Quantum tasks in holography

by

Alex May

BSc, McGill University, 2014

MSc, The University of British Columbia, 2017

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL
STUDIES

(Physics)

The University of British Columbia

(Vancouver)

July 2021

The following individuals certify that they have read, and recommend to the Faculty of Graduate and Postdoctoral Studies for acceptance, the dissertation entitled:

Quantum tasks in holography

Submitted by Alex May, in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Physics.

Examining committee:

Mark Van Raamsdonk, Professor, Physics, UBC
Supervisor

Joanna Karczmarek, Professor, Physics, UBC
Supervisory Committee Member

Gordon Semenoff, Professor, Physics, UBC
University examiner

Sven Bachmann, Professor, Mathematics, UBC
University examiner

Tadashi Takayanagi, Professor, Physics, Kyoto University
External examiner

Additional committee members:

Robert Raussendorf, Professor, UBC
Supervisory committee member

Gary Hinshaw, Professor, UBC
Supervisory committee member

Abstract

The AdS/CFT correspondence relates quantum gravity in asymptotically AdS spacetimes to conformal field theories living on the boundary of that spacetime. Here, we initiate a new perspective on the AdS/CFT correspondence. In particular we study relativistic quantum tasks, which are quantum computations with inputs and outputs occurring at specified spacetime locations. We note that the AdS/CFT correspondence implies the same tasks are possible in quantum gravity in AdS spacetimes as are possible in the dual CFT. Using this, we find a relationship between the existence of overlaps in certain light cones in the bulk spacetime and entanglement in the boundary CFT. This complements the usual perspective on geometry and entanglement in AdS/CFT, which relates minimal surfaces in AdS to entanglement in the CFT. Further, we point out various instances where this bulk/boundary tasks relationship implies novel statements about tasks.

Lay Summary

Is there a single theory that describes space, time and all forms of matter, and if so, what is it? How did the universe begin, and what happens inside of black holes? These are the ambitious questions behind the field of quantum gravity. Operating in an apparently distinct realm is quantum information, a subject driven by practical questions: what are the limits of computing? How can we communicate efficiently and securely? Despite the distinction in motivation, techniques from quantum information have driven significant progress in quantum gravity.

This thesis gives a novel framework for the application of quantum information to quantum gravity. This framework captures aspects of quantum information that are only apparent in the context of spacetime, where information cannot travel faster than the speed of light. Using these aspects of quantum information reveals new aspects of quantum gravity.

Preface

The work presented in this thesis has been carried out in collaboration with many collaborators, and by making use of valuable discussions with many research community members. This work appears in the publications [43, 63, 67, 68, 70]. I outline the contributions of myself and various coauthors to these works below. Also during the course of my PhD I completed the publications [26, 65], which are not described in this thesis.

The earliest paper which is included here is [43]. This paper has an unusual history, in that it was begun in collaboration with Patrick Hayden while I was a third year undergraduate at McGill, around 2013. The initial idea for the project was Patricks, and had grown out of our earlier paper [42]. I completed the proof of the main theorem early on, but the paper did not appear until 2018. The efficient procedure which is given in the current form of the paper and which appears here emerged from a conversation with Sephr Nezami and Patrick Hayden. The use of the one-time pad (rather than a less efficient use of teleportation) was suggested to me by Daniel Gottesman. Patrick observed that our result could be used to construct arbitrary secret sharing schemes early on, and later that the efficiency of our construction improved on earlier ones.

Chronologically the second paper which is included here is [63]. This paper intitiated the topic of quantum tasks in holography. The early ideas for this paper and the calculations in it were my own, including the conjecture of the connected wedge theorem, but benefited from conversations with Mark Van Raamsdonk, Dominik Neuenfeld, Eliot Hijano, Felix Hael and David Wakeham. The first version of this paper contained some errors, which were found out in real time during a seminar at Stanford. Following that seminar and further conversations with Patrick

Hayden, Jon Sorce, Geoff Penington and others various improvements were made. Mark Wilde also found an error in a related paper which lead to further improvements. Immediately following the same seminar a conversation with Jon Sorce, Geoff Penington, and Aaron Wall lead to the initial focusing construction which we later used to prove the connected wedge theorem. This proof was published in [70], which is coauthored by Geoff Penington and Jon Sorce. That paper also contains a number of other results. We observed there that AdS/CFT implies some improvements in the efficiency of non-local quantum computation; this observation was initially due to Patrick Hayden. Another result there was that the 'scattering region' sits inside of the relevant entanglement wedge. This was observed by Geoff Penington and the proof was detailed by myself and Jon Sorce.

The next included paper is [68]. This was carried out independently, but benefited from feedback from Jon Sorce, Kfir Dolev, and Jason Pollack. The key contribution in this work is to synthesize ideas from [43] and [63] to broaden the set of quantum tasks that can be considered holographically. This work improved on the framework developed in [63] and on the connected wedge theorem. For this reason it is the presentation developed in that reference which I have followed most closely here.

The final paper included here is [67]. This paper was done in collaboration with David Wakeham. We also benefited from early conversations with Jamie Sully which lead to a conjectured connected wedge theorem in the context of end-of-the-world branes. I then constructed the quantum tasks argument and relativistic proof of the theorem. David Wakeham carried out the CFT calculations verifying the theorem in simple cases, and contributed to the discussion of the relevance of this theorem to the islands phenomena. In the context of islands, this work also benefited from from discussions with Henry Lin, Juan Maldacena, and Mark Van Raamsdonk.

Table of Contents

List of Figures

Acknowledgments

Nonscientists probably think that scientists in their research are always using their higher mental faculties, always dealing with deep questions... If only it were so! A lot of what a researcher does is not unlike winding motors, or hoeing corn, or feeding pigs... there is some drudgery in every line of work.

John Wheeler

While the above epigraph holds true, in that my PhD has not been without its share of drudgery, I feel fortunate to have had an unusually drudgery-light PhD. No doubt this is due to the many excellent people I've had the opportunity to speak and work with. Their perspective has kept my higher faculties engaged, whether by providing new insights into deep ideas, or informing me of basic strategies to move past drudgeries efficiently.

Among the many such people are my fellow UBC graduate students David Wakeham, Chris Waddell, Petar Smizidja, and Dominik Neuenfeld. I especially thank David Wakeham, with whom a collaboration lead to insights on relating the connected wedge theorem to the appearance of islands. Another constant resource has been the many post-docs at UBC, including Jason Pollack, Eliot Hijano, Felix Hael, Jamie Sully, Tarok Anous, and Eric Mintun. I wish especially to thank Eliot with whom I collaborated on [65] (not included in this thesis), and from whom I learned many new techniques, as well as Jason Pollack, who unselfishly spent his time proof reading many of my drafts.

I have also had the opportunity to interact with a number of graduate students and post-docs at Stanford, including Jon Sorce, Geoff Pennington, Kfir Dolev,

Kianna Wan, Sam Cree, Grant Salton, and Sephr Nezami, among others. I had the good fortune to collaborate with Jon Sorce and Geoff Penington, with whom the novel but troublesome ideas appearing in [63] were transformed into rigorous and far better understood form. Collaborating on this project while on an extended visit to Stanford is among the highlights of my PhD. I also had the opportunity to collaborate with Kfir Dolev and Kianna Wan on [26] (also not included), who together pushed non-local task techniques to new levels of complexity I surely would not have reached on my own.

Finally I wish to thank the faculty members who have guided me throughout my academic career. My supervisor Mark Van Raamsdonk has provided a steady stream of insight and critique which have influenced my thinking throughout this thesis. Mark has also allowed a large degree of independence, which (I hope) has served me well, while simultaneously encouraging me to work harder and push for broader, sharper results. He has also gone beyond the norm to give me the best possible career opportunities, including by giving carefully considered suggestions on improving talks, which have been especially valuable. Finally, it is my pleasure to thank Patrick Hayden. In many ways my PhD research has been the natural outgrowth of a summer project undertaken as an undergraduate with Patrick, where I began thinking about processing quantum information in a spacetime context. In the near decade since then, Patrick's influence has become irreversibly intertwined with the "quantum tasks" research program. He has also, always unselfishly, given me sage advice in career matters, and has set for me a standard in physics and in character to aspire to.

Chapter 1

Introduction

1.1 Quantum tasks in holography

Quantum information theory is the study of how the rules of quantum mechanics dictate how information can and cannot be processed. Importantly, quantum information theory is largely uninterested in specific physical systems: it does not assume a particular Hamiltonian or action, or a specific set of symmetries. This gives quantum information theory wide applicability to all quantum mechanical systems, from particles in ion traps to conformal field theories.

Beyond quantum mechanics, additional restrictions on information processing come from relativity. In particular, in a relativistic context there is a spacetime manifold, and each quantum system we consider has some trajectory in this manifold. From an information processing perspective this amounts to a set of allowed communications: information can travel from a point p to point q when q is in the causal future of p and not otherwise.

In this thesis, we study quantum information theory in a spacetime context, and apply this to a particular system, AdS/CFT. Our broadest goal is to better understand how quantum information can and cannot be processed in the presence of the communication restrictions enforced by relativity. In keeping with the quantum information theorists creed, we abstract away from particular Hamiltonian's or actions[1].

[1]This distinguishes the approach taken in this thesis from what is usually given the name 'rel-

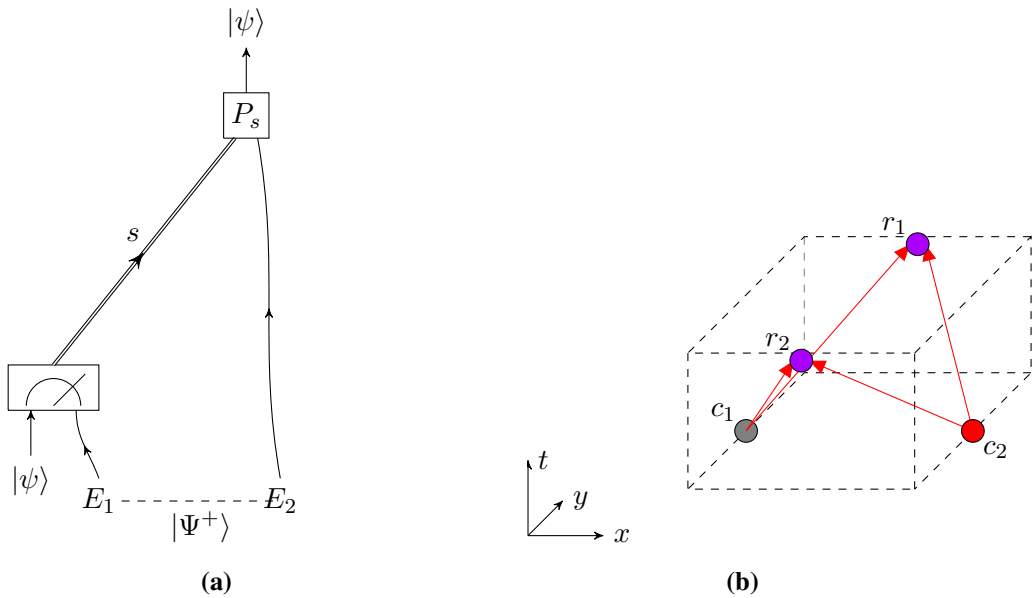


Figure 1.1: (a) The quantum teleportation protocol. Before the beginning of the protocol, there is a quantum state $|\psi\rangle$ held on the left and an entangled state $|\Psi^+\rangle$ shared between left and right. At the end of the protocol, the state $|\psi\rangle$ is held on the right. (b) A quantum information processing task which happens in a spacetime background, taken to be $2+1$ dimensional Minkowski space for concreteness. Alice is given a quantum state $|\psi\rangle$ at c_1, and a bit q at c_2. Her goal is to bring $|\psi\rangle$ to r_q. This can be achieved by sharing a maximally entangled state between c_1 and c_2 and using the quantum teleportation protocol.

Some features of quantum information are unique to a spacetime setting. To develop an example, begin with a classic topic in quantum information theory, the quantum teleportation protocol. In teleportation, a quantum system[2] A_1 in a

ativistic quantum information', where the dynamics of objects studied by information theorists are studied in a particular chosen field theory.

[2]Each quantum system we refer to, denoted with capital letters X, Y, A_1, etc. refers to a different physical system which can be separately manipulated and moved through spacetime. For example X may describe a spin 1/2 particle. Mathematically, quantum systems are described as vectors in a Hilbert space, so that system X is described by a Hilbert space $\mathcal{H}_X$. When describing multiple quantum systems, say X and Y, we use the Hilbert space composed from the tensor product of each systems separate Hilbert space, $\mathcal{H}_{XY} \equiv \mathcal{H}_X \otimes \mathcal{H}_Y$. The $|\cdot\rangle$ notation denotes vectors in a Hilbert space, and we add a subscript like $|\cdot\rangle_X$ to denote vectors in the Hilbert space $\mathcal{H}_X$

state $|\psi\rangle_{A_1}$ is sent from one location to another using a combination of classical communication and an entangled state between the two locations. This is illustrated in figure 1.1a. To perform the teleportation, an entangled state $|\Psi^+\rangle_{E_1E_2}$ is shared between two locations. Then, the A_1E_1 system is measured, producing a classical measurement outcome. After this, the system E_2 is in the state $P_s|\psi\rangle$, where P_s is one of the four Pauli operators $\{\mathcal{I}, X, Z, Y\}$. On the receiving end, the classical data s can be used to undo P_s and produce the original state $|\psi\rangle$, now residing on the E_2 system.

Quantum teleportation has an important consequence in the context of spacetime. To see this, consider the set-up shown in figure 1.1b, which shows an example of a quantum task. In a quantum task, one party, call them Alice, receives various quantum and classical systems at a set of input locations, and must process them in some way before returning them to another set of output locations. In the particular example shown Alice receives a quantum system A_1 in the state $|\psi\rangle_{A_1}$ at c_1, and a classical bit $q \in \{0, 1\}$ at c_2. Alice's goal is to return $|\psi\rangle$ to r_q. We will refer to this as the *routing task*.

Naively, it is difficult for Alice to complete this task. Consider in particular her dilemma at c_1: she holds $|\psi\rangle$ there, but q is far away. Since $|\psi\rangle$ is quantum, she can't copy and send it to both r_1 and r_2. Further, she can't wait to find out q and then send it to the appropriate location. This is because we've chosen the points c_1, c_2, r_1, r_2 in such a way that there is no spacetime location which is in the future of c_1 and c_2 (so that $|\psi\rangle$ and q can be there) and in the past of r_1 and r_2 (so that Alice can send $|\psi\rangle$ to the correct location once she knows it). Apparently, Alice's best strategy is to guess q, in which case she succeeds with probability $1/2$.[3]

Using a maximally entangled state $|\Psi^+\rangle_{E_1E_2}$ however, Alice can complete this task with probability 1 [42, 55]. To do this, Alice measures A_1E_1, using the same measurement as in the first step of the teleportation protocol. Doing so she obtains the measurement outcome s. This partly solves her problem: since s is classical, she can copy it and send it to r_1 and r_2. Additionally, the state on E_2 is now $P_s|\psi\rangle$ for some Pauli P_s, and which Pauli is fixed by s. Since E_2 is located near c_2, Alice can send the quantum part, $P_s|\psi\rangle$, to r_q. Thus both s and $P_s|\psi\rangle$ arrive at r_q. Alice

[3] In general she can succeed with somewhat higher probability by using an approximate cloning procedure [38]. She succeeds with probability half in the case where A_1 is $d \to \infty$ dimensional.

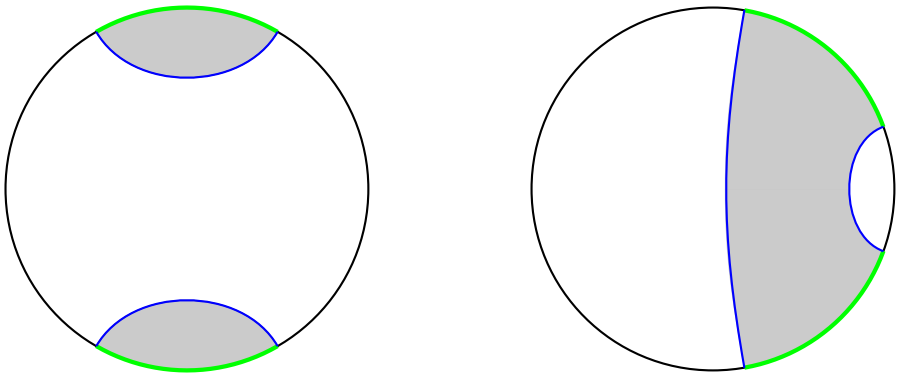


Figure 1.2: Minimal surfaces (shown in blue) enclosing the union of two intervals R_1 and R_2 (shown in green). The entanglement wedge $\mathcal{E}_W(R_1 \cup R_2)$ (shown in grey) is the region whose boundary is the union of the regions R_1 and R_2 and their minimal surfaces. For large separations or small intervals the entanglement wedge of the region $R_1 \cup R_2$ is disconnected, while for small separation or large enough regions, the entanglement wedge becomes connected, as shown at right. The entanglement wedge being connected indicates the mutual information is large, while a disconnected entanglement wedge indicates the mutual information is small.

can then undo P_s and hand in $|\psi\rangle$ at r_q, completing her task.

This protocol for completing the task shown in figure 1.1b highlights an interesting feature of quantum information, and in particular of the quantum teleportation protocol.[4] In particular, the task reveals that quantum information can be sent to an unknown spacetime location by exploiting entanglement.

One of the exciting areas quantum information theory is now applied to is the AdS/CFT correspondence [60]. There, ideas from quantum information have played an important role. A key result in relating quantum information and AdS/CFT is the Ryu-Takayanagi formula, which gives the entropy of a subregion of the CFT in terms of the minimal area of a bulk surface anchored to that portion of

[4] As a historical note, a similar observation is made in the original paper on teleportation [16].

the boundary,

$$S(A) = \min_{\gamma_A} \frac{\text{Area}[\gamma_A]}{4G_N} + O(G_N^0). \tag{1.1}$$

An example is shown in figure 1.2. The $O(G_N^0)$ term is in general much smaller than the $O(1/G_N)$ term, since we work in the $G_N \to 0$ limit. Closely related to the Ryu-Takayanagi formula is entanglement wedge reconstruction. In particular the region enclosed by $\gamma_A^{\min} \cup A$ is called the entanglement wedge, $\mathcal{E}_W(A)$. The entanglement wedge of A is the portion of the bulk which is fully fixed by the boundary subregion A. Since a particular point in the bulk will be in the entanglement wedge of many different boundary subregions, this gives AdS/CFT the structure of an error-correcting code [4, 40].

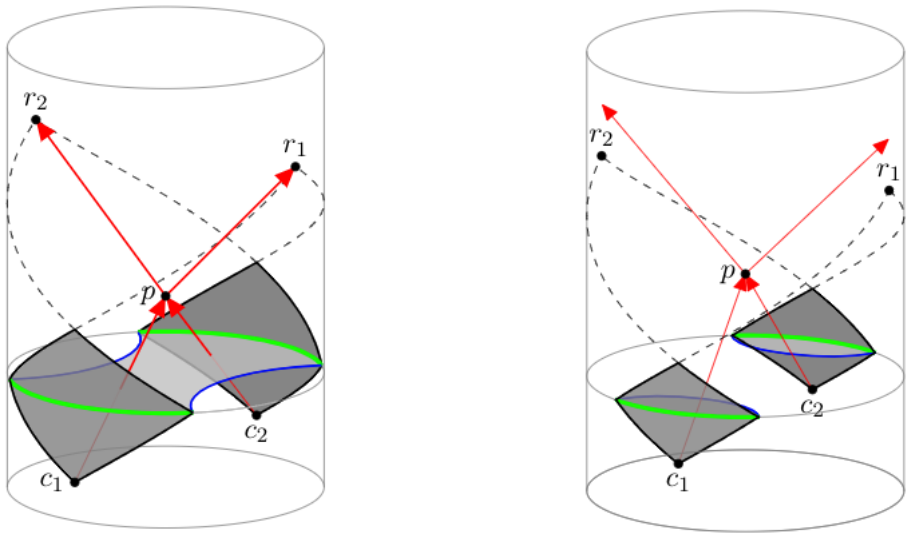
Of particular relevance in this thesis will be the case where A is chosen to be two intervals, $\mathcal{R}_1 \cup \mathcal{R}_2$. Then, the minimal surface enclosing $\mathcal{R}_1 \cup \mathcal{R}_2$ can take on two configurations, shown as figure 1.2a and 1.2b. In the first configuration the entanglement wedge is a connected region, while in the second it is disconnected. A convenient diagnostic for this transition is the mutual information,

$$I(\mathcal{R}_1 : \mathcal{R}_2) = S(\mathcal{R}_1) + S(\mathcal{R}_2) - S(\mathcal{R}_1 \cup \mathcal{R}_2). \tag{1.2}$$

When the entanglement wedge is disconnected, the minimal surface enclosing $\mathcal{R}_1 \cup \mathcal{R}_2$ is just the minimal surface for $\mathcal{R}_1$ alone union the minimal surface of $\mathcal{R}_2$ alone. This gives a $O(G_N^0)$ mutual information. On the other hand, when the entanglement wedge is connected the mutual information has a $O(1/G_N)$ term.

In AdS/CFT relativity plays an obvious and important role; the correspondence is a description of how quantum field theory along with gravity in $d+1$ dimensions can be described as a conformal field theory in d dimensions. A central claim of this thesis is that it is important to apply an understanding of quantum information theory in a spacetime context to AdS/CFT. In particular, we obtain some simple but previously unnoticed features of AdS/CFT by doing so.

As an example of how spacetime-unique features of quantum information play a role in AdS/CFT, see figure 1.3. There, we've embedded the routing task into an asymptotically AdS spacetime. The input and output locations are points at the



(a) **(b)**

Figure 1.3: (a) When a set of four boundary points $\{c_1, c_2, r_1, r_2\}$ has a bulk scattering region, associated boundary regions (black diamonds) must share large correlation. (b) When there is no scattering region in the bulk, the boundary regions need not share large correlation. This figure is reproduced from [63].

boundary of AdS. In the AdS/CFT correspondence, we can look at this task from two perspectives. First, consider a bulk perspective. There, given the way in which we've chosen the four points c_1, c_2, r_1, r_2, we can use a naive strategy to complete the task in the bulk: bring $|\psi\rangle$ from c_1 and q from c_2 together at p, then route $|\psi\rangle$ towards r_q. In the boundary however there is no such point p that sits in the future of c_1 and c_2, and the past of r_1 and r_2. Consequently an entanglement based strategy is necessary to complete the task. Since the boundary CFT describes the bulk, we can conclude that whenever p exists in the bulk, the boundary will have the necessary entanglement to complete the task. This leads to two associated boundary regions necessarily having large mutual information, and consequently a connected entanglement wedge.

A refinement of this reasoning leads to the *connected wedge theorem*, a central result to be discussed in this thesis.

Theorem 1 *($2 \to 2$ **Connected wedge theorem**) Pick four regions $\hat{\mathcal{C}}_1, \hat{\mathcal{C}}_2, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ on the boundary of an asymptotically AdS spacetime. From these, define the input regions*

$$\begin{aligned} \hat{\mathcal{V}}_1 &\equiv \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2), \\ \hat{\mathcal{V}}_2 &\equiv \hat{J}^+(\hat{\mathcal{C}}_2) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2). \end{aligned} \tag{1.3}$$

Assume that $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$. Define the entanglement scattering region

$$J^{\mathcal{E}}_{12\to 12} \equiv J^+(\mathcal{C}_1) \cap J^+(\mathcal{C}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2), \tag{1.4}$$

where $\mathcal{C}_i = \mathcal{E}_W(\hat{\mathcal{C}}_i)$ and $\mathcal{R}_i = \mathcal{E}_W(\hat{\mathcal{R}}_i)$. Then, $J^{\mathcal{E}}_{12\to 12} \neq \varnothing$ implies that $I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) = O(1/G_N)$, or equivalently that $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$ is connected.

It is interesting that the connected wedge theorem provides a relationship between causal features of the bulk geometry and boundary entanglement. This is qualitatively distinct from the Ryu-Takayanagi formula, which relates spacelike surfaces in the bulk to boundary entanglement.

More broadly, in this thesis we develop and argue for the utility of a general framework relating relativistic quantum tasks in the bulk and boundary perspectives. The $2 \to 2$ connected wedge theorem is one output from this framework. A related application of the same framework also leads to a variant of the connected wedge theorem that applies in AdS spacetimes featuring an end-of-the-world brane. Beyond these examples, there may be many more connections between the bulk and boundary descriptions in AdS/CFT to be found by reasoning about quantum tasks. This adds further motivation to our initial goal, stressed above, of better understanding quantum information theory in a relativistic context.

1.2 Outline of this thesis

We begin in chapter 2 with an introduction to quantum information theory, covering core topics including quantum channels, distinguishability of states and channels, entropy, and quantum error-correction. An unusual inclusion is port-teleportation, which plays an important role in section 4.4 and chapter 12.

Chapter 3 presents a handful of topics in quantum cryptography: secret sharing, the one-time pad, and monogamy games. Each of these serve as tools later in the thesis. In particular secret sharing and the one-time pad are used in chapter 5 to construct localize-exclude protocols, and the one-time pad appears again in section 9.3 when we discuss a loophole in the quantum tasks argument for the connected wedge theorem. Results on monogamy games are essential to the necessity of entanglement proof given in section 4.5 and the information theoretic argument for the connected wedge theorem.

Chapter 4 presents an overview of relativistic quantum tasks, the first example of which we saw in figure 1.1b. A core idea will be making precise when a quantum system is or is not inside of a given spacetime region. We then discuss a particular class of quantum tasks relevant to another topic in quantum cryptography, position-based cryptography, and the non-local computation based cheating strategies. This detour culminates in section 4.5, where we give lower bounds on the mutual information present in resource states used for non-local computation. These bounds form the technical core of the information theoretic arguments for the connected wedge theorem.

Chapter 5 presents a contribution towards better understanding relativistic quantum tasks. In particular we study a class of tasks which require Alice localize a single quantum system to a collection of spacetime regions, while keeping that system out of (excluding it from) a second collection of regions. We give a complete characterization of when this is possible. Using a combination of teleportation, quantum error-correction, classical secret sharing, and the one-time pad, we also construct explicit protocols for completing the task whenever it is possible.

Chapter 6 presents some background material in general relativity, including a discussion of AdS space and the area theorem. The area theorem is used in chapter 9 to prove the $2 \to 2$ connected wedge theorem geometrically. We also give the area theorem in the presence of an end-of-the-world brane, which is used in chapter 11 to prove the $1 \to 2$ variant of the connected wedge theorem. We have not seen the area theorem discussed in that context previously, though it is a straightforward application of Stokes' theorem.

Chapter 7 gives a brief overview of the AdS/CFT correspondence. To make the correspondence precise, we discuss the identification of the bulk field content from

the boundary operator content, and give a path integral perspective on the mapping between bulk and boundary. Then we discuss the Ryu-Takayanagi formula, which we introduced above as equation 1.1 and which relates bulk areas to boundary entropy. We also discuss the entanglement wedge $\mathcal{E}_W(A)$, which is the bulk region which can be recovered by using the boundary density matrix ρ_A. Finally, we discuss AdS/BCFT, an adaptation of the AdS/CFT correspondence to the case where the CFT lives on a manifold with a boundary. The $2 \to 2$ theorem applies to AdS/CFT, while the $1 \to 2$ theorem applies to AdS/BCFT.

Chapter 8 gives our framework for applying relativistic quantum information theory to AdS/CFT. To do so, we give a prescription for identifying a quantum task in the bulk with a quantum task in the boundary. Then, we argue that the boundary task always has at least as high of a success probability as the bulk one. We give a few basic examples of this and some simple conclusions we can draw from it. These examples already are known in the literature but we point out how they fit into our framework.

Chapter 9 focuses on the $2 \to 2$ connected wedge theorem. We give the quantum tasks argument, outlined in the introduction, and discuss in detail a possible loophole to this argument. Then we give the proof of the connected wedge theorem from general relativity, which uses the discussion of the area theorem from chapter 6.

Chapter 10 focuses on the $1 \to 2$ connected wedge theorem. We give the quantum tasks argument, highlighting the qualitative distinctions from the $2 \to 2$ theorem. Next we give the relativistic proof of this theorem, which is similar to the proof of the $2 \to 2$ theorem but uses the area theorem in the presence of a boundary.

Chapter 11 discusses the formation of islands in the Ryu-Takayanagi formula, which are disconnected regions in the entanglement wedge. Islands form in particular in the evaporation of black holes. Intriguingly, the $1 \to 2$ theorem can be used to give a causal perspective on when an island forms, at least in certain models of black hole evaporation based on AdS/BCFT. We first give the relevant background on islands and black hole evaporation before explaining how the $1 \to 2$ theorem can be applied.

Finally, in chapter 12 we discuss possible insights into quantum information

theory stemming from the AdS/CFT duality. In particular, the connection between AdS/CFT and non-local quantum computation (NLQC) revealed by the connected wedge theorem suggests improvements in existing NLQC protocols should exist. We discuss prospects for better understanding this in the future.

Chapter 2

Quantum information

This chapter is review material, the key sources used are [49, 85, 86, 99].

In this chapter I review some ideas in quantum information theory. While many of these topics are well known to many researcher in AdS/CFT, the presentation here is slightly non-standard in emphasizing operational aspects of these topics. This emphasis is consistent with the operational perspective taken in the quantum tasks framework we develop later on. We also describe port-teleportation, a topic which is largely unknown in the AdS/CFT community.

2.1 Quantum channels and measurements

States in quantum mechanics are described by vectors in a Hilbert space, and the dynamics of those states is described by unitary operators. More generally, we may be interested in the dynamics of a subsystem, say the A subsystem of a Hilbert space $\mathcal{H}_{AA'} = \mathcal{H}_A \otimes \mathcal{H}_{A'}$. In this case the state is described by the density matrix ρ_A.

How do we describe the dynamics of a subsystem in quantum mechanics? Quantum mechanics allows evolution according to a *quantum channel*.

Definition 1 *A map $\mathcal{N}_{A\to B}$ from $\mathcal{H}_A$ to $\mathcal{H}_B$ is said to be a **quantum channel** if it*

can be written in the form

$$\mathcal{N}_{A\to B}(\rho_A) = tr_{AX}(U_{ABX}(\rho_A \otimes |0\rangle\langle 0|_{BX})U_{ABX}^\dagger). \tag{2.1}$$

The state $|0\rangle_{ABX}$ is fixed and independent of ρ_A.

In words, a quantum channel consists of doing a unitary on the system of interest plus some ancilla system, then tracing out all but the output system.

A more compact and often useful representation of quantum channel is given by its Kraus decomposition,

$$\mathcal{N}_{A\to B}(\rho_A) = \sum_k E_k \rho_A E_k^\dagger. \tag{2.2}$$

The operators E_k can be calculated from the unitary U_{ABX} according to $E_k = \langle k|_{AX} U_{ABX} |0\rangle_{BX}$, which we can see from a simple calculation,

$$\begin{aligned}\mathcal{N}_{A\to B}(\rho_A) &= \mathrm{tr}_{AX}(U_{ABX}(\rho_A \otimes |0\rangle\langle 0|_{BX})U_{ABX}^\dagger), \\ &= \sum_k (\langle k|_{AX} U_{ABX} |0\rangle_{BX})\rho_A(\langle 0|_{BX} U_{ABX} |k\rangle_{AX}).\end{aligned} \tag{2.3}$$

From this we immediately learn that $\sum_k E_k^\dagger E_k = \mathcal{I}$. Equation 2.2 along with the condition $\sum_k E_k^\dagger E_k = I$ is in fact another, equivalent, way to define a channel.

Notice that while unitary evolution is always reversible, quantum channels need not be. For instance a channel where the unitary $U_{AX} \otimes \mathcal{I}_B$ swaps ρ_A with the $|0\rangle\langle 0|_X$ ancilla erases all information on A and is irreversible. Understanding how well, if at all, a quantum channel can be reversed will be one theme throughout this introduction.

Quantum channels describe the dynamics of quantum systems when we can add and trace out subsystems. We can describe measurements in the same setting. Considering only an isolated quantum system A in state ρ_A, measurements are described by a set of projectors $\{\Pi_i\}$ satisfying $\sum_i \Pi_i = I$. We obtain outcome $|\psi_i\rangle$ with probability

$$p_i = \mathrm{tr}(\Pi_i \rho_A), \tag{2.4}$$

and after measurement the state is

$$|\psi_i\rangle\langle\psi_i| = \frac{\Pi_i \rho_A \Pi_i}{p_i}. \tag{2.5}$$

If we have access to an additional subsystems, we can do a more general class of measurements.

Definition 2 *A **quantum measurement** is described by a set of operators* $\{M_i\}$ *such that* $\sum_i M_i^\dagger M_i = I$*. The probability of an outcome* i *is given by*

$$p_i = tr[M_i \rho_A M_i^\dagger] \tag{2.6}$$

and the post-measurement state is

$$\rho_A^i = \frac{M_i \rho M_i^\dagger}{p_i} \tag{2.7}$$

To understand how this type of measurement arises by adding subsystems, consider that after adding in an ancilla $|0\rangle\langle 0|_P$ and applying a joint unitary U_{AP} the joint state is

$$U_{AA'}(\rho_A \otimes |0\rangle\langle 0|_P) U_{AA'}^\dagger \tag{2.8}$$

After doing this, we can do a projective measurement on the AP system. Then the post measurement state is

$$\begin{aligned} \rho_A^j &= \Pi_j U_{AP}(\rho_A \otimes |0\rangle\langle 0|_{A'}) U_{AA'}^\dagger \Pi_j \\ &= \Pi_j U_{AA'} |0\rangle_{A'} (\rho_A) \langle 0|_{A'} U_{AA'}^\dagger \Pi_j \\ &= M_j \rho_A M_j^\dagger \end{aligned} \tag{2.9}$$

where we defined $M_j \equiv \Pi_j U_{AA'} |0\rangle_{A'}$. The relation $\sum_j M_j^\dagger M_j = I$ is then satisfied because $\sum_j \Pi_j = I$ and $U_{AA'}$ is unitary.

In some settings it is not important what the post-measurement state is. In this case we need only keep track of $M_i^\dagger M_i$, since this is the object needed to calculate the probabilities p_i of each outcome. This leads to our next definition.

Definition 3 *A **POVM** (or 'positive operator valued measure') is defined by a set of positive operators $\Lambda_i \geq 0$ such that $\sum_i \Lambda_i = I$. Performing a POVM leads to outcomes i with probabilities $p_i = tr(\Lambda_i \rho_i)$.*

To illustrate POVMs we give a useful example below.

Example 1 *The **pretty-good measurement** is a POVM which is useful in distinguishing among a set of non-orthogonal states, call them $\{\sigma^i\}$. We would like to ensure that the guessing probability*

$$p_{guess} = \sum_i tr\left(\Pi_i \sigma_i\right) \tag{2.10}$$

is high, and need to choose Π_i appropriately. A simple way we might do this is to take the Π_i to be the states σ^i themselves — this seems like a sensible step towards maximizing the overlap between Π^i and σ^i. The σ^i are indeed positive operators, but they are not normalized. To define normalized POVM elements we define

$$\Lambda_i = \sigma^{-1/2} \sigma^i \sigma^{-1/2} \tag{2.11}$$

with

$$\sigma \equiv \sum_i \sigma^i \tag{2.12}$$

and the inverse defined as inverting the support of σ and leaving the zero components unchanged.

We can wonder how good the pretty-good measurement actually does at maximizing the guessing probability. One can show that

$$p_{guess}(optimal) \leq \sqrt{p_{guess}(PGM)} \tag{2.13}$$

that is, we only lose out by a square root. For this reason the pretty-good measurement is also sometime called a square-root measurement.

Finally, we note that quantum measurements can themselves be described as

quantum channels. Given a measurement $\{M_j\}$, define Kraus operators

$$E_j = M_j \otimes |j\rangle_P. \tag{2.14}$$

The condition $\sum_j M_j^\dagger M_j = I$ then gives that $E_j^\dagger E_j = I$ as needed. Then the associated channel is

$$\mathcal{M}(\rho) = \sum_j M_j \rho M_j^\dagger \otimes |j\rangle\langle j|_P \tag{2.15}$$

It is also helpful to write this in terms of the post-measurement states 2.7,

$$\mathcal{M}(\rho) = \sum_j p_j \rho^j \otimes |j\rangle\langle j|_P. \tag{2.16}$$

Thus we can understand the channel as preparing a statistical mixture of the post measurement states along with the measurement outcome recorded into P, weighted by each outcomes probability. Finally, we can note that because a measurement can be described as a channel, it can understood as unitary evolution with a larger system followed by the trace.

In this section we have understood the most general form the dynamics of a quantum subsystem can take, which is a quantum channel. Building on this, we will be interested throughout this thesis in how quantum systems can (and cannot) be evolved in a spacetime setting.

2.2 Distinguishability of quantum states

Here we will develop a number of tools that quantify how similar or different two quantum states are. These quantities will be used in a number of places in this thesis, including our lower bound on the entanglement required in non-local quantum computation, as we discuss in section 4.5.

Our first measure of how similar two quantum states are will be a guessing probability. In particular, suppose that you are given either the state ρ_0 or the state ρ_1, each with probability $1/2$. Then, we will allow you to make any measurement in an attempt to learn if the state is ρ_0 or if it is ρ_1. The most general possible

measurement is described by a POVM with two elements $\{\Lambda_0, \Lambda_1\}$, so that

$$p^{\max}_{\text{guess}}(\rho_0, \rho_1) = \frac{1}{2} \max_{\Lambda_0, \Lambda_1} \left(\text{tr}(\rho_0 \Lambda_0) + \text{tr}(\Lambda_1 \rho_1)\right). \tag{2.17}$$

Recall that all POVMS have $\sum_i \Lambda_i = I$, which here is just $\Lambda_0 + \Lambda_1 = I$, so that we can rewrite the above

$$p^{\max}_{\text{guess}}(\rho_0, \rho_1) = \frac{1}{2} + \frac{1}{2} \max_{\Lambda_0} \text{tr}(\Lambda_0(\rho_0 - \rho_1)). \tag{2.18}$$

While the guessing probability is nicely physical quantity, our expression for it right now involves an optimization. It would be mathematically more convenient to find a closed form, which in particular means finding the optimal Λ_0. Doing so will lead us to the following definition

Definition 4 *The **trace distance** $||\rho_0 - \rho_1||_1$ is defined by*

$$||\rho_0 - \rho_1||_1 = tr\sqrt{(\rho_0 - \rho_1)^\dagger (\rho_0 - \rho_1)}. \tag{2.19}$$

The trace distance is, mathematically, a good notion of 'distance' between quantum states in that it satisfies the usual properties of a distance function: it is 0 when $\rho_0 = \rho_1$ and positive otherwise, symmetric, and satisfies the triangle inequality.

Conveniently the trace distance appears in the closed form for the guessing probability, giving the trace distance an operational interpretation, in addition to its nice mathematical properties. This is the content of the next lemma.

Lemma 1 *The guessing probability for distinguishing correctly between two density matrices ρ_0, ρ_1 is given by*

$$p^{max}_{guess}(\rho_0, \rho_1) = \frac{1}{2} + \frac{1}{4}||\rho_0 - \rho_1||_1 \tag{2.20}$$

A proof is given in [99].

There are many other notions of distance between quantum states, which in certain settings may be more useful than the trace distance. A second natural object to consider is the overlap of two pure states $|\langle\psi|\phi\rangle|$. For $|\psi\rangle = |\phi\rangle$ this overlap is 1, and for similar states we expect it is close to 1.

To turn this idea into a useful quantity we first need to generalize the overlap to mixed states. The generalization of the overlap to mixed states will be called the *fidelity*.

Definition 5 *The **fidelity** is defined by*

$$F(\rho,\sigma) = \max_{|\rho\rangle,|\sigma\rangle} |\langle\rho|\sigma\rangle| \tag{2.21}$$

where the maximization is over all purifications of the mixed states ρ and σ.

It is useful to note that the maximum value is achieved also for a fixed purification of ρ and maximizing only over the purification's of σ, or vis versa.

Similar to the trace distance, the fidelity also has a convenient closed form in terms of the density matrices ρ and σ. This is given in the next lemma.

Lemma 2 *The fidelity is given by*

$$F(\rho,\sigma) = tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}. \tag{2.22}$$

In many cases it is more convenient to work directly with the maximization formula, but it is satisfying that there is also this simple expression for the fidelity.

To establish that the fidelity is a good measure of the similarity of quantum states we can note a relation between the fidelity and trace distance [32].

Lemma 3 *The trace distance and fidelity are related by*

$$1 - \sqrt{F(\rho,\sigma)} \leq \frac{1}{2}||\rho-\sigma||_1 \leq \sqrt{1-F(\rho,\sigma)}. \tag{2.23}$$

From this we have that when the trace distance is near 0 the fidelity is close to 1, and when the fidelity is close to 1 the trace distance is near 0.

Next we give a third object used to measure how distinguishable quantum states are, called the *relative entropy*. The relative entropy, like the trace distance, has an operational interpretation, though now the setting is changed. We suppose that Alice receives either $\rho_n = \rho^{\otimes n}$ or $\sigma_n = \sigma^{\otimes n}$. Alice would like to determine which of the two states she has received, and will use a POVM $\{\Lambda_n^\rho, \Lambda_n^\sigma\}$. There are two types of error that Alice can make,

- **Type I:** Alice identifies the state as σ when it is ρ. This occurs with probability $p(\sigma|\rho) = \text{tr}(\rho_n \Lambda_n^\sigma)$.

- **Type II:** Alice identifies the state as ρ when it is σ. This occurs with probability $p(\rho|\sigma) = \text{tr}(\sigma_n \Lambda_n^\rho)$.

We will suppose that Alice is particularly concerned about type I errors, and so will require that $\text{tr}(\rho_n \Lambda_n^\sigma) \leq \epsilon$, and then will choose her POVM so as to minimize the type II error subject to this constraint. Notice that it is always possible to reduce the type I error below the given value of ϵ, since Alice could for instance simply always declare the state to be ρ.

The quantity we are interested in then is

$$p_{\epsilon,n}(\rho, \sigma) = \min_{\Lambda_n^\rho} \{p(\rho|\sigma) \mid p(\sigma|\rho) \leq \epsilon\}. \tag{2.24}$$

We would like to turn this into a measure of how distinguishable ρ and σ are. To do this we need to remove the n dependence of the above probability. To see how to do this, notice that we expect this error to go to zero exponentially in n. This is because in a simple case where we test each tensor factor individually and correctly identify the state with some probability over $1/2$, our error probability in identifying the state goes to zero like an exponential, $p_{\epsilon,n} \approx e^{-nD(\rho||\sigma)}$. Given this we expect we can remove the n dependence by studying the following quantity.

Definition 6 *The **relative entropy** is defined by*

$$D(\rho||\sigma) \equiv -\lim_{n\to\infty} \frac{1}{n} \log p_{\epsilon,n} \tag{2.25}$$

Notice that it follows immediately from this definition that the relative entropy is non-negative.

A classic result called Steins lemma gives a closed form expression for the minimal error.

Lemma 4 *The relative entropy is given in closed form by*

$$D(\rho||\sigma) = tr(\rho \log \rho - \rho \log \sigma). \tag{2.26}$$

The proof can be found in [46].

We should relate the relative entropy to the fidelity and trace distance, our two earlier measures of distinguishability.

Lemma 5 *The fidelity and relative entropy are related by*

$$D(\rho||\sigma) \geq -\log_2 F(\rho, \sigma). \tag{2.27}$$

Combining this with Lemma 2.23 then completes the set of relationships among the trace distance, fidelity, and relative entropy.

Finally, we note an important property of a measure of distinguishability, which is its monotonicity under the action of a quantum channel. In particular, the following three inequalities hold.

$$\begin{aligned} ||\rho - \sigma||_1 &\geq ||\mathcal{N}(\rho) - \mathcal{N}(\sigma)||_1 , \\ F(\rho, \sigma) &\leq F(\mathcal{N}(\rho), \mathcal{N}(\sigma)), \\ D(\rho||\sigma) &\geq D(\mathcal{N}(\rho)||\mathcal{N}(\sigma)). \end{aligned} \tag{2.28}$$

While each of these can be proven mathematically from the closed forms for these quantities, they also follow immediately from their operational meanings. In particular under the action of a quantum channel states must becomes less distinguishable, since any procedure for distinguishing ρ and σ could begin with applying the channel.

2.3 Distinguishability of quantum channels

In the last section we focused on distinguishing between quantum states. In many settings we will instead be interested in distinguishing between quantum channels. For example, we might want to reproduce the effects of one quantum channel with another. If we can show the ideal and approximated channels are nearly indistinguishable, we've shown we've reproduced the ideal one well.

As with quantum states, there are various different objects which describe the distinguishability of quantum channels. We will be most interested in the *diamond norm distance*, which is closely related to the trace distance introduced in the last

section.

The setting for the diamond norm distance is as follows. Alice is given a usage of either channel $\mathcal{M}$ or channel $\mathcal{N}$, each with probability $1/2$, but is unaware of which channel she is using. She can choose which quantum state to input to the unknown channel, and then will perform any measurement on the channels output in an attempt to determine which channel she used.

Her success probability in guessing the channel is

$$p^{\max}_{\text{guess}}(\mathcal{M},\mathcal{N}) = \max_{|\Psi\rangle_{RA}} p^{\max}_{\text{guess}}(I_R \otimes \mathcal{M}(|\Psi\rangle_{RA}), I \otimes \mathcal{N}(|\Psi\rangle_{RA})) \tag{2.29}$$

Note that we have Alice maximize over her choice of input state. Further, she can in general input the A subsystem of some pure state $|\Psi\rangle_{RA}$, and then measure both the R and A systems in her attempt to identify the channel.

Using the expression for the guessing probability between states in terms of the trace distance, we can rewrite the guessing probability for channels,

$$p^{\max}_{\text{guess}}(\mathcal{M},\mathcal{N}) = \frac{1}{2} + \frac{1}{4} \max_{|\Psi\rangle_{RA}} ||I_R \otimes \mathcal{M}(|\Psi\rangle_{RA}) - I_R \otimes \mathcal{N}(|\Psi\rangle_{RA})||_1 \tag{2.30}$$

This leads to the following definition of the *diamond norm distance*,

Definition 7 *The **diamond norm distance** between two channels $\mathcal{M},\mathcal{N}$ is defined by*

$$||\mathcal{M}-\mathcal{N}||_\diamond = \max_{|\Psi\rangle_{RA}} ||I_R \otimes \mathcal{M}(|\Psi\rangle_{RA}) - I_R \otimes \mathcal{N}(|\Psi\rangle_{RA})||_1 \tag{2.31}$$

The diamond norm distance satisfies the triangle inequality, is symmetric, and is zero if and only if $\mathcal{M} = \mathcal{N}$, as needed for a distance function. Note that there is no known closed form for the diamond norm distance, though efficient algorithms are known for computing it [15].

Next, we discuss a channel analogue of the fidelity.

Definition 8 *The **entanglement fidelity** $F(\mathcal{E},\mathcal{F})$ is defined by*

$$F_e(\mathcal{E},\mathcal{F}) = F(I_R \otimes \mathcal{E}(|\Psi^+\rangle\langle\Psi^+|_{RA}), I_R \otimes \mathcal{F}(|\Psi^+\rangle\langle\Psi^+|_{RA})) \tag{2.32}$$

where $F(\rho, \sigma)$ is the fidelity defined for quantum states, and $|\Psi^+\rangle_{RA}$ is the maximally entangled state.

In words, the entanglement fidelity $F(\mathcal{E}, \mathcal{F})$ looks at how similar of a state $\mathcal{E}$ and $\mathcal{F}$ produce when acting on one end of a maximally entangled state.

Notice that while the entanglement fidelity is defined by acting the channels on one fixed state, the maximally entangled one, the diamond norm distance was defined by optimizing over states. Despite this, there is a relationship between the entanglement fidelity and the diamond norm distance.

Lemma 6 *The diamond norm distance and entanglement fidelity are related by*

$$||\mathcal{E} - \mathcal{F}||_\diamond \leq d_A \sqrt{1 - F_e(\mathcal{E}, \mathcal{F})}. \tag{2.33}$$

Reference [13] contains a proof of this, see corollary 2.2 there. Heuristically, this follows because if the channels are similar on the maximally entangled state, by linearity they must be similar on each element in the superposition which forms the maximally entangled state. But the maximally entangled state is a superposition of each basis element in the Hilbert space, so the channels must be similar for all states.

2.4 Entropy and mutual information

In this section we review the von Neumann entropy and a few related quantities. Because these objects are by now familiar to the AdS/CFT community we keep our discussion brief.

We begin by defining the von Neumann entropy.

Definition 9 *Given a density matrix ρ_A, the von Neumann entropy of A is defined by*

$$S(A)_\rho \equiv -tr\, \rho_A \log \rho_A. \tag{2.34}$$

This object has an important operational meaning: given a state $\rho_A^{\otimes n}$, $n \times S(A)_\rho$ is the number of uses of the identity channel $\mathcal{I}_{A\to B}$ needed to reproduce ρ on the B subsystem. Since each use of the channel lets us transmit one qubit of information

to Bob, we see that $S(A)_\rho$ is measuring the number of qubits of information stored in A. For a review see for example [99].

To gain some intuition for the von Neumann entropy, notice first that the entropy of any pure state is 0. Second, the maximally mixed state

$$\rho_{mix} = \frac{I}{d} \tag{2.35}$$

has von Neumann entropy $\log d$, which is its maximal possible value.

Another object we will make use of in this thesis is the mutual information, defined in terms of the von Neumann entropy below.

Definition 10 *Given a density matrix ρ_{AB}, the **mutual information** is defined by*

$$I(A:B)_\rho = S(A)_\rho + S(B)_\rho - S(AB)_\rho. \tag{2.36}$$

The mutual information is related to the relative entropy given in lemma 4. Indeed a simple calculation reveals that

$$I(A:B)_\rho = D(\rho_{AB}||\rho_A \otimes \rho_B). \tag{2.37}$$

In words, the mutual information is a measure of distinguishability between a quantum state ρ_{AB} and the product of its marginals $\rho_A \otimes \rho_B$[1]. This indicates that the mutual information measures how correlated the A and B subsystems are. To gain some intuition for the mutual information, consider the maximally entangled state

$$|\Psi^+\rangle_{AB} = \frac{1}{2}\left(|00\rangle_{AB} + |11\rangle_{AB}\right). \tag{2.38}$$

The reduced density matrices for A and B are maximally mixed, while the state on AB is pure. Thus the mutual information has a value of 2. On the other hand if we inserted the product state $|00\rangle_{AB}$. Then the mutual information would return 0.

Importantly, the mutual information measures classical correlation, not just en-

[1] In fact, the product of the marginals is the closest product state to ρ_{AB}, so $I(A:B)_\rho = \min_{\sigma_A \otimes \sigma_B} D(\rho_{AB}||\sigma_A \otimes \sigma_B)$.

tanglement. For instance suppose we had the state

$$\rho_{AB} = \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B) \tag{2.39}$$

This corresponds to Alice and Bob holding a single perfectly correlated classical bit. Then the mutual information is 1, so that the classical correlation is still counted, although at half the value.

2.5 Inverting quantum channels

A basic feature of the dynamics of quantum mechanics is that, if we consider the full system, it is reversible. This is because the dynamics is implemented by a unitary U, which always has an inverse $U^\dagger$. This corresponds to the fact that information is preserved in quantum mechanics. In the context of quantum channels, which capture the dynamics of subsystems, information may be lost. Acting with some channel $\mathcal{N}_A$, we can ask if some of the information in A is lost to some other system, call it E, potentially preventing $\mathcal{N}_A$ from being reversible.

Our goal in this section will be to understand when a channel $\mathcal{N}_A$ is reversible. In doing so, we will introduce a number of techniques that will prove valuable later in this thesis. As well, we will simplify the discussion of quantum error correction in the next section. Our presentation loosely follows [85, 86].

Channel acts on a fixed, known state

We will first of all consider the case where the channel acts on a single, fixed state. We will assume further that the state is known, and ask when we can undo the effect of $\mathcal{N}_A$. Naively, the problem is trivial: if we know the state we could just toss out the channels output and prepare a new copy of the state. However, there is a complication. The channel acts on a subsystem A, and we want to undo its action by acting again only on A. If the input to the channel is a joint state $|\Psi\rangle_{RA}$ however, in general we cannot prepare this state by acting on A alone. Indeed if $|\Psi\rangle_{RA}$ is entangled and $\mathcal{N}_A$ breaks the entanglement between R and A, by for instance throwing out A and replacing it with a fixed state, we cannot hope to recover $|\Psi\rangle_{RA}$. This means the question is non-trivial, and we will search for

a condition that expresses when the action of $\mathcal{N}_A$ on some state $|\Psi\rangle_{RA}$ can be undone.

We use the Schmidt decomposition [73] to write the state in the form

$$|\Psi\rangle_{RQ} = \sum_k \sqrt{\lambda_k}|k\rangle_R|k\rangle_A. \tag{2.40}$$

The channel $\mathcal{N}_A$ will act on the A subsystem of this state, while the R system will remain untouched. Recall that quantum channels can be implemented as unitaries acting on some larger system, then performing a partial trace,

$$\mathcal{N}_A(\cdot) = \mathrm{tr}_E U_{AE}(\cdot \otimes |0\rangle\langle 0|_E)U_{AE}^\dagger. \tag{2.41}$$

We will postpone taking the trace, and think about the state

$$|\Phi\rangle_{RAE} = U_{AE}|\Psi\rangle_{RA}|0\rangle_E. \tag{2.42}$$

We would like to understand when, by acting on A, we can undo the effect of U_{AE} and restore the state $|\Psi\rangle_{RA}$. It will be convenient to understand this in terms of features of the state $|\Phi\rangle_{RAE}$.

To understand when we can reverse the channel $\mathcal{N}_A$, it is helpful to recall our original intuition for when this might not be possible. If information escapes from A into the E system, it won't be possible to act on A alone and restore the original state. This suggests a natural condition to study is

$$I(R:E)_\Phi = 0. \tag{2.43}$$

That is, when the reference system, initially correlated with A, remains uncorrelated with E we expect A has not lost information to E and we can undo the channel. We claim that we can undo the channel $\mathcal{N}$ acting on $|\Psi\rangle$ if and only if this is zero.

To understand this in more detail, recall that

$$I(R:E)_\Phi = D(\Phi_{RE}||\Phi_R \otimes \Phi_E), \tag{2.44}$$

so that zero mutual information means

$$\Phi_{RE} = \Phi_R \otimes \Phi_E. \tag{2.45}$$

We know also know that the state on RAE is pure. These two facts suffice to show that $|\Phi\rangle$ is in the form

$$|\Phi\rangle_{RAE} = \sum_{k,l} \sqrt{\lambda_k \mu_l}\, |k\rangle_R\, |\psi_{kl}\rangle_A\, |l\rangle_E\,, \tag{2.46}$$

where all of the sets of states $\{|k\rangle_R\}$, $\{|l\rangle_E\}$ and $\{|\psi_{kl}\rangle_A\}$ are orthonormal. This is sensible, as the above form has correlations between R and E, but only though ψ_{kl}.

From the form 2.46, we can understand how to invert the effect of the channel $\mathcal{N}_A$ and recover $|\Psi\rangle_{RA}$. It is helpful to think about this recovery in two steps. First, apply a measurement $\{M_A^l\}$

$$M_A^l \equiv \sum_k |\psi_{kl}\rangle\langle\psi_{kl}|_Q. \tag{2.47}$$

After doing so, we hold one of the states

$$\sum_k \sqrt{\lambda_k}\, |k\rangle_R\, |\psi_{kl}\rangle_A\, |l\rangle_E \tag{2.48}$$

and we know the value of l. Then, we can trace out the E system, leaving

$$\sum_k \sqrt{\lambda_k}\, |k\rangle_R\, |\psi_{kl}\rangle_A. \tag{2.49}$$

Finally, apply the unitary U_l defined such that

$$U_l |\psi_{kl}\rangle_A = |k\rangle_A \tag{2.50}$$

which recovers $|\Psi\rangle_{RA}$. This shows that if $I(R : E) = 0$ we can recover the original state.

Since measurement and the conditional unitary are both channels, we can com-

pose these together and describe the entire recovery procedure as a channel $\mathcal{N}_A^{-1}$. We refer to this as a recovery channel, as it recovers the state on A after the action of the channel $\mathcal{N}_A$. Another way we can summarize this is to write

$$\mathcal{N}_{A,\Psi}^{-1} \circ \mathcal{N}_A(|\Psi\rangle\langle\Psi|_{RA}) = |\Psi\rangle\langle\Psi|_{RA}. \tag{2.51}$$

We can also show the converse, which is that if we can recover the original state then $I(R : E) = 0$. To see this, we express the mutual information in terms of the relative entropy, then use monotonicity of the relative entropy (equation 2.28) to find

$$I(R : E)_{\mathcal{N}^{-1}\Phi=\Psi} \leq I(R : E)_{\mathcal{N}\Psi=\Phi} \leq I(R : E)_{\Psi} \tag{2.52}$$

Then note that in the Ψ state E is not correlated with R, so that $I(R : E)_{\Psi} = 0$, and so $I(R : E)_{\Phi} = 0$ as needed.

Unknown state

In the last section we developed a recovery channel which works for a specific choice of input state. In general, we may not know the input state, and are interested in understanding when an inverse exists, that is when there is a channel $\mathcal{N}_A^{-1}$ such that

$$\mathcal{N}_A^{-1} \circ \mathcal{N}_A = I. \tag{2.53}$$

To understand when this exists, we can actually notice that choosing $|\Psi\rangle$ to be a maximally entangled state produces a channel that works for all states. This observation is summarized in the next theorem.

Theorem 2 ***Inverse channels:*** *Given a quantum channel $\mathcal{N}_A$, an inverse channel exists if and only if*

$$I(R : E)_{\Phi} = 0 \tag{2.54}$$

where the state Φ is defined by

$$|\Phi\rangle_{RAE} = (I_R \otimes U_{AE})(|\Psi^+\rangle_{RA} \otimes |0\rangle) \tag{2.55}$$

and U_{AE} is any unitary extension of the channel $\mathcal{N}_A$.

To understand this theorem, consider choosing $|\Psi\rangle = |\Psi^+\rangle_{RA}$ (the maximally entangled state) and acting with the channel $\mathcal{N}_A$. Then from the last section, we know that

$$\mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A(|\Psi^+\rangle\langle\Psi^+|_{RA}) = |\Psi^+\rangle\langle\Psi^+|_{RA}. \tag{2.56}$$

But, now consider teleporting some system A' in state $|\psi\rangle_{A'}$ using the entangled state on RA. First suppose that we perform the teleportation after $\mathcal{N}^{-1}_{A,\Psi^+}$ has been performed. Then the state on RA is maximally entangled, and we reproduce the input state on the A system, so the final state is $|\psi\rangle_A$.

Next suppose that the we perform the Bell basis measurement on $A'R$ before applying the inverse or direct channels. Then the state on A is

$$X^{k_1}Z^{k_2} \circ \mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A(X^{k_1}Z^{k_2}|\psi\rangle_A). \tag{2.57}$$

Our measurement on $A'R$ must commute with the action of the channel on A, so we find

$$|\psi\rangle_A = X^{k_1}Z^{k_2} \circ \mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A(X^{k_1}Z^{k_2}|\psi\rangle_A). \tag{2.58}$$

Moving the Pauli's to the left and redefining $X^{k_1}Z^{k_2}|\psi\rangle \to |\psi\rangle$, we learn

$$|\psi\rangle_A = \mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A(|\psi\rangle_A) \qquad \forall|\psi\rangle \tag{2.59}$$

From here, it is straightforward to show that $\mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A$ also acts trivially on subsystems of a larger pure state. Doing so requires that we show

$$\mathcal{N}^{-1}_{A,\Psi^+} \circ \mathcal{N}_A(|k\rangle\langle l|) = |k\rangle\langle l| \tag{2.60}$$

It is straightforward to do this by studying the action of the channel on $|+\rangle =$

$(|k\rangle + |l\rangle)/2$ and $|-\rangle = (|k\rangle - |l\rangle)/2$.

Unknown state, approximate decoupling

Finally, we will show that an approximate version of theorem 2 also holds. That is, if the channels output is nearly decoupled from the environment, then there is a channel that nearly reverses it.

Theorem 3 ***Inverse channels:*** *Given a quantum channel $\mathcal{N}_A$, suppose that*

$$I(R:E)_\Phi \leq \epsilon \tag{2.61}$$

where the state Φ is defined by

$$|\Phi\rangle_{RAE} = (I_R \otimes U_{AE})(|\Psi^+\rangle_{RA} \otimes |0\rangle_E) \tag{2.62}$$

and U_{AE} is any unitary extension of the channel $\mathcal{N}_A$. Then there exists an approximate inverse channel $\mathcal{N}^{-1}$ such that

$$F(|\Psi\rangle_{RA}, \mathcal{I} \otimes \mathcal{N}^{-1} \circ \mathcal{N}|\Psi\rangle_{RA}) \geq 1 - \sqrt{\epsilon} \tag{2.63}$$

Proof. Recall that

$$I(R:E)_\Phi = D(\rho_{RE} : \rho_R \otimes \rho_E). \tag{2.64}$$

So that the relative entropy above is small. Relating the relative entropy to the trace distance by Pinskers inequality, and then the trace distance and the fidelity by the Fuchs van de Graff 2.23 inequalities, we learn that

$$F(\rho_{RE}, \rho_R \otimes \rho_E) \geq 1 - \sqrt{\epsilon}. \tag{2.65}$$

We know that some particular pure states will realize this fidelity,

$$F(\rho_{RE}, \rho_R \otimes \rho_E) = |\langle\Phi|\hat{\Phi}\rangle_{RAE}|. \tag{2.66}$$

The state $|\hat{\Phi}\rangle_{RAE}$ is a purification of $\rho_R \otimes \rho_E$, so has zero mutual information

$I(R:E)_{\hat{\Phi}} = 0$. This means the recovery channel described in the last section works perfectly for this state, so there exists a channel $\mathcal{E}$ which recovers $|\Psi\rangle_{RA}$ from this state. Our basic strategy is to use the fact that Φ is close to $\hat{\Phi}$ to show that this map approximately recovers Ψ from Φ as well.

We know that the fidelity increases under the action of a channel, so

$$F(\omega_{RA}, |\Psi\rangle_{RA}) \geq |\langle\Phi|\hat{\Phi}\rangle_{RQ'E'}| \tag{2.67}$$

where ω_{RA} is the state we recover from $|\Phi\rangle$ by applying $\mathcal{E}$. Then use

$$\begin{aligned} F(\omega_{RA}, |\Psi\rangle_{RA}) &\geq |\langle\Psi|\hat{\Psi}\rangle_{RAE}| \\ &= F(\rho_{RE}, \rho_R \otimes \rho_E) \\ &= 1 - \sqrt{\epsilon}. \end{aligned} \tag{2.68}$$

Thus the state we recover is approximately the original one, as needed. ■

2.6 Quantum error correction

In the context of performing useful tasks with quantum information, it is sometimes necessary to protect against the loss of information. To do this, we encode a quantum system $\mathcal{H}_L$ into a larger Hilbert space $\mathcal{H}_P$, via an *encoding channel* $\mathcal{E}_{L\to P}$. Then, some *noise channel* occurs, which acts on the $\mathcal{H}_P$ space and maps it into some space P'. In this thesis we will only be concerned with the case where the noise channel consists of tracing out some subsystem of P, which we call an *erasure error*, so that P' is a subsystem of P. The hope is that by choosing the encoding channel appropriately we can reverse the effect of at least some erasure errors and recover the L system (which also lets us recover the P system, since we can re-apply $\mathcal{E}_{L\to P}$). A choice of encoding channel $\mathcal{E}$ defines an *error correcting code*.

We can use the recovery condition from the last section to understand when we can correct the error channel. We consider the maximally entangled state $|\Psi^+\rangle_{RL}$,

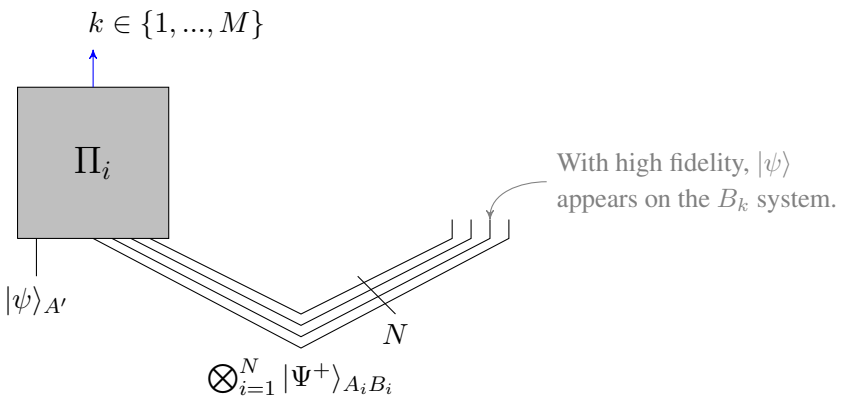


Figure 2.1: The port-teleportation protocol. A state $|\psi\rangle$ is held in system A', along with N entangled systems $|\Psi^+\rangle_{A_i B_i}$. A POVM $\{\Lambda^k\}$ is performed on the $A'A$ system producing output $k \in \{1, ..., N\}$. The state $|\psi\rangle$ then appears on the B_k system with a fidelity controlled by $1/N$.

and apply the encoding channel,

$$|\Phi\rangle_{RP} = I \otimes \mathcal{E}_{L \to P} |\Psi^+\rangle_{RL}. \tag{2.69}$$

Theorem 2 tells us we can recover L exactly when R is unentangled with the environment. For the erasure channel considered here, the environment is just the traced out subsystem $P \setminus P'$, so we can recover when

$$I(R : P \setminus P')_\Phi = 0. \tag{2.70}$$

Thus given an error correcting code, we can understand which subsystems it is possible to recover the logical system from by encoding a maximally entangled state and then calculating the mutual information of various subsystems with the reference system. Similarly, we can define an approximate error correcting code by requiring the state be approximately recovered, and the corresponding condition is that the mutual information above be small.

2.7 Port-teleportation

In this section we describe the port-teleportation protocol, first introduced in [49]. Port-teleportation will be important in understanding the non-local quantum computation protocols described in section 2.7.

The basic steps of any teleportation are as follows.

1. Distribute an entangled resource state $|\Psi\rangle_{AB}$ between Alice and Bob, where Alice holds A and Bob holds B. Further, Alice prepares the state $|\psi\rangle_{A'}$ she would like to send to Bob.
2. Alice performs a POVM measurement $\mathcal{M} = \{F_x\}_x$ on the AA' system.
3. Alice sends Bob the classical measurement outcome x.
4. Bob applies some channel $\mathcal{C}_x$ to B.

The teleportation is successful when the final state on B is $|\psi\rangle_B$.

The most familiar example of a teleportation procedure is occurs when A' is a qubit, $|\Psi\rangle_{AB} = |\Psi^+\rangle_{A'A}$ is the maximally entangled state, and the measurement is in the Bell-basis,

$$\mathcal{M} = \{|\Psi^+\rangle_{A'A}, X_A|\Psi^+\rangle_{A'A}, Z_A|\Psi^+\rangle_{A'A}, X_A Z_A|\Psi^+\rangle_{A'A}\} \tag{2.71}$$

We will call this *Bell-basis teleportation*, or just teleportation when it is clear from context that we mean this procedure specifically. An important fact about Bell-basis teleportation is that after Alice's measurement the B system is in one of the states

$$Z_B^{x_1} X_B^{x_2} |\psi\rangle_B \tag{2.72}$$

Bob's correction operation is to apply $Z_B^{x_1} X_B^{x_2}$, which he can do once he receives $x = x_1 x_2$ from Alice.

Now consider a different teleportation procedure, known as *port-teleportation* and illustrated in figure 2.1. In port-teleportation the entangled state is

$$|\Psi\rangle_{AB} = \otimes_{i=1}^{N} |\Psi^+\rangle_{A_i B_i} \tag{2.73}$$

The measurement will produce an outcome $x \in 1, ..., N$, and the correction op-

eration will be to trace out all but the xth subsystem B_i. We will discuss below how the measurement can be chosen to achieve this. The key distinctions between port-teleportation and Bell-basis teleportation are that 1) N may be quite large, so that the dimensionality of the resource system is much larger than the input system A' and 2) The correction operation is the trace, which has the interesting feature of commuting with unitaries $\otimes_i U_{B_i}$ acting on each output 'port' B_i. We discuss below why this is a valuable feature.

Lets understand how to choose the measurement step to achieve the desired functionality of port-teleportation. Let's begin by writing the entire teleportation procedure as a quantum channel,

$$\mathcal{T}_{A'\to B'}(\sigma^{in}_{A'}) = \sum_k^N \mathrm{tr}_{AA'\bar{B}_k}\left(\Lambda^k_{AA'}\left[\left(\bigotimes_{i=1}^N |\Psi^+\rangle\langle\Psi^+|_{A_iB_i}\right)\otimes\sigma^{in}_{A'}\right]\right)_{B_k\to B'}$$

The final subscript indicates that we relabel the B_k system as B' after taking the trace. System $\bar{B}_k$ refers to $B_1...B_N \setminus B_k$. We can take the trace over $\bar{B}_k$ explicitly, leading to

$$\mathcal{T}_{A'\to b}(\sigma^{in}_{A'}) = \sum_k \mathrm{tr}_{AA'}\left(\Lambda^k_{AA'}\left[\sigma^k_{AB}\otimes\sigma^{in}_{A'}\right]\right), \tag{2.74}$$

where the states σ^k_{AB} are defined by

$$\begin{aligned}\sigma^k_{AB} &= \mathrm{tr}_{\bar{B}_k}\left(\bigotimes_{i=1}^N |\Psi^+\rangle\langle\Psi^+|_{A_iB_i}\right),\\ &= |\Psi^+\rangle\langle\Psi^+|_{A_kB'}\otimes I_{\bar{A}_k}.\end{aligned} \tag{2.75}$$

Note that we've already done the relabeling to B'.

We will use the entanglement fidelity introduced in section 2.3 to quantify how close our teleportation channel $\mathcal{T}$ is to the identity. When one of the inputs in the identity, the entanglement fidelity simplifies to

$$F_e(\mathcal{T}, I) = \mathrm{tr}\left(\Psi^+_{CB'}(I_C\otimes\mathcal{T}_{A'\to B'})(\Psi^+_{CA'})\right). \tag{2.76}$$

Later we will try to make this as large as possible by a careful choice of measurement $\{\Lambda_k\}$. We can insert the form of our channel into the expression above,

$$F_e(\mathcal{T}, I) = \sum_k \text{tr}(\Psi^+_{CB'} \Lambda^k_{AA'} (\sigma^k_{AB'} \otimes \Psi^+_{CA'})). \tag{2.77}$$

To simplify this further, we can move the $\Lambda^k_{AA'}$ operator to act on AB'. To see how to do this, we can make the observation

$$(I \otimes \mathcal{O}_Y)|\Psi^+\rangle_{XY} = (\mathcal{O}_X^T \otimes I)|\Psi^+\rangle_{XY} \tag{2.78}$$

where the T superscript indicates the transpose. In our case $\Lambda^k_{AA'}$ is acting on the left of $\Psi^+_{CA'}$, so we can use a (partial) transpose to write this as an operator on the AC system. Then note that Λ_{AC} is acting on the right of $\Psi^+_{CB'}$, so we can undo that same transpose to write it on the AB' system. This gives

$$\begin{aligned} F_e(\mathcal{T}, I) &= \sum_k \text{tr}(\Psi^+_{CB'} \Lambda^k_{AB'} (\sigma^k_{AB'} \otimes \Psi^+_{CA'})), \\ &= \sum_k \text{tr}(\Psi^+_{A'B'} \Lambda^k_{AB'} (\sigma^k_{AB'})), \\ &= \sum_k \text{tr}(\Lambda^k_{AB'} \sigma^k_{AB'}). \end{aligned} \tag{2.79}$$

Notice however that this is a guessing probability: it's the probability of guessing σ^k correctly using the POVM $\{\Lambda^k\}$. In section 2.1 we discussed a sensible way to do this called the pretty-good measurement, which uses POVM elements

$$\Lambda^k = \sigma^{-1/2} \sigma^k_{AA'} \sigma^{-1/2}. \tag{2.80}$$

Using the explicit form of the states σ^k given in equation 2.75, we can calculate the entanglement fidelity when taking Λ^k to be defined by the pretty-good measurement. This turns out to be bounded below by

$$F_e(\mathcal{T}, I) \geq 1 - \frac{d^2 - 1}{N}. \tag{2.81}$$

Using lemma 6, we can also bound the diamond norm distance between this tele-

portation channel and the identity,

$$||\mathcal{T} - \mathcal{I}||_\diamond \leq \frac{4d^2}{\sqrt{N}} \tag{2.82}$$

Because the diamond distance measures how distinct the two input channels are maximized over input states, this bound shows that the teleportation channel works well for all input states.

To gain further intuition for port-teleportation, it is helpful to write out the POVM elements explicitly,

$$\Lambda^k_{AA'} = \sigma^{-1/2} \left(|\Psi^+\rangle\langle\Psi^+|_{A_i A'} \otimes \mathcal{I}_{\bar{A}_i} \right) \sigma^{-1/2}. \tag{2.83}$$

Ignoring for a moment the normalizing $\sigma^{-1/2}$ factors, these are intuitive: they are projecting in an EPR pair between A' and the A_i system, which just means mapping the A' to the B_i system identically. The addition of the $\sigma^{-1/2}$ factors smears these projectors such that this forms a complete measurement basis.

Chapter 3

Quantum cryptography

In addition to the topics in quantum information theory described in the last chapter, this thesis will also make use of a number of topics in quantum cryptography. In particular chapter 5.1 deals with a spacetime generalization of quantum secret sharing, and the quantum one-time pad will be a key tool employed there. As well our technical handle on entanglement requirements in non-local quantum computation, discussed in section 4.4 begins with monogamy games.

3.1 Classical and quantum secret sharing

A secret sharing scheme distributes classical or quantum information among several parties in such a way that only certain subsets of those parties can learn the information. We will start out by discussing the classical case, before moving on to the quantum case.

Definition 11 *A **classical secret sharing scheme** is defined by a list of parties Bob_1... Bob_n, along with*

- *A list of authorized subsets of parties, $\mathcal{A}_i$*
- *A list of unauthorized subsets of parties, $\mathcal{U}_j$*

Successfully implementing the scheme requires sharing classical keys k_m to each Bob_m such that keys $\{k_j\}_{j\in\mathcal{A}_j}$ can be used to reconstruct s, while simultaneously keys $\{k_l\}_{l\in\mathcal{U}_j}$ cannot be used to learn anything about s.

To fully understand this definition, we should make precise what we mean by some subset of the keys not holding any information about the secret. To do this, we consider random variables $S, K = K_1...K_n$ which hold the secret s in variable S, and keys k_i on variables K_i. There is some probability distribution P_{SK} which describe the values of these variables. Then we say $\{k_l\}_{l\in\mathcal{U}_j}$ cannot be used to learn anything about s if

$$I(S : \{K_l\}_{l\in\mathcal{U}_j}) = 0. \tag{3.1}$$

In this case the variables $\{k_l\}_{l\in\mathcal{U}_j}$ are uncorrelated with s.

Example 2 *Consider a secret sharing scheme with two parties Bob$_1$ and Bob$_2$, where we require each Bob separately to be unauthorized but both together to be authorized. This is realized by picking a random key k_1 and then defining k_2 such that*

$$s = k_1 \oplus k_2 \tag{3.2}$$

Since this ensures Bob$_1$ and Bob$_2$ can indeed calculate s if they collaborate, we see that this construction is correct. If we assume s is also randomly distributed, this defines P_{SK}. From this we can straightforwardly calculate $I(S : K_1) = I(S : K_2) = 0$, establishing this procedure is also secure.

Now we define a quantum secret sharing scheme.

Definition 12 *A **quantum secret sharing scheme** is defined by a list of parties Bob$_1$... Bob$_n$, along with*

- *A list of authorized subsets of parties, $\mathcal{A}_i$*
- *A list of unauthorized subsets of parties, $\mathcal{U}_j$*

Successfully implementing the scheme requires sharing quantum systems K_i to each Bob$_i$ such that systems $\{K_j\}_{j\in\mathcal{A}_j}$ can be used to reconstruct S, while simultaneously systems $\{K_j\}_{j\in\mathcal{U}_j}$ cannot be used to learn anything about S.

To define what it means precisely for $\mathcal{U}_j$ to not contain any information about S, consider taking S to be one half of a maximally entangled state $|\Psi^+\rangle_{RS}$. Then if

$$I(R : \{K_i\}_{i \in \mathcal{U}_j}) = 0 \tag{3.3}$$

theorem 2 tells us S can be recovered from $K \setminus \mathcal{U}_j$. Intuitively, since quantum information cannot be cloned, we can then say that this also means $\mathcal{U}_j$ contains no information about S. We can also define the secret sharing scheme to be secure if the above is small, and apply the results in section 2.5 on approximate recovery.

Quantum error correcting codes that correct erasure errors and secret sharing schemes are closely related. To see why, consider a quantum error correcting code where the physical space P is divided into subsystems $P_1 ... P_n$. Suppose that the code corrects errors on subsets $\mathcal{P}_i$. Then this also defines a quantum secret sharing scheme with authorized sets $\mathcal{A}_i = P \setminus P_i$ and $\mathcal{U} = \mathcal{P}_i$.

A particularly simple type of secret sharing scheme is a *threshold scheme*, where a quantum state is divided among n parties in such a way that any k of them can reconstruct the state, but no set of $k-1$ can. We denote such a threshold scheme by $((k, n))$. It is clear that a threshold scheme can exist only for $k > n/2$, since otherwise there would be two disjoint subsets of size k, who could each construct a copy of the quantum state, in violation of the no-cloning theorem. In fact this is the only condition on a threshold scheme, and they always exist whenever $k > n/2$.

We can also ask when a secret sharing scheme with a more general access structure can exist. There are two conditions which clearly must be met:

$$\begin{aligned} \mathcal{A}_i \cap \mathcal{A}_j &\neq \varnothing \\ \mathcal{A}_i \setminus \mathcal{U}_j &\neq \varnothing \end{aligned} \tag{3.4}$$

The first condition follows from no-cloning: there cannot be two disjoint authorized sets. The second condition expresses that an unauthorized set cannot contain an authorized one. Gottesman [39] proved that these conditions are also sufficient.

3.2 The classical and quantum one-time pad

In addition to quantum secret sharing, an additional tool from quantum cryptography we will make use of in this thesis is the quantum one-time pad [9].

To introduce the quantum one-time pad, it is instructive to review the classical one-time pad. There, the scenario is as follows. We have three parties, call them Alice, Bob, and Eve. Alice's goal is to send a message to Bob, and furthermore for that message to be concealed from Eve. We will take Alice's message to be a string of bits $\vec{m}$.

Assume Alice and Bob share a *public channel*, which means Eve gets to act on any messages sent from Alice to Bob. In particular, she might make copies of the bits. With this public channel alone as a resource, clearly Alice's goal is impossible. To see this, we need only note that Bob and Eve hold the same resources (a public channel connecting them to Alice), so there can not be a protocol which favours Bob over Eve.

To break the symmetry between Bob and Eve and allow Alice and Bob to communicate privately, we should give Bob some additional resource. Our strategy will be to give Alice and Bob copies of a string of random bits $\vec{k}$, which we call the *secret key*. Then Alice and Bob can follow a simple protocol to send a private message.

Protocol 1 ***Classical one-time pad:***

- *Alice computes* $\vec{x} = \vec{m} \oplus \vec{k}$
- *Alice uses the public channel to send* $\vec{x}$ *to Bob and Eve*
- *Bob computes* $\vec{x} \oplus \vec{k} = \vec{m}$

Clearly this works correctly, as $\vec{x} \oplus \vec{k} = \vec{m} \oplus \vec{k} \oplus \vec{k} = \vec{m}$. It is also secure, since $\vec{x}$ is independent of $\vec{m}$. A classic result by Shannon [88] shows that this is optimal — it is impossible to perfectly conceal a classical message of length n with fewer than n shared random classical bits.

We will be interested in a quantum analogue of the above communication task. To define this, we need a notion of a *public quantum channel*. In this case we allow

Eve to act on any qubits sent from Alice to Bob with her own channel, which might involve removing the message qubits and replacing them with other qubits.

We will be interested in the following quantum analogue of the communication task described above. Alice holds n qubits, $\bigotimes_i |\psi_i\rangle_{A_i}$. She wishes to send the n qubits to Bob, but wants to do so secretly. In particular it should be impossible for Eve to learn anything about the message qubits. However, Alice and Bob share only a public quantum channel.

To achieve this we can again have Alice and Bob hold a secret key, call it $\vec{k}$. Now though, it is not clear how large of secret key they need to hold to safely transmit n qubits, or how Alice should act on her qubits to conceal them from Eve.

We can answer both questions by considering the (Bell basis) quantum teleportation protocol [16]. Recall that in teleportation Alice holds a quantum state $|\psi\rangle$ which she wishes to send to Bob. Alice and Bob share a maximally entangled state $|\Psi^+\rangle_{A'B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and the transmission is achieved via the following steps.

Protocol 2 ***Bell-basis teleportation:***

1. *Alice measures the AA' system in the Bell basis, obtaining two bits of measurement outcome $b_1 b_2$*
2. *Alice sends $b_1 b_2$ to Bob.*
3. *Bob applies $X^{b_1} Z^{b_2}$ to system B.*

At the end of the protocol Bob holds $|\psi\rangle_B$.

To see why this tells us how long of a key is necessary in the quantum one-time pad, consider the states held by Alice and Bob after the Bell basis measurement has been performed in the teleportation protocol. The overall state is

$$|b_1 b_2\rangle_M \otimes X^{b_1} Z^{b_2} |\psi\rangle_B. \tag{3.5}$$

where M is Alice's measurement apparatus. At this stage in the protocol no information has been sent to Bob from Alice. Consequently, Bob's state must be

independent of ψ, and it follows that

$$\rho_B = \frac{1}{4}\sum_{b_1 b_2} X^{b_1} Z^{b_2} |\psi\rangle\langle\psi| X^{b_1} Z^{b_2} = \frac{I}{2} \tag{3.6}$$

We can also verify this with a direct calculation. The above reveals that just two classical bits suffice to hide a qubit, and that the encoding procedure is to apply one of the four unitaries $X^{b_1} Z^{b_2}$ to each qubit.

With this insight in hand we can give the protocol for the quantum one-time pad.

Protocol 3 ***Quantum one-time pad:*** *For each qubit $|\psi_i\rangle$,*

1. *Alice uses two bits from the key $\vec{k}$ to prepare the state $X^{k_{i1}} Z^{k_{i2}} |\psi_i\rangle_{A_i}$.*
2. *Alice inputs A_i to the public quantum channel $\mathcal{N}_{A_i \to B_i}$.*
3. *Bob applies $X^{k_{i1}} Z^{k_{i2}}$ to B_i.*

At the end of the protocol Bob holds $|\psi_i\rangle_{B_i}$, as needed. Security of the one-time pad follows from equation 3.6.

3.3 Monogamy games

In this section we study a class of games called *monogamy games*, which are played by three players, call them Alice, Bob, and Charlie. They are called monogamy games because they explore operationally the monogamy of entanglement, and indeed are one way of giving monogamy a precise meaning. Monogamy games are relevant to quantum key distribution, which is perhaps the most well established area of quantum cryptography, but our interest will be in a a second application of these games to position-based cryptography. We explore the connection to position-based cryptography in section 4.3. Our presentation follows [93] and appendix A of [63].

A *monogamy game* is defined by a set of measurements $\{\mathcal{M}^\theta\}_\theta$ on a d-dimensional system, along with a winning condition, which we define below. We will be interested in the case where $d = 2$, so each measurement is on a qubit, but the generalization to d dimensional systems is obvious. To carry out the game, Alice, Bob, and Charlie implement the following steps.

Protocol 4 ***Monogamy game:***

- ***Preparation phase****: Bob and Charlie prepare a quantum state ρ_{ABC}. They then send system A to Alice, where A consists of n qubits. Bob holds B and Charlie holds C. Once this is done, Bob and Charlie may no longer communicate.*

- ***Question phase****: Alice chooses a random string of length n, call it $\theta = \theta_1 ... \theta_n$. She then measures her ith qubit using measurement $\mathcal{M}^{\theta_i}$, obtaining outcomes $x = x_1 ... x_n$. Alice then announces θ to Bob and Charlie.*

- ***Answer phase****: Bob and Charlie each act on B and C respectively to form independent guesses x_b, x_c of Alice's measurement outcomes.*

We define Bob and Charlie to have won the game if some condition on x, x_b, x_c is met. Typically the requirement is that Bob and Charlie both guess Alice's outcome correctly, that is $x = x_b = x_c$. We will also consider a relaxation of this where Bob and Charlie correctly guess some fraction $1 - \delta$ of Alice's n measurement outcomes.

A standard monogamy game considered in quantum cryptography is the BB84 game, where we choose

$$\begin{aligned} \mathcal{M}^1 &= \{|0\rangle\langle 0|, |1\rangle\langle 1|\}, \\ \mathcal{M}^2 &= \{|+\rangle\langle +|, |-\rangle\langle -|\}. \end{aligned} \tag{3.7}$$

We will denote the corresponding game by G_{BB84}. The following bound constrains Bob and Charlies success probability.

Lemma 7 *The success probability $p_{suc}(G_{BB84})$ is upper bounded by* $\cos^2(\pi/8)$.

We refer to [93] for the proof. To understand why this success probability should be bounded above however, consider the statistics of measuring a maximally entangled state $|\Psi^+\rangle_{AX}$. Performing identical measurements of both ends of such a state always produces identical outcomes, regardless of which measurement is performed. In the context of completing the G_{BB84} task, Bob and Charlie can make use of this by preparing $|\Psi^+\rangle_{AX}$ and giving the A system to Alice. Unfortunately

though, they must split up before they learn Alice's measurement setting. If one of them holds X, and so is maximally entangled with Alice, that person can correctly guess Alice's measurement outcome. Bob and Charlie cannot both be maximally entangled with Alice however, and so the probability of both guessing correctly will be limited.

The bound in lemma 7 is actually tight. To achieve it, Bob and Charlie prepare $|\Psi^+\rangle_{AX}$, give A to Alice, then measure X in the basis $\{|\psi_0\rangle, |\psi_1\rangle\}$ where

$$\begin{aligned} |\psi_0\rangle &= \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle, \\ |\psi_1\rangle &= \cos\left(\frac{5\pi}{8}\right)|0\rangle + \sin\left(\frac{5\pi}{8}\right)|1\rangle. \end{aligned} \tag{3.8}$$

After doing so they obtain the classical measurement outcome x', which they copy and both hold after separating. They then both guess x' in the guessing phase. A straightforward analysis reveals this leads to the $\cos^2(\pi/8)$ success probability.

The G_{BB84} task defined above has A consisting of only one qubit. We can extend this task to it's *parallel repetition* $G_{BB84}^{\times n}$ on n qubits by specifying that Alice will measure each of her n qubits in one of the two bases 3.7 as specified by the string $\theta = \theta_1 ... \theta_n$. There are different ways now however of defining the winning condition for Bob and Charlie. We will declare Bob and Charlie successful if they both guess Alice's outcome correctly in a fraction $1 - \delta$ of the n rounds. We call the corresponding game $G_{\delta,BB84}^{\times n}$. The success probability is bounded in the next lemma.

Lemma 8 *The success probability of the $G_{\delta,BB84}^{\times n}$ task is upper bounded according to*

$$p_{suc}(G_{\delta,BB84}^{\times n}) \leq \left(2^{h(\delta)} \cos^2\left(\frac{\pi}{8}\right)\right)^n \equiv \left(2^{h(\delta)}\beta\right)^n \tag{3.9}$$

where the second equality defines β, and $h(x)$ is the binary entropy function $h(x) = -x \log x - (1-x)\log(1-x)$.

Again we refer to [93] for the proof.

Chapter 4

Quantum tasks

This chapter is a mix of original and review material. Each subsection cites the relevant sources.

In this chapter we introduce *relativistic quantum tasks*, which are similar to quantum channels, but their input and outputs occur at designated locations in spacetime. As we will see, this seemingly simple modification adds a large amount of complication. For instance, while the Kraus decomposition of quantum channels characterizes all operations that can be implemented in the context of quantum mechanics, it is not yet understand what the full set of achievable quantum tasks is.

After introducing a language for discussing quantum tasks, we review some of the basic results that are known in this area. One key result originates in position-based cryptography, a topic we take up in section 4.3. Position-based cryptography motivates a larger subject of non-local quantum computation, covered in section 4.4.

4.1 Localizing information to spacetime regions

This section appeared first in [68], which itself drew on my earlier work [43].

We will discuss quantum tasks where Alice is given inputs that are initially recorded into extended spacetime regions, and must be output at extended output

regions. To make this more precise, we define a notion of quantum information being localized to a spacetime region. Our definitions are adapted from [43].

Definition 13 *Suppose one party, Alice, holds system X of a quantum state $|\Psi\rangle_{XX'}$. Then we say the subsystem X is **localized** to a spacetime region $\mathcal{R}$ if a second party, Bob, for whom the state is initially unknown can prepare the X system by acting on $\mathcal{R}$ with some channel $\mathcal{M}_{\mathcal{R}\to X}$.*

If system X is localized to region $\mathcal{R}$ such that a channel $\mathcal{M}_{\mathcal{R}\to X}$ recovers X, we will say that X is **localized to $\mathcal{R}$ relative to $\mathcal{M}_{\mathcal{R}\to X}$.**

It will also be convenient to say a quantum system X is **excluded** from a spacetime region $\mathcal{R}$ if Bob cannot learn anything about X by accessing $\mathcal{R}$. One way to specify this precisely is to consider $|\Psi\rangle_{XX'}$ to be in the maximally entangled state. Then X is excluded from $\mathcal{R}$ when $I(\mathcal{R} : X') = 0$.

We should point out several features of these definitions. First, note that a system X is localized to $\mathcal{R}$ if and only if it is localized to the domain of dependence of $\mathcal{R}$, and similarly it is excluded from $\mathcal{R}$ if and only if it is excluded from the domain of dependence of $\mathcal{R}$. This follows because all the classical and quantum data in the domain of dependence of $\mathcal{R}$ is fixed by the data in $\mathcal{R}$ by time evolution. Consequently we will identify regions with their domains of dependence throughout this thesis.

Second, note that a quantum system X can be neither localized to nor excluded from a region $\mathcal{R}$ if some but not all information about X is available in $\mathcal{R}$. As well, notice that given a Cauchy surface Σ a quantum system can be excluded from both $\Sigma \cap \mathcal{R}$ and $\Sigma \setminus \mathcal{R}$. To do this, encode system X using the one-time pad (see section 3.2) using a classical key k. This hides the state on X, which can only be revealed if k is known. The X register can then be passed through $\Sigma \cap \mathcal{R}$ and k through $\Sigma \setminus \mathcal{R}$, and system X will be excluded from both regions. Of course, X will still be localized to the full Cauchy surface Σ.

There are many possible ways in which a quantum system can be localized to a given spacetime region, and a single quantum system can be localized to many different spacetime regions. Which sets of spacetime regions the same quantum information can be localized to is restricted however. In particular, if X is localized to a region $\mathcal{R}$ then it follows that X is excluded from the spacelike complement

$\mathcal{R}^c$. This is because otherwise we could act independently on $\mathcal{R}$ and $\mathcal{R}^c$ to produce copies of X, in violation of the no-cloning theorem.

As a simple example of how a single quantum system can be localized to many regions, suppose we have three subregions $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3$ which are all spacelike separated. Then define $\mathcal{R}_1 = \mathcal{X}_1 \cup \mathcal{X}_2$, $\mathcal{R}_2 = \mathcal{X}_2 \cup \mathcal{X}_3$, and $\mathcal{R}_3 = \mathcal{X}_3 \cup \mathcal{X}_1$. To localize a quantum system X to all three regions $\{\Sigma_1, \Sigma_2, \Sigma_3\}$, encode X into an error-correcting code on three subsystems $S_1 S_2 S_3$ that corrects one erasure error. Send system S_i to $\mathcal{X}_i$. Then each of the $\mathcal{R}_i$ contain two of the S_i subsystems, and X can be recovered from each of them.

Given a quantum system X, we can specify how it is localized in spacetime by specifying two sets of regions, call them $\{\mathcal{A}_X^i\}_i$ and $\{\mathcal{U}_X^i\}_i$. We specify that X is localized to each of the regions $\mathcal{A}_X^i$, and excluded from each of the regions $\mathcal{U}_X^i$. Implicitly, each region $\mathcal{A}_X^i$ comes with a specification of a channel $\mathcal{N}_{\mathcal{A}_X^i \to X}$ that specifies how X can be recovered from $\mathcal{A}_X^i$.[1] We summarize this in the next definition.

Definition 14 *A quantum system X is encoded into an **access structure** $\mathcal{S}_X = (\{\mathcal{A}_X^i\}_i, \{\mathcal{U}_X^i\}_i)$ if X is localized to each of the regions $\{\mathcal{A}_X^i\}_i$ and excluded from each of the regions $\{\mathcal{U}_X^i\}_i$.*

The term "access structure" is borrowed from the subject of quantum secret sharing, discussed in section 3.1.

4.2 The quantum tasks framework

This subsection first appeared in my work [68].

Next, we give a definition of a relativistic quantum task. Note that the notion of a quantum task was introduced in [55], although our definition follows [68].

Definition 15 *A **relativistic quantum task** is defined by a tuple $\mathbf{T} = \{\mathcal{M}, \mathscr{A}, \mathcal{S}_{\mathscr{A}}, \mathscr{B}, \mathcal{S}_{\mathscr{B}}, \mathcal{N}_{\mathscr{A} \to \mathscr{B}}\}$, where:*

- *$\mathcal{M}$ is the spacetime in which the task occurs, it is described by a manifold equipped with a metric.*

[1] In general there could be many such channels, though this will not be important for our purposes.

- *$\mathscr{A} = A_1 ... A_{n_a}$ is the collection of all the input quantum systems, and $\mathcal{S}_{\mathscr{A}} = \{\mathcal{S}_{A_1}, ..., \mathcal{S}_{A_{n_a}}\}$ is the set of all access structures for the input systems.*
- *$\mathscr{B} = B_1 ... B_{n_b}$ is the collection of all the output quantum systems, and $\mathcal{S}_{\mathscr{B}} = \{\mathcal{S}_{B_1}, ..., \mathcal{S}_{B_{n_b}}\}$ is the set of all access structures for the output systems.*
- *$\mathcal{N}_{\mathscr{A} \to \mathscr{B}}$ is a quantum channel that maps the input systems $\mathscr{A}$ to the output systems $\mathscr{B}$.*

Bob encodes the input systems A_i in such a way that the access structures $\mathcal{S}_{\mathcal{A}_i}$ are satisfied. To complete the task, Alice should apply the channel $\mathcal{N}_{\mathscr{A} \to \mathscr{B}}$ and localize each of the systems B_i according to the access structure $\mathcal{S}_{B_i}$.

To verify Alice has completed the task successfully, Bob will access one or more of the regions $\mathcal{A}^i_{B_j}$, $\mathcal{U}^i_{B_j}$ and attempt to recover system B_j. If Bob is able to produce B_j from the authorized region $\mathcal{A}^i_{B_j}$ he declares the task successful. Similarly if he is *unable* to produce B_j from the unauthorized region $\mathcal{U}^i_{B_j}$ he declares the task successful. The probability that Alice's outputs pass Bob's test is her success probability. Alice's success probability maximized over all possible protocols for completing the task is the tasks success probability, $p_{suc}(\mathbf{T})$.

Note that if Bob acts on one of the output regions $\mathcal{A}^i_{B_j}$, $\mathcal{U}^i_{B_j}$ in performing his test, we no longer require Alice have the correct outputs (or exclusions from) regions in the causal future of the accessed region. Similarly, Bob will localize the inputs A_j to regions $\mathcal{A}^i_{A_j}$ so long as Alice never interferes. She may choose to access some region $\mathcal{A}^i_{A_j}$ however and obtain A_i, in which case Bob is no longer expected to localize A_i to regions in the future of $\mathcal{A}^i_{A_j}$.

4.3 Position-based cryptography

This section is review material. Our principal sources are [18, 57].

One of the initial applications which lead to the development of quantum tasks is position-based cryptography. This application motivated better understanding the dependence of a tasks success probability on features of the geometry $\mathcal{M}$, a subject we take up in more depth in the next subsection.

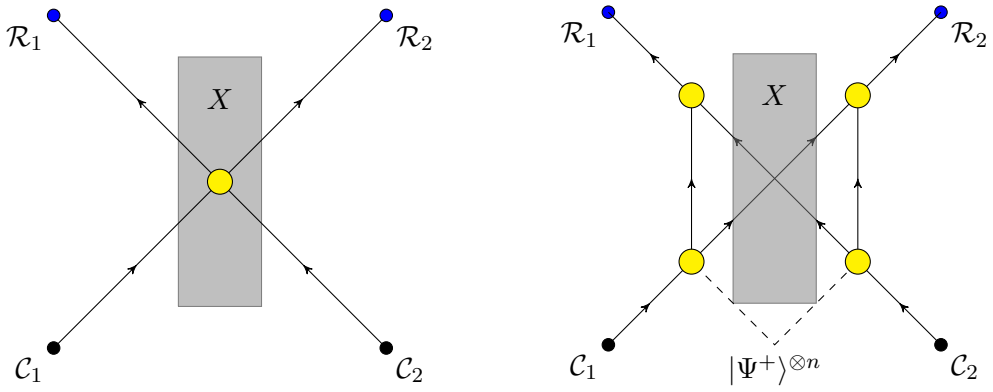


Figure 4.1: A typical set-up for position-based cryptography. By challenging Alice to complete a certain quantum task, Bob will try to verify Alice is performing quantum channels within the spacetime region X, shown in grey. An honest Alice acts as in (a), where quantum channels occur at the yellow circles. In order to cheat, Alice must complete the task using a strategy of the form shown in (b).

In position-based cryptography we consider two parties, Alice and Bob. Bob's goal is to verify that Alice can perform non-trivial quantum channels within some designated spacetime region, call it X. To do this, Bob sets up a quantum task which has inputs and outputs at regions $\mathcal{C}_i$ and $\mathcal{R}_i$ located outside of X, but chooses the task in such a way that (he hopes) Alice will be forced to act inside of X to complete it. Alice, if she is honest, acts inside of X to complete the task (see figure 4.1a). However, Alice may also try to cheat by attempting to complete the task by acting non-trivially only outside of X, and potentially sending quantum or classical signals across X (see figure 4.1b). Note that we will assume $\mathcal{C}_i \subseteq J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)$, where $J^-(\mathcal{Y})$ denotes the causal past of a region $\mathcal{Y}$. This ensures that information in $\mathcal{C}_i$ can reach either of $\mathcal{R}_1$ or $\mathcal{R}_2$.

Using the language introduced in the last section, we denote the inputs at $\mathcal{C}_1$ and $\mathcal{C}_2$ by A_1 and A_2, and the outputs required at $\mathcal{R}_1$ and $\mathcal{R}_2$ by B_1 and B_2. Bob, in an effort to force Alice to use a protocol involving a non-trivial channel applied within X, will specify some channel $\mathcal{N}_{A_1A_2\to B_1B_2}$ Alice should apply.

It is instructive to consider various possible choices of channel, and understand

if Alice is able to cheat, and if so how. To begin consider what we will call the "routing task", with inputs

$$|\psi\rangle_{A_1}, \ \ |q\rangle_{A_2} \tag{4.1}$$

where $q \in \{0, 1\}$. Alice's goal is to send $|\psi\rangle$ to region R_q.[2] The most naive strategy to complete this task would be to copy the inputs A_1 and A_2, send both to $\mathcal{R}_1$ and $\mathcal{R}_2$, then return the local copy of A_2 at the correct output. Of course, since $|\psi\rangle$ is a (unknown) quantum state this isn't possible. Nonetheless we will see below that using entanglement it is still possible to complete the task without acting non-trivially inside of the X region.

To cheat in the routing task, Alice's protocol is as follows. For simplicity we assume A_1 is a qubit, the generalization is obvious.

Protocol 5 ***(Routing task cheating strategy)***
Preparation phase:

1. *Arrange for a maximally entangled state $|\Psi^+\rangle_{F_1F_2}$ to be distributed such that F_1 is in $\mathcal{C}_1$ and F_2 is in $\mathcal{C}_2$.*

Execution phase:

1. *At $\mathcal{C}_1$, measure A_1F_1 in the Bell basis. Send the two bits of measurement outcome b_1b_2 to both $\mathcal{R}_1$ and $\mathcal{R}_2$.*
2. *At $\mathcal{R}_2$, send F_2 to $\mathcal{R}_q$.*
3. *At $\mathcal{R}_q$, apply $X^{b_1}Z^{b_2}$ to F_2, then relabel F_2 as A_2 and return it to Bob.*

To check this protocol is correct, and completes the task, we have to check 1) that each step in the protocol can be performed, in particular that the information needed for each step is available at the spacetime location that step occurs and 2) that carrying out the steps produces the correct outputs. It is straightforward to do this for the above protocol and see that it is correct.

To understand this protocol better, notice that since A_1 cannot be copied, and is located far from the information q which indicates where it should go, so Alice is unable to directly send A_1 to the correct location. Instead, she measures A_1F_1

[2] We could write this as a channel, but its not necessary.

in the Bell basis, such that F_2 is in the state $X^{b_1}Z^{b_2}|\psi\rangle$. Now the information in $|\psi\rangle$ has been effectively split into a classical part, her outcomes $b_1 b_2$, and a quantum part. The advantage gained is that the quantum part is located with q, the information about where the system needs to go. The classical part is still located far away, but it can be copied, allowing it to be sent to both possible locations.

Lets now consider a somewhat more challenging task, which we call the $\mathbf{B}_{84}$ task. The causal set-up is still as in figure 4.1. The inputs are

$$H^q|b\rangle_{A_1}, |q\rangle_{A_2} \tag{4.2}$$

where $q, b \in \{0, 1\}$ and H is the Hadamard operator[3]. As outputs, Alice should return b to both $\mathcal{R}_1$ and $\mathcal{R}_2$. Again Alice has been put into a challenging situation: without knowing which basis the state on A_1 is in, she cannot measure in a way that lets her find out b reliably. If she brings A_1 to one of $\mathcal{R}_1$ or $\mathcal{R}_2$, say $\mathcal{R}_1$, where she finds out the correct basis, she will fail to return the correct value of b at $\mathcal{R}_2$.

Nonetheless, Alice can cheat in the $\mathbf{B}_{84}$ task, again by exploiting entanglement shared between $\mathcal{C}_1$ and $\mathcal{C}_2$. The following protocol gives a cheating strategy.

Protocol 6 ***(B_{84} cheating strategy)***
Preparation phase:

1. *Arrange for a maximally entangled state $|\Psi^+\rangle_{F_1F_2}$ to be distributed such that F_1 is in $\mathcal{C}_1$ and F_2 is in $\mathcal{C}_2$.*

Execution phase:

1. *At $\mathcal{C}_1$, measure A_1F_1 in the Bell basis, producing measurement outcomes s_1, s_2.*
2. *Send s_1, s_2 to $\mathcal{R}_1$ and $\mathcal{R}_2$.*
3. *At $\mathcal{C}_2$, apply H^q to F_2. Then measure in the Z basis, producing measurement outcome s_3.*
4. *Send q, s_3 to $\mathcal{R}_1$ and $\mathcal{R}_2$.*
5. *At $\mathcal{R}_1$ and $\mathcal{R}_2$ use $(-1)^b = s_1^q s_2^{1-q} s_3$ to calculate b. Output b to Bob.*

[3]The Hadamard operator is specified by $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$.

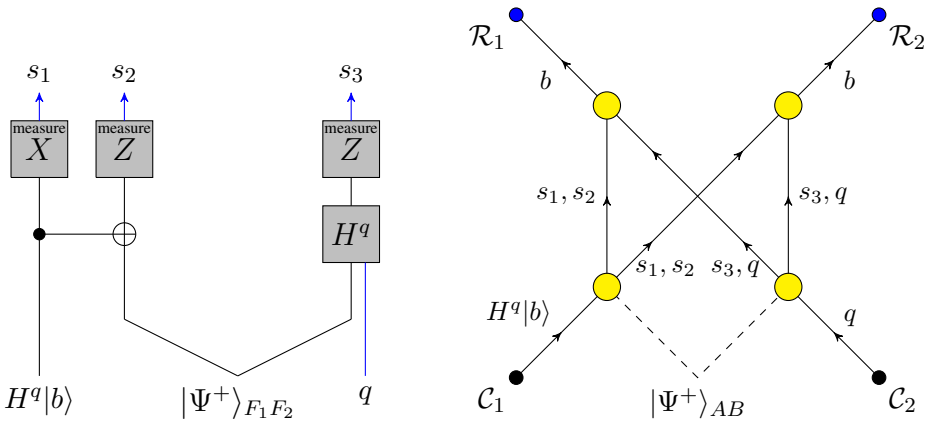


Figure 4.2: Circuit diagram that completes the $\mathbf{B}_{84}$ task. Blue lines indicate classical inputs and outputs. The protocol uses one EPR pair, $|\Psi^+\rangle_{F_1F_2} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as a resource. b is a function of the classical measurement outcomes according to $(-1)^b = s_1^q s_2^{1-q} s_3$. Importantly, the operations performed in the circuit can be placed in the nonlocal form shown in b).

The diagram shown in figure 4.2 shows the steps of this protocol. It is straightforward to verify that each step in this protocol uses only locally available information. It is also straightforward, though tedious, to directly verify that the steps in the protocol produce the correct outputs. To verify this efficiently one can use the stabilizer formalism[4].

While we have shown the routing and $\mathbf{B}_{84}$ tasks do not act as secure position-based cryptography schemes, we have not yet understood in this section if such a scheme exist. In the next section we will understand that in fact there does not exist a secure position-based cryptography scheme.

4.4 Non-local quantum computation

Note: This section is not necessary to understand the core results of this thesis presented in chapters 5 ,9, 10, and 11. It is relevant background for the discussion

[4]See [73], chapter 10 for a pedagogical review of the stabilizer formalism.

in chapter 12 however.

In the context of position-based cryptography, we have been motivated to ask if tasks which can be completed locally, as in figure 4.1a, can always be completed non-locally, as in figure 4.1b. If so, there is no secure position-based cryptography scheme.

Considering the arrangement of two input locations and two output locations in figure 4.1, it will be convenient to relabel indices $1 \to L$ and $2 \to R$, so that the input points are $\mathcal{C}_L$ and $\mathcal{C}_R$, the output points are $\mathcal{R}_L, \mathcal{R}_R$, etc.[5] In the last section we studied two simple choices of channels that define tasks on this arrangement of inputs and outputs, and found that in both cases entanglement could be used to perform these channels non-locally. More generally, we will consider a more general channel $\mathcal{N}_{A_L A_R \to B_L B_R}$ and look for a non-local strategy.

We will make a naive attempt at performing NLQC, which will illustrate the difficulty. Lets attempt to perform a unitary $U_{A_L A_R}$. Inspired by protocols 5 and 6, a natural first step is to make use of an entangled state $|\Psi^+\rangle_{F_L F_R}$ shared between $\mathcal{C}_L$ and $\mathcal{C}_R$, then measure $A_L F_L$ in the Bell basis, as if teleporting A_L to $\mathcal{C}_R$. This leads to the state $(P^i_{F_R} \otimes I)|\psi\rangle_{F_R A_R}$ held at $\mathcal{C}_R$, and the index i fixing the Pauli P^i being held at $\mathcal{C}_L$. Now, at $\mathcal{C}_R$, Alice might like to apply the desired unitary U. The trouble though is the appearance of the Pauli P^i, which, at $\mathcal{C}_R$, Alice is unable to remove.

Protocols for doing NLQC fall into two categories, based on how they handle the appearance of the P^i. The first strategy is to restrict attention to a subset of unitaries U which somehow interact with the Pauli U in a 'nice' way. In particular, the property one hopes for is that

$$UP^i = (V^i_{A_L} \otimes V^i_{A_R})U. \tag{4.3}$$

This suffices for NLQC to be accomplished, because if this is the case Alice at $\mathcal{C}_R$ can apply U, and then send A_L to $\mathcal{C}_L$ and A_R to $\mathcal{R}_R$. From $\mathcal{C}_L$, send i to both $\mathcal{R}_L$ and $\mathcal{R}_R$. At $\mathcal{C}_L$ Alice applies $V^i_{A_L}$ and at $\mathcal{C}_R$ applies $V^i_{A_R}$. The second approach to NLQC involves finding a form of teleportation such that the correction operation,

[5] Note that $\mathcal{C}_L$ sits to the left of region X, $\mathcal{C}_R$ to the right, which motivates this temporary convention.

which above was the Pauli P^i, actually commutes with all unitaries U. This is exactly what we devised when we described port-teleportation in section 2.7.

We will discuss the restricted U approach first. To define the type of unitaries we consider, first recall the definition of the Pauli group on n qubits.

Definition 16 *The Pauli group on n qubits $\mathbf{P}^n$ is defined by the generating set $\langle S_k \rangle$ where the S_i are all elements of $U(n)$ of the form*

$$S_k = P_{k_1} \otimes ... \otimes P_{k_n} \tag{4.4}$$

for $P_k \in \mathbf{P}^1$, the Pauli's on a single qubit, and $U(n)$ is the unitary group on n qubits.

Next we define the Clifford group as the normalizer of the Pauli group.

Definition 17 *The Clifford group $\mathbf{C}^{(2)}$ is defined as*

$$\mathbf{C}^{(2)} = \{X \in U(n) : XPX^\dagger \in \mathbf{P}^n\} \tag{4.5}$$

The Clifford group is a set of unitaries which satisfy 4.3, where in particular the unitaries $(V^i_{A_L} \otimes V^i_{A_R})$ are just Pauli's, and in fact are tensor product across every qubit, not just across A_L and A_R.

We can actually do a bit better than the Clifford group. Towards this we define the Clifford hierarchy.

Definition 18 *The kth level of the Clifford hierarchy is the set of unitaries*

$$\mathbf{C}^{(k)} = \{X \in U(n) : XPX^\dagger \in \mathbf{C}^{(k-1)}\} \tag{4.6}$$

Note that for $k \geq 3$ the kth level in the hierarchy is not a group. The 0th level of the hierarchy is defined to be the Pauli group, which is consistent with the way we've defined the Clifford group above. The Clifford group and Clifford hierarchy play important roles in the theory of quantum error correction and fault-tolerance [73].

Returning to non-local quantum computation, we will give a protocol for implementing unitaries in $\mathbf{C}^{(3)}$ non-locally. Our strategy assumes that Alice's agents

at $\mathcal{C}_L$ and $\mathcal{C}_R$ both know the choice of unitary, call it $U^{(3)}$, to be implemented. With this assumption, we are able to implement $U^{(3)}$ non-locally using $O(n)$ EPR pairs, where $U^{(3)}$ acts on n qubits.[6]

Call the input state $|\psi\rangle_{A_L A_R}$, and assume $\log \dim A_L = \log \dim A_R = n$.

Protocol 7 ***NLQC - Fixed unitaries in*** $\mathbf{C}_3$***:***
Preparation phase:

1. *Distribute the state* $|\Psi^+\rangle_{F_{L,1}F_{R,1}}$ *with* $\log \dim F_{L,1} = \log \dim F_{R,1} = n$ *and* $F_{L,1}$ *held on the left and* $F_{R,1}$ *held on the right.*
2. *Distribute the state* $|\Psi^+\rangle_{F_{L,2}F_{R,2}}$ *with* $\log \dim F_{L,2} = \log \dim F_{R,2} = 2n$ *and* $F_{L,2}$ *held on the left and* $F_{R,2}$ *held on the right.*

Execution phase:

1. *Measure the* $A_L F_{L,1}$ *system in the Bell basis. Then Alice holds*

$$(P_j \otimes I)|\psi\rangle_{F_{R,1}A_R} \tag{4.7}$$

   with $F_{R,1}A_R$ *on the right, and the index* j *on the left.*
2. *Apply* $U^{(3)}$ *on the right. Alice now holds*

$$U^{(3)}(P_i \otimes I)|\psi\rangle_{F_{R,1}A_R} = V_i^{(2)} U^{(3)}|\psi\rangle_{F_{R,1}A_R} \tag{4.8}$$

   on the right with $V_i^{(2)} \in \mathbf{C}^{(2)}$*, where we've used the* $U^{(3)}$ *is in* $\mathbf{C}^{(3)}$*, and the index* i *is held on the left.*
3. *Measure* $(F_{R,2})(F_{R,1}A_R)$ *in the Bell basis. Alice now holds the state*

$$P_j V_i^{(2)} U^{(3)}|\psi\rangle_{F_{L,2}} \tag{4.9}$$

   with $F_{L,2}$ *and index* i *on the left, and index* j *is held on the right.*

[6] Another possibility is to consider a setting where keys x_L and x_R are announced at $\mathcal{C}_L$ and $\mathcal{C}_R$ which fix the choice of unitary. In this setting a similar strategy to the one given here allows the unitary to be performed non-locally and using $O(n)$ EPR pairs, but only if the keys x_L, x_R specify a unitary in $\mathbf{C}^{(2)}$.

4. *Apply* $(V_i^{(2)})^\dagger$ *on the left. Alice then holds the state*

$$(V_i^{(2)})^\dagger P_j V_i^{(2)} U^{(3)} |\psi\rangle_{F_{L,2}} = P_{i,j} U^{(3)} |\psi\rangle_{F_{L,2}} \tag{4.10}$$

with system $F_{L,2}$ *and index* i *on the left, and holds index* j *on the right.*

5. *Relabel the* $2n$ *qubits composing* $F_{L,2}$ *to be* $B_L B_R$*. From* $\mathcal{C}_L$*, send* B_L *to* $\mathcal{R}_L$ *and* B_R *to* $\mathcal{R}_R$*. As well, send* i *to both* $\mathcal{R}_L$ *and* $\mathcal{R}_R$*. From* $\mathcal{C}_R$*, send* j *to both* $\mathcal{R}_L$ *and* $\mathcal{R}_R$*. Alice now holds*

$$P_{B_L}^{ij} \otimes P_{B_R}^{ij} |\psi\rangle_{B_L B_R} \tag{4.11}$$

with i, j, B_L *at* $\mathcal{R}_L$ *and* i, j, B_R *at* $\mathcal{R}_R$*.*

6. *Apply* $P_{B_L}^{ij}$ *at* $\mathcal{R}_L$ *and return* B_L *there. Apply* $P_{B_R}^{ij}$ *at* $\mathcal{R}_R$ *and return* B_R *there.*

This protocol uses $3n$ EPR pairs: n pairs to send A_L to the right, then $2n$ pairs to send the full state back to the left.

It is interesting to ask if we can use a similar strategy to perform unitaries at higher levels of the Clifford hierarchy. Indeed one can, but an exponential entanglement cost is incurred beginning at $\mathbf{C}^{(4)}$. A discussion of this is given in [19].[7]

For an arbitrary channel $\mathcal{N}_{A_L A_R \to B_L B_R}$, not necessarily a unitary in $\mathbf{C}^3$, we need a protocol which doesn't rely on any special commutation properties of the unitary to be applied. We can use the following protocol, based on port-teleportation.

Protocol 8 ***NLQC - Arbitrary channels using port-teleportation:***
Preparation phase:

1. *Distribute a maximally entangled system* $|\Psi^+\rangle_{F_R F_L}$ *consisting of* n *EPR pairs, with* F_L *sent to* $\mathcal{C}_L$ *and* F_R *to* $\mathcal{C}_R$*.*
2. *Distribute a set of* N *maximally entangled systems* $\otimes_{k=1}^N |\Psi^+\rangle_{E_{L,k} F_{R,k}}$ *consisting of* n *EPR pairs, with all* $E_{L,k}$ *sent to* $\mathcal{C}_L$ *and all* $E_{R,k}$ *to* $\mathcal{C}_R$*.*

Execution phase:

[7] This reference uses an unknown unitary, in which case the exponential cost starts already at $\mathbf{C}^{(3)}$, but otherwise the strategy is the same.

1. *At $\mathcal{C}_L$, measure $A_L F_{L,1}$ in the Bell basis, obtaining outcome i. Then Alice holds the state*

$$(P^i_{F_{R,1}} \otimes I_{A_R})|\psi\rangle_{F_{R,1}A_R} \tag{4.12}$$

   at $\mathcal{C}_R$, and the index i is held at $\mathcal{C}_L$.
2. *Perform the "pretty-good" measurement described in section 2.7, as the first step in port-teleporting $F_{R,1A_R}$ to $\mathcal{C}_L$ using the N maximally entangled pairs $|\Psi^+\rangle_{E_{L,i}E_{R,i}}$. Call the measurement outcome j. Then j is held at $\mathcal{C}_R$ and the state*

$$\Psi \approx (P^i \otimes I)|\psi\rangle_{E_{L,j}} \otimes \rho_{E_L \setminus E_{L,j}} \tag{4.13}$$

   is held at $\mathcal{C}_L$.
3. *At $\mathcal{C}_L$, apply $\mathcal{N} \circ (P^i \otimes I)$ to every subsystem $E_{L,k}$. Then Alice holds*

$$\Psi \approx \mathcal{N}(|\psi\rangle_{E_{L,j}}) \otimes \mathcal{N}^{\otimes(N-1)}(\rho_{E_L \setminus E_{L,j}}) \tag{4.14}$$

   with all E_L systems at $\mathcal{C}_L$, and j at $\mathcal{C}_R$.
4. *Relabel the $E_{L,k}$ qubits as $B_{L,k}B_{R,k}$, and send all of the $B_{L,k}$ systems to $\mathcal{R}_L$ and all of the $B_{R,k}$ systems to $\mathcal{R}_R$. Send j from $\mathcal{C}_R$ to both $\mathcal{R}_L$ and $\mathcal{R}_R$.*
5. *At $\mathcal{R}_L$ trace out all but the $B_{L,j}$ system, and return $B_{L,j}$ to Bob. Similarly at $\mathcal{R}_R$ trace out all but the $B_{R,j}$ system, and return $B_{R,j}$ to Bob.*

This completes the arbitrary channel non-locally, although the use of port-teleportation means this performs the intended channel only approximately. Using the bound 2.82 derived for port-teleportation in section 2.7, we can show that

$$||\mathcal{N} - \mathcal{N}'||_\diamond \leq \frac{2^{4n+2}}{\sqrt{N}} \tag{4.15}$$

where $\mathcal{N}$ is the intended channel, and $\mathcal{N}'$ is the applied channel. We are interested in fixing the closeness with which the channel is performed, and understanding how the entanglement required scales with n, the number of input qubits. Thus we fix $\epsilon \equiv \frac{2^{4n+2}}{\sqrt{N}}$, and find that $N = O(2^{8n+4}/\epsilon^2)$, so that an exponential number of EPR pairs are required to perform the port-teleportation protocol.

4.5 Lower bounds on mutual information for non-local quantum computation

All of the protocols discussed in the last two sections for completing quantum computations non-locally use entanglement shared between $\mathcal{C}_L$ and $\mathcal{C}_R$. This is not by accident, and in fact we can prove that entanglement is necessary to complete at least some computations non-locally. The basic strategy will be to relate the monogamy games discussed in section 3.3 to non-local computations, which will allow us to show that any strategy which does not use entanglement will have a low success probability. Then, we use some of the entropy inequality tools discussed in section 2.2 to show that any strategy which has a high probability must use a large amount of entanglement.

We discuss in particular the $\mathbf{B}_{84}$ task in detail. We've chosen this task because it is closely related to the G_{BB84} monogamy game, which was studied in detail in [93], whose results we make extensive use of. It should also be possible to prove bounds on entanglement for the routing task, though we have not done so in detail.

Recall that the $\mathbf{B}_{84}$ task has $\mathcal{C}_1$ and $\mathcal{C}_2$ as authorized regions for inputs A_1 and A_2, and $\mathcal{R}_1$ and $\mathcal{R}_2$ as authorized regions for outputs B_1 and B_2. Alice will be given a guarantee that A_1 is in one of the states $H^q|b\rangle$, and A_2 stores the classical data q. Both q and b are bits, $q, b \in \{0, 1\}$. Alice's task is to localize b to both $\mathcal{R}_1$ and $\mathcal{R}_2$.

We can also consider repeating the $\mathbf{B}_{84}$ task n times in parallel. Call this repeated task $\mathbf{B}_{84}^{\times n}$. This repeated task has inputs $A_1 = \bigotimes_{i=1}^{n} H^{q_i}|b_i\rangle$, $A_2 = \{q_i\}_i$, and required outputs $\{b_i\}_i$ at both $\mathcal{R}_1$ and $\mathcal{R}_2$. The q_i and b_i are random and independent. We will declare the task to be completed successfully if a fraction $1 - 2\epsilon$ of the n tasks are completed successfully.

We will primarily be interested in bounding the entanglement required for the non-local strategy to succeed, but it is helpful to first briefly discuss the local strategy.

Local strategy for $\mathbf{B}_{84}^{\times n}$ task

The causal features of the task in the local strategy are captured by figure 4.1a. In this case, there is a protocol which completes the task with high probability.

In particular, Alice should bring $H^q|b\rangle$ from $\mathcal{C}_1$ and q from $\mathcal{C}_2$ together inside the *scattering region*, which is the spacetime region defined by

$$J_{12\to 12} \equiv J^+(\mathcal{C}_1) \cap J^+(\mathcal{C}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \tag{4.16}$$

This is the region in the future of both $\mathcal{C}_1$ and $\mathcal{C}_2$, and in the past of both $\mathcal{R}_1$ and $\mathcal{R}_2$. Then, she applies H^q to obtain $(H^q)^2|b\rangle = |b\rangle$, measures in the computational basis to learn b, and then sends b to both $\mathcal{R}_1$ and $\mathcal{R}_2$. Assuming this can be carried out as described this completes the task with probability $p_{suc} = 1$. More physically we will allow for the presence of noise in carrying out this protocol, and say the success probability satisfies $p_{suc}(\hat{\mathbf{B}}_{84}) \geq 1 - \epsilon$.

Now consider the parallel repetition task, $\mathbf{B}_{84}^{\times n}$. Recall that we declare this task successful if a fraction $1 - 2\epsilon$ of the individual tasks are completed successfully. If each task is completed with probability $p_{suc} = 1 - \epsilon$, then this occurs with probability

$$p_{suc}(\mathbf{B}_{84}^{\times n}) = 1 - 2\epsilon^{2+n}. \tag{4.17}$$

This is the success probability for the $\mathbf{B}_{84}^{\times n}$ when a local strategy is available.

Non-local strategy for $\mathbf{B}_{84}^{\times n}$ task

In the non-local case, where no scattering region is available, we will be interested in strategies of the form shown in figure 4.1b. Recall that protocol 6 gives a concrete method for completing this task non-locally. We are interested here in the more general question of bounding the entanglement required for any non-local protocol.

To begin, recall that the protocols given above used entanglement between the regions $\mathcal{C}_1$ and $\mathcal{C}_2$. However, it suffices to have entanglement between the regions

$$\begin{aligned} \mathcal{V}_1 &= J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2), \\ \mathcal{V}_2 &= J^+(\mathcal{C}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \end{aligned} \tag{4.18}$$

This is because these are the regions in the future of one of the input regions, and

past of both output regions. Thus the steps carried out in $\mathcal{C}_1$ above can be delayed to occur in $\mathcal{V}_1$. Our earlier assumption that $\mathcal{C}_i \subseteq \mathcal{R}_1 \cap \mathcal{R}_2$ means that $\mathcal{C}_i \subseteq \mathcal{V}_i$.

We begin by assuming $I(\mathcal{V}_1 : \mathcal{V}_2) = 0$, that $\mathcal{C}_i \subseteq \mathcal{V}_i$, and considering a single instance of the task, $\mathbf{B}_{84}^{\times 1}$. We will see that this leads to a success probability bounded strictly below 1.

Lemma 9 *Consider the $\hat{\mathbf{B}}_{84}^{\times 1}$ task with $I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) = 0$. Then any strategy for completing the task has $p_{suc}(\hat{\mathbf{B}}_{84}^{\times 1}) \leq \cos^2(\pi/8)$.*

Proof. We will show that completing this task amounts to completing the monogamy game G_{BB84} discussed in section 3.3. To see this, consider that Bob can prepare the inputs for Alice in the following way.

1. Prepare a maximally entangled state $|\Psi^+\rangle_{A'_L A_L}$, and give Alice A_L at $\mathcal{C}_L$ as her input.
2. Measure A'_L in the $\{|0\rangle, |1\rangle\}$ basis if $q = 0$, and in the $\{|+\rangle, |-\rangle\}$ basis if $q = 1$. Call the outcome b.
3. Give q to Alice at $\mathcal{C}_R$.

After measuring in the second step, the post measurement state on A_L is $H^q|b\rangle$, so this prepares the correct inputs.

Now however imagine that Bob waits to measure A'_L, performing steps 1 and 3 above but holding off on performing 2. Then consider Alice's situation at $\mathcal{C}_L$. She holds one end of a maximally entangled state, with the other end held by Bob. Since she does not share entanglement with $\mathcal{C}_R$, she acts in a way independent of q. She can act on A_L and produce some output systems, call them X and Y, sending X to $\mathcal{R}_L$ and Y to $\mathcal{R}_R$. But this is exactly the preparation phase of a monogamy game, as detailed in protocol 4, where $\rho_{A'_L XY}$ is the state ρ_{ABC} described there. The question phase corresponds to Bob performing his measurement on A'_L. The data q reaching $\mathcal{R}_L$ where X is and $\mathcal{R}_R$ where Y is initiates the answer phase.

Notice that the success probability for the $\mathbf{B}_{84}$ task is actually less than or equal to the corresponding monogamy task. This is because in the monogamy task the shared state ρ_{ABC} is chosen to maximize the success probability, whereas in the $\mathbf{B}_{84}$ task this state is always of the form $\rho_{A'_L XY} = \mathcal{M}_{A'_L \to XY}(|\Psi^+\rangle_{A_L A'_L})$. From this and lemma 7, which bounds the success probability for the monogamy game,

we have

$$p_{suc}(\mathbf{B}_{84}) \leq \cos^2(\pi/8) \tag{4.19}$$

as needed. ■

Next we consider the parallel repetition of the $\mathbf{B}_{84}$ task, $\hat{\mathbf{B}}_{84}^{\times n}$, and require a fraction $1-\delta$ of the individual tasks are successful for the repeated task to be deemed successful. This is straightforwardly related to the parallel repetition of the G_{BB84} monogamy game using the same argument as we gave in the last lemma. This leads to the following lemma.

Lemma 10 *Consider the $\mathbf{B}_{84}^{\times n}$ task with $I(\mathcal{V}_1 : \mathcal{V}_2) = 0$, assume that $\mathcal{C}_i \subseteq \mathcal{V}_i$ and allow only non-local strategies. Require that a fraction $1-\delta$ of the individual $\hat{\mathbf{B}}_{84}$ tasks are successful. Then any strategy for completing the task has*

$$p_{suc}(\boldsymbol{B}_{84}^{\times n}) \leq \left(2^{h(\delta)} \cos^2\left(\frac{\pi}{8}\right)\right)^n \equiv \left(2^{h(\delta)}\beta\right)^n, \tag{4.20}$$

where $h(\delta)$ is the binary entropy function $h(\delta) \equiv -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$ and the second equality defines β.

For small enough δ we have that $2^{h(\delta)}\beta < 1$, so this gives a good bound on the success probability.

From success probability to bounds on mutual information

Note: The content in this section is original (first appearing in [63]), though is a simple combination of standard tools.

Lets suppose that we know there exists a strategy using a resource state $\rho_{\mathcal{V}_1\mathcal{V}_2}$ which completes the $\mathbf{B}_{84}$ task with probability

$$p_{suc}(\mathbf{B}_{84}, \rho_{\mathcal{V}_1\mathcal{V}_2}) \geq 1 - 2\epsilon^{2+n} \tag{4.21}$$

we've chosen this particular bound to agree with 4.17, that is, we are supposing Alice can do the task non-locally with as high of a probability as she can do it locally.

We showed above that for any resource state with zero mutual information, the success probability goes to zero like an exponential in n, according to 4.20. In particular we can note that

$$p_{suc}(\mathbf{B}_{84}, \rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}) \leq \left(2^{h(\delta)}\beta\right)^n. \tag{4.22}$$

Since an unsuccessful strategy has a small mutual information, we might expect successful strategies must have large mutual information. To show this, it is instructive to recall that the mutual information is a measure of distinguishability between $\rho_{\mathcal{V}_1\mathcal{V}_2}$ and the product of its marginals, $\rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}$. As well, we can think of the success probability of this task as a measure of distinguishability as well, as we explain below. Using this, we can find bounds on mutual information via the relationships described in section 2.2 between various measures of distinguishability. This is done in detail in the proof of the next lemma.

Lemma 11 *Suppose the $\hat{\mathbf{B}}_{84}$ task is completed with probability $p_{suc} \geq 1 - 2\epsilon^{2+n}$, using a non-local strategy with resource state $\rho_{\mathcal{V}_1\mathcal{V}_2}$. Then*

$$\frac{1}{2}I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) \geq n(-\log 2^{h(2\epsilon)}\beta) - 1 + O((\epsilon/\beta)^n). \tag{4.23}$$

Proof. We can view the success probability of the task in terms of distinguishability as follows: suppose Alice is given either $\rho_{\mathcal{V}_1\mathcal{V}_2}$ or $\rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}$, each with probability $1/2$, and not told which state she has received. By assumption, there is a protocol which completes the $\mathbf{B}_{84}^{\times n}$ task with high probability when using the state $\rho_{\mathcal{V}_1\mathcal{V}_2}$. Alice will feed her unknown state into this protocol. Then, if the protocol succeeds, she guesses that the state is $\rho_{\mathcal{V}_1\mathcal{V}_2}$. If it fails she guesses that the state is $\rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}$. This leads to a probability of distinguishing the states successfully of

$$p_{dist} = \frac{1}{2}p_{suc}(\mathbf{B}_{84}, \rho_{\mathcal{V}_1\mathcal{V}_2}) + \frac{1}{2}(1 - p_{suc}(\mathbf{B}_{84}, \rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}). \tag{4.24}$$

Recall from section 2.2, lemma 1, that the maximal success probability for distinguishing states can be written in terms of the trace distance. This leads to

$$p_{dist} \leq p_{dist}^{max} = \frac{1}{2} + \frac{1}{4}||\rho_{\mathcal{V}_1\mathcal{V}_2} - \rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2}||_1 . \tag{4.25}$$

To relate this to the mutual information, recall from lemma 3, lemma 5 and equation 2.37 that

$$\frac{1}{2}||\rho - \sigma||_1 \leq \sqrt{1 - F(\rho, \sigma)}, \tag{4.26}$$

$$-2 \log F(\rho, \sigma) \leq D(\rho||\sigma), \tag{4.27}$$

$$D(\rho_{AB}||\rho_A \otimes \rho_B) = I(A : B)_\rho. \tag{4.28}$$

Combining inequalities to lower bound the relative entropy, and hence the mutual information, in terms of success probabilities

$$I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2)_\rho \geq -2 \log[1 - |p_{suc}(\rho_{\mathcal{V}_1\mathcal{V}_2}) - p_{suc}(\rho_{\mathcal{V}_1} \otimes \rho_{\mathcal{V}_2})|^2]. \tag{4.29}$$

Finally using our bounds on success probability 4.21, 4.22 we obtain

$$\frac{1}{2} I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) \geq n(-\log 2^{h(2\epsilon)}\beta) - 1 + O((\epsilon/\beta)^n) \tag{4.30}$$

as claimed. ■

4.6 Correlation or entanglement?

Suppose that the resource state has only classical, and not quantum correlation. This means the state takes the *separable* form

$$\rho_{\mathcal{V}_1\mathcal{V}_2} = \sum_i p_i \rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}. \tag{4.31}$$

In this case, can the resource state be used to perform the $\mathbf{B}_{84}$ task with high probability?

It is straightforward to see that the answer is no. First note that the tasks success probability is necessarily convex in the input state,

$$p_{suc}(\sum_i p_i \rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}) \leq \sum_i p_i p_{suc}(\rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}). \tag{4.32}$$

We can see this must be the case operationally: on the left is Alice's success probability if she is given a probabilistic mixture of the states $\rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}$ and not told

which state she is given; on the right is her success probability if she is given the same random mixture and told which state she is given. Clearly Alice has more power in the later case. Using the above and our existing bound on the success probability for product states, we have

$$p_{suc}(\sum_i p_i \rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}) \leq \sum_i p_i p_{suc}(\rho^i_{\mathcal{V}_1} \otimes \rho^i_{\mathcal{V}_2}) \leq \beta^n \sum_i p_i = \beta^n \tag{4.33}$$

We see that the bound on success probability in lemma 10 actually applies whenever the resource state is separable.

Using that the success probability is small for any separable state, we can show that any state with large success probability is far away from a separable state.

Lemma 12 *Suppose the $\hat{\mathbf{B}}_{84}$ task is completed with probability $p_{suc} \geq 1 - 2\epsilon^{2+n}$, using a non-local strategy with $\rho_{\mathcal{V}_1\mathcal{V}_2}$. Then*

$$\min_{\sigma \in sep} D(\rho_{\mathcal{V}_1\mathcal{V}_2} || \sigma_{\mathcal{V}_1\mathcal{V}_2}) \geq n(-\log 2^{h(2\epsilon)}\beta) - 1 + O((\epsilon/\beta)^n). \tag{4.34}$$

The proof is analogous to the proof of lemma 11. The quantity appearing on the left of this inequality is known as the *relative entropy of entanglement* [95, 96].

The above bound will apply to the holographic states of CFTs in the AdS/CFT correspondence, showing that such states have a large amount of entanglement (and not just large correlation). This claim is subject however to the loophole discussed in section 9.3.

Chapter 5

Localizing and excluding quantum information

Note: The work in this chapter first appeared in [43], and covers section 2 of that publication.

In this section, we present a partial result towards the general problem of understanding which quantum tasks can be implemented in the context of quantum mechanics and special relativity. In particular we define localize-exclude tasks, and fully characterize which such tasks are possible and how to do them when they are.

5.1 The localize-exclude task

We begin by defining the localize-exclude tasks.

Definition 19 *A localize-exclude task is a quantum task where*

- *There is only one input system, call it A, which has an access structure $\mathcal{S}_A = (\{s\}, \varnothing)$, where s is a point.*
- *The channel $\mathcal{N}_{A\to B}$ is the identity.*
- *The output system is associated with an access structure $\mathcal{S}_B = (\{\mathcal{A}_1, ..., \mathcal{A}_n\}, \{\mathcal{U}_1, ..., \mathcal{U}_m\})$*

We describe a localize-exclude task using a tuple $(A, s, \{\mathcal{A}_1, ..., \mathcal{A}_n\}, \{\mathcal{U}_1, ..., \mathcal{U}_m\})$.

In the localize-exclude task, Alice is given a quantum system A which she then must move through spacetime in a way that puts A into all of the authorized regions and keeps A out of all the unauthorized regions. Thus understanding when a localize-exclude task is possible gives a very general answer to the question *how can quantum information move in spacetime?*

Answering this question is important for a number of reasons. First, it seems a reasonable first step towards answering our bigger question of how quantum information can be processed in spacetime. Second, understanding this has a number of cryptographic implications. Indeed there are relativistic bit commitment protocols [53, 54, 56, 59], which are one example[1], and we gave a proposed novel application in [43]. Third, a number of puzzles in quantum gravity concern the movement of quantum information in spacetime [77]. It seems reasonable to expect that answering the above question will provide a good general grounds from which to approach those problems. Indeed, the work we present below on quantum tasks in holography and the connected wedge theorem makes progress in this direction.

To analyze the localize-exclude task it is useful to introduce some language. We give the following definition which specifies a relation between pairs of spacetime regions.

Definition 20 *Two spacetime regions Σ_i and Σ_j are said to be **causally connected** if there is a point q_i in Σ_i and q_j in Σ_j such that there is a causal curve from q_i to q_j, or from q_j to q_i.*

We illustrate this definition in figure 5.1a. If two regions are not causally connected we say they are **causally disjoint**.

We will also need one further definition relating to spacetime geometry.

Definition 21 *Given a spacetime region Σ, the **domain of dependence** of Σ, denoted $D(\Sigma)$, is the set of all points p such that every causal curve through p must also enter Σ.*

This definition is illustrated in figure 5.1b.

[1] In fact bit commitment can be implemented using summoning tasks, of which localize-exclude tasks are a generalization.

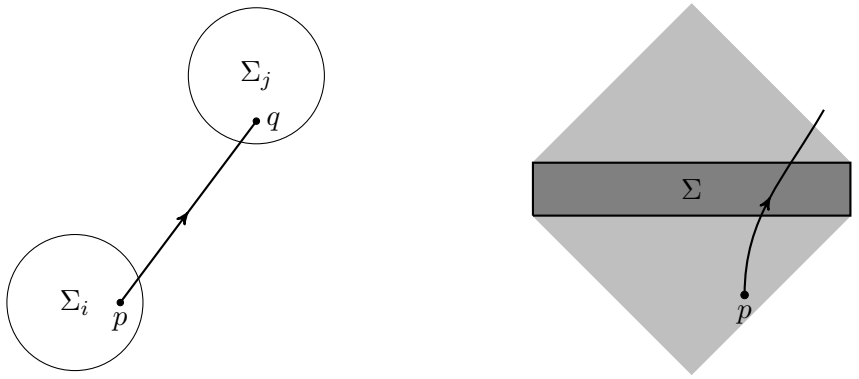


Figure 5.1: Two geometric notions used in the text. a) Two causally connected regions. Two spacetime regions Σ_i and Σ_j are said to be causally connected if there is a point q_i in Σ_i and q_j in Σ_j such that there is a causal curve from q_i to q_j, or from q_j to q_i. b) The domain of dependence (light grey) of a spacetime region Σ (dark grey). The domain of dependence is defined as the set of all points p in the spacetime such that all causal curves passing through p must also enter Σ.

5.2 Characterization of the localize task

As a first step towards the general scenario, which involves authorized as well as unauthorized regions, we will consider tasks with only authorized regions. Further, we begin by consider the localization of a quantum system to only two authorized regions $\mathscr{A}_1$ and $\mathscr{A}_2$.

Theorem 4 *Given a quantum system initially localized near a spacetime point s, the system may be localized to each of the spacetime regions $\mathscr{A}_1$ and $\mathscr{A}_2$ if and only if the following two conditions hold.*

1. *$\mathscr{A}_1$ and $\mathscr{A}_2$ both have a point in the future light cone of s.*
2. *$\mathscr{A}_1$ and $\mathscr{A}_2$ are causally connected.*

Proof. First, note that if an authorized region is entirely outside the future light cone of the start point, then successfully localizing the system to that region would constitute superluminal communication. Thus, the first condition is necessary.

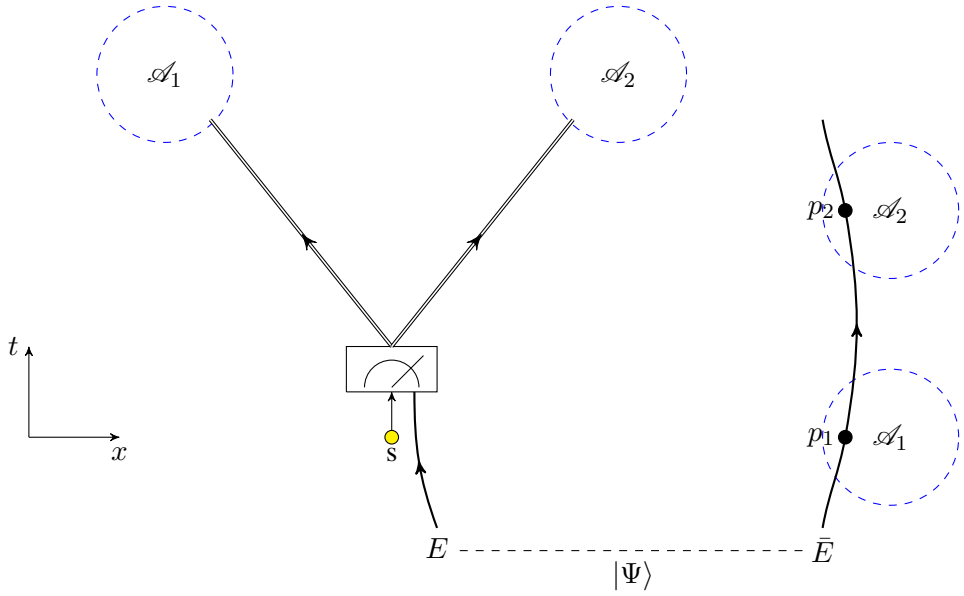


Figure 5.2: An arrangement of two authorized regions that has the minimal requirements to satisfy the conditions of theorem 4. By the first condition $\mathscr{A}_1$ and $\mathscr{A}_2$ are causally connected. This guarantees the existence of a point p_1 in $\mathscr{A}_1$ which is in the causal future of some point p_2 in $\mathscr{A}_2$ (up to relabelling). The second condition gives that each region have at least one point in the future light cone of s. However, the regions $\mathscr{A}_1$ and $\mathscr{A}_2$ may be disconnected (as shown here) and so satisfy this requirement while having the points p_1, p_2 be outside the future light cone of s. To localize a system to both regions a maximally entangled state $|\Psi\rangle_{E\bar{E}}$ is shared between s and p_1. Near to s the A system is teleported using this entanglement, and the entangled system at p_1 is sent to p_2. Meanwhile, the classical measurement outcomes from the teleportation protocol are sent to the points in $\mathscr{A}_1$ and $\mathscr{A}_2$ which are in the causal future of s. Each region has both the classical measurement outcomes and the entangled particle pass through it, so the A system is localized to each.

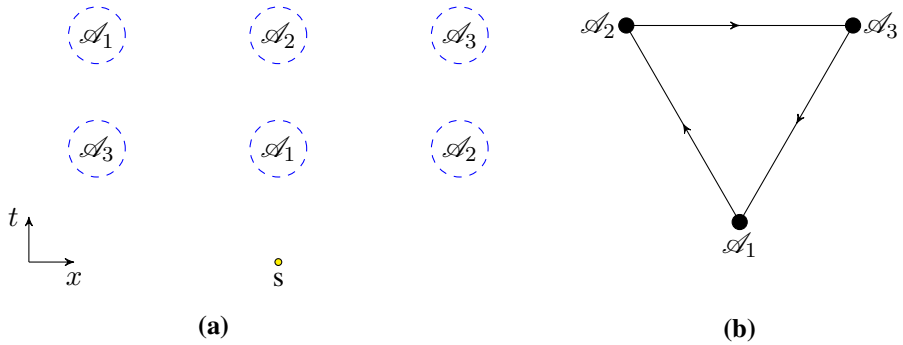


Figure 5.3: An example of a task with three authorized regions $\mathscr{A}_1, \mathscr{A}_2$ and $\mathscr{A}_3$. (a) The arrangement of the regions in spacetime, notice that each region consists of two disconnected ball-shaped regions. (b) The corresponding graph of causal connections, used in the proof of theorem 5 to construct the error-correcting code needed to complete the task.

To see necessity of the second condition suppose there exists a protocol for localizing a quantum system to two causally disjoint regions $\mathscr{A}_1$ and $\mathscr{A}_2$. Then by definition it is possible to construct the system by accessing the region $\mathscr{A}_1$, and by accessing $\mathscr{A}_2$. By causality however accessing region $\mathscr{A}_1$ cannot affect the system constructed from $\mathscr{A}_2$, and vice versa, so it would be possible to construct two copies of the quantum system. But this constitutes cloning, so no such protocol can exist.

To understand sufficiency we construct a task with the minimal properties specified by the two assumed conditions. Such a task is shown in figure 5.2. There, a point $p_1 \in \mathscr{A}_1$ is causally connected to $p_2 \in \mathscr{A}_2$, and each of $\mathscr{A}_1$ and $\mathscr{A}_2$ have a point in the future light cone of s. However, p_1 and p_2 sit outside the future light cone of s. Nonetheless it is straightforward to complete such a task. To do so, a system E is maximally entangled with $\bar{E}$, then E is brought to s while $\bar{E}$ is brought to p_1. At s, E is used to teleport the A system onto the $\bar{E}$ system. The measurement outcome from the teleportation is sent to $\mathscr{A}_1$ and $\mathscr{A}_2$ from s. Meanwhile, $\bar{E}$ is sent from p_1 to p_2. Each authorized region contains the classical measurement outcome and the system $\bar{E}$, so accessing either region allows reconstruction of A.

■

We can now move on to understanding localize tasks with arbitrary numbers of

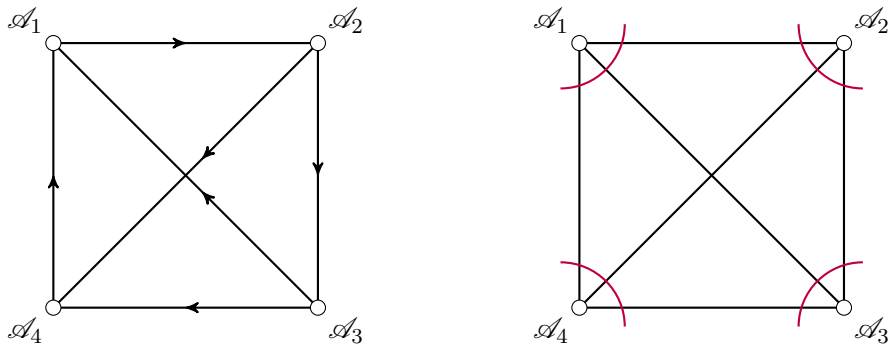
authorized regions. We find in particular that it is only the structure of causal connections between pairs of regions and the start point that are needed to characterize a task as possible or impossible.

Theorem 5 ***(Localize)*** *Given a quantum system A initially localized near a spacetime point s, the system may be localized to each spacetime region $\mathscr{A}_i$ in a collection $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$ if and only if the following two conditions hold.*

1. *Each region $\mathscr{A}_i$ has at least one point in the causal future of s*
2. *Each pair of regions $(\mathscr{A}_i, \mathscr{A}_j)$ is causally connected.*

Proof. Necessity of the two conditions follows from the same arguments as in the two region case given as theorem 4: localizing a system to a region outside of its future light cone violates no signaling, and localizing a system to two spacelike separated regions would allow two copies of the system to be produced. To demonstrate sufficiency we construct an explicit protocol for completing any task satisfying the two conditions. To this end it is useful to introduce a directed graph G which describes the causal structure of the task: for each authorized region $\mathscr{A}_i$ introduce a vertex, also labelled $\mathscr{A}_i$, to the graph. For each pair of regions $(\mathscr{A}_i, \mathscr{A}_j)$ such that there is a point in $\mathscr{A}_j$ connected by a causal curve to a point in $\mathscr{A}_i$ introduce a directed edge $(\mathscr{A}_i \to \mathscr{A}_j)$. An example of a task and its associated graph is given as figure 5.3.

From the no-cloning theorem it follows that some quantum information must be shared between every pair of authorized regions. In our construction, these quantum systems that move between pairs of authorized regions form the shares of an error-correcting code. In particular, for each edge in the graph G we associate one share. In theorem 4 and figure 5.2 we showed how to localize a quantum system to two authorized regions whenever they share a causal connection. We can execute this protocol on the shares of our error-correcting code to ensure the share associated to edge $\mathscr{A}_i \to \mathscr{A}_j$ is localized to both $\mathscr{A}_i$ and $\mathscr{A}_j$. To complete the task then, our error-correcting code should have the property that, given any vertex, the set of shares associated to the edges attached to that vertex are sufficient to construct the initial system A. We illustrate the requirement on this code in figure 5.4.



(a) **(b)**

Figure 5.4: Illustration of the error-correcting code used in theorem 5. a) A directed graph that describes the causal connections between the authorized regions of a localize task. In this case the task involves four authorized regions. b) To complete the task, we employ an error-correcting code that associates a share to each edge in the corresponding undirected graph. The encoded qubit can be reconstructed from the shares associated with the edges attached to any one vertex, corresponding to the sets of edges crossed by the purple arcs. For a single logical qubit, the shares on each edge consist of two qubits. A detailed construction of the code can be found in [42], and a more efficient version using only one qubit per edge in [100]. For infinite dimensional versions see [45].

In fact, given that every pair of vertices in this graph share an edge, which is guaranteed by condition (2), such error-correcting codes have already been constructed. To encode finite-dimensional quantum systems we constructed such codes using the codeword-stabilized formalism in the context of a similar summoning problem [42]. Constructions for continuous variable systems have also been given [45] and then adapted to the finite-dimensional case [100]. In the code-word stabilized construction a single logical qubit is recorded using 2 physical qubits for each edge in the graph, resulting in a total of $2\binom{n}{2}$ physical qubits for n the number of authorized regions. ■

This result is particularly simple and expected from earlier work on summoning, see [42].

5.3 Characterization of the localize-exclude task

Now that we have an understanding of when and how a quantum system can be localized to many spacetime regions, we can approach the localize-exclude task, where unauthorized regions are included.

As an initial approach to understanding the localize-exclude task we can list the most basic restrictions that we expect to apply. First, the two restrictions occurring in the context of the localize task are still relevant: the start point should have a point from each authorized region in its future light cone, and there should be no causally disjoint pairs of authorized regions. There are also additional restrictions relating to the unauthorized regions however. In particular, we can never have an authorized region $\mathscr{A}_i$ be contained in the domain of dependence of an unauthorized region $\mathscr{U}_j$, since then all information which enters $\mathscr{A}_i$ also enters $\mathscr{U}_j$. Finally, the start point too should not be contained in the domain of dependence of any unauthorized region. We illustrate each these conditions in figure 5.5. Remarkably, a localize-exclude task $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ will turn out to be possible to complete so long as none of the four situations in figure 5.5 occur.

As a warm-up to the general case, consider the example given in figure 5.6. There, a single unauthorized region blocks the path between two authorized ones. To complete this use the following protocol. Near the start point, A is encoded using the one-time pad using a classical key k. Once encoded, the A system is sent through both authorized regions by allowing it to pass through the unauthorized region. An access to the unauthorized region then only sees the maximally mixed state. The classical key k is also sent to both authorized regions, but along trajectories that avoid the unauthorized one.

A similar technique can be applied to the general case of many authorized and many unauthorized regions. As we show in the proof of theorem 6 given below, the strategy is to first encode the A system into an error-correcting code so that it can be localized to each authorized region. Then each share in that error-correcting code is encoded using a classical string and the quantum one-time pad. We then leverage classical secret sharing to allow us to get the encoding string to the needed authorized regions while avoiding all the unauthorized regions.

We are now ready to state theorem 6 and give the proof. The proof of suffi-

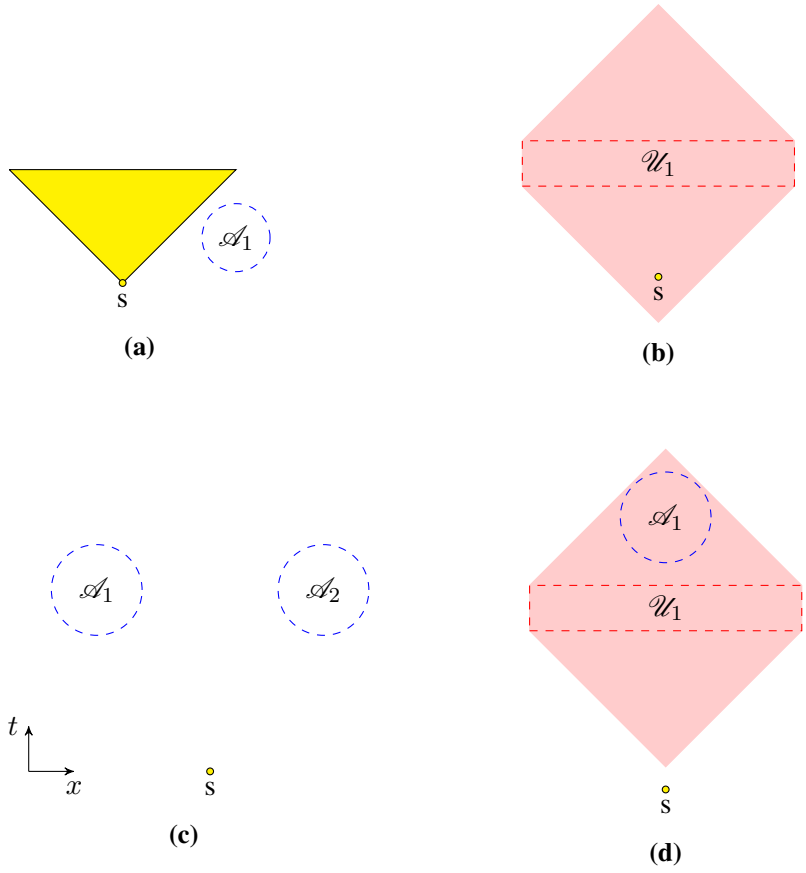


Figure 5.5: Four impossible localize-exclude tasks: (a) An authorized region is entirely outside the future light cone of s, so system A can't be localized there without violating the no-signalling principle. (b) The initial location of the quantum system is in the domain of dependence of an unauthorized region $\mathscr{U}_1$, so can be reconstructed from data in $\mathscr{U}_1$. (c) A quantum system cannot be localized to both the spacetime regions $\mathscr{A}_1$ and $\mathscr{A}_2$, due to the no-cloning theorem. (d) A quantum system cannot be localized to $\mathscr{A}_1$ without passing through the region $\mathscr{U}_1$, since there is no causal curve which passes through $\mathscr{A}_1$ and not $\mathscr{U}_1$. The red shaded region indicates the domain of dependence of the unauthorized region $\mathscr{U}_1$. The yellow shading indicates the future light cone of the start point.

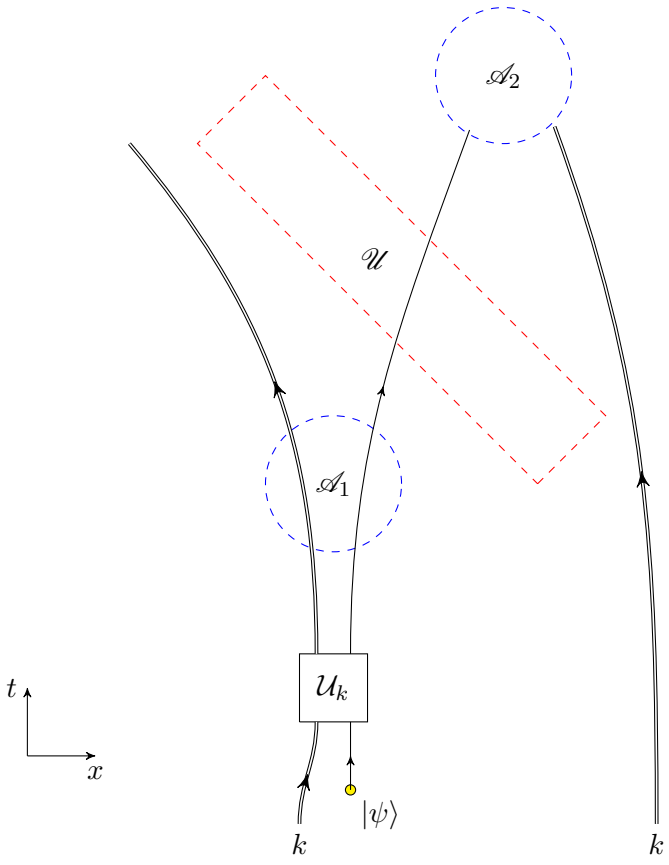


Figure 5.6: Illustration of the protocol for completing a localize-exclude task with two authorized regions and one unauthorized region that satisfies the conditions of theorem 6. In the distant past, Alice prepares copies of the classical string k. She brings one copy of k to each of $\mathscr{A}_1$ and $\mathscr{A}_2$ along a path which does not cross $\mathscr{U}$ — this is always possible by condition (3). She must also bring the classical string to the start point s, and encode the A system using the quantum one-time pad [9]. The overall state on A and it's purifying system R is then $(\mathcal{U}_k \otimes \mathcal{I})|\Psi\rangle_{AR}$. The encoded system A is sent through both authorized regions. Following this protocol both authorized regions contain k and the encoded A system, while the unauthorized region contains the encoded system only.

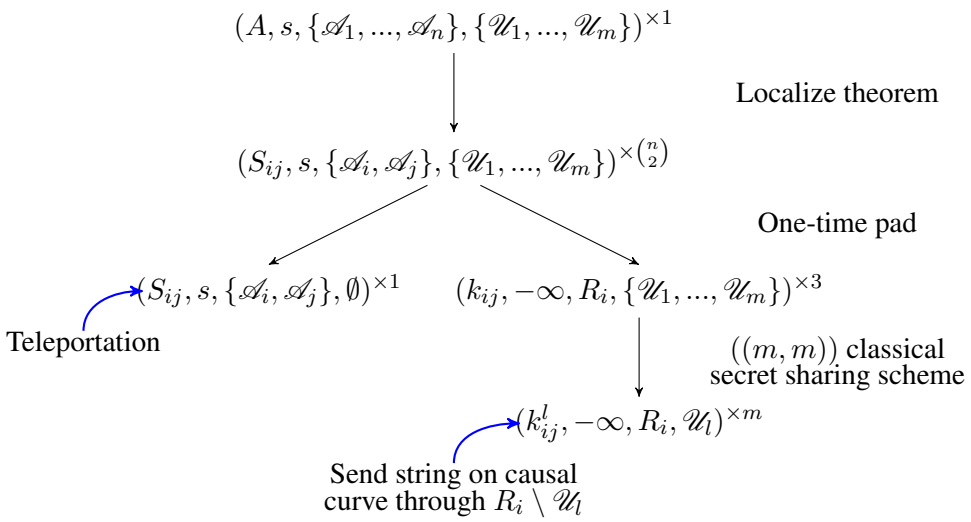


Figure 5.7: The sufficiency proof of theorem 6. In three steps, the proof reduces completing the localization task on the system A with n authorized sets and m unauthorized sets, denoted by $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, to completing $\binom{n}{2}$ instances of $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ on quantum shares, and $3m\binom{n}{2}$ instances of $(k^l_{ij}, -\infty, R_i, \mathscr{U}_l)$ on classical shares, where the region R_i may be either the start point or an authorized region. The notation $-\infty$ indicates the share is available at early times. The first step in the protocol is to recycle the error-correcting code from theorem 5 to encode the A system into shares S_{ij}. At the second step, the one-time pad is applied to each of the S_{ij}. This allows the unauthorized regions to be avoided by introducing additional classical shares, but without the need for further uses of quantum error-correcting codes.

ciency is somewhat lengthy, so we have provided figure 5.7 which summarizes the key steps taken.

Theorem 6 ***(Localize-exclude)*** *Given a collection of authorized regions $\{\mathscr{A}_1, ..., \mathscr{A}_n\}$, unauthorized regions $\{\mathscr{U}_1, ..., \mathscr{U}_m\}$, and start point s, a localize-exclude task is possible if and only if the following three conditions are satisfied.*

1. *The starting location of the system A (a) has at least one point from each authorized region in its causal future, and (b) is not in the domain of depen-*

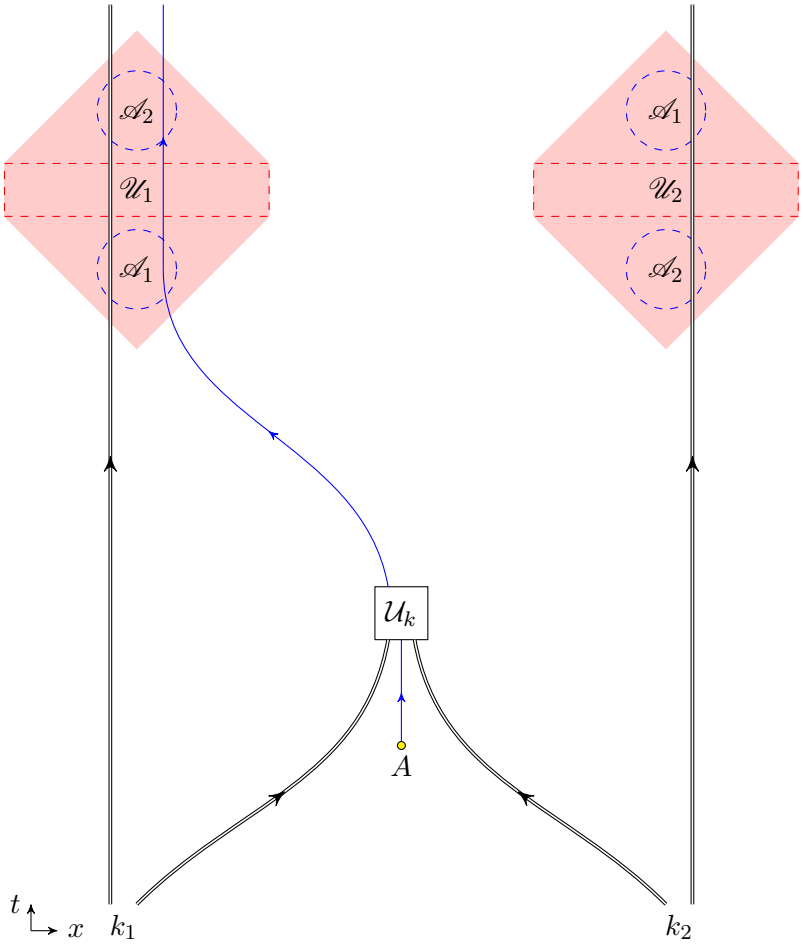


Figure 5.8: An example of a localize-exclude task and illustration of the protocol provided by theorem 6 for its completion. Near the start point the system A is encoded using the quantum one-time pad and sent (along the blue curve) through both authorized regions. The string k satisfies $k = k_1 \oplus k_2$, so that k_1, k_2 form the two shares of a $((2, 2))$ secret sharing scheme. k_1 is sent through $\mathscr{A}_1$ and $\mathscr{A}_2$ while avoiding $\mathscr{U}_1$, while k_2 is sent through $\mathscr{A}_1$ and $\mathscr{A}_2$ while avoiding $\mathscr{U}_2$. Consequently, each $\mathscr{A}_i$ contains all of the classical shares k_i along with the encoded A system, while each $\mathscr{U}_i$ is missing one k_i.

dence of any unauthorized region.

2. *Every pair of authorized regions $(\mathscr{A}_i, \mathscr{A}_j)$ are causally connected.*
3. *For every pair $(\mathscr{A}_i, \mathscr{U}_j)$ of authorized and unauthorized regions, $\mathscr{A}_i$ is not contained in the domain of dependence of $\mathscr{U}_j$.*

Proof. The necessity of conditions $(1)(a)$ and (2) follow from the same arguments as in theorem 5. To argue the necessity of condition (3), notice that if $\mathscr{A}_i$ is contained in the domain of dependence of $\mathscr{U}_j$, then the state of the quantum fields within $\mathscr{A}_j$ is determined by unitary evolution from the fields within $\mathscr{U}_i$. Then whenever the A system can be determined from $\mathscr{A}_i$ it is also possible to recover it from $\mathscr{U}_j$. Condition $(1)(b)$ is necessary for the same reason.

To demonstrate sufficiency we construct an explicit protocol to complete the task in the case where all three conditions are true. It is useful to recall the notation $(A, s, \{\mathscr{A}_1, ..., \mathscr{A}_n\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, which describes a localize-exclude task by specifying the system on which we must complete the task, the start point, authorized regions, and unauthorized regions. As a first step in constructing our protocol, we encode the system A into the error-correcting code used in theorem 5. Using this code and localizing each share in the code to its two associated authorized regions would localize the system to each authorized region. However, here we also need to exclude the system from all of the unauthorized regions. To do this, we will localize each share S_{ij} to $\mathscr{A}_i$ and $\mathscr{A}_j$ while also avoiding every unauthorized region. In other words, encoding A into the codeword stabilized code reduces completing the original task to completing the tasks $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ for every share S_{ij}.

By using the quantum one-time pad and classical secret sharing it is possible to further reduce completing the $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ task. In particular, at s use the quantum one-time pad to encode the share S_{ij} using some classical string k_{ij}. We may freely send the encoded share through $\mathscr{A}_i$ and $\mathscr{A}_j$ so long as the classical string k_{ij} is kept out of all of the unauthorized regions, and is made available at s, $\mathscr{A}_i$, and $\mathscr{A}_j$. Thus, the task $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ is equivalent to completing $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ along with $(k_{ij}, -\infty, \{s, \mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$[2].

[2]We've introduced the notation $-\infty$ to indicate the start point is located in the distant past. This is the appropriate task to consider completing on the classical system k_{ij} as Alice may prepare these strings at some early time.

To finish the protocol, we first notice that theorem 5 shows that we can complete any task of the form $(S_{ij}, s, \{\mathscr{A}_i, \mathscr{A}_j\}, \emptyset)$ given that conditions $(1)(a)$ and (2) hold. The task $(k_{ij}, -\infty, \{s, \mathscr{A}_i, \mathscr{A}_j\}, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$ is also easily handled. Note that since the task is to be completed on a classical string, we can produce three copies of k_{ij} and worry separately about sending the string to s and each of $\mathscr{A}_i$ and $\mathscr{A}_j$, so we have to complete three instances of $(k_{ij}, -\infty, R, \{\mathscr{U}_1, ..., \mathscr{U}_m\})$, where R can be s, $\mathscr{A}_i$ or $\mathscr{A}_j$. To complete these, encode k_{ij} into an $((m, m))$ secret sharing scheme[3] with shares k^l_{ij}. Then complete the tasks $(k^l_{ij}, -\infty, R, \mathscr{U}_l)$. This completes the task with all m unauthorized regions since the classical string is kept out of $\mathscr{U}_l$ so long as at least one of the shares in the $((m, m))$ scheme is.

It remains to complete the tasks of the form $(k^l_{ij}, -\infty, R, \mathscr{U}_l)$. When R is one of the authorized sets, condition (3) guarantees that R is not in the domain of dependence of $\mathscr{U}_l$, which means there is a causal curve passing through R which does not enter $\mathscr{U}_l$. To complete the task, simply send k^l_{ij} along this curve. When R is the start point s, condition $(1)(b)$ guarantees there is a causal curve passing through s and not $\mathscr{U}_l$, so again we can complete this task. ■

An example implementation of the protocol used in this proof is given as figure 5.8.

Earlier we mentioned the similarity of conditions (2) and (3) to corresponding conditions for quantum secret sharing. A quantum secret sharing scheme [39] is specified by an access structure, with the access structure consisting of subsets of parties deemed authorized and subsets deemed unauthorized. Recall from section 3.1 that a quantum secret sharing scheme can be constructed under two conditions [39]: (a) (no-cloning) no two authorized sets can be disjoint and (b) (monotonicity) no authorized set can be contained within an unauthorized set. Conditions (2) and (3) of the localize-exclude theorem are exactly these conditions rephrased in a context appropriate to spacetime.

Beyond this similarity, we can embed any secret sharing scheme into a localize-exclude task. Consider n parties, Bob_1,...,Bob_n, who each can potentially access an associated spacetime region Σ_i. Take the authorized and unauthorized regions

[3] A $((k, n))$ secret sharing scheme is one where any k of the n total shares can be used to reconstruct the secret while any $k-1$ shares reveal nothing about the secret. A $((m, m))$ scheme is the appropriate one here because we want every share to be needed to reconstruct k_{ij}.

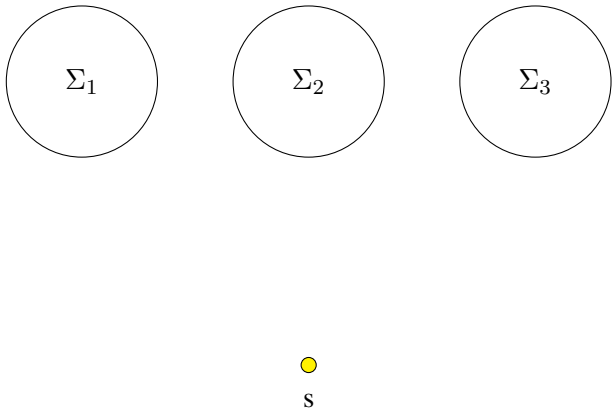


Figure 5.9: Example of the embedding of a secret sharing scheme with arbitrary access structure into a localize-exclude task. We consider a secret sharing scheme that involves three parties, and has authorized sets $S_1 = \{1, 2\}$, $S_2 = \{2, 3\}$ and $S_3 = \{1, 2, 3\}$, with all other subsets of parties deemed unauthorized. In the corresponding localize-exclude task, the three parties become three causally disjoint spacetime regions Σ_1, Σ_2 and Σ_3. Further, this localize-exclude task has authorized regions $\mathscr{A}_1 = \Sigma_1 \cup \Sigma_2$, $\mathscr{A}_2 = \Sigma_2 \cup \Sigma_3$ and $\mathscr{A}_3 = \Sigma_1 \cup \Sigma_2 \cup \Sigma_3$. The start point s has been placed at an early enough time that all the Σ_i are in its future light cone.

to consist of unions of Σ_i's, so that a full authorized region $\mathscr{A}_i$ can be accessed only if some collection of Bobs agree to cooperate. Choose the regions Σ_i to be all causally disjoint. In this setting two authorized regions being causally connected occurs if and only if they share a Σ_i. Then condition (2) of theorem 6, which requires causal connections between authorized regions, reduces to the requirement that every pair of authorized regions share at least one Σ_i. This is exactly the no-cloning requirement on secret sharing. Further, condition (3) reduces to no $\mathscr{U}_i = \Sigma_{i1} \cup ... \cup \Sigma_{in}$ containing as a subset some $\mathscr{A}_j = \Sigma_{j1} \cup ... \cup \Sigma_{j2}$ under the same restriction of having causally disjoint Σ_i, which is just the monotonicity condition. Finally, to embed our quantum secret sharing task into a localize-exclude task we should ensure that condition (1) becomes trivial, which we can do by sending the start point s to an early time. We illustrate the embedding of a secret sharing task into a localize-exclude task in figure 5.9.

Theorem 6 shows that completing a localize-exclude task with unauthorized regions requires only the same quantum error-correcting code as used in the case with no unauthorized regions. Hiding the system from the unauthorized regions can be accomplished using only the quantum one-time pad and classical secret sharing. This is similar to the approach taken in [51], where quantum error-correcting codes are combined with the quantum one-time pad to yield quantum secret sharing schemes. By using the efficient error-correcting code underlying our protocol however, we arrive at a particularly efficient construction of quantum secret sharing schemes. In particular we find that there is a universal quantum error-correcting code with $2\binom{n}{2}$ shares for n the number of authorized sets which, along with uses of the one-time pad and classical secret sharing, constructs quantum secret sharing schemes with arbitrary access structures. Using Shamir's method [87], the $3m\binom{n}{2}$ instances of the $((m, m))$ secret sharing scheme will each require $O(m \log m)$ bits, where m was the number of unauthorized sets. In total, $O(n^2)$ qubits and $O(m^2 n^2 \log m)$ classical bits are used in the construction. This provides the first construction of quantum secret sharing schemes using a number of qubits polynomial in the number of authorized sets. Previously, efficient constructions were known for threshold schemes and certain other special access structures. (See, *e.g.* [51, 61, 84].) Since the number of unauthorized sets can grow exponentially with n, the classical bits used can be exponentially large. This is to be expected since it is conjectured to be impossible to construct classical secret sharing schemes for arbitrary access structures without consuming exponential resources [14].

Chapter 6

Gravitation

Note: This chapter reviews standard material in general relativity, see for example [31] for a detailed discussion of AdS space, and [76] for the focusing theorem.. The discussion of the focusing theorem follows the approach of [67, 70] however, which emphasizes the role of Stokes theorem.

As we begin discussing in chapter 8, reasoning about quantum tasks leads to geometric consequences for the AdS/CFT correspondence. In this chapter we lay the groundwork for understanding those statements. First, we review anti-de Sitter space, which our theorems will apply to. Second, we review the focusing theorem, from which we can actually prove these theorems geometrically, independent of the tasks argument.

6.1 Anti-de Sitter space

We will be interested in asymptotically Anti-de sitter spacetimes, and in some cases these spacetimes will feature end-of-the-world (ETW) branes, which are locations where the spacetime ends in some way.

We begin with the action

$$I_{\text{bulk}} + I_{\text{brane}} = \frac{1}{16\pi G_N}\int d^{d+1}x\,\sqrt{g}(R - 2\Lambda + L_{\text{matter}}) + \frac{1}{8\pi G_N}\int_{\mathcal{B}} d^d y\,\sqrt{h}(K + L^{\mathcal{B}}_{\text{matter}})\ . \tag{6.1}$$

This action leads to Einsteins equations,

$$G_{\mu\nu} + \Lambda g_{\mu\nu} = 8\pi G\, T_{\mu\nu}, \tag{6.2}$$

along with a boundary condition at the location of the ETW brane,

$$K_{ab} - K h_{ab} = -8\pi G_N T^{\mathcal{B}}_{ab}\ . \tag{6.3}$$

The brane stress tensor $T^{\mathcal{B}}_{ab}$ is found by varying the brane matter Lagrangian with respect to the metric. We will first of all discuss solutions to Einstein's equations 6.2, and then consider solutions which feature an ETW brane and solve additionally the boundary condition 6.3.

Anti-de Sitter space

Anti-de Sitter (AdS) space is a solution to the vacuum Einstein equations 6.2 with a negative cosmological constant. We usually reparameterize the constant Λ in terms of what is called the AdS radius ℓ_{AdS}. The relation between the two is

$$\Lambda = -\frac{d(d-1)}{2\ell_{AdS}} \tag{6.4}$$

when working in AdS with total dimension $d+1$.

A convenient description of AdS is as a hyperbola sitting in a higher dimensional space with two time directions. Specifically, global AdS is the surface in $\mathbb{R}^{d+2}$ with signature $(-,-,+,...,+)$ defined by

$$-X_{-1}^2 - X_0^2 + \sum_{i=0}^{d} X_i^2 = -\ell_{AdS}^2. \tag{6.5}$$

Different coordinate systems for AdS correspond to different parameterizations of this surface. We set $\ell_{AdS} = 1$ for convenience.

In this thesis we will usually use AdS_{2+1} as our explicit example. For concreteness, we can write down a few coordinate systems that describe this spacetime. For instance, using the parameterization

$$\begin{aligned} X_{-1} &= \cosh\rho\cos\hat{t}, \\ X_0 &= \cosh\rho\sin\hat{t}, \\ X_1 &= \sin\phi\sinh\rho, \\ X_2 &= \cos\phi\sinh\rho, \end{aligned}$$

we obtain global coordinates

$$ds^2_{2+1} = -\cosh^2\rho\, d\hat{t} + d\rho^2 + \sinh^2\rho\, d\phi^2 \ . \tag{6.6}$$

In the context of AdS/CFT, we are interested in the conformal boundary of AdS space, which is where the dual CFT description will live. To find the conformal boundary, we take fixed, large ρ in the above metric

$$ds^2_b = \frac{e^\rho}{2}(-dt^2 + d\phi^2) \propto (-dt^2 + d\phi^2). \tag{6.7}$$

Thus the conformal boundary is $S^1 \times \mathbb{R}$. Global AdS_{2+1} is depicted in figure 6.1.

A second set of coordinates we will make use of is the Poincaré parameterization,

$$\begin{aligned} X_{-1} &= \frac{1}{2z}(z^2 + x^2 - t^2 + 1), \\ X_0 &= \frac{t}{z}, \\ X_1 &= \frac{1}{2z}(z^2 + x^2 - t^2 - 1), \\ X_2 &= \frac{x}{z} \end{aligned} \tag{6.8}$$

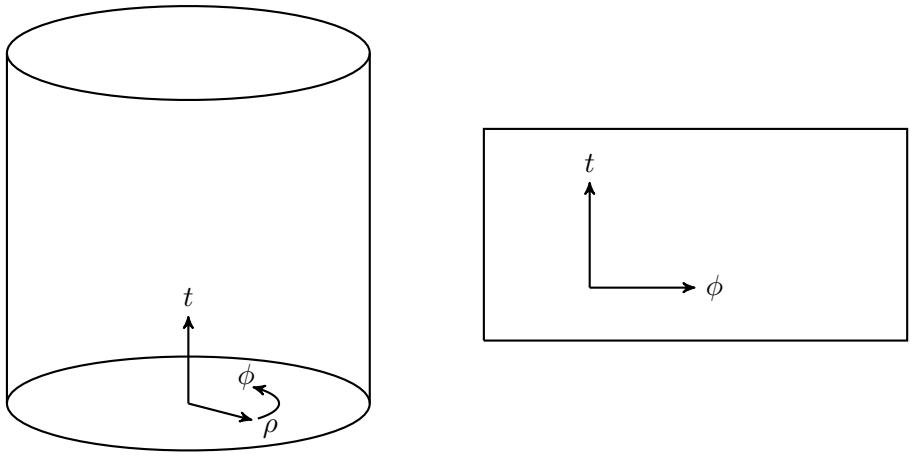


Figure 6.1: (a) Global AdS_{2+1}, described by metric 6.6. (b) The conformal boundary of global AdS_{2+1}. The left and right boundaries of the strip are identified.

which leads to a metric

$$ds^2_{d+1} = \frac{1}{z^2}(-dt^2 + dx^2 + dz^2) \ . \tag{6.9}$$

Poincaré coordinates cover only a portion of the full hyperbola 6.5, whereas the global coordinates above cover the entire spacetime. This is illustrated in figure 6.2.

The metrics given above describe pure AdS, which has no matter present. We can also consider a more general class called asymptotically AdS spacetimes. These may feature matter, but the matter content occupies a finite region of spacetime, and decays away from that region. Far away from the matter then the metric can be put into the form 6.6.

AdS spacetimes with ETW branes

In chapter 11 we will be interested in AdS spacetimes that feature ETW branes. We briefly described an example of such a spacetime in this section. Note that the ETW brane will extend to the AdS boundary; where the ETW brane reaches the

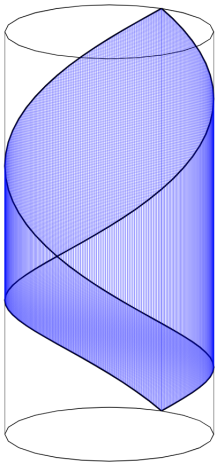


Figure 6.2: The Poincaré patch is shown in blue. It consists of a portion of global AdS. The boundary geometry is $1+1$ dimensional flat space.

AdS boundary we will refer to as the *edge*.

Consider the parameterization of AdS,

$$X_{-1} = \cosh\rho\, \cosh r \cos\nu, \tag{6.10}$$

$$X_0 = \cosh\rho\, \cosh r \sin\nu, \tag{6.11}$$

$$X_1 = \sinh\rho, \tag{6.12}$$

$$X_2 = \cosh\rho \sinh r, \tag{6.13}$$

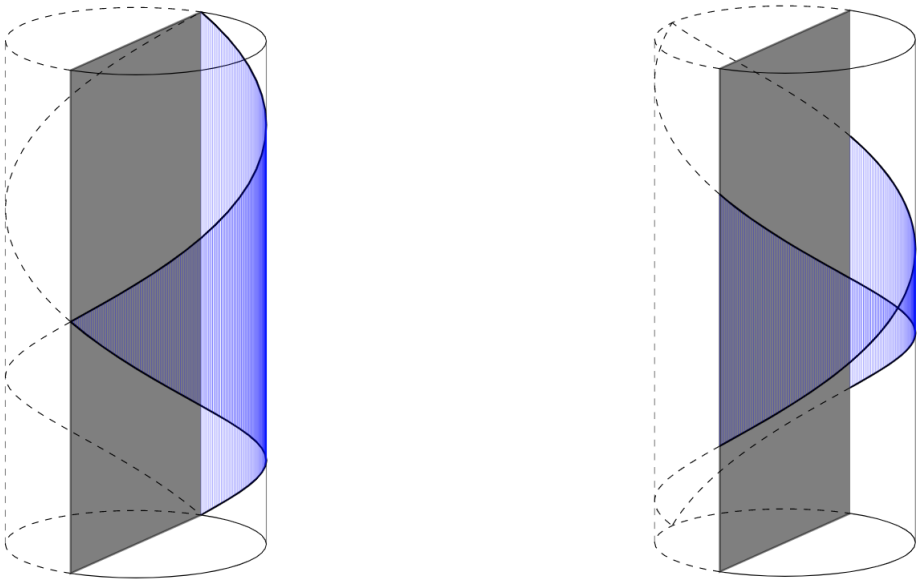
which leads to the "slicing" coordinates

$$ds^2_{d+1} = \cosh^2\rho\, \left(-\cosh^2 r d\nu^2 + dr^2\right) + d\rho^2\ , \tag{6.14}$$

$$= \cosh^2\rho\, ds^2_{1+1} + d\rho^2 \tag{6.15}$$

where the line element ds^2_{1+1} is for a $1+1$ dimensional global AdS space. To cover the full AdS spacetime the coordinate ρ has range $(-\infty, +\infty)$. We can also consider spacetimes that end at $\rho = \rho_0$. A straightforward calculation shows that

$$K_{ab} - K h_{ab} = -\tanh\rho_0 h_{ab}. \tag{6.16}$$



(a) **(b)**

Figure 6.3: Global AdS_{2+1} with an ETW brane. We've shown the $T = 0$ case for simplicity. Poincaré patches are shaded in blue. (a) An edge centered choice of Poinaré patch. In the associated Poincaré solution the ETW brane is flat, described by equation 6.19. (b) A Poincaré patch centered at $\sigma = 0$. In Poincaré coordinates the brane trajectory is a hyperbola, described by equation 6.20.

Thus we can solve the boundary condition 6.3 if we choose

$$L^B_{\text{matter}} = -\frac{1}{8\pi G_N}\int d^d y\,\sqrt{h}T. \tag{6.17}$$

and set $T = \tanh\rho_0$. Such a solution is illustrated in figure 6.3a.

The slicing coordinates are convenient in that the brane's embedding equation has the simple form $\rho = \rho_0$. We may also be interested in viewing this solution in other coordinates, for instance in Poincaré. In fact, because the Poincaré coordinates cover only a patch the global spacetime, there are different ways to view the brane in Poincaré space. Two choices are shown in figure 6.3.

In figure 6.3a, the Poincaré patch is chosen to be centered on one of the edges.

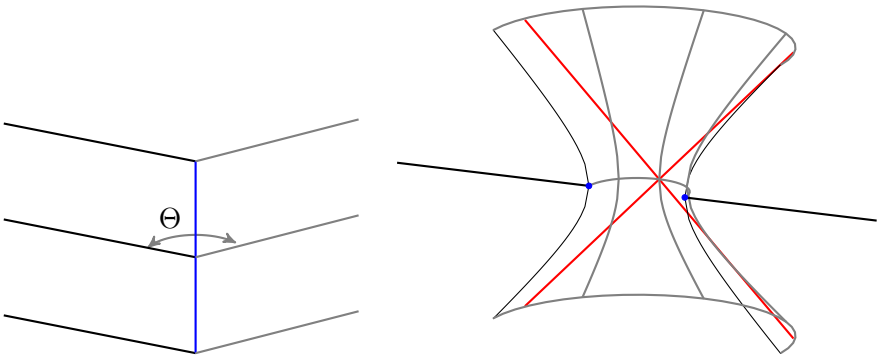


Figure 6.4: (a) Poincaré-AdS$_{2+1}$ with a constant tension ETW brane, as obtained by taking an edge-centered patch of the global spacetime, as shown in figure 6.3b. (b) Poincaré-AdS$_{2+1}$ with a constant tension ETW brane, as obtained by taking a patch as shown in figure 6.3a. The brane forms a hyperbola, and the two edge trajectories are $x = \pm\sqrt{1+t^2}$. The horizons $\sigma = \pm\nu$ chosen in the global geometry map to $x = \pm t$, $z = (1 - \sin\Theta)/\cos\Theta$ in Poincaré coordinates, which we've shown in red.

The associated Poincaré coordinates are related to slicing coordinates by

$$t = \frac{\sin\nu}{\cos\nu - \sin\sigma}, \quad x = \frac{\cos\sigma\tanh\rho}{\cos\nu - \sin\sigma}, \quad z = \frac{\cos\sigma\mathrm{sech}\rho}{\cos\nu - \sin\sigma}. \tag{6.18}$$

Under this transformation the boundary becomes the half line $x > 0$, with one edge located at $x = 0$. The other edge is at $x = \infty$. The ETW branes trajectory is

$$\frac{x}{z} = \sin\Theta, \tag{6.19}$$

where Θ is related to the tension T by $T = \tan\Theta$. Solutions of this form are shown in figure 6.4a.

The second Poincaré patch we will be interested in is centered at $\sigma = 0$, as shown in figure 6.3b. The choice of Poincaré patch implicit in equation 6.8 actually corresponds to this choice, so we can compare 6.8 and 6.10 to find the brane

equation in these Poincaré coordinates,

$$x^2 - t^2 + (z + \tan\Theta)^2 = \sec^2\Theta. \tag{6.20}$$

The edge trajectories are described by $t = \pm\sqrt{x^2 - 1}$. This solution was studied in [81] in the context of brane models of black holes and island formation, which we will also take up in section 11. A solution of this type is shown in figure 6.4b.

6.2 The area theorem

In this section we review the area theorem, which gives that the areas of certain null congruences decrease as we move along the null geodesics. The area theorem in various forms plays an important role in general relativity, for instance it is how Hawking proved that the area of a black hole always increases (at least classically).

Consider a null codimension 1 surface $\mathcal{N}$. We assume $\mathcal{N}$ is foliated by null geodesics γ^μ which start on a spacelike codimension two surface Σ_1, and end on another spacelike codimension two surface Σ_2. Call the affine parameter along the null geodesics λ, which we scale so that $\lambda = 0$ on Σ_1 and $\lambda = 1$ on Σ_2. Then, using the fundamental theorem of calculus,

$$A(\Sigma_2) - A(\Sigma_1) = \int dY\sqrt{h}_{\lambda=0} - \int dY\sqrt{h}_{\lambda=1} = \int_0^1 d\lambda \int dY\,\partial_\lambda\sqrt{h} \tag{6.21}$$

where h is the determinant of the induced metric on a constant λ slice of $\mathcal{N}$, and $\boldsymbol{Y} = dy^1 \wedge ... \wedge dy^{d-2}$.

Define the expansion, θ, and a $d-1$ form $\boldsymbol{\epsilon}$ by

$$\theta = \frac{1}{\sqrt{h}}\partial_\lambda\sqrt{h} \quad , \qquad \boldsymbol{\epsilon} = \sqrt{h}\, d\lambda \wedge dY. \tag{6.22}$$

Then the area difference can be written as

$$A(\Sigma_2) - A(\Sigma_1) = \int_{\mathcal{N}} \boldsymbol{\epsilon}\,\theta. \tag{6.23}$$

Expressing the area difference in this way is convenient, since the expansion is

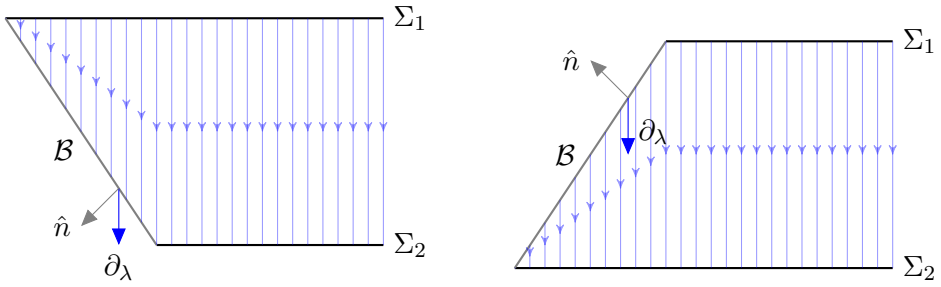


Figure 6.5: A portion of the boundary of the past $\partial J^-(\mathcal{R}_i)$, showing two cross sections Σ_1, Σ_2, and the end-of-the-world brane $\mathcal{B}$. Null geodesics generating the lightcone are shown in blue. The outward pointing normal to the brane is labelled $\hat{n}$, while the tangent vector to the null geodesics is labelled ∂_λ. (a) When $\hat{n} \cdot \partial_\lambda \geq 0$, the brane removes area. (b) When $\hat{n} \cdot \partial_\lambda \leq 0$, the brane adds area.

constrained in certain situations if we assume the null energy condition (NEC),

$$k^\mu k^\nu T_{\mu\nu} \geq 0. \tag{6.24}$$

In particular, consider an extremal surface γ. Then the boundary of the future or past of γ, $\partial J^\pm(\gamma)$, is generated by a congruence of null geodesics. Assuming the NEC, this congruence has non-positive expansion when moving away from γ, as can be shown using the Raychaudhuri equation [76]. We will call surfaces with non-positive expansion *light sheets*. Considering $\mathcal{N}$ to be a portion of either $\partial J^+(\gamma)$ or $\partial J^+(\gamma)$ then allows us to conclude $A(\Sigma_2) \leq A(\Sigma_1)$. That is, the area of a cross section of the congruence decreases as we follow the geodesics.

6.3 The area theorem with boundaries

Next, we consider the area theorem in the setting where $\mathcal{N}$ intersects the brane. The situation is shown in figure 6.5. The null surface $\mathcal{N}$ is still foliated by a null congruence, but some geodesics end or begin on an additional portion of the boundary, $\mathcal{N} \cap \mathcal{B}$. To prove an area theorem in this setting, we will need to assume the NEC holds both for the bulk stress tensor and for the branes stress tensor. This later

statement is

$$\ell^a \ell^b T^{\mathcal{B}}_{ab} \geq 0, \tag{6.25}$$

where ℓ^a is a null tangent vector to the brane. This is satisfied with equality for constant tension branes. Using the boundary condition $8\pi G_N T_{ab} = -(K_{ab} - Kh_{ab})$ we can also express this as $\ell^a \ell^b K_{ab} \leq 0$.

We will reconsider $\int \boldsymbol{\epsilon}\, \theta$ and write this as a boundary integral. A simple application of the fundamental theorem of calculus sufficed to derive 6.23, but this was only because the null geodesics meet Σ_1 and Σ_2 normally. For the additional portion of the boundary we need to use Stokes theorem in a more general form. To begin, note that

$$\boldsymbol{\epsilon}\, \theta = (\partial_\lambda \sqrt{h})\, d\lambda \wedge dY = d(\sqrt{h} dY) \equiv d\omega \tag{6.26}$$

so $\boldsymbol{\epsilon}\, \theta$ is closed. The last equality defines ω. Now we will use Stokes theorem in the form

$$\int_M d\omega = \int_{\partial M} d^{d-2}x \sqrt{\gamma} n^\mu V_\mu \tag{6.27}$$

where γ is the induced metric on the boundary, n^μ is the normal vector to the boundary[1], and $V_\mu = (-1)^{d-1}(*\omega)_\mu$ where $*$ denotes the Hodge dual.

The one-form V in 6.27 is simple to compute, $V = (-1)^{d-1} * \omega = (-1)^{d-1} d\lambda$. Along Σ_1 we have $n^\mu = -(\partial_\lambda)^\mu$, and along Σ_2 we have $n^\mu = (\partial_\lambda)^\mu$, which recovers the two boundary terms appearing in 6.23. The boundary $\mathcal{B} \cap \mathcal{N}$ returns an additional term,

$$\int_{\mathcal{N}} \boldsymbol{\epsilon}\theta = A(\Sigma_2) - A(\Sigma_1) + \int_{\Sigma \cap \mathcal{N}} d^{d-2}x \sqrt{\gamma}\, n_\lambda. \tag{6.28}$$

We will need this more general statement in chapter 11 when we prove the connected wedge theorem in the presence of an ETW brane.

For 6.28 to relate $A(\Sigma_2)$ and $A(\Sigma_1)$ we would like to fix the sign of n_λ. In

[1]For spacelike boundaries we should choose the outward pointing normal, while for timelike boundaries we shoose the inward pointing one.

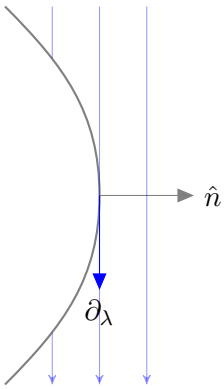


Figure 6.6: The lightsheet $\partial J^-(R_i)$ where it meets the brane. For $\hat{n} \cdot \partial_\lambda = n_\lambda \geq 0$ initially, a change in sign requires that the extrinsic curvature be positive somewhere along the brane (as shown here), which is ruled out by the NEC applied to the brane stress tensor.

particular, $n_\lambda \geq 0$ along with $\theta \leq 0$ would imply $A(\Sigma_2) \geq A(\Sigma_1)$, recovering the usual area theorem. This is illustrated in figure 6.5. In fact we can show $n_\lambda \geq 0$ in one particular but important situation. Suppose that $\mathcal{N}$ is a portion of $\partial J^-(\mathcal{R}_i)$, for $\mathcal{R}_i$ the entanglement wedge of an edge anchored region.[2] Then we have that at $\lambda = 0$,[3]

$$n_\lambda = 0. \tag{6.29}$$

This holds because the entangling surface $\gamma_{\mathcal{R}_i}$ meets the brane normally, which means the normal vectors of $\gamma_{\mathcal{R}_i} \cap \mathcal{B}$ will be tangent to the brane.

We claim the NEC imposed on the brane stress tensor ensures $n_\lambda \geq 0$ everywhere. To see this, study the derivative of n_λ as we move along the brane,

$$\ell^\mu \nabla_\mu (n_\lambda) = \ell^\mu \nabla_\mu (n_\sigma k^\sigma) = \ell^\mu k^\sigma \nabla_\mu n_\sigma + \ell^\mu n_\sigma \nabla_\mu k^\sigma. \tag{6.30}$$

[2]THe reader unfamiliar with entanglement wedges should skip the below, and refer back to this section after reading chapter 7.

[3]More generally we need only that $n_\lambda \geq 0$. We may have $n_\lambda > 0$ in some cases when r is a point in the AdS boundary and not on the edge, but it is not clear in general when this occurs.

Using

$$\begin{aligned} k^\sigma &= n_\lambda n^\sigma + \ell^\sigma, \\ 0 &= n^\nu \nabla_\mu n_\nu, \\ 0 &= k^\mu \nabla_\mu k^\nu, \end{aligned} \tag{6.31}$$

this becomes

$$\ell^\mu \nabla_\mu (n_\lambda) = \ell^\mu \ell^\sigma \nabla_\mu n_\sigma - n_\lambda n^\mu n_\sigma \nabla_\mu k^\sigma. \tag{6.32}$$

Since initially $n_\lambda = 0$, if we establish that $\nabla_\lambda n_\lambda \geq 0$ whenever $n_\lambda = 0$, we are done. But when $n_\lambda = 0$ the above is just

$$\nabla_\lambda n_\lambda = \ell^\mu \ell^\sigma \nabla_\mu n_\sigma = -\ell^a \ell^b K_{ab} \geq 0 \tag{6.33}$$

where the minus sign in the second equality is introduced because K_{ab} is defined using the inward pointing normal vector, whereas the normal vector appearing in Stokes theorem was outward pointing. The inequality is just the NEC imposed on the brane. How the curvature in the brane prevents a sign change in n_λ is illustrated in figure 6.6.

Chapter 7

The AdS/CFT correspondence

This chapter is review material. The original reference for the AdS/CFT correspondence is [60], while a useful review with an entanglement focused perspective is [79]. The Ryu-Takayanagi formula was first proposed in [83], and entanglement wedge reconstruction in [24]. AdS/BCFT was proposed in [92].

In this chapter we review the AdS/CFT correspondence, emphasizing quantum information theoretic aspects. In particular we discuss the Ryu-Takayanagi formula and its covariant generalizations, which relates the von Neumann entropy of boundary subregions to areas of extremal surfaces in the bulk. We then discuss the entanglement wedge and the role of quantum error-correction in AdS/CFT.

7.1 Statement of the correspondence

The AdS/CFT correspondence states that two physical theories are equivalent. The two theories are a particular type of conformal field theory, the CFT, and quantum gravity in asymptotically AdS spacetimes.

To understand what it means to say these theories are equivalent, consider that we can describe the two theories as a Hilbert space along with a Hamiltonian,

$$\mathcal{H}_{CFT}, H_{CFT} \quad \text{and} \quad \mathcal{H}_{AdS}, H_{AdS}. \tag{7.1}$$

One way to formally state the equivalence of these theories is to specify that there

exists a unitary mapping

$$V : \mathcal{H}_{CFT} \to \mathcal{H}_{AdS} \tag{7.2}$$

which preserves time evolution,

$$V^\dagger H_{AdS} V = H_{CFT}. \tag{7.3}$$

Given such a mapping V, we can calculate any correlation function in the CFT using the bulk AdS picture, or vis versa.

Before we can understand what is known about the map V, we should describe the bulk (AdS) and boundary (CFT) pictures in more detail.

Lets begin with the CFT. A conformal field theory is a quantum field theory with additional symmetry. In particular the Poincaré group is extended to the conformal group, which contains two additional generators. The *dilation* corresponds to a simple rescaling of coordinates,

$$\tilde{x}^\mu = \lambda x^\mu. \tag{7.4}$$

There is also the *special conformal transformation*

$$\tilde{x}^\mu = \frac{x^\mu + a^\mu x^2}{1 + a_\nu x^\nu + a^2 x^2}. \tag{7.5}$$

A general CFT is described by a set of *primary operators* $\{\mathcal{O}_i\}_i$ along with associated conformal weights Δ_i and a set of coefficients C_{ijk} that appear in three point functions. Some CFT's also have an action description, which we will assume we have for the CFT's of interest here. The primary operators are singled out by their simple transformation property under dilations,

$$\mathcal{O}_i(\lambda x) = \lambda^{-\Delta_i} \mathcal{O}_i(x). \tag{7.6}$$

All operators in the CFT can be built from the primaries by acting with derivatives, multiplication or addition of primaries, etc, so we are particularly interested in understanding primary operators and their correlation functions.

There are two parameters in the CFT which we will keep track of. The first is the *central charge*, labelled c. The central charge appears in a number of places in the CFT, including in the description of the algebra of symmetries of the CFT. Focusing on conformal field theories in $1+1$ dimensions, we will be most interested in the appearance of the central charge in the von Neumann entropy of a subregion of the CFT. In the CFT vacuum state, and considering a subregion of size L, this is given by

$$S(L) = \frac{c}{3} \log \frac{L}{\epsilon} \tag{7.7}$$

where ϵ is a length scale set by choosing a UV regulator. From this expression, we interpret the central charge as measuring the number of degrees of freedom in the CFT.

The second parameter in the CFT we will keep track of is a coupling constant, λ, controlling the strength of interactions in the CFT. In general the CFT will not have just one coupling, but we will be heuristic. We will be interested in limits of the parameter λ, which we would then have to make sense of in any specific CFT.

Next lets discuss the AdS bulk physics. In the most general case, the bulk is described by an interacting string theory. We will be focused however on a limit where this is well described by classical gravity. This occurs in the limit

$$c >> 1, \quad \lambda \to \infty. \tag{7.8}$$

which will be the setting we will always work in. The bulk action then takes the form

$$S_{\text{AdS}} = \frac{1}{16\pi G_N} \int_M d^{2+1}x \sqrt{-g} \left(R - 2\Lambda + \mathcal{L}_{\text{matter}} \right). \tag{7.9}$$

Away from a strict $\lambda \to \infty$ limit higher curvature terms also enter the action above. It is common to express the cosmological constant Λ in terms of the *AdS length* ℓ_{AdS},

$$\Lambda = -\frac{3}{\ell^2_{\text{AdS}}}. \tag{7.10}$$

The central charge is related to the gravitational parameter G_N, ℓ_{AdS} by

$$c = \frac{3\ell_{AdS}}{2G_N}. \tag{7.11}$$

Since we're working in the strict $\lambda \to \infty$ limit it doesn't enter in fixing the gravitational parameters we've kept, but away from this limit λ fixes the length scale of the higher curvature corrections to the action above.

It will be helpful to have a gauge-fixed description of the bulk gravitational degrees of freedom. A suitable gauge is Fefferman-Graham, where the metric takes the general form

$$ds^2 = \frac{\ell_{AdS}^2}{z^2}(dz^2 + \Gamma_{\mu\nu}(x,z)dx^\mu dx^\nu). \tag{7.12}$$

The function $\Gamma_{\mu\nu}$ has the form

$$\Gamma_{\mu\nu} = \eta_{\mu\nu} + O(z^{d+1}) \tag{7.13}$$

where η is the metric of the conformal boundary.

With this background on AdS and CFT physics, we can now return to discuss the map V. The most basic aspect of the correspondence is that the CFT lives on the conformal boundary of the AdS spacetime. This will be described by the metric $\eta_{\mu\nu}$ introduced in 7.13. The conformal boundary will always topologically take the form $\mathcal{B} \times \mathbb{R}$, where $\mathbb{R}$ is the Lorentzian time direction and $\mathcal{B}$ is the spatial manifold.

Next we relate the operator content of the bulk and boundary theories. The CFT stress tensor is dual to the bulk metric, in the sense that $T_{\mu\nu}$ can be computed from boundary limits of the bulk metric. See [31] for explicit formulae. Since all field theories have a stress tensor, and the bulk always has a metric, these objects can always be dual. Additionally, there will be a set of bulk fields ϕ_i dual to the primary operators $\mathcal{O}_i$ with

$$\mathcal{O}_i(x) = \lim_{z\to 0} z^{-\Delta_i}\phi_i(x,z). \tag{7.14}$$

This fixes the field content in the bulk given the CFT data.

Next, we need to understand the state of the bulk fields given the state in the

boundary. In the classical limit defined by 7.8 this map is specified implicitly by a path integral. It is convenient to first discuss the case where the state of the bulk fields has a moment of time symmetry, so that $\partial_t \phi = 0$. Later we discuss the more general case.

Choose a manifold $\mathcal{M}$, equipped with a Euclidean metric, which has a coordinate τ that we will identify as Euclidean time. We require $\mathcal{M}$ to be $\mathbb{Z}_2$ symmetric around $\tau = 0$ and the $\tau = 0$ slice to be $\mathcal{B}$. Next take the Euclidean version of our CFT and consider it on the manifold $\mathcal{M}$. For each operator in the CFT, consider a source $J_i(x, \tau)$ also defined on $\mathcal{M}$ and required to satisfy $J(x, \tau) = J^*(x, -\tau)$. To find the bulk state, solve the bulk field configurations subject to the boundary condition

$$J(x) = \lim_{z \to 0} z^{\Delta - d} \phi(z, x). \tag{7.15}$$

In this solution look at the $\tau = 0$ slice. Then the bulk field at $\tau = 0$ is described by

$$\begin{aligned} \phi_i(x, 0) &= \phi_{0i}(x), \\ \partial_\tau \phi &= 0. \end{aligned} \tag{7.16}$$

This describes the state of the bulk fields at time $\tau = 0$. To obtain the full Lorentzian spacetime, we take this as initial data on a $t = 0$ slice and set $\partial_\tau \phi = -i \partial_t \phi$. Meanwhile in the CFT, the initial dual state is described by the path integral

$$\langle \Phi_0 | \psi \rangle_{CFT} = \int^{\Phi = \Phi_0} d\Phi \, e^{-S^E_{CFT}[\Phi] + \int d^{2+1} x J(x) \Phi(x)} \tag{7.17}$$

where Φ denotes schematically the various fields in the CFT. The path integral is performed over the portion of the Euclidean boundary manifold with $\tau < 0$. One can use this state as initial data to evolve into Lorentzian time in the CFT.

To relate bulk states with non-time symmetric field configurations, we begin with one of the dual pairs of bulk and boundary time symmetric states, then add additional time evolution with Lorentzian sources to obtain a larger class of states.

In the CFT we do a Lorentzian path integral with $|\psi\rangle$ as the initial data,

$$\langle\Phi_1|\psi\rangle_{CFT} = \int_{\Phi_L=\Phi_0}^{\Phi_L=\Phi_1} D\Phi_L\, e^{iS_{CFT}[\Phi_L]+\int d^{2+1}J(x)\Phi_L(x)} \int^{\Phi_E=\Phi_0} d\Phi_E\, e^{-S^E_{CFT}[\Phi_E]+\int d^3xJ(x)\Phi_E(x)}.$$

In the bulk, we evolve the bulk fields using a similar bulk path integral. For in depth discussion of Lorentzian AdS/CFT see for example [89].

This path integral construction succeeds in identifying the bulk dual of a large class of CFT states. The construction does not immediately answer many of the possible questions we may ask about how the bulk and boundary states are related. In particular, we may be interested in identifying how objects other than primary operators or the stress-tensor in the CFT are described in terms of bulk physics. We take up one such object in the next section, the von Neumann entropy, whose bulk description is related simply to the bulk geometry.

7.2 The Ryu-Takayanagi formula

Of particular interest to us will be the Ryu-Takayanagi formula, which is a prescription for calculating the von Neumann entropy of a boundary subregion given bulk data.

To motivate the formula, lets begin by discussing black holes. As Hawking showed, a black hole radiates, and consequently has a temperature and a thermodynamic entropy. As a classical object the state of the black hole is described by a Boltzmann distribution,

$$\rho_{BH} = \frac{1}{Z}\sum_i e^{-\beta E_i}|E_i\rangle\langle E_i|. \tag{7.18}$$

For a diagonal density matrix such as this, the von Neumann entropy is just the thermodynamic entropy. The thermodynamic entropy of a black hole is, to leading order in $1/G_N$,

$$S_{BH} = \frac{\text{Area}[\gamma_{BH}]}{4G_N} \tag{7.19}$$

where γ_{BH} is the black hole horizon, so that at least in this special case the von

Neumann entropy of a spacetime region (the black hole) is given, at leading order, by the area of the region.

The above formula accounts for the entropy of the black hole in the setting where no quantum fields are present. Including additional fields in our spacetime, there is an additional contribution to the entropy of the black hole. In particular we should add to the above a von Neumann entropy of the subregion of the fields inside the black hole,

$$S_{BH} = \frac{\text{Area}[\gamma_{BH}]}{4G_N} + S_{QFT}[\text{BH interior}]. \tag{7.20}$$

This is called the *generalized entropy* of the black hole. By replacing the black hole interior, we can also define the generalized entropy of any subregion of our spacetime.

The Ryu-Takayanagi formula is a broad generalization of the black hole entropy formula. It states that

$$S(A) = \min_{\gamma_A} \operatorname*{ext}_{\gamma_A \in \text{Hom}(A)} \left(\frac{\text{Area}[\gamma_A]}{4G_N} + S_{QFT}(\mathcal{E}_W(A)) \right). \tag{7.21}$$

Understanding this formula requires some unpacking. A denotes a subregion of the CFT, whose entropy we are interested in calculating. To calculate it using bulk data, we look for extremal surfaces which are *homologous* to A. Surface γ_A is said to be homologous to a boundary region A if $A \cup \gamma_A$ forms the boundary of some region, which will be called the entanglement wedge of A, $\mathcal{E}_W(A)$.

A simple example of the RT formula is shown in figure 7.1. There, we consider AdS_{2+1}/CFT_{1+1} and a boundary region A which is the union of two intervals, call them a_1 and a_2. There are two extremal surfaces homologous to $A = a_1 \cup a_2$. First, we can have

$$\gamma'_{a_1 \cup a_2} = \gamma_{a_1} \cup \gamma_{a_2}. \tag{7.22}$$

This is an extremal surface composed of two pieces, one homologous to a_1 and the other homologous to a_2. This is shown in figure 7.1a. A second extremal surface will of the type shown in figure 7.1b, which we will call $\gamma_{a_1 \cup a_2}$. This surface is also

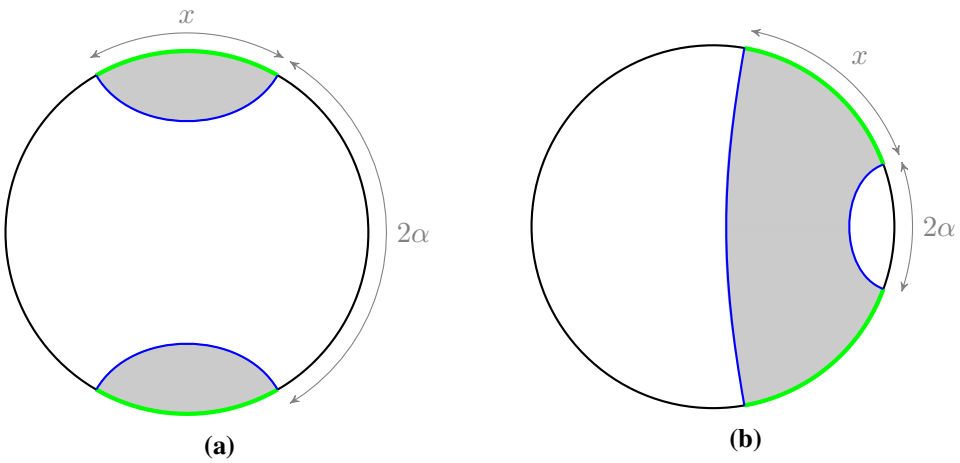


Figure 7.1: Extremal surfaces (shown in blue) for two intervals R_1 and R_2 (shown in green) of equal size x sitting on a constant time slice of AdS_{2+1}. The intervals are separated by an angle 2α. The entanglement wedge $\mathcal{E}(R_1R_2)$ (shown in grey) is the region whose boundary is the union of the regions R_1 and R_2 and their minimal surfaces. For large α and small x the entanglement wedge of the region $R_1 \cup R_2$ is disconnected, while for small α or large enough x, the entanglement wedge becomes connected, as shown at right. The entanglement wedge being connected indicates the mutual information is $O(N^2)$, while a disconnected entanglement wedge indicates the mutual information is $O(N^0)$.

composed of two components, but each component is connected across a_1 and a_2. The RT formula says that we should choose between these two possible surfaces by taking the one associated with smaller generalized entropy. One way to capture the qualitative distinction between these two surfaces is to notice that in the first case the entanglement wedge is a disconnected region, while in the second case it is connected.

There is a second, equivalent formulation of the RT formula which we will use in proving the connected wedge theorem. It is

$$S(A) = \max_{\Sigma} \min_{\gamma_A \in \Sigma} \left(\frac{\text{Area}[\gamma_A]}{4G_N} + S_{QFT}(\mathcal{E}_W(A)) \right). \tag{7.23}$$

The maximization is over choices of Cauchy surface through the bulk which include A in their boundary. The minimization is over surfaces γ_A that sit inside of Σ. Reference [3] showed that this is equivalent to the extremal surface formulation when the quantum focusing conjecture holds. To establish equivalence when considering only the $1/G_N$ terms it suffices to consider the null energy condition [97].

7.3 The entanglement wedge

We've seen that given a state in the boundary CFT, we can determine the bulk AdS state, and vis versa. It is also interesting to ask if there is a more fine grained duality: given the density matrix of a subregion A of the CFT, what portion of the bulk can we learn about?

The RT formula can be used to suggest one possible answer. The von Neumann entropy $S(A)$ can be calculated from the density matrix ρ_A. In the bulk picture, the RT formula reveals that a qubit sitting anywhere inside of the entanglement wedge $\mathcal{E}_W(A)_\rho$ affects the value of $S(A)_\rho$. This suggests that the density matrix ρ_A describes the entire entanglement wedge $\mathcal{E}_W(A)_\rho$.

This is nearly a correct statement, but comes with a caveat that we can state once we make the problem more precise. We will specify a subspace of the full bulk Hilbert space, which we will call $\mathcal{H}_{code}$. This code space is chosen to consist of bulk states with a well defined geometry and possible quantum fields living on that geometry. Further, we will assume that *all states in the code space have approximately the same quantum extremal surfaces*. Except in certain finely tuned cases, this will be the case in a classical geometry with $n < O(1/G_N)$ qubits moving through the spacetime. This is a strong assumption, and it is both possible and interesting to relax it.[1] This assumption will suffice for our purposes in the chapters below.

[1] Doing so leads to the notion of the reconstruction wedge [2, 44], and is important in understanding black hole evaporation, where the entropy of Hawking radiation becomes $O(1/G_N)$ at late times [75].

Given this assumption, we can write the RT formula in the form

$$S(A) = \min_{\gamma_A} \operatorname*{ext}_{\gamma_A \in \text{Hom}(A)} \left(\frac{\text{Area}[\gamma_A]}{4G_N} \right) + S_{QFT}(\mathcal{E}_W(A)) \tag{7.24}$$

In this setting we simply refer to the surfaces γ_A as extremal surfaces, since they do not involve extremizing the quantum entropy term.

We state our main claim for this section as follows.

Theorem 7 *Suppose that a small number*[2] *of qubits are in an unknown state and sit inside of the entanglement wedge of A, defined by*

$$\partial(E_W(A)) = \gamma_A \cup A \tag{7.25}$$

where γ_A is the extremal surface for the boundary subregion A. Then it is possible to recover the state of those qubits given access to the density matrix ρ_A.

To understand this, our first step will be to argue for an operator level version of the Ryu-Takayanagi formula. In particular we define the *modular Hamiltonian*

$$H_X = -\log \rho_X \tag{7.26}$$

of any density matrix. Then consider the relative entropy between a density matrix ρ and a nearby state $\rho + \delta\rho$. Because the relative entropy is always non-negative, and $S(\rho||\rho) = 0$, we learn that

$$S(\rho + \delta\rho||\rho) = O(\delta\rho^2) \tag{7.27}$$

Writing the relative entropy our using the closed form $S(\rho||\sigma) = \text{tr}(\rho \log \sigma) - S(\rho)$, we obtain

$$S(\rho + \delta\rho) - S(\rho) = \text{tr}(\delta\rho H_\rho) + O(\delta\rho^2) \tag{7.28}$$

this is sometimes also written as $\delta S(\rho) = \text{tr}(\delta\rho H_\rho)$ and called the first law of entanglement.

[2] As above this means $n < O(1/G_N)$.

Now begin with the RT formula,

$$S(\rho_A) = \text{tr}\left(\rho_a \frac{\text{Area}[\gamma_A]}{4G_N}\right) + S(\rho_a) \tag{7.29}$$

where γ_A is the minimal extremal surface, and we've introduced a shorthand $a = \mathcal{E}_W(A)$. Note that the area is just a number, but we will think of it here as an operator proportional to the identity. Now take a variation of both sides of this expression, and apply the first law of entanglement to both the entanglement terms,

$$\text{tr}(\delta\rho_A H_{\rho_A}) = \text{tr}\left(\delta\rho_a \left(\frac{\text{Area}[\gamma_A]}{4G_N} + H_{\rho_a}\right)\right). \tag{7.30}$$

Now, ρ_A and its dual ρ_a are arbitrary states in the code space. Lets fix one particular choice. Then consider some other state in the code space, call it σ_A with corresponding σ_a. If we decompose σ_A into a sum of many small terms $\delta\sigma_{A,i}$ then choose $\delta\rho_A = \delta\sigma_{A,i}$ in the above, we can conclude

$$\text{tr}(\sigma_A H_{\rho_A}) = \text{tr}\left(\sigma_a \left(\frac{\text{Area}[\gamma_A]}{4G_N} + H_{\rho_a}\right)\right), \tag{7.31}$$

for any state σ in the code space. Thus, we get the operator level statement

$$H_{\rho_A} = \frac{\text{Area}[\gamma_A]}{4G_N} + H_{\rho_a} \tag{7.32}$$

which holds on the code space. This was initially discussed in [50] and is often referred to as the JLMS formula.

Lets return now to consider the relative entropy. Applying the JLMS formula, we find that this is equal to the bulk relative entropy

$$S(\rho_A||\sigma_A) = S(\rho_a||\sigma_a) + O(\sqrt{G_N}) \tag{7.33}$$

The correction term arises from small variations in the location of the extremal surface for different states in the code space.[3]

[3]We didn't quantify what we meant by keeping the extremal surface approximately fixed in the code space, for simplicity we will take 7.33 to quantify what we mean by an approximately fixed extremal surface.

The equality of bulk and boundary relative entropy actually implies ρ_a can be recovered from ρ_A, and vis versa. To establish this carefully involves the theory of approximate recovery channels, and would take us too far out of our progression towards the results in later chapters. However, our discussion of decoupling and the reversal of quantum channels in section 2.5 suffices to provide a correct intuition for these results.

Define a channel

$$\mathcal{N}_{a\to A}(\rho_a) = \text{tr}_{\bar{A}}(V^\dagger(\rho_a \otimes X_{\bar{a}})V) \tag{7.34}$$

where $X_{\bar{a}}$ is some fixed state in the code space. We will argue this channel has an inverse. From our error correction theorem 3, we want to argue that a unitary extension of this channel (which here we take to be V) does not correlate its output (which here is A) to the environment (which here is $\bar{A}$). The JLMS result means ρ_A, σ_A and ρ_a, σ_a are, up the small correction, equally distinguishable. This suggests A and $\bar{A}$ must be uncorrelated, since otherwise information from a escapes to the environment, $\bar{A}$, and distinguishability would decrease under the action of the channel. Then from theorem 3 we have that an inverse channel to $\mathcal{N}_{a\to A}$ exists. See [23] for a complete argument.

7.4 AdS/BCFT

In chapter 11, we will also use a variant of AdS/CFT wherein the conformal field theory is replaced with a *boundary conformal field theory*, or BCFT.

A BCFT is a conformal field theory living on a manifold with boundary, along with a conformally invariant boundary condition. For appropriate BCFTs, the AdS/BCFT [33, 92] correspondence suggests a bulk dual description, which consists of an asymptotically AdS region along with an extension of the CFT boundary into the bulk as an end-of-the-world (ETW) brane. To avoid confusion with the bulk-boundary language of the AdS/CFT correspondence, we will refer to the CFT boundary as the *edge*.

Recall from chapter 6 that a bulk AdS spacetime with an ETW brane is de-

scribed by the action

$$I_{\text{bulk}} + I_{\text{brane}} = \frac{1}{16\pi G_N} \int d^{d+1}x \sqrt{g}(R - 2\Lambda + L_{\text{matter}}) + \frac{1}{8\pi G_N} \int_{\mathcal{B}} d^d y \sqrt{h}(K + L^{\mathcal{B}}_{\text{matter}}) \ , \tag{7.35}$$

where L_{matter} and $L^{\mathcal{B}}_{\text{matter}}$ are matter Lagrangians for fields in the bulk and brane respectively. As usual, R is the Ricci curvature and Λ the bulk cosmological constant, while K is the trace of the extrinsic curvature of the brane,

$$K_{ab} = \nabla_a n_b \ , \tag{7.36}$$

for outward normal n_j to $\mathcal{B}$, and a, b refer to brane coordinates y^a. This action leads to Einstein's equations in the bulk, along with the boundary condition

$$-\frac{1}{8\pi G_N}(K_{ab} - K h_{ab}) = T^{\mathcal{B}}_{ab} \ . \tag{7.37}$$

In AdS/BCFT, the Ryu-Takayanagi formula [82] and its covariant generalization the HRT formula [48] continue to calculate the entropy of boundary subregions, provided the homology condition is appropriately adapted [91]. In the context of AdS/CFT, and assuming the null energy condition, the HRT formula is equivalent to the maximin formula [97]. We will assume this remains the case in AdS/BCFT. Recall from above that the maximin formula states that

$$S(A) = \max_{\Sigma} \min_{\gamma_A} \left(\frac{\text{Area}[\gamma_A]}{4G_N} \right) + O(1).$$

The maximization is over Cauchy surfaces that include A in their boundary, and the minimization is over spacelike codimension 2 surfaces γ_A which are homologous to A. In spacetimes with an ETW brane we should understand the homology constraint as

$$\partial S = \gamma_A \cup A \cup b \tag{7.38}$$

for S a spacelike surface in the bulk, and where b is allowed to be any portion of the

ETW brane. For a single interval in the CFT, this allows two qualitatively distinct classes of entangling surface: those which do not include a portion of the brane to satisfy the homology constraint, which we call brane-detached, and those which do, which we call brane-attached.

Chapter 8

Quantum tasks in holography

This chapter is based on original material, first appearing in [64]. Similar earlier work also appeared in [63].

In this chapter we introduce a framework for applying quantum tasks to AdS/CFT. The next two chapters discuss concrete applications of this framework, which leads to the $2 \to 2$ and $1 \to 2$ connected wedge theorems.

8.1 Framework for holographic quantum tasks

In our definition of a quantum task in chapter 4, we used an operational framing — Bob gives Alice some quantum systems, Alice performs some computations, and Alice returns some other systems to Bob. This language is convenient, and indeed it is natural when discussing quantum cryptographic applications such as position-based cryptography.

It is possible to remove the operational language however. In particular, the protocol Alice carries out is in fact just a feature of some initial state $|\Psi\rangle$. All the instructions for her protocol are by necessity recorded there, all that happens during the execution of the protocol is time evolution according to the underlying theory's Hamiltonian. While Alice's protocol is the internal dynamics of the theory in question, Bob preparing the inputs and collecting outputs correspond to couplings to some external system. Viewing quantum tasks in this way motivates

understanding them as probes of the underlying theory they are defined in.

Because tasks probe the underlying theory, if we are given an equivalence between two theories it is natural to try and interpret this equivalence in the language of tasks. In particular we will consider the bulk and boundary theories in AdS/CFT. Within each theory, there is a set of tasks that can be defined and associated success probabilities, $\{(\mathbf{T}_i, p_{suc}(\mathbf{T}_i))_i\}$. The equivalence of bulk and boundary theories suggests that for each task $\mathbf{T}$ defined in the bulk there is some corresponding task $\hat{\mathbf{T}}$ in the boundary, and further that $p_{suc}(\hat{\mathbf{T}}) = p_{suc}(\mathbf{T})$. We will make this more precise below.

Our first step will be to restrict attention to a bulk described by classical geometry along with quantum fields living on a curved background (which may be coupled to the geometry). This means that while the boundary theory completely describes the bulk, the converse is not true. Consequently we will expect an inequality,

$$p_{suc}(\mathbf{T}) \leq p_{suc}(\hat{\mathbf{T}}). \tag{8.1}$$

Before understanding this in more detail however, we need to specify how a bulk task should be associated with a boundary task.

Given a task in the bulk $\mathbf{T} = (\mathcal{M}, \mathscr{A}, \mathcal{S}_{\mathscr{A}}, \mathscr{B}, \mathcal{S}_{\mathscr{B}}, \mathcal{N}_{\mathscr{A}\to\mathscr{B}})$, we should identify the boundary dual of each element of the tuple. Beginning with $\mathcal{M}$, the bulk geometry, we define $\hat{\mathbf{T}}$ to be in the geometry $\partial\mathcal{M}$, the boundary of $\mathcal{M}$. The inputs $\mathscr{A}$, outputs $\mathscr{B}$, and channel $\mathcal{N}_{\mathscr{A}\to\mathscr{B}}$ we may identify trivially across bulk and boundary. This is because while the bulk and boundary degrees of freedom look very different, we can record the same quantum states into these different degrees of freedom.

Next we need to discuss how to identify an access structure in the bulk with a corresponding access structure in the boundary. Note that in principle, because the AdS/CFT correspondence fixes the boundary description given the bulk, the boundary access structure $(\{\hat{\mathcal{A}}^j_{A_i}\}, \{\hat{\mathcal{U}}^j_{A_i}\}\})$ is fixed by the bulk one $(\{\mathcal{A}^j_{A_i}\}, \{\mathcal{U}^j_{A_i}\}\})$. We have not understood how to do this in the most general case, but can make some statements which will be sufficient for the applications discussed here.

First, notice that given bulk authorized regions $\{\mathcal{A}^j_{A_i}\}_j$, we have

$$\{\hat{\mathcal{A}}^k_{A_i}\}_k \supseteq \bigcup_j \{\hat{X} : \mathcal{A}^j_{A_i} \subseteq \mathcal{E}_W(\hat{X})\}. \tag{8.2}$$

This is because the entanglement wedge $\mathcal{E}_W(\hat{X})$ is the portion of the bulk which $\hat{X}$ can be used to recover, so when $\mathcal{A}^j_{A_i} \subseteq \mathcal{E}_W(\hat{X})$ the boundary region $\hat{X}$ can be used to recover A_i, which implies $\hat{X}$ is an authorized region. The other inclusion does not follow in general since there may be some boundary regions $\hat{\mathcal{A}}^j_{A_i}$ whose entanglement wedge includes a portion but not all of $\mathcal{A}^j_{A_i}$ and which still construct A_i.

Given a bulk unauthorized region, we can say that

$$\{\hat{\mathcal{U}}^k_{A_i}\}_k \supseteq \bigcup_j \{\hat{X} : \mathcal{U}^j_{A_i} \supseteq \mathcal{E}_W(\hat{X})\}. \tag{8.3}$$

This follows because $\mathcal{E}_W(\hat{X})$ is the largest bulk region whose quantum information can be reconstructed given $\hat{X}$, so $\mathcal{U}^j_{A_i} \supseteq \mathcal{E}_W(\hat{X})$ means $\hat{X}$ does not reconstruct A_i. Note that unless one or more of the $\mathcal{U}^j_{A_i}$ are anchored to the boundary, the set $\{\hat{X} : \mathcal{U}^j_{A_i} \supseteq \mathcal{E}_W(\hat{X})\}$ will be empty.

In the context of the connected wedge theorem, we will be interested only in a special case, where the bulk tasks access structures all have only authorized regions, and where those authorized regions are points. In this case the inclusion 8.2 becomes an equality, fully specifying the boundary authorized regions from the bulk ones. Further, there will be no boundary unauthorized regions[1]. Nonetheless we have described the identification of bulk and boundary access structures in as much generality as possible, as future applications may exploit more of it.

Given a bulk task $\mathbf{T}$ and associated boundary task $\hat{\mathbf{T}}$, we've claimed $p_{suc}(\mathbf{T}) \leq p_{suc}(\hat{\mathbf{T}})$. This follows because any protocol that completes the task in the bulk with some probability p will be mapped under the AdS/CFT duality to a protocol in the boundary. The bulk task's success probability is determined by the information localized to the regions $(\{\mathcal{A}^j_{A_i}\}, \{\mathcal{U}^j_{A_i}\}\})$. In the boundary description the same

[1]Of course the spacelike complements $[\mathcal{A}^k_{A_i}]^c$ do not contain any information about A_i, but it is not necessary to designate these as unauthorized, since this is immediate from the $\mathcal{A}^k_{A_i}$ being authorized.

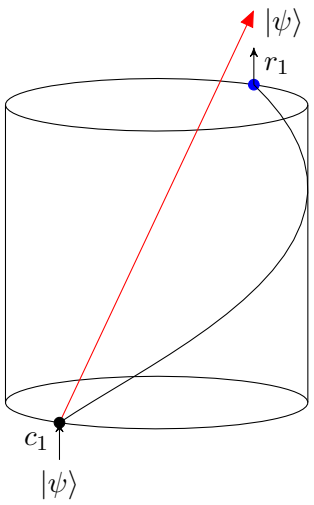


Figure 8.1: The quantum task discussed in section 8.2. A quantum state is received at a point on the boundary c_1 and must be returned at the point r_1. Equation 8.1 implies that signals cannot travel faster through the bulk than through the boundary, consistent with the usual statement of boundary causality [28, 35].

information will be available in the regions $(\{\hat{\mathcal{A}}^j_{A_i}\}, \{\hat{\mathcal{U}}^j_{A_i}\}\})$, so the boundary protocol will complete the task with probability p as well. Note that we claim only an inequality, rather than an equality, because many protocols in the boundary theory will correspond to bulk protocols that change the geometry $\mathcal{M}$, which we assumed should be fixed and unaffected by the protocol. Worse, some boundary protocols might correspond to leaving a semi-classical description of the bulk altogether.

8.2 Basic holographic quantum task examples

Bulk and boundary causality

A simple but non-trivial quantum task consists of a single input point c_1 and single output point r_1, both located at the AdS boundary. We specify that at c_1 Alice receives a quantum state $|\psi\rangle$ which she must return at r_1. Call this task $\mathbf{S}$ in the

bulk, and the corresponding boundary task $\hat{\mathbf{S}}$.

In the bulk picture, Alice can complete this task with high probability whenever $c_1 \prec r_1$, so that $p_{suc}(\mathbf{S}) \geq 1-\epsilon$. Using inequality 8.1, we get that $p_{suc}(\hat{\mathbf{S}}) \geq 1-\epsilon$ as well, which implies $\hat{c}_1 \prec \hat{r}_1$ (i.e. the same two points are causally connected in the boundary geometry). In summary then, we learn $c_1 \prec r_1$ in the bulk geometry implies $\hat{c}_1 \prec \hat{r}_1$ in the boundary geometry: a signal cannot travel faster through the bulk than through the boundary. This is just the usual statement relating bulk and boundary causality [28, 35].

Properties of entanglement wedges

We can use Theorem 6 characterizing localize-exclude tasks to recover well known features of entanglement wedges.

First, consider two boundary regions $\hat{\mathcal{A}}_1$ and $\hat{\mathcal{A}}_2$, which we take to be causally disconnected. Then Theorem 6 gives that a localize task $\hat{\mathbf{L}}$ which includes $\hat{\mathcal{A}}_1$ and $\hat{\mathcal{A}}_2$ as authorized regions is not possible, meaning it has low success probability, $p_{suc}(\hat{\mathbf{L}}) \leq \epsilon$. Using inequality 8.1, we get that the corresponding task in the bulk also has low success probability,

$$p_{suc}(\mathbf{L}) \leq \epsilon. \tag{8.4}$$

The corresponding bulk task has the entanglement wedges $\mathcal{A}_1$ and $\mathcal{A}_2$ as authorized regions. Since this task has low success probability, these bulk regions should also be causally disconnected. In other words,

$$\hat{\mathcal{A}}_1 \not\twoheadrightarrow \hat{\mathcal{A}}_2 \implies \mathcal{A}_1 \not\twoheadrightarrow \mathcal{A}_2. \tag{8.5}$$

In the case where $\hat{\mathcal{A}}_1, \hat{\mathcal{A}}_2$ are spacelike separated, we can write this as

$$\hat{\mathcal{A}}_1 \cap \hat{\mathcal{A}}_2 = \varnothing \implies \mathcal{A}_1 \cap \mathcal{A}_2 = \varnothing. \tag{8.6}$$

This is equivalent to the better known property of entanglement wedge nesting [1],

which is

$$\hat{\mathcal{X}} \subseteq \hat{\mathcal{Y}} \implies \mathcal{X} \subseteq \mathcal{Y}. \tag{8.7}$$

To see the equivalence, take $\hat{Y}$ to be the spacelike complement of $\hat{\mathcal{A}}_2$, denoted $[\hat{\mathcal{A}}_2]^c = \hat{Y}$ and take $\hat{X} = \hat{\mathcal{A}}_1$. Then use that for any two spacetime regions A, B, we have $A \subseteq [B]^c \iff A \cap B = \varnothing$.

Chapter 9

The $2 \to 2$ connected wedge theorem

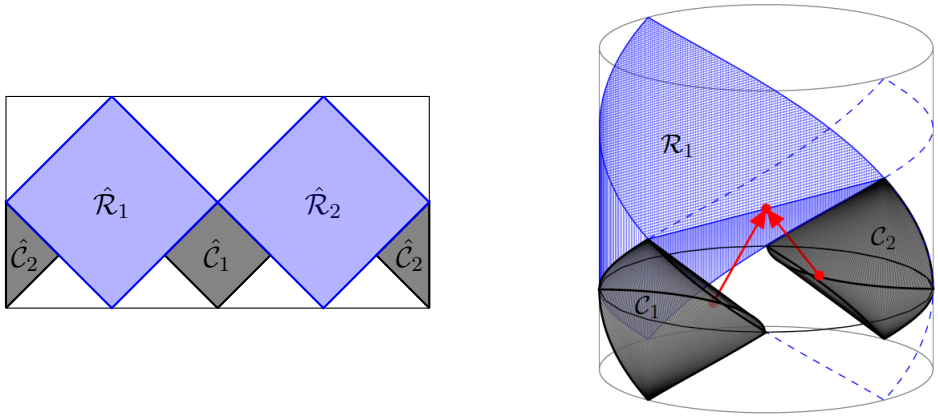
The presentation in this chapter follows [68]. However, an early version of the connected wedge theorem where the input and output regions are taken to be points was conjectured in [63] and later proven in [70].

In this chapter we discuss the $2 \to 2$ connected wedge theorem. We begin by stating the theorem formally in section 9.1, where we also discuss the converse statement and how to choose the input and output regions to make best use of the theorem. In section 9.2 we give the quantum tasks argument for the theorem. Section 9.3 discusses the remaining loophole in this argument. Section 9.4 gives the relativistic proof of the $2 \to 2$ connected wedge theorem.

9.1 Statement of the $2 \to 2$ connected wedge theorem

We state the connected wedge theorem below.

Theorem 8 ***(Connected wedge theorem)*** *Pick four regions $\hat{\mathcal{C}}_1, \hat{\mathcal{C}}_2, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ on the boundary of an asymptotically AdS spacetime. From these, define the decision*



(a) **(b)**

Figure 9.1: (a) A view of the boundary of AdS_{2+1}. Left and right edges of the diagram are identified. Shown is an example choice of input regions $\hat{\mathcal{C}}_i$ and output regions $\hat{\mathcal{R}}_i$. This particular choice is maximal for the regions $\hat{\mathcal{V}}_i$ defined by $\hat{\mathcal{C}}_i = \hat{\mathcal{V}}_i$. (b) Bulk perspective on the same choice of regions, showing the entanglement wedges $\mathcal{C}_i$ and $\mathcal{R}_i$. Only one of the out regions is shown, to avoid cluttering the diagram. In the bulk there is a non-empty entanglement scattering region $J^{\mathcal{E}}_{12\to 12}$.

regions

$$\hat{\mathcal{V}}_1 \equiv \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2),$$
$$\hat{\mathcal{V}}_2 \equiv \hat{J}^+(\hat{\mathcal{C}}_2) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2). \tag{9.1}$$

Assume that $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$. Define the entanglement scattering region

$$J^{\mathcal{E}}_{12\to 12} \equiv J^+(\mathcal{C}_1) \cap J^+(\mathcal{C}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2), \tag{9.2}$$

where $\mathcal{C}_i = \mathcal{E}_W(\hat{\mathcal{C}}_i)$ and $\mathcal{R}_i = \mathcal{E}_W(\hat{\mathcal{R}}_i)$. Then, $J^{\mathcal{E}}_{12\to 12} \neq \varnothing$ implies that $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$ is connected.

It is interesting to consider starting with a choice of regions $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$, then pick regions $\hat{\mathcal{C}}_1, \hat{\mathcal{C}}_2, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ to understand if $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ share a connected entanglement wedge. In AdS_{2+1}, and for $\hat{\mathcal{V}}_1, \hat{\mathcal{V}}_2$ single intervals, there is a unique 'best' way to do this, in the sense that one particular choice of regions will conclude there is a

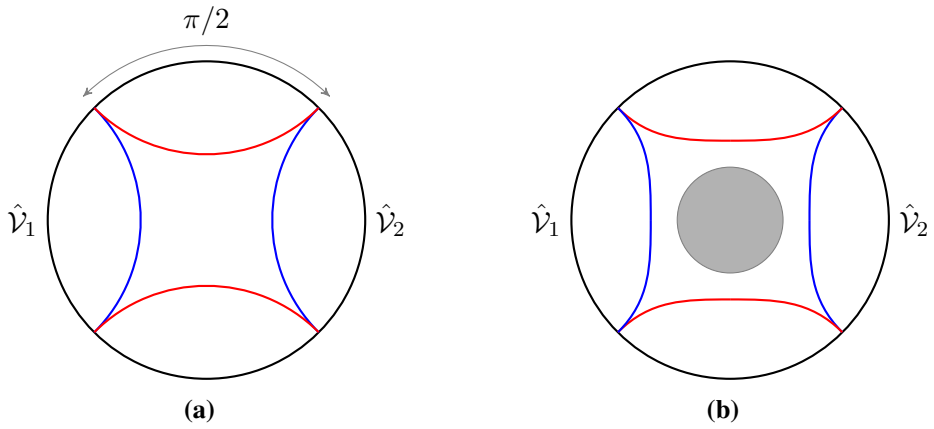


Figure 9.2: A counterexample to the converse of Theorem 8. (a) Vacuum AdS_{2+1} with regions $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ chosen antipodally and to each occupy $\pi/2$ of the boundary. Choosing the maximal consistent input and output regions, the entanglement scattering region is exactly one point, and the Ryu-Takayanagi surface is on the transition from disconnected (blue) to connected (red). (b) Spherically symmetric matter is added to the bulk. Now the entanglement wedges $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ reach less deeply into the bulk [47], and the light rays sent inward normally from their extremal surfaces are delayed. This closes the entanglement scattering region. By spherical symmetry however the Ryu-Takayanagi surface remains on the transition. Deforming $\hat{\mathcal{V}}_1$ to be larger ensures we are in the connected phase, and for small enough deformation ensures the scattering region remains empty.

connected wedge whenever any choice of regions does.

To find the optimal choice of $\hat{\mathcal{C}}_i, \hat{\mathcal{R}}_i$, we note first that there is a maximal choice of regions $\hat{\mathcal{C}}_i$ imposed by the constraint $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$: choose $\hat{\mathcal{C}}_i = \hat{\mathcal{V}}_i$. Further, there is a maximal choice of $\hat{\mathcal{R}}_i$ consistent with a given $\hat{\mathcal{V}}_1, \hat{\mathcal{V}}_2$, which is illustrated in figure 9.1a. Since any other choice $\hat{\mathcal{C}}'_i, \hat{\mathcal{R}}'_i$ has $\hat{\mathcal{C}}'_i \subseteq \hat{\mathcal{C}}_i$ and $\hat{\mathcal{R}}'_i \subseteq \hat{\mathcal{R}}_i$ these maximal choices have $J'^{\mathcal{E}}_{12\to 12} \subseteq J^{\mathcal{E}}_{12\to 12}$, so whenever a non-maximal choice has a non-empty entanglement scattering region the maximal choice will. Thus whenever $\hat{\mathcal{C}}'_i, \hat{\mathcal{R}}'_i$ can be used to conclude $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$ has a connected entanglement wedge, the maximal choice will conclude the same.

We can also consider the converse to Theorem 8: given two regions $\hat{\mathcal{V}}_1$, $\hat{\mathcal{V}}_2$,

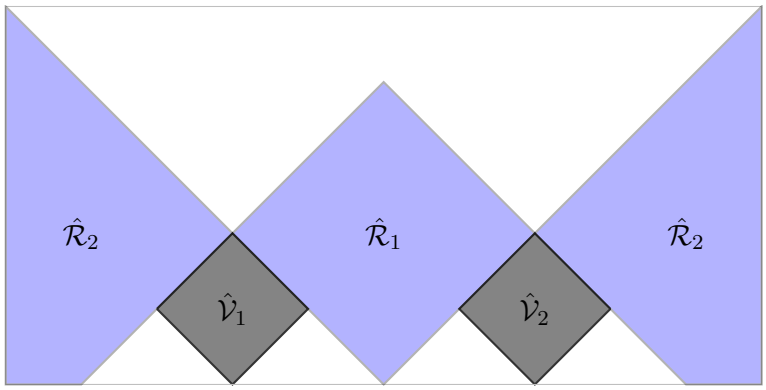


Figure 9.3: A typical choice of regions $\hat{\mathcal{C}}_1 = \hat{\mathcal{V}}_1$, $\hat{\mathcal{C}}_2 = \hat{\mathcal{V}}_2$, $\hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ in the boundary of Poincaré-AdS which leads to a non-trivial conclusion in the connected wedge Theorem 8. Region $\mathcal{R}_2$ consists of two wedges which each extend to infinity.

does their entanglement wedge being connected imply an associated scattering region is non-empty? The most interesting version of this question uses the maximal choice of regions $\hat{\mathcal{C}}_i, \hat{\mathcal{R}}_i$ so that the scattering region is as large as possible. Even taking the optimal choice of regions however the theorem does not have a converse, as we argue in figure 10.4.

Connected wedge theorem in Poincaré-AdS$_{2+1}$

The connected wedge theorem applies to any asymptotically AdS spacetime, including global AdS and Poincaré-AdS spacetimes in arbitrary dimensions. To apply the theorem meaningfully however, we need to find configurations of regions $\hat{\mathcal{C}}_1, \hat{\mathcal{C}}_2, \hat{\mathcal{R}}_2, \hat{\mathcal{R}}_2$ such that the bulk entanglement scattering region is non-empty, while the boundary scattering region is empty.

It is not immediately clear how to find non-trivial configurations of input and output regions in Poincaré-AdS$_{2+1}$. Indeed, at least for pure Poincaré-AdS$_{2+1}$ no such configurations exist when the input and output regions are chosen to be points. One way to see this is to start with non-trivial arrangements of points c_1, c_2, r_1, r_2 in global AdS$_{2+1}$, and chose a Poincaré patch which includes regions $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$. Doing so one always finds that one of the four points sit outside the patch, and consequently we cannot state the non-trivial instances of the theorem using points

directly in Poincaré AdS.

For extended regions it is straightforward to find non-trivial configurations in Poincaré AdS_{2+1}. An example configuration is shown in figure 9.3. Importantly, region $\hat{\mathcal{R}}_2$ consists of two disconnected parts, where each connected component consists of a half line. In an appendix of [64] non-trivial configurations in Poincaré have been explicitly given in the case where the bulk is pure AdS. Since many of these configurations have extended entanglement scattering regions, and the scattering regions should be deformed only a small amount for small perturbations to the bulk geometry, there will also be many non-trivial configurations when matter is added.

9.2 Quantum tasks argument

In this section we give the quantum tasks argument for the connected wedge theorem. The basic idea is to consider a $\mathbf{B}_{84}$ task embedded into AdS space. We use the results on necessity of entanglement from section 4.5 to argue for the theorem.

Argument. Consider two cases. First, supposed that $\hat{\mathcal{V}}_1 \cap \hat{\mathcal{V}}_2 \neq \varnothing$. Then we immediately have that the entanglement wedge of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2 \neq \varnothing$ is non-empty, and we are done.

Next, assume that $\hat{\mathcal{V}}_1 \cap \hat{\mathcal{V}}_2 = \varnothing$. This is just the statement that the boundary scattering region

$$\hat{J}_{12\to 12} = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^+(\hat{\mathcal{C}}_2) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2) \tag{9.3}$$

is empty. By assumption however, the bulk entanglement scattering region $J^{\mathcal{E}}_{12\to 12}$ is non-empty. This implies the existence of four points c_1, c_2, r_1, r_2 such that

$$J^+(c_1) \cap J^+(c_2) \cap J^-(r_1) \cap J^-(r_2) \neq \varnothing. \tag{9.4}$$

Choose a $\mathbf{B}_{84}^{\times n}$ task in the bulk with c_1, c_2 as input points and r_1, r_2 as output points. Then because the above region is non-empty, we can use the local strategy

(discussed in section 4.5) in the bulk, and we obtain a high success probability,

$$p_{suc}(\hat{\mathbf{B}}_{84}^{\times n}) \geq 1 - 2\epsilon^{2+n}. \tag{9.5}$$

Next, we should discuss how large we can take n. The obstruction to taking n arbitrarily large is that if we make use of too many qubits, the bulk protocol may change the geometry, deforming the geometry we are attempting to study. To avoid this we choose n to be any order in $1/G_N$ less than linear. Then if each qubit carries some energy ΔE, Einstein's equations dictate that the coupling to geometry is

$$G_{\mu\nu} = O(G_N \Delta E n). \tag{9.6}$$

Choosing $n < O(1/G_N)$ ensures that in the $G_N \to 0$ limit we have no backreaction, as needed to ensure we are studying the intended geometry.

Starting with $\mathbf{B}_{84}^{\times n}$, we label the corresponding boundary task by $\hat{\mathbf{B}}_{84}^{\times n}$. Following the discussion in section 4.2, we know $\hat{\mathbf{B}}_{84}^{\times n}$ has the same inputs and outputs as the corresponding bulk task. Further, we have by assumption that

$$\begin{aligned} c_i &\in \mathcal{E}_W(\hat{\mathcal{C}}_i), \\ r_i &\in \mathcal{E}_W(\hat{\mathcal{R}}_i). \end{aligned} \tag{9.7}$$

Thus $\hat{\mathcal{C}}_i$ is an authorized region for A_i in the boundary task, and $\hat{\mathcal{R}}_i$ is an authorized region for B_i. Since $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$, and by assumption the boundary scattering region $\hat{\mathcal{V}}_1 \cap \hat{\mathcal{V}}_2$ is empty, the boundary uses a non-local strategy. Lemma 11 of section 4.5 then applies and we can conclude

$$\frac{1}{2} I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) \geq n(-\log_2 \beta) - 1 + O((\epsilon/\beta)^n). \tag{9.8}$$

Since n is any order less than $O(1/G_N)$, we can conclude that $I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) = O(1/G_N)$, which occurs only when $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$ is connected. ■

We should note that there is a gap in this argument, which was noted also in [70]. In particular the causal diagram 4.2b does not include the regions that sit between $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$. Call these $\hat{\mathcal{X}}_1$ (which is the portion of the complement in the past of $\hat{\mathcal{R}}_1$) and $\hat{\mathcal{X}}_2$ (the portion of the complement in the past of $\hat{\mathcal{R}}_2$). In general,

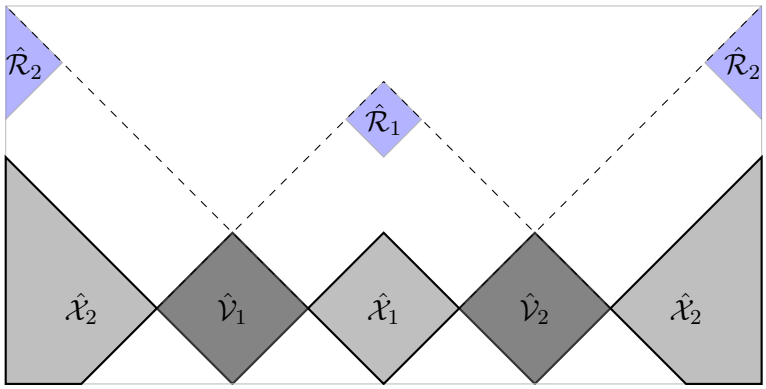


Figure 9.4: Boundary view of the $\mathbf{B}_{84}$ task. Input regions $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ are shown in dark gray. The regions X_i, shown in light gray, sit between the input regions and add some complications to the boundary proof of Theorem 8.

these regions can be made use of to complete the $\hat{\mathbf{B}}_{84}^{\times n}$ task without entanglement, as we show in the next section. However, such strategies require GHZ correlations in the CFT, which are not expected [71]. As well, it seems possible to rule out such strategies by keeping Alice ignorant of the location of the regions $\hat{\mathcal{C}}_i$ before the beginning of the task, in which case she cannot coordinate actions with the intermediate regions. We leave better understanding this to future work, and for now rely on the gravitational reasoning of section 9.4 to provide a complete proof.

It is interesting to understand why the connected wedge theorem lacks a converse from the tasks perspective. There are two reasons. First, the mutual information being large does not imply $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ are entangled, instead they could just share classical correlation, which doesn't suffice to complete the task (see section 4.6). Second, even if there is sufficient entanglement between the regions, it doesn't imply that the boundary procedure will correspond to a bulk procedure which has a simple geometric description. This is associated with equation 8.1 being an inequality when we restrict to a low energy effective description in the bulk.

9.3 Quantum tasks loophole

In the last section we commented that if Alice can make use of the complementary regions $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$ in her protocol then it becomes possible to complete the $\hat{\mathbf{B}}_{84}$ task non-locally without large correlations between the input regions. In this appendix we briefly explain how this is possible.

The protocol is based on the quantum one-time pad (see section 3.2). Recall that a one-time pad is a set of unitaries $\{U_k\}_k$ such that averaging over k returns the maximally mixed state,

$$\frac{1}{|k|}\sum_k U_k \rho_A U_k^\dagger = \frac{\mathcal{I}}{d_A}, \tag{9.9}$$

for any ρ_A. For instance, when A is a single qubit, the Pauli set $\{P_k\} = \{\mathcal{I}, X, Y, Z\}$ works as a one-time pad.

To understand how to do the $\hat{\mathbf{B}}_{84}$ task non-locally and without correlation between $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$, define the state

$$|\psi\rangle = \frac{1}{|k|}\sum_k |k\rangle_{x_1} \otimes |k\rangle_{x_2} \otimes (\mathcal{I}\otimes P_k)|\Psi^+\rangle_{v_1v_2} \tag{9.10}$$

on $\mathbb{C}^4 \otimes \mathbb{C}^4 \otimes (\mathbb{C}^2)^{\otimes 2}$, where $|\Psi^+\rangle$ is the maximally entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$. Treating the two single-qubit subsystems as a composite four-dimensional subsystem, $|\psi\rangle$ is a three-party GHZ state for systems x_1, x_2, and v_1v_2.

The state $|\psi\rangle$ has zero mutual information between v_1 and v_2, but can still be used as a resource for the $\mathbf{B}_{84}$ task as follows. First, we send systems x_i to spacetime regions $\hat{X}_i$, and systems v_i to spacetime regions $\hat{\mathcal{V}}_i$ (cf. Figure 9.4). When the nonlocal circuit of Figure 4.2a is applied to the state $\mathcal{I}\otimes P_k|\Psi^+\rangle$, the classical measurement outcomes of the circuit are related to q and b in a way that depends on $P_k = X^m Z^n$, in particular $(-1)^b = (s_1)^q (s_2)^{1-q} s_3 (-1)^{m(1-q)+nq}$. If we apply the nonlocal circuit to $|\psi\rangle$ in systems v_1v_2, and measure $|\psi\rangle$ in the k-basis in the x_i subsystems, the combined classical output of both measurements is sufficient to complete the $\mathbf{B}_{84}$ task with zero information between v_1 and v_2.

Importantly, in the context of holography, the three-party GHZ entanglement between x_1, x_2 and v_1v_2 cannot be created by acting locally at c_1 and c_2, since $\hat{\mathcal{X}}_1$

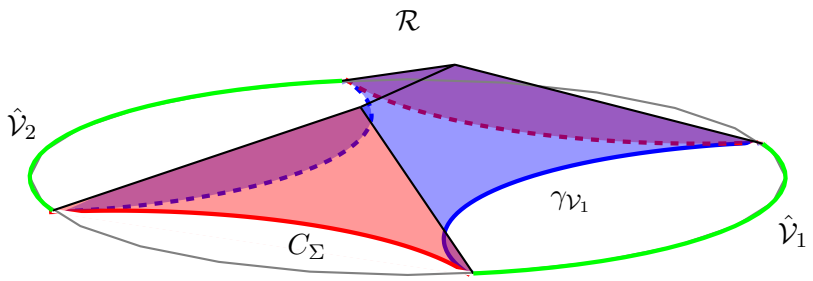


Figure 9.5: The null membrane. The blue surface is the lift $\mathcal{L}$, which is generated by the null geodesics defined by the inward, future pointing null normals to $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$, where $\gamma_{\mathcal{V}_i}$ is the Ryu-Takayanagi surface for region $\hat{\mathcal{V}}_i$. The red surfaces make up the slope $\mathcal{S}_\Sigma$, which is generated by the null geodesics defined by the inward, past directed null normals to $\gamma_{\mathcal{R}_1} \cup \gamma_{\mathcal{R}_2}$. The ridge $\mathcal{R}$ is where null rays from $\gamma_{\mathcal{V}_1}$ and $\gamma_{\mathcal{V}_2}$ collide. The contradiction surface C_Σ is where the slope meets a specified Cauchy surface Σ.

and $\hat{\mathcal{X}}_2$ are not in the future lightcone of either c_1 or c_2. Instead, the entanglement must already exist in the initial semi-classical state. It is not expected that this is ever the case.

9.4 Relativistic proof

In this section we prove the $2 \to 2$ connected wedge theorem for asymptotically AdS spacetimes. The proof relies on the null energy condition holding in the bulk.

The outline of the proof of Theorem 8 is as follows. We suppose, by way of contradiction, that $J_{12\to12} \neq \varnothing$ and the HRRT surface for region $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_1$ is disconnected. Call this surface $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$. According to the maximin procedure, this surface is minimal in some Cauchy slice Σ. We'll use the focusing theorem and the fact that $J^{\mathcal{E}}_{12\to12} \neq \varnothing$ to construct a smaller area surface in Σ which is connected, called the *contradiction surface* C_Σ. This provides a contradiction with $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$ having been the HRRT surface, showing the correct HRRT surface must be connected.

To begin, we consider two cases, corresponding to the boundary scattering

region

$$\hat{J}^{\mathcal{E}}_{12\to 12} = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^+(\hat{\mathcal{C}}_2) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2) = \hat{\mathcal{V}}_1 \cap \hat{\mathcal{V}}_2 \tag{9.11}$$

being empty or non-empty. If it is non-empty, then $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$ is a connected region, so its entanglement wedge is also connected and we are done. If it is empty, we proceed with the proof below.

Define the null surface

$$\mathcal{L} = \partial J^+(\mathcal{V}_1 \cup \mathcal{V}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \tag{9.12}$$

which we call the *lift*. This is defined by taking the inward pointing null orthogonal vectors of $\gamma_{\mathcal{V}_1}$ and $\gamma_{\mathcal{V}_2}$ as generators for a null congruence, and extending those geodesics until they reach the past of $\mathcal{R}_1$ or $\mathcal{R}_2$. Additionally, geodesics should not be extended past any caustic points — defining the lift in terms of $\partial J^+(\mathcal{V}_1 \cup \mathcal{V}_2)$ implements this for us, as geodesics leave the boundary of $J^+(\mathcal{V}_1 \cup \mathcal{V}_2)$ after developing a caustic.

There are two features of the lift that will be important. The first feature is that the region

$$\mathcal{R} = \partial J^+(\mathcal{V}_1) \cap \partial J^+(\mathcal{V}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2), \tag{9.13}$$

which we call the *ridge*, is non-empty. To see this, recall that by assumption $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$, which means

$$J^{\mathcal{E}}_{12\to 12} \subseteq J^+(\mathcal{V}_1) \cap J^+(\mathcal{V}_2) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \tag{9.14}$$

By assumption $J^{\mathcal{E}}_{12\to 12}$ is non-empty, so the region on the right is also non-empty. But this region being non-empty means $J^+(\mathcal{V}_1)$ and $J^+(\mathcal{V}_2)$ must meet in the past of $\mathcal{R}_1$ and $\mathcal{R}_2$, which means the ridge is non-empty.

The second important feature of the lift is that its boundary has a component $\mathcal{A}_1$ along $\partial J^-(\mathcal{R}_1)$ and a component $\mathcal{A}_2$ along $J^-(\mathcal{R}_2)$ which are separated by the ridge. The other possibility would be for the ridge to extend to one or more of the edges. This cannot occur however, which follows because the ridge is a

subregion of the bulk scattering region, which by assumption does not extend to the boundary.

Next define a second null sheet which we call the *slope*,

$$\mathcal{S}_\Sigma = \partial[J^-(\mathcal{R}_1) \cup J^-(\mathcal{R}_2)] \cap J^-[\partial J^+(\mathcal{V}_1 \cup \mathcal{V}_2)] \cap J^+(\Sigma). \tag{9.15}$$

The slope is generated by past-directed null geodesics beginning as the inward, past directed null normals to $\gamma_{\mathcal{R}_1}$ and $\gamma_{\mathcal{R}_2}$, and extended until they reach Σ. We will be particularly interested in

$$C_\Sigma \equiv S_\Sigma \cap \Sigma \tag{9.16}$$

which we introduced above as the contradiction surface. The lift, ridge, slope, and contradiction surface are shown in figure 9.5.

Now, we apply the focusing theorem in the form of equation 6.28 to the lift and to the slope. The lift is a portion of the boundary of the future of an extremal surface, $\partial J^+(\mathcal{V}_1)$, so the focusing theorem applies and $\theta \leq 0$ there. We choose a parameterization such that the null generators begin on $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$ and end on $\mathcal{R} \cup \mathcal{A}_1 \cup \mathcal{A}_2 \cup B_\mathcal{L}$, where $\mathcal{B}_\mathcal{L}$ is any caustics present in the lift. This leads to

$$\text{area}(\mathcal{A}_2) + \text{area}(\mathcal{A}_1) + 2\,\text{area}(B_\mathcal{L}) + 2\,\text{area}(\mathcal{R}) - \text{area}(\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}) = \int \epsilon\,\theta \leq 0. \tag{9.17}$$

Similarly, we can apply 6.28 to the slope, which is a portion of the boundary of the past of an extremal surface, $\partial[J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)]$, so again we have $\theta \leq 0$ there. Choosing the parameterization such that generators begin on $\mathcal{A}_1 \cup \mathcal{A}_2$ and end on $C_\Sigma \cup B_{S_\Sigma}$, where B_{S_Σ} is any caustics present in the slope. We have then

$$\text{area}(C_\Sigma) + 2\,\text{area}(B_{\mathcal{S}_\Sigma}) - \text{area}(\mathcal{A}_2) - \text{area}(\mathcal{A}_1) = \int \epsilon\theta \leq 0. \tag{9.18}$$

Adding these two inequalities and rearranging terms we obtain

$$\text{area}(\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}) \geq \text{area}(C_\Sigma) + 2[\text{area}(R) + \text{area}(B_{\mathcal{S}_\Sigma}) + \text{area}(B_{\mathcal{L}})] \tag{9.19}$$

$$\geq \text{area}(C_\Sigma) \tag{9.20}$$

This ensures that the disconnected surface $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$ is not of minimal area in the Cauchy slice Σ, so from the maximin procedure cannot be the correct HRRT surface, completing the proof.

We can also note that the proof gives a lower bound on the mutual information. In particular,

$$I(\hat{\mathcal{V}}_1 : \hat{\mathcal{V}}_2) = \frac{1}{4G_N}\left[\text{area}(\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}) - \text{area}(\gamma_{\mathcal{V}_1 \cup \mathcal{V}_2})\right] + O(1) \tag{9.21}$$

$$\geq \frac{1}{4G_N}\left[\text{area}(\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}) - C_\Sigma\right] + O(1) \tag{9.22}$$

$$\geq 2\mathcal{R}. \tag{9.23}$$

In the second line we used the maximin formula to compare the area of C_Σ and $\gamma_{\mathcal{V}_1 \cup \mathcal{V}_2}$, and in the third line we used 9.19. Notice that we also removed the terms coming from caustics, which in general are dependent on the choice of Cauchy surface Σ. We find that the area of the ridge lower bounds the mutual information. This means that not only does a non-empty scattering region imply an $O(1/G_N)$ mutual information, but a larger scattering region implies a larger mutual information.

9.5 The scattering region is inside the entanglement wedge

In the context of the connected wedge theorem with input and output regions taken to be points, the authors of [70] noted that the scattering region sits inside of the entanglement wedge of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$, at least in the context of $2+1$ bulk dimensions. We can straightforwardly adapt their argument to our context to see that the larger entanglement scattering region is also inside of the entanglement wedge, again in $2+1$ bulk dimensions.

To see this, define the region

$$X = \overline{J^+[\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2]^c \cap [\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2]^c}. \tag{9.24}$$

This is the closure of the spacelike complement of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$. In $2+1$ dimensions, this consists of the domains of dependence of two intervals which we call $\hat{\mathcal{X}}_1$ and $\hat{\mathcal{X}}_2$. Note that $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2 \cup \hat{\mathcal{X}}_1 \cup \hat{\mathcal{X}}_2$ is a complete Cauchy slice of the boundary, which we extend into the bulk to some Cauchy slice Σ. We will choose this extension such that γ_{X_1} and γ_{X_2} are contained in Σ.

Next we note that $\hat{\mathcal{R}}_1$ is inside the domain of dependence of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{X}}_1 \cup \hat{\mathcal{V}}_\in$, which we label $\hat{D}_1$, while $\hat{\mathcal{R}}_2$ sits inside the domain of dependence $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{X}}_2 \cup \hat{\mathcal{V}}_\in$, which we label $\hat{D}_2$. Because of this, $J^-(\mathcal{R}_1)$ will be inside $J^-(D_1)$, while $J^-(\mathcal{R}_2)$ will be inside $J^-(D_2)$. Consequently we learn

$$J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2) \subseteq J^-(D_1) \cap J^-(D_2). \tag{9.25}$$

Notice that, assuming the entanglement wedge $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$ is connected, the future boundary of $J^-(D_1) \cap J^-(D_2)$ is also the future boundary of $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$. This is because the entangling surface for $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$ consists of two components, one of which is homologous to $\hat{\mathcal{X}}_1$ and the other homologous to $\hat{\mathcal{X}}_2$, and so these two components are the entangling surfaces for $\hat{D}_1$ and $\hat{D}_2$ respectively. Thus equation 9.25 gives that $J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)$ is in the past of the future boundary of $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$. Since the scattering region is a subregion of $J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)$, it follows that this also holds for the scattering region.

It remains to show that the scattering region is to the future of the past boundary of $\mathcal{E}_W(\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2)$. This is immediate, because the past of γ_{X_1} and γ_{X_2} meets the boundary along the past boundaries of $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$. Thus any points in the future of $\mathcal{V}_1$ and $\mathcal{V}_2$ must be in the future of this past boundary.

Chapter 10

The $1 \to 2$ connected wedge theorem

This chapter reproduces the results of [67].

In this chapter we prove the $1 \to 2$ connected wedge theorem, which is a connection between bulk causal features and boundary entanglement which applies specifically in the context of AdS spacetimes with ETW branes. Such geometries are relevant to the emergence of spacetime [66, 94], holographic approaches to cosmology [10, 22, 41], and the black hole information problem [5, 6, 8, 20, 21, 36, 37, 80], where they model the formation of islands. In the island context, our theorem establishes that a causal connection from the black hole interior to the radiation system implies the existence of an island, a subject we take up in chapter 11.

10.1 Statement of the $1 \to 2$ connected wedge theorem

We state our main result of this chapter as follows.

Theorem 9 *(*$1 \to 2$ ***connected wedge theorem)*** *Consider three boundary regions* $\hat{\mathcal{C}}_1, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ *in an asymptotically AdS*$_{2+1}$ *spacetime with an end-of-the-world brane.*

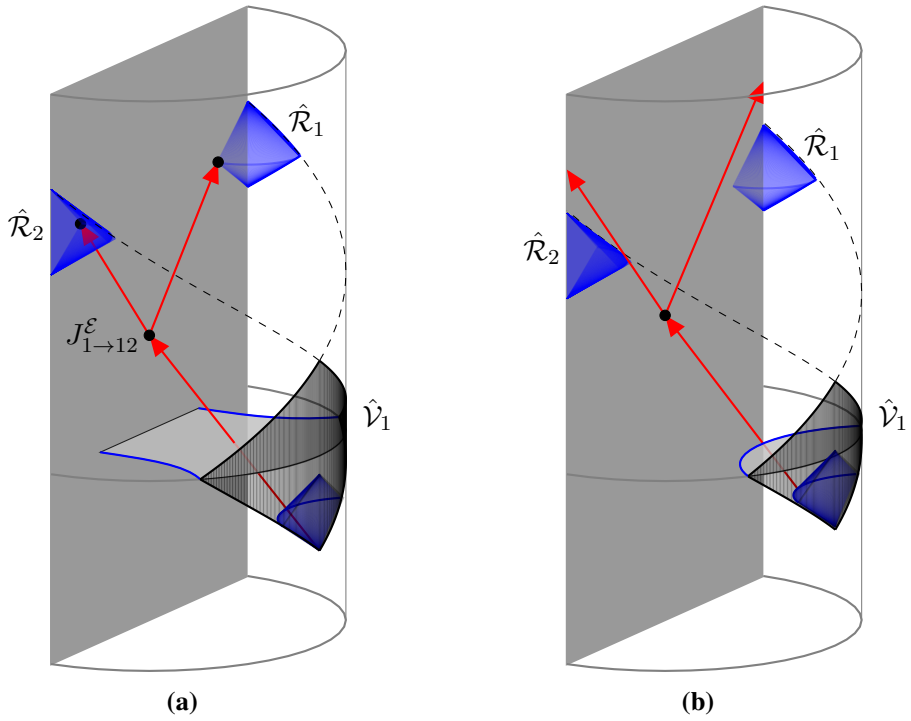


Figure 10.1: Illustration of Theorem 9, shown with a zero tension brane. The input region is taken to be a point $\mathcal{C}_1 = c_1$, while the output regions are the light blue half diamonds attached to the edge. The decision region $\hat{\mathcal{V}}_1$ is shown in black. a) When a boundary point c_1 and two edge points r_1, r_2 have a bulk scattering region which intersects the brane, the entanglement wedge of an associated domain of dependence (black shaded region) attaches to the brane. b) When there is no such scattering region, the entanglement wedge need not be connected.

Define the decision region

$$\hat{\mathcal{V}}_1 = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2). \tag{10.1}$$

Require that $\hat{\mathcal{C}}_1 \subseteq \hat{\mathcal{V}}_1$, and that $\hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ touch the brane. Define the entanglement scattering region,

$$J^{\mathcal{E}}_{1\to 12} = J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \tag{10.2}$$

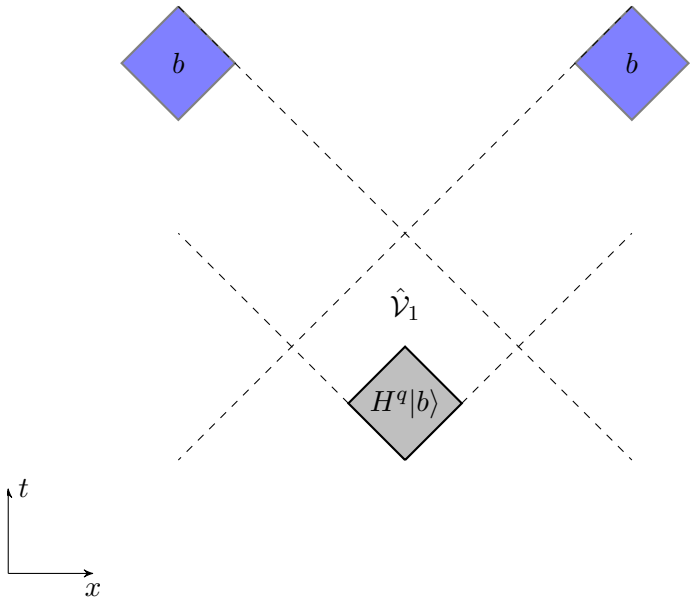


Figure 10.2: The **M** task, which we employ to argue for the $1 \to 2$ connected wedge theorem. At $\mathcal{C}_1$ the quantum system A is received which holds a state $H^q|b\rangle$. For the task to be completed successfully, b should be produced at both r_1 and r_2. We show that completing the task with a high success probability requires the bit q be available in the region $\hat{\mathcal{V}}_1 = J^+(\hat{\mathcal{C}}_1) \cap J^-(\hat{\mathcal{R}}_1) \cap J^-(\hat{\mathcal{R}}_2)$.

Then if $J^{\mathcal{E}}_{1\to 12}$ is non-empty, the entanglement wedge of $\hat{\mathcal{V}}_1$ is attached to the brane.

This theorem is illustrated in figure 10.1. Note that the converse of this theorem is not true, as we discuss in section 10.4.

10.2 Quantum tasks argument

In this section we give the quantum tasks argument for Theorem 9. Several aspects of the argument follow the argument of the $2 \to 2$ connected wedge theorem, but we emphasize that the qualitative picture of how the boundary completes the task is distinct in the two cases. In particular, in the $2 \to 2$ theorem the boundary uses a quantum non-local computation to complete the task, whereas in the $1 \to 2$ theorem the boundary employs bulk reconstruction, as we will see below.

The monogamy task

To argue for the $1 \to 2$ connected wedge theorem, we introduce a task called the *monogamy task*, which is related to but distinct from the $\mathbf{B}_{84}$ task. In this task there is one input region $\hat{\mathcal{C}}_1$ and two output regions $\hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$. System A is in one of the states $H^q|b\rangle_A$ and is localized to region $\hat{\mathcal{C}}_1$. H is the Hadamard operator, and $b, q \in \{0, 1\}$. There is an additional system Q which holds the bit q, and we leave unspecified for the moment where Q is located in spacetime. To complete the task the bit b should be localized to $\hat{\mathcal{R}}_1$ and $\hat{\mathcal{R}}_2$. This task is illustrated in figure 10.2.

We will need to introduce an equivalent formulation of $\mathbf{M}$ that we refer to as *purified* $\mathbf{M}$. The purified task is modified in two ways: (1) a second system $\bar{Q}$ is introduced, and placed in the maximally entangled state with Q; and (2) the input qubit $H^q|b\rangle_A$ is replaced with the A system of a maximally entangled state $|\Psi^+\rangle_{A\bar{A}}$. We refer to the $\bar{Q}\bar{A}$ system as the reference system. Notice that Bob can now perform measurements on the reference system to return this to the original task. To do this, Bob first measures the $\bar{Q}$ system, and obtains some output q. Then, he measures $\bar{A}$ in the computational basis if $q = 0$, and in the Hadamard basis if $q = 1$. Bob obtains one bit b of output. Meanwhile, the post-measurement state on QA is $|q\rangle_Q \otimes H^q|b\rangle_A$, so that the inputs are as in the unpurified task. Notice that Alice's success probability is unaffected whether Bob performs these measurements before or after Alice returns her outputs, since the QA and $\bar{Q}\bar{A}$ systems never interact. Thus, the purified and unpurified tasks have the same success probability.

The three regions $\hat{\mathcal{C}}_1, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ have a naturally associated spacetime region which we label $\hat{\mathcal{V}}_1$, defined according to

$$\hat{\mathcal{V}}_1 = J^+(\hat{\mathcal{C}}_1) \cap J^-(\hat{\mathcal{R}}_1) \cap J^-(\hat{\mathcal{R}}_2) \ . \tag{10.3}$$

$\hat{\mathcal{V}}_1$ is natural to consider because it is where it is possible to act on A and reach both of $\hat{\mathcal{R}}_1$ and $\hat{\mathcal{R}}_2$. We will be in particular interested in two situations: (1) the setting where Q is localized to $\hat{\mathcal{V}}_1$ and (2) the setting where Q is excluded from $\hat{\mathcal{V}}_1$.

Let us consider first the case where Q is localized to $\hat{\mathcal{V}}_1$. For convenience, take the unpurified task. Then within $\hat{\mathcal{V}}_1$ Alice should apply H^q to A to obtain $(H^q)^2|b\rangle_A = |b\rangle_A$, measure $|b\rangle_A$ in the $\{|0\rangle, |1\rangle\}$ basis, and then send the outcome

to each of r_1 and r_2. Doing so, she can complete the task with high probability, say $p_{\text{suc}} = 1 - \epsilon$. We introduce the parameter ϵ to account for the effect of any noise present in carrying out this protocol.

We can make a stronger statement by introducing a parallel repetition of the monogamy task, which we call $\mathbf{M}^{\times n}$. We consider n states $\{H^{q_i}|b_i\rangle\}_i$ being input at $\hat{\mathcal{C}}_1$, with the q_i and b_i drawn independently and at random. To complete the task, a fraction $1 - \delta$ of the b_i should be localized to both $\hat{\mathcal{R}}_i$. As discussed in the last paragraph, Alice can complete each of the n runs with a probability $p_{suc}(\mathbf{M}) = 1 - \epsilon$. For $\epsilon < \delta$, the probability that this leads to more than a fraction $1 - \delta$ of the runs being successful will be high. For concreteness take $\delta = 2\epsilon$. In this case we have, at large n,

$$p_{suc}(\mathbf{M}^{\times n}) = 1 - 2\epsilon^{2+n} \tag{10.4}$$

In particular we see that the success probability converges to 1 exponentially in n.

Next, consider the case where q is excluded from $\hat{\mathcal{V}}_1$. More precisely, we consider purified $\mathbf{M}$ and state this assumption as

$$I(\hat{\mathcal{V}}_1 : \bar{Q}) = 0 \ . \tag{10.5}$$

Then Alice will be limited in her ability to complete the task, a fact we formalize in the following lemma.

Lemma 13 *Consider the* $\mathbf{M}$ *task [cf. figure 10.2] with* $I(\hat{\mathcal{V}}_1 : \bar{Q}) = 0$*. Then any strategy for completing the task has* $p_{suc}(\mathbf{M}) \leq \cos^2(\pi/8)$.

To see why this is true, consider that Alice holds the A subsystem of a maximally entangled state on $A\bar{A}$ in the region $\hat{\mathcal{V}}_1$. After applying a quantum channel to A, she will send part of the output, call it B_1, to $\hat{\mathcal{R}}_1$ and part of the output, call it B_2, to $\hat{\mathcal{R}}_2$. At best, Alice will learn Q in the regions $\hat{\mathcal{R}}_i$. At each of the R_i then she can use B_i along with q to produce a guess for b. This is exactly the guessing game analyzed in [93], which we discussed in section 3.3. The above bound was stated there.

Notice that if B_1 and $\bar{A}$ are maximally entangled, Alice can measure in the q basis and produce an output at $\hat{\mathcal{R}}_1$ which is perfectly correlated with Bobs mea-

surement outcome. Similarly if $B_2\bar{A}$ is maximally entangled she can produce the correct output at $\hat{\mathcal{R}}_2$. The monogamy of entanglement however ensures that there will be a trade-off, and no perfect strategy will exist. This explains our naming convention $\mathbf{M}$ for the task.

We can also consider the parallel repetition of the task $\mathbf{M}^{\times n}$ in the case where $I(V:\bar{Q}) = 0$. Following the reasoning of Lemma 13, this can again be reduced to the monogamy of entanglement game, who proved that this parallel repetition of the task satisfies the following lemma.

Lemma 14 *Consider the $\mathbf{M}^{\times n}$ task with $I(\hat{\mathcal{V}}_1 : \bar{Q}) = 0$, and require that a fraction $1-\delta$ of the individual $\mathbf{M}$ tasks are successful. Then any strategy for completing the task has*

$$p_{suc} \leq \left(2^{h(\delta)} \cos^2\left(\frac{\pi}{8}\right)\right)^n \equiv \left(2^{h(\delta)}\beta\right)^n \tag{10.6}$$

where $h(\delta)$ is the binary entropy function $h(\delta) \equiv -\delta \log \delta - (1-\delta)\log(1-\delta)$ and the second equality defines β.

For small enough δ we have that $2^{h(\delta)}\beta < 1$, so that with zero mutual information the success probability is small. Our next result will be to show that a large success probability implies a large mutual information.

In fact, this argument was already completed in section 4.5, albeit in a changed setting. To apply the bond proven there to the present problem, the systems $\hat{\mathcal{V}}_1$ and $\bar{Q}$ in the $\mathbf{M}$ task play the role of systems $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$ for the $\mathbf{B}_{84}$ task. Applying lemma 11, we obtain

Lemma 15 *Suppose that the $\mathbf{M}^{\times n}$ task is completed with success probability $p_{suc} = 1 - 2\epsilon^{2+n}$. Then the bound*

$$\frac{1}{2} I(\hat{\mathcal{V}}_1 : \bar{Q}) \geq n(-\log 2^{h(2\epsilon)}\beta) - 1 + O((\epsilon/\beta)^n) \tag{10.7}$$

holds.

This will be the key technical result in the argument from quantum tasks for the connected wedge theorem, which we present in the next section.

We should highlight an important assumption made in proving Lemma 11. In addition to the region $\hat{\mathcal{V}}_1$, there is also a complementary region $X = [J^+(\hat{\mathcal{V}}_1) \cup J^-(\hat{\mathcal{V}}_1)]^c$. Lemma 14, on which Lemma 15 relies, assumes that information from this region is not made use of in Alice's protocol. If it were, one could use protocols of the type considered in section 9.3 to perform the $\mathbf{M}^{\times n}$ task without entanglement between $\hat{\mathcal{V}}_1$ and $\bar{Q}$. As discussed there, it seems sensible to assume such strategies are not allowed. In particular they require large amounts of GHZ type entanglement in the CFT, which is not expected to exist [72].

Tasks argument for the $1 \to 2$ connected wedge theorem

With Lemma 11 in hand, we are ready to complete the tasks argument for the $1 \to 2$ connected wedge theorem.

Theorem 9: *($1 \to 2$ **connected wedge theorem**) Consider three boundary regions $\hat{\mathcal{C}}_1, \hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ in an asymptotically AdS$_{2+1}$ spacetime with an end-of-the-world brane. Define the decision region*

$$\hat{\mathcal{V}}_1 = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2). \tag{10.8}$$

Require that $\hat{\mathcal{C}}_1 \subseteq \hat{\mathcal{V}}_1$, and that $\hat{\mathcal{R}}_1, \hat{\mathcal{R}}_2$ touch the brane. Define the entanglement scattering region,

$$J^{\mathcal{E}}_{1\to 12} = J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2). \tag{10.9}$$

Then if $J^{\mathcal{E}}_{1\to 12}$ is non-empty, the entanglement wedge of $\hat{\mathcal{V}}_1$ is attached to the brane.

Argument. Using our assumption that $J^{\mathcal{E}}_{1\to 12} \neq \varnothing$, we have that there exist bulk points c_1, r_1, r_2 such that

$$J^+(c_1) \cap J^-(r_1) \cap J^-(r_2) \cap \mathcal{B} \tag{10.10}$$

with $c_1 \in \mathcal{C}_1$, $r_1 \in \mathcal{R}_1, r_2 \in \mathcal{R}_2$, where recall $X = \mathcal{E}_W(\hat{X})$, with $\hat{X}$ a boundary region. We will consider a $\mathbf{M}^{\times n}$ task in the bulk such that the input system $A = A_1....A_n$ is input near c_1, and each bit b_i should be brought near r_1 and r_2. Further,

system Q will be recorded into the brane degrees of freedom.

It is easy to see that the $\mathbf{M}^{\times n}$ task can be completed in this case with high probability. To see this, note that a simple bulk strategy is to bring A to the brane, learn the q_i, and use them to recover the b_i. The b_i are then copied and sent to both r_1 and r_2. Doing so we can complete each $\mathbf{M}$ task with some probability $p = 1 - \epsilon$, leading to a success probability $p_{suc} = 1 - 2\epsilon^{2+n}$ for the $\mathbf{M}^{\times n}$ task. Since the boundary reproduces bulk physics, the boundary must also complete the task with the same probability. Lemma 11 then gives

$$\frac{1}{2} I(\hat{\mathcal{V}}_1 : \bar{Q}) \geq n(-\log 2^{h(2\epsilon)}\beta) - 1 + O((\epsilon/\beta)^n) \tag{10.11}$$

so that when the entanglement scattering region is non-empty, we have large mutual information.

This bound on mutual information actually requires the entanglement wedge of $\hat{\mathcal{V}}_1$ to attach to the brane. To see this, consider that in the purified $\mathbf{M}^{\times n}$ task there are n Bell pairs $|\Psi^+\rangle_{A_i\bar{A}_i}$ with $A = A_1...A_n$ input at $\mathcal{C}_1$, and $\bar{A} = \bar{A}_1...\bar{A}_n$ held by Bob. There are an additional n Bell pairs $|\Psi^+\rangle_{Q_i\bar{Q}_i}$, with $Q = Q_1...Q_n$ stored on the brane, and $\bar{Q} = \bar{Q}_1...\bar{Q}_n$ held by Bob. We can choose n to satisfy $O(1) < n < O(1/G_N)$, so that n grows as $G_N \to 0$ but does so more slowly than $1/G_N$.

Suppose that $\mathcal{E}_W(\hat{\mathcal{V}}_1)$ is not connected to the brane. Then the entropies of the region $\hat{\mathcal{V}}_1$ and of system $\bar{Q}$ satisfy

$$\begin{aligned} S(V) &= \frac{A_{dis}}{4G_N} + n + O(1), \\ S(\bar{Q}) &= n, \\ S(V\bar{Q}) &= \frac{A_{dis}}{4G_N} + 2n + O(1). \end{aligned} \tag{10.12}$$

The first statement is just our assumption: the disconnected surface calculates the entropy of $\hat{\mathcal{V}}_1$, and then we add the entropy of the n Bell pairs shared between $\hat{\mathcal{V}}_1$ and $\bar{A}$, along with any $O(1)$ contribution. The second statement is due to $Q\bar{Q}$ being in the maximally entangled state. The third statement follows from the disconnected surface being of minimal area along with our choice to take $n < O(1/G_N)$.

This is because the other option, of having the connected surface calculate the entropy, would imply that the quantum extremal surface has moved to enclose the n qubits of Q, which would happen only if $n > (A_{dis} - A_{con})/G_N$. Using these statements about the entropy, the mutual information is

$$I(\bar{Q} : V) = S(\bar{Q}) + S(V) - S(V\bar{Q}) = O(1), \tag{10.13}$$

so that in the disconnected phase the mutual information $O(1)$. Since 10.11 implies the mutual information is $O(n) > O(1)$, we find that the entanglement wedge must attach to the brane. ■

It is interesting to consider this result in the context of entanglement wedge reconstruction. We can observe that when the entanglement wedge connects to the brane Q is reconstructable from $\hat{\mathcal{V}}_1$. This clarifies how the boundary completes the task. Whenever the task can be completed in the bulk, the entanglement wedge connects to the brane, which means Q is available in $\hat{\mathcal{V}}_1$. Thus the boundary dynamics can recover the bits q_i and use them to decode the b_i, then forward the b_i to both output points.

We should contrast this boundary picture with the analogous feature of the connected wedge theorem in AdS/CFT. In that setting there are two input regions $\hat{\mathcal{V}}_1$ and $\hat{\mathcal{V}}_2$, with $\hat{\mathcal{V}}_1$ associated with the input $H^q|b\rangle$ and $\hat{\mathcal{V}}_2$ associated with the input q. In that case, even in the connected phase, $\hat{\mathcal{V}}_1$ does not reconstruct q. To complete the task then the boundary must make use of a different strategy. Indeed in [69] the authors argued that the boundary dynamics should be understood as a quantum non-local computation.

10.3 Relativistic proof

In this section we prove the $1 \to 2$ connected wedge theorem for asymptotically AdS spacetimes with an ETW brane. Our proof follows the earlier proof for the $2 \to 2$ connected wedge theorem appearing in section 9.4 closely, since a minor modification of the proof given there suffices to prove our theorem. We repeat the full proof in order to explain this modification clearly.

The proof relies on three assumptions: i) that the null energy condition holds in the bulk ii) that the null energy condition holds for the branes stress tensor iii)

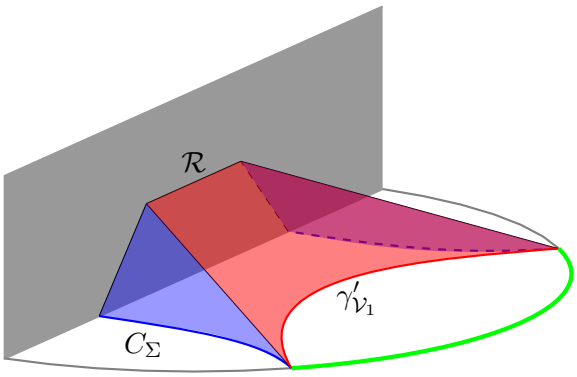


Figure 10.3: The null membrane. The red surface is the lift $\mathcal{L}$, the blue surfaces make up the slope. The ridge $\mathcal{R}$, is where the lift meets the brane.

that the maximin procedure [62, 97] for finding HRRT surfaces is correct even in the context of AdS/BCFT.

Given these assumptions, the outline of the proof of Theorem 9 is as follows. We suppose, by way of contradiction, that $J_{1\to 12} \neq \varnothing$ and the HRRT surface for region $\hat{\mathcal{V}}_1$ is brane-detached. Call this surface $\gamma'_{\mathcal{V}_1}$. According to the maximin procedure, this surface is minimal in some Cauchy slice Σ. We'll use the focusing theorem and the fact that $J^{\mathcal{E}}_{1\to 12} \neq \varnothing$ to construct a smaller area surface in Σ which is brane-connected, called the *contradiction surface* C_Σ. This provides a contradiction with $\gamma'_{\mathcal{V}_1}$ having been the HRRT surface, showing the correct HRRT surface must be brane-attached.

To begin, we consider two cases, corresponding to the boundary scattering region

$$\hat{J}^{\mathcal{E}}_{1\to 12} = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_2) \cap \mathcal{B} = \hat{\mathcal{V}}_1 \cap \mathcal{B} \tag{10.14}$$

being empty or non-empty. If it is non-empty, then $\hat{\mathcal{V}}_1$ is attached to the brane in the boundary, so its entanglement wedge is immediately brane attached and we are done. If it is empty, we proceed with the proof below.

Define the null surface

$$\mathcal{L} = \partial J^+(\mathcal{V}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2) \tag{10.15}$$

which we call the *lift*. This is defined by taking the inward pointing null orthogonal vectors of $\mathcal{E}_V$ as generators for a null congruence, and extending those geodesics until they reach the past of $\mathcal{R}_1$ or $\mathcal{R}_2$. Additionally, geodesics should not be extended past any caustic points — defining the lift in terms of $\partial J^+(\mathcal{V}_1)$ implements this for us, as geodesics leave the boundary of $J^+(\mathcal{V}_1)$ after developing a caustic.

There are two features of the lift that will be important. The first feature is that the lift has a non-empty intersection with the brane. To see this, recall that by assumption

$$J^{\mathcal{E}}_{1\to 12} = J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2) \cap \mathcal{B} \neq \varnothing. \tag{10.16}$$

Then, recall that since $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$, we have also $\mathcal{C}_i \subseteq \mathcal{V}_i$. Thus we learn

$$J^{\mathcal{E}}_{1\to 12} \subseteq J^+(\mathcal{V}_1) \cap J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2) \cap \mathcal{B} \neq \varnothing. \tag{10.17}$$

This gives that $J^+(\mathcal{V}_1)$ meets the brane while in the past of $\mathcal{R}_1$ and $\mathcal{R}_2$. In particular then the ridge, defined by

$$\mathcal{R} \equiv \mathcal{L} \cap \mathcal{B} \neq \varnothing. \tag{10.18}$$

is non-empty.

The second important feature of the lift is that its boundary has a component $\mathcal{A}_1$ along $\partial J^-(\mathcal{R}_1)$ and a component $\mathcal{A}_2$ along $J^-(\mathcal{R}_2)$ which are separated by the ridge. The other possibility would be for the ridge to extend to one or more of the edges. This cannot occur however, which follows because the ridge is a subregion of the bulk scattering region, which by assumption does not extend to the boundary.

Next define a second null sheet which we call the *slope*,

$$\mathcal{S}_\Sigma = \partial[J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)] \cap J^-[\partial J^+(\mathcal{V}_1)] \cap J^+(\Sigma). \tag{10.19}$$

The slope is generated by past-directed null geodesics beginning as the inward, past directed null normals to $\gamma_{\mathcal{R}_1}$ and $\gamma_{\mathcal{R}_2}$, and extended until they reach Σ. We

will be particularly interested in

$$C_\Sigma \equiv S_\Sigma \cap \Sigma \tag{10.20}$$

which we introduced above as the contradiction surface. The lift, ridge, slope, and contradiction surface are shown in figure 10.3.

Now, we apply the focusing theorem in the form of equation 6.28 (which includes the additional boundary term) to the lift and to the slope. The lift is a portion of the boundary of the future of an extremal surface, $\partial J^+(\mathcal{V}_1)$, so focusing applies. We choose a parameterization such that the null generators begin on $\gamma_{\mathcal{V}_1}$ and end on $\mathcal{R} \cup \mathcal{A}_1 \cup \mathcal{A}_2 \cup B_\mathcal{L}$, where $\mathcal{B}_\mathcal{L}$ is any caustics present in the lift. This leads to

$$\text{area}(\mathcal{A}_2) + \text{area}(\mathcal{A}_1) + 2\,\text{area}(B_\mathcal{L}) + \text{area}(R) - \text{area}(\gamma'_{\mathcal{V}_1}) = \int \epsilon\,\theta \leq 0. \tag{10.21}$$

Similarly, we can apply 6.27 to the slope, which is a portion of $\partial[J^-(\mathcal{R}_1) \cap J^-(\mathcal{R}_2)]$. Choosing the parameterization such that generators begin on $\mathcal{A}_1 \cup \mathcal{A}_2$ and end on $C_\Sigma \cup B_{S_\Sigma}$, where B_{S_Σ} is any caustics present in the slope. We have then

$$\text{area}(C_\Sigma) + 2\text{area}(B_{\mathcal{S}_\Sigma}) - \text{area}(\mathcal{A}_2) - \text{area}(\mathcal{A}_1) + \int_{S_\Sigma \cap \mathcal{B}} d^{d-2}x\,\sqrt{\gamma} n_\lambda = \int \epsilon\theta \leq 0.$$

Adding these two inequalities and rearranging terms we obtain

$$\begin{aligned}\text{area}(\gamma'_{\mathcal{V}_1}) &\geq \text{area}(C_\Sigma) + \text{area}(R) + \text{area}(B_{\mathcal{S}_\Sigma}) + \text{area}(B_\mathcal{L}) + \int_{S_\Sigma \cap \mathcal{B}} d^{d-2}x\,\sqrt{\gamma} n_\lambda, \\ &\geq \text{area}(C_\Sigma)\end{aligned} \tag{10.22}$$

where we've used that $n_\lambda \geq 0$, as shown in section 6.3. This ensures that the brane-disconnected surface $\gamma'_{\mathcal{V}_1}$ is not of minimal area in the Cauchy slice Σ, so from the maximin procedure cannot be the correct HRRT surface, completing the proof.

We should highlight the modifications made from the similar proof of the $2 \to 2$ connected wedge theorem. In that case, there were four regions $\mathcal{C}_1, \mathcal{C}_2, \mathcal{R}_1$ and $\mathcal{R}_2$, and two in-regions $\mathcal{V}_1$ and $\mathcal{V}_2$. The lift was formed by a null congruence of geodesics starting on $\gamma_{\mathcal{V}_1} \cup \gamma_{\mathcal{V}_2}$. Points on the ridge corresponded to where a geodesic starting on $\gamma_{\mathcal{V}_1}$ collided with a geodesic starting on $\gamma_{\mathcal{V}_2}$, whereas in our setting the ridge is formed by generators from $\gamma'_{\mathcal{V}_1}$ colliding with the brane. Another distinction is the occurrence of the boundary $S_\Sigma \cap \mathcal{B}$ and associated term in 10.22. This is handled in our case by assuming the NEC holds for the brane stress tensor.

10.4 Comments on the $1 \to 2$ connected wedge theorem

The scattering region is inside the entanglement wedge

In the context of the $2 \to 2$ theorem, section 9.5 showed that the scattering region $J_{12\to12}$ is inside of the entanglement wedge of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$. It is straightforward to adapt either of the proofs given there to the $1 \to 2$ theorem, where the analogous statement is that $J^{\mathcal{E}}_{1\to12}$ is inside the entanglement wedge of $\hat{\mathcal{V}}_1$. Since $J^{\mathcal{E}}_{1\to12}$ lives in the brane, we can be more specific and say that $J^{\mathcal{E}}_{1\to12}$ is inside the island formed by $\mathcal{V}_1 \cap \mathcal{B}$.

Relationship to $2 \to 2$ theorem and interface branes

It is possible to describe ETW brane geometries as a $\mathbb{Z}_2$ identification of an interface brane geometry. In particular, consider a spacetime $\mathcal{M}$ described by metric $g_{\mu\nu}(x^\mu)$ and satisfying the boundary condition

$$K_{ab} - K h_{ab} = -8\pi G_N T^{\mathcal{B}}_{ab} \tag{10.23}$$

at the ETW brane. Then we can define a doubled geometry featuring an interface brane, with metric $g_{\mu\nu}(x^\mu_+)$ on one side of the brane and a copy of that metric $g_{\mu\nu}(x^\mu_-)$ on the other. At the interface brane Einsteins equations require we satisfy

the Israel junction conditions

$$h^+_{ab} = h^-_{ab}, \tag{10.24}$$

$$[K^+_{ab} - K^-_{ab}] - [K^+ - K^-]h_{ab} = -8\pi G_N T^I_{ab}. \tag{10.25}$$

Setting $T^I_{ab} = 2T^B_{ab}$ satisfies this condition. Identifying points $x_+ = x_-$ then recovers the ETW brane geometry.

We can apply the $2 \to 2$ connected wedge theorem to this interface brane geometry, and in limited cases recover the $1 \to 2$ theorem. To do this choose $\hat{\mathcal{C}}_1$ and $\hat{\mathcal{C}}_2$ to be mirror images across the interface brane. Choose $\hat{\mathcal{R}}_1$ and $\hat{\mathcal{R}}_2$ to be intervals centered on the two CFT interfaces. Notice that the brane anchored scattering region $J^{\mathcal{E}}_{1\to 12}$ is not empty if and only if the bulk scattering region $J^{\mathcal{E}}_{12\to 12}$ in the interface geometry is not empty. Further, the entanglement wedge of $\hat{\mathcal{V}}_1 \cup \hat{\mathcal{V}}_2$ will be connected if and only if the entanglement wedge of $\hat{\mathcal{V}}_1$ connects to the brane in the ETW brane geometry. Thus, when the doubled geometry satisfies the conditions for the $2 \to 2$ theorem — in particular when the NEC holds in the doubled geometry — the $1 \to 2$ theorem follows from the $2 \to 2$ theorem.

Recall however the conditions for the $1 \to 2$ theorem: the bulk stress tensor and brane stress tensor should separately satisfy the NEC. There are many cases where these conditions hold, but in the associated interface brane geometry the NEC is violated. Consider for instance an ETW brane solution with

$$\begin{aligned} T_{\mu\nu} &= 0, \\ T^{\mathcal{B}}_{ab} &= -T h_{ab}. \end{aligned} \tag{10.26}$$

Then in the interface brane geometry the stress tensor is

$$T^{\mu\nu}_I = -T h^{ab} e^\mu_a e^\nu_b \, \delta(x - x_0) \tag{10.27}$$

where the delta function is turned on at the interface. To study the NEC for $T^I_{\mu\nu}$, it's convenient to rewrite this using the completeness relation,

$$g^{\mu\nu} = n^\mu n^\nu + h^{ab} e^\mu_a e^\nu_b \tag{10.28}$$

so that

$$T_I^{\mu\nu}\ell_\mu\ell_\nu = -T(g^{\mu\nu} - n^\nu n^\mu)\ell_\mu\ell_\nu = T(n^\mu\ell_\mu)^2 \tag{10.29}$$

We see that the NEC is satisfied if and only if $T > 0$. However, in the ETW brane geometry, the $1 \to 2$ theorem holds even for $T < 0$. Consequently we find that the $2 \to 2$ theorem applied to the interface geometry only recovers the $1 \to 2$ theorem in special cases.

Counterexample to the converse

We claimed in section 10.1 that the converse to Theorem 9 is false. In figure 10.4, we gave a counterexample to the converse of the $2 \to 2$ theorem. By taking a $\mathbb{Z}_2$ identification of the solution used in there it is straightforward to construct a counterexample to the converse of the $1 \to 2$ theorem. This is shown in figure 10.4a.

The out regions are not entangled

In the $2 \to 2$ connected wedge theorem, time reversal implies that in addition to the 'in' regions having a connected entanglement wedge, the 'out' regions do as well, where the out regions are defined by[1]

$$\begin{aligned}\hat{\mathcal{W}}_1 &= J^-(\hat{\mathcal{R}}_1) \cap J^+(\hat{\mathcal{C}}_1) \cap J^+(\hat{\mathcal{C}}_2)\\ \hat{\mathcal{W}}_2 &= J^-(\hat{\mathcal{R}}_2) \cap J^+(\hat{\mathcal{C}}_1) \cap J^+(\hat{\mathcal{C}}_2).\end{aligned} \tag{10.30}$$

In the context of the $1 \to 2$ theorem one can define similar 'out' regions. To do so, we define points x_1, x_2 as the points where $\partial\hat{J}^+(\hat{\mathcal{C}}_1)$ reaches edge 1 and edge 2, respectively. Then we define

$$\begin{aligned}\hat{\mathcal{W}}_1' &= \hat{J}^+(x_1) \cap J^-(\hat{\mathcal{R}}_1)\\ \hat{\mathcal{W}}_2' &= \hat{J}^+(x_2) \cap J^-(\hat{\mathcal{R}}_2).\end{aligned} \tag{10.31}$$

[1] We are interested here in the case where $\hat{W}_i \subseteq \hat{\mathcal{R}}_i$, analogous to our condition $\hat{\mathcal{C}}_i \subseteq \hat{\mathcal{V}}_i$ on the in regions.

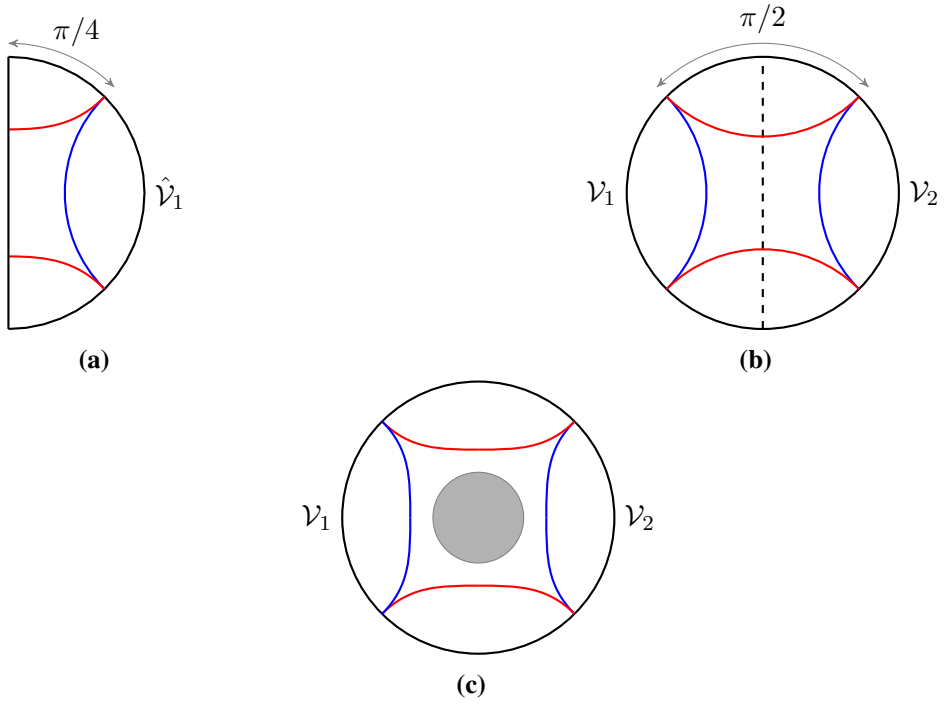


Figure 10.4: A counterexample to the converse of Theorem 9. (a) A constant time slice of a solution with a $T = 0$ brane sitting in pure AdS. We choose a region $\hat{\mathcal{V}}_1$ of size $\pi/2$ and which is centered between the two edges. This region sits exactly on the phase transition between brane-attached (red surface) and brane detached (blue surface), and the scattering region consists of a single point. (b) The $T = 0$ solution can be viewed as a $\mathbb{Z}_2$ identification of global AdS with the identification across $\rho = 0$. (c) In the unfolded geometry, we consider adding a spherically symmetric matter distribution (shown in grey). This delays light rays travelling from c_1 to the brane by some finite amount, closing the scattering region. Due to spherical symmetry, the region $\hat{\mathcal{V}}_1$ remains on the phase transition. Increasing its size infinitesimally then keeps the scattering region closed, while also ensuring the red, brane-attached surface is minimal.

We can ask if $\hat{\mathcal{W}}_1'$ and $\hat{\mathcal{W}}_2$ must also be entangled when the entanglement scattering region is non-empty.

In fact, these out regions do not need to be entangled. For an explicit counterexample, begin with the example shown in figure 10.4a, where $\hat{\mathcal{V}}_1$ consists of an interval of size $\pi/2$ centered between the two edges. Then the scattering region consists of a single point, and the minimal surface enclosing $\hat{\mathcal{W}}_1' \cup \hat{\mathcal{W}}_2$ is on the transition from giving a connected and disconnected entanglement wedge. Now decrease the tension, moving the brane inward. This shortens the light travel time from $\hat{\mathcal{C}}_1$, so increases the size of the scattering region. Meanwhile, the disconnected surface enclosing $\hat{\mathcal{W}}_1 \cup \hat{\mathcal{W}}_2$ loses area and becomes dominant, so that there is a non-empty scattering region but only $O(1)$ correlation between the out regions.

$1 \to 1$ theorem

For completeness, we also point out a $1 \to 1$ connected wedge theorem, which follows from a simple tasks argument or from geometric observations. We consider two regions $\hat{\mathcal{C}}_1, \hat{\mathcal{R}}_1$, both in the AdS boundary. We define the scattering region,

$$J^{\mathcal{E}}_{1\to 1} = J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1) \cap \mathcal{B}, \tag{10.32}$$

and the input region,

$$\hat{\mathcal{V}}_1 = \hat{J}^+(\hat{\mathcal{C}}_1) \cap \hat{J}^-(\hat{\mathcal{R}}_1). \tag{10.33}$$

By analogy with the $1 \to 2$ theorem, we expect that $J^{\mathcal{E}}_{1\to 1}$ being non-empty implies the entanglement wedge of $\hat{\mathcal{V}}_1$ is brane-attached. To verify this, we can give both a tasks and geometric argument.

From tasks, we consider an input $H^q|b\rangle_A$at $\mathcal{C}_1$ and output b at $\mathcal{R}_1$, with q recorded into the brane degrees of freedom. If $J^{\mathcal{E}}_{1\to 1}$ is non-empty, then one can use a simple bulk strategy: travel to the brane, learn q, then send q to the output point where it can be used to undo H^q and recover b. In the bulk picture knowing q is necessary to successful recover b, so $\hat{\mathcal{V}}_1$ must know q, so $\hat{\mathcal{V}}_1$ must have the brane in its entanglement wedge.[2].

[2]A more rigorous argument for this would follow the strategy of section 10.2.

To understand this from the geometric perspective, note that $J^+(\mathcal{C}_1) \cap J^-(\mathcal{R}_1)$ is inside the entanglement wedge of $\hat{\mathcal{V}}_1$, so $J^{\mathcal{B}}_{1\to 1}$ non-empty means the brane is inside the entanglement wedge of $\hat{\mathcal{V}}_1$.

Chapter 11

Islands and the connected wedge theorem

In this chapter we point out that, in certain models, the $1 \to 2$ connected wedge theorem reveals the existence of *islands* in the Ryu-Takayanagi formula. Islands are disconnected components of entanglement wedges, and have proven essential to the correct calculation of black hole entropy and have advanced the understanding of the black hole information problem. The $1 \to 2$ theorem provides a novel perspective on these topics.

11.1 Islands in the Ryu-Takayanagi formula

Recall that the complete RT formula states that

$$S(A) = \max_{\Sigma} \min_{\gamma_A \in \Sigma} \left(\frac{\text{Area}[\gamma_A]}{4G_N} + S_{QFT}(\mathcal{E}_W(A)) \right) \tag{11.1}$$

When the entropy of bulk matter fields is small, with some finely tuned exceptions, this is well approximated by

$$S(A) \approx \max_{\Sigma} \min_{\gamma_A \in \Sigma} \left(\frac{\text{Area}[\gamma_A]}{4G_N} \right) + S_{QFT}(\mathcal{E}_W(A)) \tag{11.2}$$

a fact we made use of above in discussing the entanglement wedge. When the entropy of bulk matter fields becomes large however, in particular $O(1/G_N)$, the bulk matter entropy term can affect the position of the quantum extremal surface γ_A. In this case the above approximation fails.

This shifting of the quantum extremal surface plays an important role in the understanding of black hole evaporation [7, 75]. To understand this, consider an asymptotically AdS Schwarschild black hole. The black hole releases Hawking radiation, which travels towards the AdS boundary. We set absorbing boundary conditions at the boundary, and store the escaped Hawking quanta in an external system which we will call the *radiation system*, labelled R. Then we ask, what is the entanglement wedge of the radiation system?

This is a somewhat unusual system to calculate the entanglement wedge of, since it is not part of the AdS boundary. Nonetheless we can apply the RT formula, we just need to be careful to satisfy the homology constraint correctly. Since A, the portion of the boundary included in the radiation system, is empty, we actually need

$$\partial S = \gamma_R \tag{11.3}$$

That is, γ_R should be a closed surface. This means the entanglement wedge of R, which is just the domain of dependence of S, will not be attached to the AdS boundary. For this reason entanglement wedges such as this one are called *islands*.

Lets begin by considering early times, where only $O(1)$ Hawking quanta have reached the radiation system. Then, the minimal quantum extremal surface homologous to R will just be the empty surface. This has zero area, and an empty entanglement wedge. The entropy of the radiation system will just be the $O(1)$ value of the entropy of the Hawking quanta that sit inside of it. As more quanta reach the radiation system, the entropy will increase.

Next, consider late times, where $O(1/G_N)$ Hawking quanta have reached the radiation system. The Hawking quanta in the radiation system are entangled with the interior of the black hole. When there are many quanta, we may get a reduced generalized entropy by taking a non-empty surface γ_R. This will enclose some portion of the black hole interior. Then, the entanglement wedge is no longer

empty — it consists of an island inside of the black hole. From our discussion in section 7.3, this reveals that information inside of the island can be recovered by acting on the escaped Hawking radiation. Now, as more and more Hawking quanta reach the radiation system, more and more of the radiation system is pure, and the entropy of the Hawking quanta actually decreases. This reproduces the characteristic behaviour for the entropy of a black hole predicted by Page [74].

To make the discussion above precise, the most challenging component is finding the location of the quantum extremal surface after the transition. [75] was able to argue for the existence of the non-empty candidate surface and for the transition described above. Another approach which affords better analytic control, but relies on analogue models instead of 4 dimensional black holes as in [75], is to consider a holographic BCFT. By making some appropriate choices outlined below, the edge degrees of freedom can be dual to a brane with the geometry of a black hole. The CFT then serves as the radiation system — degrees of freedom in the edge interact with the CFT and information escapes the black hole. This is the model we consider here.

11.2 The black hole and the radiation system

We will focus on the solutions described in section 6.1, which have a constant tension brane ending a pure, global, AdS_{2+1} spacetime. Recall that this was described by a metric

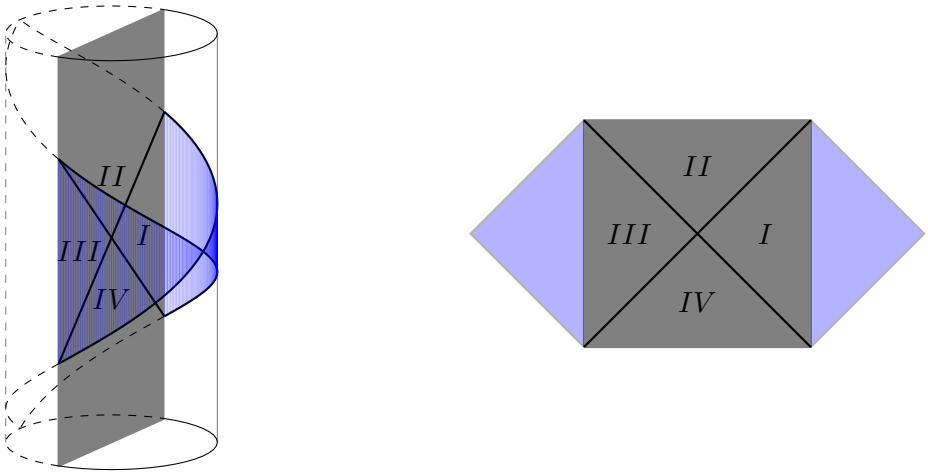
$$ds^2_{d+1} = \cosh^2 \rho \, ds^2_{1+1} + d\rho^2 \tag{11.4}$$

with the brane sitting at constant $\rho_0 = \text{arctanh}(T)$. We will use the coordinates (ν, σ) on the brane, with metric

$$ds^2_{1+1} = \frac{-d\nu^2 + d\sigma^2}{\cos^2 \sigma} \tag{11.5}$$

We are most interested in the case where $T \approx 1$, since in this case there is an effective, lower dimensional description of gravity in the brane [78].

For constant tension solutions light rays run tangent to the brane. This allows us to define horizons in the brane by choosing points r_1 and r_2 on the edge, and



(a) **(b)**

Figure 11.1: Choosing an appropriate Poincaré patch of the global spacetime, we find a two-sided black hole geometry (on the brane) coupled to two flat regions (wedges of the CFT). The end points of the two flat regions are coupled in the global picture. Note that we are most interested in the case where $T \approx 1$ and gravity localizes to the brane. We have drawn the $T = 0$ case however to simplify the diagram.

considering their forward light cones,

$$H_1 = [\partial J^+(r_1)]_{\mathcal{B}},$$
$$H_2 = [\partial J^+(r_2)]_{\mathcal{B}}. \tag{11.6}$$

These horizons intersect at $p_{\mathcal{B}} = (\sigma = 0, \nu = 0)$. From these horizons, define regions $I - IV$ as in figure 11.1. Region II is the black hole interior, while I and IV are the right and left exteriors.

To make the black hole features of these constant tension brane solutions more explicit, consider going to the Poincaré patch shown in figure 11.1a. This patch includes the entire black hole, along with two wedge shaped portions of the CFT and a portion of the AdS bulk. Forgetting the bulk and focusing on the brane coupled to CFT, we have the spacetime shown in figure 11.1b.

Recall from section 6.1 that explicitly the Poincaré patch is described by a

metric

$$ds^2 = \frac{\ell^2}{z^2}(-dt^2 + dx^2 + dz^2) \tag{11.7}$$

with brane located at

$$x^2 - t^2 + (z + \tan\Theta)^2 = \sec^2\Theta, \tag{11.8}$$

where Θ is related to the tension T according to $T = \sin\Theta$. The Poincaré patch includes only the $-\pi/2 < \nu < \pi/2$ portion of the brane. The points r_1 and r_2 are mapped to $x = t = -\infty$ and $-x = t = -\infty$.

In Poincaré coordinates the edge trajectory is $x = \pm\sqrt{1 + t^2}$. These trajectories asymptote to the light rays $x = \pm t$. Mapping the horizons $v = \pm\sigma$ to Poincaré we find horizons

$$z = \frac{1 - \sin\Theta}{\cos\Theta} \quad , \quad x = \pm t. \tag{11.9}$$

One can also verify directly in the Poincaré geometry that these are the horizons by studying null geodesics in the brane geometry [80].

Next we should identify the radiation system. The entire CFT is coupled to the black hole at the two edges, and information can escape from the black hole into anywhere in the CFT. It seems sensible however to not consider the portion of the CFT which reconstructs the black hole exterior regions as being part of the radiation system. It is straightforward to identify the CFT dual to the left and right exterior black hole regions. The interval $Y_1 = \{\sigma \in (-\pi/2, 0), \nu = 0\}$ has region I inside its entanglement wedge. Similarly the interval $Y_2 = \{\sigma \in (0, \pi/2), \nu = 0\}$ has region II inside its entanglement wedge. This excludes $D(Y_1)$ and $D(Y_2)$ from the radiation system.

The remaining portion of the CFT is the future and past of the point

$$x = (\nu = 0, \sigma = 0, \rho = \infty). \tag{11.10}$$

The future of x reconstructs region II of the brane, so we should identify this with the radiation system. To specify that radiation has been collected only up until a

certain time, we can choose a second point c_1 and define

$$\hat{R} = J^+(x) \cap J^-(c_1). \tag{11.11}$$

For c_1 at an early time so that R is small, the entanglement wedge of R will be disconnected from the brane, and R does not see inside of the black hole. At late enough times though, $\mathcal{E}_W(R)$ connects to the brane. Where this transition occurs will be controlled by the connected wedge theorem. Note also that since the minimal surfaces are at constant σ, they will in fact lie exactly on the horizons. This is illustrated in figure 11.2.

11.3 The connected wedge theorem and behind the horizon

Finally, we can apply the connected wedge theorem to this black hole on the brane. In fact, we need a time reversed variant of the theorem, which follows immediately from Theorem 9 (we also specialize to the case where the in and out regions are points),

Theorem 10 *(*$1 \to 2$ ***connected wedge theorem)*** *Consider three points r_1, r_2, c_1 in an asymptotically AdS$_{2+1}$ spacetime with an end-of-the-world brane, with c_1 in the boundary and r_1, r_2 on the edge. Then if*

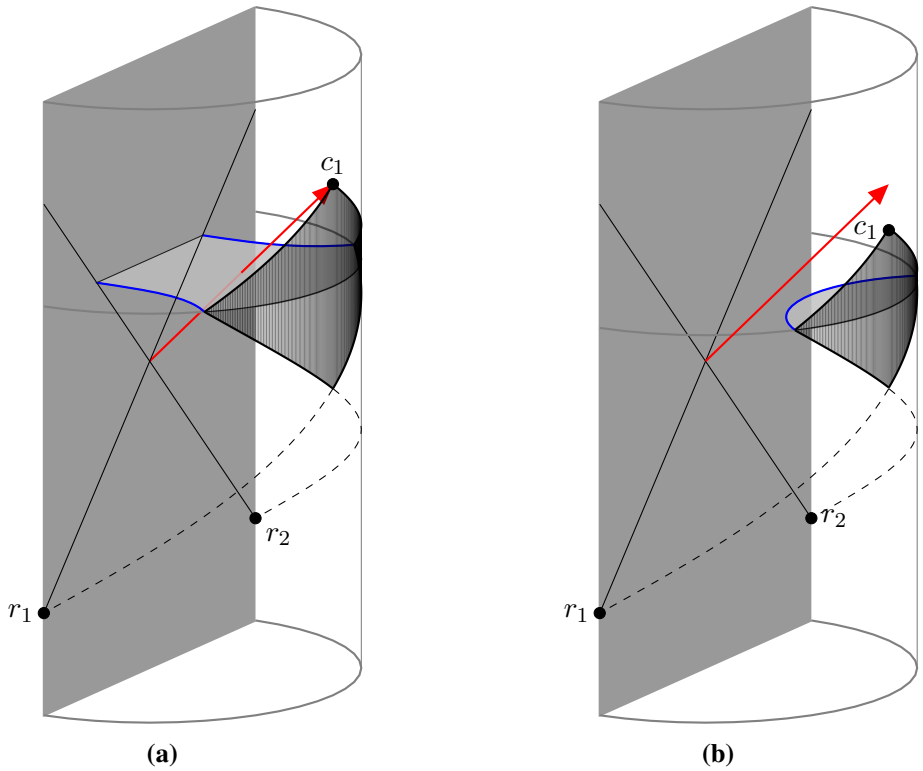
$$J_{12\to 1} = J^+(r_1) \cap J^+(r_2) \cap J^-(c_1) \tag{11.12}$$

is non-empty, the entanglement wedge of

$$\hat{R} = \hat{J}^+(r_1) \cap \hat{J}^+(r_2) \cap \hat{J}^-(c_1) \tag{11.13}$$

is attached to the brane.

The two input points of the theorem we identify with the points r_1 and r_2 we used above to define the black hole horizons H_1 and H_2. The region $\hat{\mathcal{V}}_1$ becomes the subsystem of the radiation which has been collected since $J^+(r_) \cap J^+(r_2) = J^+(x)$.



(a) **(b)**

Figure 11.2: Theorem 9 along with time reversal implies a $2 \to 1$ connected wedge theorem. We can view the light rays beginning at r_1 and r_2 as defining the horizons of a black hole. The region $\hat{\mathcal{V}}_1$ is then the radiation system. (a) When a light ray reaches $\hat{\mathcal{V}}_1$ from the black hole interior, the entanglement wedge of $\hat{\mathcal{V}}_1$ must connect to the brane, so that $\hat{\mathcal{V}}_1$ reconstructs a portion of the interior. (b) When the black hole is causally disconnected from the black hole interior, the entanglement wedge of $\hat{\mathcal{V}}_1$ may be disconnected from the brane.

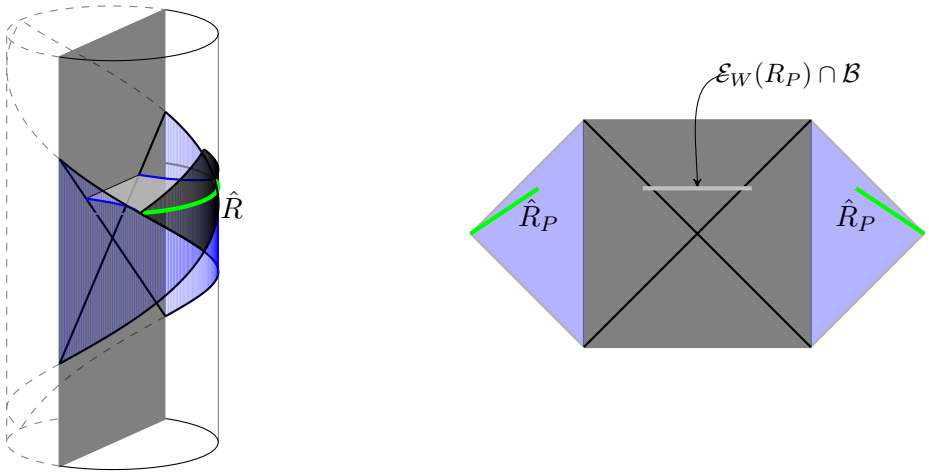


Figure 11.3: (a) The radiation system R (time-slice in green) picked out by the connected wedge theorem sits outside the Poincaré patch. (b) A nearby region $\hat{R}_P$ inside the patch has $\hat{R}_1$ inside of its domain of dependence, so that $\hat{R}_P$ has an island whenever $\hat{R}_1$ does. The entanglement wedge of $\hat{R}_P$ (shown in light gray) will include a small portion of the black hole exterior in its entanglement wedge.

Applying Theorem 10 along with its converse (which holds because we are in the constant tension solutions) gives a simple condition for when the radiation system reconstructs a portion of the black hole interior: an island forms if and only if there is a causal curve from the black hole interior into the radiation system.

This causal picture for island formation immediately reveals a set of simple operators that probe behind the black hole horizon. In particular consider an operator $\mathcal{O}_y$, which is localized near a point y, with y in $\hat{R}$ and in the future of the black hole interior (such points exist by our theorem). These operators directly probe the black hole interior by virtue of being in the future of the interior.

Notice that the radiation system $\hat{R}$ sits outside of the Poincaré patch we identified above. Thus it sits outside of the black hole spacetime. Ideally, we would understand which subregions of the Poincaré patch reconstruct the black hole interior. To do this, we need only note that a nearby subregion $\hat{R}_P$ of the Poincaré patch includes $\hat{R}$ in its domain of dependence. See figure 11.3. Evolving the state

on this subregion forward using the global Hamiltonian, we can construct the state of the earlier radiation system $\hat{\mathcal{V}}_1$. Notice that V_P is slightly larger than $\hat{\mathcal{V}}_1$ and will include a small portion of the black hole exterior in its entanglement wedge.

To write operators which probe behind the black hole horizon in the Hilbert space of V_P, we can start with the operators $\mathcal{O}_y$ which live in $\hat{\mathcal{V}}_1$ and time evolve backward using the global Hamiltonian. We continue this time evolution until $\mathcal{O}_y$ is some non-local operator $\mathcal{O}_{y,P}$ living on V_P.

It is interesting that such simple operators can be used to probe the black hole interior. However, we should perhaps be unsurprised, as the situation is analogous to the traversable wormhole [34]: in both cases we have a left and right CFT (or in our setting, BCFT), which we couple and then time evolve to find that information from behind the black hole horizon has emerged at the boundary. In the traversable wormhole the coupling is a double trace term which can be understood perturbatively, while in our setting the coupling is due to time evolution with the global Hamiltonian.[1]

[1] We thank Henry Lin for pointing out this analogy to us.

Chapter 12

Towards implications for quantum information theory

Section 12.1 of this chapter is based on unpublished material, while section 12.2 appears partly in [70].

The basic observation leading to the connected wedge theorem is that AdS/CFT necessarily implements non-local quantum computations (NLQC). Given this, we can use the necessity of entanglement results for NLQC to learn about AdS/CFT, namely we arrive at the connected wedge theorem.

We can also consider thinking in the other direction. Given that AdS/CFT defines a protocol for doing NLQC, what do we learn about NLQC? We take this up in section 12.1 below, and argue that AdS/CFT implies a large class of channels should have efficient non-local implementations, though many of these are not yet understood.

More generally, the AdS/CFT correspondence gives us relationships between pairs of corresponding quantum tasks. In particular, we learn that for dual tasks $\mathbf{T}, \hat{\mathbf{T}}$,

$$p_{suc}(\mathbf{T}) \leq p_{suc}(\hat{\mathbf{T}}) \tag{12.1}$$

This represents a potentially large amount of data about quantum tasks themselves.

We study one example beyond NLQC in section 12.2.

12.1 Efficiency of non-local quantum computation

In section 4.4 we discussed protocols for performing quantum channels non-locally. For arbitrary channels, we gave the port-teleportation based protocol which required $O(2^n)$ EPR pairs to implement a channel acting on $O(n)$ qubits. This is the best construction known in the literature for arbitrary channels. We also proved in section 4.5 that the $\mathbf{B}_{84}^{\times n}$ task requires $O(n)$ EPR pairs. If we define

$$\chi(n) \equiv \max_{\mathcal{N}_{A_1A_2\to B_1B_2}} (\#\text{EPR pairs needed to implement } \mathcal{N}_{A_1A_2\to B_1B_2} \text{ non-locally}),$$

we can summarize the state of the art in NLQC then by saying

$$O(n) \leq \chi(n) \leq O(2^n). \tag{12.2}$$

Viewed in this way, very little is known about NLQC: the upper and lower bounds on the required entanglement suffer an exponential gap. An interesting comment is that [17] showed that the non-signalling correlations given by Popescu-Rohrlich boxes allow NLQC to be performed with linear entanglement, so that the above gap collapses in that setting.

A more fine grained question we can ask is about the entanglement cost of implementing specific unitaries, rather than the worst case measure $\chi(n)$ given above. We define

$$E_c(U) = (\text{minimal number of EPR pairs needed to implement } U \text{ non-locally})$$

There is some information known about $E_c(U)$ for certain unitaries. For instance our proof that $O(n)$ EPR pairs are needed to do the $\mathbf{B}_{84}^{\times n}$ task non-locally, along with the explicit protocol 6, means

$$E_c(H^{\otimes n}) = n \tag{12.3}$$

More generally, we showed in protocol 7 that unitaries in the third level of the Clifford hierarchy can be performed non-locally with linear entanglement. One

additional fact is known: [90] constructed a protocol for unitaries whose entanglement cost scales exponentially in the number of layers of T gates in the unitaries circuit implementation.

How efficient is AdS/CFT at implementing NLQC? What can it tell us about $\chi(n)$ or $E_c(U)$? To understand this, we first note that any unitary which can be performed inside of the bulk scattering region can be performed non-locally using linear entanglement. If we can understand one of these classes of unitaries better, we learn something about the other.

Lets first of all think about the class of unitaries that can be performed inside of the scattering region. To begin we should revisit some of the comments made in the tasks argument for the connected wedge theorem (section 9.2). Recall that we argued the bulk gravitational picture allows

$$n = O(1/G_N) \tag{12.4}$$

qubits to be sent into the bulk scattering region. Sending more qubits than this risks changing the bulk geometry. In the context of the argument for the connected wedge theorem we need to avoid changing the bulk geometry at all, since we want to prove a statement about the original geometry. In our context now, we want to avoid closing the bulk scattering region, preventing the task from being completed, so the settings are somewhat different, but in general we expect these both occur at $O(1/G_N)$.

Given that we can send $O(n)$ qubits, what is the class of operations we can perform in the bulk scattering region? Naively this is $U(n)$, any unitary on n qubits, but this is actually incorrect. Gravity couples to all qubits sent into the bulk region, not just the ones the unitary acts on. In particular any data sent into the bulk to describe the unitary itself, or how that unitary can be implemented, is also counted. This means

$$n + \mathcal{K}(U_n) \leq O(n) \tag{12.5}$$

where $\mathcal{K}(U_n)$ is the Kolmogorov complexity, which is just the minimal number of bits needed to describe the unitary. More speculatively, some [58] have conjectured

that the circuit complexity, which is the number of elementary gates needed to implement a unitary, is constrained in gravity. For instance, suppose each gate performed required an additional unit energy be added to the spacetime region[1]. Then an upper bound on complexity is placed by the need to avoid adding so much energy to the region that a black hole forms. This leads to a bound

$$n + \mathcal{C}(U_n) \leq O(n) \tag{12.6}$$

The circuit complexity of a unitary acting on n qubits is always at least $O(n)$, so we can drop the first term on the left above. Supposing the complexity is low, there is no known obstruction to completing the unitary in the bulk. Via the AdS/CFT correspondence, we then expect low complexity unitaries can be performed in the boundary, where the implementation is non-local. This leads to the following conjecture.

Conjecture 1 *The entanglement cost for performing a unitary $U_{A_1A_2}$ non-locally is bounded above by the complexity of that unitary,*

$$E_c(U_{A_1A_2}) \leq O(\mathcal{C}(U_{A_1A_2})). \tag{12.7}$$

It is clear that the conjectured inequality above cannot be an equality. A simple counterexample is a product unitary $U_{A_1A_2} = V_{A_1} \otimes V_{A_2}$, which can be implemented non-locally with zero entanglement and can have complexity of up to $O(2^{n/2})$.

It is interesting to understand if there may be loopholes to our reasoning above, and consequently how conjecture 1 may be violated. The key step in the above reasoning is the claim that, aside from keeping the total number of qubits present under $O(1/G_N)$, there are no obstructions to completing the unitary in the bulk. This may be too strong of a claim, and other more subtle constraints could be present. Alternatively, the complexity may be too weak of a constraint. For instance, some combination of the finite speed of light and the holographic bound might give a tighter constraint.

[1] In fact [52] constructed methods to perform arbitrarily fast quantum computations at arbitrarily low energies. Further, it relies on the system having an unbounded spatial extent. We suspect for bounded spacetime regions an energy-time relationship holds in performing a gate.

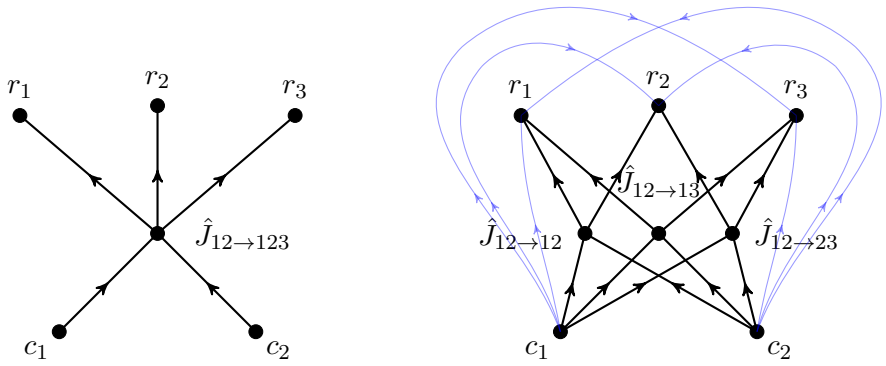


Figure 12.1: Schematic diagram of the boundary causal structure in 2-to-3 holographic scattering. The regions $\hat{J}_{12\to jk}$ are all nonempty, meaning it is possible for signals to travel from c_1 and c_2 meet, and then get to either of r_j or r_k. There are also causal curves that travel directly from c_i to r_j without passing through any of the regions $\hat{J}_{12\to jk}$. This fact is crucial for the entanglement-free procedures.

Another possibility is to instead try to understand the set of unitaries which can be performed in gravity by studying non-local quantum computation. In particular, we can ask from a quantum information perspective what the set of unitaries with $E_c(U_{A_1A_2}) \leq O(n)$ is. Then we can assert from AdS/CFT that the set of unitaries that can be performed inside of the scattering region are constrained to be a subset of these. If there are any unitaries which provably require entanglement more than linear in their complexity, this would represent a surprising constraint on quantum computation in the presence of gravity. No such unitaries are known however.

12.2 $2 \to 3$ tasks

In arguing for the connected wedge theorem, we have discussed $2 \to 2$ tasks and, in the context of spacetimes with ETW branes, $1 \to 2$ tasks. We can also consider more complicated arrangements of input and output locations. One interesting arrangement is shown in figure 12.1. There, we have two input locations and three output locations. Choosing the inputs and outputs to be points and placing those

points on the boundary of global AdS_{3+1} it is possible to have causal features in the bulk as shown in figure 12.1a, and causal features in the boundary as shown in figure 12.1b. To describe this succinctly, define the notation

$$J_{i\in\mathcal{I}\to j\in\mathcal{J}} = \left(\bigcap_{i\in\mathcal{I}} J^-(c_i)\right) \cap \left(\bigcap_{j\in\mathcal{J}} J^-(r_j)\right). \tag{12.8}$$

Then the bulk has

$$J_{12\to 123} \neq \varnothing \tag{12.9}$$

while the boundary has

$$\hat{J}_{12\to jk} \neq \varnothing \tag{12.10}$$

$$\hat{J}_{12\to 123} = \varnothing. \tag{12.11}$$

Quantum tasks of the $2 \to 3$ form, and methods for performing them using only the weaker causal features of figure 12.1b, have not been well studied in the quantum information literature. What is known, from the general theorem proven by Dolev [25], is that any channel which can be performed using the bulk causal features can be performed using only the boundary causal features along with exponential entanglement shared between $J_{1\to 123}$ and $J_{2\to 123}$.

AdS/CFT and inequality 8.1 tells us that any quantum task which can be performed using the bulk causal features can also be performed using only the boundary causal features, along with linear entanglement among the various relevant locations. Regarding the $2 \to 3$ task, this suggests only liner entanglement between input locations is required, along with linear entanglement between the intermediate locations $J_{12\to jk}$.

To better understand these tasks it is helpful to consider an explicit example. We will consider a generalization of the routing task (see section 4.3) to the $2 \to 3$ setting. At c_1, a quantum system R is input; at c_2 a classical trit $q \in \{1, 2, 3\}$ is input. The requirement is that R be output at r_q. In the bulk picture, where $J_{12\to 123}$ is nonempty, there is an obvious procedure to complete this — bring R and q into $J_{12\to 123}$ and route R towards the appropriate output point based on

q. In the boundary, where $\hat{J}_{12\to 123}$ is empty, there is actually a procedure which does not require entanglement between the input regions $\hat{J}_{i\to 123}$ nor between the intermediate regions $\hat{J}_{12\to jk}$. This goes beyond the requirement from AdS/CFT that only linear entanglement is necessary.

To see this, begin with the following naive procedure. At c_1, record R into an error correcting code that has three shares and corrects one erasure error. Call the three shares ABC, and label the system purifying the state on R by $\bar{R}$, so that

$$|\psi\rangle_{\bar{R}R} \to |\Psi\rangle_{\bar{R}ABC}. \tag{12.12}$$

Now send A to $\hat{J}_{12\to 12}$, B to $\hat{J}_{12\to 13}$, and C to $\hat{J}_{12\to 23}$. At c_2, create copies of q and send one copy to each of the $\hat{J}_{12\to jk}$. At each of the $\hat{J}_{12\to jk}$, forward the share of the error correcting code to r_q if $q \in \{j, k\}$. This will be possible at two of the three regions, so that two of the three shares will arrive at the correct output point r_q. The quantum system R can then be recovered from these two shares.

The procedure above avoids using entanglement between the input regions $\hat{J}_{i\to 123}$. However, quantum error correcting codes record information into highly entangled states. In particular the above procedure would create entanglement among the boundary regions $\hat{J}_{12\to jk}$. This entanglement too can be avoided however. To do this we exploit an additional feature of the boundary causal structure shown in Figure 12.1b: In the boundary, there are causal curves from the input points to the output points that avoid the intermediate regions.

These intermediate region avoiding curves can be used to hide the entanglement between the intermediate regions. Begin by again recording R into an error correcting code as in equation (12.12), but now additionally exploit the quantum one-time pad [9] (see section 3.2) to encrypt each of the shares A, B and C. Thus at c_2 we encode R according to

$$|\psi\rangle_{\bar{R}R} \to \sum_{k_a,k_b,k_c\in\{0,1\}^{\times 2n}} |k_a k_b\rangle_{X_1} \otimes |k_a k_c\rangle_{X_2} \otimes |k_b k_c\rangle_{X_3} \otimes [U_A^{k_a} U_B^{k_b} U_C^{k_c}]|\Psi\rangle_{RABC} \tag{12.13}$$

The one-time pad provides a way to choose the sets of unitaries $\{U^k\}$ such that averaging over k produces the maximally mixed state. The procedure now is to send

the A, B and C shares through the intermediate regions as before, but now additionally send the systems X_i to the corresponding r_i directly along the intermediate region avoiding curves. Now the intermediate regions remain unentangled, since the state on ABC is maximally mixed. Following the same routing procedure as before, two shares from the error correcting code will again arrive at the appropriate output points. The systems X_i can be used to undo the action of the one-time pad before recovering R from the shares of the error correcting code.

We have also studied generalizations of the $\mathbf{B}_{84}$ task to the 2-to-3 setting and found entanglement-free protocols in that case. As with the "routing" task described above, these protocols involve use of a one-time pad. Those protocols however rely on the only quantum operation performed being a Hadamard, which happens to be in the Clifford group. Clifford operations have simple conjugation properties with Pauli operations, and we can chose the one-time pad to involve only Pauli's. These coincidences allow an entanglement-free procedure to be designed simply. For more general tasks we do not know how to construct entanglement-free protocols, or if they exist.

It is interesting that an extremal surface calculation may resolve this question. This is because if we can check by calculating extremal surfaces that we can embed three regions into the boundary of AdS such that the causal features of figure 12.1 hold and both $I(J_{1\to 123} : J_{2\to 123}) = O(1)$ and all of the $I(J_{12\to 12} : J_{12\to 23}) = I(J_{12\to 12} : J_{12\to 13}) = I(J_{12\to 12} : J_{12\to 23}) ... = O(1)$, then the existence of a bulk procedure would imply the existence of a boundary entanglement free procedure.

There is one subtlety in applying the above reasoning. The regions $J_{12\to jk}$ are in the future of the points c_1, c_2. Thus the protocol might involve entangling them, but its not apparent that this entanglement had to be in the initial state. To see that this is the case, consider that the mutual informations $I(J_{12\to 12} : J_{12\to 23})$ etc are either $O(1)$ or $O(1/G_N)$, and are fixed by the bulk geometry. Then we can consider a protocol involving $O(n)$ qubits for $1 < O(n) < 1/G_N$. Then our $O(n)$ bulk qubits cannot change the geometry, and so the mutual informations cannot change order on account of the protocol happening. This shores up our reasoning above, and implies that the existence of a bulk protocol and $O(1)$ boundary mutual informations implies entanglement free protocols of the form in figure 12.1b.

Chapter 13

Final remarks

In this thesis, we have described the theory of relativistic quantum tasks and their application to AdS/CFT. As argued in the introduction, these tasks capture spacetime specific aspects of quantum information.

In the AdS/CFT context, these aspects of quantum information lead to the connected wedge theorem. More broadly, we have found a relationship between entanglement in the boundary theory and causal features of the bulk. This is a qualitatively distinct connection between entanglement and geometry than the usual one captured by the Ryu-Takayanagi formula, which relates entanglement and spacelike surfaces. While the Ryu-Takayanagi formula has lead to a wealth of insight into quantum gravity, the causal geometry-entanglement connection has been less explored.

There are many directions one can pursue the quantum tasks and quantum tasks in holography research directions.

Future directions for quantum tasks

The localize-exclude theorem represents our main contribution to better understanding the general theory of quantum tasks. Other recent progress has been made in understanding how entangled states can be distributed in a spacetime context [26]. There is still not a general understanding however of which quantum tasks are possible, and further what the resource requirements are for completing them

when they are. This resource requirement question is related to holography, as we discussed in detail in chapter 12.

One interesting direction is to understand if resources other than entanglement are helpful in completing some quantum tasks. For example, it is plausible that magic states are helpful in doing NLQC for unitaries beyond $\mathbf{C}^3$. For instance, it would be interesting to understand if having distributed magic states decreases the entanglement requirements for performing certain unitaries non-locally. This may be related to a recent suggestion that conformal field theories contain large amounts of magic [98].

Future directions for holographic quantum tasks

Towards a causal structure-entanglement theorem with a converse

From a tasks perspective the failure of Theorem 8 to have a converse is tied to the fact that we are interested in a fixed bulk geometry. While protocols that take place in that fixed geometric background have a boundary description, many boundary protocols will deform the geometry. Because of this, the bulk and boundary success probabilities are related by an inequality, $p_{suc}(\mathbf{T}) \leq p_{suc}(\hat{\mathbf{T}})$, so that sufficient entanglement to do the task in the boundary does not imply the task can be done in the bulk fixed geometry, and so does not signal the appearance of a bulk scattering region.

One interesting possibility is that large boundary correlation when measured in some way other than the mutual information will imply the existence of a bulk entanglement scattering region. In particular, this hypothetical measure of correlation should count only entanglement that can be made use of by operations that preserve the bulk geometry. Then, its appearance would signal that there should be a bulk protocol in that geometry which completes the required task, which in turn would imply the existence of the scattering region.

Closing the loophole

One outstanding question is if the loophole described in section 9.3 can be closed, and if so, if any additional assumptions about the boundary are necessary to do

so. A related direction would be to, using that the connected wedge theorem is true, argue the states of the conformal field theory are special in some way. In particular it might be possible to argue that any entanglement-free approach to NLQC requires the existence of large GHZ entanglement, and potentially to use the connected wedge theorem to argue holographic CFT states have little such entanglement.

Metric reconstruction

It is of considerable interest to determine how the bulk metric of general relativity is encoded in the boundary under the AdS/CFT dictionary. An early proposal for reconstructing the bulk metric from boundary data involved *light-cone cuts*: the restriction to the spacetime boundary of the light cone of a bulk point. It was shown in [29, 30] that knowledge of light-cone cuts, which can be determined from singularities in boundary correlators, can be used to reconstruct the metric. Another approach to metric reconstruction is to use the geometry of bulk extremal surfaces, whose areas are known on the boundary by the RT formula. It has been argued that in many cases the extremal surface areas determine the bulk metric [12].

The connected wedge theorem gives a nontrivial geometric relation between the causal structure of a spacetime and the areas of its extremal surfaces. It would be interesting to understand how, if at all, the intuition gleaned from Theorem 8 might assist in relating the two extant approaches to metric reconstruction.

Other tasks in holography

Another direction is to consider other quantum tasks beyond the $\mathbf{B}_{84}$ task and $\mathbf{M}$ tasks in the holographic context, which led us here to the $2 \to 2$ and $1 \to 2$ theorem. Indeed one such task and its holographic implications is already being considered in upcoming work. The idea is to consider one input region $\hat{\mathcal{C}}_1$, one output region $\hat{\mathcal{R}}_1$, and a excluded region $\hat{\mathcal{U}}_1$. In some cases there will be a causal curve passing from $\mathcal{C}_1$ to $\mathcal{R}_1$ while avoiding $\mathcal{U}_1$ in the bulk geometry, but no such curve in the boundary. This allows a message to pass from $\mathcal{C}_1$ to $\mathcal{R}_1$ in the bulk without being intercepted by someone with access to $\mathcal{U}_1$. In other words, the bulk

possesses a private channel from $\mathcal{C}_1$ to $\mathcal{R}_1$. For the boundary to simulate this private channel, correlation must be shared between appropriate regions. This leads to a distinct causal geometry - entanglement connection than the one given by the connected wedge theorem. Further, just as the $2 \to 2$ theorem lead to some insight into NLQC, we might hope this relationship to AdS/CFT may lead to some insight into private channels.

Holographic quantum tasks beyond AdS/CFT

Beyond using holographic quantum tasks to better understand AdS/CFT, there is also a possibility of applying them to other proposed holographic dualities (see, e.g. [11, 27]). A strength of the tasks approach is that it assumes very little about the boundary theory. Indeed, the tasks argument for the connected wedge theorem followed from the boundary being quantum mechanical and relativistic, we never used that it is a conformal field theory, or any details about holographic field theories (in contrast proofs of the Ryu-Takayanagi formula do rely on the boundary being a conformal field theory with particular properties). In this way it can be seen as, beginning with the bulk geometry, placing a constraint on the boundary theory. It would be interesting to apply this reasoning to holographic settings where the boundary theory is less well understood.

Bibliography

[1] C. Akers, J. Koeller, S. Leichenauer, and A. Levine. Geometric constraints from subregion duality beyond the classical regime. *arXiv preprint arXiv:1610.08968*, 2016. → pages 109

[2] C. Akers, A. Levine, and S. Leichenauer. Large breakdowns of entanglement wedge reconstruction. *Physical Review D*, 100(12):126006, 2019. → pages 99

[3] C. Akers, N. Engelhardt, G. Penington, and M. Usatyuk. Quantum maximin surfaces. *Journal of High Energy Physics*, 2020(8):1–43, 2020. → pages 99

[4] A. Almheiri, X. Dong, and D. Harlow. Bulk locality and quantum error correction in AdS/CFT. *Journal of High Energy Physics*, 2015(4):163, 2015. → pages 5

[5] A. Almheiri, T. Hartman, J. Maldacena, E. Shaghoulian, and A. Tajdini. Replica wormholes and the entropy of Hawking radiation. *Journal of High Energy Physics*, 2020(5), May 2020. ISSN 1029-8479. doi:10.1007/jhep05(2020)013. URL http://dx.doi.org/10.1007/JHEP05(2020)013. → pages 124

[6] A. Almheiri, R. Mahajan, J. Maldacena, and Y. Zhao. The Page curve of Hawking radiation from semiclassical geometry. *Journal of High Energy Physics*, 2020(3), Mar 2020. ISSN 1029-8479. doi:10.1007/jhep03(2020)149. URL http://dx.doi.org/10.1007/JHEP03(2020)149. → pages 124

[7] A. Almheiri, R. Mahajan, J. Maldacena, and Y. Zhao. The page curve of hawking radiation from semiclassical geometry. *Journal of High Energy Physics*, 2020(3):1–24, 2020. → pages 143

[8] A. Almheiri, R. Mahajan, and J. E. Santos. Entanglement islands in higher dimensions. 2020. → pages 124

[9] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 547–553. IEEE, 2000. doi:https://doi.org/10.1109/SFCS.2000.892142. → pages xiv, 38, 72, 157

[10] S. Antonini and B. Swingle. Cosmology at the end of the world. 2019. → pages 124

[11] A. Bagchi. Correspondence between asymptotically flat spacetimes and nonrelativistic conformal field theories. *Physical review letters*, 105(17): 171601, 2010. → pages 162

[12] N. Bao, C. Cao, S. Fischetti, and C. Keeler. Towards bulk metric reconstruction from extremal area variations. *Classical and Quantum Gravity*, 36(18):185002, 2019. ISSN 1361-6382. doi:10.1088/1361-6382/ab377f. URL http://dx.doi.org/10.1088/1361-6382/ab377f. → pages 161

[13] S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. → pages 21

[14] A. Beimel. Secret-sharing schemes: a survey. In *International Conference on Coding and Cryptology*, pages 11–46. Springer, 2011. doi:https://doi.org/10.1007/978-3-642-20901-7_2. → pages 78

[15] G. Benenti and G. Strini. Computing the distance between quantum channels: usefulness of the Fano representation. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 43(21):215508, 2010. → pages 20

[16] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993. → pages 4, 39

[17] A. Broadbent. Popescu-rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *Physical Review A*, 94(2):022318, 2016. → pages 152

[18] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014. doi:https://doi.org/10.1137/130913687. → pages 46

[19] K. Chakraborty and A. Leverrier. Attack strategies for position-based quantum cryptography based on the clifford hierarchy. 2015. → pages 54

[20] H. Z. Chen, R. C. Myers, D. Neuenfeld, I. A. Reyes, and J. Sandor. Quantum extremal islands made easy. Part I. Entanglement on the brane. *Journal of High Energy Physics*, 2020(10):1–69, 2020. → pages 124

[21] H. Z. Chen, R. C. Myers, D. Neuenfeld, I. A. Reyes, and J. Sandor. Quantum extremal islands made easy. Part II. Black holes on the brane. *Journal of High Energy Physics*, 2020(12):1–81, 2020. → pages 124

[22] S. Cooper, M. Rozali, B. Swingle, M. Van Raamsdonk, C. Waddell, and D. Wakeham. Black hole microstate cosmology. *Journal of High Energy Physics*, 2019(7), Jul 2019. ISSN 1029-8479. doi:10.1007/jhep07(2019)065. URL http://dx.doi.org/10.1007/JHEP07(2019)065. → pages 124

[23] J. Cotler, P. Hayden, G. Penington, G. Salton, B. Swingle, and M. Walter. Entanglement wedge reconstruction via universal recovery channels. *Physical Review X*, 9(3):031011, 2019. → pages 102

[24] B. Czech, J. L. Karczmarek, F. Nogueira, and M. Van Raamsdonk. The gravity dual of a density matrix. *Classical and Quantum Gravity*, 29(15): 155009, 2012. → pages 91

[25] K. Dolev. Constraining the doability of relativistic quantum tasks. 2019. → pages 156

[26] K. Dolev, A. May, and K. Wan. Distributing bipartite quantum systems under timing constraints. *arXiv preprint arXiv:2011.00936*, 2020. → pages v, xxiii, 159

[27] X. Dong, B. Horn, E. Silverstein, and G. Torroba. Micromanaging de sitter holography. *Classical and Quantum Gravity*, 27(24):245020, 2010. → pages 162

[28] N. Engelhardt and S. Fischetti. The gravity dual of boundary causality. *Classical and Quantum Gravity*, 33(17):175004, 2016. → pages xvii, 108, 109

[29] N. Engelhardt and G. T. Horowitz. Towards a reconstruction of general bulk metrics. *Classical and Quantum Gravity*, 34(1):015004, 2016. ISSN 1361-6382. doi:10.1088/1361-6382/34/1/015004. URL http://dx.doi.org/10.1088/1361-6382/34/1/015004. → pages 161

[30] N. Engelhardt and G. T. Horowitz. Recovering the spacetime metric from a holographic dual. 2016. → pages 161

[31] J. Erdmenger and M. Ammon. Gauge/gravity duality. → pages 79, 94

[32] C. A. Fuchs and J. Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. → pages 17

[33] M. Fujita, T. Takayanagi, and E. Tonni. Aspects of AdS/BCFT. *JHEP*, 11: 043, 2011. doi:10.1007/JHEP11(2011)043. → pages 102

[34] P. Gao, D. L. Jafferis, and A. C. Wall. Traversable wormholes via a double trace deformation. *Journal of High Energy Physics*, 2017(151), 2017. → pages 150

[35] S. Gao and R. M. Wald. Theorems on gravitational time delay and related issues. *Classical and Quantum Gravity*, 17(24):4999, 2000. → pages xvii, 108, 109

[36] H. Geng and A. Karch. Massive islands. *Journal of High Energy Physics*, 2020(9):1–19, 2020. → pages 124

[37] H. Geng, A. Karch, C. Perez-Pardavila, S. Raju, L. Randall, M. Riojas, and S. Shashi. Information transfer with a gravitating bath. *arXiv preprint arXiv:2012.04671*, 2020. → pages 124

[38] N. Gisin and S. Massar. Optimal quantum cloning machines. *Physical review letters*, 79(11):2153, 1997. → pages 3

[39] D. Gottesman. Theory of quantum secret sharing. *Physical Review A*, 61 (4):042311, 2000. doi:https://doi.org/10.1103/PhysRevA.61.042311. → pages 37, 76

[40] D. Harlow. Tasi lectures on the emergence of the bulk in AdS/CFT. *arXiv preprint arXiv:1802.01040*, 2018. → pages 5

[41] T. Hartman, Y. Jiang, and E. Shaghoulian. Islands in cosmology, 2020. → pages 124

[42] P. Hayden and A. May. Summoning information in spacetime, or where and when can a qubit be? *Journal of Physics A: Mathematical and Theoretical*, 49(17):175304, 2016. doi:https://doi.org/10.1088/1751-8113/49/17/175304. → pages v, xiii, 3, 69

[43] P. Hayden and A. May. Localizing and excluding quantum information; or, how to share a quantum secret in spacetime. *Quantum*, 3:196, 2019. → pages v, vi, 43, 44, 63, 64

[44] P. Hayden and G. Penington. Learning the alpha-bits of black holes. *Journal of High Energy Physics*, 2019(12):1–55, 2019. → pages 99

[45] P. Hayden, S. Nezami, G. Salton, and B. C. Sanders. Spacetime replication of continuous variable quantum information. *New Journal of Physics*, 18 (8):083043, 2016. doi:https://doi.org/10.1088/1367-2630/18/8/083043. → pages xiii, 69

[46] F. Hiai and D. Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in mathematical physics*, 143(1):99–114, 1991. → pages 19

[47] V. E. Hubeny. Extremal surfaces as bulk probes in AdS/CFT. *Journal of High Energy Physics*, 2012(7):93, 2012. → pages xviii, 113

[48] V. E. Hubeny, M. Rangamani, and T. Takayanagi. A covariant holographic entanglement entropy proposal. *Journal of High Energy Physics*, 2007(07): 062, 2007. → pages 103

[49] S. Ishizaka and T. Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical review letters*, 101 (24):240501, 2008. → pages 11, 31

[50] D. L. Jafferis, A. Lewkowycz, J. Maldacena, and S. J. Suh. Relative entropy equals bulk relative entropy. *Journal of High Energy Physics*, 2016 (6):4, 2016. → pages 101

[51] J. Javelle, M. Mhalla, and S. Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 1–12. Springer, 2012. doi:https://doi.org/10.1007/978-3-642-35656-8_1. → pages 78

[52] S. P. Jordan. Fast quantum computation at arbitrarily low energy. *Physical Review A*, 95(3):032305, 2017. doi:https://doi.org/10.1103/PhysRevA.95.032305. → pages 154

[53] A. Kent. Unconditionally secure bit commitment. *Physical Review Letters*, 83(7):1447, 1999. → pages 64

[54] A. Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011. → pages 64

[55] A. Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012. doi:https://doi.org/10.1088/0264-9381/29/22/224013. → pages 3, 45

[56] A. Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Physical review letters*, 109(13):130501, 2012. → pages 64

[57] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011. doi:https://doi.org/10.1103/PhysRevA.84.012326. → pages 46

[58] S. Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000. doi:https://doi.org/10.1038/35023282. → pages 153

[59] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Physical review letters*, 111(18):180504, 2013. → pages 64

[60] J. Maldacena. The large-n limit of superconformal field theories and supergravity. *International journal of theoretical physics*, 38(4): 1113–1133, 1999. → pages 4, 91

[61] D. Markham and B. C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78(4):042309, 2008. doi:https://doi.org/10.1103/PhysRevA.78.042309. → pages 78

[62] D. Marolf, A. C. Wall, and Z. Wang. Restricted maximin surfaces and HRT in generic black hole spacetimes. *Journal of High Energy Physics*, 2019(5): 127, 2019. → pages 133

[63] A. May. Quantum tasks in holography. *Journal of High Energy Physics*, 2019(10):233, 2019. → pages v, vi, xi, xxiii, 6, 40, 59, 105, 111

[64] A. May. Holographic quantum tasks with regions. *arXiv preprint arXiv:2101.08855*, 2021. → pages 105, 115

[65] A. May and E. Hijano. The holographic entropy zoo. *Journal of High Energy Physics*, 2018(10):36, 2018. → pages v, xxii

[66] A. May and M. Van Raamsdonk. Interpolating between multi-boundary wormholes and single-boundary geometries in holography. *arXiv preprint arXiv:2011.14258*, 2020. → pages 124

[67] A. May and D. Wakeham. Quantum tasks require islands on the brane. *to appear*, . → pages v, vi, 79, 124

[68] A. May and D. Wakeham. Quantum tasks with input and output regions. *to appear*, . → pages v, vi, 43, 45, 111

[69] A. May, G. Penington, and J. Sorce. Holographic scattering requires a connected entanglement wedge. *arXiv preprint arXiv:1912.05649*, 2019. → pages 132

[70] A. May, G. Penington, and J. Sorce. Holographic scattering requires a connected entanglement wedge. *Journal of High Energy Physics*, 2020(8): 1–34, 2020. → pages v, vi, 79, 111, 116, 122, 151

[71] S. Nezami and M. Walter. Multipartite Entanglement in Stabilizer Tensor Networks. 2016. → pages 117

[72] S. Nezami and M. Walter. Multipartite entanglement in stabilizer tensor networks. *Physical Review Letters*, 125(24):241602, 2020. → pages 130

[73] M. A. Nielsen and I. Chuang. Quantum computation and quantum information, 2002. → pages 24, 50, 52

[74] D. N. Page. Information in black hole radiation. *Physical review letters*, 71 (23):3743, 1993. → pages 144

[75] G. Penington. Entanglement wedge reconstruction and the information paradox. *Journal of High Energy Physics*, 2020(9):1–84, 2020. → pages 99, 143, 144

[76] E. Poisson. *A relativist's toolkit: the mathematics of black-hole mechanics*. Cambridge university press, 2004. → pages 79, 87

[77] J. Polchinski. The black hole information problem. In *New Frontiers in Fields and Strings: TASI 2015 Proceedings of the 2015 Theoretical Advanced Study Institute in Elementary Particle Physics*, pages 353–397. World Scientific, 2017. → pages 64

[78] L. Randall and R. Sundrum. An alternative to compactification. *Physical Review Letters*, 83(23):4690, 1999. → pages 144

[79] M. Rangamani and T. Takayanagi. Holographic entanglement entropy. In *Holographic Entanglement Entropy*, pages 35–47. Springer, 2017. → pages 91

[80] M. Rozali, J. Sully, M. Van Raamsdonk, C. Waddell, and D. Wakeham. Information radiation in BCFT models of black holes. *JHEP*, 05:004, 2020. doi:10.1007/JHEP05(2020)004. → pages 124, 146

[81] M. Rozali, J. Sully, M. Van Raamsdonk, C. Waddell, and D. Wakeham. Information radiation in bcft models of black holes. *Journal of High Energy Physics*, 2020(5):1–34, 2020. → pages 86

[82] S. Ryu and T. Takayanagi. Holographic derivation of entanglement entropy from AdS/CFT. *Phys. Rev. Lett.*, 96:181602, 2006. doi:10.1103/PhysRevLett.96.181602. → pages 103

[83] S. Ryu and T. Takayanagi. Holographic derivation of entanglement entropy from the anti–de sitter space/conformal field theory correspondence. *Physical review letters*, 96(18):181602, 2006. → pages 91

[84] P. Sarvepalli and R. Raussendorf. Matroids and quantum-secret-sharing schemes. *Physical Review A*, 81(5):052333, 2010. doi:https://doi.org/10.1103/PhysRevA.81.052333. → pages 78

[85] B. Schumacher and M. D. Westmoreland. Approximate quantum error correction. *Quantum Information Processing*, 1(1-2):5–12, 2002. → pages 11, 23

[86] B. Schumacher and M. D. Westmoreland. Entanglement and perfect quantum error correction. *Journal of Mathematical Physics*, 43(9): 4279–4285, 2002. → pages 11, 23

[87] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11): 612–613, 1979. doi:https://doi.org/10.1145/359168.359176. → pages 78

[88] C. E. Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949. → pages 38

[89] K. Skenderis and B. C. van Rees. Real-time gauge/gravity duality. *Physical review letters*, 101(8):081601, 2008. → pages 96

[90] F. Speelman. Instantaneous non-local computation of low t-depth quantum circuits. *arXiv preprint arXiv:1511.02839*, 2015. → pages 153

[91] J. Sully, M. V. Raamsdonk, and D. Wakeham. BCFT entanglement entropy at large central charge and the black hole interior, 2020. → pages 103

[92] T. Takayanagi. Holographic dual of a boundary conformal field theory. *Physical Review Letters*, 107(10):101602, 2011. → pages 91, 102

[93] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013. → pages 40, 41, 42, 56, 128

[94] M. Van Raamsdonk. Building up spacetime with quantum entanglement II: It from BC-bit. 2018. → pages 124

[95] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619, 1998. → pages 62

[96] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Physical Review Letters*, 78(12):2275, 1997. → pages 62

[97] A. C. Wall. Maximin surfaces, and the strong subadditivity of the covariant holographic entanglement entropy. *Classical and Quantum Gravity*, 31 (22):225007, 2014. → pages 99, 103, 133

[98] C. D. White, C. Cao, and B. Swingle. Conformal field theories are magical. *arXiv preprint arXiv:2007.01303*, 2020. → pages 160

[99] M. M. Wilde. *Quantum information theory*. Cambridge University Press, 2013. → pages 11, 16, 22

[100] Y.-D. Wu, A. Khalid, and B. C. Sanders. Efficient code for relativistic quantum summoning. *New Journal of Physics*, 20(6):063052, 2018. doi:https://doi.org/10.1088/1367-2630/aaccae. → pages xiii, 69