PROCEEDINGS OF SCIENCE

Modave Lectures on Quantum Information

An Introduction to Channels and Applications to Black Holes and AdS/CFT

Aidan Chatwin-Davies*

KU Leuven, Institute for Theoretical Physics
Celestijnenlaan 200D, B-3001 Leuven, Belgium

E-mail: aechatwi@gmail.com

These notes introduce a handful of core ideas from quantum information science that figure prominently in modern research on quantum gravity. The central concept that forms the base of these notes is that of a quantum channel; that is, the most general physically-reasonable map between quantum states and between operators on Hilbert space. After reviewing some fundamentals, we will study channels and their properties, and then go on to formulate quantum error correction in terms of quantum channels. Along the way, we will see how a handful of problems in high energy physics, such as the black hole information problem and bulk reconstruction in AdS/CFT, can be cast in the information-theoretic language being set up.

XVI Modave Summer School in Mathematical Physics - Modave 2020
9-11 September 2020
Brussels, Belgium

*Speaker

PoS(Modave 2020)003

Contents

1. Introduction

Quantum Information Science (QIS) sits at an intersection point of physics, mathematics, and computer science. The field concerns itself with the information contained in quantum mechanical systems, how that information can be encoded, manipulated, and retrieved, and how these operations' properties, capabilities, and limitations can be quantified. As we sit at the cusp of the era of quantum computers, the practical importance of QIS only continues to increase. In parallel, QIS continues to drive new discoveries and further our theoretical understanding of questions in high energy physics.

The aim of these notes is to explain a handful of core ideas from QIS that figure prominently in modern research on quantum gravity. They are certainly not a complete introduction to QIS nor its application to gravity; nevertheless, they will hopefully be both interesting and useful for someone who wants to learn a bit more about the information theory that underpins gravitational applications. These notes should be accessible to anyone with a solid command of undergraduate quantum physics.

Many parts of these notes are based on my own experiences learning about QIS as a student, and as such are heavily inspired by John Preskill's excellent set of lecture notes [1]. Other parts draw on Mark Wilde's comprehensive text on quantum Shannon theory [2]. In these parts and elsewhere, I will point the reader to original source material when available, as well as to further reading.

So, what is quantum information? The abstract and somewhat tautological answer is that it is the information contained in the state of a quantum mechanical system. It's not very illuminating, not to mention that we could give an analogously impractical definition for classical information. However, much as we can characterize classical information science concretely as the study and manipulation of bit strings,

$$x_1 x_2 \cdots x_n \qquad x_i \in \{0,1\} \ \text{ for } \ 1 \leq i \leq n, \tag{1}$$

we can similarly characterize quantum information science as the study and manipulation of *qubit* strings,

$$\sum_{x_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} c_{x_1 x_2 \cdots x_n} |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle, \tag{2}$$

where each orthonormal set $\{|x_i = 0\rangle, |x_i = 1\rangle\}$ spans a two-dimensional Hilbert space, $c_{x_1 x_2 \cdots x_n} \in \mathbb{C}$ for $1 \leq i \leq n$, and

$$\sum_{x_1 \in \{0,1\}} \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} |c_{x_1 x_2 \cdots x_n}|^2 = 1. \tag{3}$$

If we can think of classical information at a concrete level as bit strings, then a concrete way to think of quantum information is as qubit strings.

A perhaps more illuminating question to ask is how quantum information and the quantum systems that store it differ from their classical counterparts. For starters:

- *Quantum systems exhibit true randomness.*

  We can of course simulate randomness with a classical computer and use it as a resource for computation, yet such processes are fundamentally only pseudo-random. In contrast, the outcomes of indefinite quantum measurements are truly random, at least according to the conventional pragmatic viewpoint [3].

- *Quantum information cannot be cloned.*

  There are no fundamental barriers to making copies of a given bit string, even if the string is unknown—a photocopier copies regardless of the input. However, the no-cloning theorem says otherwise for quantum states. There exists no unitary process that lets one make a copy of an arbitrary, unknown state. (See, e.g. [4, Chap. 12.3].)

- *Uncertainty limits information retrieval.*

  Many quantum observables fail to commute. This places limits on the information that can be simultaneously retrieved from a state.

- *Components of a quantum system can be entangled.*

  Quantum systems can store information nonlocally. An analogy is as follows: If classical, local information is the content of the pages in a book, nonlocal information would be information stored in correlations among the pages. In particular, you need all of the pages in order to access the nonlocal information. These correlations are so strong that the quantum book's pages are altered after having been read, so reading a single page at a time generally ruins the nonlocal information.

- *Quantum states can exist in superpositions.*

  A common platitude is that the ability to manipulate qubit strings is so powerful because they have exponentially many states. While this counting is correct—the dimension of the Hilbert space of n qubits is 2^n—it is also true that one can form 2^n different strings out of n bits. Rather, what makes operations on qubit strings special is that their states can be superpositions, as in Eq. (2).

It turns out that these differences can be exploited to perform tasks that are surprising from a classical standpoint. For example, given a large positive integer that is the product of two large prime numbers, superposition may be used in a clever way to find the prime factors exponentially faster than the best known methods using a classical computer that processes bit strings. This is Shor's factoring algorithm [5]. Another example is the process known as quantum teleportation [6], in which entanglement shared between (possibly distant) parties can be used to faithfully transfer an arbitrary quantum state from one party to the other without explicitly transporting any physical qubits.

A device that manipulates qubits to perform computations is called a *quantum computer*. The design of interesting algorithms that can run on quantum computers, as well as the task of actually building such devices are some of the more practical aspects of QIS. While we will not spend much time on these topics, an introduction to QIS would be somewhat askew without mention of them, so let's at least sketch what a quantum computation is at a schematic level.

A quantum computation essentially consists of three steps, as depicted in Fig. 1. First, a quantum computer that implements a state space consisting of some number of qubits, n, is initialized to a known initial state, say $|0\rangle^{\otimes n}$. Next, the "computation" itself consists of some unitary operation,

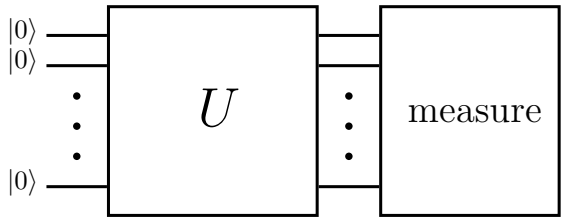


Figure 1: A quantum computation, schematically.

U, that gets applied to the n qubits.[1] In the last step, the final state is measured in the computational basis, i.e., the qubit basis $\{|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \mid x_i \in \{0,1\} \text{ for } 1 \leq i \leq n\}$. The result is that we end up sampling the probability distribution

$$\Pr(x_1, x_2, \ldots, x_n) = |\langle x_1| \otimes \langle x_2| \otimes \cdots \otimes \langle x_n| \, U \, |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle|^2. \tag{4}$$

Hopefully, a bit string that encodes the answer to an interesting problem occurs with high probability! Shor's algorithm is an example of a quantum computation. Deutsch's algorithm is a simpler introductory example, which you can find explained anywhere from Preskill's notes [1, Chap. 1] to Wikipedia.

In addition to quantum algorithms and physical device implementations, a crucial ingredient for quantum computation is *quantum error correction*. In implementing a given unitary U on a quantum computer, we are bound to make small errors along the way. Moreover, even if we never made any errors in implementation, we can never perfectly isolate the qubits inside the computer from the rest of the universe. Unwanted interactions with external degrees of freedom (like the physical components of the computer, cosmic microwave background photons, etcetera) cause the computer's qubits to bleed information into the external environment, leading to decoherence of its computational state. It's clear that we need schemes to protect computations from these types of noise and to correct errors when they occur.

Unlike algorithms and implementations, quantum error correction *is* a topic that we will take up in these notes. We will look at an example of a quantum error correcting code as a means of introducing the subject, but we will also investigate general information-theoretic features of quantum error correction. It turns out that this will lead to interesting applications in holography.

A posteriori, such a connection may not be so surprising because quantum information is universal. In a sense, all quantum systems process quantum information. While this observation naturally leads to practical applications in the case of quantum computers, applying information-theoretic tools and techniques to other quantum phenomena can result in some considerable theoretical mileage.

The core idea that will form the base of our studies here is that of a *quantum channel*. A quantum channel is the most general, physically-reasonable map between quantum states. Quantum channels therefore describe the most general way that a quantum system can evolve, and so, when applied to specific systems and circumstances, channels' information-theoretic properties are a powerful tool for understanding how systems process quantum information.

[1] Invariably, U is built out of a sequence of simpler unitary operations, or *gates*, that act on smaller numbers of qubits. A collection of gates that can approximate any unitary acting on n qubits arbitrarily well is called a *universal gate set*. See [1, Chap. 6] for more details.

In Sec. 2, we will begin by reviewing some basic concepts in quantum information science, including the indispensable quantity called Von Neumann entropy. Next, we will carefully define quantum channels in Sec. 3 and examine some of their most important properties. Sec. 4 is devoted to quantum error correction. In the first part, we will see an example of a simple quantum error-correcting code, and in the second part, we will cast quantum error correction in the language of quantum channels. Finally, in Sec. 5, we will see how all of the tools that we will have built up can be applied to the Anti de Sitter/Conformal Field Theory correspondence to understand how localized quantum gravitational degrees of freedom are encoded in the dual quantum field-theoretic description.

2. Quantum information basics

This section reviews some elementary concepts in quantum mechanics, such as states and tensor products, as well as some elementary concepts in quantum information science, such as Von Neumann entropy and relative entropy. An experienced reader could easily skip over this section, although it may be useful to refer back to for checking conventions.

2.1 States and multipartite Hilbert spaces

Let us begin by defining pure and mixed states to establish some notation.

Definition 2.1. *Let $\mathcal{H}$ be a Hilbert space with dimension $\dim\mathcal{H} = d$, and let $\{|i\rangle\}_{i=1}^{d}$ be an orthonormal basis for $\mathcal{H}$. Denote the space of linear operators on $\mathcal{H}$ by $\mathcal{L}(\mathcal{H})$.*

- *A* pure state $|\psi\rangle \in \mathcal{H}$ *is a normalized element of $\mathcal{H}$, to wit,*

$$|\psi\rangle = \sum_{i=1}^{d} c_i|i\rangle \quad \text{for some } c_i \in \mathbb{C}, \quad \text{and} \quad \langle\psi|\psi\rangle = \sum_{i=1}^{d} |c_i|^2 = 1.$$

- *A* mixed state $\rho \in \mathcal{L}(\mathcal{H})$*, also called a* density operator *or* density matrix*, is a Hermitian, positive semi-definite linear operator with unit trace, to wit,*

$$\rho = \sum_{i,j=1}^{d} \rho_{ij}|i\rangle\langle j| \quad \text{for some } \rho_{ij} \in \mathbb{C}, \quad \rho_{ij} = \rho_{ji}^{*}, \quad \sum_{i=1}^{d} \rho_{ii} = 1, \quad \langle\psi|\rho|\psi\rangle \geq 0 \ \ \forall\, |\psi\rangle \in \mathcal{H}.$$

Note: While it's fine if d is countably infinite in the definition above, in the rest of these notes we will always work with finite-dimensional Hilbert spaces unless explicitly indicated.

Note: We will denote the set of density operators on a Hilbert space $\mathcal{H}$ by $\mathcal{S}(\mathcal{H})$.

For convenience, let's collect some essential properties of density operators:

1. $\rho = \rho^{\dagger}$ (density operators are Hermitian)
2. $\langle\psi|\rho|\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$ (density operators are positive semi-definite)
3. $\operatorname{Tr}\rho = 1$ (normalization)

4. Given ρ, there exists an orthonormal basis $\{|p_a\rangle\}_{a=1}^{d}$ such that

$$\rho = \sum_a p_a |p_a\rangle\langle p_a|, \quad p_a \geq 0, \quad \sum_a p_a = 1.$$

5. ρ is pure if and only if one p_a is nonzero and equal to 1, in which case $\rho = |p_a\rangle\langle p_a|$.

6. If $\{\Lambda_k\}_{k=1}^{K}$ is a complete set of projectors (where $\sum_{i=1}^{K} \Lambda_i = I$) describing a set of measurement outcomes, the probability of obtaining outcome i is $\mathrm{Tr}(\rho\Lambda_i)$.

7. The expectation value of an operator $O \in \mathcal{L}(\mathcal{H})$ is given by $\langle O\rangle = \mathrm{Tr}(\rho O)$.

Next, recall the joint description of a Hilbert space with several factors:

Definition 2.2. *Given two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ with orthonormal bases $\{|i\rangle_A\}_{i=1}^{d_A}$ and $\{|\mu\rangle_B\}_{\mu=1}^{d_B}$, respectively, the* joint Hilbert space *is denoted by $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$. $\mathcal{H}_{AB}$ has dimension $d_{AB} = d_A d_B$, and an orthonormal basis is $\{|i\rangle_A \otimes |\mu\rangle_B\}_{i=1,\mu=1}^{d_A,d_B}$.*

In particular, we can always expand a state $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ as

$$|\psi\rangle_{AB} = \sum_{i=1}^{d_A}\sum_{\mu=1}^{d_B} c_{i\mu}|i\rangle_A \otimes |\mu\rangle_B. \tag{5}$$

We will often omit the tensor product symbol for brevity, and we will sometimes concatenate multiple kets together when the meaning is clear. Specifically, $|i\rangle_A \otimes |\mu\rangle_B$, $|i\rangle_A|\mu\rangle_B$, and $|i\mu\rangle_{AB}$ are all equivalent.

The last elementary ingredient that we need to recall is the partial trace. While the tensor product lets us build a composite Hilbert space out of two factors, the partial trace lets us reduce an operator defined on a composite Hilbert space to an operator acting on a single factor. Given $\mathcal{H}_{AB}$, suppose that we want to reduce to $\mathcal{H}_A$. We can construct the partial trace by viewing the bra $\langle\mu|_B$, which originally denotes the linear functional on $\mathcal{H}_B$ dual to $|\mu\rangle_B$, as an isometry $\langle\mu|_B : \mathcal{H}_{AB} \to \mathcal{H}_A$ whose action is defined in terms of an orthonormal basis as

$$\langle\mu|_B (|i\rangle_A \otimes |\nu\rangle_B) = |i\rangle_A \langle\mu|\nu\rangle_B = \delta_{\mu\nu}|i\rangle_A. \tag{6}$$

Definition 2.3. *The* partial trace *with respect to B is the linear map $\mathrm{Tr}_B : \mathcal{L}(\mathcal{H}_{AB}) \to \mathcal{L}(\mathcal{H}_A)$ whose action on an operator O_{AB} is given in terms of an orthonormal basis of $\mathcal{H}_B$, $\{|\mu\rangle_B\}_{\mu=1}^{d_B}$, by*

$$\mathrm{Tr}_B\, O_{AB} = \sum_{\mu=1}^{d_B} {}_B\langle\mu|O_{AB}|\mu\rangle_B.$$

The action of the resulting operator $O_A \equiv \mathrm{Tr}_B\, O_{AB}$ on a state $|\psi\rangle_A \in \mathcal{H}_A$ is given by

$$O_A|\psi\rangle_A = \sum_{\mu=1}^{d_B} {}_B\langle\mu|\left(O_{AB}(|\psi\rangle_A \otimes |\mu\rangle_B)\right).$$

Note: Of course, we can easily interchange A and B so that we reduce to the factor B (or "trace out" A) instead.

The partial trace is a way to implement ignorance about a factor of a multipartite Hilbert space. For example, if we only have access to a single part A of a larger Hilbert space, then a partial trace over the complement of A reveals how states appear and how operators act when restricted to $\mathcal{H}_A$ alone.

Example 2.4. Let ρ_{AB} be a density operator on $\mathcal{H}_{AB}$, which we write in terms of orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ as

$$\rho_{AB} = \sum_{i,\mu}\sum_{j,\nu} \rho_{i\mu\, j\nu} |i\rangle_A |\mu\rangle_B \langle j|_A \langle \nu|_B. \tag{7}$$

Taking the partial trace with respect to B gives us the reduced state on A:

$$\begin{aligned}
\rho_A \equiv \mathrm{Tr}_B\, \rho_{AB} &= \sum_\lambda \langle\lambda|_B \left(\sum_{i,\mu}\sum_{j,\nu} \rho_{i\mu\, j\nu} |i\rangle_A |\mu\rangle_B \langle j|_A \langle \nu|_B \right) |\lambda\rangle_B \\
&= \sum_{i,\mu}\sum_{j,\nu} \rho_{i\mu\, j\nu} |i\rangle\langle j|_A \left(\sum_\lambda \langle\lambda|\mu\rangle_B \langle\nu|\lambda\rangle_B \right) \\
&= \sum_{i,\mu}\sum_{j,\nu} \rho_{i\mu\, j\nu} |i\rangle\langle j|_A\, \delta_{\mu\nu} \\
&= \sum_{i,j} \left(\sum_\mu \rho_{i\mu\, j\mu} \right) |i\rangle\langle j|_A
\end{aligned}$$

As an exercise, you can check that ρ_A is Hermitian, positive semi-definite, and normalized.

□

2.2 Von Neumann entropy

Von Neumann Entropy is a quantity of singular importance for quantum information. Its definition is as follows.

Definition 2.5. *The* Von Neumann entropy *of a state $\rho \in \mathcal{S}(\mathcal{H})$, denoted by $S(\rho)$, is*

$$S(\rho) = -\,\mathrm{Tr}\,(\rho \log \rho)\,. \tag{8}$$

Note: This definition also holds for infinite-dimensional Hilbert spaces.

For example, if we write a state ρ in its eigenbasis as $\rho = \sum_i p_i |p_i\rangle\langle p_i|$, then its Von Neumann entropy is[2]

$$S(\rho) = -\sum_i p_i \log p_i. \tag{9}$$

[2]If you are familiar with classical information theory, then you might notice that this coincides with the classical Shannon entropy of the probability distribution $\{p_i\}$. We will not go into classical information theory in these notes beyond this remark, but I encourage you to take a look at Claude Shannon's original manuscripts, which are a concise and accessible introduction to the subject [7]. Likewise, Wilde's text [2] gives a thorough and positioned account of classical information theory as a precursor to quantum information theory.

We also tacitly take $p_i \log p_i$ to be continuous at $p_i = 0$, taking the value 0. In particular, this means that $S(\rho) = 0$ if $\rho = |\psi\rangle\langle\psi|$ is a pure state.

We now list several properties of Von Neumann entropy that will help us to interpret it. Again, we assume that $\dim \mathcal{H} = d < \infty$.

Proposition 2.6. *Some properties of Von Neumann entropy:*

(i) $0 \leq S(\rho) \leq \log d$*, and* $S(\rho) = \log d$ *is achieved on the maximally mixed state* $\rho = I/d$*.*

(ii) $S(\rho) = 0$ *if and only if* ρ *is pure.*

(iii) Let $|\psi\rangle \in \mathcal{H}_{AB}$ *be a pure state and* $\rho_A = \mathrm{Tr}_B\, |\psi\rangle\langle\psi|$*,* $\rho_B = \mathrm{Tr}_A\, |\psi\rangle\langle\psi|$*. Then* $S(\rho_A) = S(\rho_B)$*. Furthermore,* $S(\rho_A) = S(\rho_B) = 0$ *if and only if* $|\psi\rangle = |\phi\rangle_A \otimes |\chi\rangle_B$*, i.e.* $|\psi\rangle$ *is* unentangled *across A and B.*

(iv) $S(U\rho U^\dagger) = S(\rho)$ *for any unitary operator* U*.*

Properties (i) and (ii) tell us that $S(\rho)$ is a measure of purity. What's more, it gives us a sense of how impure the state is. Larger values of $S(\rho)$ reflect a larger lack of knowledge about the state ρ if we interpret ρ as a statistical ensemble of its pure eigenbasis states, and the maximum value is achieved on the maximally mixed state.

Property (iii) tells us that entropy is a measure of entanglement in a bipartite system. For this reason, in a bipartite setting (where the Hilbert space consists of two factors), $S(\rho_A)$ and $S(\rho_B)$ are often called *entanglement entropies*. Also notice that property (iv) implies that entanglement entropy cannot be changed by acting on a single factor at a time—in order to create entanglement, one must act nonlocally. When the total state on $\mathcal{H}_{AB}$ is pure, there is a precise sense in which entanglement entropy is the *unique* measure that quantifies bipartite entanglement. Quantifying entanglement when the state on $\mathcal{H}_{AB}$ is mixed is a more subtle question (also note that in this case, $S(\rho_A)$ and $S(\rho_B)$ need not be equal). Section 10.4 of [8] is a good point from which to jump into this discussion.

Let's sketch the proof of these properties:

Proof sketch of (i)*:* Working in the eigenbasis of ρ, our task is to extremize $S(\rho) \equiv S(p_1, \ldots, p_d) = -\sum_i p_i \log p_i$ subject to $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$. Let $p_d = 1 - \sum_{i=1}^{d-1} p_i$ to take care of the latter constraint. Then, for $1 \leq a \leq d-1$, we have

$$\frac{\partial S}{\partial p_a} = -\log p_a + \log\left(1 - \sum_{i=1}^{d-1} p_i\right) = -\log p_a + \log p_d. \tag{10}$$

For there to be a critical point, and hence for $\partial S/\partial p_a$ to vanish, it must be that $p_d = p_a$ for all $1 \leq a \leq d-1$, which is only possible if $p_a = 1/d$ for all $1 \leq a \leq d$. It's then straightforward to check that this is a maximum, and thus $S(I/d) = \log d$.

Proof sketch of (ii)*:* Since there was only one critical point of $S(p_1, \ldots, p_d)$ and it was a maximum, the minimum must occur on an edge of the domain $0 \leq p_i \leq 1$. Indeed, at any given edge point where a single $p_i = 1$ and all others vanish, it follows that $S(\rho) = 0$, and this is precisely the case where ρ is pure.

Proof sketch of (iii): This follows from the Schmidt decomposition (see Sec. 7, Exercise 1). Given a pure state $|\psi\rangle_{AB}$, there exist orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, $\{|\alpha_i\rangle_A\}_{i=1}^{d_A}$ and $\{|\beta_i\rangle_B\}_{i=1}^{d_B}$, and coefficients ψ_i (some of which could be zero) such that

$$|\psi\rangle_{AB} = \sum_{i=1}^{\min\{d_A,d_B\}} \psi_i |\alpha_i\rangle_A |\beta_i\rangle_B. \tag{11}$$

In these bases, ρ_A and ρ_B are both diagonal, and they have the same eigenvalues, $|\psi_i|^2$. Therefore, it follows that $S(\rho_A) = S(\rho_B)$. If $|\psi\rangle_{AB} = |\phi\rangle_A|\chi\rangle_B$, then $\rho_A = |\phi\rangle\langle\phi|$ and $\rho_B = |\chi\rangle\langle\chi|$ are both pure, and so their entropies vanish. Conversely, if $S(\rho_A) = S(\rho_B) = 0$, then ρ_A and ρ_B are both pure states, and so we may write $\rho_A = |\phi\rangle\langle\phi|$ and $\rho_B = |\chi\rangle\langle\chi|$ for some states $|\phi\rangle_A$ and $|\chi\rangle_B$. Since $|\psi\rangle_{AB}$ is pure by assumption, the total state (already in Schmidt form) must be $|\psi\rangle_{AB} = |\phi\rangle_A|\chi\rangle_B$.

Proof sketch of (iv): Conjugating a state ρ by a unitary operator does not change its eigenvalues, and so $S(\rho)$ is unchanged.

□

Along with these elementary properties, the Von Neumann entropies of reduced states obey many inequalities. Some of the most important ones are as follows.

Proposition 2.7. *Some Von Neumann entropy inequalities*

(i) Subadditivity: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$

(ii) Araki-Lieb: $|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB})$

(iii) Strong Subadditivity: $S(\rho_{AB}) + S(\rho_{BC}) \geq S(\rho_{ABC}) + S(\rho_B)$

We will not prove these inequalities here, but their proofs may be found in any relatively complete textbook on quantum information (e.g. [9]). For brevity, we also often equivalently write $S(\rho_A) \equiv S(A)$. So, for example, strong subadditivity can be written as $S(AB) + S(BC) \geq S(ABC) + S(B)$.

2.3 Relative entropy

Having defined Von Neumann entropy, there are many other useful entropic quantities that can be defined and interpreted. For our purposes, we will need to make extensive use of relative entropy.

Definition 2.8. *Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. The* relative entropy *of ρ and σ is*

$$D(\rho \,\|\, \sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma). \tag{12}$$

Note: Relative entropy is only well-defined if the kernel of σ is contained in the kernel of ρ, denoted $\ker \sigma \subseteq \ker \rho$, or equivalently if the support of ρ is contained in the support of σ, denoted $\mathrm{supp}\ \rho \subseteq \mathrm{supp}\ \sigma$. In other words, any eigenvector of σ with eigenvalue zero must also be an eigenvector of ρ with eigenvalue zero. This is enough to ensure that $\mathrm{Tr}(\rho \log \sigma)$ is finite.

Relative entropy has two key properties that make it a particularly useful quantity. First, relative entropy is a positive quantity:

$$D(\rho \,\|\, \sigma) \geq 0 \qquad \text{with equality if and only if } \rho = \sigma \tag{13}$$

(Exercise 3 in Sec. 7 gives a guided derivation of this property.) We will come back to this property in the next section.

Second, relative entropy obeys an inequality known as *Pinsker's inequality*[3]:

$$D(\rho \,\|\, \sigma) \geq \frac{1}{2\log 2}\|\rho - \sigma\|_1^2 \tag{14}$$

The one-norm, or trace norm of an operator is defined as

$$\|O\|_1 = \operatorname{Tr}\sqrt{O^\dagger O}. \tag{15}$$

In particular, $\|\rho - \sigma\|_1$ is a good measure of the *distinguishability* of two states ρ and σ. In other words, the smaller the value of $\|\rho - \sigma\|_1$, then the harder it is to tell the states ρ and σ apart using any measurement protocol that you could possibly invent. (Exercise 2 in Sec. 7 makes this explanation precise.) Pinsker's inequality therefore says that the relative entropy of two states is an upper bound on their distinguishability, and this will play an important role in the holographic application that we will discuss in Sec. 5.

2.4 Application: the black hole information problem

The small number of basics that we covered in this section already give us enough vocabulary to start asking information-theoretic questions in other areas of physics. For instance, we can now take up the celebrated black hole information problem [10–12], provided that you are willing to take a few facts about black holes and quantum field theory on curved space-time as given.

The earliest version of the black hole information problem is arguably a problem of thermodynamics from the early days of black holes in classical general relativity. As people realized that black holes—space-time regions whose curvature is such that no object on a causal trajectory can leave the region—were robust predictions of general relativity, they also realized that the following thermodynamic problem had to be taken seriously. If truly nothing escapes a black hole, then a black hole is a zero-temperature object. It cannot give off any heat! This also makes a black hole an entropy sink. By tossing entropic objects into a black hole, it would seem that you could reduce the total entropy of the universe, in violation of the second law of thermodynamics.

In hindsight, this early black hole "entropy problem" is not too hard to patch up. Owing to initial work on black hole thermodynamics [13], as well as the seminal work of Hawking and Bekenstein [14, 15], we now realize that black holes are indeed well-behaved classical thermodynamic objects. A black hole has a temperature that depends on its mass, and an entropy that is proportional to the surface area, A, of the black hole's event horizon (roughly, the "point of no return" from the black hole):

$$S = \frac{A}{4G_N} \tag{16}$$

[3] For a proof, see [2, Chap. 10.8]

This formula is known as the Bekenstein-Hawking entropy, G_N is Newton's constant, and we are working in units where $c = \hbar = k_B = 1$. In particular, tossing an object into a black hole increases its surface area, which hence increases the black hole's entropy, and Bekenstein argued that this increase in black hole entropy would always be enough to preserve the second law of thermodynamics.

While this is a nice resolution from the perspective of classical thermodynamics, the quantum story is quite different. Hawking argued, based on principles of quantum field theory in curved space-time, that a black hole should radiate particles at a specific temperature. While this is compelling evidence that black holes obey the laws of thermodynamics, the calculation also comes with the awkward conclusion that the radiation that leaves the black hole is in a *mixed* state. This is problematic, because nothing in principle prevents us from making a black hole out of matter that is initially in a pure state. If we let this black hole emit radiation and slowly evaporate away, we are left with a collection of radiation that is in a mixed state at the end of the day. In other words, it would seem that the formation and subsequent evaporation of a black hole is not a *unitary* process.

Of course, non-unitarity in and of itself is not a problem for quantum mechanics. When a system is *open*, meaning that it is allowed to exchange information with other degrees of freedom, then generically its evolution will be non-unitary and states that are initially pure can end up mixed. In fact, we will look at such non-unitary evolution extensively in the next section. The problem occurs when the system is *closed*. In this case, when we have truly accounted for all degrees of freedom, quantum evolution should be unitary, so that information does not dissipate away. Suffice it to say that bad things happen if a closed system evolves non-unitarily, like non-conservation of probabilities. To Hawking's dismay, his black hole evaporation calculation applies to closed systems.

For a long time, it was believed that subtle corrections to Hawking's calculation would solve the problem—that the radiation that comes out of a black hole is actually in a complicated pure state that only appears thermal on coarse scales. However, Mathur sharpened the problem in a way that challenges this expectation [10]. Almheiri, Marolf, Polchinski, Stanford, and Sully (collectively referred to as "AMPSS") subsequently streamlined the argument[4] by proposing four postulates, each of which seems very reasonable based on what we know about black holes and quantum mechanics:

1. *Unitarity* – The formation and evaporation of a black hole is a unitary quantum mechanical process.

2. *Local Effective Field Theory* – Outside of the horizon of a black hole, physics is well-described by an effective local quantum field theory.

3. *Quantum Black Holes* – Black holes are themselves quantum mechanical systems with a discrete spectrum of states.

4. *No Drama* – For a large enough black hole, such that the local curvature at the horizon is very small, nothing special happens to an observer who falls across the horizon into the black hole.

AMPSS then concluded that these postulates cannot all be mutually consistent [17, 18].

[4]Many of AMPSS' refinements specifically aimed to rebut a proposal called black hole complementarity [16].

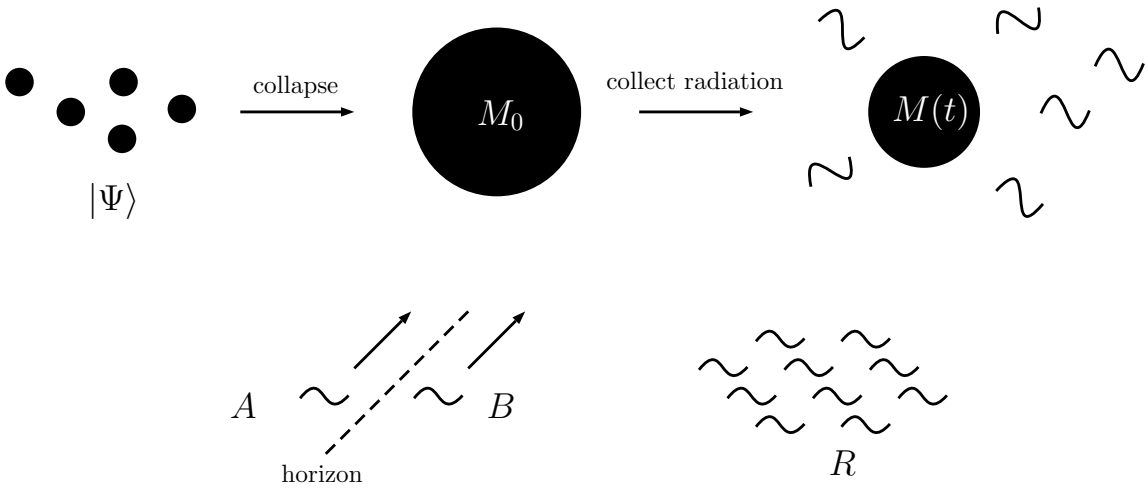


Figure 2: The Mathur/AMPSS thought experiment.

Here is a semi-rigorous version of Mathur's argument as rendered by AMPSS, which is illustrated in Fig. 2. Suppose that we begin with a collection of matter that is in some pure state and we collapse it into a black hole of mass M_0. This black hole starts radiating, and we collect all of the radiation that it emits until some time when the mass of the black hole is substantially less than $M_0/2$. Let ρ_R be the state of the radiation that we have collected. Consider a particular mode of the radiation—in other words, roughly, a wave-packet of radiation—just outside of the black hole horizon and that is leaving the black hole, and denote its state by ρ_B. From quantum field theoretic arguments, this mode will have a partner mode just inside of the horizon, whose state we denote by ρ_A. Moreover, according to postulates (2) and (4), the joint state of A and B is entangled and pure, meaning that

$$(i) \qquad S(A) = S(B) \neq 0, \quad S(AB) = 0.$$

Subadditivity of entanglement entropy (Prop. 2.7-(i)) has the saturation property that $S(XY) = S(X) + S(Y)$ if and only if $\rho_{XY} = \rho_X \otimes \rho_Y$. Since ρ_{AB} is pure, it follows that $\rho_{ABR} = \rho_{AB} \otimes \rho_R$, and so

$$(ii) \qquad S(ABR) = S(R).$$

Next, postulate (1) implies that

$$(iii) \qquad S(BR) < S(R).$$

This is the mathematical statement that once the black hole has lost roughly half of its initial mass to evaporation[5], any quantum of radiation that subsequently leaves the black hole should purify the radiation that came out earlier if black hole evaporation is unitary. (At the end of unitary evaporation, we must have that $S(R) = 0$, since R is all that is left.) Finally, we also have strong subadditivity (Prop. 2.7-(iii)) among the A, B, and R subsystems:

$$(iv) \qquad S(AB) + S(BR) \geq S(ABR) + S(B)$$

[5]More precisely, past the *Page time*, at which point the black hole's horizon area reaches half its initial value.

Putting it all together, we find the following:

$$\begin{aligned} S(R) + S(B) &= S(ABR) + S(B) && \text{using } (ii) \\ &\leq S(AB) + S(BR) && \text{using } (iv) \\ &< S(AB) + S(R) && \text{using } (iii) \\ &= S(R) && \text{using } (i) \end{aligned}$$

Since $S(B) \neq 0$, we have therefore arrived at a contradiction!

AMPSS' conclusion was that one of their four postulates has to be modified. How palatable the ensuing consequences are is up to you to reason through.

1. If we drop unitarity, then black holes destroy quantum information [19].
2. One way to modify local effective field theory is to delete the word "local" and allow for small amounts of nonlocality [20], although such an approach is not without its rebuttals, e.g. [21, Sec. 8]. Holographic resolutions of the black hole information problem (and AdS/CFT itself) are also nonlocal in the sense that degrees of freedom are replicated in both the bulk space-time and its boundary (see Sec. 5).
3. One way to evade AMPSS' argument is if black holes never finish evaporating and instead leave behind a small and extremely entropic remnant [22]. Or, perhaps black holes are just not described by quantum mechanics.
4. If A and B are not in a pure entangled state such that $S(AB) \neq 0$, then it's possible to evade the contradiction. However, such states have large local energy densities. In our setting, it would be as if there was a firewall waiting just behind the horizon that an infalling observer would hit as they entered the black hole. As AMPSS pointed out, the result is considerable drama for the observer.

The references given above are by no means a complete account of the literature and only represent a handful of the big ideas in their corresponding directions. The second AMPSS paper [18] is a traditional place to start looking for more literature if you want to learn more about different approaches to the black hole information problem. Refs. [10–12] are accessible and pedagogical reviews, and Ref. [21] gives a particularly thorough and modern review of the subject.

Recent attempts at resolving the black hole information problem have focused on black holes in AdS/CFT (for a review, see [23]). In this setting at least, it seems that unitarity is maintained by having the Hawking radiation encode the interior of the black hole so that a violation of strong subadditivity is avoided. Morally, these resolutions are a relaxation of locality, since distant Hawking radiation encodes a faraway region inside the black hole, but this nonlocality is no more drastic than holography itself, in which distant degrees of freedom at the boundary of a space-time encode physics deep inside. Whether and how this reasoning extends to more general black holes is a topic of current research.

3. Quantum channels

We largely focused on properties of states in the last section. In this section, we will study how quantum states evolve. When we first learn about quantum mechanics, we learn about unitary

evolution according to the Schrödinger equation. But, as you may already be aware of, much more general yet physically reasonable quantum evolution is possible. Such evolution is described by quantum channels.

3.1 Definition and properties

Informally, a *quantum channel* is a map that sends states to states.

Example 3.1. Unitary evolution is a quantum channel. Let $\rho \in \mathcal{S}(\mathcal{H})$ and $U \in \mathcal{L}(\mathcal{H})$ be a unitary operator. The map

$$\begin{aligned} \mathcal{N}_U : \ & \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}) \\ & \rho \mapsto U\rho U^\dagger \end{aligned} \tag{17}$$

is a quantum channel. □

Example 3.2. A channel can also describe non-unitary evolution. Let Let $\rho_A \in \mathcal{S}(\mathcal{H}_A)$, $|0\rangle_B \in \mathcal{H}_B$ be some fixed state, and let $U_{AB} \in \mathcal{L}(\mathcal{H}_{AB})$ be a unitary operator. The map

$$\begin{aligned} \mathcal{N} : \ & \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_A) \\ & \rho_A \mapsto \mathrm{Tr}_B\left[U_{AB}\left(\rho_A \otimes |0\rangle\langle 0|_B\right) U_{AB}^\dagger\right] \end{aligned} \tag{18}$$

is a quantum channel. For generic choices of U_{AB}, $\mathcal{N}(\rho_A)$ will not in general be pure even if ρ_A is pure. □

Let's now be a bit more systematic. Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a map from linear operators on $\mathcal{H}_A$ to linear operators on $\mathcal{H}_B$. If we want $\mathcal{N}$ to map states to states, what is the minimal set of properties that should it have?

1. $\mathcal{N}$ should be *trace-preserving*, i.e.,

$$\mathrm{Tr}_B[\mathcal{N}(O)] = \mathrm{Tr}_A[O]. \tag{19}$$

This will ensure that the image of a density operator will still have unit trace.

2. $\mathcal{N}$ should be *linear*, i.e.,

$$\mathcal{N}(\lambda_1 O_1 + \lambda_2 O_2) = \lambda_1 \mathcal{N}(O_1) + \lambda_2 \mathcal{N}(O_2) \tag{20}$$

for all $\lambda_1, \lambda_2 \in \mathbb{C}$. This is reasonable to require so that the ensemble interpretation of density operators continues to hold. Explicitly, suppose that we decompose a density operator as a probabilistic ensemble,

$$\rho = \sum_i p_i \rho_i, \tag{21}$$

for a collection of density operators ρ_i and probabilities $p_i \in [0,1]$ such that $\sum_i p_i = 1$. The interpretation of such an ensemble is that the state ρ describes a configuration where the state ρ_i is prepared with probability p_i. If we send ρ through the channel $\mathcal{N}$, it should then be that the state $\mathcal{N}(\rho_i)$ occurs with probability p_i, i.e., $\mathcal{N}(\rho) = \sum_i p_i \mathcal{N}(\rho_i)$.

Still, it's fun to ask what happens if a map between states is nonlinear. The next example demonstrates a specific strange occurrence.

Example 3.3. Consider the map whose action on a qubit state $\rho \in \mathcal{S}(\mathcal{H})$, $\mathcal{H} = \text{span}\{|0\rangle, |1\rangle\}$, is given by

$$\mathcal{E}(\rho) = e^{i\pi X \,\text{Tr}[X\rho]}\, \rho\, e^{-i\pi X \,\text{Tr}[X\rho]}, \tag{22}$$

where X is the Pauli x operator (i.e. $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$). This map is trace-preserving (as can be seen using the cyclic property of the trace), but it is clearly not a linear map. In a first scenario, suppose that we prepare a state $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Since $\text{Tr}[X\rho_1] = 0$, it follows that $\mathcal{E}(\rho_1) = \rho_1$. In a second scenario, however, suppose that we first prepare ρ_1 and then perform an operation such that if the state $|1\rangle$ is prepared, it gets rotated to the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, resulting in a state $\rho_2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$. Since $\text{Tr}[X\rho_2] = \frac{1}{2}$, it follows that $\mathcal{E}(\rho_2) = X\rho_2 X = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|+\rangle\langle +|$.

This is very strange evolution in light of the ensemble interpretation of density operators. Comparing the two scenarios, we see that the state $|0\rangle\langle 0|$, which is prepared with probability $\frac{1}{2}$ in each case, evolves differently depending on how we *would have* prepared the other state had we not prepared $|0\rangle\langle 0|$. In other words, $\mathcal{E}$ describes evolution that depends on possibilities that are not actually realized. □

Since density operators describe probabilities, $\mathcal{N}$ itself should certainly be *positive*, i.e., if O is positive semi-definite, then $\mathcal{N}(O)$ should also be positive semi-definite. This is the strict minimum needed to ensure that the image of a density operator is positive semi-definite, but we will actually require something a bit stronger:

3. $\mathcal{N}$ should be *completely positive*. Given any other auxiliary Hilbert space $\mathcal{H}_R$, we require that the map

$$\text{id}_R \otimes \mathcal{N} : \mathcal{L}(\mathcal{H}_R \otimes \mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_R \otimes \mathcal{H}_B) \tag{23}$$

is positive, where id_R is the identity map on $\mathcal{L}(\mathcal{H}_R)$.

This requirement should seem fairly innocuous, and it's certainly reasonable on physical grounds. If A is the part of the universe under consideration and R is some other part, or even the rest of the universe itself, then evolving A with $\mathcal{N}$ and doing nothing to the rest of the universe should map a state of the universe to a state of the universe. It turns out that complete positivity will let us prove a powerful result about channels (Thm. 3.6 below). Before doing this, let's see an example of a map that is positive, but not completely positive.

Example 3.4. Let $\mathcal{H} = \text{span}\{|i\rangle\}_{i=1}^{d}$. The transpose map

$$^T : |i\rangle\langle j| \mapsto |j\rangle\langle i| \tag{24}$$

is a positive map. If $O = \sum_{ij} O_{ij}|i\rangle\langle j|$ is positive semi-definite, then for any $|\psi\rangle = \sum_i \psi_i |i\rangle$, we have that

$$\langle\psi|O^T|\psi\rangle = \sum_{ij} \psi_i^* (O^T)_{ij} \psi_j = \sum_{ij} \psi_j O_{ji} \psi_i^* = \langle\psi^*|O|\psi^*\rangle \geq 0, \tag{25}$$

where $|\psi^*\rangle$ denotes the state $\sum_i \psi_i^* |i\rangle$. However, let $\mathcal{H} \equiv \mathcal{H}_A$, and suppose that we augment the Hilbert space with $\mathcal{H}_R \cong \mathcal{H}_A$. Define the (unnormalized) maximally entangled state

$$|\Gamma\rangle_{RA} = \sum_i |i\rangle_R |i\rangle_A \tag{26}$$

and consider the action of $\mathrm{id}_R \otimes {}^T$ on $|\Gamma\rangle\langle\Gamma|_{RA}$:

$$\begin{aligned}(\mathrm{id}_R \otimes {}^T)(|\Gamma\rangle\langle\Gamma|_{RA}) &= (\mathrm{id}_R \otimes {}^T)\left(\sum_{ij} |i\rangle\langle j|_R \otimes |i\rangle\langle j|_A\right) \\ &= \sum_{ij} |i\rangle\langle j|_R \otimes |j\rangle\langle i|_A \\ &\equiv \mathrm{SWAP}_{RA}\end{aligned}$$

$|\Gamma\rangle\langle\Gamma|_{RA}$ therefore maps to the SWAP operator, which interchanges the state on A with the state on R. However, $(\mathrm{SWAP})^2 = I$, which means that the eigenvalues of SWAP are ± 1. Since SWAP has negative eigenvalues, it is not a positive semi-definite operator. □

We can now give a formal definition of a quantum channel:

Definition 3.5. *A* quantum channel *is a map $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ that is linear, trace-preserving, and completely positive.*

3.2 The operator-sum representation

A further motivation for requiring complete positivity is that it lets us prove the following theorem, which is a powerful characterization of the general structure of quantum channels. We will first state the theorem, look at a simple example, and then go on to prove the theorem. The proof is a mix of the proofs given by Refs. [1] and [2], and it includes a few of my own touches. Following Wilde's notation, we will sometimes add a subscript to a channel to indicate its domain and range.

Theorem 3.6 (Choi-Kraus)**.** *A linear map $\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is completely positive and trace-preserving (CPTP) if and only if*

$$\mathcal{N}_{A\to B}(X_A) = \sum_{\ell=1}^{d} M_\ell X_A M_\ell^\dagger \tag{27}$$

for all $X_A \in \mathcal{L}(\mathcal{H}_A)$, where the $M_\ell \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$ are linear maps from $\mathcal{H}_A$ to $\mathcal{H}_B$ satisfying

$$\sum_{\ell=1}^{d} M_\ell^\dagger M_\ell = I_A \tag{28}$$

and that may be chosen such that $d \leq d_A d_B$.

Note: Eq. (27) is the *operator-sum* representation of $\mathcal{N}_{A\to B}$ and the operators M_ℓ are called *Kraus operators*. The Kraus operators for a given channel are not unique, but we will come back to this point in Sec. 3.3.2.

Example 3.7. Reconsider the channel from Ex. 3.2:

$$\begin{aligned}\mathcal{N}(\rho_A) &= \mathrm{Tr}_B\left[U_{AB}\left(\rho_A \otimes |0\rangle\langle 0|_B\right)U_{AB}^\dagger\right] \\ &= \sum_{j=1}^{d_B} {}_B\langle j|U_{AB}|0\rangle_B\left(\rho_A\right){}_B\langle 0|U_{AB}^\dagger|j\rangle_B \\ &\equiv \sum_{j=1}^{d_B} M_j\rho_A M_j^\dagger\end{aligned}$$

The operators M_j are linear, and we can check the completeness relation:

$$\begin{aligned}\sum_j M_j^\dagger M_j &= \sum_j {}_B\langle 0|U_{AB}^\dagger|j\rangle\langle j|U_{AB}|0\rangle_B \\ &= {}_B\langle 0|U_{AB}^\dagger\left(\sum_j |j\rangle\langle j|\right)U_{AB}|0\rangle_B \\ &= {}_B\langle 0|U_{AB}^\dagger U_{AB}|0\rangle_B \\ &= {}_B\langle 0|I_{AB}|0\rangle_B \\ &= I_A\end{aligned}$$

We have therefore exhibited an operator-sum decomposition of $\mathcal{N}$ and a set of Kraus operators. □

Proof (Choi-Kraus Theorem): First we prove the forward direction. Suppose that the action of $\mathcal{N}_{A\to B}$ is given by Eq. (27). This action clearly defines a linear map. To establish complete positivity, consider the action of $\mathrm{id}_R \otimes \mathcal{N}_{A\to B}$ on a positive semi-definite operator $X_{RA} \in \mathcal{L}(\mathcal{H}_{RA})$:

$$(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(X_{RA}) = \sum_\ell (I_R \otimes M_\ell)X_{RA}(I_R \otimes M_\ell^\dagger) \tag{29}$$

Given any state $|\psi\rangle_{RB} \in \mathcal{H}_{RB}$, if we define the state $|\tilde{\psi}_\ell\rangle_{RA} = (I_R \otimes M_\ell^\dagger)|\psi\rangle_{RB}$, for each ℓ we can write

$${}_{RB}\langle\psi|(I_R \otimes M_\ell)X_{RA}(I_R \otimes M_\ell^\dagger)|\psi\rangle_{RB} = {}_{RA}\langle\tilde{\psi}_\ell|X_{RA}|\tilde{\psi}_\ell\rangle_{RA} \geq 0. \tag{30}$$

Therefore, ${}_{RB}\langle\psi|(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(X_{RA})|\psi\rangle_{RB} \geq 0$, and so $\mathcal{N}_{A\to B}$ is completely positive. To check that $\mathcal{N}_{A\to B}$ is trace-preserving, we just calculate. Let $X_A \in \mathcal{L}(\mathcal{H}_A)$:

$$\begin{aligned}\mathrm{Tr}_B\left[\mathcal{N}_{A\to B}(X_A)\right] &= \mathrm{Tr}_B\left[\sum_\ell M_\ell X_A M_\ell^\dagger\right] \\ &= \mathrm{Tr}_A\left[\sum_\ell M_\ell^\dagger M_\ell X_A\right] \\ &= \mathrm{Tr}_A[X_A]\end{aligned}$$

Checking that the cyclic property of the trace still holds for the partial traces above (i.e., going from the first to the second line) is the short Exercise 4 in Sec. 7.

Next we prove the reverse direction. Suppose that $\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is a linear, CPTP map. We must show that it has an operator-sum representation. First, let us make a brief digression to introduce a useful tool:

Definition 3.8. *Let $\mathcal{H}_R \cong \mathcal{H}_A$ and recall the unnormalized maximally entangled state $|\Gamma\rangle_{RA}$ defined in Eq. (26). The* Choi operator *is the operator*

$$(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA}) = \sum_{i,j=1}^{d_A} |i\rangle\langle j|_R \otimes \mathcal{N}_{A\to B}(|i\rangle\langle j|_A). \tag{31}$$

Next, we make two observations. First, since $\mathcal{N}_{A\to B}$ is completely positive, the Choi operator is itself a (non-normalized) state. We can therefore diagonalize it and write

$$(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA}) = \sum_{\ell=1}^{d} |\phi_\ell\rangle\langle\phi_\ell|_{RB} \tag{32}$$

for some (non-normalized) non-zero vectors $\{|\phi_\ell\rangle_{RB}\}_{\ell=1}^{d}$, where $d \leq d_R d_B = d_A d_B$. Second, given any vector $|\psi\rangle_A \in \mathcal{H}_A$, we can write

$$|\psi\rangle_A = \sum_{i=1}^{d_A} \psi_i\, |i\rangle_A = \sum_{i=1}^{d_A} \psi_i ({}_R\langle i|\Gamma\rangle_{RA}) = {}_R\langle\psi^*|\Gamma\rangle_{RA}. \tag{33}$$

Putting these two observations together, for $|\psi\rangle_A, |\chi\rangle_A \in \mathcal{H}_A$, we find the following:

$$\begin{aligned}
\mathcal{N}_{A\to B}(|\psi\rangle\langle\chi|_A) &= \mathcal{N}_{A\to B}\left({}_R\langle\psi^*|\Gamma\rangle\langle\Gamma|\chi^*\rangle_R\right) \\
&= {}_R\langle\psi^*|(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA})|\chi^*\rangle_R \\
&= \sum_{\ell=1}^{d} {}_R\langle\psi^*|(|\phi_\ell\rangle\langle\phi_\ell|_{RB})|\chi^*\rangle_R
\end{aligned}$$

With this in mind, for each ℓ, define a linear operator

$$\begin{aligned}
M_\ell :\ \mathcal{H}_A &\to \mathcal{H}_B \\
|\psi\rangle_A &\to {}_R\langle\psi^*|\phi_\ell\rangle_{RB}
\end{aligned} \tag{34}$$

with an adjoint that satisfies

$${}_A\langle\psi|M_\ell^\dagger = (M_\ell|\psi\rangle_A)^\dagger = {}_{RB}\langle\phi_\ell|\psi^*\rangle_R. \tag{35}$$

We can therefore write

$$\mathcal{N}_{A\to B}(|\psi\rangle\langle\chi|_A) = \sum_{\ell=1}^{d} M_\ell|\psi\rangle\langle\chi|_A M_\ell^\dagger. \tag{36}$$

Any linear operator X_A can be written as a sum over single-rank operators like $|\psi\rangle\langle\chi|$, and so by linearity, we we have that

$$\mathcal{N}_{A\to B}(X_A) = \sum_{\ell=1}^{d} M_\ell X_A M_\ell^\dagger \tag{37}$$

for all $X_A \in \mathcal{L}(\mathcal{H}_A)$. The last thing that we have to show is that the M_ℓ obey the required completeness relation. To this end, we exploit the fact that $\mathcal{N}_{A\to B}$ is trace preserving:

$$\mathrm{Tr}_B[\mathcal{N}_{A\to B}(|i\rangle\langle j|_A)] = \mathrm{Tr}_A[|i\rangle\langle j|_A] = \delta_{ij} \tag{38}$$

However, according to the operator-sum decomposition that we found,

$$\begin{aligned}\mathrm{Tr}_B[\mathcal{N}_{A\to B}(|i\rangle\langle j|_A)] &= \mathrm{Tr}_B\left[\sum_{\ell=1}^{d} M_\ell |i\rangle\langle j|_A M_\ell^\dagger\right] \\ &= \mathrm{Tr}_A\left[\sum_{\ell=1}^{d} M_\ell^\dagger M_\ell |i\rangle\langle j|_A\right] \\ &= \langle j|\left(\sum_{\ell=1}^{d} M_\ell^\dagger M_\ell\right)|i\rangle_A\end{aligned}$$

Therefore, it must be that $\sum_{\ell=1}^{d} M_\ell^\dagger M_\ell = I_A$, which completes the proof of the theorem.

□

We were a bit quick about it in the proof above, but it's worth noting that $M_\ell^\dagger$ as defined through Eq. (35) is indeed a well-defined map from $\mathcal{H}_B$ to $\mathcal{H}_A$. From our definitions, we can write the following:

$$\begin{aligned}{}_A\langle\psi|M_\ell^\dagger|\chi\rangle_B &= {}_{RB}\langle\phi_\ell|\psi^*\rangle_R|\chi\rangle_B \\ &= {}_R\langle\psi|_B\langle\chi^*|\phi^*\rangle_{RB} \\ &= {}_R\langle\psi|(M_\ell^\dagger|\chi\rangle_B)_R\end{aligned}$$

Since $\mathcal{H}_R \cong \mathcal{H}_A$, we can relabel the last lines to define the action of $M_\ell^\dagger$ as

$$M_\ell^\dagger : |\chi\rangle_B \mapsto {}_B\langle\chi^*|\phi^*\rangle_{AB}. \tag{39}$$

3.3 Further properties and results

In the last part of this section, we examine a handful of further properties of channels in light of the Choi-Kraus theorem and its proof.

3.3.1 Channel-state duality

The Choi operator (Def. 3.8) that we introduced during the proof of Thm. 3.6 defines a one-to-one correspondence between states and channels that is known as *channel-state duality*, or the *Choi-Jamiolkowski isomorphism*. The Choi operator itself, via Eq. (32), associates a state to a given channel $\mathcal{N}_{A\to B}$ that encodes all of the channel's properties, including its action. Conversely, given any state on a Hilbert space $\mathcal{H}_{RB}$, which we write in diagonal form as $\sum_{\ell=1}^{d} |\phi_\ell\rangle\langle\phi_\ell|_{RB}$, Eq. (36) and the operators M_ℓ defined by Eq. (34) together define a channel $\mathcal{N}_{A\to B}$ from a Hilbert space $\mathcal{H}_A \cong \mathcal{H}_R$ to $\mathcal{H}_B$. We will not make any further use of channel-state duality, but it's worth being aware of since it's a useful tool in quantum information theory that you will surely encounter again.

3.3.2 Isometric dilation

An important consequence of the Choi-Kraus theorem is that we can always think of a channel as coming from an isometric operator, called its *isometric dilation*, on a larger Hilbert space.

Proposition 3.9. *Let $\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a CPTP map, and let $\mathcal{H}_E$ be an auxiliary Hilbert space such that $\dim \mathcal{H}_E \geq d$, where d is as defined in Thm. 3.6. Then, there exists a linear isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ such that*

$$\mathrm{Tr}_E[VX_AV^\dagger] = \mathcal{N}_{A\to B}(X_A) \tag{40}$$

for all $X_A \in \mathcal{L}(X_A)$, where $V^\dagger V = I_A$ and $VV^\dagger = \Pi_{BE}$. The operator Π_{BE} denotes the projector onto the image of $\mathcal{L}(\mathcal{H}_A)$ under V.

Several comments are in order. First, an *isometry* is an inner product-preserving map linear map, i.e. $\langle V\phi|V\psi\rangle = \langle\phi|\psi\rangle$. Furthermore, it's easy to extend an isometry to a unitary operator by adding extra Hilbert spaces to its domain or range. For example, let $\mathcal{H}_A = \mathrm{span}\{|0\rangle_A\}$, $\mathcal{H}_B = \mathrm{span}\{|0\rangle_B, |1\rangle_B\}$, and define the isometry $V : |0\rangle_A \mapsto \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B)$. If we introduce an extra Hilbert space $\mathcal{H}_{A'} = \mathrm{span}\{|1\rangle_{A'}\}$, then it's straightforward to extend V to a unitary operator $U : \mathcal{H}_A \oplus \mathcal{H}_{A'} \to \mathcal{H}_B$ such that the restriction of U to $\mathcal{H}_A$ is V, i.e. $U|_A = V$. For instance,

$$\begin{aligned} U :\ |0\rangle_A &\mapsto \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) \\ |1\rangle_{A'} &\mapsto \frac{1}{\sqrt{2}}(|0\rangle_B - |1\rangle_B) \end{aligned} \tag{41}$$

does the trick. The take-home message of this discussion is that it is always possible to think of non-unitary evolution in a given Hilbert space as unitary evolution in a larger Hilbert space in which we are ignorant of certain degrees of freedom.

Given that $V^\dagger V = I_A$, it's straightforward to see that $VV^\dagger$ has to be a projector, because

$$(VV^\dagger)(VV^\dagger) = V(V^\dagger V)V^\dagger = VI_AV^\dagger = VV^\dagger. \tag{42}$$

The isometry V is itself easy to construct. Let $\{M_j\}$ be a set of Kraus operators for $\mathcal{N}_{A\to B}$, and let $\{|e_j\rangle_E\}$ be an orthonormal basis for $\mathcal{H}_E$. Then, V is given by

$$V = \sum_{j=1}^{d} M_j \otimes |e_j\rangle_E, \tag{43}$$

and its action on a state $|\psi\rangle_A \in \mathcal{H}_A$ is

$$V|\psi\rangle_A = \sum_{j=1}^{d} (M_j|\psi\rangle_A) \otimes |e_j\rangle_E. \tag{44}$$

We can check that $V^\dagger V = I_A$:

$$\begin{aligned} V^\dagger V &= \sum_{i,j} M_i^\dagger M_j \langle e_i|e_j\rangle_E \\ &= \sum_i M_i^\dagger M_i \\ &= I_A \end{aligned}$$

Finally, tracing out E indeed reproduces the action of $\mathcal{N}_{A\to B}$:

$$\begin{aligned}\mathrm{Tr}_E[VX_AV^\dagger] &= \mathrm{Tr}_E\left[\sum_{i,j} M_iX_AM_j^\dagger \otimes |e_i\rangle\langle e_j|_E\right] \\ &= \sum_{i,j} M_iX_AM_j^\dagger \langle e_j|e_i\rangle_E \\ &= \sum_i M_iX_AM_i^\dagger \\ &= \mathcal{N}_{A\to B}(X_A)\end{aligned}$$

The isometric dilation also gives us a way to easily show that the choice of Kraus operators in an operator-sum decomposition is not unique. Suppose we perform a unitary change of basis in $\mathcal{H}_E$ and write

$$|e_i\rangle_E = \sum_j W_{ij}|\tilde{e}_j\rangle_E. \tag{45}$$

Then V remains an isometric dilation of $\mathcal{N}_{A\to B}$, but we see that

$$V = \sum_i M_i \otimes \sum_j W_{ij}|\tilde{e}_j\rangle_E = \sum_j \left(\sum_i W_{ij}M_i\right) \otimes |\tilde{e}_j\rangle_E \equiv \sum_j N_j \otimes |\tilde{e}_j\rangle_E, \tag{46}$$

and so we have found another set of Kraus operators, $\{N_j\}$. It turns out that two sets of Kraus operators are always related unitarily in this way if they correspond to the same channel. For a proof, see [1].

3.3.3 Monotonicity of relative entropy

The final topic we will look at in this section is a combined property of relative entropy and channels:

Theorem 3.10 (Monotonicity of relative entropy)**.** *Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a CPTP map. Then, for all $\rho, \sigma \in \mathcal{S}(\mathcal{H}_A)$, it follows that $D(\rho \,\|\, \sigma) \geq D(\mathcal{N}(\rho) \,\|\, \mathcal{N}(\sigma))$.*

The mathematical content of this theorem is that evolution by a channel can never cause the relative entropy between two states to increase. In light of our discussion from Sec. 2.3, the physical content of this theorem is that a channel can only degrade states. At best, a pair of states can only remain as distinguishable as they were before. For a proof of this theorem, see [2, Thm. 11.8.1].

4. Quantum error correction

As we briefly touched on in the introduction, errors are certain to occur whenever we try to implement a quantum computation. Whether they are due to unwanted interactions with the surrounding environment, faulty implementations of unitary operations, or some other reason, we need a way to protect computations from errors. This is what we achieve with quantum error correction.[6]

[6]Quantum error correction is distinct from *fault tolerance*, which is equally crucial for computation, but which we will not cover here. For an introduction, see [24].

The basic idea of quantum error correction is to embed a smaller Hilbert space, called the *logical space* or *code subspace*, into a larger Hilbert space, called the *physical space*:

$$\mathcal{H}_{\text{code}} \hookrightarrow \mathcal{H}_{\text{phys}}$$

The actual physical degrees of freedom of a quantum computer are described by $\mathcal{H}_{\text{phys}}$, but the logical computation that we want to achieve takes place in $\mathcal{H}_{\text{code}}$. A specific embedding is a *quantum error correcting code* (QECC), and for a QECC to be good, it must protect the logical computation from errors that are likely to occur. More precisely, this means that we must be able to use the extra degrees of freedom afforded by $\mathcal{H}_{\text{phys}}$ to monitor the computer's state for errors, and we must able to correct these errors when they occur. We typically expect that errors tend to be largely uncorrelated and localized in the physical space,[7] and so good QECCs tend to encode the logical information *nonlocally* in $\mathcal{H}_{\text{phys}}$ What's more, we have to be very clever in how we carry out monitoring and error recovery tasks so as not to disturb the information contained in the computer's computational state!

Rather than dwell further on abstract features, the best way to become familiar with quantum error correction is to see an example of a QECC. This is what we will do in the first part of this section. In the second part, we will reformulate quantum error correction in the language of quantum channels, which ties into the previous section and sets us up for the holographic applications discussed in the next.

4.1 Two quantum error correcting codes

Before we begin, let us briefly confirm some notation and conventions. The Hilbert space of a single qubit is spanned by two basis vectors, $|0\rangle$ and $|1\rangle$, that are eigenstates of the Pauli z operator, which we denote by Z, i.e.,

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle. \tag{47}$$

Similarly, the other Pauli operators are denoted by X and Y. We will denote a basis state for n qubits by a binary string,

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \equiv |x_1 x_2 \ldots x_n\rangle, \quad x_i \in \{0,1\} \text{ for } 1 \leq i \leq n, \tag{48}$$

and we call this basis the *computational basis*. Finally, we indicate that a single-qubit operator O acts on the i^{th} qubit with a subscript, O_i, and we usually suppress any identity operators and tensor product symbols. For example,

$$\begin{aligned} Z_1 X_3 Z_4 X_4 |x_1 x_2 x_3 x_4\rangle &\equiv (Z_1 \otimes I_2 \otimes X_3 \otimes Z_4 X_4)|x_1 x_2 x_3 x_4\rangle \\ &= (Z_1|x_1\rangle) \otimes |x_2\rangle \otimes (X_3|x_3\rangle) \otimes (Z_4 X_4|x_4\rangle). \end{aligned}$$

4.1.1 A rudimentary 3-qubit code

Suppose that we want to design a QECC for a single logical qubit. For our first attempt, suppose that we have three physical qubits at our disposal and that we try the following encoding:

$$|\bar{0}\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \qquad |\bar{1}\rangle := \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) \tag{49}$$

[7] From a practical standpoint, a QECC is only as good as the extent to which the errors it is designed to correct faithfully model the errors that actually occur.

The states $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are read as "logical zero" and "logical one," and are often also called "codewords."

A useful feature of this encoding is that we can detect and correct a single erroneous bit flip, meaning that we can deduce whether X_1, X_2, or X_3 was applied to one of the physical qubits and then undo the damage. For example, suppose that X_1 gets applied erroneously to one of the codewords:

$$X_1|\bar{0}\rangle = |100\rangle + |011\rangle \qquad X_1|\bar{1}\rangle = |100\rangle - |011\rangle \tag{50}$$

(Here and henceforth, we will omit the factors of $1/\sqrt{2}$ to avoid cluttering the math in the rest of this section.) Notice that $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are eigenstates of the operators Z_1Z_2 and Z_2Z_3 with eigenvalue $+1$. However, after applying X_1, we see that

$$\begin{aligned} Z_1Z_2(|100\rangle \pm |011\rangle) &= -(|100\rangle \pm |011\rangle) \\ Z_2Z_3(|100\rangle \pm |011\rangle) &= +(|100\rangle \pm |011\rangle) \end{aligned} \tag{51}$$

Similarly, if we measure Z_1Z_2 and Z_1Z_3 after applying X_2 or X_3, we can build up the following table:

	error		
measurement	X_1	X_2	X_3
Z_1Z_2	-1	-1	$+1$
Z_2Z_3	$+1$	-1	-1

Therefore, we can use the results of measuring Z_1Z_2 and Z_2Z_3 to deduce whether X_1, X_2, X_3, or no error occurred ($+1$ is obtained in both measurements). Then, since $X_i^2 = I$, all we have to do is apply the right X operator again to correct the error.

The codewords are also eigenstates of Z_1Z_3 with eigenvalue $+1$, and they become eigenstates with eigenvalue -1 after a single bit flip error occurs. This is not independent information, however, since $Z_1Z_3 = (Z_1Z_2)(Z_2Z_3)$. More generally, $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are the $+1$ eigenstates of the *group* generated by Z_1Z_2 and Z_2Z_3. We call this group the *stabilizer group*, S. Z_1Z_2 and Z_2Z_3 are called *stabilizer generators*, and we write $S = \langle Z_1Z_2, Z_2Z_3\rangle$. This formalism generalizes in a powerful way, resulting in a class of QECCs that are called *stabilizer codes*. For an introduction to these codes, see [25].

While we can correct a single bit flip, a single phase flip (Z_1, Z_2, or Z_3) on the other hand is bad news. From Eq. (49), we see that

$$Z_i|\bar{0}\rangle = |\bar{1}\rangle \qquad Z_i|\bar{1}\rangle = |\bar{0}\rangle. \tag{52}$$

In other words, each Z_i is a representation of a *logical* $\bar{X}$ operator, and so a single erroneous phase flip results in a change of the logical state of the encoded qubit. (Analogously, the logical $\bar{Z}$ operator is given by $\bar{Z} = X_1X_2X_3$.) Unfortunately, this QECC is not very robust.

4.1.2 The 9-qubit Shor code

The 3-qubit code protected against a bit flip error, so perhaps more copies of this code can protect against a phase flip as well. This is the gist of the 9-qubit Shor code [24, 26]. Suppose we have 9 physical qubits and that we encode our logical qubit as follows:

$$|\bar{0}\rangle := (|000\rangle + |111\rangle)^{\otimes 3} \qquad |\bar{1}\rangle := (|000\rangle - |111\rangle)^{\otimes 3} \tag{53}$$

Each codeword is made of three blocks, each of which is a copy of the corresponding 3-qubit codeword. As such, we can detect a single bit flip in each block (for a total of up to 3 bit flips) by measuring the operators

$$Z_1Z_2,\ Z_2Z_3,\ Z_4Z_5,\ Z_5Z_6,\ Z_7Z_8,\ Z_8Z_9. \tag{54}$$

This time, we can also detect a single phase flip (in total) by measuring the operators

$$X_1X_2X_3X_4X_5X_6,\ X_4X_5X_6X_7X_8X_9. \tag{55}$$

Again notice that $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are $+1$ eigenstates of these two operators. Suppose, for example, that Z_5 gets applied erroneously. Then for an arbitrary logical state, we have that

$$\begin{aligned} X_1X_2X_3X_4X_5X_6(Z_5(a|\bar{0}\rangle + b|\bar{1}\rangle)) &= -Z_5(a|\bar{0}\rangle + b|\bar{1}\rangle) \\ X_4X_5X_6X_7X_8X_9(Z_5(a|\bar{0}\rangle + b|\bar{1}\rangle)) &= -Z_5(a|\bar{0}\rangle + b|\bar{1}\rangle). \end{aligned} \tag{56}$$

Proceeding similarly, we can build up a table as we did before:

	error		
measurement	Z_1 or Z_2 or Z_3	Z_4 or Z_5 or Z_6	Z_7 or Z_8 or Z_9
$X_1X_2X_3X_4X_5X_6$	-1	-1	$+1$
$X_4X_5X_6X_7X_8X_9$	$+1$	-1	-1

Therefore, by measuring these two strings of X operators, we can figure out in which block the phase flip occurred. It does not matter that we are ignorant of which particular qubit experienced the Z error, since applying Z to any qubit in the right block will flip the phase back.

In the language of stabilizer codes, the stabilizer group is generated by the operators (54) and (55). We also see that representatives of the logical $\bar{Z}$ and $\bar{X}$ operators are

$$\bar{Z} = X_1X_2X_3 \qquad \bar{X} = Z_1Z_4Z_7. \tag{57}$$

Multiplying these representations by elements of the stabilizer group produces different equivalent representations of the logical $\bar{Z}$ and $\bar{X}$ operators.

Already in these two examples we see the features of QECCs that we highlighted before. These two codes encode logical information nonlocally across 3 and 9 qubits, respectively, and they cannot correct arbitrary errors. Error diagnosis is always carried out by performing collective measurements that access several physical qubits at once. It is imperative that we never make any local measurements so that we do not disturb the computational state. Such measurements are typically made using extra *ancillary* qubits. For example, Exercise 5 discusses how to collectively and non-destructively measure Z_1Z_2 and $X_1X_2X_3X_4X_5X_6$.

4.2 Quantum error correction as a quantum channel

Schematically, we can represent quantum error correction as a series of steps, as shown in Fig. 3. We start with some initial logical state $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$ that we encode in $\mathcal{H}_{\text{phys}}$. Noise then gets applied to the encoded state, which we then attempt to recover from and decode to get back to a logical state $\tilde{\rho}$. For error correction to be successful, we must have $\tilde{\rho} \approx \rho$.

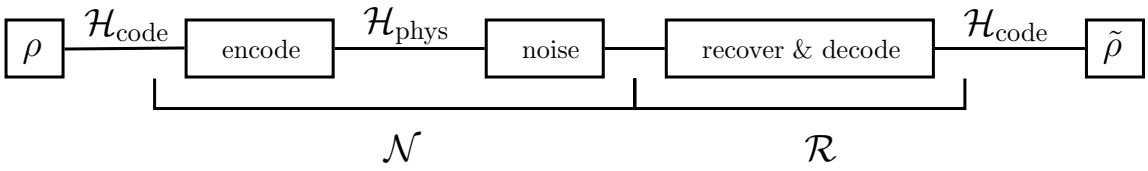


Figure 3: Quantum error correction as a quantum channel.

Each one of the steps in this process—encoding, noise, recovery, and decoding—is a quantum channel. If we denote the encoding and noise steps by the channel $\mathcal{N}$ and the recovery and decoding steps by the channel $\mathcal{R}$, then the signature of successful error correction is

$$(\mathcal{R} \circ \mathcal{N})(\rho) \approx \rho. \tag{58}$$

In other words, we want to *reverse* the channel $\mathcal{N}$ as best as is possible.

What are the criteria that ensure that error correction will be successful? In other words, given an encoding and noise channel $\mathcal{N}$, when does there exist a faithful recovery channel $\mathcal{R}$? We can gain some heuristic intuition by considering the purified theory. Recall from Sec. 3.3.2 that we can think of any quantum channel as being a unitary process in a larger Hilbert space. If we call $\mathcal{H}_{\text{code}}$ the system, S, which we augment with ancillas, A, that are used in encoding and decoding, as well as an environment, E, that participates in the noisy interactions, then a unitary version of the error correction process is as shown in Fig. 4. Heuristically, it must be that the final state of E cannot depend on the initial state of S in order for no information to be lost and for perfect recovery to be possible.

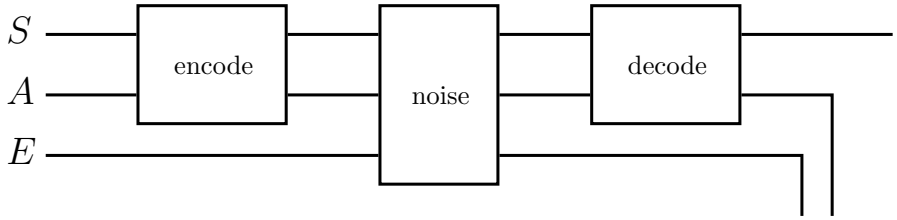


Figure 4: Quantum error correction as a unitary process.

More precisely, the following theorem lays out when it is possible to exactly reverse a quantum channel [27]:

Theorem 4.1 (Petz and Ohya)**.** *Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel and $Q \subseteq \mathcal{S}(\mathcal{H}_A)$. $\mathcal{N}$ is exactly reversible on Q if and only if*

$$D(\rho \,\|\, \sigma) = D(\mathcal{N}(\rho) \,\|\, \mathcal{N}(\sigma)) \tag{59}$$

for all $\rho, \sigma \in Q$. Furthermore, for any $\sigma \in Q$ such that $\operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$ for all $\rho \in Q$, a channel that undoes the action of $\mathcal{N}$ is

$$\mathcal{P}_{\sigma,\mathcal{N}} \,:\, \rho \,\mapsto\, \sigma^{1/2}\mathcal{N}^{\dagger}\left[\mathcal{N}(\sigma)^{-1/2}\,\rho\,\mathcal{N}(\sigma)^{-1/2}\right]\sigma^{1/2}. \tag{60}$$

The channel $\mathcal{P}_{\sigma,\mathcal{N}}$ is called the *Petz map*. While the Petz map is somewhat complicated, the criterion for exact recovery, $D(\rho\,\|\,\sigma) = D(\mathcal{N}(\rho)\,\|\,\mathcal{N}(\sigma))$, has a clear meaning in light of Thm. 3.10: A channel $\mathcal{N}$ is only reversible for a collection of states when $\mathcal{N}$ does not reduce their distinguishability.

A complete proof of Petz and Ohya's theorem is well beyond what we can succinctly accomplish here. If you are interested in seeing the proof, Chapter 12 of Ref. [2] is largely devoted to this. It's almost trivial that $(\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\sigma) = \sigma$ (the only missing step is showing that $\mathcal{N}^\dagger(I) = I$). The harder part is showing that $(\mathcal{P}_{\sigma,\mathcal{N}} \circ \mathcal{N})(\rho) = \rho$ for other $\rho \in Q$. Instead, let's check that the Petz map works for a specific simple example.[8]

Example 4.2. Let $\dim \mathcal{H}_{\text{code}} = d_{\text{code}}$ and suppose that we use an isometry, V, to embed $\mathcal{H}_{\text{code}}$ into a larger Hilbert space with the tensor product structure $\mathcal{H}_{\text{phys}} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$. Explicitly,

$$V : \mathcal{H}_{\text{code}} \to \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}, \qquad V^\dagger V = I_{\text{code}}, \qquad \text{and} \qquad VV^\dagger = \Pi_{\text{code}}, \tag{61}$$

where Π_{code} is the projector onto $V(\mathcal{H}_{\text{code}}) \subset \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$. Define a channel

$$\begin{aligned} \mathcal{N} \;:\; \mathcal{S}(\mathcal{H}_{\text{code}}) &\to \mathcal{S}(\mathcal{H}_A) \\ \rho &\mapsto \text{Tr}_{\bar{A}}(V\rho V^\dagger), \end{aligned} \tag{62}$$

which embeds a code state ρ into $\mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ and then "erases" $\mathcal{H}_{\bar{A}}$. Let's also fix a full-rank fiducial state $\sigma \in \mathcal{S}(\mathcal{H}_{\text{code}})$, i.e., letting $\{|a\rangle_{\text{code}}\}_{a=1}^{d_{\text{code}}}$ be a basis for $\mathcal{H}_{\text{code}}$, pick a state $\sigma = \sum_{a=1}^{d_{\text{code}}} \sigma_a |a\rangle\langle a|$ with each $\sigma_a \neq 0$.

For exact recovery to be possible on all of $\mathcal{H}_{\text{code}}$, information cannot leak into $\bar{A}$ and become lost when we trace this factor out. Therefore, in a setting where exact recovery is possible, we must have

$$\mathcal{H}_A \cong \mathcal{H}_1 \otimes \mathcal{H}_2 \oplus \mathcal{H}_3, \tag{63}$$

where $\dim \mathcal{H}_1 \equiv d_1 = d_{\text{code}}$, $\dim \mathcal{H}_2 \equiv d_2 \geq 1$, and $\dim \mathcal{H}_3 \equiv d_3 \geq 0$. (The space $\mathcal{H}_3$ plays no other role than to make sure that the dimensions $d_1 d_2 + d_3$ add up to d_A.) In this case, we can choose a basis of $\mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$ such that

$$V|a\rangle_{\text{code}} = |a\rangle_1 \otimes |\chi\rangle_{2\bar{A}}, \tag{64}$$

where $|\chi\rangle_{2\bar{A}} \in \mathcal{H}_2 \otimes \mathcal{H}_{\bar{A}}$ is the same fixed state for every $1 \leq a \leq d_{\text{code}}$.

Now, let's piece together the action of the Petz map. We first evaluate $\mathcal{N}(\sigma)$:

$$\begin{aligned} \mathcal{N}(\sigma) &= \text{Tr}_{\bar{A}}\left[\sum_{a=1}^{d_{\text{code}}} \sigma_a |a\rangle\langle a|_1 \otimes |\chi\rangle\langle\chi|_{2\bar{A}}\right] \\ &= \left(\sum_{a=1}^{d_{\text{code}}} \sigma_a |a\rangle\langle a|_1\right) \otimes \text{Tr}_{\bar{A}}\,|\chi\rangle\langle\chi|_{2\bar{A}} \\ &\equiv \sigma_1 \otimes \chi_2 \end{aligned}$$

[8] This example is inspired by an example that appears in Ref. [28] to illustrate a novel kind of entanglement wedge reconstruction in AdS/CFT.

Therefore, it follows that $\mathcal{N}(\sigma)^{-1/2} = \sigma_1^{-1/2} \otimes \chi_2^{-1/2}$. Similarly, for an arbitrary state $\rho = \sum_{b,c=1}^{d_{\text{code}}} \rho_{bc}|b\rangle\langle c|_{\text{code}}$, one finds that $\mathcal{N}(\rho) = \rho_1 \otimes \chi_2$. We therefore arrive at

$$\mathcal{N}(\sigma)^{-1/2}\mathcal{N}(\rho)\mathcal{N}(\sigma)^{-1/2} = (\sigma^{-1/2}\rho\sigma^{-1/2})_1 \otimes I_2. \tag{65}$$

The next step is to deduce the action of $\mathcal{N}^\dagger$. Let $\langle M, N\rangle \equiv \text{Tr}(M^\dagger N)$ denote the operator inner product. Letting $\tau, \omega \in \mathcal{S}(\mathcal{H}_{\text{code}})$, from the definition of the adjoint, we have:

$$\begin{aligned}\langle \mathcal{N}(\tau), \omega_1 \otimes I_2\rangle_A &= \text{Tr}_A[(\tau_1 \otimes \chi_2)(\omega_1 \otimes I_2)] \\ &= \text{Tr}_1(\tau\omega)\,\text{Tr}_2(\chi) \\ &= \text{Tr}_{\text{code}}\left[\tau\left([\text{Tr}\,\chi]\omega\right)\right] \\ &= \langle \tau, (\text{Tr}\,\chi)\omega\rangle_{\text{code}}\end{aligned}$$

Therefore, $\mathcal{N}^\dagger(\omega_1 \otimes I_2) = (\text{Tr}\,\chi)\omega_{\text{code}}$.

Putting it all together, we therefore have that

$$\begin{aligned}\mathcal{P}_{\sigma,\mathcal{N}}[\mathcal{N}(\rho)] &= \sigma^{1/2}(\sigma^{-1/2}\rho\sigma^{-1/2})\sigma^{1/2} \cdot \text{Tr}\,\chi \\ &= \rho \cdot \text{Tr}\,\chi\end{aligned} \tag{66}$$

But, notice that

$$\text{Tr}\,\chi = \text{Tr}_2(\text{Tr}_{\bar{A}}[|\chi\rangle\langle\chi|_{2\bar{A}}]) = \langle\chi|\chi\rangle_{2\bar{A}} = 1, \tag{67}$$

and so we indeed find that $\mathcal{P}_{\sigma,\mathcal{N}}[\mathcal{N}(\rho)] = \rho$.

Since the Petz map perfectly recovers all states in $\mathcal{H}_{\text{code}}$, Petz and Ohya's theorem guarantees that the recoverability condition (59) holds. Nevertheless, this can also be verified by direct computation:

$$D(\mathcal{N}(\rho)\,\|\,\mathcal{N}(\sigma)) = D(\rho_1 \otimes \chi_2\,\|\,\sigma_1 \otimes \chi_2) = D(\rho\,\|\,\sigma) \tag{68}$$

The last equality is derived in Exercise 6 in Sec. 7. □

The Petz map is a remarkable constructive result; however, a limitation of Thm. 4.1 is that it only lays out criteria for when a channel can be perfectly reversed. If the condition (59) does not hold or only approximately holds, then Thm. 4.1 does not say if and how well the Petz map will work. The following theorem of Junge, Renner, Sutter, Wilde, and Winter lays out precisely this refinement [29]:

Theorem 4.3 (Universal Recovery)**.** *Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a quantum channel. For all $\rho, \sigma \in \mathcal{S}(\mathcal{H}_A)$ such that* $\text{supp}\,\rho \subseteq \text{supp}\,\sigma$*, the recovery channel*

$$\mathcal{R}_{\sigma,\mathcal{N}}(\rho) = \int_{\mathbb{R}} dt\, \beta_0(t)\sigma^{-it/2}\mathcal{P}_{\sigma,\mathcal{N}}\left[\mathcal{N}(\sigma)^{it/2}\,\rho\,\mathcal{N}(\sigma)^{-it/2}\right]\sigma^{it/2}, \tag{69}$$

where $\beta_0(t) = \frac{\pi}{2}(\cosh(\pi t) + 1)^{-1}$, satisfies

$$D(\rho\,\|\,\sigma) - D(\mathcal{N}(\rho)\,\|\,\mathcal{N}(\sigma)) \geq -2\log F(\rho, \mathcal{R}_{\sigma,\mathcal{N}} \circ \mathcal{N}[\rho]). \tag{70}$$

The function $F(\rho,\sigma) = \|\rho^{1/2}\sigma^{1/2}\|_1$ is known as *fidelity*. It is another measure of the closeness of two states, taking values between 0 and 1 and saturating at $F(\rho,\rho) = 1$. The theorem above therefore says that the faithfulness with which $\mathcal{R}_{\sigma,\mathcal{N}}$ succeeds in reversing the action of $\mathcal{N}$ is upper bounded by the exact recoverability condition (59). In other words, the less a channel degrades the distinguishability of states on which it acts, the better its action can be reversed for these states. The map $\mathcal{R}_{\sigma,\mathcal{N}}$ is known as a *universal recovery channel*.

5. An application to holography

The Anti de Sitter/Conformal Field Theory (AdS/CFT) correspondence is a remarkable duality between certain gravitational theories and certain quantum field theories without gravity [30, 31]. In that sense, AdS/CFT is a genuine theory of quantum gravity, and so even if the gravitational side of the duality differs somewhat from the space-time of our Universe as we know it, AdS/CFT remains a window into quantum gravity.

In these notes, we will take AdS/CFT to mean the following:

> Among certain quantum field theories without gravity in d space-time dimensions called conformal field theories (CFTs), certain CFTs are exactly equivalent to quantum theories of asymptotically Anti de Sitter (AdS) space-times in $d+1$ dimensions. Moreover, in the right limit, certain CFT states are in exact correspondence with certain fixed asymptotically AdS space-times.

I like to think of the definition above as "AdS/CFT: the conjecture," which is to be distinguished from "AdS/CFT: the theorem." The latter refers to the precise and rigorous correspondence between specific superconformal field theories and specific string theories in specific limits and in specific numbers of dimensions. The former envisions a much broader scope of applicability, but has correspondingly less backing by formal calculations in string theory and conformal field theory. Nevertheless, the broader applicability has made it possible to use tools and techniques from quantum information to study the correspondence, which has given us deep information-theoretic insights into AdS/CFT, and more generally (we think) quantum gravity itself.

We will not go into any precise details of AdS/CFT in these notes. All we will do is illustrate the basic idea of the duality with a simple example and then point out the information-theoretic connection. For a more comprehensive introduction to AdS/CFT, Ref. [32] is one place you could start. Afterwards, we will see how the information-theoretic tools that we have developed can be used to relate operators on the gravitational side of the duality to corresponding operators in the dual field theory.

5.1 How to bluff your way through AdS/CFT

A CFT is a quantum field theory with a specific set of symmetries (namely, conformal symmetry) which make it so that there is no inherent absolute notion of scale in the theory. We say that a CFT is *holographic* when it has a dual gravitational description in terms of asymptotically AdS space-times. In the simplest case, the ground state of a holographic CFT in d space-time dimensions is dual to pure $(d+1)$-dimensional AdS space-time.

AdS is a maximally symmetric space-time with constant negative curvature. In an appropriate set of coordinates, one way to visualize AdS_{d+1} is as a cylinder, as shown in Fig. 5. Time τ runs up along the cylinder, and slices of the cylinder are d-dimensional hyperbolic spaces. The *Poincaré patch* is only a portion of AdS_{d+1}, but it is covered by a simple set of coordinates that makes the geometry easy to understand:

$$ds^2 = \frac{L^2}{z^2}\left(-dt^2 + dz^2 + dx_i dx^i\right) \tag{71}$$

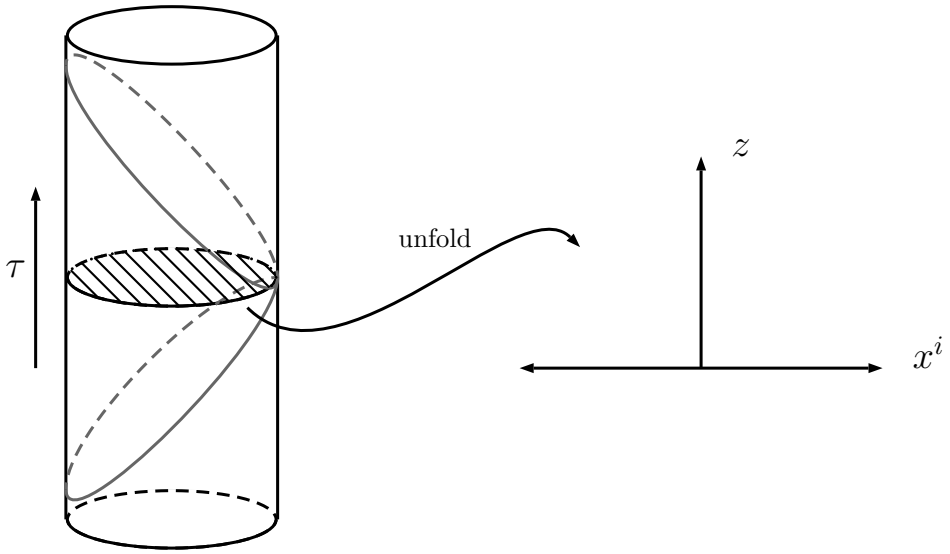


Figure 5: Anti de Sitter space-time. Slices of the global cylinder are hyperbolic spaces. The Poincaré patch is the space-time in between the two tilted circles. Unfolding the $\tau = 0$ slice gives us the a slice of the Poincaré patch in planar coordinates, where proper distances increase as one approaches the boundary at $z = 0$.

L is called the AdS length, and it is related to the cosmological constant by

$$\Lambda = -\frac{d(d-1)}{2L^2}. \tag{72}$$

If we take the $\tau = 0$ slice of the cylinder in Fig. 5 (which coincides with $t = 0$) and imagine making an incision at a point on its boundary, then we can unfold the slice into an upper half-plane as shown in the right side of Fig. 5. The coordinate z starts at $z = 0$ at the boundary and increases as we move into the AdS bulk, and the x^i coordinates are parallel to the boundary. In this plane, the interpretation of the line element (71) is clear: Setting $dt = dz = 0$, we see that a small fixed coordinate displacement dx^i has larger proper length the closer we are to the AdS boundary. Notice that the AdS boundary has d space-time dimensions. As such, it is often very convenient to think of the dual CFT as living on the AdS boundary.

In general, the connection that quantum information has to AdS/CFT is that *information-theoretic quantities in the boundary CFT correspond to geometric quantities in the AdS bulk*. The most basic example of this is a formula that relates the entanglement entropy of a reduced state in the boundary CFT to the area of an extremal surface in the AdS bulk.

Let A be a (spacelike) subregion of a holographic boundary CFT state that is dual to a fixed asymptotically AdS space-time, and let ρ_A be the reduced CFT state on this subregion. Then, its entropy is given by

$$S(\rho_A) = \min \operatorname*{ext}_{A\sim\tilde{A}} \frac{\text{area}(\tilde{A})}{4G_N} + O(G_N^0). \tag{73}$$

The formula above says that we look for co-dimension 2 spacelike surfaces $\tilde{A}$ in the bulk that are *extremal*, meaning that their area is locally stationary under null variations (equivalently, the expansions of orthogonal null congruences anchored to the boundary of $\tilde{A}$ vanish). Furthermore,

$A \sim \tilde{A}$ denotes that $\tilde{A}$ must be *homologous* to A, meaning that it can be smoothly deformed into A. Then, if there are many such surfaces $\tilde{A}$, we take the one with the smallest area, and $1/4$ of this area in Planck units gives $S(\rho_A)$. Fig. 6 illustrates this geometry.

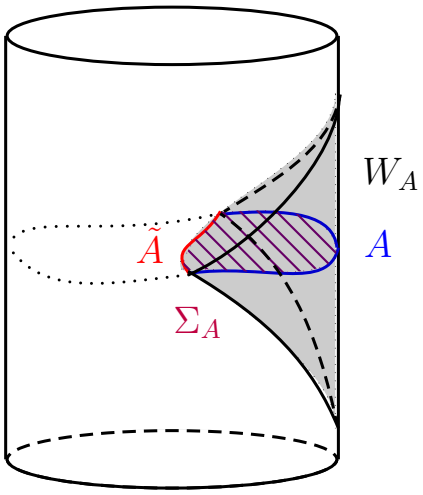


Figure 6: Various geometric objects: a boundary subregion, A (blue); the HRT surface, $\tilde{A}$ (red); the entanglement wedge, W_A (shaded grey); and a complete spacelike slice through the entanglement wedge, Σ_A, such that $\partial\Sigma_A = A \cup \tilde{A}$ (hatched purple).

Eq. (73) is known as the *Hubeny-Rangamani-Takayanagi* (HRT) formula, and the smallest-area extremal surface is called the *HRT surface of A* [33]. As a historical note, this is a refinement of the original entropy formula due to Ryu and Takayanagi (RT), which is applicable to the case where the dual space-time is static [34]. In this case, one only needs to look for minimal surfaces in a spacelike slice of the space-time, and so the RT formula more simply reads

$$S(\rho_A) = \min_{A\sim\tilde{A}} \frac{\text{area}(\tilde{A})}{4G_N} + O(G_N^0). \tag{74}$$

5.2 Bulk reconstruction

If AdS/CFT is to be a true duality, then *any* quantity in the bulk AdS must be encoded somehow in the boundary CFT. Naturally, then, we might ask: What do bulk operators look like in the boundary CFT, or equivalently, how do we reconstruct bulk operators using boundary CFT operators? This is the subject of *bulk reconstruction*.

5.2.1 The extrapolate dictionary

One of the earliest answers to this question was given by Hamilton, Kabat, Lifshytz, and Lowe (HKLL) for a free scalar field ϕ of mass m in AdS_{d+1} [35]. HKLL is based on the "extrapolate dictionary,"

$$\lim_{r\to\infty} r^{\Delta}\phi(r,t,x^i) = O(t,x^i), \tag{75}$$

where $r \propto z^{-1}$ so that $r \to \infty$ is the AdS boundary. The extrapolate dictionary basically says that ϕ is in correspondence with an operator O in the boundary CFT (a primary operator with scaling dimension Δ that is related to m, L, and d) if you push ϕ to the boundary while weighting it with

a factor r^{Δ}. You would be right to think that Eq. (75) is a bit incongruous, since it looks like we are equating a bulk AdS operator on the left side with a boundary CFT operator on the right side. More correctly, the basic strategy is to look for a CFT operator $\tilde{\phi}$ that satisfies (75) (with $\phi \to \tilde{\phi}$, of course) as well as an equation of motion

$$(\Box - m^2)\tilde{\phi} = 0, \tag{76}$$

where $\Box$ is the scalar d'Alembertian coming from the bulk theory for ϕ. In other words, $\tilde{\phi}$ is a CFT operator that depends on the boundary coordinates (t, x^i), but that also has an additional parameter r so that it altogether satisfies Eqs. (75) and (76).

HKLL showed that such an operator may be expressed as

$$\tilde{\phi}(x) = \int dX K(x, X) O(X), \tag{77}$$

where $x \equiv (r, t, x^i)$ denotes a bulk point and $X \equiv (t, x^i)$ denotes a boundary point. The function $K(x, X)$ is known as the *smearing function*, and it ends up being expressed in terms of the mode functions of ϕ. The boundary operator $\tilde{\phi}$ succeeds in reconstructing the bulk operator ϕ in the sense that boundary expectation values of $\tilde{\phi}$ reproduce the bulk expectation values of ϕ:

$$\langle \phi(x_1)\phi(x_2)\cdots\rangle_{\text{AdS}} = \langle \tilde{\phi}(x_1)\tilde{\phi}(x_2)\cdots\rangle_{\text{CFT}} \tag{78}$$

The smearing function $K(x, X)$ has the property that it is only non-zero on boundary points that are spacelike-separated from x, as shown in Fig. 7. If we pick a single Cauchy slice Γ of the boundary within the support of K, then it turns out that it's possible to propagate $K(x, X)$ backwards and forwards towards this slice to obtain a new smearing function that only has support on Γ. In some sense, this results in a more "efficient" boundary representation of ϕ. In the next subsection, we will see that entanglement wedge reconstruction leads to even more efficient representations.

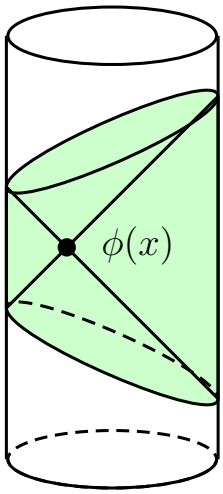


Figure 7: In the HKLL reconstruction of a bulk operator $\phi(x)$, only boundary points that are spacelike-separated from x contribute to the reconstruction, shown shaded.

5.2.2 Entanglement wedge reconstruction and error correction

Let's begin by defining the entanglement wedge.

Definition 5.1. *Given a boundary subregion A with a HRT surface $\tilde{A}$, the* entanglement wedge *of A, denoted W_A, is the bulk domain of dependence of any spacelike surface Σ_A such that $\partial\Sigma_A = A \cup \tilde{A}$.*

Note: The domain of dependence of Σ_A is the collection of points p such that any causal curve through p intersects Σ_A, and $\partial\Sigma_A$ denotes the boundary of Σ_A.

An example of an entanglement wedge is illustrated in Fig. 6 above.

The entanglement wedge is important for bulk reconstruction because if a bulk operator has support on W_A, then it can be represented by a CFT operator that has support only on A. This principle is known as *entanglement wedge reconstruction*. Moreover, it establishes a notion of equivalence between specific bulk and boundary regions that we call *subregion-subregion duality*. In the sense of bulk reconstruction at least, a boundary subregion A is dual to its entanglement wedge W_A in the bulk. This characterization of entanglement wedge reconstruction is fairly imprecise, but we will look at a much more careful and precise version in the next subsection.

We should note that entanglement wedge reconstruction raises a question of interpretation that we will also address precisely. For any given bulk operator whose support is not the entire bulk, then there is no unique boundary subregion whose entanglement wedge contains that operator, as shown in Fig. 8. It would then seem that it's possible to represent the same bulk operator with different CFT operators on different boundary subregions that need not have any overlap. In what sense are these different CFT operators the "same"?

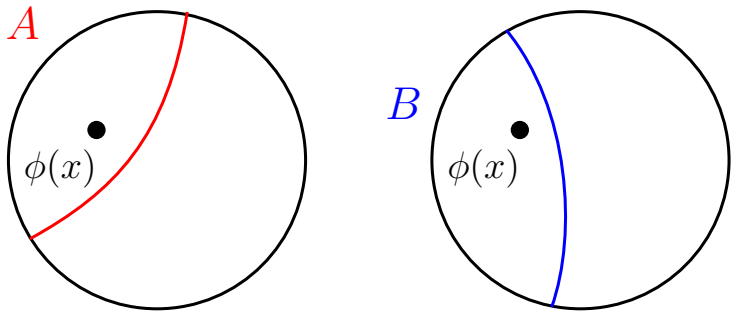


Figure 8: A single operator $\phi(x)$ is in the entanglement wedge of infinitely many boundary subregions.

The answer that we will substantiate in the next section is that we can think of the encoding of bulk operators in the CFT boundary as a quantum error correcting code that protects against deletion of portions of the boundary. The bulk is encoded nonlocally and redundantly in the boundary such that we can recover a given bulk operator provided we hold enough of the boundary. Moreover, once a bulk operator has been encoded in the boundary via AdS/CFT, we can think of its reconstruction as a CFT operator on a subregion A as a recovery map on A after having discarded the complementary region $\bar{A}$, just as in Ex. 4.2.

5.2.3 Bulk reconstruction as a universal recovery channel

Currently, the most precise characterization of entanglement wedge reconstruction is the following one, due to Cotler, Hayden, Penington, Salton, Swingle, and Walter [36].

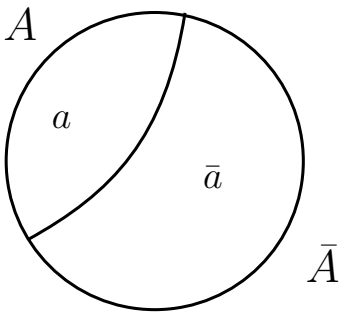


Figure 9: Operators in a can be reconstructed on A.

Given a holographic CFT and a boundary subregion A, write $\mathcal{H}_{\text{CFT}} = \mathcal{H}_A \otimes \mathcal{H}_{\bar{A}}$, and correspondingly factorize $\mathcal{H}_{\text{bulk}} = \mathcal{H}_a \otimes \mathcal{H}_{\bar{a}}$, where a is a Cauchy surface for W_A and $a \cup \bar{a}$ is a Cauchy surface for the entire bulk.[9] This is illustrated in Fig. 9. Let $\mathcal{H}_{\text{code}} \subset \mathcal{H}_{\text{bulk}}$ be generated by a finite collection of states that have the same dual bulk geometry in a neighbourhood of a up to corrections that are $O(\sqrt{G_N})$ in size (so that the bulk factorization makes sense for all code states, among other reasons). We assume that the AdS/CFT correspondence supplies us with an isometry $J : \mathcal{H}_{\text{code}} \hookrightarrow \mathcal{H}_{\text{CFT}}$ that embeds $\mathcal{H}_{\text{code}}$ into $\mathcal{H}_{\text{CFT}}$. Then, given a bulk operator $\phi_a \in \mathcal{L}(\mathcal{H}_a)$, our goal is to find a CFT operator $O_A \in \mathcal{L}(\mathcal{H}_A)$ such that

$$\left|\langle O_A\rangle_{J\rho J^\dagger} - \langle \phi_a\rangle_\rho\right| \leq \delta\|\phi_a\| \tag{79}$$

for all $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$. $\langle O_A\rangle_{J\rho J^\dagger}$ denotes a CFT expectation value with respect to the state $J\rho J^\dagger$, $\langle\phi_a\rangle_\rho$ denotes a bulk expectation value with respect to ρ, δ is a small fixed constant, and $\|\phi_a\| \equiv \max_{\|v\|=1}\|\phi_a v\|$ is the operator norm of ϕ_a. We will call success in this task "entanglement wedge reconstruction."

There is an important additional result from AdS/CFT due to Jafferis, Lewkowycz, Maldacena, and Suh (JLMS) [37] that we will need in order to bound the left side of (79). In terms of the language that we are using here, the result reads

$$|D(\rho_A\,\|\,\sigma_A) - D(\rho_a\,\|\,\sigma_a)| \leq O(\sqrt{G_N}) \qquad \forall\,\rho,\sigma \in \mathcal{S}(\mathcal{H}_{\text{code}}), \tag{80}$$

where $\rho_a = \text{Tr}_{\bar{a}}\,\rho$ and $\rho_A = \text{Tr}_{\bar{A}}[J\rho J^\dagger]$ (and similarly for σ). In particular, this result is what fixes the region that we can reconstruct, a, to be the entanglement wedge of A.

The first strategy that comes to mind is to try mimicking what we did in Ex. 4.2. If we define a channel $\tilde{\mathcal{N}}(\rho) = \text{Tr}_{\bar{A}}[J\rho J^\dagger]$, then we can write down a universal recovery channel for it. Then, applying the bound from Thm. 4.3, perhaps we can use the JLMS bound on relative entropy to arrive at the desired inequality (79)?

A problem with this simple strategy is that $\text{Tr}_{\bar{A}}[J\rho J^\dagger]$ in principle depends on $\bar{a}$ as well. If we are really after reconstruction in the *entanglement wedge*, then all of our results had better only depend on states defined on a and A. While we therefore cannot immediately declare victory, it turns out that only minor modifications are needed to get an approach that works.

[9] Following Cotler *et al.*, we assume that the Hilbert spaces factorize for convenience. This is not a given for a holographic CFT; however, all of their arguments can be made more carefully at the level of operator algebras without assuming Hilbert space factorization.

The proof proceeds in 3 steps. First, one defines a channel

$$\mathcal{N}(\rho_a) = \mathrm{Tr}_{\bar{A}}\left[J\left(\rho_a \otimes \bar{\sigma}_{\bar{a}}\right)J^\dagger\right], \tag{81}$$

where $\bar{\sigma}_{\bar{a}} \in \mathcal{S}(\mathcal{H}_{\bar{a}})$ is some fixed full-rank state that we choose. Choosing another full-rank state $\sigma_a \in \mathcal{S}(\mathcal{H}_a)$, Thm. 4.3 supplies us with a universal recovery map $\mathcal{R}_{\sigma_a,\mathcal{N}}$ such that Eqs. (70) and (80) give us

$$-2\log F(\rho_a, \mathcal{R}_{\sigma_a,\mathcal{N}} \circ \mathcal{N}[\rho_a]) \leq |D(\rho_A \,\|\, \sigma_A) - D(\rho_a \,\|\, \sigma_a)| \leq \epsilon, \tag{82}$$

for all $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$ of the form $\rho_a \otimes \bar{\sigma}_{\bar{a}}$, and where ϵ is a fixed constant of size $O(\sqrt{G_N})$. Second, one shows that this channel $\mathcal{R}_{\sigma_a,\mathcal{N}}$ still succeeds in reversing $\mathcal{N}$ for arbitrary $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$ by using the bound (82) to show that

$$\| \rho_a - \mathcal{R}[\mathrm{Tr}_{\bar{A}}(J\rho J^\dagger)] \|_1 \leq \delta, \tag{83}$$

where we have dropped the subscript on $\mathcal{R}$ for neatness and where δ is another parametrically small constant that depends on ϵ. (In other words, here we start with an arbitrary $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$, trace out $\bar{a}$ to obtain ρ_a, and then try to recover $\mathcal{N}(\rho_a)$ with $\mathcal{R}$, which is *a priori* only guaranteed to work well had ρ taken the specific form $\rho = \rho_a \otimes \bar{\sigma}_{\bar{a}}$.) Third, one defines the operator

$$O_A = \mathcal{R}^\dagger[\phi_a] \tag{84}$$

and shows that it satisfies Eq. (79).

The technical steps of the proof are not too difficult to follow either, provided that you are willing to refer to a couple of other sources for the proofs of some inequalities. The calculation given here is essentially verbatim the calculation from Cotler *et al.* [36], although I have explained a handful of inequalities to make these notes self-contained.

First, with the bound (82) in hand, one uses the Fuchs-Van de Graaf inequality [38] to show that

$$\|\rho_a - \mathcal{R}(\mathcal{N}[\rho_a])\|_1 \leq 2\sqrt{\epsilon} \equiv \delta_1. \tag{85}$$

for all $\rho_a \in \mathcal{S}(\mathcal{H}_a)$.

To attack the second step, let $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}})$, $\rho_a = \mathrm{Tr}_{\bar{A}}\,\rho$, and observe that

$$\begin{aligned}\|\mathcal{N}(\rho_a) - (J\rho J^\dagger)_A\|_1^2 &= \|(J\,\rho_a \otimes \bar{\sigma}_a\,J^\dagger)_A - (J\rho J^\dagger)_A\|_1^2 \\ &\leq (2\log 2) D((J\,\rho_a \otimes \bar{\sigma}_a\,J^\dagger)_A \,\|\, (J\rho J^\dagger)_A).\end{aligned} \tag{86}$$

Following Cotler *et. al*, we use a bracket with a subscript to denote a partial trace, i.e., $(O)_A \equiv \mathrm{Tr}_{\bar{A}}(O)$. To go to the second line, we used Pinsker's inequality (14). Next, we apply JLMS to a "trivial" case to obtain

$$|D(\rho_a \,\|\, \rho_a) - D((J\,\rho_a \otimes \bar{\sigma}_a\,J^\dagger)_A \,\|\, (J\rho J^\dagger)_A)| \leq \epsilon. \tag{87}$$

$D(\rho_a \,\|\, \rho_a) = 0$ of course, and so letting $(2\log 2)\epsilon \equiv \delta_2^2$, we combine Eqs. (86) and (87) to obtain

$$\|\mathcal{N}(\rho_a) - (J\rho J^\dagger)_A\|_1 \leq \delta_2. \tag{88}$$

Finally, we have the following calculation:

$$\begin{aligned}\| \rho_a - \mathcal{R}[(J\rho J^\dagger)_A] \|_1 &\leq \| \rho_a - \mathcal{R}(\mathcal{N}[\rho_a]) \|_1 + \| \mathcal{R}(\mathcal{N}[\rho_a]) - \mathcal{R}[(J\rho J^\dagger)_A] \|_1 \\ &\leq \| \rho_a - \mathcal{R}(\mathcal{N}[\rho_a]) \|_1 + \| \mathcal{N}(\rho_a) - (J\rho J^\dagger)_A \|_1 \\ &\leq \delta_1 + \delta_2 \equiv \delta\end{aligned}$$

In the first line we used the triangle inequality, and to go to the second line, we used the fact that $\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1 \leq \|\rho - \sigma\|_1$ for any channel $\mathcal{E}$ (for a proof, see [2, Exercise 9.1.9]). This completes the second step of the proof.

For the third step, we let $O_A := \mathcal{R}^\dagger[\phi_a]$ and calculate:

$$\begin{aligned}\left|\langle O_A\rangle_{J\rho J^\dagger} - \langle\phi_a\rangle_\rho\right| &= \left|\operatorname{Tr}\left[\mathcal{R}^\dagger[\phi_a](J\rho J^\dagger)_A\right] - \operatorname{Tr}[\phi_a\rho_a]\right| \\ &= \left|\operatorname{Tr}\left[\phi_a\mathcal{R}[(J\rho J^\dagger)_A]\right] - \operatorname{Tr}[\phi_a\rho_a]\right| \\ &= \left|\operatorname{Tr}\left[\phi_a\left(\mathcal{R}[(J\rho J^\dagger)_A] - \rho_a\right)\right]\right| \\ &\leq \left\|\phi_a\left(\mathcal{R}[(J\rho J^\dagger)_A] - \rho_a\right)\right\|_1 \\ &\leq \left\|\mathcal{R}[(J\rho J^\dagger)_A] - \rho_a\right\|_1 \|\phi_a\| \\ &\leq \delta\|\phi_a\|\end{aligned}$$

The only "new" ingredient that we used in these manipulations was Holder's inequality, $\|XY\|_1 \leq \|X\|_p\|Y\|_q$ for $p^{-1} + q^{-1} = 1$, to go from the fourth line to the fifth line (as well as the fact that $q \to \infty$ coincides with the operator norm). We therefore obtain an accurate reconstruction of ϕ_a in terms of an operator O_A that only has support on A.

6. Conclusion

These notes introduced a handful of core ideas in quantum information through the lens of quantum channels. In that sense, Sec. 3 was the core part of these notes, where we carefully defined what a channel is as well as certain channel properties. In particular, we drew on the relative entropy machinery that we developed in Sec. 2 to characterize a channel as a process that degrades distinguishability. This characterization would prove key to understanding quantum error correction as a channel in Sec. 4, where we viewed encoding and noise as a channel that we attempt to reverse through a decoding channel. We initially introduced universal recovery channels to this end, but they subsequently played a crucial role in Sec. 5 in interpreting bulk reconstruction in AdS/CFT as a quantum error correcting code.

The topics that we covered were chosen with an eye towards applications in high energy physics, particularly within the AdS/CFT correspondence, and so you should be well-equipped now to embark on further studies. For example, the question of how one recovers information from a black hole can be thought of as an attempt to reverse a channel, and tools that we saw, like the Petz map, are showing up in some of the most recent studies of this problem [23]. It's an exciting time to be studying quantum information in quantum gravity.

Acknowledgments

I am grateful to the Modave Organizing Committee for organizing this school and for giving me the opportunity to attend as a lecturer, and to Kwinten Fransen for carefully proofreading these notes and handling the editorial aspects of publication. I am also grateful to the other attendees and lecturers, whose contributions and interactions made the school a stimulating experience. I would like to thank John Preskill for giving his permission to include Exercises 2 and 3 in these notes. I am a Postdoctoral Fellow (Fundamental Research) of the Research Foundation – Flanders (Fonds Wetenschappelijk Onderzoek), File Number 12ZL920N, and this work was supported by this fellowship.

7. Exercises

The purpose of these exercises is to give you a chance work with some of the tools that were introduced in these notes while filling in technical details. Some of the exercises are based on homework problems that I had to solve when I was a student, and I am sure that that these problems or variations on them are still in use. For this reason, I have not included solutions to the exercises. Even so, if generations of students have made it through these problems in the past, I am sure that you will be able to do the same!

Exercise 1. The Schmidt decomposition
Let $\mathcal{H}_{AB}$ be a separable Hilbert space, i.e. it admits a countable basis of orthonormal eigenvectors. Furthermore, suppose that $\mathcal{H}_{AB}$ factorizes into the tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, and let $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$. We can always write

$$|\psi\rangle_{AB} = \sum_i \sum_\mu a_{i\mu} |i\rangle_A |\mu\rangle_B \tag{89}$$

where $\{|i\rangle_A\}$ and $\{|\mu\rangle_B\}$ are orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. For each i, let us define the vector $|\tilde{i}\rangle_B = \sum_\mu a_{i\mu}|\mu\rangle_B$, so that

$$|\psi\rangle_{AB} = \sum_i |i\rangle_A |\tilde{i}\rangle_B. \tag{90}$$

Note that the $|\tilde{i}\rangle_B$ need not be normalized nor orthogonal.

a) Suppose that $\{|i\rangle_A\}$ is the basis in which $\rho_A = \mathrm{Tr}_B\, |\psi\rangle\langle\psi|_{AB}$ is diagonal, and let the set S label the non-zero eigenvalues of ρ_A, i.e. $p_i \neq 0 \Leftrightarrow i \in S$. In other words,

$$\rho_A = \sum_{i\in S} p_i |i\rangle\langle i|_A. \tag{91}$$

Starting from Eq. (90), compute ρ_A by taking the partial trace over B and show that

$$\rho_A = \sum_i \sum_{i'} \langle\tilde{i}'|\tilde{i}\rangle_B |i\rangle\langle i'|_A. \tag{92}$$

b) Compare Eqs. (91) and (92). What do you conclude about the overlap $\langle\tilde{i}'|\tilde{i}\rangle$? Use this to write down a set of orthonormal vectors in B.

c) Write down $|\psi\rangle_{AB}$ using the basis $\{|i\rangle\}_A$ and the orthonormal set of vectors in B that you found above. What are the eigenvalues of ρ_B?

Note: This important result is known as the *Schmidt decomposition*. Any bipartite pure state $|\psi\rangle_{AB}$ can be written in the form

$$|\psi\rangle_{AB} = \sum_j \sqrt{p_j} |\phi_j\rangle_A |\chi_j\rangle_B, \tag{93}$$

where the vectors $|\phi_j\rangle_A$ and $|\chi_j\rangle_B$ are orthonormal in A and B, separately. Note that this decomposition is state-dependent. In general, if $|\omega\rangle_{AB}$ is some other state, then it will not have such a decomposition in terms of the same vectors.

Exercise 2. Distinguishability via the trace norm
Adapted with permission from Exercise 2.7 of J. Preskill, Lecture Notes for Ph219/CS219: Quantum Information and Computation*, Chapter 2 (2013 edition).*

In many cases, we would like to be able to meaningfully quantify how "close" two quantum states are to each other. For example, if we are trying to correct errors made during a quantum computation, we would like to quantify how close the post-recovery state is to the original state. In this problem, we will see why the 1-norm is a good measure of closeness.

Consider two quantum states described by density operators ρ and $\tilde{\rho}$ in a N-dimensional Hilbert space, and consider the complete orthogonal measurement $\{E_a : a = 1, 2, \ldots, N\}$, where the E_a's are one-dimensional projectors satisfying

$$\sum_{a=1}^{N} E_a = I. \tag{94}$$

When the measurement is performed, outcome a occurs with probability $p_a = \mathrm{Tr}\,\rho E_a$ if the state is ρ and with probability $\tilde{p}_a = \mathrm{Tr}\,\tilde{\rho} E_a$ if the state is $\tilde{\rho}$.

The (normalized) L^1 distance between the two probability distributions is defined as

$$d(p, \tilde{p}) \equiv \|p - \tilde{p}\|_1 \equiv \frac{1}{2} \sum_{a=1}^{N} |p_a - \tilde{p}_a|. \tag{95}$$

This distance is zero if the two distributions are identical, and attains its maximum value of one if the two distributions have support on disjoint sets.

a) Show that

$$d(p, \tilde{p}) \leq \frac{1}{2} \sum_{i=1}^{N} |\lambda_i|, \tag{96}$$

where the λ_i's are the eigenvalues of the Hermitian operator $\rho - \tilde{\rho}$. *Hint:* Working in the basis in which $\rho - \tilde{\rho}$ is diagonal, find an expression for $|p_a - \tilde{p}_a|$, and then find an upper bound on $|p_a - \tilde{p}_a|$. Finally, use the completeness property Eq. (94) to bound $d(p, \tilde{p})$.

b) Find a choice for the orthogonal projectors $\{E_a\}$ that saturates the upper bound Eq. (96).

Define a distance $d(\rho, \tilde{\rho})$ between density operators as the maximal L^1 distance between the corresponding probability distributions that can be achieved by any orthogonal measurement. From the results of (a) and (b), we have found that

$$d(\rho, \tilde{\rho}) = \frac{1}{2} \sum_{i=1}^{N} |\lambda_i|. \tag{97}$$

c) The trace norm, or Schatten 1-norm $\|A\|_1$ of an operator A is defined as

$$\|A\|_1 \equiv \mathrm{Tr}\left[(A^\dagger A)^{1/2}\right]. \tag{98}$$

How can the distance $d(\rho, \tilde{\rho})$ be expressed as the 1-norm of an operator?

Now suppose that the states ρ and $\tilde{\rho}$ are pure states $\rho = |\psi\rangle\langle\psi|$ and $\tilde{\rho} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. If we adopt a suitable basis in the space spanned by the two vectors, and appropriate phase conventions, then these vectors can be expressed as

$$|\psi\rangle = \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix} \qquad |\tilde{\psi}\rangle = \begin{pmatrix} \sin\theta/2 \\ \cos\theta/2 \end{pmatrix}. \tag{99}$$

d) Express the distance $d(\rho, \tilde{\rho})$ in terms of the angle θ.

e) Express $\||\psi\rangle - |\tilde{\psi}\rangle\|^2$ (where $\|\cdot\|$ denotes the Hilbert space norm, i.e., the 2-norm $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$) in terms of θ, and by comparing with the results of (d), derive the bound

$$d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|) \leq \||\psi\rangle - |\tilde{\psi}\rangle\|. \tag{100}$$

f) Why is $\||\psi\rangle - |\tilde{\psi}\rangle\|$ *not* a good measure of the distinguishability of the pure quantum states ρ and $\tilde{\rho}$? *Hint:* Remember that quantum states are *rays*.

Exercise 3. Positivity of relative entropy
Adapted with permission from Exercise 10.1 of J. Preskill, Lecture Notes for Ph219/CS219: Quantum Information and Computation*, Chapter 10 (2018 edition).*

a) Show that $\log x \leq x - 1$ for all positive real numbers, with equality if and only if $x = 1$.

b) The classical relative entropy of a probability distribution $\{p(x)\}$ relative to $\{q(x)\}$ is defined as

$$H(p \,\|\, q) = \sum_x p(x)\left(\log p(x) - \log q(x)\right), \tag{101}$$

for distributions such that $p(x) = 0$ if $q(x) = 0$, and where the sum is over x such that $q(x) \neq 0$. Show that

$$H(p \,\|\, q) \geq 0, \tag{102}$$

with equality if and only if the distributions are identical. (*Hint:* apply the inequality from (a) to $\log(q(x)/p(x))$.)

c) The quantum relative entropy of the density operator ρ with respect to σ is

$$D(\rho \,\|\, \sigma) = \mathrm{Tr}\left[\rho \log \rho - \rho \log \sigma\right], \tag{103}$$

and it is well-defined provided $\ker\sigma \subseteq \ker\rho$. Let $\{p_i\}$ denote the eigenvalues of ρ and $\{q_a\}$ denote the eigenvalues of σ. Show that

$$D(\rho\,\|\sigma) = \sum_i p_i \left(\log p_i - \sum_a D_{ia} \log q_a\right), \tag{104}$$

where D_{ia} is a doubly stochastic matrix. Express D_{ia} in terms of the eigenstates of ρ and σ. (A matrix is doubly stochastic if its entries are nonnegative real numbers, where each row and each column sums to one.)

d) Show that if D_{ia} is doubly stochastic, then (for each i)

$$\log\left(\sum_a D_{ia} q_a\right) \geq \sum_a D_{ia} \log q_a, \tag{105}$$

with equality only if $D_{ia} = 1$ for some a.

e) Show that

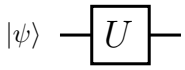
$$D(\rho\,\|\,\sigma) \geq H(p\,\|r), \tag{106}$$

where $r_i = \sum_a D_{ia} q_a$.

f) Show that $D(\rho\,\|\,\sigma) \geq 0$, with equality if and only if $\rho = \sigma$.

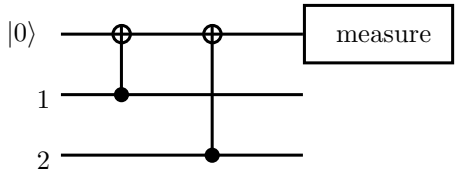
Exercise 4. Cyclicity of the partial trace
Let $V \in \mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$, $W \in \mathcal{L}(\mathcal{H}_B, \mathcal{H}_A)$, and $\tau \in \mathcal{L}(\mathcal{H}_B)$. Show that $\mathrm{Tr}_A[W\tau V] = \mathrm{Tr}_B[VW\tau]$.

Exercise 5. Syndrome measurement in the 9-qubit code
Circuits are a useful way of depicting a sequence of unitary operations. For example, the following circuit depicts $U|\psi\rangle$.

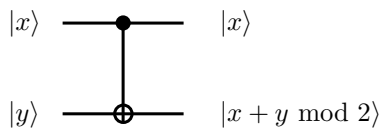


A horizontal line denotes a degree of freedom (such as a qubit), and boxes represent unitary operators. Circuits are read left to right. A box with the word "measure" denotes a measurement in the computational basis.

a) Show that the following circuit measures $Z_1 Z_2$.



The two-qubit operator



denotes the controlled-not, or CNOT operator. Its action on two qubits is $\text{CNOT}|x\rangle|y\rangle = |x\rangle|x + y \bmod 2\rangle$.

b) Find a circuit that collectively and non-destructively measures $X_1X_2X_3X_4X_5X_6$. You may find that the single-qubit operator H known as the *Hadamard operator* is a helpful ingredient. Its action is

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle.$$

Exercise 6. Additivity of relative entropy
Show that $D(\rho_A \otimes \chi_B \,\|\, \sigma_A \otimes \tau_B) = D(\rho_A \,\|\, \sigma_A) + D(\chi_B \,\|\, \tau_B)$. You can assume that σ_A and τ_B are full-rank (no zero eigenvalues) to avoid divergences in relative entropy.

Note: If we think of D as a measure of distinguishability, then the result above is clear. The uncorrelated states in B cannot influence the distinguishability of the states of A and vice-versa. This can also be viewed as a special case of monotonicity of relative entropy, $D(\rho_{AB} \,\|\, \sigma_{AB}) \geq D(\rho_A \,\|\, \sigma_A)$.

References

[1] J. Preskill, "Quantum computation." http://theory.caltech.edu/~preskill/ph219/index.html.

[2] M. M. Wilde, "From Classical to Quantum Shannon Theory," arXiv:1106.1445.

[3] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics Physique Fizika* **1** (1964) 195–200.

[4] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*. Cambridge University Press, 3 ed., 2018.

[5] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Sci. Statist. Comput.* **26** (1997) 1484, arXiv:quant-ph/9508027.

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.* **70** (1993) 1895–1899.

[7] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal* **27** no. 3, (1948) 379–423.

[8] J. Preskill, "Quantum Shannon Theory," arXiv:1604.07450.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[10] S. D. Mathur, "The Information paradox: A Pedagogical introduction," *Class. Quant. Grav.* **26** (2009) 224001, arXiv:0909.1038.

[11] J. Polchinski, "The black hole information problem," in *Proceedings, Theoretical Advanced Study Institute in Elementary Particle Physics: New Frontiers in Fields and Strings (TASI 2015): Boulder, CO, USA, June 1-26, 2015*, pp. 353–397. 2017. arXiv:1609.04036.

[12] D. Harlow, "Jerusalem lectures on black holes and quantum information," *Rev. Mod. Phys.* **88** (2016) 015002, arXiv:1409.1231.

[13] J. M. Bardeen, B. Carter, and S. W. Hawking, "The four laws of black hole mechanics," *Comm. Math. Phys.* **31** no. 2, (1973) 161–170.

[14] S. W. Hawking, "Particle creation by black holes," *Commun. Math. Phys.* **43** (1975) 199–220.

[15] J. D. Bekenstein, "A Universal Upper Bound on the Entropy to Energy Ratio for Bounded Systems," *Phys. Rev. D* **23** (1981) 287.

[16] L. Susskind, L. Thorlacius, and J. Uglum, "The Stretched horizon and black hole complementarity," *Phys. Rev. D* **48** (1993) 3743–3761, arXiv:hep-th/9306069.

[17] A. Almheiri, D. Marolf, J. Polchinski, and J. Sully, "Black holes: complementarity or firewalls?," *JHEP* **02** (2013) 062, arXiv:1207.3123.

[18] A. Almheiri, D. Marolf, J. Polchinski, D. Stanford, and J. Sully, "An apologia for firewalls," *JHEP* **09** (2013) 018, arXiv:1304.6483.

[19] W. G. Unruh and R. M. Wald, "Information loss," *Rept. Prog. Phys.* **80** (2017) 092002, arXiv:1703.02140.

[20] S. B. Giddings, "Nonviolent nonlocality," *Phys. Rev. D* **88** (2013) 064023, arXiv:1211.7070.

[21] S. Raju, "Lessons from the Information Paradox," arXiv:2012.05770 [hep-th].

[22] P. Chen, Y. C. Ong, and D.-h. Yeom, "Black hole remnants and the information loss paradox," *Phys. Rept.* **603** (2015) 1, arXiv:1412.8366.

[23] A. Almheiri, T. Hartman, J. Maldacena, E. Shaghoulian, and A. Tajdini, "The entropy of Hawking radiation," arXiv:2006.06872.

[24] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics* **76** no. 7, (2013) 076001.

[25] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," arXiv:0904.2557.

[26] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A* **52** (1995) R2493–R2496.

[27] M. Ohya and D. Petz, *Quantum Entropy and Its Use*. Texts and monographs in physics. Springer-Verlag, 1993.

[28] G. Penington, S. H. Shenker, D. Stanford, and Z. Yang, "Replica wormholes and the black hole interior," arXiv:1911.11977.

[29] M. Junge, R. Renner, D. Sutter, M. M. Wilde, and A. Winter, "Universal Recovery Maps and Approximate Sufficiency of Quantum Relative Entropy," *Annales Henri Poincare* **19** no. 10, (2018) 2955–2978, arXiv:1509.07127.

[30] J. M. Maldacena, "The large N limit of superconformal field theories and supergravity," *Int. J. Theor. Phys.* **38** (1999) 1113–1133, arXiv:hep-th/9711200. [*Adv. Theor. Math. Phys.* **2** (1998) 231].

[31] E. Witten, "Anti-de Sitter space and holography," *Adv. Theor. Math. Phys.* **2** (1998) 253–291, arXiv:hep-th/9802150.

[32] H. Nastase, "Introduction to AdS-CFT," arXiv:0712.0689.

[33] V. E. Hubeny, M. Rangamani, and T. Takayanagi, "A covariant holographic entanglement entropy proposal," *JHEP* **07** (2007) 062, arXiv:0705.0016.

[34] S. Ryu and T. Takayanagi, "Aspects of holographic entanglement entropy," *JHEP* **08** (2006) 045, arXiv:hep-th/0605073.

[35] A. Hamilton, D. N. Kabat, G. Lifschytz, and D. A. Lowe, "Holographic representation of local bulk operators," *Phys. Rev. D* **74** (2006) 066009, arXiv:hep-th/0606141.

[36] J. Cotler, P. Hayden, G. Penington, G. Salton, B. Swingle, and M. Walter, "Entanglement Wedge Reconstruction via Universal Recovery Channels," *Phys. Rev. X* **9** no. 3, (2019) 031011, arXiv:1704.05839.

[37] D. L. Jafferis, A. Lewkowycz, J. Maldacena, and S. J. Suh, "Relative entropy equals bulk relative entropy," *JHEP* **06** (2016) 004, arXiv:1512.06431.

[38] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory* **45** no. 4, (1999) 1216–1227.