |m\rangle\langle m|_M \otimes \text{Tr}\left\{\Gamma_{E^n}^{\hat{m}} \theta_{E^n}^{x^n(m)}\right\} |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}, \tag{5.17}$$

where

$$\theta_{E^n}^{x^n(m)} \equiv \bigotimes_{i=1}^{n} \theta_E^{x_i(m)}. \tag{5.18}$$

The success probability $p_{\text{succ}} := 1 - p_{\text{err}}$ is defined as

$$p_{\text{succ}} := \frac{1}{|M|} \sum_{m \in \mathscr{M}} \text{Tr}\left\{\Gamma_{E^n}^m \theta_{E^n}^{x^n(m)}\right\}. \tag{5.19}$$

The output state in (5.12) after Bob's decoding measurement in a reading protocol that uses the memory cell $\hat{\mathscr{E}}$ is

$$\tau_{M\hat{M}} = \sum_m \frac{1}{|M|} |m\rangle\langle m|_M \otimes \sum_{\hat{m}} \text{Tr}\left\{\Gamma_{E^n}^{\hat{m}} \hat{\theta}_E^{\otimes n}\right\} |\hat{m}\rangle\langle\hat{m}|_{\hat{M}}. \tag{5.20}$$

Then a generalized divergence can be bounded as follows:

$$\mathbf{D}(\{p_{\text{succ}}, 1 - p_{\text{succ}}\} \| \{1/|M|, 1 - 1/|M|\})$$

$$\leq \mathbf{D}(\sigma_{M\hat{M}} \| \tau_{M\hat{M}})$$

$$\leq \mathbf{D}\left(\sum_m \frac{1}{M} |m\rangle\langle m|_M \otimes \theta_{E^n}^{x^n(m)} \, \middle\| \, \sum_m \frac{1}{M} |m\rangle\langle m|_M \otimes \hat{\theta}_E^{\otimes n}\right) \tag{5.21}$$

The first inequality follows from applying the comparator test in (5.13) to $\sigma_{M\hat{M}}$ and $\tau_{M\hat{M}}$. The second inequality follows from the data-processing inequality in (2.57) as the final measurement is a quantum channel. Since the above bound holds for all $\hat{\theta}_E$, it can be concluded that

$$\mathbf{D}(\{p_{\text{succ}}, 1 - p_{\text{succ}}\} \| \{1/|M|, 1 - 1/|M|\}) \leq$$

$$\inf_{\hat{\theta}} \mathbf{D}\left(\sum_m \frac{1}{|M|} |m\rangle\langle m|_M \otimes \theta_{E^n}^{x^n(m)} \, \middle\| \, \sum_m \frac{1}{|M|} |m\rangle\langle m|_M \otimes \hat{\theta}_E^{\otimes n}\right) \tag{5.22}$$

Now optimizing over all input distributions, we arrive at the following general bound:

$$\mathbf{D}(\{p_{\text{succ}}, 1 - p_{\text{succ}}\} \| \{1/|M|, 1 - 1/|M|\}) \leq$$

$$\sup_{p_{X^n}} \inf_{\hat{\theta}} \mathbf{D}\left(\sum_{x^n \in \mathscr{X}^n} p_{X^n}(x^n) |x^n\rangle\langle x^n|_{X^n} \otimes \theta_{E^n}^{x^n} \, \middle\| \, \sum_{x^n \in \mathscr{X}^n} p_{X^n}(x^n) |x^n\rangle\langle x^n|_{X^n} \otimes \hat{\theta}_E^{\otimes n}\right), \tag{5.23}$$

where $x^n := x_1 x_2 \cdots x_n$ and $\theta_{E^n}^{x^n} = \bigotimes_{i=1}^n \theta_E^{x_i}$. Observe that the lower bound contains the relevant performance parameters such as success probability and number of messages, while the upper bound is an information quantity, depending exclusively on the memory cell $\mathscr{E}_{\mathscr{X}}$.

Substituting the hypothesis testing divergence in the above and applying (5.15), we obtain the following bound for an (n, R, ε) reading protocol that uses an environment-parametrized memory cell:

$$\log_2 |M| = nR \leq$$

$$\sup_{p_{X^n}} \inf_{\hat{\theta}} D_h^{\varepsilon} \left(\sum_{x^n \in \mathscr{X}^n} p_{X^n}(x^n) |x^n\rangle\langle x^n|_{X^n} \otimes \theta_{E^n}^{x^n} \middle\| \sum_{x^n \in \mathscr{X}^n} p_{X^n}(x^n) |x^n\rangle\langle x^n|_{X^n} \otimes \hat{\theta}_E^{\otimes n} \right) \quad (5.24)$$

This concludes our proof. ■

A direct consequence of Lemma 5.1 and [231, Theorem 4] is the following proposition:

Proposition 5.3 *For an (n, R, ε) quantum reading protocol for an environment-parametrized memory cell $\mathscr{E}_{\mathscr{X}} = \{\mathcal{N}^x\}_{x \in \mathscr{X}}$ (Definition 5.1), the following inequality holds*

$$R \leq \max_{p_X} I(X; E)_\theta + \sqrt{\frac{V_\varepsilon(\mathscr{E}_{\mathscr{X}})}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right), \quad (5.25)$$

where

$$\theta_{XE} = \sum_{x \in \mathscr{X}} p_X(x) |x\rangle\langle x|_X \otimes \theta_E^x, \quad (5.26)$$

$\Phi^{-1}(\varepsilon)$ *is the inverse of the cumulative distribution function[1], and*

$$V_\varepsilon(\mathscr{E}_{\mathscr{X}}) = \begin{cases} \min_{p_X \in P(\mathscr{E}_{\mathscr{X}})} V(\theta_{XE} \| \theta_X \otimes \theta_E), & \varepsilon \in (0, 1/2] \\ \max_{p_X \in P(\mathscr{E}_{\mathscr{X}})} V(\theta_{XE} \| \theta_X \otimes \theta_E), & \varepsilon \in (1/2, 1) \end{cases}, \quad (5.28)$$

where $V(\rho \| \sigma)$ denotes the variance between $\rho, \sigma \in \mathscr{D}(\mathcal{H})$ and $P(\mathscr{E}_{\mathscr{X}})$ denotes a set $\{p_X\}$ of probability distributions that achieve the maximum in $\max_{p_X} I(X; E)_\theta$.

Proposition 5.4 *The success probability p_{succ} of any (n, R, ε) quantum reading protocol for an*

---

[1]The cumulative distribution function corresponding to the standard normal random variable is defined as

$$\Phi(a) := \int_{-\infty}^{a} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2} x^2\right) dx. \quad (5.27)$$

Its inverse is also useful for us and is defined as $\Phi^{-1}(a) := \sup \{a \in \mathbb{R} | \Phi(a) \leq \varepsilon\}$, which reduces to the usual inverse for $\varepsilon \in (0, 1)$.

environment-parametrized memory cell $\mathscr{E}_{\mathscr{X}}$ (Definition 5.1) is bounded from above as

$$p_{\text{succ}} \leq 2^{-n \sup_{\alpha>1}\left(1-\frac{1}{\alpha}\right)\left(R-\widetilde{I}_{\alpha}(\mathscr{E}_{\mathscr{X}})\right)}, \tag{5.29}$$

where

$$\widetilde{I}_{\alpha}(\mathscr{E}_{\mathscr{X}}) = \max_{p_X} \widetilde{I}_{\alpha}(X;E)_{\theta}, \tag{5.30}$$

for θ_{XE} as defined in (5.26).

Proof. A proof follows by combining the bound in (5.23) with the main result of [65] (see also [232] for arguments about extending the range of α from $(1,2]$ to $(1,\infty)$). ∎

Theorem 5.1 *The quantum reading capacity of any environment-parametrized memory cell $\mathscr{E}_{\mathscr{X}} = \{\mathcal{N}^x_{B'\to B}\}_{x\in\mathscr{X}}$ (Definition 5.1) is bounded from above as*

$$\mathcal{C}(\mathscr{E}_{\mathscr{X}}) \leq \max_{p_X} I(X;E)_{\theta}, \tag{5.31}$$

where θ_{XE} is defined in (5.26).

Proof. The statement follows from Proposition 5.3, by taking the limit $n \to \infty$. Alternatively, the statement can also be concluded from Definition 5.6 and Proposition 5.4, by taking the limit $\alpha \to 1$. ∎

Direct consequences of the above theorems and Remark 5.2 are the following corollaries:

Corollary 5.1 *For any (n, R, ε) quantum reading protocol and jointly teleportation-simulable memory cell $\mathscr{T}_{\mathscr{X}}$ (Definition 2.2) with associated resource states $\{\omega^x_{RB}\}_{x\in\mathscr{X}}$, the reading rate R is bounded from above as*

$$R \leq \max_{p_X} I(X;RB)_{\omega} + \sqrt{\frac{V_{\varepsilon}(\mathscr{T}_{\mathscr{X}})}{n}} \Phi^{-1}(\varepsilon) + \mathcal{O}\left(\frac{\log n}{n}\right), \tag{5.32}$$

where

$$\omega_{XRB} := \sum_{x\in\mathscr{X}} p_X(x) |m\rangle\langle m|_X \otimes \omega^x_{RB} \tag{5.33}$$

and

$$V_\varepsilon(\mathscr{T}_\mathscr{X}) := \left\{ \begin{array}{ll} \min_{p_X \in P(\mathscr{T}_\mathscr{X})} V\left(\omega_{XRB} \| \omega_X \otimes \omega_{RB}\right), & \varepsilon \in (0, 1/2] \\ \max_{p_X \in P(\mathscr{T}_\mathscr{X})} V\left(\omega_{XRB} \| \omega_X \otimes \omega_{RB}\right), & \varepsilon \in (1/2, 1) \end{array} \right\}. \quad (5.34)$$

In the above, $P(\mathscr{T}_\mathscr{X})$ denotes a set $\{p_X\}$ of probability distributions that are optimal for $\max_{p_X} I(X; RB)_\omega$.

Corollary 5.2 *The quantum reading capacity of any jointly teleportation-simulable memory cell $\mathscr{T}_\mathscr{X} = \{\mathcal{T}^x_{B' \to B}\}_{x \in \mathscr{X}}$ associated with a set $\{\omega^x_{RB}\}$ of resource states is bounded from above as*

$$\mathcal{C}(\mathscr{T}_\mathscr{X}) \leq \max_{p_X} I(X; RB)_\omega, \quad (5.35)$$

where

$$\omega_{XRB} = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x|_X \otimes \omega^x_{RB}. \quad (5.36)$$

The capacity bounds given above are tight for a wide variety of channels, as clarified in the following remark:

Remark 5.3 *The quantum reading capacity is achieved for a jointly teleportation-simulable memory cell $\mathscr{T}_\mathscr{X} = \{\mathcal{T}^x_{B' \to B}\}_{x \in \mathscr{X}}$ when, for all $x \in \mathscr{X}$, ω^x_{RB} is equal to the Choi state of the channel $\mathcal{T}^x_{B' \to B}$. More finely, the upper bound in Corollary 5.1 is achieved in such a case by invoking [231, Theorem 4].*

5.3.2 Weak converse bound for a non-adaptive reading protocol

In this section, we establish a general weak converse when the strategy employed is non-adaptive. Consider a state $\rho_{MRB'^n}$ of the form

$$\rho_{MRB'^n} = \frac{1}{|M|} \sum_{m \in \mathscr{M}} |m\rangle\langle m|_M \otimes \rho_{RB'^n}. \quad (5.37)$$

Suppose that $\rho_{RB'^n}$ is purified by the pure state $\psi_{RSB'^n}$. Bob passes the transmitter state $\rho_{RB'^n}$ through a codeword sequence $\mathcal{N}^{x^n(m)}_{B'^n \to B^n} := \bigotimes_{i=1}^n \mathcal{N}^{x_i(m)}_{B'_i \to B_i}$, where the choice m depends on the classical value $m \in \mathscr{M}$ in the register M. Let $\mathcal{U}^{\mathcal{N}^{x^n(m)}}_{B'^n \to B^n E^n} := \bigotimes_{i=1}^n \mathcal{U}^{\mathcal{N}^{x_i(m)}}_{B'_i \to B_i E_i}$, where $\mathcal{U}^{\mathcal{N}^{x_i(m)}}_{B'_i \to B_i E_i}$ denotes an

isometric quantum channel extending $\mathcal{N}_{B'_i \to B_i}^{x_i(m)}$, for all $i \in [n]$. After the isometric channel acts, the overall state is as follows:

$$\sigma_{MRSB^n E^n} = \frac{1}{|M|} \sum_m |m\rangle\langle m|_M \otimes \mathcal{U}_{B'^n \to B^n E^n}^{\mathcal{N}^{x^n(m)}} (\psi_{RSB'^n}). \tag{5.38}$$

Let $\sigma'_{M\hat{M}} = \mathcal{D}_{RB^n \to \hat{M}}(\sigma_{MRB^n})$ be the output state at the end of protocol after the decoding measurement $\mathcal{D}$ is performed by Bob. Let $\overline{\Phi}_{M\hat{M}}$ denote the maximally classically correlated state:

$$\overline{\Phi}_{M\hat{M}} := \frac{1}{|M|} \sum_{m \in \mathcal{M}} |m\rangle\langle m|_M \otimes |m\rangle\langle m|_{\hat{M}}. \tag{5.39}$$

Proposition 5.5 *The non-adaptive reading capacity of any quantum memory cell $\mathscr{S}_{\mathcal{X}} = \{\mathcal{N}^x\}_{\mathcal{X}}$ is upper bounded as*

$$\mathcal{C}_{\text{non-adaptive}}(\mathscr{S}_{\mathcal{X}}) \leq \sup_{p_X, \phi_{RB'}} I(XR; B)_\tau, \tag{5.40}$$

where

$$\tau_{XRB} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}_{B' \to B}^x(\phi_{RB'}), \tag{5.41}$$

and it suffices for $\phi_{RB'}$ to be a pure state such that $\dim(\mathcal{H}_R) = \dim(\mathcal{H}'_B)$.

Proof. For any (n, R, ε) quantum reading protocol using a non-adaptive strategy, one has

$$\frac{1}{2} \left\| \overline{\Phi}_{M\hat{M}} - \sigma'_{M\hat{M}} \right\|_1 \leq \varepsilon. \tag{5.42}$$

Then consider the following chain of inequalities:

$$\log_2 |M| = I(M; \hat{M})_{\overline{\Phi}} \tag{5.43}$$

$$\leq I(M; \hat{M})_{\sigma'} + f(n, \varepsilon) \tag{5.44}$$

$$\leq I(M; RSB^n)_{\sigma} + f(n, \varepsilon) \tag{5.45}$$

$$= I(M; RS)_{\sigma} + I(M; B^n | RS)_{\sigma} + f(n, \varepsilon) \tag{5.46}$$

$$= I(M; B^n | RS)_{\sigma} + f(n, \varepsilon) \tag{5.47}$$

$$= S(B^n | RS)_{\sigma} - S(B^n | RSM)_{\sigma} + f(n, \varepsilon) \tag{5.48}$$

$$= S(B^n | RS)_{\sigma} + S(B^n | E^n M)_{\sigma} + f(n, \varepsilon) \tag{5.49}$$

The first inequality follows from the uniform continuity of conditional entropy [61,62], where $f(n, \varepsilon)$ is a function of n and the error probability ε such that $\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{f(n, \varepsilon)}{n} = 0$. The second inequality follows from data processing. The second equality follows from the chain rule for the mutual information. The third equality follows because the reduced state of systems M and RS is a product state. The fifth equality follows from the duality of the conditional entropy. Continuing, it follows that

$$(5.49) \leq \sum_{i=1}^{n} [S(B_i | RS)_{\sigma} + S(B_i | E_i M)_{\sigma}] + f(n, \varepsilon) \tag{5.50}$$

$$= \sum_{i=1}^{n} \left[S(B_i | RS)_{\sigma} - S(B_i | RSB'_{[n] \setminus \{i\}} M)_{\sigma} \right] + f(n, \varepsilon) \tag{5.51}$$

$$= \sum_{i=1}^{n} I(MB'_{[n] \setminus \{i\}}; B_i | RS)_{\sigma} + f(n, \varepsilon) \tag{5.52}$$

$$\leq \sum_{i=1}^{n} I(MB'_{[n] \setminus \{i\}} RS; B_i)_{\sigma} + f(n, \varepsilon) \tag{5.53}$$

$$= nI(MR'; B | Q)_{\sigma} + f(n, \varepsilon) \tag{5.54}$$

$$\leq n \sup_{p_X, \phi_{\widetilde{R}B'}} I(X\widetilde{R}; B)_{\tau} + f(n, \varepsilon). \tag{5.55}$$

The first inequality follows from subadditivity of quantum entropy. The final inequality follows because the average can never exceed the maximum. In the above, $B'_{[n] \setminus \{i\}}$ denotes the joint system

$B'_1 B'_2 \cdots B'_{i-1} B'_{i+1} \cdots B'_n$, such that system B'_i is excluded. Furthermore,

$$\sigma_{MQR'B} = \frac{1}{M} \frac{1}{n} \sum_{m=1}^{|M|} \sum_{i=1}^{n} |m\rangle\langle m|_M \otimes |i\rangle\langle i|_Q \otimes \mathcal{N}^{x_i(m)}_{B'_i \to B_i}(\sigma_{RSB'_i B'_{[n]\setminus i}}), \quad (5.56)$$

where we have introduced an auxiliary classical register Q, and $R' := RSB'_{[n]\setminus i}$. Also,

$$\tau_{X\tilde{R}B} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}^x(\phi_{\tilde{R}B'}). \quad (5.57)$$

Now we argue that it is sufficient to take $\phi_{\tilde{R}B'}$ to be a pure state. Suppose that $\phi_{\hat{R}B'}$ is a mixed state and let R'' be a purifying system for it. Then by the data-processing inequality, it follows that

$$I(X\hat{R}; B)_\tau \leq I(X\hat{R}R''; B)_\tau, \quad (5.58)$$

where $\tau_{X\hat{R}R''B}$ is a state of the form in (5.57). The statement in the theorem about the dimension of the reference system follows from the Schmidt decomposition and the fact that the reference system purifies the system B' being input to the channel. ∎

5.3.3 Weak converse bound for a quantum reading protocol

Now we establish a general weak converse bound for the quantum reading capacity of an arbitrary memory cell.

Theorem 5.2 *The quantum reading capacity of a quantum memory cell $\mathscr{S}_{\mathscr{X}} = \{\mathcal{N}^x\}_{\mathscr{X}}$ is bounded from above as*

$$\mathcal{C}(\mathscr{S}_{\mathscr{X}}) \leq \sup_{\rho_{XRB'}} \left[I(X; B|R)_\omega - I(X; B'|R)_\rho \right], \quad (5.59)$$

where

$$\omega_{XRB} := \sum_{x \in} p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}^x_{B' \to B}(\rho^x_{RB'}), \quad (5.60)$$

$$\rho_{XRB'} = \sum_{x \in \mathscr{X}} p_X(x) |x\rangle\langle x|_X \otimes \rho^x_{RB'}, \quad (5.61)$$

and $\dim(\mathcal{H}_R)$ *can be unbounded.*

Remark 5.4 *It should be noted that the upper bound* $\sup_{\rho_{XRB'}} [I(X;B|R)_\omega - I(X;B'|R)_\rho]$ *is non-negative. A particular choice of the input state* $\rho_{XRB'}$ *is* $\rho_{XRB'} = \sum_{x\in\mathscr{X}} p_X(x) |x\rangle\langle x|_X \otimes \rho_{RB'}$. *Then in this case,*

$$I(X;B|R)_\omega - I(X;B'|R)_\rho = I(X;RB)_\omega - I(X;RB')_\rho = I(X;RB)_\omega \geq 0, \qquad (5.62)$$

with $\omega_{XRB} = \sum_{x\in\mathscr{X}} p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}^x_{B'\to B}(\rho_{RB'})$. *Thus, we can conclude that*

$$\sup_{\rho_{XRB'}} [I(X;B|R)_\omega - I(X;B'|R)_\rho] \geq 0. \qquad (5.63)$$

Proof of Theorem 5.2. For any (n,R,ε) quantum reading protocol as stated in Definition 5.4, we have

$$\frac{1}{2} \left\| \overline{\Phi}_{M\hat{M}} - \sigma'_{M\hat{M}} \right\|_1 \leq \varepsilon, \qquad (5.64)$$

where $\overline{\Phi}_{M\hat{M}}$ is a maximally classically correlated state (5.39) and

$$\sigma'_{M\hat{M}} = \mathcal{D}_{R_n B_n \to \hat{M}} \left(\sigma^n_{MR_n B_n} \right) \qquad (5.65)$$

is the output state at the end of the protocol after Bob performs the final decoding measurement. The input state before the ith call of the channel is denoted as

$$\rho^i_{MR_i B'_i} = \frac{1}{|M|} \sum_{m\in\mathcal{M}} |m\rangle\langle m|_M \otimes \mathcal{A}^{(i-1)}_{R_{i-1}B_{i-1}\to R_i B'_i} \circ \mathcal{N}^{x_{i-1}(m)}_{B'_{i-1}\to B_{i-1}} \circ \cdots$$

$$\cdots \circ \mathcal{N}^{x_2(m)}_{B'_2 \to B_2} \circ \mathcal{A}^{(1)}_{R_1 B_1 \to R_2 B'_2} \circ \mathcal{N}^{x_1(m)}_{B'_1 \to B_1}(\rho_{R_1 B'_1}), \quad (5.66)$$

and the output state after the ith call of the channel is denoted as

$$\omega^i_{MR_i B_i} = \frac{1}{|M|} \sum_{m\in\mathcal{M}} |m\rangle\langle m|_M \otimes \mathcal{N}^{x_i(m)}_{B'_i \to B_i} \circ \mathcal{A}^{(i-1)}_{R_{i-1}B_{i-1}\to R_i B'_i} \circ \mathcal{N}^{x_{i-1}(m)}_{B'_{i-1}\to B_{i-1}} \circ \cdots$$

$$\cdots \circ \mathcal{N}^{x_2(m)}_{B'_2 \to B_2} \circ \mathcal{A}^{(1)}_{R_1 B_1 \to R_2 B'_2} \circ \mathcal{N}^{x_1(m)}_{B'_1 \to B_1}(\rho_{R_1 B'_1}). \quad (5.67)$$

The initial part of our proof follows steps similar to those in the proof of Proposition 5.5.

$$\log_2 |M| = I(M; \hat{M})_{\overline{\Phi}} \tag{5.68}$$

$$\leq I(M; \hat{M})_{\sigma'} + f(n, \varepsilon) \tag{5.69}$$

$$\leq I(M; R_n B_n)_{\sigma^n} + f(n, \varepsilon) \tag{5.70}$$

$$= I(M; R_n B_n)_{\omega^n} - I(M; R_1 B_1')_{\rho^1} + f(n, \varepsilon) \tag{5.71}$$

$$= I(M; R_n B_n)_{\omega^n} - I(M; R_n B_n')_{\rho^n} + I(M; R_n B_n')_{\rho^n} - I(M; R_{n-1} B_{n-1}')_{\rho^{n-1}}$$

$$+ I(M; R_{n-1} B_{n-1}')_{\rho^{n-1}} - \cdots - I(M; R_2 B_2')_{\rho^2}$$

$$+ I(M; R_2 B_2')_{\rho^2} - I(M; R_1 B_1')_{\rho^1} + f(n, \varepsilon) \tag{5.72}$$

$$\leq I(M; R_n B_n)_{\omega^n} - I(M; R_n B_n')_{\rho^n} + I(M; R_{n-1} B_{n-1})_{\omega^{n-1}} - I(M; R_{n-1} B_{n-1}')_{\rho^{n-1}}$$

$$+ I(M; R_{n-2} B_{n-2})_{\omega^{n-2}} - \cdots - I(M; R_2 B_2')_{\rho^2}$$

$$+ I(M; R_1 B_1)_{\omega^1} - I(M; R_1 B_1')_{\rho^1} + f(n, \varepsilon) \tag{5.73}$$

The second equality follows because the state ρ^1 is product between systems M and $R_1 B_1'$. The third equality follows by adding and subtracting equal information quantities. The third inequality follows from the data-processing inequality: mutual information is non-increasing under the local action of quantum channels. Continuing, it follows that

$$(5.73) = \sum_{i=1}^n \left[I(M; R_i B_i)_{\omega^i} - I(M; R_i B_i')_{\rho^i} \right] + f(n, \varepsilon) \tag{5.74}$$

$$= \sum_{i=1}^n \left[I(M; B_i | R_i)_{\omega^i} - I(M; B_i' | R_i)_{\rho^i} \right] + f(n, \varepsilon) \tag{5.75}$$

$$= n \left[I(M; B | RQ)_{\overline{\omega}} - I(M; B' | RQ)_{\overline{\rho}} \right] + f(n, \varepsilon) \tag{5.76}$$

$$\leq n \sup_{\rho_{XRB'}} \left[I(X; B | R)_{\omega} - I(X; B' | R)_{\rho} \right] + f(n, \varepsilon), \tag{5.77}$$

The second equality follows from the chain rule for conditional mutual information. The third

equality follows by defining the following states:

$$\overline{\omega}_{QMRB} = \sum_{i=1}^{n} \frac{1}{n} |i\rangle\langle i|_Q \otimes \omega^i_{MR_iB_i}, \tag{5.78}$$

$$\overline{\rho}_{QMRB'} = \sum_{i=1}^{n} \frac{1}{n} |i\rangle\langle i|_Q \otimes \rho^i_{MR_iB'_i}. \tag{5.79}$$

The final inequality follows by defining the following states:

$$\omega_{XRB} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}^x_{B'\to B}(\rho^x_{RB'}), \tag{5.80}$$

$$\rho_{XRB'} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \rho^x_{RB'}, \tag{5.81}$$

and realizing that the states $\overline{\omega}_{QMRB}$ and $\overline{\rho}_{QMRB'}$ are particular examples of the states ω_{XRB} and $\rho_{XRB'}$, respectively, with the identifications $M \to X$ and $QR \to R$. Putting everything together, we get

$$\frac{1}{n} \log_2 |M| \leq \sup_{\rho_{XRB'}} [I(X;B|R)_\omega - I(X;B'|R)_\rho] + \frac{1}{n} f(n,\varepsilon) \tag{5.82}$$

Taking the limit as $n \to \infty$ and then as $\varepsilon \to 0$ concludes the proof. ∎

Now we develop a general upper bound on the energy-constrained quantum reading capacity of a beamsplitter memory cell $\mathscr{B}_{\mathscr{X}} = \{\mathcal{B}^x\}_{x\in\mathscr{X}}$, where $x \in \mathscr{X}$ represents the transmissivity η and phase ϕ of the beamsplitter $\mathcal{B}^x$ [233, Eqns. (5)–(6)] (see Section 4.3.1). This bound has implications for the reading protocols considered in [216].

Let $\hat{O}$ denote the familiar $a^\dagger a$ number observable and let $N_S \in [0,\infty)$. The energy-constrained reading capacity $\mathcal{C}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S)$ of a beamsplitter memory cell $\mathscr{B}_{\mathscr{X}}$ is defined in the obvious way, such that the average input to each call of the memory is bounded from above by $N_S \geq 0$. This definition implies that the function to optimize in the capacity upper bound has the following constraint: for any input ensemble $\{p_X(x), \rho^x_{RB'}\}$,

$$\text{Tr}\left\{\hat{O} \int p_X(x)\rho^x_{B'}\right\} \leq N_S. \tag{5.83}$$

Since the energy of the output state of $\mathcal{B}^x$ does not depend on the phase ϕ, the dependence of x

on ϕ is dropped and $x = \eta$ is taken for the discussion. For a memory cell $\mathscr{B}_{\mathscr{X}}$, the energy of the output state is constrained as

$$\text{Tr}\left\{\sum_{x\in\mathscr{X}} p_X(x)\mathcal{B}^x(\rho_{B'}^x)\hat{O}\right\} = \sum_{x\in\mathscr{X}} p_X(x)\,\text{Tr}\left\{\mathcal{B}^x(\rho_{B'}^x)\hat{O}\right\} \tag{5.84}$$

$$= \sum_{x\in\mathscr{X}} p_X(x)\eta\,\text{Tr}\left\{\rho_{B'}^x\hat{O}\right\} \tag{5.85}$$

$$\leq N_S, \tag{5.86}$$

where the second equality holds because the transmissivity of each $\mathcal{B}^x$ is $\eta \in [0,1]$.

Based on the above discussion, the following theorem can be stated.

Corollary 5.3 *The energy-constrained reading capacity of a beamsplitter memory cell $\mathscr{B}_{\mathscr{X}} = \{\mathcal{B}^x\}_{x\in\mathscr{X}}$ is bounded from above as*

$$\mathcal{C}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S) \leq 2g(N_S), \tag{5.87}$$

where θ^{N_S} is a thermal state (5.118) such that $\text{Tr}\{\hat{O}\theta^{N_S}\} = N_S$ and $g(y) := (y+1)\log_2(y+1) - y\log_2 y$.

Proof. From a straightforward extension of Theorem 5.2, which takes into account the energy constraint, we find that

$$\mathcal{C}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S) \leq \sup_{\{p_X(x),\rho_{RB'}^x\}\ :\ \mathbb{E}_X\{\text{Tr}\{\hat{O}\rho_{B'}^X\}\}\leq N_S} I(X;B|R)_\omega - I(X;B'|R)_\rho \tag{5.88}$$

$$\leq \sup_{\{p_X(x),\rho_{RB'}^x\}\ :\ \mathbb{E}_X\{\text{Tr}\{\hat{O}\rho_{B'}^X\}\}\leq N_S} I(X;B|R)_\rho \tag{5.89}$$

$$\leq \sup_{\{p_X(x),\rho_{RB'}^x\}\ :\ \mathbb{E}_X\{\text{Tr}\{\hat{O}\rho_{B'}^X\}\}\leq N_S} 2S(B)_\rho \tag{5.90}$$

$$\leq 2S(\theta^{N_S}) \tag{5.91}$$

$$= 2g(N_S). \tag{5.92}$$

The first inequality follows from the extension of Theorem 5.2. The second inequality follows from non-negativity of the conditional quantum mutual information. The third inequality follows from a standard entropy bound for the conditional quantum mutual information. The fourth inequality

follows because the thermal state of mean energy N_S has the maximum entropy under a fixed energy constraint (see, e.g., [234]). The final equality follows because the observable $\hat{O}$ is the familiar $a^\dagger a$ number observable, for which the entropy of its thermal state of mean photon number N_S is given by $g(N_S)$. ∎

Remark 5.5 *It follows that* $\mathcal{C}_{\text{non-adaptive}}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S) \leq 2g(N_S)$ *because* $\mathcal{C}_{\text{non-adaptive}}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S) \leq \mathcal{C}(\mathscr{B}_{\mathscr{X}}, \hat{O}, N_S)$ *by the definition of the energy-constrained quantum reading capacity of a memory cell* $\mathscr{B}_{\mathscr{X}}$.

5.4 Examples of environment-parametrized memory cells

In this section, we calculate the quantum reading capacities of several environment-parametrized memory cells, including a thermal memory cell, and a jointly covariant memory cell formed from a channel $\mathcal{N}$ and a group $\mathscr{G}$ with respect to which $\mathcal{N}$ is covariant (Definition 5.3). Examples of such a jointly covariant memory cell include qudit erasure and depolarizing memory cells formed respectively from erasure and depolarizing channels.

5.4.1 Jointly covariant memory cell: $\mathscr{N}_{\mathscr{G}}^{\text{cov}}$

Now we show that the quantum reading capacity of a memory cell $\mathscr{N}_{\mathscr{G}}^{\text{cov}}$ (see Definition 5.7 below) is equal to the entanglement-assisted classical capacity of the underlying channel $\mathcal{N}$. This result makes use of the fact that the entanglement-assisted classical capacity of a covariant channel $\mathcal{T}$ is equal to $I(R;B)_{\mathcal{T}(\Phi)}$ [210, 235]. Furthermore, we use this result to evaluate the quantum reading capacity of a qudit erasure memory cell (Definition 5.8) and a qudit depolarizing memory cell (Definition 5.9).

Definition 5.7 ($\mathscr{N}_{\mathscr{G}}^{\text{cov}}$) *Let* $\mathcal{N}$ *be a covariant channel (Definition 2.1) with respect to a group* $\mathscr{G}$. *The memory cell* $\mathscr{N}_{\mathscr{G}}^{\text{cov}}$ *is defined as*

$$\mathscr{N}_{\mathscr{G}}^{\text{cov}} = \{\mathcal{N}_{B' \to B} \circ \mathcal{U}_{B'}^g\}_{g \in \mathscr{G}}, \tag{5.93}$$

where $\mathcal{U}^g_{B'} := U_{B'}(g)(\cdot)U^\dagger_{B'}(g)$. It follows from (2.33) that

$$\mathcal{N}_{B'\to B} \circ \mathcal{U}^g_{B'} = \mathcal{V}^g_B \circ \mathcal{N}_{B'\to B}, \tag{5.94}$$

where $\mathcal{V}^g_B := V_B(g)(\cdot)V^\dagger_B(g)$. It also follows that $\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}}$ is a jointly covariant memory cell.

Theorem 5.3 *The quantum reading capacity $\mathcal{C}(\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}})$ of the jointly covariant memory cell $\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}} = \{\mathcal{N}_{B'\to B} \circ \mathcal{U}^g_{B'}\}_{g\in\mathscr{G}}$ (Definition 5.7), is equal to the entanglement-assisted classical capacity of $\mathcal{N}$:*

$$\mathcal{C}(\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}}) = I(R;B)_{\mathcal{N}(\Phi)}, \tag{5.95}$$

where $\mathcal{N}(\Phi) := \mathcal{N}_{B'\to B}(\Phi_{RB'})$ is the Choi state of the underlying channel $\mathcal{N}$.

Proof. Proof here consists of two parts: the converse part and the achievability part. We first show the converse part:

$$\mathcal{C}\left(\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}}\right) \leq I(R;B)_{\mathcal{N}(\Phi)}. \tag{5.96}$$

From Remark 5.3, we can conclude that the quantum reading capacity of $\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}}$ is as follows:

$$\mathcal{C}\left(\mathscr{N}^{\mathrm{cov}}_{\mathscr{G}}\right) = \max_{p_G} I(G;RB)_\omega, \tag{5.97}$$

where

$$\omega_{GRB} := \sum_{g\in\mathscr{G}} p_G(g)\, |g\rangle\langle g|_G \otimes \omega^g_{RB}, \tag{5.98}$$

such that $\{|g\rangle\}_{g\in\mathscr{G}} \in \mathrm{ONB}(\mathcal{H}_G)$ and

$$\forall g \in \mathscr{G} : \ \omega^g_{RB} = (\mathcal{N}_{B'\to B} \circ \mathcal{U}^g_{B'})(\Phi_{RB'}). \tag{5.99}$$

Let us consider p_G to be fixed. Then

$$I(G; RB)_\omega = S\left(\sum_{g \in \mathscr{G}} p_G(g)\omega_{RB}^g\right) - \sum_{g \in \mathscr{G}} p_G(g)S(\omega_{RB}^g) \tag{5.100}$$

$$= S\left(\sum_{g \in \mathscr{G}} p_G(g)(\mathcal{V}_B^g \circ \mathcal{N}_{B' \to B})(\Phi_{RB'})\right) - \sum_{g \in \mathscr{G}} p_G(g)H((\mathcal{V}_B^g \circ \mathcal{N}_{B' \to B})(\Phi_{RB'})) \tag{5.101}$$

$$= \sum_{g' \in \mathscr{G}} \frac{1}{|G|} S\left(\sum_{g \in \mathscr{G}} p_G(g)(\mathcal{V}_B^{g'} \circ \mathcal{V}_B^g \circ \mathcal{N}_{B' \to B})(\Phi_{RB'})\right) - S(\mathcal{N}_{B' \to B}(\Phi_{RB'})) \tag{5.102}$$

$$\leq S\left(\frac{1}{|G|} \sum_{g,g' \in \mathscr{G}} p_G(g)(\mathcal{V}_B^{g'} \circ \mathcal{V}_B^g \circ \mathcal{N}_{B' \to B})(\Phi_{RB'})\right) - S(\mathcal{N}_{B' \to B}(\Phi_{RB'})) \tag{5.103}$$

$$= S\left(\mathcal{N}_{B' \to B}\left(\frac{1}{|G|} \sum_{g' \in \mathscr{G}} \mathcal{U}_{B'}^{g'}\left(\sum_{g \in \mathscr{G}} p_G(g)\mathcal{U}_{B'}^g(\Phi_{RB'})\right)\right)\right) - S(\mathcal{N}_{B' \to B}(\Phi_{RB'})) \tag{5.104}$$

$$= S\left(\mathcal{N}_{B' \to B}(\pi_R \otimes \pi_{B'})\right) - S(\mathcal{N}_{B' \to B}(\Phi_{RB'})) \tag{5.105}$$

$$= S\left(\pi_R\right) + S\left(\mathcal{N}_{B' \to B}(\pi_B)\right) - S(\mathcal{N}_{B' \to B}(\Phi_{RB'})) \tag{5.106}$$

$$= I(R; B)_{\mathcal{N}(\Phi)}. \tag{5.107}$$

The second equality follows from (5.94). The third equality follows because entropy is invariant with respect to unitary or isometric channels. The first inequality follows from the concavity of entropy. The fourth equality follows from (5.94). The fifth equality follows from Definition 2.1. The sixth equality follows because entropy is additive for product states. Since the above upper bound holds for any p_G, it follows that

$$\mathcal{C}\left(\mathscr{N}_{\mathscr{G}}^{\text{cov}}\right) = \max_{p_G} I(G; RB)_\omega \leq I(R; B)_{\mathcal{N}(\Phi)}. \tag{5.108}$$

To prove the achievability part, we take p_G to be a uniform distribution, i.e., $p_G \sim \frac{1}{|G|}$. Putting $p_G \sim \frac{1}{|G|}$ in (5.101), we obtain the following lower bound

$$\mathcal{C}\left(\mathscr{N}_{\mathscr{G}}^{\text{cov}}\right) \geq I(G; RB)_\omega = I(R; B)_{\mathcal{N}(\Phi)}. \tag{5.109}$$

Thus, from (5.108) and (5.109), we conclude the statement of the theorem: $\mathcal{C}\left(\mathscr{N}_{\mathscr{G}}^{\text{cov}}\right) = I(R; B)_{\mathcal{N}(\Phi)}$.

∎

Now we state two corollaries, which are direct consequences of the above theorem. These corollaries establish the quantum reading capacities for jointly covariant memory cells formed from the erasure channel and depolarizing channel with respect to the Heisenberg–Weyl group $\mathbf{H}$, as discussed below (see Appendix A for some basic notations and definitions related to qudit systems).

Definition 5.8 (Qudit erasure memory cell) *The qudit erasure memory cell $\mathscr{Q}_{\mathscr{X}}^q = \{\mathcal{Q}_{B' \to B}^{q,x}\}_{x \in \mathscr{X}}$, where the size of $\mathscr{X}$ is $|X| = d^2$, consists of the following qudit channels:*

$$\mathcal{Q}^{q,x}(\cdot) = \mathcal{Q}^q(\sigma^x(\cdot)(\sigma^x)^\dagger), \tag{5.110}$$

where $\mathcal{Q}^q$ is a qudit erasure channel [236]:

$$\mathcal{Q}^q(\rho_{B'}) = (1 - q)\rho + q\,|e\rangle\langle e| \tag{5.111}$$

such that $q \in [0, 1]$, $\dim(\mathcal{H}_{B'}) = d$, $|e\rangle\langle e|$ is an erasure state orthogonal to the support of all possible input states ρ, and $\forall x \in \mathscr{X} : \sigma^x \in \mathbf{H}$ are the Heisenberg–Weyl operators as given in (A.7). Observe that $\mathscr{Q}_{\mathscr{X}}^q$ is jointly covariant with respect to the Heisenberg–Weyl group $\mathbf{H}$ because the qudit erasure channel $\mathcal{Q}^q$ is covariant with respect to $\mathbf{H}$.

Definition 5.9 (Qudit depolarizing memory cell) *The qudit depolarizing memory cell $\mathscr{D}_{\mathscr{X}}^q = \{\mathcal{D}_{B' \to B}^{q,x}\}_{x \in \mathscr{X}}$, where $\mathscr{X}$ is of size $|\mathcal{X}| = d^2$, consists of qudit channels*

$$\mathcal{D}^{q,x}(\cdot) = \mathcal{D}^q\left(\sigma^x(\cdot)(\sigma^x)^\dagger\right) \tag{5.112}$$

where $\mathcal{D}^q$ is a qudit depolarizing channel:

$$\mathcal{D}^q(\rho) = (1 - q)\rho + q\pi, \tag{5.113}$$

where $q \in \left[0, \frac{d^2}{d^2-1}\right]$, $\dim(\mathcal{H}_{B'}) = d$ and $\forall x \in \mathscr{X} : \sigma^x \in \mathbf{H}$ are the Heisenberg–Weyl operators as given in (A.7). Observe that $\mathscr{D}_{\mathscr{X}}^q$ is jointly covariant with respect to the Heisenberg–Weyl group $\mathbf{H}$ because the qudit depolarizing channel $\mathcal{D}^q$ is covariant with respect to $\mathbf{H}$.

As a consequence of Theorem 5.3, one immediately finds the quantum reading capacities of the above memory cells:

Corollary 5.4 *The quantum reading capacity $\mathcal{C}(\mathscr{Q}_{\mathscr{X}}^q)$ of the qudit erasure memory cell $\mathscr{Q}_{\mathscr{X}}^q$ (Definition 5.8) is equal to the entanglement-assisted classical capacity of the erasure channel $\mathcal{Q}^q$ [210]:*

$$\mathcal{C}(\mathscr{Q}_{\mathscr{X}}^q) = 2(1-q)\log_2 d. \tag{5.114}$$

Corollary 5.5 *The quantum reading capacity $\mathcal{C}(\mathscr{D}_{\mathscr{X}}^q)$ of the qudit depolarizing memory cell $\mathscr{D}_{\mathscr{X}}^q$ (Definition 5.9) is equal to the entanglement-assisted classical capacity of the depolarizing channel $\mathcal{D}^q$ [210]:*

$$\mathcal{C}(\mathscr{D}_{\mathscr{X}}^q) = 2\log_2 d + \left(1 - q + \frac{q}{d^2}\right)\log_2\left(1 - q + \frac{q}{d^2}\right) + (d^2 - 1)\frac{q}{d^2}\log_2\left(\frac{q}{d^2}\right). \tag{5.115}$$

5.4.2 A thermal memory cell

Now we discuss an example of a thermal memory cell $\hat{\mathscr{E}}_{\mathscr{X},\eta} = \{\mathcal{E}^{x,\eta}\}_x$, which is an environment-parametrized memory cell consisting of thermal channels $\mathcal{E}^{x,\eta}$ with known transmissivity parameter $\eta \in [0, 1]$ and unknown excess noise x. Let $\hat{a}, \hat{b}, \hat{e}, \hat{e}'$ be the respective field-mode annihilation operators for Bob's input, Bob's output, the environment's input, and the environment's output of these channels. The interaction channel in this case is a fixed bipartite unitary $U_{B'E \to BE'}$ corresponding to a beamsplitter interaction, defined from the following Heisenberg input-output relations:

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}, \tag{5.116}$$

$$\hat{e}' = -\sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{e}. \tag{5.117}$$

The environmental mode $\hat{e}$ of a thermal channel $\mathcal{E}^{x,\eta}$ is prepared in a thermal state $\theta^x := \theta(N_B = x)$ of mean photon number $N_B \geq 0$:

$$\theta(N_B) := \frac{1}{N_B + 1}\sum_{k=0}^{\infty}\left(\frac{N_B}{N_B + 1}\right)^k |k\rangle\langle k|, \tag{5.118}$$

131

where $\{|k\rangle\}_{k\in\mathbb{N}}$ is the orthonormal, photonic number-state basis. Parameter x is the excess noise of the thermal channel $\mathcal{E}^{x,\eta}$. Note that for $x = 0$, θ^x reduces to a vacuum state and the channel $\mathcal{E}^{x,\eta}$ is called the pure-loss channel (see Section 4.3.1).

Proposition 5.6 *The quantum reading capacity* $C(\hat{\mathscr{E}}_{\mathscr{X},\eta})$ *of the thermal memory cell* $\hat{\mathscr{E}}_{\mathscr{X},\eta} = \{\mathcal{E}^{x,\eta}\}_x$ *(as described above) is equal to*

$$C(\hat{\mathscr{E}}_{\mathscr{X},\eta}) = \max_{p_X} \left[S(\overline{\theta}) - \int dx\ p_X(x) S(\theta^x) \right], \tag{5.119}$$

where p_X *is a probability distribution for the parameter* x *and* $\overline{\theta} := \int dx\ p_X(x)\theta^x$.

Proof. We begin by proving the achievability part, which corresponds to the inequality

$$C(\hat{\mathscr{E}}_{\mathscr{X},\eta}) \geq I(X;E)_\theta, \tag{5.120}$$

where $\theta_{XE} := \int dx\ p_X(x)\ |x\rangle\langle x|_X \otimes \theta^x_E$. The main idea for the achievability part builds on the results of [230, Eqns. (38)–(48)].

The two-mode squeezed vacuum state is equivalent to a purification of the thermal state in (5.118) and is defined as

$$\left|\phi^{\text{TMS}}(N_S)\right\rangle_{RB'} := \frac{1}{\sqrt{N_S+1}} \sum_{k=0}^{\infty} \left[\frac{N_S}{N_S+1}\right]^{\frac{k}{2}} |k\rangle_R |k\rangle_{B'}. \tag{5.121}$$

When sending the B' system of this state through the channel $\mathcal{E}^{x,\eta}_{B'\to B}$, the output state is as follows:

$$\omega^{x,\eta}_{RB}(N_S) := (\text{id}_R \otimes \mathcal{E}^{x,\eta}_{B'\to B})\left(\phi^{\text{TMS}}_{RB'}(N_S)\right) \tag{5.122}$$

$$= \text{Tr}_{E'}\left\{U_{B'E\to BE'}\left(\phi_{RB'}(N_S) \otimes \theta^x_E\right)(U_{B'E\to BE'})^\dagger\right\}, \tag{5.123}$$

and the average output state is as follows, when the channel $\mathcal{E}^{x,\eta}_{B'\to B}$ being applied is chosen with

probability $p_X(x)$:

$$\sum_{x \in \mathscr{X}} p_X(x) \omega_{RB}^{x,\eta}(N_S) = \sum_{x \in \mathscr{X}} p_X(x) \operatorname{Tr}_{E'} \left\{ U_{B'E \to BE'} \left(\phi_{RB'}(N_S) \otimes \theta_E^x \right) (U_{B'E \to BE'})^\dagger \right\} \quad (5.124)$$

$$= \operatorname{Tr}_{E'} \left\{ U_{B'E \to BE'} \left(\phi_{RB'}(N_S) \otimes \sum_{x \in \mathscr{X}} p_X(x) \theta_E^x \right) (U_{B'E \to BE'})^\dagger \right\}. \quad (5.125)$$

Consider the following classical–quantum state:

$$\omega_{XRB}^\eta(N_S) := \sum_{x \in \mathscr{X}} p_X(x) |x\rangle\langle x|_X \otimes \omega_{RB}^{x,\eta}, \quad (5.126)$$

and

$$I(X; RB)_{\omega^\eta(N_S)} = \sum_{x \in \mathscr{X}} p_X(x) D \left(\omega_{RB}^{x,\eta}(N_S) \middle\| \sum_{x \in \mathscr{X}} p_X(x) \omega_{RB}^{x,\eta}(N_S) \right). \quad (5.127)$$

The Wigner characteristic function covariance matrix [237] for $\omega_{RB}^{x,\eta}(N_S)$ in (5.122) is as follows:

$$V_{\omega^{x,\eta}(N_S)} = \begin{bmatrix} a & c & 0 & 0 \\ c & b & 0 & 0 \\ 0 & 0 & a & -c \\ 0 & 0 & -c & b \end{bmatrix}, \quad (5.128)$$

where

$$a = \eta N_S + (1 - \eta) x + \frac{1}{2}, \quad b = N_S + \frac{1}{2}, \quad c = \sqrt{\eta N_S(N_S + 1)}. \quad (5.129)$$

Now consider the following symplectic transformation [230]:

$$S^\eta(N_S) = \begin{bmatrix} \gamma_+ & -\gamma_- & 0 & 0 \\ -\gamma_- & \gamma_+ & 0 & 0 \\ 0 & 0 & \gamma_+ & \gamma_- \\ 0 & 0 & \gamma_- & \gamma_+ \end{bmatrix}, \quad (5.130)$$

133

where

$$\gamma_+ = \sqrt{\frac{1 + N_S}{1 + (1 - \eta)N_S}}, \qquad \gamma_- = \sqrt{\frac{\eta N_S}{1 + (1 - \eta)N_S}} \ . \tag{5.131}$$

Action of the symplectic matrix $S^\eta(N_S)$ on the covariance matrix $V_{\omega^{x,\eta}(N_S)}$ gives

$$\hat{V}_{\omega^{x,\eta}(N_S)} := S^\eta(N_S)V_{\omega^{x,\eta}(N_S)}\left(S^\eta(N_S)\right)^{\mathrm{T}} = \begin{bmatrix} a_s & -c_s & 0 & 0 \\ -c_s & b_s & 0 & 0 \\ 0 & 0 & a_s & c_s \\ 0 & 0 & c_s & b_s \end{bmatrix}, \tag{5.132}$$

where

$$a_s = x + \frac{1}{2} + \mathcal{O}\left(\frac{1}{N_S}\right), \tag{5.133}$$

$$b_s = (1 - \eta)\,N_S + \eta x + \frac{1}{2} + \mathcal{O}\left(\frac{1}{N_S}\right), \tag{5.134}$$

$$c_s = \sqrt{\eta}x + \mathcal{O}\left(\frac{1}{N_S}\right) \ . \tag{5.135}$$

Thus, by applying this transformation to $\omega^{x,\eta}(N_S)$ and tracing out the second mode, we are left with a state that becomes indistinguishable from a thermal state of mean photon number x in the limit as $N_S \to \infty$. Note that this occurs independent of the value of the transmissivity η.

The symplectic transformation $S^\eta(N_S)$ can be realized by a two-mode squeezer, which corresponds to a unitary transformation acting on the tensor-product Hilbert space. Letting the unitary transformation be of the form $W_{RB \to EB}$, then $\hat{V}_{\omega^{x,\eta}(N_S)}$ represents the covariance matrix of the state $\omega_{EB}^{x,\eta}(N_S)$.

We use the formula for fidelity between two thermal states [230, Equation 34] and the relation between trace norm and fidelity [23, Theorem 9.3.1] to conclude that

$$\lim_{N_S \to \infty} \|\omega_E^{x,\eta}(N_S) - \theta_E^x\|_1 \le \lim_{N_S \to \infty} \sqrt{1 - F\left(\omega_E^x(N_S), \theta_E^x\right)} = 0. \tag{5.136}$$

From the convexity of trace norm, we obtain

$$\left\| \sum_{x \in \mathscr{X}} p_X(x) \omega_E^x(N_S) - \sum_{x \in \mathscr{X}} p_X(x) \theta_E^x \right\|_1 \leq \sum_{x \in \mathscr{X}} p_X(x) \left\| \omega_E^x(N_S) - \theta_E^x \right\|_1, \tag{5.137}$$

which in turn implies that

$$\lim_{N_S \to \infty} \left\| \sum_{x \in \mathscr{X}} p_X(x) \omega_E^x(N_S) - \sum_{x \in \mathscr{X}} p_X(x) \theta_E^x \right\|_1 = 0. \tag{5.138}$$

Invoking the result of [230, Equation 28] and the lower semi-continuity of relative entropy, one gets

$$\lim_{N_S \to \infty} D\left(\omega_{RB}^{x,\eta}(N_S) \,\middle\|\, \sum_{x \in \mathscr{X}} p_X(x) \omega_{RB}^{x,\eta}(N_S) \right) = D\left(\theta_E^x \,\middle\|\, \sum_{x \in \mathscr{X}} p_X(x) \theta_E^x \right). \tag{5.139}$$

Thus, from the above relations, we obtain the following result

$$\lim_{N_S \to \infty} I(X; RB)_{\omega^\eta(N_S)} = I(X; E)_\theta, \tag{5.140}$$

where

$$\theta_{XE} = \sum_{x \in \mathscr{X}} p_X(x) \, |x\rangle\langle x|_X \otimes \theta_E^x, \tag{5.141}$$

for θ_E^x defined in (5.123). This shows that $I(X; E)_\theta$ is an achievable rate for any p_X.

The converse part of the proof, which corresponds to the inequality

$$\mathcal{C}(\hat{\mathscr{E}}_{\mathcal{X},\eta}) \leq \max_{p_X} I(X; E)_\theta, \tag{5.142}$$

follows directly from Theorem 5.1. ∎

5.5 Zero-error quantum reading capacity

In an (n, R, ε) quantum reading protocol (Definition 5.4) for a memory cell $\mathscr{S}_{\mathscr{X}} = \{\mathcal{M}_{B' \to B}^x\}_{x \in \mathscr{X}}$, one can demand the error probability to vanish, i.e., $\varepsilon = 0$. In this section, we define zero-error quantum reading protocols and the zero-error quantum reading capacity for any memory cell. We provide an explicit example of a memory cell for which a quantum reading protocol using an adaptive strategy has a clear advantage over a quantum reading protocol that uses a non-adaptive strategy.

Definition 5.10 (Zero-error quantum reading protocol) *A zero-error quantum reading protocol of a memory cell $\mathscr{S}_{\mathscr{X}}$ is a particular (n, R, ε) quantum reading protocol for which $\varepsilon = 0$.*

Definition 5.11 (Zero-error quantum reading capacity) *The zero-error quantum reading capacity $\mathcal{Z}(\mathscr{S}_{\mathscr{X}})$ of a memory cell $\mathscr{S}_{\mathscr{X}}$ is defined as the largest rate R such that there exists a zero-error reading protocol.*

A zero-error non-adaptive quantum reading protocol of a memory cell is a special case of a zero-error quantum reading protocol in which the reader uses a non-adaptive strategy to decode the message.

5.5.1 Advantage of an adaptive strategy over a non-adaptive strategy

Now we employ the main example from [224] to illustrate the advantage of an adaptive zero-error quantum reading protocol over a non-adaptive zero-error quantum reading protocol.

Let us consider a memory cell $\mathscr{B}_{\mathscr{X}} = \{\mathcal{M}^x_{B' \to B}\}_{x \in \mathscr{X}}$, $\mathscr{X} = \{1, 2\}$, consisting of the following quantum channels that map two qubits to a single qubit, acting as

$$\mathcal{M}^x(\cdot) = \sum_{j=1}^{5} A_j^x (\cdot) \left(A_j^x\right)^\dagger, \; x \in \mathscr{X}, \tag{5.143}$$

where

$$A_1^1 = |0\rangle\langle 00|, \; A_2^1 = |0\rangle\langle 01|, \quad A_3^1 = |0\rangle\langle 10|, \quad A_4^1 = \frac{1}{\sqrt{2}}|0\rangle\langle 11|, \qquad A_5^1 = \frac{1}{\sqrt{2}}|1\rangle\langle 11|,$$

$$A_1^2 = |+\rangle\langle 00|, \; A_2^2 = |+\rangle\langle 01|, \; A_3^2 = |1\rangle\langle 1+|, \quad A_4^2 = \frac{1}{\sqrt{2}}|0\rangle\langle 1-|, \; A_5^2 = \frac{1}{\sqrt{2}}|1\rangle\langle 1-|, \tag{5.144}$$

and the standard bases for the channel inputs and outputs are $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and $\{|0\rangle, |1\rangle\}$, respectively.

It follows from [222, 224] that it is possible to discriminate perfectly these two channels using an adaptive strategy that makes two calls to the unknown channel $\mathcal{M}^x$. This implies that the encoder can encode two classical messages (one bit) into two uses of the quantum channels from $\mathscr{B}_{\mathscr{X}}$ such that Bob can perfectly read the message, i.e., with zero error. Thus, it can be concluded that the

zero-error quantum reading capacity of $\mathscr{B}_{\mathscr{X}}$ is bounded from below by $\frac{1}{2}$ (one bit per two channel uses).

Closely following the arguments of [224, Section 4], we can show that non-adaptive strategies can never realize perfect discrimination of the sequences $\mathcal{M}^{x^n}_{B'^n \to B^n}$ and $\mathcal{M}^{y^n}_{B'^n \to B^n}$, for any finite number n of channel uses if $x^n \neq y^n$. Equivalently,

$$\text{for } x^n \neq y^n : \|\mathcal{M}^{x^n}_{B'^n \to B^n} - \mathcal{M}^{y^n}_{B'^n \to B^n}\|_\diamond < 2 \ \forall n \in \mathbb{N} \tag{5.145}$$

where $\|\cdot\|_\diamond$ is the diamond norm (4.110). Thus, the zero-error non-adaptive quantum reading capacity of $\mathscr{B}_{\mathscr{X}}$ is equal to zero.

To prove the above claim, we proceed with a proof by contradiction along the lines of that given in [224, Section 4]. We need to show that: for any finite $n \in \mathbb{N}$, if $x^n \neq y^n$, then there does not exist any state $\sigma_{RB'^n}$ such that the two sequences $\mathcal{M}^{x^n}_{B'^n \to B^n}$ and $\mathcal{M}^{y^n}_{B'^n \to B^n}$ can be perfectly discriminated. Note that perfect discrimination is possible if and only if

$$\text{Tr}\left\{ \left(\text{id}_R \otimes \mathcal{M}^{x^n}_{B'^n \to B^n}\right)(\sigma_{RB'^n}) \left(\text{id}_R \otimes \mathcal{M}^{y^n}_{B'^n \to B^n}\right)(\sigma_{RB'^n}) \right\} = 0. \tag{5.146}$$

Now assume that there exists a $\sigma_{RB'^n}$ such that (5.146) holds. Convexity then implies that (5.146) holds for some pure state $\psi_{RB'^n}$. Then, by carefully following the steps from [224, Section 4], (5.146) implies that for any set of complex coefficients $\{\alpha^{x,y}_{j,k} \in \mathbb{C} : 1 \leq j, k \leq 5, \ x, y \in \mathscr{X}\}$

$$\langle\psi|_{RB'^n} \left[\mathbb{1}_R \otimes \sum_{1 \leq j,k \leq 5 \,:\, i \in [n]} \alpha^{x_1,y_1}_{j_1,k_1} \cdots \alpha^{x_n,y_n}_{j_n,k_n} \left(B'^{y_1}_{j_1}\right)^\dagger B'^{x_1}_{k_1} \otimes \cdots \otimes \left(B'^{y_n}_{j_n}\right)^\dagger B'^{x_n}_{k_n} \right] |\psi\rangle_{RB'^n} = 0. \tag{5.147}$$

Let us choose the coefficients $\{\alpha^{x,y}_{j,k} \in \mathbb{C} : 1 \leq j, k \leq 5, \ x, y \in \mathscr{X}\}$ as follows:

$$\begin{cases} \text{for } x \neq y: \quad \alpha^{x,y}_{1,1} = \alpha^{x,y}_{2,2} = \sqrt{2}, \ \alpha^{x,y}_{3,5} = \alpha^{x,y}_{4,3} = 1, \ \alpha^{x,y}_{4,4} = -2\sqrt{2}, \text{ otherwise } \alpha^{x,y}_{j,k} = 0, \\ \text{for } x = y: \qquad\qquad\qquad\qquad\quad \alpha^{x,y}_{j,k} = \delta_{j,k} \end{cases} \tag{5.148}$$

where, if $j = k$ then $\delta_{j,k} = 1$, else $\delta_{j,k} = 0$.

For the above choice of the coefficients, it follows that

$$\mathbb{1}_R \otimes \sum_{1 \leq j,k \leq 5 \,:\, i \in [n]} \alpha_{j_1,k_1}^{x_1,y_1} \cdots \alpha_{j_n,k_n}^{x_n,y_n} \left(A_{j_1}^{y_1}\right)^\dagger A_{k_1}^{x_1} \otimes \cdots \otimes \left(A_{j_n}^{y_n}\right)^\dagger A_{k_n}^{x_n} = I_R \otimes P^{x_1,y_1} \otimes \cdots \otimes P^{x_n,y_n}$$

where

$$\text{for } i \in [n] : \quad P^{x_i,y_i} = \begin{cases} P > 0, & x_i \neq y_i \\ I > 0, & \text{otherwise,} \end{cases}$$

and $P = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 11| + |1-\rangle\langle 1-|$. Observe that the operator $\mathbb{1}_R \otimes P^{x_1,y_1} \otimes \cdots \otimes P^{x_n,y_n}$ is positive definite. This means that there cannot exist any state that satisfies (5.147), and as a consequence (5.146), and this concludes the proof.

From the above discussion, we can conclude that the zero-error quantum reading capacity of the memory cell $\mathscr{B}_{\mathscr{X}}$ is bounded from below by $\frac{1}{2}$ whereas the zero-error non-adaptive quantum reading capacity is equal to zero.

5.6 Conclusion

In this chapter, we have introduced the most general and natural definitions for quantum reading protocols and quantum reading capacities. We have defined environment-parametrized memory cells for quantum reading, which are sets of quantum channels obeying certain symmetries. We have determined upper bounds on the quantum reading capacity and the non-adaptive quantum reading capacity of an arbitrary memory cell. We have also derived strong converse and second-order bounds on quantum reading capacities of environment-parametrized memory cells. We have calculated quantum reading capacities for a thermal memory cell, a qudit erasure memory cell, and a qudit depolarizing memory cell. Finally, we have shown the advantage of an adaptive strategy over a non-adaptive strategy in the context of zero-error quantum reading capacity of a memory cell.

We note that it is possible to use the methods developed here to obtain bounds on the quantum reading capacities of memory cells based on amplifying bosonic channels, in the same spirit as the results of a thermal memory cell (the argument follows from [230]).

A natural question following from the developments in this chapter is whether there exists a memory cell for which the quantum reading capacity is larger than what we could achieve by using

a non-adaptive strategy. As discussed above, we have found a positive answer to this question in the setting of zero error. However, the question remains open for the case of Shannon-theoretic capacity (i.e., with arbitrarily small error). We may suspect that this question will have a positive answer, and we may strongly suspect it will be the case in the setting of non-asymptotic capacity, our latter suspicion being due to the fact that feedback is known to help in non-asymptotic settings for communication (see, e.g., [238]). We leave the investigation of this question for future work.

Chapter 6   Private Reading of Memory Devices

Devising a communication or information processing protocol that is secure against an eavesdropper is an area of primary interest and concern in information science and technology. In this chapter, we introduce the task of private reading of information stored in a memory device. A secret message can either be encrypted in a computer program with circuit gates [109] or in a physical storage device [212], such as a CD-ROM, DVD, etc. Here we limit the discussion to the case in which these computer programs or physical storage devices are used for read-only tasks; for simplicity, we refer to such media as memory devices.

In a reading protocol (see Chapter 5 for precise description), it is assumed that the reader has a description of a memory cell, which is a set of quantum channels. The memory cell is used to encode a classical message in a memory device. The memory device containing the encoded message is then delivered to the interested reader, whose task is to read out the message stored in it. To decode the message, the reader can transmit a quantum state to the memory device and perform a quantum measurement on the output state. In general, since quantum channels are noisy, there is a loss of information to the environment, and there is a limitation on how well information can be read out from the memory device.

To motivate the task of private reading, consider that the computational and information processing capability of an adversary is limited only by the laws of quantum theory. A memory device is to be read using computer. There could be a circumstance in which an individual (reader) would have to access a computer in a public library under the surveillance of a librarian or other adversarial party, who supposedly is a passive eavesdropper, Eve. At a fundamental level, any reading mechanism involves transmitting of a probe system through a sequence of quantum channels, which are noisy in general. In such a situation, the reader would want information in a memory device not to be leaked to Eve, who has complete access to the environment, for security and privacy reasons. This naturally gives rise to the question of whether there exists a protocol for reading out a classical message that is secure from a passive eavesdropper.

Most of this chapter is based on [31], a joint work with Stefan Bäuml and Mark M. Wilde.

In what follows, we introduce the details of private reading [31]: briefly, it is the task of reading out a classical message (key) stored in a memory device, encoded with a memory cell, by the reader such that the message is not leaked to Eve. We note here that private reading can be understood as a particular kind of secret-key-agreement protocol that employs a particular kind of bipartite interaction, and thus, there is a strong link between the developments in Section 3.3 and what follows. In Section 6.1, we present formal description of a private reading protocol, whose goal is to generate a secret key between an encoder and a reader. In Section 6.2, we present purified (coherent) version of the private reading protocol. In both of the aforementioned sections, we derive both lower and upper bounds on the private reading capacities. In Section 6.3, we discuss a protocol whose goal is to generate entanglement between two parties who have coherent access to a memory cell, and we derive a lower bound on the entanglement generation capacity in this setting.

6.1 Private reading protocol

In a private reading protocol, we consider an encoder and a reader (transceiver: receiver and decoder). Alice, an encoder, is one who encodes a secret classical message onto a read-only memory device that is delivered to Bob, a receiver, whose task is to read the message. Bob is also referred as the reader. The private reading task comprises the estimation of the secret message encoded in the form of a sequence of quantum wiretap channels chosen from a given set $\{\mathcal{M}^x_{B'\to BE}\}_{x\in\mathscr{X}}$ of quantum wiretap channels (called a *wiretap memory cell*), where $\mathscr{X}$ is an alphabet of finite size $|X|$, such that there is negligible leakage of information to Eve, who has access to the system E. A special case of this is when each wiretap channel $\mathcal{M}^x_{B'\to BE}$ is an isometric channel. In the most natural and general setting, the reader can use an adaptive strategy when decoding, as considered in the reading protocol described in Chapter 5.

Consider a set $\{\mathcal{M}^x_{B'\to BE}\}_{x\in\mathscr{X}}$ of wiretap quantum channels, where the size of B', B, and E are fixed and independent of x. The memory cell from the encoder Alice to the reader Bob is as follows: $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{M}^x_{B'\to B}\}_x$, where

$$\forall x \in \mathscr{X} : \ \mathcal{M}^x_{B'\to B}(\cdot) := \mathrm{Tr}_E\{\mathcal{M}^x_{B'\to BE}(\cdot)\}, \tag{6.1}$$

which may also be known to Eve, before executing the reading protocol. It is assumed that only

141

the systems E are accessible to Eve for all channels $\mathcal{M}^x$ in a memory cell. Thus, Eve is a passive

eavesdropper in the sense that all she can do is to access the output of the channels

$$\forall x \in \mathcal{X} : \ \mathcal{M}^x_{B' \to E}(\cdot) = \text{Tr}_B \left\{ \mathcal{M}^x_{B' \to BE}(\cdot) \right\}. \tag{6.2}$$

Consider a finite classical message set $\mathcal{K}$ of size $|K|$, and let K_A be an associated system

denoting a classical register for the secret message. In general, Alice encodes a message $k \in \mathcal{K}$

using a codeword $x^n(k) = x_1(k)x_2(k)\cdots x_n(k)$ of length n, where $x_i(k) \in \mathcal{X}$ for all $i \in [n]$. Each

codeword identifies with a corresponding sequence of quantum channels chosen from the wiretap

memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$:

$$\left(\mathcal{M}^{x_1(k)}_{B'_1 \to B_1 E_1}, \mathcal{M}^{x_2(k)}_{B'_2 \to B_2 E_2}, \ldots, \mathcal{M}^{x_n(k)}_{B'_n \to B_n E_n} \right). \tag{6.3}$$

Each quantum channel in a codeword, each of which represents one part of the stored information,
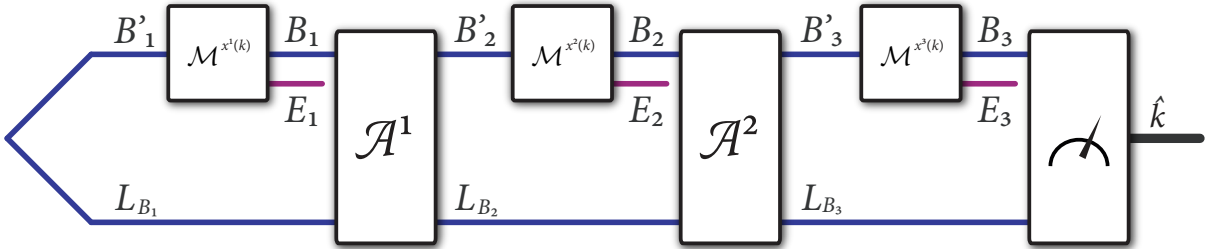
is only read once.

Figure 6.1. The figure depicts a private reading protocol that calls a memory cell three times to
decode the key k as $\hat{k}$. See the discussion in Section 6.1 for a detailed description of a private
reading protocol.

An adaptive decoding strategy makes n calls to the memory cell, as depicted in Figure 6.1.

It is specified in terms of a transmitter state $\rho_{L_{B_1} B'_1}$, a set of adaptive, interleaved channels

$\{\mathcal{A}^i_{L_{B_i} B_i \to L_{B_{i+1}} B'_{i+1}}\}_{i=1}^{n-1}$, and a final quantum measurement $\{\Lambda^{(\hat{k})}_{L_{B_n} B_n}\}_{\hat{k}}$ that outputs an estimate $\hat{k}$ of

the message k. The strategy begins with Bob preparing the input state $\rho_{L_{B_1} B'_1}$ and sending the B'_1

system into the channel $\mathcal{M}^{x_1(k)}_{B'_1 \to B_1 E_1}$. The channel outputs the system B_1 for Bob. He adjoins the

system B_1 to the system L_{B_1} and applies the channel $\mathcal{A}^1_{L_{B_1} B_1 \to L_{B_2} B'_2}$. The channel $\mathcal{A}^i_{L_{B_i} B_i \to L_{B_{i+1}} B'_{i+1}}$

is called adaptive because it can take an action conditioned on the information in the system B_i,

which itself might contain partial information about the message k. Then, he sends the system B_2' into the channel $\mathcal{M}_{B_2' \to B_2 E_2}^{x_2(k)}$, which outputs systems B_2 and E_2. The process of successively using the channels interleaved by the adaptive channels continues $n - 2$ more times, which results in the final output systems L_{B_n} and B_n with Bob. Next, he performs a measurement $\{\Lambda_{L_{B_n} B_n}^{(\hat{k})}\}_{\hat{k}}$ on the output state $\rho_{L_{B_n} B_n}$, and the measurement outputs an estimate $\hat{k}$ of the original message k. It is natural to assume that the outputs of the adaptive channels and their complementary channels are inaccessible to Eve and are instead held securely by Bob.

It is apparent that a non-adaptive strategy is a special case of an adaptive strategy. In a non-adaptive strategy, the reader does not perform any adaptive channels and instead uses $\rho_{L_B B'^n}$ as the transmitter state with each B_i' system passing through the corresponding channel $\mathcal{M}_{B_i' \to B_i E_i}^{x_i(k)}$ and L_B being a reference system. The final step in such a non-adaptive strategy is to perform a decoding measurement on the joint system $L_B B^n$.

As argued in the previous chapter, based on the physical setup of (quantum) reading, in which the reader assumes the role of both a transmitter and receiver, it is natural to consider the use of an adaptive strategy when defining the private reading capacity of a memory cell.

Definition 6.1 (Private reading protocol) *An $(n, P, \varepsilon, \delta)$ private reading protocol for a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is defined by an encoding map $\mathcal{K}_{\mathrm{enc}} \to \mathcal{X}^{\otimes n}$, an adaptive strategy with measurement $\{\Lambda_{L_{B_n} B_n}^{(\hat{k})}\}_{\hat{k}}$, such that, the average success probability is at least $1 - \varepsilon$ where $\varepsilon \in (0, 1)$:*

$$1 - \varepsilon \leq 1 - p_{\mathrm{err}} := \frac{1}{|K|} \sum_k \mathrm{Tr} \left\{ \Lambda_{L_{B_n} B_n}^{(k)} \rho_{L_{B_n} B_n}^{(k)} \right\}, \tag{6.4}$$

where

$$\rho_{L_{B_n} B_n E^n}^{(k)} = \left(\mathcal{M}_{B_n' \to B_n E_n}^{x_n(k)} \circ \mathcal{A}_{L_{B_{n-1}} B_{n-1} \to L_{B_n} B_n'}^{n-1} \circ \cdots \circ \mathcal{A}_{L_{B_1} B_1 \to L_{B_2} B_2'}^1 \circ \mathcal{M}_{B_1' \to B_1 E_1}^{x_1(k)} \right) \left(\rho_{L_{B_1} B_1'} \right). \tag{6.5}$$

Furthermore, the security condition is that

$$\frac{1}{|K|} \sum_{k \in \mathcal{K}} \frac{1}{2} \left\| \rho_{E^n}^{(k)} - \tau_{E^n} \right\|_1 \leq \delta, \tag{6.6}$$

where $\rho_{E^n}^{(k)}$ denotes the state accessible to the passive eavesdropper when message k is encoded. Also, τ_{E^n} is some fixed state. The rate $P := \frac{1}{n} \log_2 |K|$ of a given $(n, |K|, \varepsilon, \delta)$ private reading protocol is equal to the number of secret bits read per channel use.

Based on the discussions in [80, Appendix B], there are connections between the notions of private communication given in Section 3.3.2 and Definition 6.1, and we exploit these in what follows.

To arrive at a definition of the private reading capacity, we demand that there exists a sequence of private reading protocols, indexed by n, for which the error probability $p_{\mathrm{err}} \to 0$ and security parameter $\delta \to 0$ as $n \to \infty$ at a fixed rate P.

A rate P is called achievable if for all $\varepsilon, \delta \in (0, 1]$, $\delta' > 0$, and sufficiently large n, there exists an $(n, P - \delta', \varepsilon, \delta)$ private reading protocol. The private reading capacity $P^{\mathrm{read}}(\overline{\mathcal{M}}_{\mathscr{X}})$ of a wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$ is defined as the supremum of all achievable rates P.

An $(n, P, \varepsilon, \delta)$ private reading protocol for a wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$ is a non-adaptive private reading protocol when the reader abstains from employing any adaptive strategy for decoding. The non-adaptive private reading capacity $P_{\mathrm{n\text{-}a}}^{\mathrm{read}}(\overline{\mathcal{M}}_{\mathscr{X}})$ of a wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$ is defined as the supremum of all achievable rates P for a private reading protocol that is limited to non-adaptive strategies.

6.1.1 Non-adaptive private reading capacity

In what follows we restrict our attention to reading protocols that employ a non-adaptive strategy, and we now derive a regularized expression for the non-adaptive private reading capacity of a general wiretap memory cell.

Theorem 6.1 *The non-adaptive private reading capacity of a wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$ is given by*

$$P_{\mathrm{n\text{-}a}}^{\mathrm{read}}\left(\overline{\mathcal{M}}_{\mathscr{X}}\right) = \sup_n \max_{p_{X^n}, \sigma_{L_B B'^n}} \frac{1}{n} \left[I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau \right], \tag{6.7}$$

where

$$\tau_{X^n L_B B^n E^n} := \sum_{x^n} p_{X^n}(x^n) \, |x^n\rangle\langle x^n|_{X^n} \otimes \mathcal{M}_{B'^n \to B^n E^n}^{x^n}(\sigma_{L_B B'^n}), \tag{6.8}$$

and it suffices for $\sigma_{L_B B'^n}$ to be a pure state such that $L_B \simeq B'^n$.

Proof. Let us begin by defining a cq-state corresponding to the task of private reading. Consider a wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{M}^x_{B' \to BE}\}_{x \in \mathscr{X}}$. The initial state $\rho_{K_A L_B B'^n}$ of a non-adaptive private reading protocol takes the form

$$\rho_{K_A L_B B'^n} := \frac{1}{|K|} \sum_k |k\rangle\langle k|_{K_A} \otimes \rho_{L_B B'^n}. \tag{6.9}$$

Bob then passes the transmitter state $\rho_{L_B B'^n}$ through a channel codeword sequence $\mathcal{M}^{x^n(k)}_{B'^n \to B^n E^n} := \bigotimes_{i=1}^n \mathcal{M}^{x_i(k)}_{B'_i \to B_i E_i}$. Then the resulting state is

$$\rho_{K_A L_B B^n E^n} := \frac{1}{|K|} \sum_k |k\rangle\langle k|_{K_A} \otimes \mathcal{M}^{x^n(k)}_{B'^n \to B^n E^n} (\rho_{L_B B'^n}). \tag{6.10}$$

Let $\rho_{K_A K_B} := \mathcal{D}_{L_B B^n \to K_B} (\rho_{K_A L_B B^n})$ be the output state at the end of the protocol after the decoding channel $\mathcal{D}_{L_B B^n \to K_B}$ is performed by Bob. The privacy criterion (Definition 6.1) requires that

$$\frac{1}{|K|} \sum_{k \in \mathscr{K}} \frac{1}{2} \|\rho^{x^n(k)}_{E^n} - \tau_{E^n}\|_1 \le \delta, \tag{6.11}$$

where $\rho^{x^n(k)}_{E^n} := \mathrm{Tr}_{L_B B^n}\{\mathcal{M}^{x^n(k)}_{B'^n \to B^n E^n}(\rho_{L_B B'^n})\}$ and τ_{E^n} is some arbitrary constant state. Hence

$$\delta \ge \frac{1}{2} \sum_k \frac{1}{|K|} \|\rho^{x^n(k)}_{E^n} - \tau_{E^n}\|_1 \tag{6.12}$$

$$= \frac{1}{2} \|\rho_{K_A E^n} - \pi_{K_A} \otimes \tau_{E^n}\|_1, \tag{6.13}$$

where π_{K_A} denotes maximally mixed state, i.e., $\pi_{K_A} := \frac{1}{|K|} \sum_k |k\rangle\langle k|_{K_A}$. We note that

$$I(K_A; E^n)_\rho = S(K_A)_\rho - S(K_A|E^n)_\rho \tag{6.14}$$

$$= S(K_A|E^n)_{\pi \otimes \tau} - S(K_A|E^n)_\rho \tag{6.15}$$

$$\le \delta \log_2 |K| + g(\delta), \tag{6.16}$$

which follows from an application of Lemma 2.5.

We are now ready to derive a weak converse bound on the private reading rate:

$$\log_2 |K| = S(K_A)_\rho = I(K_A; K_B)_\rho + S(K_A|K_B)_\rho \tag{6.17}$$

$$\leq I(K_A; K_B)_\rho + \varepsilon \log_2 |K| + h_2(\varepsilon) \tag{6.18}$$

$$\leq I(K_A; L_B B^n)_\rho + \varepsilon \log_2 |K| + h_2(\varepsilon) \tag{6.19}$$

$$\leq I(K_A; L_B B^n)_\rho - I(K_A; E^n)_\rho + \varepsilon \log_2 |K| + h_2(\varepsilon) + \delta \log_2 |K| + g(\delta) \tag{6.20}$$

$$\leq \max_{p_{X^n}, \sigma_{L_B B'^n} \in \mathscr{D}(\mathcal{H}_{L_B B'^n})} [I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau] + \varepsilon \log_2 |K| + h_2(\varepsilon) + \delta \log_2 |K| + g(\delta), \tag{6.21}$$

where $\tau_{X^n L_B B^n E^n}$ is a state of the form in (6.8). The first inequality follows from Fano's inequality [239]. The second inequality follows from the monotonicity of mutual information under the action of a local quantum channel by Bob (Holevo bound). The final inequality follows because the maximization is over all possible probability distributions and input states. Then,

$$\frac{\log_2 |K|}{n}(1 - \varepsilon - \delta) \leq \max_{p_{X^n}, \sigma_{L_B B'^n}} \frac{1}{n} [I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau] + \frac{h_2(\varepsilon) + g(\delta)}{n}. \tag{6.22}$$

Now considering a sequence of non-adaptive $(n, P, \varepsilon_n, \delta_n)$ protocols with $\lim_{n\to\infty} \frac{\log_2 K_n}{n} = P$, $\lim_{n\to\infty} \varepsilon_n = 0$, and $\lim_{n\to\infty} \delta_n = 0$, the converse bound on non-adaptive private reading capacity of memory cell $\overline{\mathcal{M}_{\mathscr{X}}}$ is given by

$$P \leq \sup_n \max_{p_{X^n}, \sigma_{L_B B'^n}} \frac{1}{n} [I(X^n; L_B B^n)_\tau - I(X^n; E^n)_\tau], \tag{6.23}$$

which follows by taking the limit as $n \to \infty$.

It follows from the results of [103, 104] that right-hand side of (6.23) is also an achievable rate in the limit $n \to \infty$. Indeed, the encoder and reader can induce the cq-wiretap channel $x \to \mathcal{M}_{B'\to BE}^x(\sigma_{L_B B'})$, to which the results of [103, 104] apply. A regularized coding strategy then gives the general achievability statement. Therefore, the non-adaptive private reading capacity is given as stated in the theorem. ∎

6.2 Purifying private reading protocols

As observed in [78, 79] and reviewed in Section 2.7, any protocol of the above form (see Section 6.1.1) can be purified in the following sense. In this section, we assume that each wiretap memory cell consists of a set of isometric channels, written as $\{\mathcal{U}_{B' \to BE}^{\mathcal{M}^x}\}_{x \in \mathcal{X}}$. Thus, Eve has access to system E, which is the output of a particular isometric extension of the channel $\mathcal{M}_{B' \to B}^x$, i.e., $\widehat{\mathcal{M}}_{B' \to E}^x(\cdot) = \text{Tr}_B\{\mathcal{U}_{B' \to BE}^{\mathcal{M}^x}(\cdot)\}$, for all $x \in \mathcal{X}$. Such memory cell is to be referred as an *isometric wiretap memory cell*.

We begin by considering non-adaptive private reading protocols. A non-adaptive purified secret-key-agreement protocol that uses an isometric wiretap memory cell begins with Alice preparing a purification of the maximally classically correlated state:

$$\frac{1}{\sqrt{|K|}} \sum_{k \in \mathcal{K}} |k\rangle_{K_A} |k\rangle_{\hat{K}} |k\rangle_C, \tag{6.24}$$

where $\mathcal{K}$ is a finite classical message set of size $|K|$, and K_A, $\hat{K}$, and C are classical registers. Alice coherently encodes the value of the register C using the memory cell, the codebook $\{x^n(k)\}_k$, and the isometric mapping $|k\rangle_C \to |x^n(k)\rangle_{X^n}$. Alice makes two coherent copies of the codeword $x^n(k)$ and stores them safely in coherent classical registers X^n and $\hat{X}^n$. At the same time, she acts on Bob's input state $\rho_{L_B B'^n}$ with the following isometry:

$$\sum_{x^n} |x^n\rangle\langle x^n|_{X^n} \otimes U_{B'^n \to B^n E^n}^{\mathcal{M}^{x^n}} \otimes |x^n\rangle_{\hat{X}^n}. \tag{6.25}$$

For the task of reading, Bob inputs the state $\rho_{L_B B'^n}$ to the channel sequence $\mathcal{M}^{x^n(k)}$, with the goal of decoding k. In the purified setting, the resulting output state is $\psi_{K_A \hat{K} X^n L_B' L_B B^n E^n \hat{X}^n}$, which includes all concerned coherent classical registers or quantum systems accessible by Alice, Bob and Eve:

$$|\psi\rangle_{K_A \hat{K} X^n L_B' L_B B^n E^n \hat{X}^n} := \frac{1}{\sqrt{|K|}} \sum_k |k\rangle_{K_A} |k\rangle_{\hat{K}} |x^n(k)\rangle_{X^n} U_{B'^n \to B^n E^n}^{\mathcal{M}^{x^n}} |\psi\rangle_{L_B' L_B B'^n} |x^n(k)\rangle_{\hat{X}^n}, \tag{6.26}$$

where $\psi_{L_B' L_B B'^n}$ is a purification of $\rho_{L_B B'^n}$ and the systems L_B', L_B, and B^n are held by Bob,

whereas Eve has access only to E^n. The final global state is $\psi_{K_A \hat{K} X^n L'_B K_B E^n \hat{X}^n}$ after Bob applies the decoding channel $\mathcal{D}_{L_B B^n \to K_B}$, where

$$|\psi\rangle_{K_A \hat{K} X^n L'_B L''_B K_B E^n \hat{X}^n} := U^{\mathcal{D}}_{L_B B^n \to L''_B K_B} |\psi\rangle_{K_A \hat{K} X^n L'_B L_B B^n E^n \hat{X}^n}, \tag{6.27}$$

$U^{\mathcal{D}}$ is an isometric extension of the decoding channel $\mathcal{D}$, and L''_B is part of the shield system of Bob.

At the end of the purified protocol, Alice possesses the key system K_A and the shield systems $\hat{K} X^n \hat{X}^n$, Bob possesses the key system K_B and the shield systems $L'_B L''_B$, and Eve possesses the environment system E^n. The state $\psi_{K_A \hat{K} X^n L'_B L''_B K_B \hat{X}^n E^n}$ at the end of the protocol is a pure state.

For a fixed n, $|K| \in \mathbb{N}$, $\varepsilon \in [0,1]$, the original protocol is an $(n, P, \sqrt{\varepsilon}, \sqrt{\varepsilon})$ private reading protocol if the memory cell is called n times as discussed above, where private reading rate $P := \frac{1}{n} \log_2 |K|$, and if

$$F(\psi_{K_A \hat{K} X^n L'_B L''_B K_B \hat{X}^n}, \gamma_{S_A K_A K_B S_B}) \geq 1 - \varepsilon, \tag{6.28}$$

where γ is a private state such that $S_A = \hat{K} X^n \hat{X}^n$, $K_A = K_A$, $K_B = K_B$, $S_B = L'_B L''_B$. See [80, Appendix B] for further details.

Similarly, it is possible to purify a general adaptive private reading protocol, but we omit the details.

6.2.1 Converse bounds on private reading capacities

In this section, we derive different upper bounds on the private reading capacity of an isometric wiretap memory cell. The first is a weak converse upper bound on the non-adaptive private reading capacity in terms of the squashed entanglement. The second is a strong converse upper bound on the (adaptive) private reading capacity in terms of the bidirectional max-relative entropy of entanglement. Finally, we evaluate the private reading capacity for an example: a qudit erasure memory cell.

We derive the first converse bound on non-adaptive private reading capacity by making the following observation, related to the development in [80, Appendix B]: any non-adaptive $(n, P, \varepsilon, \delta)$ private reading protocol of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$, for reading out a secret key, can be realized by an $(n, P, \varepsilon'(2 - \varepsilon'))$ non-adaptive purified secret-key-agreement reading protocol,

where $\varepsilon' := \varepsilon + 2\delta$. As such, a converse bound for the latter protocol implies a converse bound for the former.

First, we derive an upper bound on the non-adaptive private reading capacity in terms of the squashed entanglement [36]:

Proposition 6.1 *The non-adaptive private reading capacity $P_{\text{n-a}}^{\text{read}}(\overline{\mathcal{M}}_{\mathscr{X}})$ of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{U}_{B' \to BE}^{\mathcal{M}^x}\}_{x \in \mathscr{X}}$ is bounded from above as*

$$P_{\text{n-a}}^{\text{read}}(\overline{\mathcal{M}}_{\mathscr{X}}) \leq \sup_{p_X, \psi_{LB'}} E_{\text{sq}}(XL_B; B)_\omega, \tag{6.29}$$

where $\omega_{XL_BB} = \text{Tr}_E\{\omega_{XL_BBE}\}$, such that $\psi_{L_BB'}$ is a pure state and

$$|\omega\rangle_{XLBE} = \sum_{x \in \mathscr{X}} \sqrt{p_X(x)} |x\rangle_X \otimes U_{B' \to BE}^{\mathcal{M}^x} |\psi\rangle_{L_BB'}. \tag{6.30}$$

Proof. For the discussed purified non-adaptive secret-key-agreement reading protocol, when (6.28) holds, the dimension of the secret key system is upper bounded as [240, Theorem 2]:

$$\log_2 |K| \leq E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A; K_BL_BL_B'')_\psi + f_1(\sqrt{\varepsilon}, |K|), \tag{6.31}$$

where

$$f_1(\varepsilon, |K|) := 2\varepsilon \log_2 |K| + 2g(\varepsilon). \tag{6.32}$$

We can then proceed as follows:

$$\log_2 |K| \leq E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A; K_BL_B''L_B')_\psi + f_1(\sqrt{\varepsilon}, |K|) \tag{6.33}$$

$$= E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A; B^nL_BL_B')_\psi + f_1(\sqrt{\varepsilon}, |K|). \tag{6.34}$$

where the first equality is due to the invariance of E_{sq} under isometries.

For any five-partite pure state $\phi_{B'B_1B_2E_1E_2}$, the following inequality holds [96, Theorem 7]:

$$E_{\text{sq}}(B'; B_1B_2)_\phi \leq E_{\text{sq}}(B'B_2E_2; B_1)_\phi + E_{\text{sq}}(B'B_1E_1; B_2)_\phi. \tag{6.35}$$

This implies that

$$E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A; B^nL_BL'_B)_\psi$$

$$\leq E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AL_BL'_BB^{n-1}E^{n-1}; B_n)_\psi + E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AB_nE_n; L_BL'_BB^{n-1})_\psi \qquad (6.36)$$

$$= E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AL_BL'_BB^{n-1}E^{n-1}; B_n)_\psi + E_{\text{sq}}(\hat{K}X^n\hat{X}^{n-1}K_AB'_n; L_BL'_BB^{n-1})_\psi. \qquad (6.37)$$

where the equality holds by considering an isometry with the following uncomputing action:

$$|k\rangle_{K_A}|k\rangle_{\hat{K}}|x^n(k)\rangle_{X^n}U^{\mathcal{M}^{x^n}}_{B'^n\to B^nE^n}|\psi\rangle_{L'_BL_BB'^n}|x^n(k)\rangle_{\hat{X}^n}$$

$$\to |k\rangle_{K_A}|k\rangle_{\hat{K}}|x^n(k)\rangle_{X^n}U^{\mathcal{M}^{x^{n-1}}}_{B'^{n-1}\to B^{n-1}E^{n-1}}|\psi\rangle_{L'_BL_BB'^n}|x^{n-1}(k)\rangle_{\hat{X}^{n-1}}. \qquad (6.38)$$

Applying the inequality in (6.35) and uncomputing isometries like the above repeatedly to (6.37), we get

$$E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A; B^nL_BL'_B)_\psi \leq \sum_{i=1}^n E_{\text{sq}}(\hat{K}X^n\hat{X}_iK_AL_BL'_BB'^{n\backslash\{i\}}; B_i), \qquad (6.39)$$

where the notation $B'^{n\backslash\{i\}}$ indicates the composite system $B'_1B'_2\cdots B'_{i-1}B'_{i+1}\cdots B'_n$, i.e. all $n-1$ B'-labeled systems except B'_i. Each summand above is equal to the squashed entanglement of some state of the following form: a bipartite state is prepared on some auxiliary system Z and a control system X, a bipartite state is prepared on systems L_B and B', a controlled isometry $\sum_x |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}$ is performed from X to B', and then E is traced out. By applying the development in [123, Appendix A], we conclude that the auxiliary system Z is not necessary. Thus, the state of systems X, L_B, B', and E can be taken to have the form in (6.30). From (6.34) and the above reasoning, since $\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{f_1(\sqrt{\varepsilon},|K|)}{n}=0$, we can conclude that

$$\widetilde{P}^{\text{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathscr{X}}) \leq \sup_{p_X,\psi_{L_BB'}} E_{\text{sq}}(XL; B)_\omega, \qquad (6.40)$$

where $\omega_{XL_BB} = \text{Tr}_E\{\omega_{XL_BBE}\}$, such that $\psi_{L_BB'}$ is a pure state and

$$|\omega\rangle_{XL_BBE} = \sum_{x\in\mathscr{X}} \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B'\to BE}|\psi\rangle_{L_BB'}. \qquad (6.41)$$

This concludes the proof. ∎

We now bound the strong converse private reading capacity of an isometric wiretap memory cell in terms of the bidirectional max-relative entropy (see Chapter 3).

Theorem 6.2 *The strong converse private reading capacity $\widetilde{P}^{\text{read}}(\overline{\mathcal{M}}_{\mathscr{X}})$ of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{U}_{B'\to BE}^{\mathcal{M}^x}\}_{x\in\mathscr{X}}$ is bounded from above by the bidirectional max-relative entropy of entanglement $E_{\max}^{2\to2}(\mathcal{N}_{X'B'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}})$ of the bidirectional channel $\mathcal{N}_{X'B'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}}$, i.e.,*

$$\widetilde{P}^{\text{read}}(\overline{\mathcal{M}}_{\mathscr{X}}) \leq E_{\max}^{2\to2}(\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}}), \tag{6.42}$$

where

$$\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}}(\cdot) := \text{Tr}_E\left\{U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}}(\cdot)\left(U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}}\right)^\dagger\right\}, \tag{6.43}$$

such that

$$U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}} := \sum_{x\in\mathscr{X}}|x\rangle\langle x|_X \otimes U_{B'\to BE}^{\mathcal{M}^x}. \tag{6.44}$$

Proof. First we recall, as stated previously, that a $(n, P, \varepsilon, \delta)$ (adaptive) private reading protocol of a memory cell $\overline{\mathcal{M}}_{\mathscr{X}}$, for reading out a secret key, can be realized by an $(n, P, \varepsilon'(2 - \varepsilon'))$ purified secret-key-agreement reading protocol, where $\varepsilon' := \varepsilon + 2\delta$. Given that a purified secret-key-agreement reading protocol can be understood as particular case of a bidirectional secret-key-agreement protocol (as discussed in Section 3.3.2), we can conclude that the strong converse private reading capacity is bounded from above by

$$\widetilde{P}_{\text{n-a}}^{\text{read}}(\overline{\mathcal{M}}_{\mathscr{X}}) \leq E_{\max}^{2\to2}(\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}}), \tag{6.45}$$

where the bidirectional channel is

$$\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathscr{X}}}(\cdot) = \text{Tr}_E\left\{U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}}(\cdot)\left(U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}}\right)^\dagger\right\}, \tag{6.46}$$

such that

$$U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}} := \sum_{x\in\mathscr{X}}|x\rangle\langle x|_X \otimes U_{B'\to BE}^{\mathcal{M}^x}. \tag{6.47}$$

The reading protocol is a particular instance of an LOCC-assisted bidirectional secret-key-agreement protocol in which classical communication between Alice and Bob does not occur. The local operations of Bob in the bidirectional secret-key-agreement protocol are equivalent to adaptive operations by Bob in reading. Therefore, applying Theorem 3.2, we find that (6.42) holds, where the strong converse in this context means that $\varepsilon + 2\delta \to 1$ in the limit as $n \to \infty$ if the reading rate exceeds $E_{\max}^{2\to2}(\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathcal{X}}})$.[1] ∎

Qudit erasure wiretap memory cell

The main goal of this section is to evaluate the private reading capacity of the qudit erasure wiretap memory cell (cf. Definition 5.8).

Definition 6.2 (Qudit erasure wiretap memory cell) *The qudit erasure wiretap memory cell* $\overline{\mathcal{Q}}_{\mathcal{X}}^q = \{\mathcal{Q}_{B'\to BE}^{q,x}\}_{x\in\mathcal{X}}$, *where $\mathcal{X}$ is of size $|X| = d^2$, consists of the following qudit channels:*

$$\mathcal{Q}^{q,x}(\cdot) = \mathcal{Q}^q(\sigma^x(\cdot)(\sigma^x)^\dagger), \tag{6.48}$$

where $\mathcal{Q}^q$ is an isometric channel extending the qudit erasure channel [236]:

$$\mathcal{Q}^q(\rho_{B'}) = U^q \rho_{B'}(U^q)^\dagger, \tag{6.49}$$

$$U^q|\psi\rangle_{B'} = \sqrt{1-q}|\psi\rangle_B|e\rangle_E + \sqrt{q}|e\rangle_B|\psi\rangle_E, \tag{6.50}$$

such that $q \in [0,1]$, $\dim(\mathcal{H}_{B'}) = d$, $|e\rangle\langle e|$ is an erasure state orthogonal to the support of all possible input states ρ, and $\forall x \in \mathcal{X} : \sigma^x \in \mathbf{H}$ are the Heisenberg–Weyl operators as reviewed in (A.7). Observe that $\mathcal{Q}_{\mathcal{X}}^q$ is jointly covariant with respect to the Heisenberg–Weyl group $\mathbf{H}$ because the qudit erasure channel $\mathcal{Q}^q$ is covariant with respect to $\mathbf{H}$.

Now we establish the private reading capacity of the qudit erasure wiretap memory cell.

---

[1]Such a bound might be called a "pretty strong converse," in the sense of [241]. However, we could have alternatively defined a private reading protocol to have a single parameter characterizing reliability and security, as in [80], and with such a definition, we would get a true strong converse.

Proposition 6.2 *The private reading capacity and strong converse private reading capacity of the qudit erasure wiretap memory cell $\overline{\mathcal{Q}}_{\mathcal{X}}^q$ are given by*

$$P^{\mathrm{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^q) = \widetilde{P}^{\mathrm{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^q) = 2(1-q)\log_2 d. \tag{6.51}$$

Proof. To prove the proposition, let us consider that $\mathcal{N}^{\overline{\mathcal{Q}}_{\mathcal{X}}^q}$ as defined in (6.43) is bicovariant and $\mathcal{Q}_{B' \to B}^q$ is covariant. Thus, to get an upper bound on the strong converse private reading capacity, it is sufficient to consider the action of a coherent use of the memory cell on a maximally entangled state (see Corollary 3.5). We furthermore apply the development in [123, Appendix A] to restrict to the following state:

$$
\begin{aligned}
\phi_{XL_BBE} &:= \frac{1}{\sqrt{|X|}} \sum_{x \in \mathcal{X}} |x\rangle_X \otimes U_{B' \to BE}^{\mathcal{Q}^{q,x}} |\Phi\rangle_{L_BB'} \\
&= \sqrt{\frac{1-q}{d|X|}} \sum_{i=0}^{d} \sum_{x} |x\rangle_X \otimes \sigma^x |i\rangle_B |i\rangle_{L_B} |e\rangle_E + \sqrt{\frac{q}{d|X|}} \sum_{i=0}^{d} \sum_{x} |x\rangle_X \otimes |e\rangle_B |i\rangle_{L_B} \otimes \sigma^x |i\rangle_E.
\end{aligned}
\tag{6.52}
$$

Observe that $\sum_{i=0}^{d-1} \sum_x |x\rangle_X \otimes |e\rangle_B |i\rangle_{L_B} \otimes \sigma^x |i\rangle_E$ and $\sum_{i=0}^{d-1} \sum_x |x\rangle_X \otimes \sigma^x |i\rangle_B |i\rangle_{L_B} |e\rangle_E$ are orthogonal. Also, since, $|e\rangle$ is orthogonal to the input Hilbert space, the only term contributing to the relative entropy of entanglement is $\sqrt{1-q}\frac{1}{d}\sum_{i=0}^{d}\sum_x |x\rangle_X \otimes \sigma^x |i\rangle_B |i\rangle_{L_B}$. Let

$$|\psi\rangle_{XL_BB} = \frac{1}{\sqrt{|X|}} \sum_{x=0}^{d^2-1} |x\rangle_X \otimes \sigma^x |\Phi\rangle_{BL_B}. \tag{6.53}$$

$\{\sigma^x |\Phi\rangle_{BL_B}\}_{x \in \mathcal{X}} \in \mathrm{ONB}(\mathcal{H}_B \otimes \mathcal{H}_{L_B})$ (see Appendix A), so

$$|\psi\rangle_{XL_BB} = |\Phi\rangle_{X:BL_B} = \frac{1}{d}\sum_{x=0}^{d^2-1} |x\rangle_X \otimes |x\rangle_{BL_B}, \tag{6.54}$$

and $E(X; LB)_\Phi = 2\log_2 d$. Applying Corollary 3.5 and convexity of relative entropy of entanglement, we can conclude that

$$\widetilde{P}^{\mathrm{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^q) \le 2(1-q)\log_2 d. \tag{6.55}$$

From Theorem 6.1, the following bound holds

$$P^{\mathrm{read}}(\overline{\mathcal{Q}}_{\mathscr{X}}^q) \geq P_{\mathrm{n\text{-}a}}^{\mathrm{read}}(\overline{\mathcal{Q}}_{\mathscr{X}}^q) \tag{6.56}$$

$$\geq I(X; L_B B)_\rho - I(X; E)_\rho, \tag{6.57}$$

where

$$\rho_{XL_BBE} = \frac{1}{d^2} \sum_{x=0}^{d^2-1} |x\rangle\langle x|_X \otimes \mathcal{U}_{B' \to BE}^{\mathcal{Q}^{q,x}}(\Phi_{X:L_BB'}). \tag{6.58}$$

After a calculation, we find that $I(X; E)_\rho = 0$ and $I(X; L_B B)_\rho = 2(1-q)\log_2 d$. Therefore, from (6.55) and the above, the statement of the theorem is concluded. ∎

From the above and Corollary 5.4, we can conclude that there is no difference between the private reading capacity of the qudit erasure memory cell and its reading capacity.

6.3 Entanglement generation from a coherent memory cell

In this section, we consider an entanglement distillation task between two parties Alice and Bob holding systems X and B, respectively. The set up is similar to purified secret key generation when using a memory cell (see Section 6.2). The goal of the protocol is as follows: Alice and Bob, who are spatially separated, try to generate a maximally entangled state between them by making coherent use of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathscr{X}} = \{\mathcal{U}_{B' \to BE}^{\mathcal{M}^x}\}_{x \in \mathscr{X}}$ known to both parties. That is, Alice and Bob have access to the following controlled isometry:

$$U_{XB' \to XBE}^{\overline{\mathcal{M}}_{\mathscr{X}}} := \sum_{x \in \mathscr{X}} |x\rangle\langle x|_X \otimes U_{B' \to BE}^{\mathcal{M}^x}, \tag{6.59}$$

such that X and E are inaccessible to Bob. Using techniques from [104], we can state an achievable rate of entanglement generation by coherently using the memory cell.

Theorem 6.3 *The following rate is achievable for entanglement generation when using the controlled isometry in* (6.59)*:*

$$I(X\rangle L_B B)_\omega, \tag{6.60}$$

where $I(X \rangle L_B B)_\omega$ is the coherent information of state ω_{XL_BB} (2.48) such that

$$|\omega\rangle_{XL_BBE} = \sum_{x \in \mathcal{X}} \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B' \to BE}|\psi\rangle_{L_BB'}. \tag{6.61}$$

Proof. Let $\{x^n(m,k)\}_{m,k}$ denote a codebook for private reading, as discussed in Section 6.1.1, and let $\psi_{L_BB'}$ denote a pure state that can be fed in to each coherent use of the memory cell. The codebook is such that for each $m \in \mathcal{M}$ and $k \in \mathcal{K}$, the codeword $x^n(m,k)$ is unique. The rate of private reading is given by

$$I(X; L_BB)_\rho - I(X; E)_\rho, \tag{6.62}$$

where

$$\rho_{XB'BE} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \mathcal{U}^{\mathcal{M}^x}_{B' \to BE}(\psi_{L_BB'}). \tag{6.63}$$

Note that the following equality holds

$$I(X; L_BB)_\rho - I(X; E)_\rho = I(X \rangle L_BB)_\omega, \tag{6.64}$$

where

$$|\omega\rangle_{XL_BBE} = \sum_x \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B' \to BE}|\psi\rangle_{L_BB'}. \tag{6.65}$$

The code is such that there is a measurement $\Lambda^{m,k}_{L_B^n B^n}$ for all m, k, for which

$$\mathrm{Tr}\{\Lambda^{m,k}_{L_B^n B^n} \mathcal{M}^{x^n(m,k)}_{B'^n \to B^n}(\psi^{\otimes n}_{L_BB'})\} \geq 1 - \varepsilon, \tag{6.66}$$

and

$$\frac{1}{2}\left\|\frac{1}{|K|}\sum_k \widehat{\mathcal{M}}^{x^n(m,k)}_{B'^n \to E^n}(\psi^{\otimes n}_{B'}) - \sigma_{E^n}\right\|_1 \leq \delta. \tag{6.67}$$

From this private reading code, we construct a coherent reading code as follows. Alice begins by preparing the state

$$\frac{1}{\sqrt{|M||K|}}\sum_{m,k} |m\rangle_{M_A}|k\rangle_{K_A}. \tag{6.68}$$

Alice performs a unitary that implements the following mapping:

$$|m\rangle_{M_A}|k\rangle_{K_A}|0\rangle_{X^n} \rightarrow |m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}, \tag{6.69}$$

so that the state above becomes

$$\frac{1}{\sqrt{|M||K|}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}. \tag{6.70}$$

Bob prepares the state $|\psi\rangle^{\otimes n}_{L_B B'}$, so that the overall state is

$$\frac{1}{\sqrt{|M|K|}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}|\psi\rangle^{\otimes n}_{L_B B'}. \tag{6.71}$$

Now Alice and Bob are allowed to access n instances of the controlled isometry

$$\sum_x |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\rightarrow BE}, \tag{6.72}$$

and the state becomes

$$\frac{1}{\sqrt{|M||K|}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}U^{\mathcal{M}^{x^n(m,k)}}_{B'^n\rightarrow B^n E^n}|\psi\rangle^{\otimes n}_{L_B B'}. \tag{6.73}$$

Bob now performs the isometry

$$\sum_{m,k}\sqrt{\Lambda^{m,k}_{L^n_B B^n}} \otimes |m\rangle_{M_1}|k\rangle_{K_1}, \tag{6.74}$$

and the resulting state is close to

$$\frac{1}{\sqrt{|M||K|}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}U^{x^n(m,k)}_{B'^n\rightarrow B^n E^n}|\psi\rangle^{\otimes n}_{L_B B'}|m\rangle_{M_1}|k\rangle_{K_1}. \tag{6.75}$$

At this point, Alice locally uncomputes the unitary from (6.69) and discards the X^n register, leaving

the following state:

$$\frac{1}{\sqrt{|M||K|}} \sum_{m,k} |m\rangle_{M_A} |k\rangle_{K_A} U^{\mathcal{M}_\mathcal{A}^{x^n(m,k)}}_{B'^n \to B^n E^n} |\psi\rangle^{\otimes n}_{L_B B'} |m\rangle_{M_1} |k\rangle_{K_1}. \tag{6.76}$$

Following the scheme of [104] for entanglement distillation, she then performs a Fourier transform on the register K_A and measures it, obtaining an outcome $k' \in \{0, \ldots, K-1\}$, leaving the following state:

$$\frac{1}{\sqrt{|M||K|}} \sum_{m,k} e^{2\pi i k'k/K} |m\rangle_{M_A} U^{\mathcal{M}_\mathcal{A}^{x^n(m,k)}}_{B'^n \to B^n E^n} |\psi\rangle^{\otimes n}_{L_B B'} |m\rangle_{M_1} |k\rangle_{K_1}. \tag{6.77}$$

She communicates the outcome to Bob, who can then perform a local unitary on system K_1 to bring the state to

$$\frac{1}{\sqrt{|M||K|}} \sum_{m,k} |m\rangle_{M_A} U^{\mathcal{M}^{x^n(m,k)}}_{B'^n \to B^n E^n} |\psi\rangle^{\otimes n}_{L_B B'} |m\rangle_{M_1} |k\rangle_{K_1}. \tag{6.78}$$

Now consider that, conditioned on a value m in register M, the local state of Eve's register E^n is given by

$$\frac{1}{|K|} \sum_k \widehat{\mathcal{M}}^{x^n(m,k)}_{B'^n \to E^n} (\psi^{\otimes n}_{B'}). \tag{6.79}$$

Thus, by invoking the security condition in (6.67) and Uhlmann's theorem [75], there exists a isometry $V^m_{L_B^n B^n K_1 \to \widetilde{B}}$ such that

$$V^m_{L_B^n B^n K_1 \to \widetilde{B}} \left[\frac{1}{\sqrt{|K|}} \sum_k U^{\mathcal{M}^{x^n(m,k)}}_{B'^n \to B^n E^n} |\psi\rangle^{\otimes n}_{L_B B'} |k\rangle_{K_1} \right] \approx |\varphi^\sigma\rangle_{E^n \widetilde{B}}. \tag{6.80}$$

Thus, Bob applies the controlled isometry

$$\sum_m |m\rangle\langle m|_{M_1} \otimes V^m_{L_B^n B^n K_1 \to \widetilde{B}}, \tag{6.81}$$

and then the overall state is close to

$$\frac{1}{\sqrt{|M|}} \sum_m |m\rangle_{M_A} |\varphi^\sigma\rangle_{E^n \widetilde{B}} |m\rangle_{M_1}. \tag{6.82}$$

Bob now discards the register $\widetilde{B}$ and Alice and Bob are left with a maximally entangled state that

is locally equivalent to approximately $n[I(X; L_B B)_\rho - I(X; E)_\rho] = nI(X \rangle L_B B)_\omega$ ebits. ∎

6.4 Conclusion

In this chapter, we discussed a private communication task called private reading. This task allows for secret key agreement between an encoder and a reader in the presence of a passive eavesdropper. Observing that access to an isometric wiretap memory cell by an encoder and the reader is a particular kind of bipartite quantum interaction, we were able to leverage bounds derived on the LOCC-assisted bidirectional secret-key-agreement capacity (Section 3.3.2) to determine bounds on its private reading capacity. We also determined a regularized expression for the non-adaptive private reading capacity of an arbitrary wiretap memory cell. For particular classes of memory cells obeying certain symmetries, such that there is an adaptive-to-non-adaptive reduction in a reading protocol (see Chapter 5), the private reading capacity and the non-adaptive private reading capacity are equal. We derived a single-letter, weak converse upper bound on the non-adaptive private reading capacity of an isometric wiretap memory cell in terms of the squashed entanglement. We also proved a strong converse upper bound on the private reading capacity of an isometric wiretap memory cell in terms of the bidirectional max-relative entropy of entanglement. We applied discussed results to show that the private reading capacity and the reading capacity of the qudit erasure memory cell are equal. Finally, we determined an achievable rate at which entanglement can be generated between two parties who have coherent access to a memory cell.

We note that there is a connection to private reading protocol and floodlight quantum key distribution (FL-QKD) protocol [242, 243]. In FL-QKD, Alice transmits system (signal) A' in the state $\rho_{LA'}$ to Bob through a channel $\mathcal{A}_{A' \to B}$ and keeps idler system L with her. Bob performs some unitary channel $\mathcal{U}^k_{B \to B}$, which is noiseless, based on a key (k) that he wants to communicate to Alice. Next, Bob performs another transformation $\mathcal{B}_{B \to A'}$ on the local output after the action of $\mathcal{U}^k$. Now the system A' in the state $\mathcal{B}_{B \to A'} \circ \mathcal{U}^k_{B \to B} \circ \mathcal{A}_{A' \to B}(\rho_{LA'})$ is transmitted to Alice over the channel $\mathcal{A}_{A' \to B}$. It is assumed that Eve has complete access to complementary $\hat{\mathcal{A}}_{A' \to E}$ of $\mathcal{A}$. Bob performs joint measurement on LB in the state $\mathcal{A}_{A' \to B} \circ \mathcal{B}_{B \to A'} \circ \mathcal{U}^k_{B \to B} \circ \mathcal{A}_{A' \to B}(\rho_{LA'})$ to decode the key.

Now let us modify the above FL-QKD protocol in the following way. Let us assume $\mathcal{A}_{A' \to B}$ to be

noiseless channel and constraining access of Eve only to losses due to noisy local operations $\mathcal{B} \circ \mathcal{U}^k$ for all k, where encoding of key is such that the system (loss) accessible to Eve is independent of k. Then the modified FL-QKD protocol effectively reduces to a private reading protocol. Hence, framework to derive bounds on the private capacity here may provide some insight for deriving converse bounds on the private capacity of FL-QKD. We leave this question open for future direction.

Chapter 7   Hiding Digital Information in Quantum Processes for Security

In this era of rapidly-advancing technologies, there is a pertinent need for protocols that allow for secure reading of memory devices under adversarial scrutiny. Security requirements may vary depending on the situation the reader is in; for example, a person reading a document in a library (or internet café) wants to ensure that the librarian is not eavesdropping (cf. Chapter 6). Similarly, a spy desires to read messages securely from his or her home organization when in the vicinity of a rival organization, without arousing suspicion of the rival organization.

By exploiting the laws of quantum mechanics, the capabilities of information processing and computing tasks can be pushed beyond the limitations imposed by classical information theory. This also provides the opportunity to devise new information processing protocols, e.g., quantum key distribution [16, 17] and quantum teleportation [18, 19]. The tasks of imaging, reading, sensing, or spectroscopy of an (unknown) object of interest essentially involves the identification of an interaction process between probe system, which is in known state, and the object of interest [20, 31, 109, 212, 244–246]. It is known that the most interaction processes that lead to physical transformation of the state can be understood as a quantum channel. This makes it natural to model any reading task as the read-out of classical bits of information encoded as a sequence of quantum channels chosen from a particular set.

In this chapter, we discuss information processing and communication protocols for the secure reading of digital information hidden in quantum processes. Here we consider two kinds of adversaries: a passive adversary who has access only to the environment and a semi-passive adversary who has access to the memory device but cannot alter it. Before introducing secure reading protocols in Section 7.2, we briefly discuss secure communication protocol with zero-error where message is hidden in noiseless gates, i.e., unitary operations. Then we formally introduce secure reading protocols where message is encoded in noisy gates, i.e., quantum channels. In Section 7.3, we illustrate the possibility of secure reading by providing examples where memory device is encoded using a bi-

---

nary memory cell consisting of amplitude damping channels [21, 198] or depolarizing channels [210]. Finally, we briefly discuss the application of aforementioned protocols to threat level identification (TLI), which is inspired by IFF: identification, friend or foe [247].

7.1   Secure communication using gate circuit

Let us assume a situation where two distant friends, Hardy and Ramanujan, share a computer network. Assume that Hardy's computer is also accessible to Littlewood. Ramanujan wants to share a message on network intended only for Hardy. Message is not top secret and so Ramanujan is fine with communicating message on network if chances of getting discovered by Littlewood is low.

Consider that a bipartite computer network between Ramanujan and Hardy has five ports, labeled as M, K, K', B', B. M is message register taking values $m \in \mathscr{M}$ and K, K' are key registers taking values $k \in \mathscr{K}$, where $K = K'$, and B', B corresponds to probing and reading ports, respectively. It is publicly known that computer performs a unitary operation $\mathcal{U}^g_{B' \to B}(\cdot) :=$ $U^g_{B' \to B}(\cdot)(U^g_{B' \to B})^\dagger$ on input system B' to yield B. Furthermore, we consider that $\{U^g_{B' \to B}\}_{g \in \mathscr{G}}$ forms a gate-set of unitary one-design. Ramanujan and Hardy share key k that is unknown to Littlewood. Ramanujan has access to M, K, Hardy has access to K', B', B, but Littlewood has access only to B', B. For simplicity, Ramanjuan and Hardy devise communication strategy such that $|M|$ and $|K|$ are both equal to the size $|G|$ of $\mathscr{G}$.

Now Ramanujan inputs message m and key k in his message and key registers, respectively, and following computation is set on computer network:

$$|m\rangle\!\langle m|_M \otimes |k\rangle\!\langle k|_K \otimes |k\rangle\!\langle k|_{K'} \otimes \mathcal{U}^{x(m,k)}_{B' \to B}(\rho_{LB'}), \tag{7.1}$$

where

$$x(m, k) := (m \oplus k) \mod |G| \tag{7.2}$$

and ρ_{LB} is a probe state inserted on demand by the reader, Hardy or Littlewood. L is an idler system that is held by the reader[1]. Ramanujan can send message m with an apriori probability

---

[1]We know that two non-orthogonal quantum states cannot be perfectly distinguishable whenever only a finite number of copies are available [248, 249]. However, any two different unitary operations

$p(m)$ (see [109]). However, for now we consider a case when message and key are chosen uniformly at random. Under such scenario, the resulting state of composite system MB is a product state after the computation takes place,

$$|m\rangle\langle m|_M \otimes \frac{1}{|G|} \sum_m \mathcal{U}^{x(m,k)}_{B'\to B}(\rho_{LB'}) = |m\rangle\langle m|_M \otimes \rho_L \otimes \frac{\mathbb{1}_B}{|G|}, \qquad (7.3)$$

which holds for any input state $\rho_{LB'}$. It is clear that M, B, and L are all uncorrelated in absence of key, and any measurement by Littlewood on output system LB will give random value for m. This is equivalent to success probability of Littlewood in guessing m with probability $1/|M|$.

Now we inspect the ability of Hardy to decode the message. Since Hardy possess key, situation boils down to the discussion in [109]. There exists a scheme for Hardy where the correlation between M and B are non-zero and may attain the maximum in presence of key [109]. One such case is when the states $\mathcal{U}^{x(m,k)}_{B'\to B}(\rho_{B'})$ are pure and orthogonal for all x [109]. In general, it was shown in [250] that a unitary operation secretly chosen from a gate-set can be determined with certainty by sequentially applying only a finite amount of the unknown unitary operation. Once Hardy is able to identify the given operation, he can use key to decode the message.

7.2 Secure identification protocols

Any secure reading protocol consists of two parties of interest, an encoder and a reader, and an adversary. The encoder, Alice, encodes a secret classical message m from a set of messages $\mathcal{M}$ onto a read-only memory device. Consider that the size of $\mathcal{M}$ is $|M|$. It is assumed that the memory device is delivered to the reader, Bob, whose task is to decode, i.e., read the message in a secure way despite scrutiny of adversary.

We now define a secure reading protocol, which consists of an encoding scheme, a reading scheme with reliability criterion, and a security criterion.

---

can always be perfectly distinguishable by taking a suitable entangled state as input and then applying only a finite number of runs of the unknown unitary operation [218,219]. Later, it was shown that entangled input is not necessary for the perfect discrimination of unitary operations [250].

Encoding scheme

The digital memory device is defined by a set $\overline{\mathcal{M}}_{\mathscr{X}} := \{\mathcal{N}^x_{B' \to BE}\}_{x \in \mathscr{X}}$ of wiretap quantum channels [31], where $\mathscr{X}$ is an alphabet and the size of B', B, E' are fixed and independent of x. We call outputs of channels $\mathcal{N}^x_{B' \to BE}$ as ports, and output B is accessible in reading port and output E is accessible in bath port. Both encoder and reader agree upon the memory cell. The memory cell from Alice to Bob is then given by $\{\mathcal{M}^x_{B' \to B}\}_{x \in \mathscr{X}}$, where

$$\forall x \in \mathscr{X} : \; \mathcal{M}^x_{B' \to B}(\cdot) := \mathrm{Tr}_E\{\mathcal{M}^x_{B' \to BE}(\cdot)\}, \tag{7.4}$$

which may also be known to adversary. The reader does not have access to bath port.

We also assume that Alice and Bob share a secret key taking values in a set $\mathscr{K}$, where the size of $\mathscr{K}$ is $|K|$. Then, for each message $m \in \mathscr{M}$ and key $k \in \mathscr{K}$, we define an encoding of strings $x^n(m, k) = x_1(m, k) \cdots x_n(m, k) \in \mathscr{X}^n$ of blocklength $n \in \mathbb{N}$ into codewords:

$$x^n(m, k) \mapsto \left(\mathcal{N}^{x_1(m,k)}_{B'_1 \to B_1 E_1}, \dots, \mathcal{N}^{x_n(m,k)}_{B'_n \to B_n E_n} \right). \tag{7.5}$$

Each quantum channel in a codeword, each of which represents one part of the stored information is only read once.

Reliability criterion for non-adaptive scheme

Reading of the memory device is defined by the channel

$$\mathcal{N}^{x^n(m,k)}_{B'^n \to B^n E^n} := \mathcal{N}^{x_1(m,k)}_{B'_1 \to B_1 E_1} \otimes \cdots \otimes \mathcal{N}^{x_n(m,k)}_{B_n \to B_n E_n}, \tag{7.6}$$

an input state $\rho_{LB'^n}$ and a positive operator-valued measure (POVM) $\left\{ \Lambda^{(m,k)}_{LB^n} \right\}_m$ for each k, where L is an arbitrary reference system belonging to the reader. Bob transmits the state $\rho_{LB'^n}$ through the wiretap channel $\mathcal{N}^{x^n(m,k)}_{B'^n \to B^n E^n}$, measures the output using the POVM $\left\{ \Lambda^{(m,k)}_{LB^n} \right\}_m$, and uses the measurement outcome to guess the message m.

For reliable reading of the message, the following reliability criterion should hold for each $k \in \mathscr{K}$

and $m \in \mathcal{M}$,

$$\text{Tr}\{\Lambda_{LB^n}^{(m,k)} \mathcal{N}_{B'^n \to B^n E^n}^{x^n(m,k)}(\rho_{R^n B'^n})\} \geq 1 - \varepsilon, \tag{7.7}$$

which states that Bob's reading error probability p_e is less than $\varepsilon \in (0,1)$.

Let us consider following definitions.

$$\sigma_{LB^n E^n}^{x^n(m,k)} := \mathcal{N}_{B'^n \to B^n E^n}^{x^n(m,k)}(\rho_{LB'^n}), \qquad \overline{\sigma}_{LB^n E^n} := \frac{1}{|M||K|} \sum_{m \in \mathcal{M}, k \in \mathcal{K}} \sigma_{LB^n E^n}^{x^n(m,k)}, \tag{7.8}$$

and 1-norm[2] $\|\cdot\|_1$ of a Hermiticity preserving map $\mathcal{M}_{B' \to B}$ is given as

$$\max_{\rho_{B'} \in \mathscr{D}(\mathcal{H}_{B'})} \|\mathcal{M}_{B' \to B}(\rho_{B'})\|_1. \tag{7.10}$$

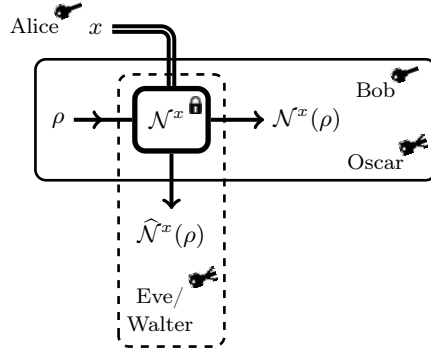**Security criterion for non-adaptive scheme**

Figure 7.1. The scenario of secure reading along with the two types of adversaries being considered. Oscar is an adversary who can have direct access to the memory device. Walter and Eve, on the other hand, do not have direct access to the device. Furthermore, while both Alice and Bob possess a key, neither of the three adversaries do.

The criterion for secure reading will depend on the adversarial situation in which the reader, Bob, is. Here we consider three natural types of adversarial conditions, which correspond to three different

---

[2]The success probability of discriminating two channels $\mathcal{A}_{B' \to B}$ and $\mathcal{B}_{B' \to B}$ when observer is not allowed to use entangled states is

$$\frac{1}{2}\left(1 + \frac{1}{2}\|\mathcal{A}_{B' \to B} - \mathcal{B}_{B' \to B}\|_1\right), \tag{7.9}$$

where $\|\mathcal{M}_{B' \to B}\|_1$ for a Hemiticity preserving map $\mathcal{M}_{B' \to B}$ is defined as (7.10).

secure reading protocols. These security criteria are motivated by those presented in [31, 251–254]. These adversarial conditions are illustrated in Fig. 7.1.

1. Incognito reading: the adversary, Oscar, can have access to the memory device. The goal of Alice and Bob is to ensure that Oscar cannot figure out that the memory device contains any useful information intended for Bob. Oscar has access to the reading port but has no access to bath port. To this end, Alice and Bob share a prior secret key, which will give Bob the required advantage over Oscar. Formally, we require that

$$\left\|\frac{1}{|M||K|}\sum_{m\in\mathscr{M},k\in\mathscr{K}}\mathcal{N}^{x^n(m,k)}_{B'^n\to B^n}-\left(\mathcal{N}^0_{B'\to B}\right)^{\otimes n}\right\|_\diamond\leq\delta'_I,\qquad(7.11)$$

where $\delta'_I\in(0,1)$ and $\|\cdot\|_\diamond$ is the diamond norm (4.110). A memory device containing no information is assumed to be encoded with the single-element memory cell $\{\mathcal{N}^{x=0}_{B'\to BE}\}$. We call $\mathcal{N}^0_{B'\to BE}$ the innocent channel. This means that, if the reader does not possess the key, the memory device cannot be distinguished from one containing no information. To achieve this security criterion, we make stronger assumption

$$\max_{\rho_{LB'^n}\in\mathscr{D}(\mathcal{H}_{LB'^n})}D\left(\bar{\sigma}_{LB^n}\big\|\sigma^0_{LB^n}\right)\leq\delta_I,\qquad(7.12)$$

where $\delta_I\in(0,1)$ and $\sigma^0_{LB^n}=\mathrm{Tr}_{E^n}\{\mathcal{N}^{\otimes n}_{B'\to BE}(\rho_{LB'^n})\}$. Note that it suffices to take optimization in (7.12) over pure states $\rho_{LB'^n}$ such that $L\simeq B'^n$.

2. Covert reading: the adversary, Walter, has access to the bath port only and no access to any other ports of memory device, reading or transmitter. The goal of Alice and Bob is to ensure that Walter cannot detect that any useful information is being read by Bob. In this case, Bob has an advantage over Walter if the wiretap memory cell consists of degradable channels, i.e., $\mathcal{N}^x_{B'\to E}=\mathcal{N}^x_{B\to E}\circ\mathcal{N}^x_{B'\to B}$ for all $x\in\mathscr{X}$, where $\mathcal{N}^x_{B\to E}$ is a quantum channel. In general, however, we assume that Alice and Bob share a prior secret key in order for Bob to have an

advantage over Walter. Formally, we require that

$$\left\| \frac{1}{|M||K|} \sum_{m \in \mathscr{M}, k \in \mathscr{K}} \mathcal{N}_{B' \to E}^{x^n(m,k)} - \left(\mathcal{N}_{B' \to E}^0\right)^{\otimes n} \right\|_1 \leq \delta_C', \tag{7.13}$$

where $\delta_C' \in (0,1)$ and $\|\cdot\|_1$ of a Hermiticity preserving map is defined as (7.10). To achieve this security criterion, we make stronger assumption

$$\max_{\rho_{B'^n}} D\left(\overline{\sigma}_{E^n} \| \left(\sigma_{E^n}^0\right)\right) \leq \delta_C, \tag{7.14}$$

where $\delta_C \in (0,1)$ and $\sigma_{E^n}^0 = \text{Tr}_{LB^n}\{\mathcal{N}_{B' \to BE}^{\otimes n}(\rho_{LB'^n})\}$.

3. Confidential reading: the adversary, Eve, has complete access to the bath port but no direct access to the reading port. The goal of Alice and Bob is to ensure that no information stored in the device is leaked to Eve. In general, we assume that Alice and Bob share a prior secret key in order for Bob to have an advantage over Eve. We demand that for all $m \in \mathscr{M}$,

$$\left\| \frac{1}{|K|} \sum_{k \in \mathscr{K}} \mathcal{N}_{B' \to E}^{x^n(m,k)} - \left(\mathcal{N}_{B' \to E}^0\right)^{\otimes n} \right\|_1 \leq \delta_P, \tag{7.15}$$

where $\delta_P \in (0,1)$.

It is to be noted that all the above security criteria for non-adaptive secure reading protocols can be generalized straightforwardly to secure reading protocols, in which adaptive strategies are employed as part of the reading protocols (see Chapter 5), in the same way as for private reading protocols (see Chapter 6).

An $(n, P, \varepsilon, \delta)$ secure reading protocol is called incognito reading, covert reading, or confidential reading when $\delta = \delta_I$, $\delta = \delta_C$, or $\delta = \delta_P$, respectively, where $P := \frac{1}{n} \log_2 |M|$. The rate of an $(n, P, \varepsilon, \delta)$ secure reading protocol is equal to $\frac{1}{n} \log_2 |M|$. To define the capacity of a secure reading protocol, we demand that there exists a sequence of secure reading protocols indexed by n for which $\varepsilon \to 0$ and $\delta \to 0$ as $n \to \infty$ at a fixed rate P. A rate P is called achievable if for all $\varepsilon, \delta \in (0,1]$, $\xi > 0$, and sufficiently large n, there exists an $(n, P - \xi, \varepsilon, \delta)$ secure reading protocol. The secure reading capacity $P^{\text{secure}}(\overline{\mathcal{M}}_{\mathscr{X}})$ of a wiretap memory cell is defined as the supremum of all achievable

rates P.

It can be concluded that there exists a reduction from secure reading protocols to non-adaptive secure reading protocols for jointly covariant memory cells, in the sense that the former can simulated by the latter (see Chapter 5).

7.3 Illustration of secure reading

Here we provide examples of non-adaptive secure reading protocols for memory devices encoded with a binary memory cell $\{\mathcal{N}^x_{B'\to BE}\}_{x\in\{0,1\}}$ consisting of depolarizing channels or generalized amplitude damping channels $\mathcal{N}^x_{B'\to B}$ for the reader and complementary of these channels $\widehat{\mathcal{N}}^x_{B'\to E}$ for Walter. Goal of this section is to determine number of non-innocent symbols that can be securely transmitted from Alice to Bob. The encoding of the message onto the memory device, e.g., a
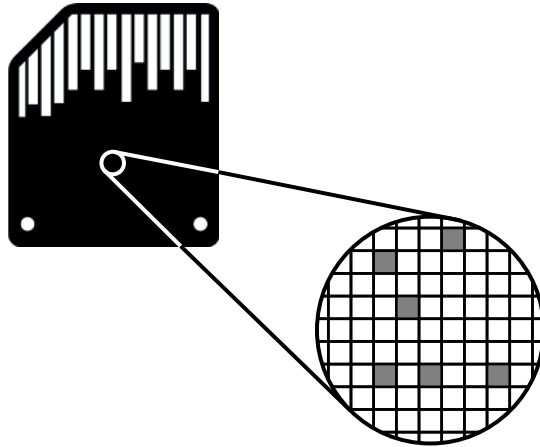

Figure 7.2. The encoding of a message into a digital memory device. The message is encoded into certain domains (indicated by the shaded squares) based on the key shared by the encoder and the reader.

CD-ROM or a flash memory drive, corresponds to either the innocent channel $\mathcal{N}^0_{B'\to B}$ or $\mathcal{N}^1_{B'\to B}$ at each of the sites (domains) of the underlying physical components comprising the device. We assume that Alice uses N of these sites to encode the message. The length of the codewords is thus N, which is spread over the entire reading space; see Figure 7.2. For secure reading, Alice and Bob share a set of secret keys. The keys correspond to a particular choice of sites used to encode the message. With probability $q \ll 1$, Alice encodes each of these sites with $\mathcal{N}^1_{B'\to B}$, and with probability $1 - q$ she encodes it with $\mathcal{N}^0_{B'\to B}$. The rest of N sites are left blank, i.e., encoded with $\mathcal{N}^0_{B'\to B}$. This implies Alice sending on average Nq non-innocent channels that corresponds to

meaningful secure signals.

Suppose that each $\mathcal{N}^x_{B'\to B} = \mathcal{D}^\theta_{B'\to B,\eta_x}$, i.e., the memory cell consists of a two-parameter family of channels. For the sites on which Alice encodes her message, the effective channel is $q\mathcal{D}^\theta_{B'\to B,\eta_1} + (1-q)\mathcal{D}^\theta_{B'\to B,\eta_0}$, and for the empty sites the channel is $\mathcal{D}^\theta_{B'\to B,\eta_0}$, whereas the effective channels to adversary are $q\widehat{\mathcal{D}}^\theta_{B'\to E,\eta_1} + (1-q)\widehat{\mathcal{D}}^\theta_{B'\to E,\eta_0}$ and $\widehat{\mathcal{D}}^\theta_{B'\to E,\eta_0}$, respectively. We assume that any reader who has access to the memory device (reading port) transmits a tensor product $(\Phi^+)^{\otimes N}$ of N maximally entangled states $\Phi^+_{RB'}$. During useful reading, the reader's output state is $\omega_{R^N B^N} = (q\omega^\theta_{RB,\eta_1} + (1-q)\omega^\theta_{RB,\eta_0})^{\otimes N}$, where $\omega^\theta_{RBE,\eta_x} := U^{\mathcal{D}^\theta_{\eta_x}}_{RB'\to RBE}(\Phi^+_{RB'})(U^{\mathcal{D}^\theta_{\eta_x}}_{RB'\to RBE})^\dagger$. When the memory device is blank, the output state is $\omega^0_{R^N B^N E^N} = (\omega^\theta_{RBE,\eta_0})^{\otimes N}$, where $R^N B^N$ is accessible only at the reading port for Bob or Oscar and E^N is accessible only to Walter.

The security criterion for non-adaptive incognito reading reduces to $D_I := D(\omega_{RB}\|\omega^0_{RB}) \le \frac{\delta_I}{N}$, and for non-adaptive covert reading it reduces to $D_C := D(\omega_E\|\omega^0_E) \le \frac{\delta_C}{N}$. For given strategies, it turns out that $D_I = D_C$.
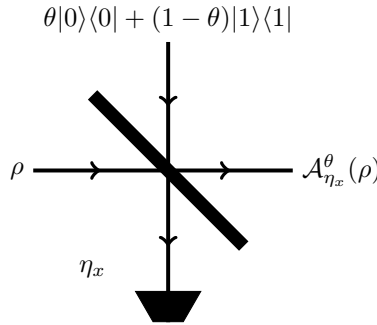

$$\theta|0\rangle\langle 0| + (1-\theta)|1\rangle\langle 1|$$

$$\rho \longrightarrow \qquad \longrightarrow \mathcal{A}^\theta_{\eta_x}(\rho)$$

$$\eta_x$$

Figure 7.3. The generalized amplitude damping channel as an interaction of the input signal ρ with a beamsplitter of transmissivity η_x followed by discarding the state of the environment. The parameter θ quantifies the noise of the reading environment.

Example 1. Consider a binary memory cell $\{\mathcal{A}^\theta_{\eta_x}\}_{x\in\{0,1\}}$ consisting of two generalized damping channels, where $\mathcal{A}^\theta_{B'\to B,\eta_x}$ acts on qubits and is defined as $\mathcal{A}^\theta_{B'\to B,\eta_x}(\cdot) = \sum_{i=1}^4 E_i(\cdot)E_i^\dagger$, where $\theta, \eta \in [0,1]$ and

$$E_1 = \sqrt{\theta}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\eta_x} \end{pmatrix}, \quad E_2 = \sqrt{\theta}\begin{pmatrix} 0 & \sqrt{1-\eta_x} \\ 0 & 0 \end{pmatrix},$$

$$E_3 = \sqrt{1-\theta}\begin{pmatrix} \sqrt{\eta_x} & 0 \\ 0 & 1 \end{pmatrix}, \quad E_4 = \sqrt{1-\theta}\begin{pmatrix} 0 & 0 \\ \sqrt{1-\eta_x} & 0 \end{pmatrix}.$$
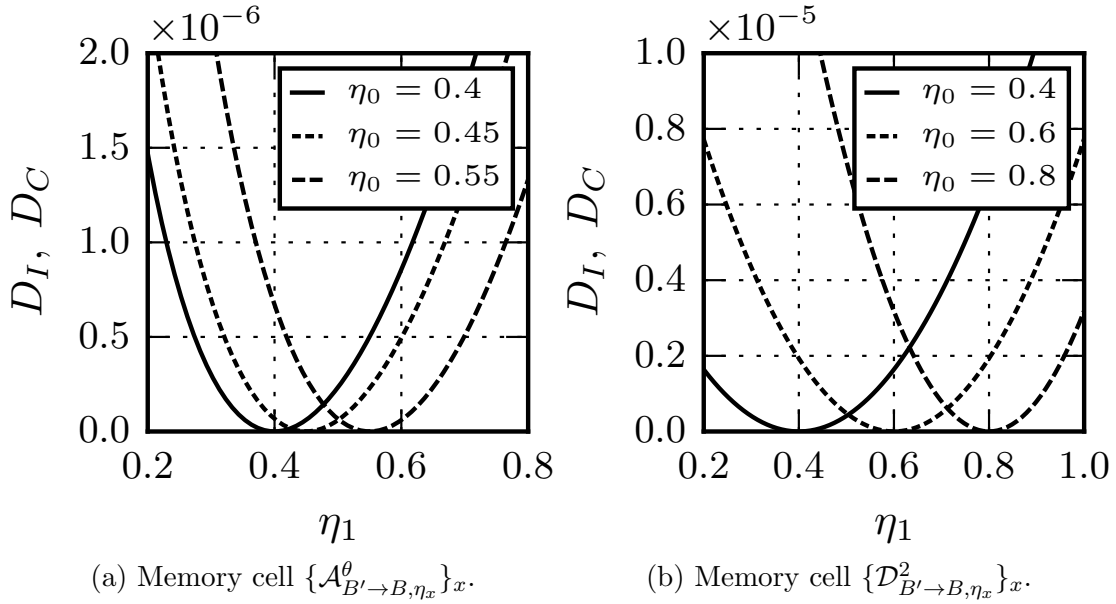
(a) Memory cell $\{\mathcal{A}^\theta_{B'\to B,\eta_x}\}_x$.

(b) Memory cell $\{\mathcal{D}^2_{B'\to B,\eta_x}\}_x$.

Figure 7.4. Values of the relative entropy on the left-hand side of (7.12),(7.14) corresponding to the security parameter δ_I, δ_C for incognito and covert reading, respectively, when the input is restricted to the maximally entangled state. (a) Memory cell $\{\mathcal{A}^\theta_{B'\to B,\eta_x}\}_x$ with $q = 0.005$, $\theta = 0.5$. (b) Memory cell $\{\mathcal{D}^2_{B'\to B,\eta_x}\}_x$ with $q = 0.005$ and $d = 2$.

The generalized amplitude damping channel can be viewed as an interaction of the input signal with a qubit environment by means of a beamsplitter, followed by discarding the state of the environment. The parameter θ corresponds to the noise injected by the environment when the memory is being read and may be intrinsic to the memory reading device.

If we let $N = 1000$, $\eta_0 = 0.45$, $\eta_1 = 0.4$, and $\theta = 0.5$, then we can send on average 5 non-innocent channels corresponding to secure information can be encoded with security parameter $\delta_I, \delta_C = 7 \times 10^{-5}$; see Fig. 7.4.

Example 2. Consider memory cell $\{\mathcal{D}^d_{B'\to B,\eta_x}\}_{x\in\{0,1\}}$ consisting of two qudit depolarizing channels, where $\mathcal{D}^d_{B'\to B,\eta_x}(\rho) = \eta_x\rho + (1-\eta_x)\frac{1}{d}$, and $\eta_x \in \left[0, \frac{d^2}{d^2-1}\right]$. Parameter $1 - \eta_x$ depends on the deviation of the channel $\mathcal{D}_{B'\to B,\eta_x}$ from any unitary evolution [31, Proposition 11]. In this case, the security criterion for non-adaptive incognito reading is

$$\lambda_1^\omega \log_2\left(\frac{\lambda_1^\omega}{\lambda_1^{\omega^0}}\right) + (d^2 - 1)\lambda_2^\omega \log_2\left(\frac{\lambda_2^\omega}{\lambda_2^{\omega^0}}\right) \leq \frac{\delta_I}{N}, \tag{7.16}$$

where $\{\lambda_i^\rho\}_i$ denotes the spectrum of the state ρ and

$$\lambda_1^{\omega^0} = \eta_0 + \frac{1-\eta_0}{d^2}, \qquad\qquad \lambda_1^\omega = (q\eta_1 + (1-q)\eta_0) + \frac{1}{d^2}(q(1-\eta_1) + (1-q)(1-\eta_0)),$$
$$\lambda_2^{\omega^0} = \frac{1-\eta_0}{d^2}, \qquad\qquad \lambda_2^\omega = \frac{1}{d^2}(q(1-\eta_1) + (1-q)(1-\eta_0)).$$

If we let $d = 2$, $N = 1000$, $q = 0.005$, $\eta_0 = 0.8$, and $\eta_1 = 0.7$ or $\eta_1 = 0.9$, then we can send on average 5 non-innocent channels corresponding to secure information with security parameter $\delta_I, \delta_C = 8.5 \times 10^{-4}$; see Fig. 7.4.

7.4 Threat level identification

Our protocol for non-adaptive incognito reading can be applied to threat level identification (TLI), in which the messages $m \in \mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$ correspond to the threat level posed by an adversary, Oscar. A friendly aircraft, to be used as a spy for stealthy surveillance, can be embedded with a memory device and share a secret key with the friendly base. Since Oscar does not have the key, it will not be able to identify the aircraft as being a spy. The aircraft can thus collect information about Oscar's base and report back to its headquarter with a message indicating the threat level. Non-adaptive incognito reading protocols are natural in this context since the memory device and the reader are at distant locations and scout situations, which are time sensitive, may not allow enough time to execute adaptive protocols.

Open problems

For future work, it would be interesting to explore the task of secure reading when the memory cell consists of channels acting on continuous variable systems [25, 27]. Since reading protocols are based on channel discrimination and there are connections between parmameter estimation in metrology, process tomography, and channel discrimination, another future direction is to study the possibility of some new secure parameter estimation protocols in the context of metrology and sensing [20, 255, 256] (see also [257–259] for the literature on secure parameter estimation).

References

[1] P. A. M. Dirac, *The Principles of Quantum Mechanics, Fourth Edition.* International series of monographs on physics 27, Clarendon Press, 1981.

[2] J. J. Sakurai and E. D. Commins, *Modern Quantum Mechanics, Revised Edition*, vol. 63. American Association of Physics Teachers (AAPT), January 1995.

[3] W. Gerlach and O. Stern, "Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld," *Zeitschrift für Physik*, vol. 9, pp. 349–352, December 1922.

[4] W. Gerlach and O. Stern, "Der experimentelle Nachweis des magnetischen Moments des Silberatoms," *Zeitschrift für Physik*, vol. 8, pp. 110–111, December 1922.

[5] W. Heisenberg, "über den anschaulichen inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift für Physik*, vol. 43, pp. 172–198, March 1927.

[6] J. S. Bell and A. Aspect, *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, 2004.

[7] D. Home, D. Saha, and S. Das, "Multipartite Bell-type inequality by generalizing Wigner's argument," *Physical Review A*, vol. 91, p. 012102, January 2015. arXiv:1410.7936.

[8] S. Das, S. Aravinda, R. Srikanth, and D. Home, "Unification of Bell, Leggett-Garg and Kochen-Specker inequalities: Hybrid spatio-temporal inequalities," *EPL (Europhysics Letters)*, vol. 104, no. 6, p. 60006, 2013. arXiv:1308.0270.

[9] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, "Entropic uncertainty relations and their applications," *Reviews of Modern Physics*, vol. 89, p. 015002, February 2017. arXiv:1511.04857v2.

[10] C. H. Bennett, "Notes on landauer's principle, reversible computation, and maxwell's demon," *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, vol. 34, no. 3, pp. 501 – 510, 2003. Quantum Information and Computation.

[11] J. D. Bekenstein, "Universal upper bound on the entropy-to-energy ratio for bounded systems," *Physical Review D*, vol. 23, pp. 287–298, January 1981.

[12] R. Bousso, "The holographic principle," *Reviews of Modern Physics*, vol. 74, pp. 825–874, August 2002. arXiv:hep-th/0203101.

[13] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of Physics*, vol. 1, pp. 23–33, March 1970.

[14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, October 1982.

[15] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, pp. 271–272, November 1982.

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing, IEEE, 1984*, pp. 175–179, 1984.

[17] R. Renner, *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich, December 2005. arXiv:quant-ph/0512258.

[18] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, pp. 1895–1899, March 1993.

[19] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, "Criteria for continuous-variable quantum teleportation," *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 267–278, 2000.

[20] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Reviews of Modern Physics*, vol. 89, July 2017. arXiv:1611.02427.

[21] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2000.

[22] A. Rivas and S. F. Huelga, *Open Quantum Systems: An Introduction*. SpringerBriefs in Physics, Springer Berlin Heidelberg, 2011.

[23] M. M. Wilde, *Quantum Information Theory, Second Edition*. Cambridge University Press, 2017. arXiv:1106.1445v7.

[24] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, July 1948.

[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, second ed., 2006.

[26] J. Watrous, *Theory of Quantum Information*. 2015. Available at `https://cs.uwaterloo.ca/~watrous/TQI/`.

[27] A. S. Holevo, *Quantum systems, channels, information: A mathematical introduction*, vol. 16. Walter de Gruyter, 2012.

[28] J. von Neumann, *Mathematische grundlagen der quantenmechanik*. Verlag von Julius Springer Berlin, 1932.

[29] E. Schrödinger, "Discussion of probability relations between separated systems," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, p. 555563, October 1935.

[30] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, pp. 777–780, May 1935.

[31] S. Das, S. Bäuml, and M. M. Wilde, "Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices," December 2017. arXiv:1712.00827.

[32] S. Das, S. Khatri, G. Siopsis, and M. M. Wilde, "Fundamental limits on quantum dynamics based on entropy change," *Journal of Mathematical Physics*, vol. 59, p. 012205, January 2018. arXiv:1707.06584.

[33] F. Buscemi, S. Das, and M. M. Wilde, "Approximate reversibility in the context of entropy gain, information gain, and complete positivity," *Physical Review A*, vol. 93, p. 062314, June 2016. arXiv:1601.01207v3.

[34] S. Das and M. M. Wilde, "Quantum reading capacity: General definition and bounds," March 2017. arXiv:1703.03706.

[35] M. Srednicki, "Entropy and area," *Physical Review Letters*, vol. 71, pp. 666–669, August 1993.

[36] M. Christandl and A. Winter, ""Squashed entanglement": An additive entanglement measure," *Journal of Mathematical Physics*, vol. 45, pp. 829–840, March 2004. arXiv:quant-ph/0308088.

[37] L. J. Rogers, "An extension of a certain theorem in inequalities," *Messenger of Mathematics*, vol. XVII, pp. 145–150, February 1888.

[38] O. Hölder, "Ueber einen mittelwerthabsatz," *Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universitt zu Göttingen*, vol. 1889, pp. 38–47, 1889.

[39] R. Bhatia, *Matrix Analysis*. Springer New York, 1997.

[40] M. M. Wolf, "Quantum channels & operations: Guided tour," 2012. Notes available at https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf.

[41] W. F. Stinespring, "Positive functions on C*-algebras," *Proceedings of the American Mathematical Society*, vol. 6, pp. 211–216, 1955.

[42] G. T. Horowitz and J. Maldacena, "The black hole final state," *Journal of High Energy Physics*, vol. 2004, pp. 008–008, February 2004. arXiv:hep-th/0310281.

[43] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Physics Letters A*, vol. 223, pp. 1–8, November 1996. arXiv:quant-ph/9605038.

[44] A. Peres, "Separability criterion for density matrices," *Physical Review Letters*, vol. 77, pp. 1413–1415, August 1996. arXiv:quant-ph/9604005.

[45] K. Audenaert, B. De Moor, K. G. H. Vollbrecht, and R. F. Werner, "Asymptotic relative entropy of entanglement for orthogonally invariant states," *Physical Review A*, vol. 66, p. 032310, September 2002. arXiv:quant-ph/0204143.

[46] E. M. Rains, "Bound on distillable entanglement," *Physical Review A*, vol. 60, pp. 179–184, July 1999. arXiv:quant-ph/9809082.

[47] E. M. Rains, "A semidefinite program for distillable entanglement," *IEEE Transactions on Information Theory*, vol. 47, pp. 2921–2933, November 2001. arXiv:quant-ph/0008047.

[48] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, "Entangling operations and their implementation using a small amount of entanglement," *Physical Review Letters*, vol. 86, pp. 544–547, January 2001. arXiv:quant-ph/0007057.

[49] A. S. Holevo, "Remarks on the classical capacity of quantum channel," December 2002. quant-ph/0212025.

[50] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, pp. 3824–3851, November 1996. arXiv:quant-ph/9604024.

[51] M. Horodecki, P. Horodecki, and R. Horodecki, "General teleportation channel, singlet fraction, and quasidistillation," *Physical Review A*, vol. 60, pp. 1888–1898, September 1999. arXiv:quant-ph/9807091.

[52] R. F. Werner, "All teleportation and dense coding schemes," *Journal of Physics A: Mathematical and General*, vol. 34, p. 7081, August 2001. arXiv:quant-ph/0003070.

[53] G. Chiribella, G. M. DAriano, and P. Perinotti, "Realization schemes for quantum instruments in finite dimensions," *Journal of Mathematical Physics*, vol. 50, p. 042101, April 2009. arXiv:0810.3211.

[54] E. Kaur and M. M. Wilde, "Amortized entanglement of a quantum channel and approximately teleportation-simulable channels," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, p. 035303, December 2017. arXiv:1707.07721.

[55] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Physical Review A*, vol. 54, pp. 2629–2635, October 1996. arXiv:quant-ph/9604022.

[56] H. Umegaki, "Conditional expectations in an operator algebra, IV (entropy and information)," *Kodai Mathematical Seminar Reports*, vol. 14, pp. 59–85, June 1962.

[57] A. Mueller-Hermes and D. Reeb, "Monotonicity of the quantum relative entropy under positive maps," *Annales Henri Poincaré*, vol. 18, pp. 1777–1788, January 2017. arXiv:1512.06117.

[58] G. Lindblad, "Completely positive maps and entropy inequalities," *Communications in Mathematical Physics*, vol. 40, pp. 147–151, June 1975.

[59] E. H. Lieb and M. B. Ruskai, "Proof of the strong subadditivity of quantum-mechanical entropy," *Journal of Mathematical Physics*, vol. 14, pp. 1938–1941, December 1973.

[60] E. H. Lieb and M. B. Ruskai, "A fundamental property of quantum-mechanical entropy," *Physical Review Letters*, vol. 30, pp. 434–436, March 1973.

[61] R. Alicki and M. Fannes, "Continuity of quantum conditional information," *Journal of Physics A: Mathematical and General*, vol. 37, pp. L55–L57, February 2004. arXiv:quant-ph/0312081.

[62] A. Winter, "Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints," *Communications in Mathematical Physics*, vol. 347, pp. 291–313, October 2016. arXiv:1507.07775.

[63] Y. Polyanskiy and S. Verdú, "Arimoto channel coding converse and Rényi divergence," in *Proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computation*, pp. 1327–1333, September 2010.

[64] N. Sharma and N. A. Warsi, "On the strong converses for the quantum channel capacity theorems," May 2012. arXiv:1205.1712.

[65] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy," *Communications in Mathematical Physics*, vol. 331, pp. 593–622, October 2014. arXiv:1306.1586.

[66] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: a new definition and some properties," *Journal of Mathematical Physics*, vol. 54, p. 122203, December 2013. arXiv:1306.3142.

[67] R. L. Frank and E. H. Lieb, "Monotonicity of a relative Rényi entropy," *Journal of Mathematical Physics*, vol. 54, p. 122201, December 2013. arXiv:1306.5358.

[68] S. Beigi, "Sandwiched Rényi divergence satisfies data processing inequality," *Journal of Mathematical Physics*, vol. 54, p. 122202, December 2013. arXiv:1306.5920.

[69] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, pp. 2816–2826, June 2009. arXiv:0803.2770.

[70] N. Datta, "Max-relative entropy of entanglement, alias log robustness," *International Journal of Quantum Information*, vol. 7, pp. 475–491, January 2009. arXiv:0807.2536.

[71] M. Gupta and M. M. Wilde, "Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity," *Communications in Mathematical Physics*, vol. 334, pp. 867–887, March 2015. arXiv:1310.7028.

[72] F. Buscemi and N. Datta, "The quantum capacity of channels with arbitrarily correlated noise," *IEEE Transactions on Information Theory*, vol. 56, pp. 1447–1460, March 2010. arXiv:0902.0158.

[73] L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Physical Review Letters*, vol. 108, no. 20, p. 200501, 2012. arXiv:1007.5456.

[74] M. Christandl and A. Müller-Hermes, "Relative entropy bounds on quantum, private and repeater capacities," *Communications in Mathematical Physics*, vol. 353, pp. 821–852, July 2017. arXiv:1604.03448.

[75] A. Uhlmann, "The "transition probability" in the state space of a *-algebra," *Reports on Mathematical Physics*, vol. 9, no. 2, pp. 273–279, 1976.

[76] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory*, vol. 45, pp. 1216–1227, May 1999. arXiv:quant-ph/9712042.

[77] M. Ohya and D. Petz, *Quantum Entropy and Its Use.* Springer, 1993.

[78] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical Review Letters*, vol. 94, p. 160502, April 2005. arXiv:quant-ph/0309110.

[79] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "General paradigm for distilling classical key from quantum states," *IEEE Transactions on Information Theory*, vol. 55, pp. 1898–1929, April 2009. arXiv:quant-ph/0506189.

[80] M. M. Wilde, M. Tomamichel, and M. Berta, "Converse bounds for private communication over quantum channels," *IEEE Transactions on Information Theory*, vol. 63, pp. 1792–1817, March 2017. arXiv:1602.08898.

[81] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Review of Modern Physics*, vol. 81, pp. 865–942, June 2009. arXiv:quant-ph/0702225.

[82] M. Horodecki and P. Horodecki, "Reduction criterion of separability and limits for a class of distillation protocols," *Physical Review A*, vol. 59, pp. 4206–4216, June 1999. arXiv:quant-ph/9708015.

[83] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of very noisy mixed states and implications for NMR quantum computing," *Physical Review Letters*, vol. 83, pp. 1054–1057, August 1999. arXiv:quant-ph/9811018.

[84] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, "On the capacities of bipartite Hamiltonians and unitary gates," *IEEE Transactions on Information Theory*, vol. 49, pp. 1895–1911, August 2003. arXiv:quant-ph/0205057.

[85] M. S. Leifer, L. Henderson, and N. Linden, "Optimal entanglement generation from quantum operations," *Physical Review A*, vol. 67, p. 012306, January 2003. arXiv:quant-ph/0205055.

[86] K. Ben Dana, M. García Díaz, M. Mejatty, and A. Winter, "Resource theory of coherence: Beyond states," *Physical Review A*, vol. 95, p. 062327, June 2017. arXiv:1704.03710.

[87] L. Rigovacca, G. Kato, S. Bäuml, M. Kim, W. J. Munro, and K. Azuma, "Versatile relative entropy bounds for quantum networks," *New Journal of Physics*, vol. 20, p. 013033, January 2018. arXiv:1707.05543.

[88] M. Tomamichel, M. M. Wilde, and A. Winter, "Strong converse rates for quantum communication," *IEEE Transactions on Information Theory*, vol. 63, pp. 715–727, January 2017. arXiv:1406.2946.

[89] X. Wang and R. Duan, "A semidefinite programming upper bound of quantum capacity," in *2016 IEEE International Symposium on Information Theory (ISIT)*, IEEE, July 2016. arXiv:1601.06888.

[90] X. Wang, K. Fang, and R. Duan, "Semidefinite programming converse bounds for quantum communication," September 2017. arXiv:1709.00200.

[91] M. Berta and M. M. Wilde, "Amortization does not enhance the max-rains information of a quantum channel," *New Journal of Physics*, vol. 20, p. 053044, May 2018. arXiv:1709.00200.

[92] X. Wang and R. Duan, "Improved semidefinite programming upper bound on distillable entanglement," *Physical Review A*, vol. 94, p. 050301, November 2016. arXiv:1601.07940.

[93] V. Vedral and M. B. Plenio, "Entanglement measures and purification procedures," *Physical Review A*, vol. 57, pp. 1619–1633, March 1998. arXiv:quant-ph/9707035.

[94] R. R. Tucci, "Quantum entanglement and conditional information transmission," September 1999. arXiv: quant-ph/9909041.

[95] R. R. Tucci, "Entanglement of distillation and conditional mutual information," Februrary 2002. arXiv:quant-ph/0202144.

[96] M. Takeoka, S. Guha, and M. M. Wilde, "The squashed entanglement of a quantum channel," *IEEE Transactions on Information Theory*, vol. 60, pp. 4987–4998, August 2014. arXiv:1310.0129.

[97] M. E. Shirokov, "Squashed entanglement in infinite dimensions," *Journal of Mathematical Physics*, vol. 57, p. 032203, March 2016. arXiv:1507.08964.

[98] M. B. Plenio and S. Virmani, "An introduction to entanglement measures," *Quantum Information & Computation*, vol. 7, pp. 1–51, January 2007. arXiv:quant-ph/0504163.

[99] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, August 2018. arXiv:1801.00862v3.

[100] E. Kaur, S. Das, M. M. Wilde, and A. Winter, "Extendibility limits the performance of quantum processors," March 2018. arXiv:1803.10710.

[101] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Physical Review A*, vol. 53, pp. 2046–2052, April 1996. arXiv:quant-ph/9511030.

[102] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, pp. 722–725, January 1997. arXiv:quant-ph/9511027.

[103] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, pp. 44–55, January 2005. arXiv:quant-ph/0304127.

[104] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, pp. 207–235, January 2005. arXiv:quant-ph/0306078.

[105] C. E. Shannon, "Two-way communication channels," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, (Berkeley, California), pp. 611–644, University of California Press, 1961.

[106] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, "Conditional quantum dynamics and logic gates," *Physical Review Letters*, vol. 74, pp. 4083–4086, May 1995. arXiv:quant-ph/9503017.

[107] P. Zanardi, C. Zalka, and L. Faoro, "Entangling power of quantum evolutions," *Physical Review A*, vol. 62, p. 030301, August 2000. arXiv:quant-ph/0005031.

[108] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, "Optimal local implementation of nonlocal quantum gates," *Physical Review A*, vol. 62, p. 052317, October 2000. arXiv:quant-ph/0005101.

[109] S. Bose, L. Rallan, and V. Vedral, "Communication capacity of quantum computation," *Physical Review Letters*, vol. 85, pp. 5448–5451, December 2000. arXiv:quant-ph/0003072.

[110] D. Collins, N. Linden, and S. Popescu, "Nonlocal content of quantum operations," *Physical Review A*, vol. 64, p. 032302, August 2001. arXiv:quant-ph/0005102.

[111] A. M. Childs, D. W. Leung, and G. Vidal, "Reversible simulation of bipartite product Hamiltonians," *IEEE Transactions on Information Theory*, vol. 50, pp. 1189–1197, June 2004. arXiv:quant-ph/0303097.

[112] B. Jonnadula, P. Mandayam, K. Życzkowski, and A. Lakshminarayan, "Impact of local dynamics on entangling power," *Physical Review A*, vol. 95, p. 040302, April 2017. arXiv:1611.00479.

[113] S. Das, G. Siopsis, and C. Weedbrook, "Continuous-variable quantum Gaussian process regression and quantum singular value decomposition of non-sparse low rank matrices," *Physical Review A*, vol. 97, p. 022315, February 2018. arXiv:1707.00360.

[114] Y. Sekino and L. Susskind, "Fast scramblers," *Journal of High Energy Physics*, vol. 2008, p. 065, October 2008. arXiv:0808.2096.

[115] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, "Chaos in quantum channels," *Journal of High Energy Physics*, vol. 2016, February 2016. arXiv:1511.04021.

[116] D. Ding, P. Hayden, and M. Walter, "Conditional mutual information of bipartite unitaries and scrambling," *Journal of High Energy Physics*, vol. 2016, December 2016. arXiv:1608.04750.

[117] P. Hayden and J. Preskill, "Black holes as mirrors: quantum information in random subsystems," *Journal of High Energy Physics*, vol. 2007, pp. 120–120, September 2007. arXiv:0708.4025.

[118] S. W. Hawking, "Breakdown of predictability in gravitational collapse," *Physical Review D*, vol. 14, pp. 2460–2473, November 1976.

[119] A. M. Childs, D. W. Leung, and H.-K. Lo, "Two-way quantum communication channels," *International Journal of Quantum Information*, vol. 04, pp. 63–83, February 2006. arXiv:quant-ph/0506039.

[120] S. Bravyi, "Upper bounds on entangling rates of bipartite Hamiltonians," *Physical Review A*, vol. 76, p. 052319, November 2007. arXiv:0704.0964.

[121] N. Linden, J. A. Smolin, and A. Winter, "Entangling and disentangling power of unitary transformations are not equal," *Physical Review Letters*, vol. 103, p. 030501, July 2009. arXiv:quant-ph/0511217.

[122] E. Wakakuwa, A. Soeda, and M. Murao, "A coding theorem for bipartite unitaries in distributed quantum computation," *IEEE Transactions on Information Theory*, vol. 63, pp. 5372–5403, August 2017. arXiv:1505.04352.

[123] L. Chen and L. Yu, "Entangling and assisted entangling power of bipartite unitary operations," *Physical Review A*, vol. 94, p. 022307, August 2016. arXiv:1604.05788.

[124] T. Eggeling, K. Vollbrecht, R. Werner, and M. Wolf, "Distillability via protocols respecting the positivity of partial transpose," *Physical Review Letters*, vol. 87, November 2001. arXiv:quant-ph/0104095.

[125] G. M. D'Ariano and P. Perinotti, "Programmable quantum channels and measurements," October 2005. arXiv quant-ph/0510033.

[126] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, "Parameter estimation of quantum channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 5172–5185, November 2008. arXiv:quant-ph/0610060.

[127] R. Demkowicz-Dobrzański and L. Maccone, "Using entanglement against noise in quantum metrology," *Physical Review Letters*, vol. 113, p. 250801, December 2014. arXiv:1407.2934.

[128] T. Fritz, "Resource convertibility and ordered commutative monoids," *Mathematical Structures in Computer Science*, vol. 27, pp. 850–938, October 2015. arXiv:1504.03661.

[129] F. G. Brandão and G. Gour, "Reversible framework for quantum resource theories," *Physical Review Letters*, vol. 115, p. 070503, August 2015. arXiv:1502.03149.

[130] A. Soeda, P. S. Turner, and M. Murao, "Entanglement cost of implementing controlled-unitary operations," *Physical Review Letters*, vol. 107, p. 180501, October 2011. arXiv:1008.1128.

[131] D. Gottesman, "The Heisenberg representation of quantum computers," in *Group Theoretical Methods in Physics: Proceedings* (P. D. J. S. P. Corney, Robert Delbourgo, ed.), 22, Cambridge, USA: International Press, July 1999. arXiv:quant-ph/9807006.

[132] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, November 1999. arXiv:quant-ph/9908010.

[133] M. A. Nielsen and I. L. Chuang, "Programmable quantum gate arrays," *Physical Review Letters*, vol. 79, pp. 321–324, July 1997. arXiv:quant-ph/9703032.

[134] W. Dür, M. J. Bremner, and H. J. Briegel, "Quantum simulation of interacting high-dimensional systems: The influence of noise," *Physical Review A*, vol. 78, p. 052325, November 2008. arXiv:0706.0154.

[135] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," *IEEE 41st Annual Symposium on Foundations of Computer Science*, pp. 547–553, November 2000. arXiv:quant-ph/0003101.

[136] S. R. De Groot and P. Mazur, *Non-equilibrium thermodynamics*. North-Holland Publishing Company, Amsterdam, 1962.

[137] J. D. Bekenstein, "Black holes and entropy," *Physical Review D*, vol. 7, pp. 2333–2346, April 1973.

[138] S. Carnot, "Reflections on the motive power of fire, and on machines fitted to develop that power," *Paris: Bachelier*, 1824.

[139] E. Mendoza, *Reflections on the motive power of fire by Sadi Carnot and other papers on the Second Law of thermodynamics by E. Clapeyron and R. Clausius.* Dover Publications New York, 1960.

[140] P. Attard, *Non-equilibrium thermodynamics and statistical mechanics: Foundations and applications.* Oxford University Press, 2012.

[141] I. I. Hirschman, "A note on entropy," *American Journal of Mathematics*, vol. 79, no. 1, pp. 152–156, 1957.

[142] W. Beckner, "Inequalities in Fourier analysis," *Annals of Mathematics*, vol. 102, no. 1, pp. 159–182, 1975.

[143] I. Białynicki-Birula and J. Mycielski, "Uncertainty relations for information entropy in wave mechanics," *Communications in Mathematical Physics*, vol. 44, pp. 129–132, June 1975.

[144] H. Maassen and J. B. M. Uffink, "Generalized entropic uncertainty relations," *Physical Review Letters*, vol. 60, pp. 1103–1106, March 1988.

[145] J. M. Bardeen, B. Carter, and S. W. Hawking, "The four laws of black hole mechanics," *Communications in Mathematical Physics*, vol. 31, pp. 161–170, June 1973.

[146] L. Bombelli, R. K. Koul, J. Lee, and R. D. Sorkin, "Quantum source of entropy for black holes," *Physical Review D*, vol. 34, pp. 373–383, July 1986.

[147] J. Eisert, M. Cramer, and M. B. Plenio, "Colloquium," *Reviews of Modern Physics*, vol. 82, pp. 277–306, February 2010. arXiv:0808.3773v4.

[148] H. Carmichael, *An open systems approach to quantum optics: lectures presented at the Université Libre de Bruxelles, October 28 to November 4, 1991*, vol. 18. Springer Science & Business Media, 2009.

[149] U. Weiss, *Quantum dissipative systems*, vol. 13. World scientific, fourth ed., 2012.

[150] P. M. Alberti and A. Uhlmann, "The order structure of states in C*-and W*-algebras," in *International Conference on Operator Algebras, Ideals, and their Applications in Theoretical Physics*, pp. 126–135, Leipzig: Teubner, BSB, September 1978.

[151] P. M. Alberti and A. Uhlmann, *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing.* Mathematics and Its Applications, Springer Netherlands, 1982.

[152] R. F. Streater, "Convergence of the quantum Boltzmann map," *Communications in Mathematical Physics*, vol. 98, no. 2, pp. 177–185, 1985.

[153] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems.* Oxford University Press, 2002.

[154] D. Chruściński and A. Kossakowski, "Markovianity criteria for quantum evolution," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 45, p. 154002, July 2012. arXiv:1201.5987v1.

[155] A. Müller-Hermes, D. S. Frana, and M. M. Wolf, "Entropy production of doubly stochastic quantum channels," *Journal of Mathematical Physics*, vol. 57, no. 2, p. 022203, 2016. arXiv:1505.04678.

[156] A. M. Alhambra and M. P. Woods, "Dynamical maps, quantum detailed balance, and the Petz recovery map," *Physical Review A*, vol. 96, p. 022118, August 2017. arXiv:1609.07496v4.

[157] K. Życzkowski, P. Horodecki, M. Horodecki, and R. Horodecki, "Dynamics of quantum entanglement," *Physical Review A*, vol. 65, p. 012101, December 2001.

[158] H. Spohn, "Entropy production for quantum dynamical semigroups," *Journal of Mathematical Physics*, vol. 19, no. 5, pp. 1227–1230, 1978.

[159] R. König and G. Smith, "The entropy power inequality for quantum systems," *IEEE Transactions on Information Theory*, vol. 60, pp. 1536–1548, March 2014. arXiv:1205.3409.

[160] N. Datta, Y. Pautrat, and C. Rouzé, "Contractivity properties of a quantum diffusion semigroup," *Journal of Mathematical Physics*, vol. 58, p. 012205, January 2017. arXiv:1607.04242.

[161] H.-P. Breuer, E.-M. Laine, and J. Piilo, "Measure for the degree of non-Markovian behavior of quantum processes in open systems," *Physical Review Letters*, vol. 103, p. 210401, November 2009. arXiv:0908.0238.

[162] V. Baccetti and M. Visser, "Infinite Shannon entropy," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2013, p. P04010, April 2013. arXiv:1212.5630.

[163] H. Falk, "Inequalities of J. W. Gibbs," *American Journal of Physics*, vol. 38, no. 7, pp. 858–869, 1970.

[164] G. Lindblad, "Entropy, information and quantum measurements," *Communications in Mathematical Physics*, vol. 33, pp. 305–322, December 1973.

[165] M. A. Nielsen, "An introduction to majorization and its applications to quantum mechanics," *Lecture Notes, Department of Physics, University of Queensland, Australia*, 2002.

[166] G. P. Beretta, "Nonlinear quantum evolution equations to model irreversible adiabatic relaxation with maximal entropy production and other nonunitary processes," *Reports on Mathematical Physics*, vol. 64, pp. 139 – 168, August 2009. arXiv:0907.1977.

[167] W. Rudin, *Principles of Mathematical Analysis*. International series in pure and applied mathematics, McGraw-Hill, 1976.

[168] W. K. Wootters, "Entanglement of formation and concurrence," *Quantum Information & Computation*, vol. 1, pp. 27–44, January 2001.

[169] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, "Quantifying entanglement," *Physical Review Letters*, vol. 78, pp. 2275–2279, March 1997. arXiv:quant-ph/9702027.

[170] T. J. Osborne and M. A. Nielsen, "Entanglement in a simple quantum phase transition," *Physical Review A*, vol. 66, p. 032110, September 2002. arXiv:quant-ph/0202162.

[171] A. Kossakowski, "On quantum statistical mechanics of non-Hamiltonian systems," *Reports on Mathematical Physics*, vol. 3, pp. 247 – 274, December 1972.

[172] R. Alicki and K. Lendi, *Quantum dynamical semigroups and applications.* Lectures Notes in Physics, Berlin: Springer, 2007.

[173] M. M. Wolf and J. I. Cirac, "Dividing quantum channels," *Communications in Mathematical Physics*, vol. 279, pp. 147–168, April 2008. arXiv:math-ph/0611057v3.

[174] A. Rivas, S. F. Huelga, and M. B. Plenio, "Quantum non-Markovianity: characterization, quantification and detection," *Reports on Progress in Physics*, vol. 77, p. 094001, August 2014. arXiv:1405.0303v2.

[175] A. Rivas, S. F. Huelga, and M. B. Plenio, "Entanglement and non-Markovianity of quantum evolutions," *Physical Review Letters*, vol. 105, p. 050403, July 2010. arXiv:0911.4270v2.

[176] V. Gorini, A. Kossakowski, and E. C. G. Sudarshan, "Completely positive dynamical semi-groups of N-level systems," *Journal of Mathematical Physics*, vol. 17, pp. 821–825, May 1976.

[177] G. Lindblad, "On the generators of quantum dynamical semigroups," *Communications in Mathematical Physics*, vol. 48, pp. 119–130, June 1976.

[178] M. M. Wolf, J. Eisert, T. S. Cubitt, and J. I. Cirac, "Assessing non-Markovian quantum dynamics," *Physical Review Letters*, vol. 101, p. 150402, October 2008. arXiv:0711.3172v2.

[179] E.-M. Laine, J. Piilo, and H.-P. Breuer, "Measure for the non-Markovianity of quantum processes," *Physical Review A*, vol. 81, p. 062115, June 2010. arXiv:1002.2583v2.

[180] M. J. W. Hall, J. D. Cresser, L. Li, and E. Andersson, "Canonical form of master equations and characterization of non-Markovianity," *Physical Review A*, vol. 89, p. 042120, April 2014. arXiv:1009.0845v4.

[181] F. Benatti and H. Narnhofer, "Entropy behaviour under completely positive maps," *Letters in Mathematical Physics*, vol. 15, pp. 325–334, May 1988.

[182] C. Ou, R. V. Chamberlin, and S. Abe, "Lindbladian operators, von Neumann entropy and energy conservation in time-dependent quantum open systems," *Physica A: Statistical Mechanics and its Applications*, vol. 466, pp. 450 – 454, January 2017. arXiv:1601.07874v3.

[183] E. B. Davies, "Markovian master equations," *Communications in Mathematical Physics*, vol. 39, pp. 91–110, June 1974.

[184] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Communications in Mathematical Physics*, vol. 143, pp. 99–114, December 1991.

[185] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Transactions on Information Theory*, vol. 46, pp. 2428–2433, November 2000. arXiv:quant-ph/9906090v1.

[186] B. Bylicka, D. Chruściński, and S. Maniscalco, "Non-Markovianity and reservoir memory of quantum channels: a quantum information theory perspective," *Scientific Reports*, vol. 4, p. 5720, July 2014.

[187] T. Heinosaari, A. S. Holevo, and M. M. Wolf, "The semigroup structure of Gaussian channels," *Quantum Information and Computation*, vol. 10, pp. 619–635, July 2010. arXiv:0909.0408.

[188] V. Giovannetti, A. S. Holevo, S. Lloyd, and L. Maccone, "Generalized minimal output entropy conjecture for one-mode Gaussian channels: definitions and some exact results," *Journal of Physics A: Mathematical and Theoretical*, vol. 43, p. 415305, September 2010. arXiv:1004.4787v2.

[189] D. Chruściński and S. Maniscalco, "Degree of non-Markovianity of quantum evolution," *Physical Review Letters*, vol. 112, p. 120404, March 2014. arXiv:1311.4213v1.

[190] X.-M. Lu, X. Wang, and C. P. Sun, "Quantum Fisher information flow and non-Markovian processes of open systems," *Physical Review A*, vol. 82, p. 042103, October 2010. arXiv:0912.0587v5.

[191] S. Lorenzo, F. Plastina, and M. Paternostro, "Role of environmental correlations in the non-Markovian dynamics of a spin system," *Physical Review A*, vol. 84, p. 032124, September 2011. arXiv:1106.5447v1.

[192] S. Luo, S. Fu, and H. Song, "Quantifying non-Markovianity via correlations," *Physical Review A*, vol. 86, p. 044101, October 2012.

[193] W. Zhong, Z. Sun, J. Ma, X. Wang, and F. Nori, "Fisher information under decoherence in Bloch representation," *Physical Review A*, vol. 87, p. 022337, February 2013. arXiv:1212.0917v2.

[194] J. Liu, X.-M. Lu, and X. Wang, "Nonunital non-Markovianity of quantum dynamics," *Physical Review A*, vol. 87, p. 042103, April 2013. arXiv:1301.5763.

[195] S. Lorenzo, F. Plastina, and M. Paternostro, "Geometrical characterization of non-Markovianity," *Physical Review A*, vol. 88, p. 020102, August 2013. arXiv:1302.6673v1.

[196] S. Haseli, S. Salimi, and A. S. Khorashad, "A measure of non-Markovianity for unital quantum dynamical maps," *Quantum Information Processing*, vol. 14, pp. 3581–3594, September 2015. arXiv:1406.0180v4.

[197] C. Pineda, T. Gorin, D. Davalos, D. A. Wisniacki, and I. García-Mata, "Measuring and using non-Markovianity," *Physical Review A*, vol. 93, p. 022117, Feb 2016.

[198] A. Fujiwara, "Estimation of a generalized amplitude-damping channel," *Physical Review A*, vol. 70, p. 012317, July 2004.

[199] A. Nayak and P. Sen, "Invertible quantum operations and perfect encryption of quantum states," *Quantum Information and Computation*, vol. 7, pp. 103–110, January 2007. arXiv:quant-ph/0605041v4.

[200] F. Hiai, M. Ohya, and M. Tsukada, "Sufficiency, KMS condition and relative entropy in von Neumann algebras.," *Pacific Journal of Mathematics*, vol. 96, pp. 99–109, January 1981.

[201] O. Bratteli and D. W. Robinson, *Operator algebras and quantum statistical mechanics. Vol. 2: Equilibrium states. Models in quantum statistical mechanics.* Berlin, Germany: Springer, 1996.

[202] K. M. R. Audenaert and J. Eisert, "Continuity bounds on the quantum relative entropy," *Journal of Mathematical Physics*, vol. 46, p. 102104, October 2005. arXiv:quant-ph/0503218v3.

[203] K. M. R. Audenaert and J. Eisert, "Continuity bounds on the quantum relative entropy – II," *Journal of Mathematical Physics*, vol. 52, p. 112201, November 2011. arXiv:1105.2656v3.

[204] J. Wallman, C. Granade, R. Harper, and S. T. Flammia, "Estimating the coherence of noise," *New Journal of Physics*, vol. 17, p. 113020, November 2015. arXiv:1503.07865.

[205] P. Hayden, D. Leung, P. W. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," *Communications in Mathematical Physics*, vol. 250, pp. 371–391, September 2004. arXiv:quant-ph/0307104v3.

[206] G. Aubrun, "On almost randomizing channels with a short Kraus decomposition," *Communications in Mathematical Physics*, vol. 288, pp. 1103–1116, June 2009. arXiv:0805.2900.

[207] A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys*, vol. 52, pp. 1191–1249, December 1997.

[208] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, pp. 231–252, June 1969.

[209] C. W. Helstrom, *Quantum Detection and Estimation Theory.* Mathematics in Science and Engineering : a series of monographs and textbooks, Academic Press, 1976.

[210] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Physical Review Letters*, vol. 83, pp. 3081–3084, October 1999. arXiv:quant-ph/9904023.

[211] E. Magesan, J. M. Gambetta, and J. Emerson, "Characterizing quantum gates via randomized benchmarking," *Physical Review A*, vol. 85, p. 042311, Apr 2012.

[212] S. Pirandola, "Quantum reading of a classical digital memory," *Physical Review Letters*, vol. 106, p. 090504, March 2011. arXiv:1103.3478.

[213] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, "Quantum reading capacity," *New Journal of Physics*, vol. 13, p. 113012, November 2011. arXiv:1107.3500.

[214] S. Guha, Z. Dutton, R. Nair, J. Shapiro, and B. Yen, "Information capacity of quantum reading," in *Laser Science*, p. LTuF2, Optical Society of America, 2011.

[215] S. Guha and M. M. Wilde, "Polar coding to achieve the Holevo capacity of a pure-loss optical channel," in *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 546–550, IEEE, 2012. arXiv:1202.0533.

[216] M. M. Wilde, S. Guha, S.-H. Tan, and S. Lloyd, "Explicit capacity-achieving receivers for optical communication and quantum reading," in *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 551–555, IEEE, 2012. arXiv:1202.0518.

[217] C. Lupo and S. Pirandola, "Super-additivity and entanglement assistance in quantum reading," *Quantum Information and Computation*, vol. 17, pp. 0611–0622, June 2017. arXiv:1603.01433.

[218] G. M. D'Ariano, P. L. Presti, and M. G. A. Paris, "Using entanglement improves the precision of quantum measurements," *Physical Review Letters*, vol. 87, p. 270404, December 2001. arXiv:quant-ph/0109040.

[219] A. Acin, "Statistical distinguishability between unitary operations.," *Physical Review Letters*, vol. 87, p. 177901, October 2001. arXiv:quant-ph/0102064.

[220] G. Wang and M. Ying, "Unambiguous discrimination among quantum operations," *Physical Review A*, vol. 73, p. 042301, April 2006. arXiv:quant-ph/0512142.

[221] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, "Quantum illumination with Gaussian states," *Physical Review Letters*, vol. 101, p. 253601, December 2008. arXiv:0810.0534.

[222] R. Duan, Y. Feng, and M. Ying, "Perfect distinguishability of quantum operations," *Physical Review Letters*, vol. 103, p. 210501, November 2009. arXiv:0908.0119.

[223] T. Cooney, M. Mosonyi, and M. M. Wilde, "Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication," *Communications in Mathematical Physics*, vol. 344, pp. 797–829, June 2016. arXiv:1408.3373.

[224] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, "Adaptive versus nonadaptive strategies for quantum channel discrimination," *Physical Review A*, vol. 81, p. 032339, March 2010. arXiv:0909.0256.

[225] R. Duan, C. Guo, C.-K. Li, and Y. Li, "Parallel distinguishability of quantum operations," in *IEEE International Symposium on Information Theory (ISIT)*, pp. 2259–2263, 2016. arXiv:1605.02294.

[226] N. Datta and R. Renner, "Smooth Renyi entropies and the quantum information spectrum," *IEEE Transactions on Information Theory*, vol. 55, pp. 2807–2815, June 2009. arXiv:0801.0282.

[227] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, vol. 5. Springer, 2015. arXiv:1504.00233.

[228] A. Muller-Hermes, "Transposition in quantum information theory," Master's thesis, Technical University of Munich, September 2012.

[229] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, April 2017.

[230] M. Takeoka and M. M. Wilde, "Optimal estimation and discrimination of excess noise in thermal and amplifier channels," November 2016. arXiv:1611.09165.

[231] M. Tomamichel and V. Y. F. Tan, "Second-order asymptotics for the classical capacity of image-additive quantum channels," *Communications in Mathematical Physics*, vol. 338, pp. 103–137, May 2015. arXiv:1308.6503.

[232] D. Ding and M. M. Wilde, "Strong converse exponents for the feedback-assisted classical capacity of entanglement-breaking channels," vol. 54, pp. 1–19, January 2018. arXiv:1506.02228.

[233] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Review of Modern Physics*, vol. 79, pp. 135–174, January 2007. arXiv:quant-ph/0512071.

[234] E. A. Carlen, "Trace inequalities and quantum entropy: An introductory course," *Contemporary Mathematics*, vol. 529, pp. 73–140, 2010. Available at `www.ueltschi.org/AZschool/notes/EricCarlen.pdf`.

[235] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Transactions on Information Theory*, vol. 48, pp. 2637–2655, October 2002. arXiv:quant-ph/0106052.

[236] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Physical Review A*, vol. 56, p. 33, July 1997. arXiv:quant-ph/9610042.

[237] G. Adesso, S. Ragy, and A. R. Lee, "Continuous variable quantum information: Gaussian states and beyond," *Open Systems and Information Dynamics*, vol. 21, p. 1440001, June 2014. arXiv:1401.4679.

[238] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Feedback in the non-asymptotic regime," *IEEE Transactions on Information Theory*, vol. 57, pp. 4903–4925, August 2011.

[239] R. M. Fano, "Fano inequality," *Scholarpedia*, vol. 3, no. 10, p. 6648, 2008.

[240] M. M. Wilde, "Squashed entanglement and approximate private states," *Quantum Information Processing*, vol. 15, pp. 4563–4580, November 2016. arXiv:1606.08028.

[241] C. Morgan and A. Winter, ""Pretty strong" converse for the quantum capacity of degradable channels," *IEEE Transactions on Information Theory*, vol. 60, pp. 317–333, January 2014. arXiv:1301.4927.

[242] J. H. Shapiro, "Defeating passive eavesdropping with quantum illumination," *Physical Review A*, vol. 80, p. 022320, August 2009. arXiv:0904.2490.

[243] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates," *Physical Review A*, vol. 94, July 2016. arXiv:1510.08737.

[244] C. Miquel, J. P. Paz, M. Saraceno, E. Knill, R. Laflamme, and C. Negrevergne, "Interpretation of tomography and spectroscopy as dual forms of quantum computation," *Nature*, vol. 418, pp. 59–62, July 2002. arXiv:quant-ph/0109072.

[245] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," *Science*, vol. 321, no. 5895, pp. 1463–1465, 2008. arXiv:0803.2022.

[246] J. Yuen-Zhou and A. Aspuru-Guzik, "Quantum process tomography of excitonic dimers from two-dimensional electronic spectroscopy. i. general theory and application to homodimers," *The Journal of Chemical Physics*, vol. 134, p. 134505, April 2011. arXiv:1101.2716.

[247] L. Bowden, "The story of iff (identification friend or foe)," *IEE Proceedings A - Physical Science, Measurement and Instrumentation, Management and Education - Reviews*, vol. 132, pp. 435–437, October 1985.

[248] A. Chefles, "Unambiguous discrimination between linearly dependent states with multiple copies," *Physical Review A*, vol. 64, p. 062305, November 2001. arXiv:quant-ph/0105016.

[249] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, "Discriminating states: The quantum chernoff bound," *Physical Review Letters*, vol. 98, p. 160501, April 2007.

[250] R. Duan, Y. Feng, and M. Ying, "Entanglement is not necessary for perfect discrimination between unitary operations," *Physical Review Letters*, vol. 98, p. 100503, March 2007. arXiv:quant-ph/0601150.

[251] B. A. Shaw and T. A. Brun, "Quantum steganography with noisy quantum channels," *Physical Review A*, vol. 83, p. 022310, February 2011. arXiv:1006.1934.

[252] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," *Nature Communications*, vol. 6, p. 8626, October 2015.

[253] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, pp. 3493–3503, June 2016. arXiv:1506.03236.

[254] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, pp. 2334–2354, May 2016. arXiv:1503.08778.

[255] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[256] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum metrology," *Physical Review Letters*, vol. 96, p. 010401, January 2006. arXiv:quant-ph/0509179.

[257] G. Chiribella, L. Maccone, and P. Perinotti, "Secret quantum communication of a reference frame," *Physical Review Letters*, vol. 98, p. 120501, March 2007. arXiv:quant-ph/0608042.

[258] C. N. Gagatsos, B. A. Bash, S. Guha, and A. Datta, "Bounding the quantum limits of precision for phase estimation with loss and thermal noise," *Physical Review A*, vol. 96, p. 062306, Dec 2017. arXiv:1701.05518.

[259] Z. Huang, C. Macchiavello, and L. Maccone, "Cryptographic quantum metrology," 2017. arXiv:1706.03894.

[260] O. Fawzi, P. Hayden, I. Savov, P. Sen, and M. M. Wilde, "Classical communication over a quantum interference channel," *IEEE Transactions on Information Theory*, vol. 58, pp. 3670–3691, June 2012. arXiv:1102.2624.

[261] K. Audenaert, N. Datta, and M. Ozols, "Entropy power inequalities for qudits," *Journal of Mathematical Physics*, vol. 57, no. 5, p. 052202, 2016.

[262] R. König and G. Smith, "Limits on classical communication from quantum entropy power inequalities," *Nature Photonics*, vol. 7, no. 2, p. 142, 2013.

[263] G. M. Palma, K.-A. Suominen, and A. K. Ekert, "Quantum computers and dissipation," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 452, pp. 567–584, The Royal Society, 1996.

Appendix A   Qudit Systems and Heisenberg–Weyl Group

Here we introduce some basic notations and definitions related to qudit systems. A system represented with a d-dimensional Hilbert space is called a qu$d$it system. Let $J_{B'} = \{|j\rangle_{B'}\}_{j \in \{0,\dots,d-1\}}$ be a computational orthonormal basis of $\mathcal{H}_{B'}$ such that $\dim(\mathcal{H}_{B'}) = d$. There exists a unitary operator called *cyclic shift operator* $X(k)$ that acts on the orthonormal states as follows:

$$\forall |j\rangle_{B'} \in J_{B'}: \quad X(k)|j\rangle = |k \oplus j\rangle, \tag{A.1}$$

where $\oplus$ is a cyclic addition operator, i.e., $k \oplus j := (k+j) \bmod d$. There also exists another unitary operator called the *phase operator* $Z(l)$ that acts on the qudit computational basis states as

$$\forall |j\rangle_{B'} \in J_{B'}: \quad Z(l)|j\rangle = \exp\left(\frac{\iota 2\pi l j}{d}\right)|j\rangle. \tag{A.2}$$

The d^2 operators $\{X(k)Z(l)\}_{k,l \in \{0,\dots,d-1\}}$ are known as the Heisenberg–Weyl operators. Let $\sigma(k,l) := X(k)Z(l)$. The maximally entangled state $\Phi_{R:B'}$ of qudit systems RB' is given as

$$|\Phi\rangle_{RB'} := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_R |j\rangle_{B'}, \tag{A.3}$$

and we define

$$|\Phi^{k,l}\rangle_{RB'} := (\mathbb{1}_R \otimes \sigma_{B'}^{k,l})|\Phi\rangle_{R:B'}. \tag{A.4}$$

The d^2 states $\{|\Phi^{k,l}\rangle_{RB'}\}_{k,l \in \{0,\dots,d-1\}}$ form a complete, orthonormal basis:

$$\langle \Phi^{k_1,l_1}|\Phi^{k_2,l_2}\rangle = \delta_{k_1,k_2}\delta_{l_1,l_2}, \tag{A.5}$$

$$\sum_{k,l=0}^{d-1} |\Phi^{k,l}\rangle\langle\Phi^{k,l}|_{RB'} = \mathbb{1}_{RB'}. \tag{A.6}$$

Let $\mathscr{W}$ be a discrete set of size $|W| = d^2$. There exists one-to-one mapping $\{(k,l)\}_{k,l \in \{0,d-1\}} \leftrightarrow \{w\}_{w \in \mathscr{W}}$. For example, we can use the following map: $w = k + d \cdot l$ for $\mathscr{W} = \{0, \dots, d^2 - 1\}$. This

allows us to define $\sigma^w := \sigma(k, l)$ and $\Phi_{RB'}^w := \Phi_{RB'}^{k,l}$. Let the set of d^2 Heisenberg–Weyl operators be denoted as

$$\mathbf{H} := \{\sigma^w\}_{w \in \mathcal{W}} = \{X(k)Z(l)\}_{k,l \in \{0,\dots,d-1\}}, \tag{A.7}$$

and we refer to $\mathbf{H}$ as the Heisenberg–Weyl group.

Appendix B   Bidirectional Max-Rains Information: Examples

This appendix contains unpublished work of Stefan Baüml, Siddhartha Das, and Mark M. Wilde.

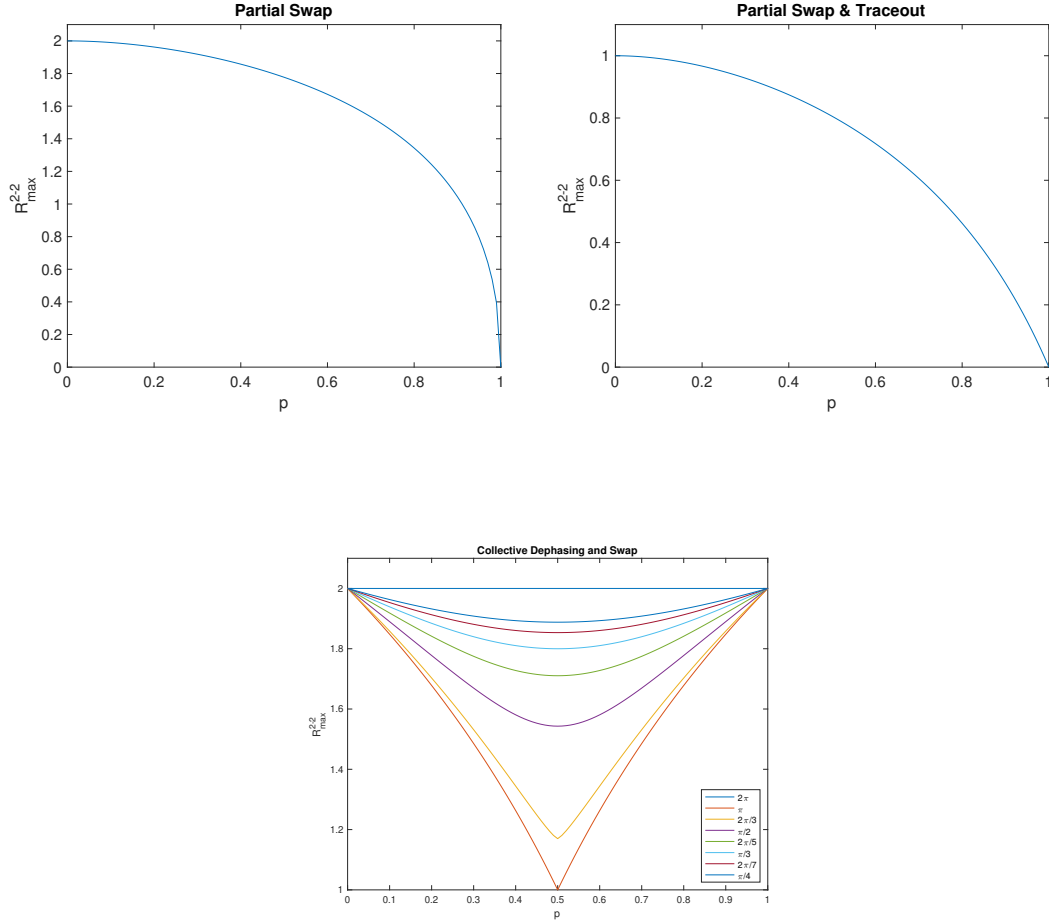Here we restrict $d = 2$ in Appendix A to consider qubit systems.

Figure B.1. Our bounds plotted versus channel parameter p. From top to bottom they belong to (i) the qubit partial swap operation, (ii) the qubit partial swap operation followed by traceout of Alice's output and (iii) a qubit swap operation followed by collective dephasing with various phases ϕ.

As an example, we have numerically computed $R_{\max}^{2 \to 2}$ for the qubit partial swap operation [260, 261], which is performed by application of the unitary $U_p = \sqrt{p}\mathbb{I} + \iota\sqrt{1-p}S$, where $S = \sum_{ij} |ij\rangle\langle ji|$ is the swap operator. Such an operation, which can be followed by a traceout of Alice's subsystem, can be compared to a beamsplitter [262]. As a second example, we have computed $R_{\max}^{2 \to 2}$ for a

qubit swap operator, followed by collective dephasing [263], which is a typical model for noise in a quantum computer. In the qubit case, collective dephasing acts as $|0\rangle \to |0\rangle$, $|1\rangle \to e^{\iota\phi}|1\rangle$ for some phase ϕ. Hence $|00\rangle \to |00\rangle$, $|01\rangle \to e^{\iota\phi}|01\rangle$, $|10\rangle \to e^{\iota\phi}|10\rangle$, and $|11\rangle \to e^{2\iota\phi}|11\rangle$. The collective dephasing occurs with probability $1 - p$.

Our results are plotted in Figure B.1. For the partial swap, the top plot shows the expected decline from two ebits to zero, as the channel tends towards total depolarization. For the partial swap and traceout, the decline is from one ebit to zero. In the example of collective dephasing, as expected, the performance is the worst at $p = 1/2$, where there is the most uncertainty about whether the collective dephasing has taken place. For phase $\phi = \pi$, we can have a reduction of a factor of $1/2$. Let us remark that this bound can actually be achieved. To do so, Alice and Bob both locally create two Bell states $\Phi^+_{L_A A'}$ and $\Phi^+_{B' L_B}$. After the swap operation and the collective dephasing they end up in a state $\frac{1}{2}\Phi^+_{AL_B} \otimes \Phi^+_{BL_A} + \frac{1}{2}\Phi^-_{AL_B} \otimes \Phi^-_{BL_A}$. To find out the phase, Alice and Bob can locally measure either A and L_B or L_A and B in the X-basis, thus sacrificing one ebit. If their results agree, they have Φ^+, and otherwise Φ^-, which can be locally rotated to Φ^+.

Appendix C   Rate of Entropy Change: Examples

Here, we review [32, Appendix B] to discuss the subtleties involved in determining the rate of entropy change using the formula (4.10) (Theorem 4.1) by considering some examples of dynamical processes.

Let us first consider a system in a pure state ψ_t undergoing a unitary time evolution. In this case, the entropy is zero for all time, and thus the rate of entropy change is also zero for all time. Note that even though the rank of the state remains the same for all time, the support changes. This implies that the kernel changes with time. However, $\dot{\psi}_t$ is well defined. This allows us to invoke Theorem 4.1, so the formula (4.10) is applicable.

Formula (4.10) is also applicable to states with higher rank whose kernel changes in time and have non-zero entropy. For example, consider the density operator $\rho_t \in \mathcal{D}(\mathcal{H})$ with the following time-dependence:

$$\forall\, t \geq 0 : \quad \rho_t = \sum_{i \in \mathcal{I}} \lambda_i(t) U_i(t) \Pi_i(0) U_i^\dagger(t), \tag{C.1}$$

where $\mathcal{I} = \{i : 1 \leq i \leq d,\ d < \dim(\mathcal{H})\}$, $\sum_{i \in \mathcal{I}} \lambda_i(t) = 1$, $\lambda_i(t) \geq 0$ and the time-derivative $\dot{\lambda}_i(t)$ of $\lambda_i(t)$ is well defined for all $i \in \mathcal{I}$. The operators $U_i(t)$ are time-dependent unitary operators associated with the eigenvalues $\lambda_i(t)$ such that the time-derivative $\dot{U}_i(t)$ of $U_i(t)$ is well defined and $[U_i(0), \Pi_i(0)] = 0$ for all $i \in \mathcal{I}$. The operators $\Pi_i(0)$ are projection operators associated with the eigenvalues $\lambda_i(0)$ such that the spectral decomposition of ρ_t at $t = 0$ is

$$\rho_0 = \sum_{i \in \mathcal{I}} \lambda_i(0) \Pi_i(0), \tag{C.2}$$

where $1 < \mathrm{rank}(\rho_0) < \dim(\mathcal{H})$. The evolution of the system is such that $\mathrm{rank}(\rho_t) = \mathrm{rank}(\rho_0)$ for all $t \geq 0$. It is clear from (C.1) and (C.2) that the projection Π_t onto the support of ρ_t depends on time:

$$\Pi_t = \sum_{i \in \mathcal{I}} U_i(t) \Pi_i(0) U_i^\dagger(t), \tag{C.3}$$

and the time-derivative $\dot{\Pi}_t$ of Π_t is well defined. The entropy of the system is zero if and only if the

state is pure.

Let us consider a qubit system A undergoing a damping process such that its state ρ_t at any time $t \geq 0$ is as follows:

$$\rho_t = (1 - e^{-t}) |0\rangle\langle 0| + e^{-t} |1\rangle\langle 1|, \tag{C.4}$$

where $\{|0\rangle, |1\rangle\} \in \text{ONB}(\mathcal{H}_A)$. The entropy $S(\rho_t)$ of the system at time t is

$$S(\rho_t) = -(1 - e^{-t}) \log(1 - e^{-t}) - e^{-t} \log(e^{-t}), \tag{C.5}$$

which is continuously differentiable for all $t > 0$ and not differentiable at $t = 0$. At $t = 0$, $\Pi_0 = |1\rangle\langle 1|$ and $\text{rank}(\rho_0) = 1$. At $t = 0^+$, there is a jump in the rank from 1 to 2, and the rank and the support remains the same for all $t \in (0, \infty)$. In this case, the formula (4.10) agrees with the derivative of (C.5).

Now, suppose that the system A undergoes an oscillatory process such that for any time $t \geq 0$ the state ρ_t of the system is given by

$$\rho_t = \cos^2(\pi t) |0\rangle\langle 0| + \sin^2(\pi t) |1\rangle\langle 1|. \tag{C.6}$$

In this case, for all $t \geq 0$, the entropy $S(\rho_t)$ is

$$S(\rho_t) = -\cos^2(\pi t) \log \cos^2(\pi t) - \sin^2(\pi t) \log \sin^2(\pi t), \tag{C.7}$$

and its derivative is

$$\frac{\mathrm{d}}{\mathrm{d}t} S(\rho_t) = \pi \sin(2\pi t) \left[\log \cos^2(\pi t) - \log \sin^2(\pi t) \right], \tag{C.8}$$

which exists for all $t \geq 0$. At $t = \frac{n}{2}$ for all $n \in \mathbb{Z}^+ \cup \{0\}$, there is a jump in the rank from 1 to 2 and the support changes discontinuously at these instants. One can check that (4.10) and (C.8) are in agreement for all $t \geq 0$.

Appendix D Reuse and Permissions

access to their work within one of our subscription-based journals.

Q: May I include previously published material from another source in my AIP Publishing article?

If you are including material taken from another source, it is your responsibility to obtain written permission for that material directly from the copyright holder. AIP Publishing assists authors in this regard by providing them with a form for this purpose (Reuse of Previously Published Material). More specific information can also be found in the Author Permission FAQ.

Q: May I include my AIP Publishing article in my thesis or dissertation?

AIP Publishing permits authors to include their published articles in a thesis or dissertation. It is understood that the thesis or dissertation may be published in print and/or electronic form and offered for sale on demand, as well as included in a university's repository. Formal permission from AIP Publishing is not needed. If the university requires written permission, however, we are happy to supply it.

Permission to Reuse AIP Publishing Material

Q: How do I obtain permission to reuse AIP Publishing material?

Using RightsLink®: AIP Publishing has partnered with the Copyright Clearance Center to offer Rightslink, a convenient online service that streamlines the permissions process. Rightslink allows users to instantly obtain permissions and pay any related fees for reuse of material, directly from AIP Publishing's website. Once licensed, the material may be reused legally, according to the terms and conditions set forth in each unique license agreement.

To use the service, access the article you wish to license on Scitation and simply click on the Reprints & Permissions link in the abstract. If you have questions about Rightslink, click on the link as described, and then click the "Help" button located in the top right-hand corner of the Rightslink page.

Without using RightsLink: Send requests for permission for republication or other reuse of AIP Publishing journal or conference proceedings material to rights@aip.org.

Contact address:

Office of Rights and Permissions
AIP Publishing
1305 Walt Whitman Road
Suite 300
Melville, NY 11747-4502
Telephone: +1 516-576-2268

Q: What information does AIP Publishing require in a permission request?

Please provide as much information as possible when requesting permission. Be sure to include the following:

- Citation information for the article containing the material you wish to reuse.
- A description of the material you wish to reuse, including the figure and/or table number as it appears in the article.
- The title, authors, name of the publisher, and expected publication date of the new work.
- The format(s) the new work will appear in—print, electronic, CD-ROM, for example.
- Information as to how the new work will be distributed and whether it will be offered for sale.

Q: Is permission needed to adapt or redraw AIP Publishing material?

This appendix contains permission of AIP Publishing to include [32] in this thesis.

Vita

Siddhartha Das was born in the year 1991. He passed SLC examination (X^{th} board) from Koshi Vidya Mandir, Biratnagar. He passed AISSCE (XIIth board) from Millia Convent School, Purnea. He enrolled in BS-MS Dual Degree Programme (August 2009–May 2014) at Indian Institute of Science Education and Research Pune. He received his BS and MS degree on 15th June, 2014. Later, he joined the Department of Physics and Astronomy at Louisiana State University, Baton Rouge for PhD starting Fall semester in 2014. He plans to graduate in December 2018, by the end of Fall semester. He has accepted postdoctoral position in the group of Nicolas Cerf at Université libre de Bruxelles, Brussels. He plans to start his postdoctoral position in early 2019.