UNIVERSITY OF CALGARY

RESOURCE THEORIES IN QUANTUM INFORMATION

by

Yuval Rishu Sanders

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

and

INSTITUTE FOR QUANTUM INFORMATION SCIENCE

CALGARY, ALBERTA

NOVEMBER, 2010

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Resource Theories in Quantum Information" submitted by Yuval Rishu Sanders in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Supervisor, Dr. Gilad Gour
Department of Mathematics & Statistics

Dr. Clifton Cunningham
Department of Mathematics & Statistics

Dr. David L. Feder
Department of Physics & Astronomy

Date

I dedicate this thesis to my parents, Shanno and Barry, because they gave me life, love, and liberty. I could not have done any of this without their unconditional support. I can never thank them enough.

Abstract

Many quantum information processing tasks require the consumption of various types of informational resource. Entanglement is a well-studied example of this type of resource; frameness is another. Both types of resource may be quantified through the use of real-valued functions known as monotones, a collection of which can fully characterize the resourcefulness of a state. A complete characterization of the entanglement or frameness of even a finite-dimensional quantum state might require an infinite collection of monotones, despite finiteness of the descriptions of the states in question.

We propose a new framework of relative monotones. A relative monotone quantifies the resourcefulness of a quantum state relative to another quantum state. We give an example of the efficacy of relative monotones by characterizing a simple type of frameness with a single relative monotone. This type of frameness is unlikely to yield to analysis with 'absolute' monotones.

Acknowledgements

My supervisor, Dr. Gilad Gour, has provided kind but stern guidance to me for many years. He has pushed me to my limits intellectually and philosophically, and he taught me to love my work. I thank him for many wise teachings through the years and specifically for whatever mastery I have gained of the subject of quantum information. I acknowledge that it was he who saw the wider potential of the relative monotones defined in this thesis and focussed me on this result.

I also thank Dr. Ben Fortescue for the patient support and critical ear he provided me over the last year. He helped me to turn incoherent calculations into comprehensible results. In addition, I thank Michael Skotiniotis and Borzumehr Toloui Semnani for their discussions with me on the nature of the resource theory of reference frames and of resource theories in general. I thank Dr. Robert Spekkens and Iman Marvian for extremely helpful discussions and criticisms on the nature of relative monotones. I thank Dr. Ady Mann, Thomas Nedunthally, and Robert Parkinson for lending their ears as I strove to understand my own results. I thank Dr. Barry Sanders for many constructive criticisms on many drafts of this thesis. I do not know if I could have provided a non-technical introduction to entanglement in section 1.2 without arguing with him.

Finally, I thank NSERC for their financial support during the summers of 2008, 2009, and 2010 in developing the results presented in this thesis.

Table of Contents

Approval Page ii
Abstract iv
Acknowledgements v
Table of Contents vi
List of Figures vii
1 Introduction: quantifying resourcefulness 1
1.1 Informational resources 2
1.2 Entanglement 3
1.3 Frameness 6
1.4 The value of a resource 8
1.5 Results 10
2 The formalism of quantum informational resource theories 11
2.1 States and measurements 12
2.2 LOCC channels 15
2.3 Frame-invariant channels 18
3 Entanglement catalysis 22
3.1 The trumping relation 23
3.2 Factorizing concurrences 25
3.3 Bounding the dimension of a catalyst 28
4 Relative monotones 33
4.1 Relative monotones versus absolute monotones 34
4.2 Relative Z_n-frameness 38
4.3 U(1)-frameness 44
5 Conclusion 48
Bibliography 51

List of Figures

3.1 A plot of $\Delta T_\nu = T_\nu(|\psi\rangle) - T_\nu(|\phi\rangle)$, where T_ν represents Turgut's monotone of order $\nu \in \mathbb{R}$, and $|\psi\rangle$ and $|\phi\rangle$ are defined in Example 3.1. 31

4.1 Depiction of states in the form $\sqrt{x}\,|0\rangle + \sqrt{y}\,|1\rangle + \sqrt{z}\,|2\rangle$ (where $0 \leq x, y, z \leq 1$ and $x + y + z = 1$) that can be mapped to or from a specified state $|\eta\rangle$. In each figure, the vertical axis represents $\sqrt{3}x$, and the horizontal axis is $z - y$. The red dot in each figure represents $|\eta\rangle$, whereas the blue dots represent the non-resource states $|0\rangle$, $|1\rangle$, and $|2\rangle$ that form the vertices of the region of all states. The interior red region represents the states that can be mapped to $|\eta\rangle$ with Z_3-invariant operations, whereas the exterior blue region represents states to which $|\eta\rangle$ can be transformed using Z_3-invariant operations. 43

Chapter 1

Introduction: quantifying resourcefulness

Many quantum information processing tasks require consumable resources. My thesis studies the quantification of such quantum informational resources. In particular, I study entanglement and frameness. The resourcefulness of entanglement is well-known, and many famous quantum information processing tasks explicitly require the consumption of entanglement [1, 2]. The resource theory of frameness has been developed more recently for the theoretical analysis of certain practical implementations of quantum informational protocols [3]. These resources can be quantified through the use of real-valued functions known as monotones.

This first chapter of my thesis provides a non-technical introduction to both entanglement and frameness. The second chapter presents these concepts in a technical fashion and, in particular, defines entanglement monotones and frameness monotones. In the third chapter, I present necessary conditions on states that can 'catalyze' a transformation of entangled states [4]. These conditions are expressed as bounds on the values certain entanglement monotones can take for a catalyst state.

The characterization of resourcefulness with a collection of monotones can be difficult, and may be unnecessarily prolix even if accomplished: sometimes infinitely many monotones are required to characterize a resource. I give a new framework for the quantification of resourcefulness in chapter four. This new framework quantifies the resourcefulness of a state with respect to another state. Such 'relative monotones' are sometimes more easily found than 'absolute' monotones, as I show for a simple type of frameness, and a single relative monotone always suffices to characterize the ability to transform resources.

1.1 Informational resources

Information is ideally transmitted through a noiseless communication channel [5]. As the communication channel becomes noisier, the cost of transmission rises because some method of error correction will be required to correctly interpret the message. For example, if the message is encoded in a bit string, there may be a small probability p of a single bit-flip error. Such an error can be partially corrected by implementing the repetition code [6]: replace each bit 0 with the string 000 and each bit 1 with the string 111. The message is then decoded by 'majority vote', where the repeated bit is chosen if there is disagreement between the three bits representing one message bit. The probability of error in the decoded message is approximately p^2 for each message bit, thereby reducing the error quadratically by increasing the size of the transmission.

The important point is that the degradation of information can be ameliorated at the cost of a resource resource, namely message length. The goal of resource theory is to identify an appropriate cost function for a resource and ultimately to minimize this cost. This goal remains unchanged when considering information in a quantum framework rather than classical, though many new subtleties arise.

There are a wide variety of consumable informational resources; transmission size is just one example. Shared secret random bits are another informational resources and are required for many cryptographic protocols [6]. Another example, which appears basic, is the establishment of physical states corresponding to logical 0 and to logical 1. These states may correspond to voltage pulses V_1 and V_2 transmitted over a wire, with V_1 representing 0 and V_2 representing 1 or vice versa. Each party agrees on such a choice, which can be accomplished by having the sender transmit a 0 before transmitting her message so each recipient knows which voltage corresponds to logical 0. Thus one bit is consumed to initialize communication.

Historically, information theory has focussed on the consumption of resources to communicate information through a noisy communication channel [5]. The subject has recently been enriched by studying the transmission of quantum information through a noisy quantum communication channel. Such transmission is required for the implementation of quantum cryptographic protocols [7] and of distributed quantum computing [8]. There are a variety of resources for alleviating the noise present in such channels, many of which are analogous to resources for classical communication.

My thesis focusses on quantifying two types of resources useful for quantum communication. Entanglement can provide shared secret random bits between separate parties, and tokens of a reference frame can initialize communication. In section 1.2 I will introduce entanglement and discuss its ability to serve as a quantum informational resource. I will discuss the 'frameness' of a quantum state in section 1.3 as a quantity indicating the capacity of that state to transmit information about a choice of reference frame. The quantification of resourcefulness is discussed in section 1.4, wherein I also present my results.

1.2 Entanglement

Entanglement is a correlation that can exist between separate quantum systems that is stronger than that which can exist between separate classical systems. Entanglement is important because it can enable critical tasks such as the transmission of quantum information through classical communication channels [1]. In order to understand entanglement, we need to appreciate the nature of composite physical systems and the correlations that can exist between them.

A physical system is a portion of the universe selected for analysis. The state of a physical system is the best description of the properties of that system based on existing

knowledge. Most simply, the state could be expressed as a string of bits (informationally speaking). The state of a system can also be described by a probability distribution of bit strings or by a quantum state representing superpositions of bit strings. The knowledge of a system is obtained by performing measurements on that system. A measurement is a physical process that distinguishes between different possible states of a system. The outcome of such a process provides information about the properties of the system.

A physical system may comprise several disjoint subsystems. In this case, the system is called 'composite'. The state of a composite physical system comprising independent disjoint subsystems is described by the concatenating the states of the subsystems. The distinction between dependent and independent subsystems can be discerned by performing measurements on the subsystems and searching for correlations in the measurement outcomes. Correlated systems are then described by joint states that are not merely concatenated states of subsystems. If the states of the subsystems are correlated (classically), the state of the composite system can be described as a joint distribution of states. Entangled systems cannot be described by such joint distributions.

A composite system is used for information processing and communication, either classical or quantum. Information processing is achieved by applying operations to the system. If the state of a system is given by a bit string, for example, we could transform the string to a different one, measure part of the string, or add or remove bits from the string. 'Local' operations are those performed on a single subsystem, while nonlocal operations could be performed jointly on more than one subsystem.

Operations can be performed sequentially. After performing an operation with several possible outcomes, such as measuring part of a system, the subsequent operations (even on different systems) could be conditioned on knowledge of this outcome. This is an example of a sequence of local operations with classical communication (LOCC). LOCC corresponds to an important class of sequential operations wherein the result of

an operation dictates the choice of subsequent operations. Classically, all sequences of operations can be expressed as LOCC sequences. This is not true for quantum information: correlations can exist between measurement results that could not be created via LOCC sequences. An 'entangled' state is one that could not have been prepared by an LOCC sequence of operations acting on initially independent subsystems.

These entangled states are resources for the communication of quantum information. Consider the simple case of two systems holding one quantum bit (a 'qubit' [9]) of information; that is, each system has a subsystem whose state is a superposition of logical 0 and logical 1 (which may be represented by a unit vector in $\mathbb{C}^2$ if the state is 'pure'). If the systems are never measured to be in the joint state 01 or 10, the systems are maximally correlated. Consider a light switch connected to a lightbulb: the state of the light switch (on or off) is perfectly correlated with the state of the bulb (on or off). If the same local measurement produces the same outcome when performed on either system, the systems are maximally entangled. Such correlation between measurement outcomes is central to many quantum information tasks such as quantum teleportation [1].

In its simplest form, the teleportation protocol allows a sender (whom the literature usually calls 'Alice') to transmit one unknown qubit to a receiver ('Bob') through an LOCC sequence of operations. Alice and Bob are assumed to share one maximally entangled pair of qubits. Alice performs a local measurement on her system, which contains two qubits: her half of the entangled pair and the unknown qubit she wishes to transmit. This measurement has four possible outcomes. Alice informs Bob of the outcome by transmitting at least two bits through a classical channel, whereupon Bob performs one of four operations to his system depending on the message he received from Alice. After performing this operation, Bob possesses the unknown qubit whereas Alice does not. In fact, Alice gains no information about the state [10]. The unknown qubit has been teleported.

If Alice and Bob share entanglement not in the form of maximally entangled qubits, they may wish to ascertain how many such pairs of qubits can be produced using only LOCC sequences of operations. More generally, Alice and Bob may wish to ascertain their ability to transform some given shared entangled state to another one. Nielsen's theorem [11] characterizes the ability to transform 'pure' entangled states under LOCC sequences. This characterization is made with reference to a collection of quantifiers of entanglement known as Vidal's monotones [12].

The quantification of entanglement can be subtle because entanglement can be 'borrowed'. In a phenomenon known as entanglement catalysis [4], an entangled state (called an 'entanglement catalyst') can be used to enact a previously prohibited state transformation under LOCC restrictions yet be returned intact at the end of the transformation. The entanglement of the catalyst has thus been used without being consumed, because the transformation was not possible without the catalyst.

1.3 Frameness

The frameness of a state is a resource for the communication of quantum information and has become important for the analysis of certain practical implementations of quantum information processing tasks [3]. A state with frameness has the ability to convey information about a choice of reference frame. Some discussion of reference frames is appropriate before explaining frameness.

A reference frame may be a choice between which of voltage pulses V_1 and V_2 should represent 0 or 1. A more complex example is the choice of a Cartesian co-ordinate frame for a laboratory. A choice of reference frame is often important because measurements are usually made with respect to this choice. The choice of $V_1 = 0$ or $V_2 = 0$ is relatively simple because only one bit is required to specify that choice. The additional resource

cost for transmitting quantum information in the absence of a shared choice of Cartesian co-ordinate frame is considerably larger.

Alleviating the lack of a shared reference frame is important if a transmitted message is to be interpreted correctly. If Alice does not communicate her choice of $V_1 = 0$ or $V_2 = 0$ to Bob, Bob simply measures a sequence of voltage pulses V_1 and V_2 and cannot distinguish between the true message and the binary complement of that message. If Alice has sent the string $V_1V_2V_1$, for example, the message is equally likely to be 010 as 101. Thus Bob's lack of knowledge of a reference frame has effectively degraded the information he has received.

In quantum formalism, the lack of a reference frame can be treated as a form of decoherence [13]. Decoherence can be regarded as correlation with an inaccessible environment, and in this case the environment is a reference system. Without access to the reference system of Alice, Bob averages over all possible choices of reference frame to describe his state. Such a state cannot exhibit coherence between quantum states whose form is independent of the choice of reference frame. This lack of coherence can prevent some practical implementations of quantum information processing protocols [3].

Reference frame information can be communicated by transmitting states with frameness. The frameness of the state of a physical system is defined as its capacity for storing a choice of reference frame [14]. For example, the axis of rotation of a spinning isotropic ball stores a choice of direction in physical space, but the rotational symmetry of the ball prevents it from storing any frame information when it is not spinning. Its capacity for storing frame information is thus dependent on its state. This principle is also true within a quantum information framework. If Alice provides Bob with a state that carries information about her choice of a reference frame, Bob gains some ability to interpret messages encoded with respect to that reference frame.

The literature often assumes that the collection of possible reference frame choices is

related by a group of operations. The possible choices of spatial direction, for example, may be related by the group of 3×3 orthogonal matrices with determinant one. Suppose Alice has an isotropic ball at rest (so its state carries no frameness), and she wishes to encode a choice of direction 'up' in space. She may do so by spinning the ball counter-clockwise about an axis aligned with her choice of up. The new state contains frame information so her operation increases the frameness of the state of the ball and does so by treating one direction preferentially. The preference for direction is evident: if Alice alters her choice of 'up', she has enacted a different operation on the rest state since the outcome is different. Mathematically, Alice's preparation is altered by conjugating with an element of the group of transitions between reference frame choices. Conversely, an operation that is not altered by conjugation is one that cannot increase frameness.

1.4 The value of a resource

Up to this point, we have considered states that serve as resources so that tasks that are impossible within the restricted set of operations become achievable. For example, teleportation allows entanglement to be consumed to send quantum states down classical channels. This could not have been achieved through LOCC sequences of operations in the absence of entanglement. Similarly, a state with frameness is a resource when restricted to operations invariant under change of reference frame.

In principle, the resourcefulness of a state cannot increase under application of a restricted class of operations. If such operations could transform state ρ into state σ, ρ must be considered at least as resourceful as σ for any task achievable with these operations. Thus the state ρ is more entangled than σ when σ can be produced from ρ by means of LOCC sequences of operations, and ρ has more frameness when ρ can be converted to σ through frame-invariant operations.

Entanglement can be quantified by entanglement monotones. An entanglement monotone f assigns a real number (usually greater than or equal to zero) to each state ρ with the property that $f(\rho) \geq f(\rho')$ if ρ' can be obtained from ρ via LOCC sequences of operations. This is now regarded as the sole requirement of an entanglement monotone [15], though further axioms were once required [16]. Frameness can be quantified similarly: a frameness monotone is a real-valued function of a state whose value is non-increasing when frame-invariant operations are applied to the state.

The collection of state mappings achievable with LOCC sequences of operations can be characterized by producing a collection of entanglement monotones known as Vidal's monotones. This collection $\{f_k\}$, k an index, has the property that $f_k(\rho) \geq f_k(\rho')$ for every k if and only if there is an LOCC sequence of operations transforming ρ into ρ' [11]. This result is known as Nielsen's theorem. Strictly speaking, Nielsen's theorem only holds for a restricted class of states known as 'pure' states. I make this distinction clearer in the next chapter.

Similar theorems have been produced for other collections of operations. Entanglement catalysis, for example, can be viewed as a resource theory with a larger collection of allowed sequences of operations called eLOCC, for entanglement-assisted LOCC. Turgut's theorem [17] characterizes pure-state transformations under eLOCC restrictions by providing a collection of entanglement monotones whose monotonic behaviour for states ρ and ρ' is both necessary and sufficient for the existence of an eLOCC sequence of operations transforming ρ to ρ'. Finding such results for frameness theories is a subject of current research [18].

1.5 Results

My thesis presents new results for quantifying entanglement and frameness. The first result is a procedure for bounding the entanglement of any state that catalyzes an LOCC-restricted transformation. These bounds are expressed in terms of the generalized concurrence monotones [19]. As an undergraduate researcher, I discovered the techniques used to provide criteria on the entanglement of a catalyst state. As a graduate student, I found an example of where the bound is nontrivial and prepared this work for publication [20].

My main result, presented as Theorem 4.2, fully characterizes the frameness of a pure state in the case that the group relating possible frame choices is finite and cyclic. This result can be expressed in a new framework of 'relative monotones'. Rather than defining a collection of monotones to express the value of a resource, we present a single function that characterizes the relative frameness of one state with respect to another.

The framework of relative monotones subsumes the common framework of monotones. Precedent exists for rethinking this framework: the definition of an entanglement monotone has previously been revised due to inadequacies discovered in the original definition [15, 21]. In the final chapter of my thesis, I discuss the outlook for the 'relative' approach to resource quantification.

Chapter 2

The formalism of quantum informational resource theories

In this chapter, I present much of the terminology that will be used throughout the thesis. The central concept is that of a quantum state, which is a mathematical object that represents all known information about a physical system. A quantum state then enables computation of all possible outcomes for any measurements, as well as the likelihood of each outcome. A quantum state may serve as a resource for the accomplishment of various kinds of quantum information processing tasks.

A given quantum information processing task often requires a specific state as a resource. The processing of quantum states is modelled through the application of quantum channels. Certain types of processing cannot increase the resourcefulness of a quantum state. Entanglement, for example, cannot increase under application of LOCC sequences of operations. Such sequences are modelled by LOCC channels. Similarly, frame-invariant channels cannot increase the frameness of a state. LOCC channels or frame-invariant channels cannot increase the entanglement or frameness, respectively, of a state. An entanglement monotone is a real-valued function of states that is non-increasing under the action of LOCC channels, and frameness monotones are non-increasing under the action of frame-invariant channels. Monotones then exist for any resource theory that presents such a well-defined collection of channels that do not increase the resourcefulness of states.

I give a technical introduction to quantum states and quantum channels in section 2.1, which culminates in a general definition of a monotone. Sections 2.2 and 2.3 present the restrictions of LOCC and frame-invariance, respectively.

2.1 States and measurements

A quantum mechanical experiment may be operationally described in two stages: preparation and measurement. A physical system is prepared in some state, and then various possible outcomes are physically distinguished. This preparation can be described with a mathematical object known as a quantum state.

Definition 2.1. A Hilbert space $\mathscr{H}$ is assigned to every quantum system. The collection $\mathscr{B}(\mathscr{H})$ of bounded linear operators $B : \mathscr{H} \to \mathscr{H}$ is known as the *state space* for that system. A *quantum state* is a trace-one, positive-semidefinite, self-adjoint, bounded-linear operator $\rho : \mathscr{H} \to \mathscr{H}$. A rank-one quantum state is called *pure*; otherwise the state is *mixed*. We assume $\dim(\mathscr{H}) < \infty$ throughout.

Pure states are thus projectors onto one-dimensional subspaces of $\mathscr{H}$. Each one-dimensional subspace of $\mathscr{H}$ is the span of a unit vector, called a 'ket' and denoted $|\psi\rangle \in \mathscr{H}$. The dual of the subspace $\text{span}\{|\psi\rangle\} \subset \mathscr{H}$ is then the span of the covector $\langle\psi| \in \mathscr{H}^*$, or 'bra', of $|\psi\rangle$. The inner product of $|\psi\rangle$ and $|\phi\rangle$ is then denoted $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$, which is called a 'bracket'. We have $\langle\psi|\psi\rangle = 1$ for every unit vector $|\psi\rangle \in \mathscr{H}$. The outer product of $|\psi\rangle$ with $|\phi\rangle$ is denoted $|\psi\rangle\langle\phi| = |\psi\rangle \otimes \langle\phi|$.

Every pure state can then be written $|\psi\rangle\langle\psi|$ for some $|\psi\rangle \in \mathscr{H}$. When referring to pure states, we will often refer only to the unit vector $|\psi\rangle \in \mathscr{H}$. Note that the choice of $|\psi\rangle$ is unique up to a phase: $|\psi'\rangle\langle\psi'| = |\psi\rangle\langle\psi|$ iff $|\psi'\rangle = \exp(\iota\theta)\,|\psi\rangle$ for some $\theta \in \mathbb{R}$ (where $\iota = \sqrt{-1}$). By the spectral theorem [22], every mixed state can be written as $\rho = \sum_\alpha p_\alpha\,|\psi_\alpha\rangle\langle\psi_\alpha|$ for some orthonormal set $\{|\psi_\alpha\rangle\} \subset \mathscr{H}$ indexed by α. Each $p_\alpha \geq 0$ because ρ is positive-semidefinite, and $\sum_\alpha p_\alpha = 1$ because $\text{Tr}(\rho) = 1$.

A quantum mechanical measurement is a physical process yielding information about the state of a system. Such a measurement takes place by distinguishing between previously indistinguishable aspects of a system; usually by disturbing the system. The

outcome of a measurement will generally be indeterministic: many different possible outcomes with corresponding probabilities are to be expected. Formally, a measurement is a choice of operators $\{E_k\} \subset \mathscr{B}(\mathscr{H})$ (for some state space $\mathscr{B}(\mathscr{H})$ and some index k) such that $\sum_k E_k^\dagger E_k \leq I$ (that is, $\sum_k E_k^\dagger E_k$ is a positive-semidefinite operator with all eigenvalues at most one). After the measurement is performed, the resulting state of the system is

$$\sigma_k = \frac{E_k \rho E_k^\dagger}{\mathrm{Tr}\left(E_k^\dagger E_k \rho\right)} \tag{2.1}$$

and the probability of obtaining this outcome is $\mathrm{Tr}\left(E_k^\dagger E_k \rho\right)$.

Processing of the physical system can take place between the preparation and measurement stages of the system. The apparatus used in the experiment could be recalibrated, for example, or processing could occur between the preparation and measurement stages. All such processing may be described through the use of quantum channels.

Definition 2.2. A bounded linear map $\mathcal{E} : \mathscr{B}\left(\mathbb{C}^n\right) \to \mathscr{B}\left(\mathbb{C}^m\right)$ (for natural numbers n and m) is *positive* if $\mathcal{E}(A)$ is a positive-semidefinite operator whenever $A \in \mathscr{B}(\mathscr{H})$ is positive-semidefinite. $\mathcal{E}$ is *completely positive* if $\mathcal{I}_k \otimes \mathcal{E} : \mathscr{B}\left(\mathbb{C}^k \otimes \mathbb{C}^n\right) \to \mathscr{B}\left(\mathbb{C}^k \otimes \mathbb{C}^m\right)$ is positive for each natural number k for $\mathcal{I}_k : \mathscr{B}\left(\mathbb{C}^k\right) \to \mathscr{B}\left(\mathbb{C}^k\right)$ the identity map. If $\mathscr{H}_1$ and $\mathscr{H}_2$ are Hilbert spaces assigned to physical systems, a completely positive map $\mathcal{E} : \mathscr{B}\left(\mathscr{H}_1\right) \to \mathscr{B}\left(\mathscr{H}_2\right)$ is called a *quantum channel*.

Quantum channels are required to be completely positive rather than positive because the physical process described by the channel $\mathcal{E}$ over a Hilbert space $\mathscr{H}$ can instead be described as $\mathcal{E} \otimes \mathcal{I}$ over $\mathscr{H} \otimes \mathscr{H}'$, where $\mathscr{H}'$ is the Hilbert space representing any ancillary physical system to which nothing is being done.

Definition 2.3. If $\mathcal{E} : \mathscr{B}\left(\mathbb{C}^n\right) \to \mathscr{B}\left(\mathbb{C}^m\right)$ is a completely positive map and $A \in \mathscr{B}\left(\mathbb{C}^n\right)$ is any positive-semidefinite operator, there exists a collection of operators $\{E_k : \mathbb{C}^n \to \mathbb{C}^m\}$

(where k is an index) such that $\sum_k E_k^\dagger E_k \leq I$ (that is, every eigenvalue of $\sum_k E_k^\dagger E_k$ is no greater than one) and $\mathcal{E}(A) = \sum_k E_k A E_k^\dagger$ [23]. Such a representation of a quantum channel is called a *Kraus representation*, or *operator-sum representation* [24], of a channel. The operators E_k are *Kraus operators*.

The Kraus representation of a quantum channel $\mathcal{E}$ is not unique [23]. Consider a Kraus representation $\{A_k\}$ of a channel $\mathcal{E}$, where $k \in K$ is an index. Choose any other index set L with cardinality not less than that of K and define a collection $\{u_{lk} \in \mathbb{C} | k \in K, l \in L\}$ so that

$$\sum_{l \in L} u_{lk}^* u_{lk'} = \begin{cases} 1 & \text{if } k = k', \\ 0 & \text{if } k \neq k'. \end{cases} \tag{2.2}$$

Define $B_l = \sum_k u_{lk} A_k$ for each $l \in L$. Then, for any $\rho \in \mathscr{B}(\mathscr{H})$,

$$\sum_{l \in L} B_l \rho B_l^\dagger = \sum_{k,k' \in K, l \in L} (u_{lk} A_k) \, \rho \left(u_{lk'}^* A_{k'}^\dagger \right) = \sum_{k \in K} A_k \rho A_k^\dagger \tag{2.3}$$

and $\sum_l B_l^\dagger B_l = \sum_k A_k^\dagger A_k \leq I$. Thus $\{B_l\}$ is another Kraus representation of $\mathcal{E}$. This fact is the 'unitary freedom' of Kraus operators [24]; notice that, if L and K have the same cardinality, the matrix with entries u_{lk} is a unitary matrix.

Many quantum channels are physically or practically impossible. A restricted collection $\mathfrak{T}$ of allowable channels imposes a pre-order on the collection of quantum states: $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$ if there is an $\mathcal{E} \in \mathfrak{T}$ with $\mathcal{E}(\rho) = \rho'$ (otherwise $\rho \overset{\mathfrak{T}}{\not\mapsto} \rho'$). If $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$ and $\rho' \overset{\mathfrak{T}}{\mapsto} \rho$, we say that $\rho \overset{\mathfrak{T}}{\sim} \rho'$ (otherwise $\rho \overset{\mathfrak{T}}{\not\sim} \rho'$). ρ is a 'resource' if there is a state σ such that $\sigma \overset{\mathfrak{T}}{\not\mapsto} \rho$ (otherwise, ρ is a 'non-resource').

Definition 2.4. Let $\mathfrak{T}$ be a collection of quantum channels $\{\mathcal{E} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{H})\}$ and $C \subset \mathscr{B}(\mathscr{H})$ be a collection of states. A $\mathfrak{T}$-*monotone* is a function $f : C \to \mathbb{R}$ with the property that $f(\rho) \geq f(\rho')$ if $\rho, \rho' \in C$ satisfy $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$.

If f is a $\mathfrak{T}$-monotone and ρ and σ are two non-resource states, then $f(\rho) = f(\sigma)$ because $\rho \overset{\mathfrak{T}}{\sim} \sigma$. Thus f is constant on the set of non-resource states. It is common to define

our monotone such that $f(\rho) = 0$ for non-resource states ρ. Notice that our definition allows a monotone to be defined only on a restricted collection of states. Throughout this thesis, monotones are often defined only for pure states.

Entanglement monotones are the prototypical example of monotone. In the next section we will define the collection $\mathfrak{L}$ of quantum channels that can be achieved through LOCC sequences of operations. Such operations cannot increase entanglement, and a state σ is disentangled if for every ρ there is an LOCC channel $\mathcal{E}$ such that $\mathcal{E}(\rho) = \sigma$. An entanglement monotone is then an $\mathfrak{L}$-monotone. Frameness monotones are presented in a similar fashion.

2.2 LOCC channels

In this section, I discuss LOCC channels. These are quantum channels achievable via LOCC sequences of operations. The characterization of all such channels is difficult [21], but characterizing the collection of pure-state transformations is made simpler by a result of Lo and Popescu [25]. This work allows us to prove Nielsen's theorem [11], which gives a collection of necessary and sufficient conditions for the existence a transformation $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$. I express these conditions in terms of a collection of $\mathfrak{L}$-monotones known as Vidal's monotones [12].

The Hilbert space associated to a composite physical system is the tensor product of the Hilbert spaces of each component system. Consider the simple case of two separate physical systems with Hilbert spaces $\mathscr{H}^A$ and $\mathscr{H}^B$. The minimal Hilbert space $\mathscr{H}^{AB}$ describing the joint physical system has a basis formed by choosing orthonormal bases for $\mathscr{H}^A$ and $\mathscr{H}^B$ and concatenating them. Suppose $\left\{|i\rangle^A\right\}$ and $\left\{|j\rangle^B\right\}$ are these respective bases. The state of physical system B can be prepared independently of A, so $|i\rangle^A |j\rangle^B$ is a pure state of the joint system, where i and j are chosen inde-

pendently. The Hilbert space for the joint system is given by $\mathscr{H}^{AB} = \mathscr{H}^{A} \otimes \mathscr{H}^{B} = \text{span}\left\{|i\rangle^{A} \otimes |j\rangle^{B} = |i\rangle^{A} |j\rangle^{B} = |ij\rangle^{AB}\right\}$, where $\otimes$ represents the Kronecker product.

Definition 2.5. A state $\rho \in \mathscr{B}\left(\mathscr{H}^{A} \otimes \mathscr{H}^{B}\right)$ is called *separable* if $\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B$ for some finite probability distribution p_i and collections of states $\left\{\rho_i^A \in \mathscr{H}^{A}\right\}$, $\left\{\rho_i^B \in \mathscr{H}^{B}\right\}$. A state that cannot be written in this way is called *entangled*.

Thus an entangled state cannot be written as a joint probability distribution of independent states of each subsystem. The correlations present in separable states could have been introduced using LOCC sequences of operations because the choice of index i may be transmitted classically. Note that I have defined entanglement over a 'bipartite' Hilbert space $\mathscr{H}^{A} \otimes \mathscr{H}^{B}$, which corresponds to a physical system with only two subsystems. Multipartite separability and entanglement are defined over Hilbert spaces composed of more tensor products. I discuss only bipartite entanglement in this thesis.

The most general class of channels that do not increase entanglement are those achievable using only local operations (i.e. channels of the form $\mathcal{E}_A \otimes \mathcal{E}_B$, where $\mathcal{E}_A : \mathscr{B}\left(\mathscr{H}^{A}\right) \to \mathscr{B}\left(\mathscr{H}^{A}\right)$ and $\mathcal{E}_B : \mathscr{B}\left(\mathscr{H}^{B}\right) \to \mathscr{B}\left(\mathscr{H}^{B}\right)$) assisted by classical communication (meaning Alice and Bob may communicate measurement outcomes). This choice of restriction is justified because local operations can never create entanglement, as entanglement is a global (with respect to a partition) property of a quantum system. Furthermore, entanglement cannot be increased by classical communication because entanglement is a purely quantum correlation.

Definition 2.6. A channel $\mathcal{E} : \mathscr{B}\left(\mathscr{H}^{A} \otimes \mathscr{H}^{B}\right) \to \mathscr{B}\left(\mathscr{H}^{A} \otimes \mathscr{H}^{B}\right)$ is called *separable* if it has a Kraus decomposition $\left\{K_i^A \otimes K_i^B\right\}$, where $\left\{K_i^A\right\}$ and $\left\{K_i^B\right\}$ are Kraus operators on $\mathscr{H}^{A}$ and $\mathscr{H}^{B}$ respectively. Every LOCC channel is separable, but not every separable channel is LOCC [21].

Proposition 2.1 (Lo and Popescu [25])**.** *If* $|\psi\rangle \in \mathscr{H}^{AB}$ *and* $|\phi\rangle \in \mathscr{H}^{AB}$ *are pure*

states satisfying $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$*, there exists a quantum channel* $\mathcal{E}$ *with Kraus decomposition* $\{K_i \otimes U_i\}$ *such that* $\mathcal{E}(|\psi\rangle\langle\psi|) = |\phi\rangle\langle\phi|$*, where* $\{K_i\}$ *is a collection of Kraus operators on* $\mathscr{H}^A$ *and* $\{U_i\}$ *is a collection of unitary operators on* $\mathscr{H}^B$*.*

An entanglement monotone is a function $f : C \subset \mathscr{B}\left(\mathscr{H}^A \otimes \mathscr{H}^B\right) \to \mathbb{R}$ (where C is some collection of states) such that $f(\rho) \geq f(\Lambda(\rho))$ for any LOCC channel Λ and any state $\rho \in C$ such that $\Lambda(\rho) \in C$. One can fully characterize the entanglement of a state by producing a (possibly infinite) collection of entanglement monotones $\{f_\alpha\}$, where α is an index, such that $\rho \overset{\mathfrak{L}}{\mapsto} \sigma$ if and only if $f_\alpha(\rho) \geq f_\alpha(\sigma)$ for each α. To know the value of $f_\alpha(\rho)$ for each α is to know the totality of possible transformations of ρ under LOCC and therefore how much entanglement can be extracted from a bipartite state ρ in principle. For pure states, such monotones can be defined in terms of the Schmidt coefficients [24].

Theorem 2.2. *Suppose* $|\psi\rangle \in \mathscr{H}^A \otimes \mathscr{H}^B$ *is a state vector. There exists a collection of orthonormal vectors* $\left\{|i\rangle^A\right\} \subset \mathscr{H}^A$ *and* $\left\{|i\rangle^B\right\} \subset \mathscr{H}^B$ *and a probability distribution* p_i *such that*

$$|\psi\rangle = \sum_i \sqrt{p_i}\, |i\rangle^A |i\rangle^B . \tag{2.4}$$

The numbers p_i *are called the* Schmidt coefficients *of the state* $|\psi\rangle$*.*

Thus two bipartite pure states $|\psi\rangle$ and $|\phi\rangle$ are interconvertible via LOCC channels (i.e. $|\psi\rangle \overset{\mathfrak{L}}{\sim} |\phi\rangle$) if and only if $|\psi\rangle$ and $|\phi\rangle$ possess the same Schmidt coefficients. Moreover, any conditions that determine whether $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$ or $|\psi\rangle \overset{\mathfrak{L}}{\not\mapsto} |\phi\rangle$ may be expressed in terms of the Schmidt coefficients of these states. It is convenient to define a unique 'Schmidt vector' for each bipartite pure state.

Definition 2.7. Suppose $\{p_i\}$ are the Schmidt coefficients of a bipartite pure state $|\psi\rangle \in \mathscr{H}^A \otimes \mathscr{H}^B$. The vector consisting of entries p_i arranged in decreasing order is called the *Schmidt vector* of $|\psi\rangle$ and is denoted $(\!(\psi)\!)$. The number of non-zero entries in the Schmidt vector is called the *Schmidt number* of the state $|\psi\rangle$.

Any conditions on the ability to enact $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$ then depend only on $(\!(\psi)\!)$ and $(\!(\phi)\!)$. Theorem 2.3 gives necessary and sufficient conditions for the existence of such a transformation. These conditions are placed on the values of Vidal's monotones for $|\psi\rangle$ and $|\phi\rangle$.

Definition 2.8. Let $|\psi\rangle \in \mathscr{H}^A \otimes \mathscr{H}^B$ be a pure state with Schmidt vector $(\!(\psi)\!) = (p_1, p_2, \ldots, p_n)$ (with Schmidt number less than or equal to n). *Vidal's monotones* are the functions

$$\begin{aligned} f_1(|\psi\rangle) &= 1 - p_1 \\ f_2(|\psi\rangle) &= 1 - (p_1 + p_2) \\ f_3(|\psi\rangle) &= 1 - (p_1 + p_2 + p_3) \\ &\vdots \\ f_{n-1}(|\psi\rangle) &= 1 - (p_1 + p_2 + \cdots + p_{n-1}) = p_n. \end{aligned} \tag{2.5}$$

Theorem 2.3 (Nielsen [11])**.** $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$ *if and only if* $f_k(|\psi\rangle) \geq f_k(|\phi\rangle)$ *for* $k = 1, \ldots, n-1$*, where* n *is the Schmidt number of* $|\psi\rangle$*.*

Given any two bipartite pure states $|\psi\rangle$ and $|\phi\rangle$, Nielsen's theorem allows us to determine whether $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$ or not. This characterization of pure-state LOCC transformations is provided in terms of a collection of entanglement monotones. Throughout my thesis, Nielsen's theorem is considered a model for the results I wish to present. Theorems 3.1 and 4.2 are direct analogues of Nielsen's theorem for other resource theories.

2.3 Frame-invariant channels

The frameness of a quantum state is its capacity for storing reference frame information. A simple case is the choice of $|0\rangle$ and $|1\rangle$ as logical 0 and 1 states for encoding quantum information. Suppose a sender, Alice, has made such a choice and transmits a message (say, $|010\rangle$) to a receiver, Bob. Bob is aware of Alice's choice of $|0\rangle$ and $|1\rangle$ but not of her

labels: he has chosen the states $|0\rangle'$ and $|1\rangle'$ and is not sure if $|0\rangle' = |0\rangle$ or $|0\rangle' = |1\rangle$. Bob must describe the message state $|010\rangle$ according to his best knowledge of the preparation of the state, which corresponds to an equal chance of having obtained $|010\rangle'$ or $|101\rangle'$. His state will therefore be $\frac{1}{2}\left(|010\rangle\langle 010|' + |101\rangle\langle 101|'\right)$.

Naturally, Alice may alleviate this restriction by initializing communication through sending Bob the state $|0\rangle$. Bob then performs the measurement $\left\{|0\rangle\langle 0|', |1\rangle\langle 1|'\right\}$, yielding outcome $|0\rangle'$ or $|1\rangle'$ depending on whether $|0\rangle' = |0\rangle$ or $|0\rangle' = |1\rangle$. Bob then gains perfect knowledge of Alice's choice of reference frame.

Alice cannot communicate her choice of $|0\rangle$ by sending an eigenstate of the operator $X = |1\rangle\langle 0| + |0\rangle\langle 1|$. For example, if Alice sends the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, Bob will notice that $|\psi\rangle\langle\psi| = X|\psi\rangle\langle\psi|X$ so he may not obtain any information about Alice's choice of reference frame.

The quality of a state $|\psi\rangle$ for transmitting a choice of $b = 0, 1$ in the above example is known as the Z_2-frameness of $|\psi\rangle$, where Z_n refers to the cyclic group on n letters throughout my thesis. In general, it is assumed that all possible reference frame choices are related by some group of automorphisms of the state space. This assumption was defended in chapter 1. In the case we have just discussed, the group relating possible basis choices was $\{I, X\}$, which is the image of a representation of Z_2 on the Hilbert space span $\{|0\rangle, |1\rangle\}$.

A frameness theory is then presented by defining a unitary representation T of a group G on the automorphisms of the Hilbert space $\mathscr{H}$ associated to the physical system being analyzed. This representation is chosen to relate all reference frame choices. For convenience, G is assumed to be compact so that averages over all possible reference frame choices may be computed using the Haar measure. Such averages are calculated in the case of maximal ignorance of a choice of reference frame.

Suppose the measurement $\{E_k\}$ is made with respect to reference frame A. If the

outcome of this measurement is to be described with respect to a different reference frame B, the measurement must be described by $\left\{T(g)E_kT(g)^\dagger\right\}$, where $g \in G$ represents the translation from reference frame A to reference frame B. A measurement is then frame-invariant when $T(g)E_kT(g)^\dagger = E_k$ for each $g \in G$.

The same principle applies when performing quantum channels. If $\{E_k\}$ is the Kraus decomposition of a quantum channel $\mathcal{E}$, the Kraus decomposition of the translated channel $\mathcal{E}'$ should be $\left\{T(g)E_kT(g)^\dagger\right\}$. Thus

$$\mathcal{E}'(\rho) = \sum_k T(g)E_kT(g)^\dagger\rho T(g)E_k^\dagger T(g)^\dagger = T(g)\mathcal{E}\left(T(g)^\dagger\rho T(g)\right)T(g)^\dagger. \tag{2.6}$$

This is not to say that each Kraus representation is invariant under the action of G: in general, we expect that $T(g)E_kT(g)^\dagger \neq E_k$. By the unitary freedom of the Kraus representation, there is a unitary operator $\mathcal{U}(g)$ for each $g \in G$ over the linear span of the collection $\{E_k\}$ such that $\mathcal{U}(g)\left(E_k\right) = T(g)E_kT(g)^\dagger$. This collection $\{\mathcal{U}(g)\}$ forms a unitary representation of G on $\operatorname{span}\{E_k\}$ which may therefore be block-diagonalized by the Peter-Weyl theorem. This fact may be used to prove the following theorem.

Theorem 2.4 (Gour and Spekkens [18])**.** *A G-invariant operation admits a Kraus decomposition with Kraus operators $\{K_{jm\alpha}\}$ where j indexes the irreducible representations of G, m indexes a basis for the irreducible representation j, and α is a multiplicity index for m. This Kraus representation satisfies*

$$T(g)K_{jm\alpha}T(g)^\dagger = \sum_{m'} u^{(j)}_{mm'}(g)K_{jm'\alpha}, \forall g \in G, \tag{2.7}$$

where $u^{(j)}$ is an irreducible unitary representation of G on the linear span of $\{K_{jm\alpha}\}$.

In the particular case that G is an abelian group, Theorem 2.4 implies that there is a Kraus representation $\{K_{j,\alpha}\}$ for any G-invariant quantum channel such that $T(g)K_{j,\alpha}T(g)^\dagger = \exp\left(\iota\theta_{g,j}\right)K_{j,\alpha}$, where $\theta_{g,j} \in \mathbb{R}$ is an angle depending on g and j. This fact is crucial to the proof of Theorem 4.2.

I have thus presented entanglement and frameness within a unified perspective and given tools for the analysis of both types of resource. In the next chapter, I discuss an extension of LOCC channels that includes the ability to 'borrow' entanglement to enact otherwise prohibited pure-state LOCC transformations. I return to frameness in chapter four.

Chapter 3

Entanglement catalysis

This chapter presents results on the quantification of an entanglement catalyst. An entanglement catalyst is an entangled state that can be used as a resource for enacting some previously prevented state transformation. After the transformation is enacted, however, the catalyst state is returned unharmed. Thus there are state transformations of the form $|\psi\rangle\,|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle\,|\chi\rangle$ even when $|\psi\rangle \overset{\mathfrak{L}}{\not\mapsto} |\phi\rangle$.

This is a consequence of Nielsen's theorem. Suppose that $(\!(\psi)\!) = \left(\frac{2}{5}, \frac{2}{5}, \frac{1}{10}, \frac{1}{10}\right)$ and $(\!(\phi)\!) = \left(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}, 0\right)$. Then $|\psi\rangle \overset{\mathfrak{L}}{\not\mapsto} |\phi\rangle$ because

$$f_2(|\psi\rangle) = 1 - \left(\frac{2}{5} + \frac{2}{5}\right) < 1 - \left(\frac{1}{2} + \frac{1}{4}\right) = f_2(|\phi\rangle). \tag{3.1}$$

Now suppose $(\!(\chi)\!) = \left(\frac{3}{5}, \frac{2}{5}\right)$ for some ancillary state $|\chi\rangle$. We can use Nielsen's theorem to find that $|\psi\rangle\,|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle\,|\chi\rangle$. Thus the state $|\chi\rangle$ is used as a resource without being consumed. Such states are known as entanglement catalysts [4].

We must be cautious to note that the 'catalyzed' transformation takes place over a larger Hilbert space. Suppose $|\psi\rangle$ and $|\phi\rangle$ were both state vectors in $\mathscr{H}^{AB} = \mathscr{H}^{A} \otimes \mathscr{H}^{B}$, while $|\chi\rangle$ is an element of $\mathscr{H}^{A'B'} = \mathscr{H}^{A'} \otimes \mathscr{H}^{B'}$. Then an LOCC channel $\mathcal{E}$ satisfying $\mathcal{E}(|\psi\rangle\langle\psi| \otimes |\chi\rangle\langle\chi|) = |\phi\rangle\langle\phi| \otimes |\chi\rangle\langle\chi|$ is LOCC with respect to the bipartition $\mathscr{H}^{AA'} \otimes \mathscr{H}^{BB'}$, where $\mathscr{H}^{XX'} = \mathscr{H}^{X} \otimes \mathscr{H}^{X'}$ $(X = A, B)$. Any state transformation that can be accomplished in this fashion is said to be achievable by 'entanglement-assisted' LOCC channels (eLOCC), the collection of which is denoted $\mathfrak{L}'$.

Turgut's theorem [17] provides a collection of necessary and sufficient conditions for the existence of a pure state transformation $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$. These necessary and sufficient conditions presented in section 3.1 as a collection of $\mathfrak{L}'$ monotones. Turgut's theorem does

not provide conditions on the catalyst itself. The purpose of this chapter is to present my results on characterizing possible catalysts for a given eLOCC transformation of pure states. These results are obtained through consideration of a collection of entanglement monotones called the generalized concurrences [19]. I discuss the concurrences in section 3.2 and, in particular, show that some of these entanglement monotones are not $\mathfrak{L}'$-monotones. Analysis of the failure of certain concurrences to behave monotonically under entanglement-assisted LOCC channels leads to various necessary conditions imposed on a potential catalyst state; most prominently, a lower bound on the Schmidt number of a catalyst state. This result is presented in section 3.3.

3.1 The trumping relation

Nielsen's theorem and Turgut's theorem play similar roles in the characterization of $\mathfrak{L}$ pure-state transformations and $\mathfrak{L}'$ pure-state transformations, respectively. Both theorems present a collection of monotones that completely characterize the resourcefulness of a pure state with respect to the relevant restricted collection of channels.

Nielsen's theorem was originally presented in terms of a preorder $\prec$ on real vectors called 'majorization' so that $|\psi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle$ if and only if $(\!(\psi)\!) \prec (\!(\phi)\!)$. Entanglement-assisted LOCC state transformations then exist if and only if there is a state $|\chi\rangle$ such that $(\!(\psi)\!) \otimes (\!(\chi)\!) \prec (\!(\phi)\!) \otimes (\!(\chi)\!)$. The 'trumping' preorder $\prec_T$ is then defined so that $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$ if and only if $(\!(\psi)\!) \prec_T (\!(\phi)\!)$. Turgut's theorem provides necessary and sufficient conditions on $\boldsymbol{x}$ and $\boldsymbol{y}$ to determine if $\boldsymbol{x} \prec_T \boldsymbol{y}$.

Definition 3.1. Suppose $\boldsymbol{p} = (p_1,\ p_2,\ \ldots,\ p_n)$ and $\boldsymbol{q} = (q_1,\ q_2,\ \ldots,\ q_n)$ are real vectors. Define $\boldsymbol{p}^{\downarrow} = \left(p_1^{\downarrow},\ p_2^{\downarrow},\ \ldots,\ p_n^{\downarrow}\right)$ such that $p_k^{\downarrow} \geq p_{k+1}^{\downarrow}$ and there is a permutation σ so that $p_k^{\downarrow} = p_{\sigma(k)}$. Define $\boldsymbol{q}^{\downarrow}$ similarly. Then $\boldsymbol{p}$ is *majorized* by $\boldsymbol{q}$ ($\boldsymbol{p} \prec \boldsymbol{q}$) if, for each $1 \leq k \leq n$, $\sum_{i=1}^{k} p_i^{\downarrow} \leq \sum_{i=1}^{k} q_i^{\downarrow}$.

Thus majorization provides a preorder on the collection of real vectors and a partial order on the collection of Schmidt vectors in particular. The language of majorization is sometimes more convenient than that of monotones because the theory of majorization is well-established [26]. The phenomenon of entanglement catalysis is a consequence of the existence of vectors $\boldsymbol{z} \in \mathbb{R}^m$ such that $\boldsymbol{x} \otimes \boldsymbol{z} \prec \boldsymbol{y} \otimes \boldsymbol{z}$ for some vectors $\boldsymbol{x} \not\prec \boldsymbol{y} \in \mathbb{R}^n$.

Definition 3.2. $\boldsymbol{x} \in \mathbb{R}^n$ is *trumped* by $\boldsymbol{y} \in \mathbb{R}^n$ ($\boldsymbol{x} \prec_T \boldsymbol{y}$) if there exists $\boldsymbol{z} \in \mathbb{R}^m$ for some m such that $\boldsymbol{x} \otimes \boldsymbol{z} \prec \boldsymbol{y} \otimes \boldsymbol{z}$.

It is straightforward to determine if $\boldsymbol{x} \prec \boldsymbol{y}$ for some pair of vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ by the definition of majorization, but deciding if $\boldsymbol{x} \prec_T \boldsymbol{y}$ when $\boldsymbol{x} \not\prec \boldsymbol{y}$ requires a proof of the existence of a vector $\boldsymbol{z}$ such that $\boldsymbol{x} \otimes \boldsymbol{z} \prec \boldsymbol{y} \otimes \boldsymbol{z}$. There is, as yet, no constructive method to obtain such a vector. The existence of $\boldsymbol{z}$ may be inferred by evaluating the Rényi entropies [27] on $\boldsymbol{x}$ and $\boldsymbol{y}$.

Definition 3.3. Let $\boldsymbol{x} \in \mathbb{R}^n$ be entry-wise strictly positive with entries summing to one. The *Rényi entropy* of order $0 \leq \nu \leq \infty$ of $\boldsymbol{x}$ is given by

$$S_\nu(\boldsymbol{x}) = \frac{1}{1-\nu} \log \left(\sum_{i=1}^{n} x_i^\nu \right) \tag{3.2}$$

if $\nu \neq 0, 1, \infty$. $S_0(\boldsymbol{x}) = -\log n$, $S_1(\boldsymbol{x}) = -\sum_i x_i \log x_i$, and $S_\infty(\boldsymbol{x}) = \max_i x_i$. Notice that equation 3.2 is well-defined for all real ν. This assumption will be made in Theorem 3.1.

Theorem 3.1 (Turgut [17])**.** *Suppose $\boldsymbol{x}$, $\boldsymbol{y} \in \mathbb{R}^n$ are entry-wise positive vectors such that $\boldsymbol{y} \not\prec \boldsymbol{x}$. $\boldsymbol{x} \prec_T \boldsymbol{y}$ if and only if, for every $\nu \in \mathbb{R}$, $\frac{1}{\nu} S_\nu(\boldsymbol{x}) > \frac{1}{\nu} S_\nu(\boldsymbol{y})$.*

Thus Turgut's theorem fully characterizes the trumping relation by producing a collection of 'catalytic monotones', which are monotones under the collection of entanglement-assisted LOCC channels. Explicitly, we may define 'Turgut's monotones' by $T_\nu(|\psi\rangle) =$

$\frac{1}{\nu}S_\nu(((\psi)))$ for any $\nu \in \mathbb{R}$. Turgut's theorem then tells us that $|\psi\rangle \overset{\mathfrak{C}'}{\mapsto} |\phi\rangle$ if and only if $T_\nu(|\psi\rangle) > T_\nu(|\phi\rangle)$ (with the caveat that $|\phi\rangle \overset{\mathfrak{C}}{\not\mapsto} |\psi\rangle$).

In the next section, I provide tools to gain information about a $\boldsymbol{z}$ satisfying $\boldsymbol{x} \otimes \boldsymbol{z} \prec \boldsymbol{y} \otimes \boldsymbol{z}$ when $\boldsymbol{x} \not\prec \boldsymbol{z}$. Such conditions then impose restrictions on the possible Schmidt vectors for a catalyst state.

3.2 Factorizing concurrences

The generalized concurrences [19], as their name suggests, are generalizations of an entanglement monotone called the 'concurrence', which is defined only for entangled pairs of qubits. The original concurrence [28] is useful because it is easy to calculate and fully characterizes the entanglement of a pure state of a qubit pair. There are multiple generalizations of the concurrence when considering pairs of d-level quantum systems ($d > 2$). The I-concurrence [29] and G-concurrence [19] are two examples of such generalizations.

Both the I-concurrence and G-concurrence are members of a family of monotones known as the generalized concurrences. For a d-level quantum system, we may define $d - 1$ concurrences. The first of these corresponds to the I-concurrence and the last corresponds to the G-concurrence. The family of concurrences is most simply defined in terms of the 'elementary symmetric polynomials'.

Definition 3.4. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ be any n-tuple of real numbers. The *elementary*

symmetric polynomials are given by

$$\begin{aligned}
\mathfrak{e}_0(\boldsymbol{x}) &= 1, \\
\mathfrak{e}_1(\boldsymbol{x}) &= x_1 + x_2 + \cdots + x_n, \\
\mathfrak{e}_2(\boldsymbol{x}) &= \textstyle\sum_{i<j} x_i x_j, \\
\mathfrak{e}_3(\boldsymbol{x}) &= \textstyle\sum_{i<j<k} x_i x_j x_k, \\
&\vdots \\
\mathfrak{e}_n(\boldsymbol{x}) &= x_1 x_2 \cdots x_n.
\end{aligned} \tag{3.3}$$

The k^{th} *concurrence* of a state vector $|\psi\rangle$ (with Schmidt vector $(\!(\psi)\!) \in \mathbb{R}^n$) is then given by

$$C_k(|\psi\rangle) := \left(\frac{\mathfrak{e}_k((\!(\psi)\!))}{\mathfrak{e}_k\left(\frac{1}{n}, \frac{1}{n}, \cdots, \frac{1}{n}\right)} \right)^{\frac{1}{k}} \tag{3.4}$$

for $k \geq 2$. We consider $C_0(|\psi\rangle) = C_1(|\psi\rangle) = 1$.

The second concurrence may be written as $C_2(|\psi\rangle) = \frac{1}{2}\sqrt{1 - \mathfrak{p}_2((\!(\psi)\!))}$, where $\mathfrak{p}_k$ represents the k^{th} 'power-sum symmetric polynomial'. This definition corresponds more directly to the literature [29].

Definition 3.5. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ be any n-tuple of real numbers. The *power-sum symmetric polynomials* are given by

$$\mathfrak{p}_k(\boldsymbol{x}) = x_1^k + x_2^k + \cdots + x_n^k \tag{3.5}$$

for $k = 1 \ldots n$.

Suppose the Schmidt numbers of $|\psi\rangle$ and $|\phi\rangle$ are equal (to n). If $k \neq 2$ and $k \neq n$, it is possible that $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$ but $C_k(|\psi\rangle) < C_k(|\phi\rangle)$. By contrast, if $|\chi\rangle$ is a catalyst of Schmidt number m, $C_k(|\psi\rangle|\chi\rangle) \geq C_k(|\phi\rangle|\chi\rangle)$ for any $k = 2, 3, \ldots, nm$. I now give expressions for $C_k(|\psi\rangle|\chi\rangle)$ as a polynomial of the concurrences of $|\psi\rangle$ and $|\chi\rangle$. These expressions are found by computing $\mathfrak{e}_k(\boldsymbol{x} \otimes \boldsymbol{z})$ in terms of the elementary symmetric functions of $\boldsymbol{x}$ and $\boldsymbol{z}$.

This computation requires the use of Newton's Identities. In section 3.3, I demonstrate how such expressions yield conditions on the values of the concurrences of $|\chi\rangle$.

Theorem 3.2 (Newton's Identities)**.** *Let* $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ *be any* n*-tuple of real numbers and* $1 \leq k \leq n$ *be any integer. Then*

$$k\mathfrak{e}_k(\boldsymbol{x}) = \sum_{\ell=1}^{k} (-1)^{\ell-1} \mathfrak{e}_{k-\ell}(\boldsymbol{x})\, \mathfrak{p}_\ell(\boldsymbol{x}). \tag{3.6}$$

We may use these identities to write the elementary symmetric polynomials in terms of the power sum polynomials, and vice versa.

$$\begin{aligned}
\mathfrak{e}_1 &= \mathfrak{p}_1 & \mathfrak{p}_1 &= \mathfrak{e}_1 \\
\mathfrak{e}_2 &= \tfrac{1}{2}(\mathfrak{p}_1^2 - \mathfrak{p}_2) & \mathfrak{p}_2 &= \mathfrak{e}_1^2 - 2\mathfrak{e}_2 \\
\mathfrak{e}_3 &= \tfrac{1}{6}(\mathfrak{p}_1^3 - 3\mathfrak{p}_1\mathfrak{p}_2 + 2\mathfrak{p}_3) & \mathfrak{p}_3 &= \mathfrak{e}_1^3 - 3\mathfrak{e}_1\mathfrak{e}_2 + 3\mathfrak{e}_3 \\
\mathfrak{e}_4 &= \tfrac{1}{24}(\mathfrak{p}_1^4 - 6\mathfrak{p}_1^2\mathfrak{p}_2 + 3\mathfrak{p}_2^2 + 8\mathfrak{p}_1\mathfrak{p}_3 - 6\mathfrak{p}_4) & \mathfrak{p}_4 &= \mathfrak{e}_1^4 - 4\mathfrak{e}_1^2\mathfrak{e}_2 + 2\mathfrak{e}_2^2 + 4\mathfrak{e}_1\mathfrak{e}_3 - 4\mathfrak{e}_4 \\
&\vdots & &\vdots
\end{aligned} \tag{3.7}$$

Now we can exploit the identity $\mathfrak{p}_k(\boldsymbol{x} \otimes \boldsymbol{z}) = \mathfrak{p}_k(\boldsymbol{x})\mathfrak{p}_k(\boldsymbol{z})$ (where $\boldsymbol{x} \in \mathbb{R}^n$ and $\boldsymbol{z} \in \mathbb{R}^m$) to inductively derive what I call the 'factoring identities' for the elementary symmetric polynomials. The first of Newton's identities tells us that $\mathfrak{e}_1 = \mathfrak{p}_1$ (which was already clear), so we can plainly see that

$$\mathfrak{e}_1(\boldsymbol{x} \otimes \boldsymbol{z}) = \mathfrak{p}_1(\boldsymbol{x} \otimes \boldsymbol{z}) = \mathfrak{p}_1(\boldsymbol{x})\mathfrak{p}_1(\boldsymbol{z}) = \mathfrak{e}_1(\boldsymbol{x})\mathfrak{e}_1(\boldsymbol{z}). \tag{3.8}$$

The second identity is more complicated. Equation 3.7 implies

$$\begin{aligned}
\mathfrak{e}_2(\boldsymbol{x} \otimes \boldsymbol{z}) &= \tfrac{1}{2}(\mathfrak{p}_1(\boldsymbol{x} \otimes \boldsymbol{z})^2 - \mathfrak{p}_2(\boldsymbol{x} \otimes \boldsymbol{z})) \\
&= \tfrac{1}{2}(\mathfrak{p}_1(\boldsymbol{x})^2\mathfrak{p}_1(\boldsymbol{z})^2 - \mathfrak{p}_2(\boldsymbol{x})\mathfrak{p}_2(\boldsymbol{z})) \\
&= \tfrac{1}{2}(\mathfrak{e}_1(\boldsymbol{x})^2\mathfrak{e}_1(\boldsymbol{z})^2 - (\mathfrak{e}_1^2(\boldsymbol{x}) - 2\mathfrak{e}_2(\boldsymbol{x}))(\mathfrak{e}_1^2(\boldsymbol{z}) - 2\mathfrak{e}_2(\boldsymbol{z}))) \\
&= \mathfrak{e}_1(\boldsymbol{x})^2\mathfrak{e}_2(\boldsymbol{z}) + \mathfrak{e}_2(\boldsymbol{x})\mathfrak{e}_1(\boldsymbol{z})^2 - 2\mathfrak{e}_2(\boldsymbol{x})\mathfrak{e}_2(\boldsymbol{z}).
\end{aligned} \tag{3.9}$$

A similar calculation gives

$$\begin{aligned}\mathfrak{e}_3(\boldsymbol{x}\otimes\boldsymbol{z}) &= \mathfrak{e}_3(\boldsymbol{x})\mathfrak{e}_1(\boldsymbol{z})^3+\mathfrak{e}_1^3(\boldsymbol{x})\mathfrak{e}_3(\boldsymbol{z})+\mathfrak{e}_1(\boldsymbol{x})\mathfrak{e}_2(\boldsymbol{x})\mathfrak{e}_1(\boldsymbol{z})\mathfrak{e}_2(\boldsymbol{z})-2\mathfrak{e}_1(\boldsymbol{x})\mathfrak{e}_2(\boldsymbol{x})\mathfrak{e}_3(\boldsymbol{z})\\ &\quad -2\mathfrak{e}_3(\boldsymbol{x})\mathfrak{e}_1(\boldsymbol{z})\mathfrak{e}_2(\boldsymbol{z})+3\mathfrak{e}_3(\boldsymbol{x})\mathfrak{e}_3(\boldsymbol{z}).\end{aligned} \tag{3.10}$$

The expressions for $\mathfrak{e}_k(\boldsymbol{x}\otimes\boldsymbol{z})$ become more complicated as k becomes larger. I am presently unaware of a general formula giving these expressions. As k approaches nm, however, the expressions become simpler. Indeed,

$$\mathfrak{e}_{nm}(\boldsymbol{x}\otimes\boldsymbol{z})=\prod_{i=1}^{n}\prod_{j=1}^{m}x_iz_j=\left(\prod_{i=1}^{n}x_i\right)^m\left(\prod_{j=1}^{m}z_j\right)^n=\mathfrak{e}_n(\boldsymbol{x})^m\mathfrak{e}_m(\boldsymbol{z})^n. \tag{3.11}$$

To calculate expressions for k close to nm, we make use of the following lemma.

Lemma 3.3. *Suppose* $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$ *with* $x_k\neq 0$ *for each* k. *Define* $\boldsymbol{x}^{-1}=\left(\frac{1}{x_1},\frac{1}{x_2},\cdots,\frac{1}{x_n},\right)$. *Then* $\mathfrak{e}_k\left(\boldsymbol{x}^{-1}\right)=\mathfrak{e}_{n-k}(\boldsymbol{x})/\mathfrak{e}_n(\boldsymbol{x})$.

Proof.

$$\mathfrak{e}_{n-k}(\boldsymbol{x})=\sum_{i_1<\cdots<i_k}\frac{x_1\cdots x_n}{x_{i_1}\cdots x_{i_k}}=\mathfrak{e}_k\left(\boldsymbol{x}^{-1}\right)\mathfrak{e}_n(\boldsymbol{x}). \tag{3.12}$$

□

Thus,

$$\begin{aligned}\mathfrak{e}_{nm-1}(\boldsymbol{x}\otimes\boldsymbol{z}) &= \mathfrak{e}_1\left(\boldsymbol{x}^{-1}\otimes\boldsymbol{z}^{-1}\right)\mathfrak{e}_{mn}(\boldsymbol{x}\otimes\boldsymbol{z})\\ &= \mathfrak{e}_1\left(\boldsymbol{x}^{-1}\right)\mathfrak{e}_1\left(\boldsymbol{z}^{-1}\right)\mathfrak{e}_n(\boldsymbol{x})^m\mathfrak{e}_m(\boldsymbol{z})^n\\ &= \mathfrak{e}_n(\boldsymbol{x})^{m-1}\mathfrak{e}_{n-1}(\boldsymbol{x})\mathfrak{e}_m(\boldsymbol{z})^{n-1}\mathfrak{e}_{m-1}(\boldsymbol{z}).\end{aligned} \tag{3.13}$$

In the next section, these factoring identities are used to analyze the concurrences of a potential catalyst state for a pure-state transformation $|\psi\rangle\overset{\mathfrak{S}'}{\mapsto}|\phi\rangle$.

3.3 Bounding the dimension of a catalyst

We are now ready to analyze possible catalysts of a given entanglement-assisted LOCC transformation. Given states $|\psi\rangle$ and $|\phi\rangle$ with Schmidt number n and $|\chi\rangle$ with Schmidt

number m satisfying $|\psi\rangle|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle|\chi\rangle$, we must have $C_k(|\psi\rangle|\chi\rangle) \geq C_k(|\phi\rangle|\chi\rangle)$ for each $2 \leq k \leq nm$ even if $C_k(|\psi\rangle) < C_k(|\phi\rangle)$. Nontrivial conditions may be obtained for the values of the concurrences of $|\chi\rangle$ when $C_k(|\psi\rangle) < C_k(|\phi\rangle)$ because only certain values will allow this 'reversal' of inequalities.

This reversal cannot happen for $k = 2$: $C_2(|\psi\rangle|\chi\rangle) \geq C_2(|\phi\rangle|\chi\rangle)$ implies $C_2(|\psi\rangle) \geq C_2(|\phi\rangle)$. By equation 3.9, $C_2(|\psi\rangle|\chi\rangle) \geq C_2(|\phi\rangle|\chi\rangle)$ if and only if

$$\mathfrak{e}_2(((\psi))) + \mathfrak{e}_2(((\chi))) - 2\mathfrak{e}_2(((\psi)))\mathfrak{e}_2(((\chi))) \geq \mathfrak{e}_2(((\phi))) + \mathfrak{e}_2(((\chi))) - 2\mathfrak{e}_2(((\phi)))\mathfrak{e}_2(((\chi))), \quad (3.14)$$

which implies $\mathfrak{e}_2(((\psi))) \geq \mathfrak{e}_2(((\phi)))$ and thus $C_2(|\psi\rangle) \geq C_2(|\phi\rangle)$. The I-concurrence is then a catalytic monotone. So is the G-concurrence: $C_{nm}(|\psi\rangle|\chi\rangle) \geq C_{nm}(|\phi\rangle|\chi\rangle)$ if and only if $C_n(|\psi\rangle) \geq C_n(|\phi\rangle)$.

The simplest condition on the entanglement of a potential catalyst state arises from consideration of $k = mn - 1$. This condition is a lower bound on the Schmidt number m of a potential catalyst state. The bound is non-trivial for the transformation $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$ only if $C_{n-1}(|\psi\rangle) < C_{n-1}(|\phi\rangle)$, where n is the Schmidt number of $|\psi\rangle$.

Proposition 3.4. *Suppose there is a state vector $|\chi\rangle$ such that $|\psi\rangle|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle|\chi\rangle$, where $|\psi\rangle$ and $|\phi\rangle$ both have Schmidt number n and $C_n(|\psi\rangle) > C_n(|\phi\rangle)$. If the Schmidt number of $|\chi\rangle$ is m, then*

$$m \geq 1 + \left(\frac{n-1}{n}\right) \frac{\log[C_{n-1}(|\phi\rangle)] - \log[C_{n-1}(|\psi\rangle)]}{\log[C_n(|\psi\rangle)] - \log[C_n(|\phi\rangle)]}. \quad (3.15)$$

Proof. If $|\psi\rangle|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle|\chi\rangle$, we must have that $C_{nm-1}(|\psi\rangle|\chi\rangle) \geq C_{nm-1}(|\psi\rangle|\chi\rangle)$. This is true if and only if $\mathfrak{e}_{nm-1}(((\psi)) \otimes ((\chi))) \geq \mathfrak{e}_{nm-1}(((\phi)) \otimes ((\chi)))$. According to equation 3.13, this implies

$$\mathfrak{e}_n(((\psi)))^{m-1}\mathfrak{e}_{n-1}(((\psi))) \geq \mathfrak{e}_n(((\phi)))^{m-1}\mathfrak{e}_{n-1}(((\phi))) \quad (3.16)$$

after cancelling the terms $\mathfrak{e}_m(((\chi)))$ and $\mathfrak{e}_{m-1}(((\chi)))$. Thus,

$$m-1 \geq \frac{\log\left(\mathfrak{e}_{n-1}(((\phi)))\right) - \log\left(\mathfrak{e}_{n-1}(((\psi)))\right)}{\log\left(\mathfrak{e}_n(((\psi)))\right) - \log\left(\mathfrak{e}_n(((\phi)))\right)} = \left(\frac{n-1}{n}\right) \frac{\log[C_{n-1}(|\phi\rangle)] - \log[C_{n-1}(|\psi\rangle)]}{\log[C_n(|\psi\rangle)] - \log[C_n(|\phi\rangle)]}. \tag{3.17}$$

□

Notice that, if $C_n(|\psi\rangle) = C_n(|\phi\rangle)$, $C_{n-1}(|\psi\rangle) \geq C_{n-1}(|\phi\rangle)$ by equation 3.16. Proposition 3.4 makes no claim about the existence of a catalyst state. To ascertain the existence of a catalyst, we must make use of Turgut's theorem. An example of the use of this bound is presented in the next example.

Example 3.1. Consider state vectors $|\psi\rangle$ and $|\phi\rangle$ with Schmidt vectors

$$(\!(\psi)\!) = \left(\frac{89}{351}, \frac{3}{13}, \frac{71}{351}, \frac{64}{351}, \frac{1}{13}, \frac{19}{351}\right) \text{ and } (\!(\phi)\!) = \left(\frac{59}{196}, \frac{3}{14}, \frac{5}{28}, \frac{13}{98}, \frac{25}{196}, \frac{9}{196}\right).$$

$|\psi\rangle \overset{\mathfrak{L}}{\not\mapsto} |\phi\rangle$ because $C_5(|\psi\rangle) = 0.8981 < 0.8994 = C_5(|\phi\rangle)$. $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$, however (see figure 3.1). According to Proposition 3.4, the Schmidt number of a catalyst must be greater than or equal to 2.7077, so no catalyst of Schmidt number 2 exists.

Proposition 3.4 is not the only condition on possible catalysts. Further conditions may be obtained by considering the behaviour of other concurrences. For example, $k = 3$ yields the following condition.

Proposition 3.5. *Suppose* $|\psi\rangle|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle|\chi\rangle$. *Then*

$$\frac{\mathfrak{e}_2(((\chi))) - 2\mathfrak{e}_3(((\chi)))}{1 - 2\mathfrak{e}_2(((\chi))) + 3\mathfrak{e}_3(((\chi)))} \geq -\frac{\mathfrak{e}_3(((\psi))) - \mathfrak{e}_3(((\phi)))}{\mathfrak{e}_2(((\psi))) - \mathfrak{e}_2(((\phi)))}. \tag{3.18}$$

The proof of this proposition is analogous to that of Proposition 3.4. The result constitutes a complicated condition on the possible entanglement of $|\chi\rangle$ as quantified by the second and third concurrences. In example 3.1, Proposition 3.5 demands that $2\mathfrak{e}_2(((\chi))) < 1 + 3\mathfrak{e}_3(((\chi)))$ and $1 + 0.904\mathfrak{e}_2(((\chi))) \geq 2.809\mathfrak{e}_3(((\chi)))$.

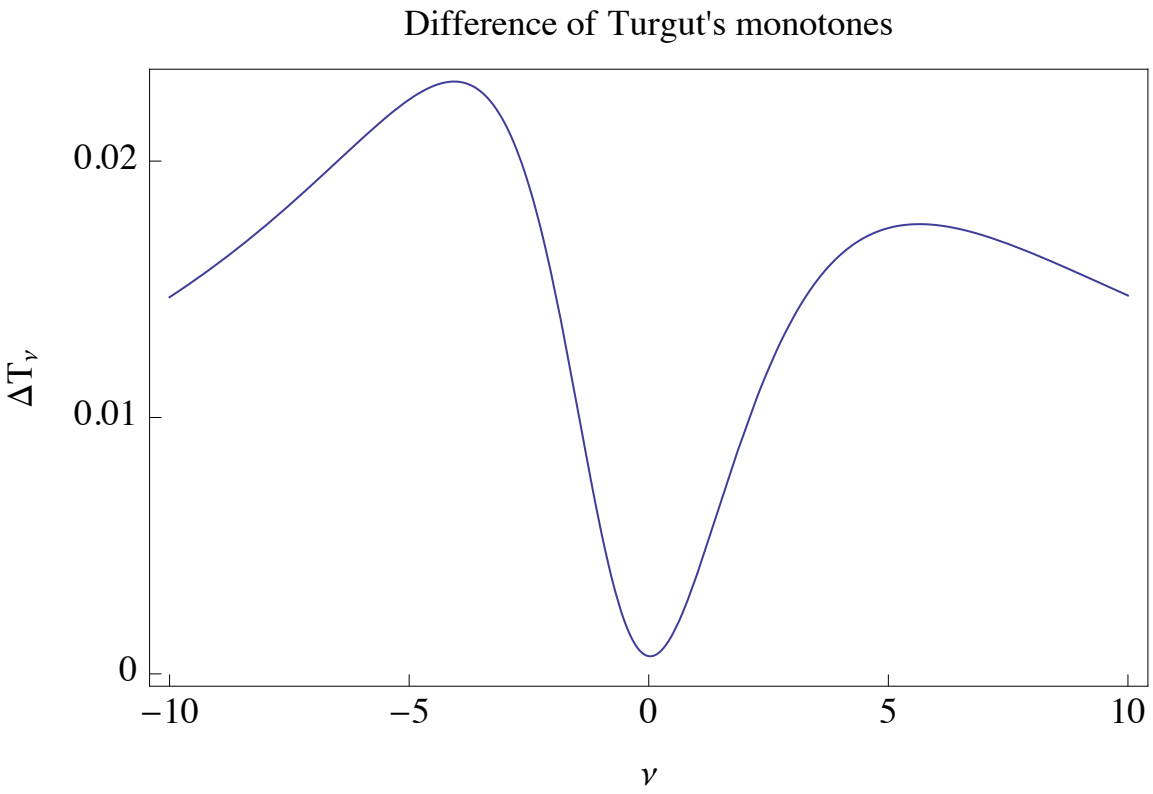


Figure 3.1: A plot of $\Delta T_\nu = T_\nu(|\psi\rangle) - T_\nu(|\phi\rangle)$, where T_ν represents Turgut's monotone of order $\nu \in \mathbb{R}$, and $|\psi\rangle$ and $|\phi\rangle$ are defined in Example 3.1.

Consideration of other concurrences yield even more complicated conditions. The following proposition follows from the monotonicity of the $(mn-2)^{th}$ concurrence.

Proposition 3.6. *Suppose* $|\psi\rangle|\chi\rangle \overset{\mathfrak{L}}{\mapsto} |\phi\rangle|\chi\rangle$. *If the Schmidt number of* $|\psi\rangle$ *is equal to the Schmidt number of* $|\phi\rangle$ *(which is called* n*) and the Schmidt number of* $|\chi\rangle$ *is* m*,*

$$\frac{\mathfrak{e}_{m-1}(((\chi)))^2}{\mathfrak{e}_m(((\chi)))\mathfrak{e}_{m-2}(((\chi)))} \geq \frac{\Lambda}{\mathfrak{e}_{n-2}(((\psi)))\mathfrak{e}_n(((\psi)))^{m-1} - \mathfrak{e}_{n-2}(((\phi)))\mathfrak{e}_n(((\phi)))^{m-1}}, \tag{3.19}$$

where

$$\begin{aligned} \Lambda &= 2\mathfrak{e}_{n-2}(((\psi)))\mathfrak{e}_n(((\psi)))^{m-1} - \mathfrak{e}_{n-1}(((\psi)))^2\mathfrak{e}_n(((\psi)))^{m-2} \\ &\quad -2\mathfrak{e}_{n-2}(((\phi)))\mathfrak{e}_n(((\phi)))^{m-1} - \mathfrak{e}_{n-1}(((\phi)))^2\mathfrak{e}_n(((\phi)))^{m-2}. \end{aligned} \tag{3.20}$$

Notice that the condition of equation 3.19 depends explicitly on m, the Schmidt number of the catalyst state. This limits the usefulness of this condition. Other necessary conditions on a potential catalyst state may be derived through consideration of other concurrences, but these conditions are even more difficult to apply in practice.

In conclusion, we have produced a lower bound on the Schmidt number of a catalyst state allowing some given entanglement-assisted LOCC transformation of pure states $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$. This lower bound is expressed in terms of the concurrences of $|\psi\rangle$ and $|\phi\rangle$. The techniques used to produce this lower bound may be extended to produce other necessary conditions on entanglement catalysts, though the conditions become increasingly complicated.

Chapter 4

Relative monotones

When a quantum state can be used to alleviate restrictions on achievable operations, that state is called a resource. The resourcefulness of a quantum state is often quantified with functions known as monotones. Entanglement monotones, for example, quantify the ability of a state to alleviate LOCC restrictions [16]. Such characterizations are useful for the comparison of different resource states that may be used to accomplish a given quantum informational task [30].

The approach of quantifying resourcefulness with monotones is sometimes difficult. The U(1)-frameness of a pure state, for example, has not been fully characterized with a collection of monotones despite the discovery of a necessary and sufficient condition for the existence of a U(1)-invariant pure-state transformation [18]. In contrast, other characterizations of resourcefulness [11, 17] may be interpreted in terms of a collection of monotones.

I introduce a new approach to the characterization of the resourcefulness of a quantum state. Rather than quantifying resourcefulness in an absolute sense, I characterize the Z_n-frameness of a pure state relative to other states. A single relative measure of resourcefulness suffices to characterize Z_n-invariant pure-state transformations. I call such measures 'relative monotones'.

There is precedent for updating the notion of a monotone. The original entanglement monotone was required to satisfy a convexity property [16] that was later deemed unnecessarily restrictive [15]. Monotones with such a convexity property ('ensemble monotones') sometimes characterize resourcefulness with unnecessary prolixity [31]. Conversely, 'absolute monotones' may provide more succinct characterizations of resourcefulness. Unfor-

tunately, expressing results such as Turgut's theorem [17] in terms of absolute monotones can still be unacceptably prolix. Such results may be concisely expressed with a single relative monotone.

Section 4.1 introduces relative monotones and compares the characterization of resourcefulness with relative monotones to that provided by ensemble and absolute monotones. In section 4.2, I present my results on characterizing the Z_n-frameness of a pure state in terms of relative monotones. I argue that a characterization with relative monotones is preferable to a characterization with absolute monotones in Z_3-frameness because a single relative monotone suffices to determine the existence of a Z_3-invariant pure-state transformation. This is in marked contrast to any characterization in terms of absolute monotones, because such a characterization will require many absolute monotones. Analogous results hold when considering the more important example of U(1)-frameness of finite-dimensional quantum states, though the paradigm of relative monotones is of less use in this case. I discuss these results in section 4.3.

4.1 Relative monotones versus absolute monotones

I used absolute monotones to characterize the ability to transform states under restrictions on achievable operations. Indeed, absolute monotones are defined by this property: a monotone is non-increasing under the action of achievable operations because such operations cannot increase the resourcefulness of a state in alleviating these restrictions. I then characterized the ability to perform state transformations under such restrictions by producing some collection of monotones $\{f_\alpha\}$ (where α is an index) with the property that $f_\alpha(\rho) \geq f_\alpha(\sigma)$ for each α if and only if ρ can be transformed to σ with an achievable quantum channel.

This approach is originally due to Vidal [16]. Vidal's paper defines an entanglement

monotone as "any magnitude $\mu(\rho)$ that does not increase, on average, under local transformations". Vidal captures the notion of non-increasing "on average" by demanding that, for any collection of LOCC measurements on ρ that produce outcome σ_i with probability p_i, $\mu(\rho) \geq \sum_i p_i \mu(\sigma_i)$. Furthermore, Vidal requires that $\sum_j q_j \mu(\rho_j)$ for any collection of states ρ_j such that $\sum_j q_j \rho_j = \rho$ for a probability vector $\boldsymbol{q}$. These conditions were later deemed too restrictive by Plenio [15].

Plenio's argument for removing the requirement that monotones not increase on average under LOCC measurements is as follows: the measurements on ρ yielding σ_i with probability p_i may be interpreted as LOCC processing of ρ to obtain the state $\sum_i p_i \sigma_i \otimes |i\rangle\langle i|$, where $|i\rangle\langle i|$ is an orthonormal collection of states on an ancillary Hilbert space and then performing the collection of measurements $\{|i\rangle\langle i|\}$ on that ancillary space. Physically, this may be interpreted as correlating the outcome of certain measurements indexed by i to the state of an environment represented by the ancillary Hilbert space. Measurements are then performed on the environment.

If an entanglement monotone f cannot increase under LOCC processing, f must satisfy $f(\rho) \geq f\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|\right)$ because this only requires a reasonable extension of f to the larger Hilbert space obtained by including the measurement Hilbert space. Vidal's condition that $f(\rho) \geq \sum_i p_i f(\sigma_i)$ may then be viewed as a convexity requirement on f; that is,

$$f\left(\sum_i p_i \sigma_i \otimes |i\rangle\langle i|\right) \geq \sum_i p_i f(\sigma_i). \tag{4.1}$$

Plenio then produces a function (the 'logarithmic negativity') that is an LOCC monotone in our sense and yet do not satisfy such a convexity requirement. I distinguish Vidal's notion of a monotone from Plenio's notion by referring to the former as an 'ensemble monotone' and the latter as an 'absolute monotone'.

Any resource theory may be characterized by a collection of ensemble monotones. Define $P_\sigma(\rho)$ to be the maximum probability of obtaining the state σ from the state ρ

under a collection $\mathfrak{T}$ of allowable operations. $\{P_\sigma|\sigma \text{ a state}\}$ is a collection of ensemble monotones that completely characterizes all possible transformations under $\mathfrak{T}$.

Lemma 4.1. *$\rho \overset{\mathfrak{T}}{\mapsto} \rho'$ if and only if $P_\sigma(\rho) \geq P_\sigma(\rho')$ for every state σ.*

Proof. $P_\sigma(\rho)$ is an ensemble $\mathfrak{T}$-monotone for every state σ because, if $\rho \overset{\mathfrak{T}}{\mapsto} \{p_i, \gamma_i\}$, the maximum probability of obtaining σ from ρ with $\mathfrak{T}$ operations is at least that of obtaining σ from the ensemble $\{p_i, \gamma_i\}$ (given by $\sum_i p_i P_\sigma(\gamma_i)$). Thus $P_\sigma(\rho) \geq \sum_i p_i P_\sigma(\gamma_i)$, which implies in particular that $P_\sigma(\rho) \geq P_\sigma(\rho')$ if $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$. Furthermore, if $P_\sigma(\rho) \geq P_\sigma(\rho')$ for every state σ, $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$ because $P_{\rho'}(\rho) \geq P_{\rho'}(\rho') = 1$, which implies $P_{\rho'}(\rho) = 1$. □

The difficulty with ensemble monotones is not their capability of characterizing state transformations but rather the prolixity of such a description. Gour demonstrates that a characterization of even a simple collection of LOCC state transformations cannot be accomplished with finitely many ensemble entanglement monotones [31].

There are resource theories whose characterizations seem even to require an infinite collection of absolute monotones. Turgut's theorem, for example, provides an infinite collection of monotones that characterize pure state transformations allowable with entanglement-assisted LOCC channels. This is again too prolix: a quantum state over a finite-dimensional Hilbert space can be specified with finitely many real numbers, so a comparison between two such states should also require finitely many real numbers. Such characterizations are possible with relative monotones.

Definition 4.1. Let $\mathfrak{T}$ be a collection of quantum channels $\{\mathcal{E} : \mathscr{B}(\mathscr{H}_1) \to \mathscr{B}(\mathscr{H}_2)\}$ and let $C_1 \subset \mathscr{B}(\mathscr{H}_1)$ and $C_2 \subset \mathscr{B}(\mathscr{H}_2)$ be two collections of states. A *relative $\mathfrak{T}$-monotone* is a function $f : C_1 \times C_2 \to \mathbb{R}$ with the property that $f(\rho, \sigma) \geq 0$ whenever $\rho \overset{\mathfrak{T}}{\mapsto} \sigma$.

It is possible to characterize every resource theory with a single relative monotone. Suppose $\mathfrak{T}$ is the collection of allowable operations and $P_\sigma(\rho)$ is the ensemble monotone

defined above. Define $\mathcal{R}(\rho,\rho') = \inf_\sigma [P_\sigma(\rho) - P_\sigma(\rho')]$. Then $\mathcal{R}(\rho,\rho') \geq 0$ if and only if $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$. Of course, $\mathcal{R}(\rho,\rho') \leq P_{\rho'}(\rho) - P_{\rho'}(\rho') \leq 0$, so $\mathcal{R}(\rho,\rho') = 0$ when $\rho \overset{\mathfrak{T}}{\mapsto} \rho'$. Note that $\mathcal{R}$ cannot be expressed as the difference of absolute monotones, because $\mathcal{R}(\rho,\rho') + \mathcal{R}(\rho',\rho) \neq 0$ in general.

A more informative relative monotone is given as follows. Let D represent the Bures metric [32] on a space of density matrices. The precise definition of D is not important for our purposes; I require only the fact that D is a metric. For a given ρ and σ, the maximum rate of distillation R of σ from ρ under a collection $\mathfrak{T}$ of allowable operations is given by [33]:

$$R = \inf\left\{E \,\middle|\, \forall\delta,\epsilon > 0,\ \exists\mathcal{E}\in\mathfrak{T},\ m,n\in\mathbb{N} \text{ s.t. } \left|E - \frac{m}{n}\right| < \delta \text{ and } D\left(\mathcal{E}\left(\rho^{\otimes m}\right), \sigma^{\otimes n}\right) < \epsilon\right\}. \tag{4.2}$$

Then, if $\rho \overset{\mathfrak{T}}{\mapsto} \sigma$, $\mathcal{R}(\rho,\sigma) := \log(R) \geq 0$. This relative monotone $\mathcal{R}$ gives the logarithm of the average distillation rate of σ from ρ given many copies of ρ. Of course, there is no explicit algorithm for calculating $\mathcal{R}(\rho,\sigma)$ in this case.

In specific resource theories, there exist relative monotones that can be calculated more explicitly. If Turgut's monotones are labelled by $T_\nu(|\psi\rangle) = \frac{1}{\nu}S_\nu((\!(\psi)\!))$, where $\nu \in \mathbb{R}$ (see equation 3.2), we may define

$$\mathcal{R}(|\psi\rangle, |\phi\rangle) = \inf_{\nu\in\mathbb{R}} [T_\nu(|\psi\rangle) - T_\nu(|\phi\rangle)] \tag{4.3}$$

so that $|\psi\rangle \overset{\mathfrak{L}'}{\mapsto} |\phi\rangle$ if and only if $\mathcal{R}(|\psi\rangle, |\phi\rangle) \geq 0$. This infimum, of course, is rather difficult to compute.

The examples of relative monotones I have given in this section are rather artificial. In the next section, I present a relative monotone $\mathcal{R}_n$ with a simple formula that characterizes the resource theory of Z_n-frameness. Similar techniques may be applied to U(1)-frameness also, though it is less profitable to interpret the resulting conditions as a relative monotone. These techniques are discussed in section 4.3.

4.2 Relative Z_n-frameness

In this section, I characterize the Z_n-frameness of a pure state. This characterization is first provided by demanding the existence of a vector $\boldsymbol{w}$ with certain properties. Thus $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$ if and only if $\boldsymbol{w}$ exists. This result is analogous to a characterization of the U(1)-frameness of a pure state [18]. I then present a relative monotone $\mathcal{R}_n$ such that $\mathcal{R}_n(|\psi\rangle, |\phi\rangle) \geq 0$ if and only if $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$. I will discuss this result for $n = 3$ in particular, as it is unlikely to have a concise characterization in terms of absolute frameness monotones.

We consider a representation of Z_n on any Hilbert space $\mathscr{H}$. The image of this representation is denoted $\left\{I, R, R^2, \ldots, R^{n-1} = R^\dagger\right\}$ for some unitary operator R. Since R is normal, it is diagonalizable and has eigenvalues $\exp\left(\iota\frac{2k\pi}{n}\right)$, $k = 0, 1, \ldots, n-1$. Define $\mathscr{H}_k^{(n)}$ to be the eigenspace of eigenvalue $\exp\left(\iota\frac{2k\pi}{n}\right)$. If we define $U = U_0 \oplus U_1 \oplus \cdots \oplus U_{n-1}$ for some collection of unitary operators $\left\{U_k : \mathscr{H}_k^{(n)} \to \mathscr{H}_k^{(n)} | k = 0, 1, \ldots, n-1\right\}$, we have $RU = UR$. Thus $|\psi\rangle \overset{Z_n}{\sim} U|\psi\rangle$. Define the projection operator $\Pi_k^{(n)} : \mathscr{H} \to \mathscr{H}_k^{(n)}$ for each $k = 0, 1, \ldots, n-1$ and $p_k^{(n)}(|\psi\rangle) = \langle\psi| \Pi_k^{(n)} |\psi\rangle \geq 0$. Note that $p_k^{(n)}(|\psi\rangle) = p_k^{(n)}(U|\psi\rangle)$.

In the case that $n = 2$, the function $\mathcal{C}(|\psi\rangle) = \min\left\{p_0^{(2)}(|\psi\rangle), p_1^{(2)}(|\psi\rangle)\right\}$ is a frameness monotone. In fact, $|\psi\rangle \overset{Z_2}{\mapsto} |\phi\rangle$ if and only if $\mathcal{C}(|\psi\rangle) \geq \mathcal{C}(|\phi\rangle)$ [18]. An analogous result does not hold for $n > 2$, however. Both of these facts will be seen as consequences of what follows.

Define $\left|\psi_k^{(n)}\right\rangle = \frac{1}{\sqrt{p_k^{(n)}(|\psi\rangle)}} \Pi_k^{(n)} |\psi\rangle$ for each $k = 0, 1, \ldots, n-1$, provided $p_k^{(n)}(|\psi\rangle) \neq 0$. If $p_k^{(n)}(|\psi\rangle) = 0$ for some value of k we will be able to choose any $\left|\psi_k^{(n)}\right\rangle \in \mathscr{H}_k^{(n)}$ in what follows, provided $\dim\left(\mathscr{H}_k^{(n)}\right) \neq 0$. We will assume $\dim\left(\mathscr{H}_k^{(n)}\right) > 0$ for each k; there is no loss of generality because a representation of Z_n that is 'missing' an eigenspace $\mathscr{H}_k^{(n)}$ can be extended to one with such an eigenspace and restrict attention to the pure states

$|\psi\rangle$ satisfying $p_k^{(n)}(|\psi\rangle) = 0$. We can therefore write:

$$|\psi\rangle = \sum_{k=0}^{n-1} \sqrt{p_k^{(n)}(|\psi\rangle)} \left|\psi_k^{(n)}\right\rangle . \tag{4.4}$$

Define a collection of states $\left\{|k\rangle \in \mathscr{H}_k^{(n)} | k = 0, 1, \ldots, n-1\right\}$ and, for any state $|\psi\rangle \in \mathscr{H}$, unitary operators $U_k(|\psi\rangle) : \mathscr{H}_k^{(n)} \to \mathscr{H}_k^{(n)}$ such that $U_k\left(\left|\psi_k^{(n)}\right\rangle\right) = |k\rangle$. Define $U(|\psi\rangle) = U_0(|\psi\rangle) \oplus U_1(|\psi\rangle) \oplus \cdots \oplus U_{n-1}(|\psi\rangle)$. Then

$$\left|\overline{\psi}\right\rangle := U(|\psi\rangle)\,|\psi\rangle = \sum_{k=0}^{n-1} \sqrt{p_k^{(n)}(|\psi\rangle)}\,|k\rangle \overset{Z_n}{\sim} |\psi\rangle . \tag{4.5}$$

Thus $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$ if and only if $\left|\overline{\psi}\right\rangle \overset{Z_n}{\mapsto} \left|\overline{\phi}\right\rangle$.

Thus the Z_n-frameness of a state $|\psi\rangle$ depends only on the vector

$$\boldsymbol{p}(|\psi\rangle) := \left(p_0^{(n)}(|\psi\rangle), p_1^{(n)}(|\psi\rangle), \ldots, p_{n-1}^{(n)}(|\psi\rangle)\right), \tag{4.6}$$

in much the same way that the entanglement of a pure state depends only on its Schmidt vector. An important difference is that the ordering of the Schmidt coefficients is irrelevant to the entanglement of the state. In contrast, if there is a permutation σ such that $\boldsymbol{p}(|\phi\rangle) = \left(p_{\sigma(0)}^{(n)}(|\psi\rangle), p_{\sigma(1)}^{(n)}(|\psi\rangle), \ldots, p_{\sigma(n-1)}^{(n)}(|\psi\rangle)\right)$ for some pure state $|\phi\rangle$, it is possible that $|\phi\rangle \overset{Z_n}{\nsim} |\psi\rangle$.

Theorem 4.2. *$|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$ if and only if there exists a vector $\boldsymbol{w} = (w_0, w_1, \ldots, w_{n-1})$ such that $w_k \geq 0$ for each k, $\sum_k w_k = 1$, and*

$$p_\ell^{(n)}(|\psi\rangle) = \sum_{k=0}^{n-1} w_k p_{\ell-k}^{(n)}(|\phi\rangle) \tag{4.7}$$

for each $\ell = 0, 1, \ldots, n-1$, where the subscript addition $\ell - k$ is performed modulo n.

Proof. Without loss of generality, we will assume $|\psi\rangle = \left|\overline{\psi}\right\rangle$ and $|\phi\rangle = \left|\overline{\phi}\right\rangle$, which is to say $|\psi\rangle = \sum_k \sqrt{p_k^{(n)}(|\psi\rangle)}\,|k\rangle$ and $|\phi\rangle = \sum_k \sqrt{p_k^{(n)}(|\phi\rangle)}\,|k\rangle$ for some fixed collection of unit vectors $\left\{|k\rangle \in \mathscr{H}_k^{(n)} | k = 0, 1, \ldots, n-1\right\}$.

Suppose $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$. By Theorem 2.4, any trace-preserving Z_n-invariant quantum channel $\mathcal{E}$ satisfying $\mathcal{E}(|\psi\rangle\langle\psi|) = |\phi\rangle\langle\phi|$ has a Kraus representation of the form $\{E_{k,\alpha}\}$, where $k = 0, 1, \ldots, n-1$ and α is some multiplicity index depending on k, satisfying

$$E_{k,\alpha} = \sum_{\ell=0}^{n-1} \sqrt{c_\ell^{(k,\alpha)}}\, |\ell + k\rangle\langle\ell|\,, \tag{4.8}$$

where $c_\ell^{(k,\alpha)}$ is a collection of positive real numbers and the addition $\ell + k$ is performed modulo n. Because $\mathcal{E}$ is trace-preserving, $\sum_{k,\alpha} E_{k,\alpha}^\dagger E_{k,\alpha} = I$, so $\sum_{k,\alpha} c_\ell^{(k,\alpha)} = 1$ for each $\ell = 0, 1, \ldots, n-1$. Furthermore,

$$E_{k,\alpha}\,|\psi\rangle = \sum_{\ell=0}^{n-1} \sqrt{c_\ell^{(k,\alpha)}} \sqrt{p_\ell^{(n)}(|\psi\rangle)}\,|\ell + k\rangle = \sqrt{w_{k,\alpha}} \sum_{\ell=0}^{n-1} \sqrt{p_\ell^{(n)}(|\phi\rangle)}\,|\ell\rangle \tag{4.9}$$

for some positive real number $w_{k,\alpha}$ (recall that the rank of $\mathcal{E}(|\psi\rangle\langle\psi|)$ would be greater than one if this were not true). We have $\sum_{k,\alpha} w_{k,\alpha} = 1$ because $\mathcal{E}$ is trace-preserving. Define $w_k = \sum_\alpha w_{k,\alpha}$. We may then calculate

$$p_\ell^{(n)}(|\psi\rangle) = \sum_{k,\alpha} c_\ell^{(k,\alpha)} p_\ell^{(n)}(|\psi\rangle) = \sum_{k=0}^{n-1} w_k p_{\ell-k}^{(n)}(|\phi\rangle), \tag{4.10}$$

where $\boldsymbol{w} := (w_0, w_1, \ldots, w_{n-1})$ is a probability vector.

If we have such a vector $\boldsymbol{w}$, there exists a Z_n invariant channel $\mathcal{E}$ such that $\mathcal{E}(|\psi\rangle\langle\psi|) = |\phi\rangle\langle\phi|$. Define the Kraus operators

$$E_k = \sum_{\ell=0}^{n-1} \sqrt{c_\ell^{(k)}}\,|\ell + k\rangle\langle\ell| \tag{4.11}$$

for each $k = 0, 1, \ldots, n-1$, where

$$c_\ell^{(k)} = \begin{cases} w_k p_{\ell-k}^{(n)}(|\phi\rangle)/p_\ell^{(n)}(|\psi\rangle) & \text{if } p_\ell^{(n)}(|\psi\rangle) \neq 0 \\ 1/n & \text{if } p_\ell^{(n)}(|\psi\rangle) = 0 \end{cases} \tag{4.12}$$

Then define $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$. □

Consider the simple case of Z_2-frameness. $|\psi\rangle \overset{Z_2}{\mapsto} |\phi\rangle$ if and only if there exists a vector $\boldsymbol{w} = (w_0, w_1)$ consisting of positive real entries satisfying

$$\begin{aligned} p_0^{(2)}(|\psi\rangle) &= w_0 p_0^{(2)}(|\phi\rangle) + w_1 p_1^{(2)}(|\phi\rangle) \\ p_1^{(2)}(|\psi\rangle) &= w_1 p_0^{(2)}(|\phi\rangle) + w_0 p_1^{(2)}(|\phi\rangle) \end{aligned} \tag{4.13}$$

Notice that $|\phi'\rangle := \sqrt{p_1^{(2)}(|\phi\rangle)}\,|0\rangle + \sqrt{p_0^{(2)}(|\phi\rangle)}\,|1\rangle \overset{Z_2}{\approx} |\phi\rangle$. Thus we may assume $p_0^{(2)}(|\phi\rangle) \geq p_1^{(2)}(|\phi\rangle)$ (and $p_0^{(2)}(|\psi\rangle) \geq p_1^{(2)}(|\psi\rangle)$) without loss of generality. Furthermore, if $p_0^{(2)}(|\phi\rangle) = p_1^{(2)}(|\phi\rangle) = 1/2$, $|\psi\rangle \overset{Z_2}{\mapsto} |\phi\rangle$ if and only if $p_0^{(2)}(|\psi\rangle) = p_1^{(2)}(|\psi\rangle) = 1/2$. We then assume $p_0^{(2)}(|\phi\rangle) > p_1^{(2)}(|\phi\rangle)$. In this case, equation 4.13 has a unique solution

$$w_0 = \frac{p_0^{(2)}(|\psi\rangle)p_0^{(2)}(|\phi\rangle) - p_1^{(2)}(|\psi\rangle)p_1^{(2)}(|\phi\rangle)}{p_0^{(2)}(|\phi\rangle) - p_1^{(2)}(|\phi\rangle)},\ w_1 = \frac{p_1^{(2)}(|\psi\rangle)p_0^{(2)}(|\phi\rangle) - p_0^{(2)}(|\psi\rangle)p_1^{(2)}(|\phi\rangle)}{p_0^{(2)}(|\phi\rangle) - p_1^{(2)}(|\phi\rangle)}. \tag{4.14}$$

By Theorem 4.2, $|\psi\rangle \overset{Z_2}{\mapsto} |\phi\rangle$ if and only if $w_0 \geq 0$ and $w_1 \geq 0$, or

$$p_0^{(2)}(|\psi\rangle)p_0^{(2)}(|\phi\rangle) \geq p_1^{(2)}(|\psi\rangle)p_1^{(2)}(|\phi\rangle) \text{ and } p_1^{(2)}(|\psi\rangle)p_0^{(2)}(|\phi\rangle) \geq p_0^{(2)}(|\psi\rangle)p_1^{(2)}(|\phi\rangle), \tag{4.15}$$

which is true if and only if $p_1^{(2)}(|\psi\rangle) \geq p_1^{(2)}(|\phi\rangle)$. We have thus reproduced the Z_2-frameness monotone of Gour and Spekkens [18] and shown that it fully characterizes the Z_2-frameness of a pure state.

A single absolute monotone cannot fully characterize the Z_3-frameness of a pure state because there exist states $|\psi\rangle$ and $|\phi\rangle$ such that $|\psi\rangle \overset{Z_3}{\not\mapsto} |\phi\rangle$ and $|\phi\rangle \overset{Z_3}{\not\mapsto} |\psi\rangle$, though this does not prevent a single relative monotone from characterizing the relative Z_3-frameness of a pure state. $|\psi\rangle \overset{Z_3}{\mapsto} |\phi\rangle$ if and only if there exists a vector (w_0, w_1, w_2) of positive real numbers with the property that

$$\begin{pmatrix} p_0^{(3)}(|\psi\rangle) \\ p_1^{(3)}(|\psi\rangle) \\ p_2^{(3)}(|\psi\rangle) \end{pmatrix} = \begin{pmatrix} p_0^{(3)}(|\phi\rangle) & p_2^{(3)}(|\phi\rangle) & p_1^{(3)}(|\phi\rangle) \\ p_1^{(3)}(|\phi\rangle) & p_0^{(3)}(|\phi\rangle) & p_2^{(3)}(|\phi\rangle) \\ p_2^{(3)}(|\phi\rangle) & p_1^{(3)}(|\phi\rangle) & p_0^{(3)}(|\phi\rangle) \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ w_2 \end{pmatrix} \tag{4.16}$$

and $w_0 + w_1 + w_2 = 1$. Equation 4.16 could also be written in the form $\boldsymbol{p}(|\psi\rangle) = \boldsymbol{P}(|\phi\rangle) \cdot \boldsymbol{w}$, where $\boldsymbol{P}(|\phi\rangle)$ is the 3×3 matrix. This collection of linear equations has a unique solution whenever $\det(\boldsymbol{P}(|\phi\rangle)) \neq 0$. By the arithmetic-geometric mean inequality, $\frac{1}{3}\left(\left[p_0^{(3)}(|\phi\rangle)\right]^3 + \left[p_1^{(3)}(|\phi\rangle)\right]^3 + \left[p_2^{(3)}(|\phi\rangle)\right]^3\right) \geq \sqrt[3]{\left[p_0^{(3)}(|\phi\rangle)\right]^3 \left[p_1^{(3)}(|\phi\rangle)\right]^3 \left[p_2^{(3)}(|\phi\rangle)\right]^3}$, so

$$\det(\boldsymbol{P}(|\phi\rangle)) = \left[p_0^{(3)}(|\phi\rangle)\right]^3 + \left[p_1^{(3)}(|\phi\rangle)\right]^3 + \left[p_2^{(3)}(|\phi\rangle)\right]^3 - 3p_0^{(3)}(|\phi\rangle)p_1^{(3)}(|\phi\rangle)p_2^{(3)}(|\phi\rangle) \geq 0 \tag{4.17}$$

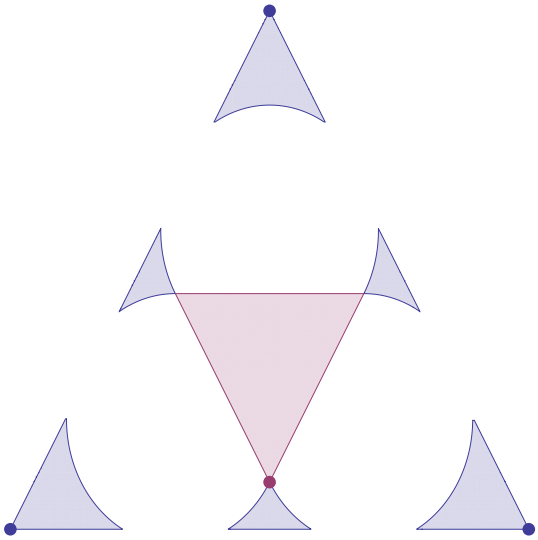
with equality if and only if $p_0^{(3)}(|\phi\rangle) = p_1^{(3)}(|\phi\rangle) = p_2^{(3)}(|\phi\rangle) = \frac{1}{3}$. If this is the case, $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$ if and only if $p_0^{(3)}(|\psi\rangle) = p_1^{(3)}(|\psi\rangle) = p_2^{(3)}(|\psi\rangle) = \frac{1}{3}$. Otherwise, equation 4.16 has a unique solution $\boldsymbol{w}$ given by

$$w_k = \frac{\sum_{\ell=0}^{2} p_{k+\ell}^{(3)}(|\psi\rangle)\left(\left[p_\ell^{(3)}(|\phi\rangle)\right]^2 - p_{\ell+1}^{(3)}(|\phi\rangle)p_{\ell+2}^{(3)}(|\phi\rangle)\right)}{\left[p_0^{(3)}(|\phi\rangle)\right]^3 + \left[p_1^{(3)}(|\phi\rangle)\right]^3 + \left[p_2^{(3)}(|\phi\rangle)\right]^3 - 3p_0^{(3)}(|\phi\rangle)p_1^{(3)}(|\phi\rangle)p_2^{(3)}(|\phi\rangle)} \tag{4.18}$$

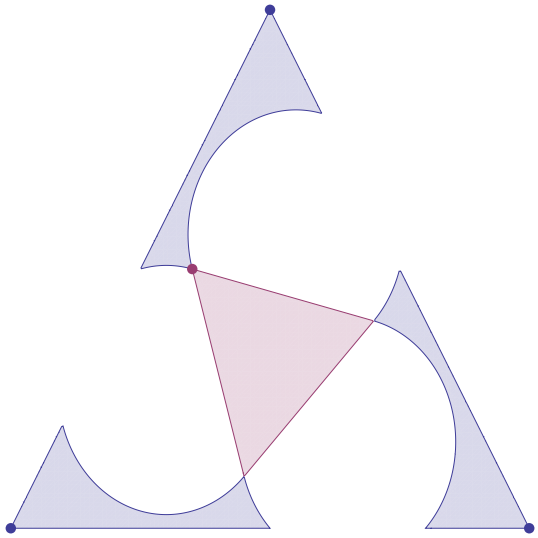
(for $k = 0, 1, 2$), where, again, the subscript additions are performed modulo 3. By Theorem 4.2, $|\psi\rangle \overset{Z_3}{\mapsto} |\phi\rangle$ if and only if $\min_k w_k \geq 0$.

Thus the relative Z_3-frameness of a pure state $|\psi\rangle$ with respect to $|\phi\rangle$ may be characterized with a single relative frameness monotone. Define $\mathcal{R}_3(|\psi\rangle, |\phi\rangle) = \min_k w_k$ when $\boldsymbol{p}(|\phi\rangle) \neq \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$, $\mathcal{R}_3(|\psi\rangle, |\phi\rangle) = 0$ when $\boldsymbol{p}(|\psi\rangle) = \boldsymbol{p}(|\phi\rangle) = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$, and $\mathcal{R}_3(|\psi\rangle, |\phi\rangle) = -1$ otherwise. Then $\mathcal{R}_3(|\psi\rangle, |\phi\rangle) \geq 0$ if and only if $|\psi\rangle \overset{Z_3}{\mapsto} |\phi\rangle$. The ability to transform one state to another with Z_3-invariant operations is illustrated in figure 4.1. It is clear that a single absolute monotone cannot characterize Z_3-invariant transformations because there exist pairs of states $|\psi\rangle$ and $|\phi\rangle$ such that $|\psi\rangle \overset{Z_3}{\not\mapsto} |\phi\rangle$ and $|\phi\rangle \overset{Z_3}{\not\mapsto} |\psi\rangle$.

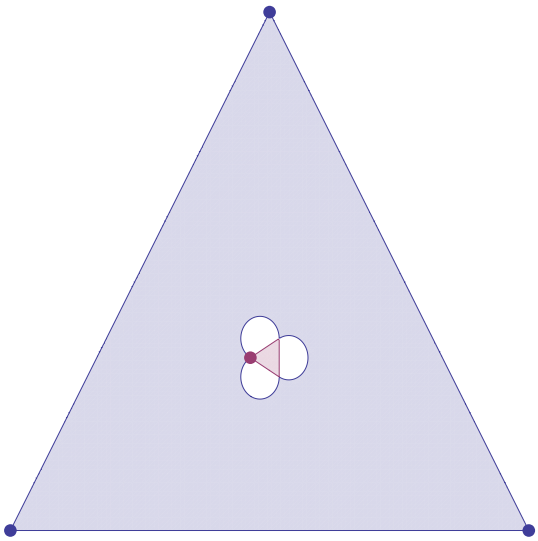
In general, equation 4.7 can be written in the form $\boldsymbol{p}(|\psi\rangle) = \boldsymbol{P}(|\phi\rangle) \cdot \boldsymbol{w}$, so a unique solution $\boldsymbol{w}$ exists whenever $\det(\boldsymbol{P}(|\phi\rangle)) \neq 0$. In the case that $\det(\boldsymbol{P}(|\phi\rangle)) = 0$, there may be no solutions or many. If there are no solutions, $|\psi\rangle \overset{Z_n}{\not\mapsto} |\phi\rangle$. If there are many solutions, we must check to see if there are any with all positive entries. Define



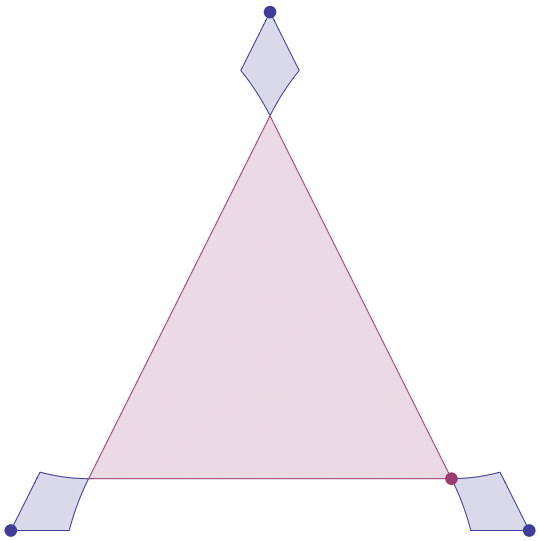
(a) $|\eta\rangle = \sqrt{1/11}\,|0\rangle + \sqrt{5/11}\,|1\rangle + \sqrt{5/11}\,|2\rangle$



(b) $|\eta\rangle = \sqrt{1/2}\,|0\rangle + \sqrt{2/5}\,|1\rangle + \sqrt{1/10}\,|2\rangle$



(c) $|\eta\rangle = \sqrt{1/3}\,|0\rangle + \sqrt{10/27}\,|1\rangle + \sqrt{8/27}\,|2\rangle$



(d) $|\eta\rangle = \sqrt{1/10}\,|0\rangle + \sqrt{1/10}\,|1\rangle + \sqrt{4/5}\,|2\rangle$

Figure 4.1: Depiction of states in the form $\sqrt{x}\,|0\rangle + \sqrt{y}\,|1\rangle + \sqrt{z}\,|2\rangle$ (where $0 \leq x, y, z \leq 1$ and $x + y + z = 1$) that can be mapped to or from a specified state $|\eta\rangle$. In each figure, the vertical axis represents $\sqrt{3}x$, and the horizontal axis is $z - y$. The red dot in each figure represents $|\eta\rangle$, whereas the blue dots represent the non-resource states $|0\rangle$, $|1\rangle$, and $|2\rangle$ that form the vertices of the region of all states. The interior red region represents the states that can be mapped to $|\eta\rangle$ with Z_3-invariant operations, whereas the exterior blue region represents states to which $|\eta\rangle$ can be transformed using Z_3-invariant operations.

$\mathcal{R}_n(|\psi\rangle, |\phi\rangle) = \min_k w_k$ when a unique solutions $\boldsymbol{w}$ exists, $\mathcal{R}_n(|\psi\rangle, |\phi\rangle) = \max_{\boldsymbol{w}} \min_k w_k$ when there are many solutions (where the maximum is taken over all possible solutions $\boldsymbol{w}$), and $\mathcal{R}_n(|\psi\rangle, |\phi\rangle) = -1$ when no solution $\boldsymbol{w}$ exists. Then $|\psi\rangle \overset{Z_n}{\mapsto} |\phi\rangle$ if and only if $\mathcal{R}_n(|\psi\rangle, |\phi\rangle) \geq 0$.

4.3 U(1)-frameness

In the previous section, I have presented necessary and sufficient conditions for the existence of a Z_n-invariant pure-state transformation. These conditions could be expressed in terms of the positivity of a single easily calculable relative monotone. Similar necessary and sufficient conditions exist for U(1)-invariant pure-state transformations, but the relative monotone interpretation is less valuable.

According to the Peter-Weyl theorem, any unitary representation T of U(1) on a Hilbert space $\mathscr{H}$ may be decomposed into a direct sum of irreducible unitary representations. Write $\mathrm{U}(1) \cong \mathbb{R}/(2\pi\mathbb{Z})$, so that each element of U(1) is denoted by an angle $\theta \in [0, 2\pi)$, and, for each $h \in \mathbb{Z}$, denote by $\mathscr{H}_h$ the maximal subspace of $\mathscr{H}$ such that $T(\theta)|\psi\rangle = \exp(\imath h\theta)|\psi\rangle$. Of course, $\mathscr{H} \cong \bigoplus_{h\in\mathbb{Z}} \mathscr{H}_h$. Define the projection operator $\Pi_h : \mathscr{H} \to \mathscr{H}_h$ for each $h \in \mathbb{Z}$ and define $p_h(|\psi\rangle) = \langle\psi|\Pi_h|\psi\rangle$. p_h plays a similar role to the functions $p_k^{(n)}$ of the previous section.

Theorem 4.3 (Gour and Spekkens [18])**.** $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$ *if and only if there exists a collection of positive real numbers* $\{w_h | h \in \mathbb{Z}\}$ *such that* $w_h \geq 0$ *for each* k, $\sum_h w_h = 1$, *and*

$$p_\ell(|\psi\rangle) = \sum_{h\in\mathbb{Z}} w_h p_{\ell-h}(|\phi\rangle) \tag{4.19}$$

for each $\ell \in \mathbb{Z}$.

The similarity of Theorem 4.3 to Theorem 4.2 is quite clear, but it seems we must solve an infinite collection of linear equations in order to extract relative monotones

characterizing U(1)-invariant transformations. If $\mathscr{H}$ is finite-dimensional, however, this is not true. Note that $\dim(\mathscr{H}_h) = 0 \Rightarrow p_h(|\psi\rangle) = 0$ and that $\dim(\mathscr{H}_h) = 0$ for almost all $h \in \mathbb{Z}$ if $\dim(\mathscr{H}) < \infty$. Furthermore, $|\psi\rangle \overset{\mathrm{U}(1)}{\sim} |\phi\rangle$ if $p_h(|\psi\rangle) = p_{h-\ell}(|\phi\rangle)$ for each $h \in \mathbb{Z}$ and some fixed $\ell \in \mathbb{Z}$. Without loss of generality, we may assume

$$|\psi\rangle = \sum_{h=0}^{N-1} \sqrt{p_h(|\psi\rangle)}\,|h\rangle \;\text{ and }\; |\phi\rangle = \sum_{h=0}^{M-1} \sqrt{p_h(|\phi\rangle)}\,|h\rangle \tag{4.20}$$

for some natural numbers N and M such that $p_0(|\psi\rangle) \neq 0$, $p_0(|\phi\rangle) \neq 0$, $p_{N-1}(|\psi\rangle) \neq 0$, $p_{M-1}(|\phi\rangle) \neq 0$, $p_h(|\psi\rangle) = 0$ if $h \geq N$, $p_h(|\phi\rangle) = 0$ if $h \geq M$, and $p_h(|\psi\rangle) = p_h(|\phi\rangle) = 0$ if $h < 0$. For simplicity of notation, we will write $n_h = p_h(|\psi\rangle)$ for $0 \leq h \leq N-1$ and $n_h = 0$ for any other $h \in \mathbb{Z}$. Similarly, $m_h = p_h(|\phi\rangle)$ for $0 \leq h \leq M-1$ and $m_h = 0$ otherwise. Thus

$$|\psi\rangle = \sum_{h\in\mathbb{Z}} \sqrt{n_h}\,|h\rangle \;\text{ and }\; |\phi\rangle = \sum_{h\in\mathbb{Z}} \sqrt{m_h}\,|h\rangle\,, \tag{4.21}$$

and $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$ if and only if there is a collection $\{w_\ell | \ell \in \mathbb{Z}\}$ such that $w_\ell \geq 0$ for each $\ell \in \mathbb{Z}$, $\sum_\ell w_\ell = 1$, and $n_h = \sum_\ell w_\ell q_{h-\ell}$ for each $h \in \mathbb{Z}$.

If $h < 0$, $n_h = w_h m_0 + (\text{other terms}) = 0$. Because each summand is positive, they must all be zero for this equation to be satisfied. In particular, $w_h m_0 = 0 \Rightarrow w_h = 0$ for each $h < 0$ because $m_0 \neq 0$ by hypothesis. In addition, $n_0 = w_0 m_0 + w_1 m_{-1} + \ldots = w_0 m_0$, so $w_0 = n_0/m_0 \neq 0$ by hypothesis. We have $1 - n_0 \geq 1 - m_0$ because $w_0 \leq 1$, so the function $1 - p_0$ is a U(1)-monotone.

If $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$, we must have $M \leq N$. If not, $0 = n_{M-1} = w_0 m_{M-1} + (\text{other terms}) \Rightarrow m_{M-1} = 0$, contradicting our choice of M. If $M = N$, $0 = n_{N-1+\ell} = w_\ell m_{N-1} + (\text{other terms}) \Rightarrow w_\ell = 0$ for any $\ell > 0$. Thus, for any $0 \neq \ell \in \mathbb{Z}$, $w_\ell = 0$, so $w_0 = 1$. This implies $m_h = n_h$ for each $h \in \mathbb{Z}$, or that $|\psi\rangle = |\phi\rangle$. Henceforth, I assume $M < N$.

In the case $M = 2$, a relative monotone will fully characterize pure-state transformations $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$. Indeed, such a transformation exists if and only if there is a collection

$\{w_0, w_1, \ldots, w_{N_1}\}$ of positive real numbers such that

$$\begin{pmatrix} n_0 \\ n_1 \\ \vdots \\ n_{N-2} \\ n_{N-1} \end{pmatrix} = \begin{pmatrix} m_0 & 0 & \cdots & 0 & 0 \\ m_1 & m_0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & m_0 & 0 \\ 0 & 0 & \cdots & m_1 & m_0 \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{N-2} \\ w_{N-1} \end{pmatrix}, \tag{4.22}$$

which has the unique solution

$$\begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_{N-2} \\ w_{N-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{m_0} & 0 & \cdots & 0 & 0 \\ \frac{-m_1}{m_0^2} & \frac{1}{m_0} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{(-m_1)^{N-2}}{m_0^{N-1}} & \frac{(-m_1)^{N-3}}{m_0^{N-2}} & \cdots & \frac{1}{m_0} & 0 \\ \frac{(-m_1)^{N-1}}{m_0^{N}} & \frac{(-m_1)^{N-2}}{m_0^{N-1}} & \cdots & \frac{-m_1}{m_0^2} & \frac{1}{m_0} \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{N-2} \\ p_{N-1} \end{pmatrix}. \tag{4.23}$$

Thus, in the case $M = 2$, the relative monotone $\min_k w_k$ calculated from equation 4.23 fully characterizes the ability to enact $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$.

For larger values of M, the matrix composed of values $p_k(|\phi\rangle)$ becomes non-square, so there are many solutions to equation 4.19. One solution may be obtained through linear regression: if equation 4.19 is written in the form $\boldsymbol{p}(|\psi\rangle) = \boldsymbol{P}(|\phi\rangle)\boldsymbol{w}$, a possible solution is $\boldsymbol{w} = \left(\boldsymbol{P}^T(|\phi\rangle)\boldsymbol{P}(|\phi\rangle)\right)^{-1} \boldsymbol{P}^T(|\phi\rangle)\boldsymbol{p}(|\psi\rangle)$, where ^{T} represents the transpose of a matrix. Extra conditions may be required on $\boldsymbol{p}(|\psi\rangle)$ and $\boldsymbol{p}(|\phi\rangle)$ for there to exist solutions.

Consider the extremal case $M = N - 1$. In this situation, the existence of a solution to equation 4.19 is highly nontrivial whereas the solution itself is trivial. Indeed, there are only two nonzero values of w_k, namely w_0 and w_1. Furthermore, $w_0 = n_0/m_0$ and $w_1 = n_{N-1}/m_{N-2}$. So, should a solution exist to equation 4.19, that solution is already known. The problem is then to find conditions on the existence of a solution.

In fact, the conditions are given by substituting our values of w_0 and w_1 into equa-

tion 4.19. This yields:

$$n_k = \frac{n_0}{m_0} m_k + \frac{n_{N-1}}{m_{N-2}} m_{k-1} \tag{4.24}$$

for each $k = 0, 1, \ldots, N-1$. Furthermore, $n_0/m_0 + n_{N-1}/m_{N-2} = 1$. Rather than a collection of inequalities, then, the existence of the transformation $|\psi\rangle \overset{\mathrm{U}(1)}{\mapsto} |\phi\rangle$ depends on this collection of equalities being satisfied.

This behaviour can be captured with relative monotones, though such monotones are artificial. For instance, the equality $n_0/m_0 + n_{N-1}/m_{N-2} = 1$ may be captured by demanding that the relative monotone

$$\mathcal{R}(|\psi\rangle, |\phi\rangle) = \min\left\{n_0/m_0 + n_{N-1}/m_{N-2} - 1, 1 - n_0/m_0 - n_{N-1}/m_{N-2}\right\} \tag{4.25}$$

be positive. All of the required equalities may be captured similarly, though there is little meaning to such a description.

In conclusion, I have shown that it is possible to characterize the resourcefulness of a state in a relative fashion even when absolute quantifiers of resourcefulness remain elusive. I gave a relative monotone that completely characterized the ability to transform pure states under Z_n-invariant operations in section 4.2, and showed the similarity of such techniques to characterizations of U(1)-frameness. More generally, I argue that relative monotones may be of value in the study of other resource theories. Finding such relative monotones can alleviate certain difficulties encountered when attempting to characterize resources with the more common absolute monotones.

Chapter 5

Conclusion

Certain properties of a quantum mechanical physical system may be exploited to communicate quantum information. My thesis focusses on two such properties: entanglement and frameness. The resourcefulness of entanglement for the communication of quantum information is well-known; for example, in the achievement of quantum teleportation [1]. The resource theory of frameness is a newer development and is useful for the theoretical analysis of certain practical implementations of quantum information processing tasks [3].

In many cases, the resourcefulness of a quantum system is degraded after enacting a protocol requiring that resource. The successful teleportation of a qubit, for example, can be accomplished by reducing the entanglement between sender and receiver. Resources such as entanglement are difficult to produce, so it is desirable to minimize the resource cost of quantum information processing tasks. Such minimization is often accomplished with respect to some cost function. One example of such a cost function is a monotone.

A monotone is a real-valued function of quantum states intended to characterize the resourcefulness of that state in alleviating restrictions on achievable operations. An important requirement of a monotone is then that it not increase when achievable operations are applied. Thus, if $\mathcal{E}$ is an achievable channel and f is a monotone, we require $f(\rho) \geq f(\mathcal{E}(\rho))$ for any state ρ. This notion of monotone is a direct extension of entanglement monotones [21], which cannot increase under the application of LOCC channels to the argument state. This is in fact the only requirement of an entanglement monotone [15], though further conditions were once imposed [16].

Entanglement monotones are powerful for analyzing tasks requiring entanglement. In Chapter 3, I present in some detail the phenomenon of entanglement catalysis [4], wherein

entanglement may be used as a resource without being consumed. The ability of a given entangled state to serve as a catalyst can be quantified with entanglement monotones. I have given conditions on the values of a collection of entanglement monotones known as the generalized concurrences [19] for a state to be able to catalyze a given entanglement-assisted LOCC pure-state transformation.

The ability of the generalized concurrences to characterize the entanglement of a potential catalyst is a consequence of their non-monotonic behaviour under the application of entanglement-assisted LOCC channels. The concurrences are therefore not 'catalytic' monotones. A catalytic monotone is defined in the same way as an entanglement monotone, except that it does not increase even under eLOCC channels. Monotones may in fact be defined whenever the set of achievable quantum channels is restricted. In frameness theory, the restriction is that every channel must commute with some given group action.

There has been some uncertainty in the literature regarding the appropriate definition of an entanglement monotone, in particular with regard to the quantification of the average entanglement output of a local measurement procedure. Vidal's original definition of an entanglement monotone required that the weighted average of the entanglement of possible outcomes of a local measurement should not be greater than the entanglement present before the measurement [16]. Plenio argued that this definition excludes reasonable measures of entanglement and is therefore too restrictive [15]. It is now accepted that the only requirement for an entanglement monotone is that it is a real-valued function of states that does not increase under application of LOCC channels to the argument [21]. The stronger 'convexity' requirement of Vidal leads to what we call an 'ensemble monotone', and is distinct from the 'absolute monotone' of Plenio.

Even the notion of an absolute monotone can be inadequate for the characterization of some types of resourcefulness. As evidence, I present a characterization of the frameness

of a pure state in the case that reference choices are related by the action of a cyclic group. In Chapter 4, I characterize this resource theory with a type of cost function I call a 'relative monotone'. This assigns a resource cost to a state defined relative to another state, rather than in isolation.

I argue that relative monotones should be considered valid quantifiers of resourcefulness for three reasons. First, any resourcefulness that may be described using absolute monotones may also be described with relative monotones. Second, descriptions of resourcefulness can be made more concise with relative monotones. Third, there are resource theories whose description with absolute monotones remains elusive though a description with relative monotones is readily available.

The relative approach could have wider consequences for the field of entanglement theory. Bipartite entanglement has been studied for some time with entanglement monotones, but this approach has limitations when applied to multipartite entanglement. For example, there are two distinct classes of tripartite entanglement for three qubits [34]. The distinction between these classes is due to the inability to convert states in one class to states in another via LOCC channels with any nonzero probability. When considering four-party entanglement, the number of distinct classes becomes infinite. This suggests that an 'absolute' characterization of multipartite entanglement will require an infinite collection of monotones in most cases. A characterization in terms of relative monotones will be far more concise.

Bibliography

[1] Bennett, C., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., and Wootters, W., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **70**(13), 1895–1899 (1993).

[2] Bennett, C. H. and Wiesner, S. J., "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.* **69**, 2881–2884 (Nov 1992).

[3] Rudolph, T. and Sanders, B., "Requirement of optical coherence for continuous-variable quantum teleportation," *Physical Review Letters* **87**(7), 77903 (2001).

[4] Jonathan, D. and Plenio, M., "Entanglement-assisted local manipulation of pure quantum states," *Physical Review Letters* **83**(17), 3566–3569 (1999).

[5] Shannon, C., "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review* **5**(1), 3–55 (2001).

[6] Cover, T. and Thomas, J., [*Elements of information theory*], Wiley Online Library (1991).

[7] Bennett, C., Brassard, G., et al., "Quantum cryptography: Public key distribution and coin tossing," in [*Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*], **175**, 0, Bangalore, India (1984).

[8] Cirac, J., Ekert, A., Huelga, S., and Macchiavello, C., "Distributed quantum computation over noisy channels," *Physical Review A* **59**(6), 4249–4254 (1999).

[9] Schumacher, B., "Quantum coding," *Phys. Rev. A* **51**, 2738–2747 (Apr 1995).

[10] Wootters, W. K. and Zurek, W. H., "A single quantum cannot be cloned," *Nature* **299**, 802–803 (October 1982).

[11] Nielsen, M., "Conditions for a class of entanglement transformations," *Physical Review Letters* **83**(2), 436–439 (1999).

[12] Vidal, G., "Entanglement of pure states for a single copy," *Physical Review Letters* **83**(5), 1046–1049 (1999).

[13] Bartlett, S., Rudolph, T., and Spekkens, R., "Reference frames, superselection rules, and quantum information," *Reviews of Modern Physics* **79**(2), 555–609 (2007).

[14] Bartlett, S., Rudolph, T., Spekkens, R., and Turner, P., "Degradation of a quantum reference frame," *New Journal of Physics* **8**, 58 (2006).

[15] Plenio, M., "Logarithmic negativity: A full entanglement monotone that is not convex," *Physical review letters* **95**(9), 90503 (2005).

[16] Vidal, G., "Entanglement monotones," *Journal of Modern Optics* **47**(2), 355–376 (2000).

[17] Turgut, S., "Necessary and sufficient conditions for the trumping relation," *Journal of Physics A* **40**, 12185–12212 (2007).

[18] Gour, G. and Spekkens, R., "The resource theory of quantum reference frames: manipulations and monotones," *New Journal of Physics* **10**, 033023 (2008).

[19] Gour, G., "Family of concurrence monotones and its applications," *Physical Review A* **71**(1), 12318 (2005).

[20] Sanders, Y. R. and Gour, G., "Necessary conditions for entanglement catalysts," *Physical Review A* **79**(5), 54302 (2009).

[21] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K., "Quantum entanglement," *Reviews of Modern Physics* **81**(2), 865–942 (2009).

[22] Conway, J., [*A course in functional analysis*], Springer (1990).

[23] Kraus, K., [*States, effects, and operations : fundamental notions of quantum theory : lectures in mathematical physics at the University of Texas at Austin*], Springer-Verlag, Berlin ; New York : (1983).

[24] Nielsen, M. and Chuang, I., [*Quantum computation and quantum information*], Cambridge University Press, Cambridge : (2000).

[25] Lo, H. and Popescu, S., "Concentrating entanglement by local actions: Beyond mean values," *Physical Review A* **63**(2), 22301 (2001).

[26] Marshall, A. W. and Olkin, I., [*Inequalities : theory of majorization and its applications*], Academic Press, New York : (1979).

[27] Rényi, A., "On measures of entropy and information," in [*Fourth Berkeley Symposium on Mathematical Statistics and Probability*], 547–561 (1961).

[28] Hill, S. and Wootters, W., "Entanglement of a pair of quantum bits," *Physical review letters* **78**(26), 5022–5025 (1997).

[29] Rungta, P., Bužek, V., Caves, C., Hillery, M., and Milburn, G., "Universal state inversion and concurrence in arbitrary dimensions," *Physical Review A* **64**(4), 42315 (2001).

[30] Bennett, C., Bernstein, H., Popescu, S., and Schumacher, B., "Concentrating partial entanglement by local operations," *Physical Review A* **53**(4), 2046–2052 (1996).

[31] Gour, G., "Infinite number of conditions for local mixed-state manipulations," *Physical Review A* **72**(2), 22323 (2005).

[32] Fuchs, C. A., *Distinguishability and Accessible Information in Quantum Theory*, PhD thesis, University of New Mexico (1996).

[33] Hayden, P., Horodecki, M., and Terhal, B., "The asymptotic entanglement cost of preparing a quantum state," *Journal of Physics A: Mathematical and General* **34**, 6891 (2001).

[34] Dür, W., Vidal, G., and Cirac, J., "Three qubits can be entangled in two inequivalent ways," *Physical Review A* **62**(6), 62314 (2000).