2022-01

Conic Linear Programming in Quantum Informatio

Zafar, Fasiha Binat

UNIVERSITY OF CALGARY

Conic Linear Programming in Quantum Information

by

Fasiha Binat Zafar

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

JANUARY, 2022

Abstract

A frequently studied problem in quantum resource theories (QRTs) is converting one resource state into another by applying free operations. If convexity arises in QRTs, convex analysis tools can be utilized in the analysis of these problems. The separating hyperplane theorem ensures the existence of at least one witness for each resource state in convex QRTs. By using this idea, necessary and sufficient conditions in terms of resource monotones are derived for generic convex static QRTs. We use this result to derive the complete family of conversion resource monotones for majorization as a subset of f-divergences. For classical conditional majorization, necessary and sufficient conditions for state conversion are derived in the form of a homogeneous convex function. We unified the pre-existing results under the umbrella of resource-theoretic framework. The new approach helps in the significant simplification of the proofs. Furthermore, we extend the work to derive a new complete family of conversion monotones for quantum conditional majorization in terms of min-entropy using the same techniques and procedures. We expect the quantum conditional majorization will find operational applications in future work similar to its classical counterpart.

Acknowledgements

First, I would like to express my heartfelt gratitude to my supervisor Dr. Gilad Gour and co-supervisor Dr. Carlo Maria Scandolo, for their unwavering support and guidance. Their knowledge and experience motivated me at each crucial juncture of my masters' studies. I would not have been able to accomplish this seemingly insurmountable task without their due attention and tutelage. I am also thankful to the committee member Dr. Barry Sanders for his suggestions and recommendations for improvement. His guidance played a pivotal role in refining this study. I am grateful to Dr. Paul Barclay for agreeing to join my committee. I would like to extend my appreciation and acknowledgement to my peers Gaurav Saxena and Jianing Geng, whom I always approach for constructive discussion regarding the subject material. I would like to extend thanks to the "Department of Mathematics and Statistics" for the financial assistance that allowed me to complete my masters' degree. Last but not least, I would like to acknowledge my parents for their unwavering support at each and every step of my life.

To the memory of my grandmother.

Table of Contents

Abstract ii

Acknowledgements iii

Dedication iv

Table of Contents v

List of Figures and Illustrations vii

List of Symbols, Abbreviations and Nomenclature viii

1 Introduction 1

2 Preliminaries 6
2.1 Hilbert Spaces . . . 6
2.1.1 Bounded Operators . . . 9
2.1.2 Dirac Notation . . . 10
2.1.3 Direct Sum of Hilbert Spaces . . . 11
2.1.4 Tensor Product of Hilbert Spaces . . . 12
2.2 Quantum State . . . 15
2.3 Quantum Measurement . . . 18
2.4 A Space of Linear Operators . . . 19
2.5 Quantum Channel . . . 20
2.5.1 Choi Representation . . . 23
2.6 Resource Theory . . . 26
2.6.1 Quantum Resource Theory . . . 27
2.6.2 Tensor Structure in Quantum Resource Theories . . . 29
2.6.3 Convex Quantum Resource Theory . . . 30
2.6.4 Resource Quantifiers . . . 30
2.6.5 Witness-based Quantifiers . . . 32
2.7 Notation . . . 32

3 Convex Analysis 33
3.1 Convex functions and sets . . . 33
3.1.1 Convex functions . . . 36

3.2 Supporting and separating hyperplane 38
3.3 Conic programming 39

4 Complete Characterization of Static-Resources **45**
4.1 Background 46
4.2 A complete family of static monotones 47

5 Relative Majorization and f-Divergences **53**
5.1 Majorization 55
5.2 Re-derivation of RSS Theorem 58

6 Classical Conditional Majorization **61**
6.1 Classical Conditional Random Relabelling 61
6.2 Characterization of Classical Conditional Majorization 63

7 Quantum Conditional Majorization **68**
7.1 Classical-Quantum State 68
7.2 Quantum Conditional Random Relabelling 69
7.3 Characterization of Quantum Conditional Majorization 70

8 Conclusion **76**

Bibliography **78**

List of Figures and Illustrations

5.1 Lorenz curve for pair of two probability vectors $(\mathbf{p}, \mathbf{q})$ and $(\mathbf{p}', \mathbf{q}')$, when $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{p}', \mathbf{q}')$. 57

6.1 Alice and Bob initially share a classical-classical state P. Bob can apply any arbitrary classical operations on his register. Alice performs random relabeling operations on her register conditioned on classical outputs obtained by Bob. Double line shows classical communication. 62

7.1 Alice and Bob initially share a classical-quantum state. Bob preforms an arbitrary quantum operation on his subsystem which produces a classical as well as quantum output. Alice then carries out random relabeling operations on her register, possibly conditioned on classical outputs obtained by Bob. Double lines represents classical communication and a single line is used for quantum communication. 70

List of Symbols, Abbreviations and Nomenclature

Symbol or abbreviation	Definition
CPTP	Completely Positive Trace Preserving map.
A, B, C	Quantum systems.
X, Y	Classical Systems.
$\mathcal{H}^A$	Hilbert space of dimension $\|A\|$.
$\mathfrak{B}(A, B)$	Space of bounded linear operators from $\mathcal{H}^A$ to $\mathcal{H}^B$.
$\mathrm{Herm}(A, B)$	Hermitian operators in $\mathfrak{B}(A, B)$.
$\mathfrak{D}(A)$	Density operators in $\mathrm{Herm}(A, B)$.
$\mathfrak{L}(A, B)$	Space of linear maps from $\mathfrak{B}(A) \to \mathfrak{B}(B)$.
id^A	Identity map:$\mathfrak{B}(A) \to \mathfrak{B}(A)$.
$\mathcal{E}, \mathcal{N}, \mathcal{M}$	Quantum channels.
$J_{\mathcal{E}}$	Choi Jamiołkowski matrix of the map of $\mathcal{E}$.
a, c	Real numbers.
$(\cdot)^T$	Transpose of $(\cdot)$.
$(\cdot)^\dagger$	Transpose conjugate of $(\cdot)$.
$\mathrm{Tr}[\rho]$	Trace of ρ.
$\to$	Quantum output / input.
$\Longrightarrow$	Classical output / input.
$[\|A\|]$	The set $\{1, 2, \cdots, \|A\|\}$.

Chapter 1

Introduction

The theory of quantum mechanics provides the explanation of phenomena and dynamics at the atomic and subatomic levels. Information theory is the study of how information can be transferred, processed or stored. The merging of these two very significant theories gives rise to quantum information theory. Quantum information encompasses how quantum mechanical phenomena play a part in the transmission, processing and storage of information. The difference between quantum information theory and classical information theory lies in how superposition and entanglement, etc., which are nonexistent in the classical realm, can be used to perform information processing tasks. A superposition of quantum states is intrinsically and mathematically a linear combination of vectors, while entanglement is instead a more complicated phenomenon. Entanglement is inherently a correlation between separate systems that is stronger than what can be achieved classically Ref. (Sharma, 2010). These types of correlations can even exist for the systems that are spatially apart. The importance of entanglement was identified in its ability to efficiently simulate quantum systems Ref. (Feynman, 1982). This inspired the new era of quantum computation with the prospect that one day a quantum computer can be built which will be able to solve problems more efficiently and quickly compared to the classical computers Ref. (Raussendorf and Briegel, 2001). It was proved that entanglement is a crucial resource to achieve computa-

tional speedups compared to the classical algorithms that attain the same results Ref. (Vidal, 2003). Entanglement is an essential consumable resource to perform tasks like quantum teleportation Ref. (Bennett, Brassard, et al., 1993) and dense coding Ref. (Bennett and Wiesner, 1992) which can not be done classically. Also, it is helpful for secure quantum communication and cryptography Ref. (Bennett and Brassard, 2014).

In quantum information theory, convex structures arise naturally in several scenarios whenever the set of all possible operations and quantum states is convex. Because of this convex structure, convex analysis tools can be used. Convex optimization is used in quantum information widely to quantify quantum resources. An example is entanglement, where quantification is often expressed as convex optimization Ref. (R. Horodecki et al., 2009). In the early stage of the development of quantum information theory, it was evident that the fundamental resource theoretic task in QRTs is to analyze the conversion of one resource into another. The resource theory perspective tackles this problem in a natural way. Instead of residing with the detail of *mechanics* of transition of states, it deals with the criteria of when(not how) inter-convertibility of states is possible. The motivational idea behind resource theories is intuitive and general. All possible operations are divided in two categories *free* and *prohibited*. Free states are free preparation procedures, there exist states that don't fall in this category are called the resources. A resource theory induces partial preorder which generates a hierarchy. If one state can be converted into another via free operation then the former is more resourceful than the latter. Real-valued functions that quantifies resourcefulness of quantum states according to hierarchy generated by resource theories or resource theoretic task under consideration are called resource monotones. A famous example is the quantum resource theory of entanglement, in which an entangled state is treated as a resource and local operations and classical communication are free operations. If the set of free states and free operations is convex then we call them *Convex Quantum Resource Theories* and convex analysis tools can be used to analyze the problems. These resources in different scenarios are either of the forms of classical, quantum, classical-quantum, classical-

classical, noisy states etc. We have considered some particular cases in this thesis. The class of resource theories for which the objects of interest are states is called *Static Quantum Resource Theories*. Necessary and sufficient conditions for transition of states in terms of monotonic functions are derived for generic static convex quantum resource theory. Such monotonic functions are then written in terms of a conic linear program. This generalized result is used to re-derive some already existing results like f-divergence and classical conditional majorization, significance of which is already known, like divergences have known far and wide applications to economics, statistics, game theory etc. Conditional majorization is used to derive the generalized conditional uncertainty relation Ref. (Gour, Grudka, et al., 2018) in the presence of classical memory. The generalized conditional uncertainty principle in some cases outperforms the entropic conditional uncertainty principle Refs. (Hall, 1995; Renes and Boileau, 2009). In Ref. (Brandsen, Geng, and Gour, 2021) operational meaning for this has been presented, where monotones reduce to pair of functions and each pair function provides the best probability to win certain games of chance.

In the end, by using the same framework, a new result is proved. A complete family of monotones is derived that quantifies the conversion of one classical-quantum state into another via free operations. We expect this result will find applications to different scenarios like its classical counterpart, discussed in the last paragraph.

The structure of this thesis is discussed below. Chapters 2 and 3 contain the necessary mathematical background for quantum information, the underlying theory and convex analysis. Chapter 4 includes the derivation of the theorem used in chapters 5 and 6 to re-derive the pre-existing results from a resource theoretic prospective. Chapter 7 consists of the new result. A brief chapter-by-chapter breakdown of the thesis is given below.

Chapter 2 (Preliminaries) : This chapter includes all the mathematical preliminaries, background knowledge, tools and techniques needed to understand the thesis. Mathematical definitions of the fundamental structures in quantum mechanics like quantum state, quantum channel etc are presented. At the end, the resource theoretic framework is discussed and

applied in the context of quantum information.

Chapter 3 (Convex Analysis) : In chapter 3, the main concepts of convex analysis used in this thesis are presented. Basic definitions necessary to understand the tool of convex analysis (i.e. separating hyperplane theorem etc.), like convex functions, convex sets etc., are provided. At the end of the chapter, conic linear programming and its duality are reviewed.

Chapter 4 (Complete Characterization of Static-Resources) : This chapter includes the simplified version of the theorem proved in Ref. (Gour and Scandolo, 2020). Then the explanatory proof of the theorem is provided, which gives the complete set of monotones for inter-convertibility of quantum state. The version of the theorem discussed in the chapter is for the convex static quantum resource theories. In subsequent chapters, corollaries of this theorem in different scenarios are provided one by one.

Chapter 5 (f-Divergences) : In chapter 5, we look at the concept of f-divergences from the resource theoretic point of view. This approach helps us re-derive the theorem in Ref. (Ruch and Mead, 1976). The theorem provides the necessary and sufficient condition for transforming one pair of probability vectors into another by applying the same column-stochastic matrix to both vectors in the form of some monotonic functions, which turn out to be a subset of f-divergences.

Chapter 6 (Classical Conditional Majorization) : In chapter 6, we re-derive the theorem first presented in Ref. (Gour, Grudka, et al., 2018) using resource theories, which provides a complete family of monotonic conditions for the conversion of one classical-classical state into another by the application of free operations. Free operation for this case are classical conditional random relabelling; an arbitrary classical operations can be applied on one classical subsystem and random relabelling on the other possibly depending on the classical outputs of the operations performed on the former. This approach has leads a significant simplification of proof.

Chapter 7 (Quantum Conditional Majorization) : This chapter presents new work that is yet to be published. This chapter uses the theorem given in chapter 4 to

provide a complete family of monotonic functions for inter-convertibility of classical-quantum states. These monotones are min-entropic function which provides necessary and sufficient conditions for the transition of states by the application of free operations. Free operation for this case are quantum conditional random relabelling; an arbitrary quantum operation can be applied on quantum subsystem and random relabelling on classical one possibly depending on the classical outputs of the operations performed on the former. We expect the future applications of this theorem will be similar to the classical case discussed in chapter 6.

Chapter 2

Preliminaries

Linear algebra over complex vector spaces provides the primary language of expression for quantum information theory. Notations used in quantum information differ from usual notations used in linear algebra, especially Dirac notation (bra-ket notation). This chapter will give an overview of the underlying theory of quantum information, notations and mathematical preliminaries that will be used throughout thesis. We will restrict our attention to finite-dimensional quantum information theory.

2.1 Hilbert Spaces

Every physical system has an associated complex Hilbert space Ref. (Toyoda, 1973) according to the postulates of quantum mechanics. To understand the definition of Hilbert space, we first present the necessary concepts to lay out the framework on which the working definition of Hilbert space is based.

- **Field**: A basic algebraic structure, field ($\mathbb{F}$) is the set on which the operation of addition and multiplication are defined; also, there exists the additive and multiplicative inverse (for non-zero elements) in the set. Common examples of field are the sets of all real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$.

- **Vector Space**: A vector space V, also called linear space, is a set closed under operations of addition and multiplication by scalars (Scaling). A very well-known example of vector space is $\mathbb{R}^2$, where the elements of this space are two-dimensional vectors. Thus, adding two vectors yields a vector that is also in the vector space. Similarly a scaled vector is also in $\mathbb{R}^2$. A vector space satisfies the following set of axioms:

  - Commutativity: $\phi_1 + \phi_2 = \phi_2 + \phi_1$, $\forall \phi_1, \phi_2 \in V$.
  - Associativity in vector addition: $(\phi_1 + \phi_2) + \phi_3 = \phi_1 + (\phi_2 + \phi_3)$, $\forall \phi_1, \phi_2, \phi_3 \in V$.
  - Additive identity: $\phi_1 + 0 = \phi_1$, $\forall \phi_1 \in V$ and $\exists 0 \in V$.
  - Additive inverse: $\phi_1 + (-\phi_1) = 0$, $\forall \phi_1 \in V$, $\exists -\phi_1 \in V$ and $\exists 0 \in V$.
  - Distributivity in Scalar Addition: $(a + b)\phi_1 = a\phi_1 + b\phi_1$, $\forall \phi_1 \in V$ and $\forall a, b \in \mathbb{F}$.
  - Associativity in Scalar Multiplication: $(ab)\phi_1 = a(b\phi_1)$, $\forall \phi_1 \in V$ and $\forall a, b \in \mathbb{F}$.
  - Distributivity in Vector Addition: $a(\phi_1 + \phi_2) = a\phi_1 + a\phi_2$, $\forall \phi_1, \phi_2 \in V$ and $\forall a \in \mathbb{F}$.
  - Scalar Multiplicative identity: $1\phi_1 = \phi_1$, $\forall \phi_1 \in V$ and $\exists 1 \in \mathbb{F}$.

- **Inner Product Space**: A vector space over the field $\mathbb{C}$ with an additional structure of inner product map is called an inner product space V. The inner product map is represented as $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$.

  An inner product space satisfies the following three properties for all vectors $\phi, \psi, \omega \in V$ and all scalars $a \in \mathbb{C}$;

  - Conjugate symmetry: $\langle \psi, \phi \rangle = \overline{\langle \phi, \psi \rangle}$.
  - Linearity in the second argument: $\langle \psi + \omega, a\phi \rangle = a\langle \psi, \phi \rangle + a\langle \omega, \phi \rangle$.
  - Positive-definiteness: $\langle \phi, \phi \rangle \geq 0$, equality only holds only if $\phi = 0$.

  We will use the Dirac notation $\langle .|. \rangle$ instead of $\langle ., . \rangle$ in this thesis, which will be discussed later in more detail.

  A norm is a function on vector space that satisfies the following properties;

- Non-negativity: $\|\phi\| \geq 0$ and equality holds only if $\phi = 0$, $\forall \phi \in V$.
- Multiplication by Scalar: $\|a\phi\| = |a|\|\psi\|$, $\forall \phi \in V$ and $\forall a \in \mathbb{C}$.
- Triangular Inequality: $\|\phi + \psi\| \leq \|\phi\| + \|\psi\|$, $\forall \phi, \psi \in V$.

The existence of inner product structure in the vector space induces the norm $\|\phi\|_2 = \sqrt{\phi^\dagger \phi}$, which in turn induces the metric $d(\phi, \psi) = \|\phi - \psi\|_2$. A metric gives the notion of *distance* between two objects of a space. For vector spaces, objects are vectors. The aforementioned metric satisfies the following properties;

- Identity of indiscernible: $\|\phi - \psi\|_2 = 0 \implies \phi = \psi$, $\forall \phi, \psi \in V$.
- Symmetry: $\|\phi - \psi\|_2 = \|\psi - \phi\|_2$, $\forall \phi, \psi \in V$.
- Triangular Inequality: $\|\phi - \psi\|_2 \leq \|\phi - \omega\|_2 + \|\omega - \psi\|_2$, $\forall \phi, \psi, \omega \in V$.

- **Completeness**: A sequence of vectors $\{\phi\}_x$ for $x \in \{1, 2, \cdots\}$, in inner product vector space is called a Cauchy sequence if for $\epsilon > 0$, there exist $M \in \mathbb{N}$ such that for any $n, m \geq M$,

$$\|\phi_n - \phi_m\| < \epsilon.$$

An inner product vector space is complete if every Cauchy sequence converges in the metric induced by the inner product structure. A Cauchy sequence is said to converge if there exists ϕ in the inner product space such that $\lim_{x \to \infty} \|\phi_x - \phi\| = 0$.

We are now equipped with the necessary background to present the definition of *Hilbert Space*.

Hilbert Space
A complete inner product vector space is called Hilbert space.

Well-known examples of Hilbert space are $\mathbb{R}^n$ and $\mathbb{C}^n$. All finite-dimensional inner product spaces are complete: finite-dimensional inner product spaces are isomorphic to $\mathbb{R}^n$ or $\mathbb{C}^n$

and hence, are complete. Isomorphism, in a generic sense, is a *structure-preserving map* between two groups that can be reversed through inverse mapping. In a strictly mathematical sense, it is a homomorphism (structure-preserving map, in linear case preserves abelian group structure and scalar multiplication) with bijection(onto and one-to-one). The notation that will be used in this text to represent the d dimensional Hilbert space is $\mathcal{H}^d$. A Hilbert space associated with physical system A will be denoted as $\mathcal{H}^A$, and $|A|$ represents the dimension of $\mathcal{H}^A$. Sometimes for convenience, A is used to denote the same Hilbert space. Some plausible physical assumptions are posed when considering the framework for the quantum mechanics. The basic features of quantum mechanics are that states are positive trace one operators which can exhibit phase. These requirements are fulfilled completely by complex Hilbert spaces.

2.1.1 Bounded Operators

Proceeding to a discussion of linear maps taking one Hilbert space to another, the understanding of bounded operators is essential. Quantum operators and quantum states are subsets of this larger set referred to as bounded operators.

Bounded Linear Operator

A bounded linear operator is a liner map $L : \mathcal{H}^A \to \mathcal{H}^B$ such that,

$$\frac{\|L\phi\|}{\|\phi\|} \leq N,$$

where $N \geq 0$, $\forall \phi \in \mathcal{H}^A$ and $\phi \neq 0$.

We will be denoting the set of bounded operators that take Hilbert space $\mathcal{H}^A$ to $\mathcal{H}^B$ as $\mathfrak{B}(A, B)$. The of set bounded operators $\mathcal{H}^A \to \mathcal{H}^A$ will be represented as $\mathfrak{B}(A)$.

To each physical system is ascribed a Hilbert space. As in quantum mechanics, a system is probabilistic in nature, requiring a mathematical structure that can assign probabilities to measurements of the observable properties. This requirement is fulfilled by assigning a

trace class operator (An operator for which trace is defined and is finite independent of the basis) to a state of system that has to be normalized (trace is equal to 1) and positive semi-definite to comply with the probabilistic nature of the system. Now we formally present the definition of quantum state.

Quantum State

$\rho \in \mathfrak{B}(A) = \mathfrak{B}^*(A)$ (Hermitian) is said to be a quantum state if;

- $\langle\phi|\,\rho\,|\phi\rangle \geq 0, \quad \forall\phi \in \mathfrak{B}(A)$ (Positive Semi-definiteness).
- $\mathrm{Tr}[\rho] = 1$ (Normalized).

Where $*$ represents the adjoint.

'Tr' in the above-mentioned definition represents the trace operation, the sum of all diagonal elements of a matrix (for finite-dimensional case).

Quantum state is Hermitian as well as normalized (trace is equal to 1) and positive semi-definite. The latter two are the additional constraints so the set of quantum state denoted as $\mathfrak{D}(A) \subset \mathrm{Herm}(A)$, where $\mathrm{Herm}(A)$ is a set of Hermitian matrices acting on $\mathcal{H}^A$ and $\mathrm{Herm}(A) \subset \mathfrak{B}(A)$. We will use the terms density operator or matrix and state interchangeably and $\mathfrak{D}(A)$ is a set of all density matrices.

2.1.2 Dirac Notation

The Dirac notation Ref. (Dirac, 1939), introduced by Paul Dirac, is widely used in quantum information.

In Dirac notation vector $\phi \in \mathcal{H}$ is represented as $|\phi\rangle$ called ket vector. The conjugate transpose of vector $|\phi\rangle$, i.e. $|\phi\rangle^\dagger$, is represented as $\langle\phi|$ called bra vector. Hence the inner product between vectors $|\phi\rangle$ and $|\psi\rangle \in \mathcal{H}$ is represented as $\langle\phi|\psi\rangle$.

The standard basis (also called the computational basis) of $\mathbb{C}^d$ will be denoted as $|0\rangle, |1\rangle, ..., |d-1\rangle$. The orthogonality of basis is represented as $\langle v|w\rangle = \delta_{vw}$ for all $v, w \in \{0, 1, \cdots, d-1\}$.

For $\mathbb{C}^d$, the standard basis elements in matrix form are written as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots \quad , |d-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{2.1}$$

A linear functional on a Hilbert space $\mathcal{H}$ is a function $f_\phi : \mathcal{H} \to \mathbb{C}$, that satisfies the following properties:

1. $f_\phi(|\psi\rangle + |\omega\rangle) = f_\phi(|\psi\rangle) + f_\phi(|\omega\rangle)$, $\forall \phi, \psi \in \mathcal{H}$.

2. $f_\phi(a\,|\psi\rangle) = a f_\phi(|\psi\rangle)$, $\forall \psi \in \mathcal{H}$ and $\forall a \in \mathbb{C}$.

Using this notion of linear functional we give the definition of dual of Hilbert space.

The dual of Hilbert space $\mathcal{H}$ represented as $\mathcal{H}^*$ is the set of linear functionals on the Hilbert space $\mathcal{H}$. For $|\psi\rangle \in \mathcal{H}$, the linear functional $f_\phi \in \mathcal{H}^*$ can be defined in terms of inner product as $f_\phi(|\psi\rangle) := \langle\phi|\psi\rangle \;\; \forall\, |\psi\rangle \in \mathcal{H}$. Hence the standard basis elements for the dual of $\mathbb{C}^d$ in matrix forms are just row matrices written as,

$$\langle 0| = (1\ 0\ \cdots\ 0), \quad \langle 1| = (0\ 1\ \cdots\ 0), \quad \cdots \quad , \langle d-1| = (0\ 0\ \cdots\ 1). \tag{2.2}$$

This notation is precise and convenient as it saves a lot of time and effort by getting rid of the excessive script. The inner product of vectors $\phi, \psi \in \mathcal{H}$ is usually represented as $\psi^\dagger \phi$ and in the bra-ket notation it is denoted as $\langle\psi|\phi\rangle$, which is seamless and intuitive. The norm of vector is defined as $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$.

2.1.3 Direct Sum of Hilbert Spaces

Consider two Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ then the direct sum of these will be represent as $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ if $\mathcal{H}_2 \cap \mathcal{H}_1 = \{0\}$ and $\mathcal{H} = \mathcal{H}_1 + \mathcal{H}_2$. Formally direct sum of $\mathcal{H}_1$ and $\mathcal{H}_2$ is

defined as follows:

$$\mathcal{H} := \{(\psi, \phi) : |\phi\rangle \in \mathcal{H}_1 \text{ and } |\psi\rangle \in \mathcal{H}_2\}. \tag{2.3}$$

Following the properties of the direct sum of the Hilbert spaces;

- Addition Rule: $(\psi_1, \phi_1) + (\psi_2, \phi_2) := (\psi_1 + \psi_2, \phi_1 + \phi_2)$, where $\forall \psi_1, \psi_2 \in \mathcal{H}_1$, $\forall \phi_1, \phi_2 \in \mathcal{H}_2$ and $\forall (\psi_1, \phi_1), (\psi_2, \phi_2) \in \mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$.

- Scalar Multiplication Rule: $c(\psi, \phi) = (c\psi, c\phi)$, where $\forall \psi \in \mathcal{H}_1$, $\forall \phi \in \mathcal{H}_2$, $c \in \mathbb{F}$ and $\forall (\psi, \phi) \in \mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$.

- Inner Product: $\langle (\psi_1, \phi_1) | (\psi_2, \phi_2) \rangle := \langle \phi_1 | \psi_1 \rangle + \langle \phi_2 | \psi_2 \rangle$, where $\forall \psi_1, \psi_2 \in \mathcal{H}_1$, $\forall \phi_1, \phi_2 \in \mathcal{H}_2$ and $\forall (\psi_1, \phi_1), (\psi_2, \phi_2) \in \mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$.

The dimension of $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ is equal to $\dim(\mathcal{H}) = \dim(\mathcal{H}_1) + \dim(\mathcal{H}_2)$. Elements of $|\psi\rangle \in \mathcal{H}_1$ can be identified as $(\psi, 0) \in \mathcal{H}$. An example is $\mathbb{R}^4$ can be written as the direct sum of $\mathbb{R}^2 \oplus \mathbb{R}^2$.

2.1.4 Tensor Product of Hilbert Spaces

If there are two Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ with dimensions $|A|$ and $|B|$ respectively, the tensor product of these two Hilbert spaces is represented as $\mathcal{H}^{AB} := \mathcal{H}^A \otimes \mathcal{H}^B$ with dimensions $|A||B|$, where $\otimes$ represents the standard tensor product. If $\{|v\rangle\}_{v=0}^{|A|-1}$ and $\{|w\rangle\}_{v=0}^{|B|-1}$ are the standard bases of $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively, then the elements of $\mathcal{H}^{AB}$ can be written as linear combinations of $|vw\rangle := |v\rangle \otimes |w\rangle$. For $\{|\phi_i\rangle\} \in \mathcal{H}^A$, $\{|\psi_j\rangle\} \in \mathcal{H}^B$ and $a \in \mathbb{C}$, the tensor product on Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ satisfies the following properties:

- $|\sum_i \phi_i\rangle \otimes |\psi_j\rangle = \sum_i |\phi_i\rangle \otimes |\psi_j\rangle$.

- $|\phi_i\rangle \otimes |\sum_j \psi_j\rangle = \sum_j |\phi_i\rangle \otimes |\psi_j\rangle$.

- $a(|\phi_i\rangle \otimes |\psi_j\rangle) = a\,|\phi_i\rangle \otimes |\psi_j\rangle = |\phi_i\rangle \otimes a\,|\psi_j\rangle$.

Generalizing the notion of tensor product for a collection of Hilbert spaces $\{\mathcal{H}_j\}_{j\in I}$, the tensor product of collection of these Hilbert spaces is $\bigotimes_{j\in I}\mathcal{H}_j$ with its orthonormal basis represented as $\sum_{j_1,j_2,\cdots,j_{|I|}}|v_{j_1}\rangle\otimes|v_{j_2}\rangle\otimes\cdots\otimes|v_{j_{|I|}}\rangle$, where $\{v_{j_i}\}$ is the orthonormal basis of $\mathcal{H}_i$. The dimension of $\bigotimes_{j\in I}\mathcal{H}_j$ is equal to product of dimensions of all Hilbert spaces $\dim(\bigotimes_{j\in I}\mathcal{H}_j)=\prod_{j=1}^{|I|}\dim(\mathcal{H}_j)$. Now for the ease of understanding, let us consider an example of tensor product of two Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ with orthonormal basis $\{|v\rangle\}_{v=0}^{|A|-1}$ and $\{|w\rangle\}_{w=0}^{|B|-1}$ respectively. The elements of tensor product space $\mathcal{H}^{AB}$ are represented as follows:

$$\mathcal{H}^{AB}=\Big\{\sum_{v,w=0}^{|A|-1,|B|-1}m_{vw}\,|v\rangle^A\otimes|w\rangle^B\Big\}. \tag{2.4}$$

Consider two elements $|\psi\rangle\,,|\phi\rangle\in\mathcal{H}^{AB}$ written as

$$|\psi\rangle^{AB}=\sum_{v,w=0}^{|A|-1,|B|-1}m_{vw}\,|v\rangle^A\otimes|w\rangle^B\,.$$

$$|\phi\rangle^{AB}=\sum_{v,w=0}^{|A|-1,|B|-1}n_{vw}\,|v\rangle^A\otimes|w\rangle^B\,.$$

$n_{vw},m_{vw}\in\mathbb{C}$, are the entries of matries N and M respectively. The inner product for these two elements can be written as follows:

$$\langle\phi|\psi\rangle=\mathrm{Tr}[N^\dagger M], \tag{2.5}$$

The tensor product of vectors is the Kronecker Tensor Product of matrices. As finite n-dimensional Hilbert spaces are isomorphic to $\mathbb{C}^n$; hence to every vector $|\psi\rangle^A=\sum_{v=0}^{|A|-1}a_v\,|v\rangle^A\in\mathcal{H}^A$ and $|\phi\rangle^B=\sum_{w=0}^{|B|-1}b_w\,|w\rangle^B\in\mathcal{H}^B$ a complex column vectors can be assigned as follows;

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{|A|-1} \end{pmatrix}, \qquad \mathbf{b} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{|B|-1} \end{pmatrix}. \tag{2.6}$$

Such that $a_v, b_w \in \mathbb{C}$.

The tensor product of vectors is $|\psi\rangle^A \otimes |\phi\rangle^B$ and corresponds to the column vector $\mathbf{a} \otimes \mathbf{b}$ ($\mathbf{a} \in \mathbb{C}^{|A|}$ and $\mathbf{b} \in \mathbb{C}^{|B|}$) given as follows:

$$\mathbf{a} \otimes \mathbf{b} = \begin{pmatrix} a_0\mathbf{b} \\ a_1\mathbf{b} \\ \vdots \\ a_{|A|-1}\mathbf{b} \end{pmatrix}. \tag{2.7}$$

Similarly proceeding to the Kronecker Tensor product of matrix, first consider two matrices $A \in \mathbb{C}^{n\times m}$ and $B \in \mathbb{C}^{n'\times m'}$ written as follows:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1m'} \\ b_{21} & b_{22} & \cdots & b_{2m'} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n'1} & b_{n'2} & \cdots & b_{n'm'} \end{pmatrix}. \tag{2.8}$$

The matrix corresponding to the Kronecker product $A \otimes B$ is computed as follows:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix} \in \mathbb{C}^{nn'\times mm'}. \tag{2.9}$$

Note that the outer-product of vectors in Hilbert space is an operator. More accurately,

for vector $|\psi\rangle^A$ the outer-product with itself is $|\psi\rangle\langle\psi| \in \mathfrak{B}(A)$ or $|\psi\rangle\langle\psi| \in \mathbb{C}^{|A|\times|A|}$. We already discussed that $\mathfrak{B}(A)$ is also a Hilbert space, the tensor product of $\mathfrak{B}(A)$ and $\mathfrak{B}(B)$ is given by the Kronecker tensor product of square matrices in $\mathbb{C}^{|A|\times|A|}$ and $\mathbb{C}^{|B|\times|B|}$. Generalized case for the Kronecker tensor product of rectangular matrices is shown above.

2.2 Quantum State

Unlike a classical system, a quantum system upon measurement of observable properties gives probabilistic outcome Ref. (Born, 1926). The Kronecker tensor product composition of probability vectors is also a probability vector representing joint probability distribution. However, direct sum composition of probability vectors in general is not a probability vector. For this particular reason, direct sum composition is not used to represent the joint system; hence we will compose the Hilbert spaces using the Kronecker tensor product.

First Postulate of Quantum Mechanics

Every physical system has an associated Hilbert space $\mathcal{H}$, and the system's state is assigned an operator $\psi \in \mathfrak{B}(\mathcal{H})$.

The postulate states that quantum system is ascribed a Hilbert space and complete information about it is stored in the state of the system. A state of system is a positive semi-definite, Hermitian operator with trace 1. For isolated system, state is a ray in the Hilbert space $e^{i\theta}|\psi\rangle$ where $\theta \in [0, 2\pi]$ is a global phase and $|\psi\rangle \in \mathcal{H}$. Global phase can be ignored. This postulate is radical in a sense that it implies the superposition of two quantum states is also a quantum state. For $c_1, c_2 \in \mathbb{C}$, $|\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}$ and $|c_1|^2 + |c_2|^2 = 1$, then a superposition of these states is

$$|\phi\rangle = c_1|\phi_1\rangle + c_2|\phi_2\rangle,$$

where $|\phi\rangle \in \mathcal{H}$. Consider that $|\phi_1\rangle, |\phi_2\rangle$ represents some property of the electron like location.

The double-slit experiment forces us to consider superposition of these two locations as a state too.

A quantum analogue of classical bit (Classical bit has two states 0 or 1) is called a qubit. An example of a qubit is spin of an electron having only two possible values up or down, which a two-dimensional Hilbert space can entirely describe. A three-level system is called qutrit, and if we generalize the notion to d-level system, it is called qudit, and a d-dimensional Hilbert space can be associated with it. An example of qudit is first d energy levels of hydrogen atom as its excited states are the possible d outcomes.

Second Postulate of Quantum Mechanics

A composite of two systems A and B with ascribed Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively is represented by the tensor product of these Hilbert spaces $\mathcal{H}^A \otimes \mathcal{H}^B$.

Consider the state of a physical system A as $|\phi^A\rangle$ and the state of some other physical system B represented as $|\psi^B\rangle$. These two systems can be spatially distant, but second postulate of quantum mechanics allows us to describe these two physical systems simultaneously by a state $|\phi^A\rangle \otimes |\phi^B\rangle$.

A composite system described in the second postulate can be in superposition state. Consider $|v_1\rangle^A, |v_2\rangle^A \in \mathcal{H}^A$ and $|w_1\rangle^B, |w_2\rangle^B \in \mathcal{H}^B$ be two orthonormal vectors describing states of corresponding physical system. Then the state $|\phi\rangle^{AB} \in \mathcal{H}^A \otimes \mathcal{H}^B$ can describe the composite state completely, where

$$|\phi\rangle^{AB} = \frac{1}{\sqrt{2}}\big(\,|v_1\rangle^A\,|w_1\rangle^B + |v_2\rangle^A\,|w_2\rangle^B\,\big)$$

All information cannot be extracted from individual systems. The only information we can infer from an individual system upon measurement is that if system A is in state $|v_1\rangle^A$, then system B will be in state $|w_1\rangle^B$. Likewise if A upon measurement gives us $|v_2\rangle^A$ then B is in state $|w_2\rangle^B$. This gives rise to a "non-local behaviour", according to which one system doesn't have a local description of the state of the system independent of the other one.

The concept of quantum state is already discussed (Definition 2.1.1). We will now dive deep into this concept and explore different types of quantum states. A pure state is described by a ray in Hilbert space $|\psi\rangle \in \mathcal{H}$ or by associated density matrix $|\psi\rangle\langle\psi|$. The density matrix associated with pure state is of rank one; hence pure states are projections onto one-dimensional sub-spaces of $\mathcal{H}$. Pure states form extreme points of the set of density operators, which is closed and convex. For normalized vectors $\{\phi_i\}_{i=1}^n$ with associated probabilities $\{p_i\}_{i=1}^n$ is called an ensemble of states. Quantum states for the ensemble $\{\phi_i, p_i\}$ is

$$\sigma = \sum_i^n p_i |\phi_i\rangle\langle\phi_i| ,$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. This is pure state decomposition of quantum state σ. Any density operator can be expressed as the convex combination of (not unique) pure state.

Pure State

Quantum state $\rho \in \mathfrak{D}(A)$ is said to be pure quantum state if

- $\text{Rank}(\rho) = 1$.
- $\text{Tr}[\rho^2] = \text{Tr}[\rho]$.

In general, quantum state does not need to be of rank one. Consider a small hypothetical experiment where we have an m faced dice, such that whenever the dice is rolled, the probability of x numbered side of dice to face up is p_x. We strategize that upon rolling a dice, based on the outcome x, a quantum state is prepared $|\psi_x\rangle\langle\psi_x|$. In other words the prepared quantum state $|\psi_x\rangle\langle\psi_x|$ has associated probability p_x. After preparing a state, we leave vicinity for some time to grab lunch. Upon return, we can not recall the value of x. Therefore, we end up with a probabilistic quantum state, which can be any state out of m possible states with a certain probability. As a consequence, we end up with the ensemble $\{|\psi_x\rangle\langle\psi_x| \ , \ p_x\}_{x=1}^m$ and the state that was prepared initially is one out of the m states from the ensemble. Such state is called a mixed quantum state.

Mixed State

A quantum state $\rho \in \mathfrak{D}(\mathcal{H})$ is mixed if it takes the form:

$$\rho = \sum_{x=1}^{m} p_x \left|\psi_x\right\rangle \left\langle\psi_x\right|, \tag{2.10}$$

where $\left|\psi_x\right\rangle \left\langle\psi_x\right| \in \mathfrak{D}(\mathcal{H})$, $\text{Rank}\Big(\left|\psi_x\right\rangle \left\langle\psi_x\right|\Big) = 1$, $\forall x \in \{1, 2, \cdots, m\}$, and $p_x \geq 0$, $\sum_{x=1}^{m} p_x = 1$.

The distribution $(1,\ 0,\ 0,\ \cdots)$ and all its permutations in the previous experiment again correspond to pure state. Another concept is covered under the label of quantum states, titled separable states.

Separable States

A bipartite quantum state $\sigma^{AB} \in \mathfrak{D}(AB)$ is separable, if

$$\sigma^{AB} = \sum_{x=1}^{m} p_x \gamma_x^A \otimes \rho_x^B, \tag{2.11}$$

where $\gamma_x^A \in \mathfrak{D}(A)$, $\rho_x^B \in \mathfrak{D}(B)$ $\forall x \in \{1, \cdots, m\}$ and $p_x \geq 0$, $\sum_{x=1}^{m} p_x = 1$.

In general, states γ_x^A and ρ_x^B can be mixed or pure states. If these states are mixed ρ^{AB} is called a mixed separable state, and if they are pure and $p^T = (1\ 0\ \cdots\ 0)$ or any permutation of this p, ρ^{AB} is a pure separable state. A quantum bipartite state is called a separable state (product state) if it can be written in the product form. Quantum bipartite states that can not be written as a product state and are not separable are entangled. An example of entangled state is Bell state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (Pure entangled state).

2.3 Quantum Measurement

As already discussed, each physical system has an associated Hilbert space and physical quantities to measure are represented by self-adjoint operators acting on the corresponding

Hilbert space, also referred to as observable. Examples of such observable are position, momentum, energy etc.

Third Postulate of Quantum Mechanics

A self-adjoint operator represents the observable of a physical system.

The measurement on finite-dimensional system $\mathcal{H}^A$ is a set of operators $\{\prod_i\}_{i=1}^n$ such that $\sum_{i=1}^n \prod_i = \mathrm{id}$. For every value of i there is a possible outcome of measurement. Let the initial state of the system be $\rho \in \mathfrak{D}(A)$, then the probability of observing each i is $p_i = \mathrm{Tr}[\rho \prod_i]$. Any such set $\{\prod_i\}_{i=1}^n$ is called a Positive Operator Valued Measure (POVM).

2.4 A Space of Linear Operators

We represent the set of all linear transformations from $\mathcal{H}^A$ to $\mathcal{H}^B$ as $\mathfrak{B}(A, B)$. In finite dimensions all linear transformations are bounded, hence same notation is used. In the context of this thesis, we are only concerned about finite-dimensional Hilbert spaces. The set $\mathfrak{B}(A, B)$ itself is a Hilbert space of linear operators and is isomorphic to $\mathbb{C}^{|A|\times|B|}$. Inner product map for this space is defined as follows;

$$\langle \mathcal{M}|\mathcal{N}\rangle := \mathrm{Tr}[\mathcal{M}^*\mathcal{N}],$$

where $\mathcal{M}, \mathcal{N} \in \mathfrak{B}(A, B)$. In general $|A| \neq |B|$, hence trace of $\mathcal{M}$ and $\mathcal{N}$ individually is not always well defined. All the elements of $\mathfrak{B}(A, B)$ can be written in terms of the standard basis of form $|x\rangle\langle y|$, where $|y\rangle \in \mathcal{H}^A$ and $|x\rangle \in \mathcal{H}^B$ such that $x = 1, \cdots, |B|$ and $y = 1, \cdots, |A|$. Important components of quantum mechanics like the quantum state, quantum measurement etc. are represented by Hermitian operators. The space of Hermitian operators is the vector space over the real numbers in $\mathfrak{B}(A, B)$. It can not be a vector space over complex numbers as;

$$(c\mathcal{M})^* = c^*\mathcal{M}^* = c^*\mathcal{M} \neq c\mathcal{M},$$

where $c \in \mathbb{C}$ and $\mathcal{M}$ is in vector space of Hermitian operators in $\mathfrak{B}(A, B)$. The vector space of Hermitian operators in $\mathfrak{B}(A, B)$ will be represented as $\text{Herm}(A, B)$ and $\text{Herm}(A, B) \subset \mathfrak{B}(A, B)$.

2.5 Quantum Channel

The evolution of the quantum system can be described in terms of quantum channels. Since a density matrix characterizes state of quantum system, so the evolution of this quantum system can be explained by a linear map $\mathcal{E}$ taking density operator to another density operator or, in other words, the transition from quantum states in $\mathfrak{D}(\mathcal{H}^A)$ to quantum state in $\mathfrak{D}(\mathcal{H}^B)$. The dimensionality of state can change when it undergoes evolution, which means that $|A|$ is not equal to $|B|$ in general.

Consider an experiment, a box full of balls with the number x imprinted on them is given. We are not allowed to peek inside the box when drawing a ball from it, but we know the probability of drawing each ball, which is p_x for ball with number x imprinted on it. Based on outcome a state ρ_x is prepared. The prepared state ρ_x can be converted into another by the evolution $\mathcal{E}(\rho_x)$. If we leave the lab for a day and come back the next day and have already forgotten what state was prepared, then we are left with state of form $\sum_x p_x \rho_x$. By applying the same logic state after evolution will be $\sum_x p_x \mathcal{E}(\rho_x)$. Therefore

$$\mathcal{E}\Big(\sum_x p_x \rho_x\Big) = \sum_x p_x \mathcal{E}(\rho_x). \tag{2.12}$$

The above mentioned equation implies that quantum channel or quantum evolution is a linear transformation and it can be extended to whole vector space $\mathfrak{B}(A)$ not just $\mathfrak{D}(A)$ ($\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$).

As already mentioned, that quantum channel takes density matrix to density matrix, so such evolution should preserve the mathematical structure of quantum states. As density matrices are Hermitian, a quantum channel is Hermitian preserving map. As in definition

2.1.1, it was mentioned that trace of a quantum state is equal to 1 to comply with the probabilistic nature of quantum system. Therefore quantum channel does not change the trace of a quantum state. In general, quantum channels are trace-preserving even when matrix it is acting on is not Hermitian.

One other inherent mathematical property of quantum state mentioned in definition 2.1.1 is positive semi-definiteness of associated matrix, and thus quantum evolution preserves the positive semi-definiteness—whence called positive maps.

Consider a composite of two systems A and B, which can be in the bipartite quantum state $\rho^{AB} \in \mathfrak{D}(\mathcal{H}^A \otimes \mathcal{H}^B)$. Now if subsystem B undergoes a quantum evolution $\mathcal{E} : \mathfrak{B}(B) \to \mathfrak{B}(C)$ and the other subsystem A does not change at all, then this process is described mathematically as

$$\tau^{AC} = \big(\mathrm{id}^{\mathrm{A}} \otimes \mathcal{E}\big)(\rho^{AB}). \tag{2.13}$$

Now $\mathrm{id}^{\mathrm{A}} \otimes \mathcal{E} : \mathfrak{B}(AB) \to \mathfrak{B}(AC)$ is physical evolution from density matrices to density matrices which means that $\mathrm{id}^{\mathrm{A}} \otimes \mathcal{E}$ should preserve positive semi-definiteness for any system A. There are examples of maps that themselves are positive but their composite with id^A is not positive. One famous example is transposition map $\mathcal{T} : \mathfrak{B}(A) \to \mathfrak{B}(A)$ defined as

$$\mathcal{T}(\rho) := \rho^T, \ \ \forall \rho \in \mathfrak{D}(A). \tag{2.14}$$

The transpose map preserves the eigenvalues; therefore is a trace-preserving positive map. Now consider a system in the state $\rho^{AB} = |\phi\rangle\langle\phi|$ where $|\phi\rangle = |00\rangle + |11\rangle$, matrix form of which can be written as follows:

$$\rho^{AB} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.15}$$

Taking transpose of subsystem B would give

$$\mathrm{id}^A \otimes \mathcal{T}(\rho^{AB}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.16}$$

It can easily be found that $\mathrm{id}^A \otimes \mathcal{T}(\rho^{AB})$ has one negative eigenvalue; thus is not positive semi-definite.

n-Positive Map

A bounded linear map $\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$ is n-positive if $(\mathrm{id}^n \otimes \mathcal{E})$ is positive, where $\mathrm{id}^n : \mathfrak{B}(\mathbb{C}^n) \to \mathfrak{B}(\mathbb{C}^n)$ is an identity map.

Completely Positive Map

A bounded linear map $\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$ is said to be completely positive if it is n-positive for all $n \geq 1$. The set of all completely positive maps from $\mathfrak{B}(A) \to \mathfrak{B}(B)$ is denoted $\mathrm{CP}(A \to B)$.

It is easy to see that, every map that is n-positive is also n_0-positive if $n_0 \leq n$. There exist some examples of bounded linear maps that are n-positive but not $(n+1)$-positive. Following is the list essential mathematical properties of a quantum channel:

1. It is linear.
2. It is trace-preserving (TP).
3. It is completely positive (CP).

Such maps are called CPTP maps. Complete positivity makes sense in a way that if a process is physical, we should be able to apply it on just one register of whole system and still have a valid state.

Dual or Adjoint of Linear Map

For a linear map $\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$, dual or adjoint map is $\mathcal{E}^* : \mathfrak{B}(B) \to \mathfrak{B}(A)$ such that

$$\mathrm{Tr}[\omega^* \mathcal{E}(\rho)] = \mathrm{Tr}\big[(\mathcal{E}^*(\omega))^* \rho\big] \quad \forall \rho \in \mathfrak{B}(A) \text{ and } \forall \omega \in \mathfrak{B}(B).$$

$\mathcal{E}$ is self-adjoint if $|A| = |B|$ and $\mathcal{E} = \mathcal{E}^*$.

List of properties of dual or adjoint of CPTP map is as follows:

- $\mathcal{E}$ is trace preserving iff its dual $\mathcal{E}^*$ is unital; i.e. $\mathcal{E}^*(\mathrm{id}^B) = \mathrm{id}^A$.
- $\mathcal{E}$ is positive iff its dual $\mathcal{E}^*$ is positive.
- $\mathcal{E}$ is completely positive iff its dual $\mathcal{E}^*$ is completely positive.

We now will present a representation of the quantum channels (quantum process) that will ameliorate our understanding of its properties.

2.5.1 Choi Representation

In this section, we discuss Choi-Jamiolkowski representation, also called Choi representation. This is an isomorphism from linear maps to matrices which allows us to interpret quantum channels as matrices. Properties of quantum channels in this representation are much easier to interpret. Let us start by recalling that a linear map $\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$ is completely positive if the map $\mathrm{id}^n \otimes \mathcal{E}$ is positive for all n. As already mentioned, Choi representation depicts complete positiveness of linear map in much simpler way. Positive semi-definite matrices in this representation can represent the quantum channels. Consequently, this representation of quantum channels is utilized to express particular optimization problem into semi-definite programming in many applications of quantum information science.

Choi Representation

The Choi matrix of a linear map $\mathcal{E} : \mathfrak{B}(A) \to \mathfrak{B}(B)$, is defined by the action of $\mathcal{E}$ on one register of maximally entangled state, represented as follows:

$$J_{\mathcal{E}}^{AB} = \mathrm{id}^{A} \otimes \mathcal{E}^{\tilde{A}\to B}(\phi_{+}^{A\tilde{A}}), \tag{2.17}$$

where $\phi_{+}^{\tilde{A}A} = \sum_{x,y\in[|A|]} |x^A x^{\tilde{A}}\rangle \langle y^A y^{\tilde{A}}|$ and $[|A|] = \{1, 2, \cdots, |A|\}$, thus

$$\mathcal{E}(\sigma) = \mathrm{Tr}_A[J_{\mathcal{E}}^{AB}((\sigma^A)^T \otimes I^B)].$$

$\mathrm{Tr}_A : \mathfrak{B}(AB) \to \mathfrak{B}(B)$ is a linear map that can be defined by its action on the basis of $\mathfrak{B}(AB)$ as follows:

$$\mathrm{Tr}_A[|x\rangle \langle x'|^A \otimes |y\rangle \langle y'|^B] = |y\rangle \langle y'|^B \mathrm{Tr}[|x\rangle \langle x'|^A] = |y\rangle \langle y'|^B \delta_{xx'}.$$

We dedicate this paragraph to understand that linear operators can be viewed as bipartite vectors. This concept will help understand the proofs given for Choi representation. Tilde notation ($\tilde{A}$) indicates the copy of A space thus, have same dimensionality. For two finite-dimensional Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$, tensor product Hilbert space $\mathcal{H}^A \otimes \mathcal{H}^B$ is (isometrically) isomorphic to Hilbert space of matrices $\mathbb{C}^{|A|\times|B|}$. Consider a bipartite vector $|\psi^{AB}\rangle \in \mathfrak{D}(AB)$ that can be expressed in terms of the orthonormal basis $|x^A\rangle \otimes |y^B\rangle$ as

$$|\psi^{AB}\rangle = \sum_{x=1}^{|A|} \sum_{y=1}^{|B|} m_{xy} |x^A\rangle \otimes |y^B\rangle, \tag{2.18}$$

where $m_{xy} \in \mathbb{C}$. $|x\rangle \in \mathcal{H}^A$ and $|y\rangle \in \mathcal{H}^B$. Let $M_\psi : \mathcal{H}^B \to \mathcal{H}^A$ be a linear operator and it operates on basis $|y^{\tilde{B}}\rangle$ as follows:

$$M_\psi |y^{\tilde{B}}\rangle = \sum_{x=1}^{|A|} m_{xy} |x^A\rangle.$$

Now bipartite vector $|\psi^{AB}\rangle$ can be expressed as

$$|\psi^{AB}\rangle = \sum_{y=1}^{|B|} M_\psi \, |y^{\tilde{B}}\rangle \otimes |y^B\rangle = M_\psi \otimes \mathrm{id}^B \, |\phi_+^{\tilde{B}B}\rangle \,, \tag{2.19}$$

where $|\phi_+^{\tilde{B}B}\rangle = \sum_{y=1}^{|B|} |y^{\tilde{B}} y^B\rangle$ is maximally entangled state. This representation of the bipartite vector will be used in the proofs of properties of Choi representation of CPTP map.

Theorem

A linear map $\mathcal{E} \in \mathfrak{B}(A) \to \mathfrak{B}(B)$ is completely positive if and only if

$$J_{\mathcal{E}}^{AB}(\phi_+^{\tilde{A}A}) = \mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A}) \geq 0.$$

Proof: If a linear map $\mathcal{E} \in \mathfrak{B}(A) \to \mathfrak{B}(B)$ is completely positive then $\mathrm{id} \otimes \mathcal{E}(\phi_+^{\tilde{A}A}) \geq 0$ by definition. For converse suppose that $\mathrm{id} \otimes \mathcal{E}(\phi_+^{\tilde{A}A}) \geq 0$ $|\psi^{BA}\rangle \in \mathbb{C}^B \otimes \mathbb{C}^A$ can be written as $M_\psi \otimes \mathrm{id}^A \, |\phi_+^{\tilde{A}A}\rangle$, where $|\phi_+^{\tilde{A}A}\rangle$ is maximally entangled state. M_ψ is linear operator $\mathcal{H}^{\tilde{A}} \to \mathcal{H}^B$.

$$\begin{aligned}(\mathrm{id}^B \otimes \mathcal{E})(|\psi^{BA}\rangle \langle\psi^{BA}|) &= (\mathrm{id}^B \otimes \mathcal{E})\Big((M_\psi \otimes \mathrm{id}^A) \, |\phi_+^{\tilde{A}A}\rangle \langle\phi_+^{\tilde{A}A}| \, (M_\psi^* \otimes \mathrm{id}^A)\Big), \\ &= (M_\psi \otimes \mathrm{id}^B)\Big((\mathrm{id}^A \otimes \mathcal{E}) \, |\phi_+^{\tilde{A}A}\rangle \langle\phi_+^{\tilde{A}A}| \, \Big)(M_\psi^* \otimes \mathrm{id}^B) \geq 0.\end{aligned} \tag{2.20}$$

Now, as we have proved it for an arbitrary pure state $|\psi^{BA}\rangle \in \mathbb{C}^B \otimes \mathbb{C}^A$ any quantum state can be expressed as ensemble of pure states (pure state decomposition), hence the converse is true for all quantum states. □

The Choi representation also characterizes the trace-preserving property of quantum channels, and the following theorem indicates this property.

Theorem

A linear map $\mathcal{E} \in \mathfrak{B}(A) \to \mathfrak{B}(B)$ is trace preserving if and only if

$$\mathrm{Tr}_B[\mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A})] = \mathrm{id}^A.$$

Proof: First suppose that $\mathcal{E}$ is trace preserving, then $J_{\mathcal{E}}^A = \mathrm{Tr}_B[J_{\mathcal{E}}^{AB}] = \mathrm{Tr}_B[\mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A})] = \mathrm{id}^A$ can be solved as follows:

$$\begin{aligned}\mathrm{Tr}_B[\mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A})] &= \sum_{x,y=1}^{|A|} |x\rangle\langle y|^A \mathrm{Tr}[\mathcal{E}(|x\rangle\langle y|^{\tilde{A}})] \\ &= \sum_{x,y=1}^{|A|} |x\rangle\langle y|^A \mathrm{Tr}[|x\rangle\langle y|^{\tilde{A}}] \\ &= \sum_{x,y=1}^{|A|} |x\rangle\langle y|^A \delta_{xy} = \mathrm{id}^A.\end{aligned} \tag{2.21}$$

To prove converse, suppose $J_{\mathcal{E}}^A = \mathrm{Tr}_B[J_{\mathcal{E}}^{AB}] = \mathrm{id}^A$, then for quantum state $\sigma \in \mathfrak{D}(A)$,

$$\begin{aligned}\mathrm{Tr}[\mathcal{E}(\sigma^A)] &= \mathrm{Tr}[\mathrm{id}^A \otimes \mathcal{E}((\sigma^A)^T \otimes \mathrm{id}^{\tilde{A}})] \\ &= \mathrm{Tr}[J_{\mathcal{E}}^{AB}((\sigma^A)^T \otimes \mathrm{id}^{\tilde{A}})] \\ &= \mathrm{Tr}[J_{\mathcal{E}}^A(\sigma^A)^T] \\ &= \mathrm{Tr}[(\sigma^A)^T] \\ &= \mathrm{Tr}[\sigma^A]. \qquad \square\end{aligned} \tag{2.22}$$

The theorems proved above characterized quantum channels completely. A linear map $\mathcal{E} \in \mathfrak{B}(A) \to \mathfrak{B}(B)$ is a quantum channel if and only if $\mathrm{Tr}_B[\mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A})] = \mathrm{id}^A$ and $\mathrm{id}^A \otimes \mathcal{E}(\phi_+^{\tilde{A}A}) \geq 0$.

Other representations of quantum channels like Kraus representation and Stinespring representation hold significant importance, but they are not reported here, for they have no direct consequences for the rest of the thesis.

2.6 Resource Theory

Resource theory is an intuitive and versatile framework that revolutionized the problem-solving approach in quantum physics. To comprehend the intuitive aspect of this framework, an application is presented in this section. Following applications will also provide insight

into the versatility and strength of the resource theoretic approach. Electricity is a basic need in this new world of 21th century. Every building has an extensive, meticulously laid out map of wires to make electricity available for all equipment in use. If there is any malfunction, the electrician is called in to make the fix. Electrician's own abilities (like physical movements, thinking, knowledge to analyze the problem) and a limited kit of tools are readily available to be used (free). If the problem is complex, an advanced tool might be required to fix it. Electrician then has to put in extra effort (cost etc.) to acquire that tool. Such devices necessary to perform the task at hand but extremely rare or hard to obtain will be the most valuable (resource). There can be other equipment, difficult to acquire (microscope etc.), but does not play any role in performing the required task is resource with zero significance. Likewise, all scenarios in nature can be looked upon from this perspective.

The strength of resource theoretic framework in quantum information resides in the natural approach for studying quantum physical phenomenon: instead of specifying the actual details of the mechanics implementing transformation between two quantum states, this aims to study the inter-convertibility conditions between states, namely when (and not how) a state can be transitioned into another.

We will now proceed to formal definition of quantum resource theories supported with an example.

2.6.1 Quantum Resource Theory

As discussed earlier, possible operations and states in the quantum realm are phenomena at the atomic and sub-atomic levels. Entangled states are a significant consumable resource for tasks like teleportation, dense-coding etc. Quantum entangled states are difficult to prepare; associated difficulties and cost regarding its preparation make it a valuable resource. Free operations like classical communication (telephonic communication) and local operations (LOCC) can not create an entangled state. Consequently, it is intuitive to take quantum entanglement as a resource, and indeed it was the first quantum resource to be studied

extensively Ref. (R. Horodecki et al., 2009). An example of a state that cannot be prepared by LOCC is Bell state $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ (entangled state). It is discussed here to present an application of this framework in quantum realm.

Several quantum resource theories (QRTs) were introduced over the past decade Refs. (Gour and Spekkens, 2008; M. Horodecki, K. Horodecki, et al., 2003; M. Horodecki, P. Horodecki, et al., 2005; Oppenheim et al., 2002). The formal and precise mathematical definition of QRTs was provided in Refs. (Chitambar and Gour, 2019; Gour and Scandolo, 2020). QRTs are usually distinguished into two categories depending on the nature of the object of interest, whether static or dynamic. For the scope of this thesis, we confine our attention to only static QRTs.

Static Quantum Resource Theories

Let $\mathfrak{F}(A \to B) \subset \mathrm{CPTP}(A \to B)$ be a set of linear transformation from physical systems A to B, with corresponding associated Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively. $\mathfrak{F}$ is said to specify a static resource theory if following statements holds;

- For every physical system A, $\mathfrak{F}(A \to A)$ contains id^A.
- For physical systems A, B and C, $\mathcal{M} \in \mathfrak{F}(A \to B)$ and $\mathcal{N} \in \mathfrak{F}(B \to C)$, then $\mathcal{M} \circ \mathcal{N} \in \mathfrak{F}(A \to C)$.

$\mathfrak{F}(A) := \mathfrak{F}(1 \to A) \subset \mathfrak{D}(A)$ is induced mapping on Hilbert space $\mathcal{H}^A$, where 1 represents the trivial system. $\mathfrak{F}(A)$ is the set of free states (channel with trivial input).

The first statement translates a natural concept that doing nothing should be free in mathematical terms. The second statement signifies that free static operations can be applied in any sequence and any number of times. The set of free static states is $\mathfrak{F}(1 \to A)$ and $\mathfrak{D}(A) \backslash \mathfrak{F}(1 \to A)$ is the set of static resource states. Preparation of free state is also a free operation.

2.6.2 Tensor Structure in Quantum Resource Theories

The definition in the previous section presents minimal vital mathematical structure exhibited by QRTs; practically, we might desire for some more natural and convenient structures to exist in QRTs. QRTs discussed in this thesis have tensor product structure, elaborated in Ref. (Chitambar and Gour, 2019).

Tensor-Product Structure

A quantum resource theory is said to admit tensor product structure if it satisfies the following conditions;

- The free operations in QRTs are "completely free". Let three physical systems A, B, and C, if $\mathcal{M} \in \mathfrak{F}(A \to B)$ then $\mathrm{id}^C \otimes \mathcal{M} \in \mathfrak{F}(CA \to CB)$, where id^C is the identity map on $\mathfrak{B}(C)$.
- Discarding physical system (taking trace of physical system) should be free, means $\mathfrak{F}(A \to \mathbb{R})$ is not empty.
- Appending the physical system is also a free operation means for any free state ρ in $\mathfrak{D}(A)$, CPTP map $\mathcal{M}_\sigma(\rho) = \rho \otimes \sigma$ belongs to the set $\mathfrak{F}(A \to AB)$ for σ in $\mathfrak{D}(B)$.

The first condition is similar to notion of complete positivity; if a linear map is free, applying it to just one subsystem of a joint system should also be free. Such maps are called completely free. This condition also implies that parallel or tensor composition of free operations is also free.

There are many significant consequences of the aforementioned conditions. Condition three stimulates that creation of free state is a free operation. Similarly, condition two indicates that partial trace is free. Tensor product composition of free states is also a free state.

2.6.3 Convex Quantum Resource Theory

Identification of convex structure in Quantum resource theories is mathematically very convenient, allowing the use of powerful convex optimization tools. Convexity in QRTs implies that the set of free quantum operations is convex: for $\mathcal{M}, \mathcal{N} \in \mathfrak{F}(A \to B)$, $p\mathcal{M} + (1-p)\mathcal{N} \in \mathfrak{F}(A \to B)$ such that $p \in [0, 1]$. Set of free quantum states is a special case of free quantum operations; consequently, a convex set of free operations implies the convexity of the set of free states. The converse, in general, is not true. Many famous QRTs like quantum resource theory of entanglement, quantum resource theory of athermality etc., exhibit convex structure.

Even though convexity is a mathematically convenient structure, it is not always present. An example of non-convex resource theory is presented in Ref. (Chitambar and Gour, 2019) it is the QRT of total correlation. In the QRT of total correlation, classical communication is prohibited due to certain restrictions. So only allowed operations are local ones; hence, elements of a set of free operations are of the form $\mathcal{M} \otimes \mathcal{N}$, tensor product of CPTP maps $\mathcal{M}$ and $\mathcal{N}$. The objects of theory are bipartite tensor product states of form $\rho \otimes \sigma$. Resource states are bipartite states containing either classical or quantum correlation. In this case, set of free states and free operations are not convex (As $p(\rho_1 \otimes \sigma_1) + (1-p)(\rho_2 \otimes \sigma_2)$ is not a free state even if $\rho_1 \otimes \sigma_1$ and $\rho_2 \otimes \sigma_2$ are free).

2.6.4 Resource Quantifiers

As discussed earlier, some states are easily accessible and abundant; hence are free. Rare ones are valuable. This framework induces a hierarchy of states. Mathematically, this hierarchy is translated into a partial preorder induced by channels easy to implement in particular settings (free operations). A state is considered more valuable compared to another if the former can produce a larger set of states via free operations. This gives rise to a need of quantifiers of resourcefulness of states consistent with the hierarchy. Real valued functions that quantify quantum states are called resource monotones. Extensive study

about calculation and characterization of resource quantifiers in general QRTs was done in Ref. (Bromley et al., 2018; Liu, Hu, and Lloyd, 2017; Regula, 2017). Essential properties of resource measures are reviewed in the following section.

Resource quantifiers should be able to measure the resourcefulness of quantum states or density matrices. So they should be functions that take density matrices to non-negative real numbers $f : \cup\mathfrak{D}(\mathcal{H}) \to \mathbb{R}_{\geq 0}$, with the following properties;

- **Zero for Free State:**

  Intuitively, free states have zero resourcefulness; hence the resource quantifiers should assign a zero value to such states.

  $$f(\rho) = 0,$$

  where ρ is a free state. If converse is valid for this statement, then is called faithful. However, it is not always true; sometimes, resource states do not provide any operational benefit compared to the free states for a given task. This property has been discussed in detail with an example in Ref. (Chitambar and Gour, 2019) of distillable entanglement which is a measure of entanglement; it vanishes for bound entangled states.

- **Monotonicity:**

  Another intuitive property of resource quantifiers is that resourcefulness of any physical system cannot increase by application of free operations. The monotonicity captures this aspect. If one state ρ^A can be converted into another σ^B via free operation $\mathcal{M} \in \mathfrak{F}(A \to B)$, $\sigma^B = \mathcal{M}(\rho^A)$ then resource monotone is a function $f : \cup\mathfrak{D}(\mathcal{H}) \to \mathbb{R}_{\geq 0}$, such that

  $$f(\rho^A) \geq f\big(\mathcal{M}(\rho^A)\big).$$

  If both ρ^A and σ^B are free states then the first property implies that $f(\rho^A) = f(\sigma^B) = 0$.

2.6.5 Witness-based Quantifiers

Now we are going to discuss generalized tool to measure resource, based on the idea of resource witnessing. In QRTs witness-based quantifiers are defined as follows,

Resource Witness

A quantum observable $W \in \mathfrak{B}(\mathcal{H})$ is called a resource witness such that

$$\begin{aligned} \exists \rho \notin \mathfrak{F}(\mathcal{H}): \quad & \mathrm{Tr}[W\rho] < 0 \\ \exists \tau \in \mathfrak{F}(\mathcal{H}): \quad & \mathrm{Tr}[W\tau] \geq 0 \end{aligned} \tag{2.23}$$

A quantum observable that satisfies the aforementioned conditions is said to witness the resourcefulness of state ρ.

In Ref. (Barvinok, 2002) it was presented that for every convex closed QRTs, the separating hyperplane theorem ensures the existence of at least one witness for every resource state. A separating hyperplane can be drawn for any state that is not the member of convex set of free states which can serve as witness for the resourcefulness of the state.

2.7 Notation

We represent quantum system by A, B, C, and classical system as X, Y, Z, etc. Quantum states, are represented by lower case Greek letters ρ, σ, τ etc. Elements of classical systems will be represented by lower case alphabets a, b, c etc. Solid line will represent the quantum system in figures, and double line will denote the classical system. The notation $\mathcal{H}^A$ is utilized for Hilbert space of quantum system A with dimensions $|A|$. The set of bounded operators that take system A to B will be denoted as $\mathfrak{B}(A, B)$. The set of density operators acting on Hilbert space $\mathcal{H}^A$ is represented as $\mathfrak{D}(A)$. CPTP$(A \to B)$ or CPTP(A, B) is the set of quantum channels (completely positive trace-preserving linear maps from $\mathfrak{B}(A)$ to $\mathfrak{B}(B)$). Scripted letters are used to denote quantum channels, i.e., $\mathcal{E}$, $\mathcal{N}$ etc.

Chapter 3

Convex Analysis

This chapter will cover all minimal necessary definitions and convex analysis background needed to understand the contents of thesis. We will confine our attention to the finite-dimensional case. The author has consulted book Ref. (Boyd and Vandenberghe, 2004) and Ref. (Girard, 2017) for the subject material of this chapter.

3.1 Convex functions and sets

We start by presenting necessary and fundamental definitions. An inner product space is a vector space V over a field $\mathbb{F}$ with an additional structure of inner product map, i.e. $\langle \cdot | \cdot \rangle : V \times V \to \mathbb{F}$; it is also called Euclidean space (finite dimensional space).

Convex Set

Let $u, v \in W$, then the set W is a convex set if $\omega_\lambda \in W$; where,

$$\omega_\lambda := \{\lambda u + (1-\lambda)v, 0 \leq \lambda \leq 1\}. \tag{3.1}$$

A famous example of convex set is $\mathbb{R}$: the definition of convex set implies that all points of the line segment that joins two points in $\mathbb{R}$ are also in $\mathbb{R}$. The empty set is considered to be convex by convention.

Following are some of the operations that preserve convexity:

1. Intersection ($\cap_{i=1}^{n} U_i$) of any number of convex sets $\{U_i\}_{i=1}^{n}$ is convex.

2. The vector sum of convex sets is convex. (Let U_1 and U_2 be two convex sets then the vector sum of these two sets is $U_1 + U_2 = \{x + y | x \in U_1 \text{ and } y \in U_2\}$.)

3. The set obtained by taking product of a convex set with a scalar is convex. (Let a convex set U, and $\lambda \in \mathbb{R}$ then λU is also convex, moreover if U_1 and U_2 are convex sets and λ_1 and λ_2 are positive scalars then $\lambda_1 U_1 + \lambda_2 U_2$ is also convex.)

4. The interior and closure of convex set are convex.

Some more definitions of frequently used convex sets are discussed now.

- **Hyperplane:** A hyperplane X can be written as a single linear equation of form

$$X := \Big\{ \mathbf{x} | \sum_i a_i x_i = b, i = 1, 2, \cdots \Big\}, \tag{3.2}$$

  where $x_i \in \mathbb{R}$ are the elements of the vector $\mathbf{x}$, $\mathbf{a}$ is non-zero vector with components $a_i \in \mathbb{R}$ and b is scalar.

- **Halfspace:** A halfspace X can be written as a single linear inequality of form

$$X := \Big\{ \mathbf{x} | \sum_i a_i x_i \leq b, i = 1, 2, \cdots \Big\}, \tag{3.3}$$

  where $x_i \in \mathbb{R}$ are elements of vector $\mathbf{x}$, $\mathbf{a}$ is non-zero vector with components $a_i \in \mathbb{R}$ and b is scalar.

- **Affine Set:** Let $u, v \in W'$, then the set W' is said to be affine if $tu + (1-t)v \in W'$ for $t \in \mathbb{R}$.

- **Cone:** A set U is said to be a cone if for all $x \in U$ and $\lambda \geq 0$, $\lambda x \in U$. In general cone need not be convex.

- **Convex Cone:** The convex cone U' is a cone as well as a convex set such that for all $x_1, x_2 \in U'$ and $\lambda_1, \lambda_2 \geq 0$, $\lambda_1 x_1 + \lambda_2 x_2 \in U'$. We are only concerned about convex cones for the scope of this thesis so we will be using convex cone and cone interchangeably to mean convex cone.

- **Affine Hull:** Affine hull of set U is the set of all possible affine combinations (Affine combination of $x_1, x_2, \cdots, x_n$ is a linear combination $\sum_{i=1}^{n} \alpha_i x_i = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ such that $\sum_{i=1}^{n} \alpha_i = 1$.) of elements in set U and is represented as

$$\text{aff}(U) := \Big\{ \sum_i t_i x_i | x_i \in U \text{ and } t_i \in \mathbb{R},\ i = 1, 2, \cdots,\ \sum_i t_i = 1 \Big\}. \tag{3.4}$$

- **Convex Hull:** Convex hull of set U is the set of all possible convex combinations (Convex combination of $x_1, x_2, \cdots, x_n$ is a linear combination $\sum_{i=1}^{n} \alpha_i x_i = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ such that $\sum_{i=1}^{n} \alpha_i = 1$ and $\alpha_i \geq 0$.) of elements in set U and is represented as

$$\text{convx}(U) := \Big\{ \sum_i t_i x_i | x_i \in U \text{ and } t_i \in \mathbb{R}_+,\ i = 1, 2, \cdots,\ \sum_i t_i = 1 \Big\}. \tag{3.5}$$

- **Interior of Set:** Interior of set U is the set of all points x such that there exist a ball $B = \{y \in U | \|x - y\| < \epsilon, \epsilon > 0\}$, centered at x, which is all contained in U.

$$\text{int}(U) := \{x \in U | B \subseteq U\}. \tag{3.6}$$

- **Closure of Set:** Closure of set U is

$$\text{cl}(U) := \{y \in V | \forall \epsilon > 0, \exists x \in U, \|y - x\| < \epsilon\}, \tag{3.7}$$

where V is an inner product space over the field $\mathbb{F}$.

Consider an example that $U \subset \mathbb{R}$ is a line segment between two distinct points, then the affine hull of this set will be the line containing this line segment.

Note that a set U is convex when $\text{convx}(U) = U$. In the previous example, as the set (line segment) is convex, it is a convex hull of itself.

3.1.1 Convex functions

We start this section by defining real-valued convex functions.

Convex Function

Let $U \subseteq \mathbb{R}^n$ be a convex set. We say that a function $f : U \to \mathbb{R}$ is convex if

$$f(ax + (1-a)y) \leq af(x) + (1-a)f(y) \quad \forall x, y \in U \text{ and } a \in [0,1]. \tag{3.8}$$

Note that for the convexity of a function $f : U \to \mathbb{R}$, the convexity of domain is prerequisite. Hence, when we state that a function is convex, we also imply that the function's domain is convex. A function $f : U \to \mathbb{R}$ is strictly convex if the inequality in the definition of convex function is strict for $x, y \in U$, $x \neq y$ and $a \in (0,1)$. A function $f : U \to \mathbb{R}$ is concave if $(-f)$ is convex. A norm is an example of convex function as triangular inequality gives us convexity;

$$\|ax + (1-a)y\| \leq a\|x\| + (1-a)\|y\| \quad \forall x, y \in \mathbb{R}^n \text{ and } a \in [0,1]. \tag{3.9}$$

If we have convex functions, like some affine (An affine function is a linear function + constant and its graph is a straight line.) and norm function, then we can create new convex functions from these by applying certain operations that preserve convexity. Examples of these operations are as follows:

1. Addition of convex functions is convex. Multiplying convex function with a non-negative scalar preserves convexity.

2. Taking the point-wise supremum of function $f(x, y)$ convex in x for each $y \in \mathcal{C}$ denoted as $\sup_{y\in\mathcal{C}} f(x, y)$ is convex. An example is the support function of some set $\mathcal{C}$, $\text{supp}_{\mathcal{C}}(x) = \sup_{y\in\mathcal{C}} y^T x$ is convex.

3. Composition of $f : \mathbb{R}^n \to \mathbb{R}$ with scalar function (Scalar function is a function in one or more variable with one-dimensional range) $g : \mathbb{R} \to \mathbb{R}$ represented as $g \circ f(x) = g(f(x))$ is convex when g is convex and f is convex or f is concave and g is convex non-increasing function. Example of this composition is $\frac{1}{f(x)}$, which is convex when $f(x)$ is concave and positive.

Some other operations preserve convexity of functions too, but those are not required in context of this thesis.

To identify the convexity of function, some set of criteria are presented. Let $f : U \to \mathbb{R}$ be a differentiable function, where $U \subset \mathbb{R}^n$. This function is convex if and only if U is a convex set and

$$f(x) - f(y) \geq \nabla f(y)(x - y) \quad \forall x, y \in U. \tag{3.10}$$

First order Taylor approximation of function f is $h(x) = \nabla f(y)(x - y) + f(y)$ near y. This first order Taylor approximation according to Eq. (3.10) gives a global lower-bound of function f. Conversely, if first order Taylor approximation is a global lower-bound then function is convex. f is strictly convex if strict inequality holds in the equation above for $x \neq y$.

If a function is twice differentiable then the second derivative test can be used to find if the function is convex or not. For the non-empty convex set $U \subset \mathbb{R}^n$, the twice differentiable function $f : U \to \mathbb{R}$ is convex if and only if U is a convex set and

$$\nabla^2 f(x) \geq 0.$$

Or more precisely

1. The function is convex if $\nabla^2 f(x)$ is positive semi-definite for $x \in U$.

2. The function is strictly convex if $\nabla^2 f(x)$ is positive definite for $x \in U$.

3.2 Supporting and separating hyperplane

We present versions of supporting and separating hyperplane theorems used in this thesis to prove results.

Consider two disjoint ($U_1 \cap U_2 = \emptyset$) convex sets U_2 and U_1. These two sets can be separated via hyperplane $H = \{\mathbf{x}|\mathbf{a}^T\mathbf{x} = b\}$ where $\mathbf{a} \in \mathbb{R}^n$ and $b \in \mathbb{R}$, such that each of the sets lies in different halfspace formed by this hyperplane; hence,

$$\langle a|x_1\rangle < b \leq \langle a|x_2\rangle \quad \forall x_1 \in U_1,\ \forall x_2 \in U_2,\ b \in \mathbb{R}. \tag{3.11}$$

Or

$$\langle a|x_2\rangle < b \leq \langle a|x_1\rangle \quad \forall x_1 \in U_1,\ \forall x_2 \in U_2,\ b \in \mathbb{R}. \tag{3.12}$$

If x' belongs to the boundary of U (convex set), a hyperplane separating x' from int(U) can be constructed which inherently passes through x'. That means there exists $\mathbf{a} \neq 0$, such that

$$\langle a|x'\rangle \leq \langle a|x\rangle \quad \forall x \in U. \tag{3.13}$$

Supporting hyperplane theorem is a special case of separating hyperplane theorem. A supporting hyperplane can be imagined as any hyperplane that touches U.

Separating Hyperplane Theorem

Consider two convex sets U_1 and U_2 subset of $\mathbb{R}^n$. If U_1 and U_2 are disjoint then there exists a hyperplane that can separate these two sets. There exists a vector $\mathbf{a} \neq 0$ such that

$$\langle a|x_1\rangle < b \leq \langle a|x_2\rangle \quad \forall x_1 \in U_1,\ \forall x_2 \in U_2,\ b \in \mathbb{R}. \tag{3.14}$$

A hyperplane is an affine set, and separating hyperplane theorem states that a hyperplane can separate the point x_2 from convex set U_1 if x_2 is not in U_1. If U_1 is a cone then we can take $b = 0$. Since it indicates non-membership of x_2 in U_1, it can be regarded as a resource witness; hence, separating hyperplane theorem ensures the existence of at least one witness for every resource state. A separating hyperplane can be drawn for any state that is not the member of convex set of free states which can serve as witness for the resourcefulness of the state. If U_1 is a cone, we may take b to be zero.

Supporting Hyperplane Theorem

Let U be a non-empty convex set, subset of $\mathbb{R}^n$ and x' be a non-interior point of U. There exists a hyperplane that passes through x', such that U is fully contained in one of the half-spaces, i.e there exists a vector $\mathbf{a} \neq 0$;

$$\langle a|x'\rangle \leq \langle a|x\rangle \quad \forall x \in U. \tag{3.15}$$

3.3 Conic programming

We already discussed definitions of cone, convex cone and convex hull etc. Here will be discussing some more definitions in addition to the ones mentioned earlier.

Dual Cone

For a cone $\mathcal{K} \subset \mathcal{H}$, dual cone is a set,

$$\mathcal{K}^* = \{y | x \in \mathcal{K}, \langle x|y\rangle \geq 0\}. \tag{3.16}$$

Cone is said to be self-dual if $\mathcal{K} = \mathcal{K}^*$.

Dual cone is also a cone, to prove this we need to prove that $\alpha y \in \mathcal{K}^*$ for $y \in \mathcal{K}^*$ and $\alpha > 0$. This is equivalent to $\langle x|\alpha y\rangle = \alpha \langle x|y\rangle \geq 0$ for $x \in \mathcal{K}$, which is true as $\alpha > 0$ and $\langle x|y\rangle \geq 0$, hence dual cone is also a cone.

Conic Hull

For any $U \subset \mathcal{H}$, conic hull of set U is

$$\text{cone}(U) = \Big\{ \sum_i t_i x_i | \forall x_i \in U, \forall t_i \in \mathbb{R}_+, i = 1, 2, \cdots \Big\}. \tag{3.17}$$

Conic hull is a convex set.

An example of a convex cone is first quadrant in $\mathbb{R}^2$; it is self-dual as well. The entire Hilbert space is also an example of convex cone, and the dual cone of the entire Hilbert space is the origin or zero vector or matrix.

Let us now discuss some properties of a convex cone. If $\mathcal{K}$ is a closed convex cone then taking the dual of this set twice will give the closed convex cone itself; $\mathcal{K} = \mathcal{K}^{**}$. Operations that preserve convexity can be used to conclude that for two closed convex cones $\mathcal{K}_1$ and $\mathcal{K}_2$, their vector sum $(\mathcal{K}_1 + \mathcal{K}_2)$ is also a closed convex cone. Consider $\mathcal{K}_1$ and $\mathcal{K}_2$ be two closed convex cones, then following holds;

$$(\mathcal{K}_1 + \mathcal{K}_2)^* = \mathcal{K}_1^* \cap \mathcal{K}_2^* \quad \text{and} \quad (\mathcal{K}_1 \cap \mathcal{K}_2)^* = \mathcal{K}_1^* + \mathcal{K}_2^*. \tag{3.18}$$

Familiarity with the cone's interior is important in determining duality properties of closed convex cone. The interior of a closed convex cone is defined as follows:

Interior of Dual Cone

For a closed convex cone $\mathcal{K}$ subset of a real Euclidean space V, the interior of $\mathcal{K}^*$ is

$$\text{int}(\mathcal{K}^*) = \{x \in V | \langle x|y\rangle > 0, \forall y \in \mathcal{K}, y \neq 0\}. \tag{3.19}$$

The most commonly discussed cone in quantum information is the cone of positive semi-definite hermitian operators on a Hilbert space $\mathcal{H}$ represented as $\text{Herm}(\mathcal{H})_+$, a subset of the Hilbert space of hermitian operators. This closed convex cone of positive semi-definite matrices is self-dual, and the interior of this cone is

$$\text{int}(\text{Herm}(\mathcal{H})_+) = \{X \in \text{Herm}(\mathcal{H}) | X > 0\}, \tag{3.20}$$

which is the cone of positive definite operators.

In convex analysis, there are several tools to solve for optimal values of optimization problems. Conic optimization is a sub-field of convex optimization, which deals with minimization or maximization of convex functions over the intersection of convex cones and affine sets. Conic programming is normally used to solve such conic optimization problem. Conic optimization includes the most famous class of convex optimization problems like linear programming and semi-definite programming.

For this thesis, it is sufficient to consider only conic programs defined over the space of a Hermitian operators over Hilbert space ($\text{Herm}(\mathcal{H})$). The space of Hermitian operators on a Hilbert space $\mathcal{H}$ is equipped with Hilbert-Schmidt inner product

$$\langle M|N\rangle := \text{Tr}[M^*N] \quad \forall M, N \in \text{Herm}(\mathcal{H}). \tag{3.21}$$

Consider two Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ with dimensions $|A|$ and $|B|$ respectively and cones $\mathcal{K}_1 \subseteq \text{Herm}(\mathcal{H}^A)$ and $\mathcal{K}_2 \subseteq \text{Herm}(\mathcal{H}^B)$, and two fixed hermitian matrices $H_1 \in \text{Herm}(\mathcal{H}^A)$ and $H_2 \in \text{Herm}(\mathcal{H}^B)$. Let $\mathcal{N} : \text{Herm}(\mathcal{H}^A) \to \text{Herm}(\mathcal{H}^B)$ be a hermiticity-

preserving linear map, then a conic linear program is denoted by the ordered set $(\mathcal{N}, H_1, H_2, \mathcal{K})$. Such conic program has the following associated optimization primal problem:

$$\begin{aligned}
&\alpha := \inf \mathrm{Tr}[XH_1]. \\
&\text{Subject to :} \\
&X \in \mathcal{K}, \\
&\mathcal{N}(X) = H_2.
\end{aligned}$$

Corresponding dual problem is:

$$\begin{aligned}
&\beta := \sup \mathrm{Tr}[YH_2]. \\
&\text{Subject to :} \\
&Y \in \mathrm{Herm}(\mathcal{H}^B), \\
&H_1 - \mathcal{N}^*(Y) \in \mathcal{K}^*,
\end{aligned}$$

where $\mathcal{K}^* = \{W \in \mathrm{Herm}(A) | \mathrm{Tr}[W^*M] \geq 0, M \in \mathcal{K}\}$ is the dual cone. The primal feasible set $\mathcal{A} \subset \mathrm{Herm}(\mathcal{H}^A)$ and dual feasible set $\mathcal{B} \subset \mathrm{Herm}(\mathcal{H}^B)$ of the above mentioned conic linear program are

$$\begin{aligned}
\mathcal{A} &:= \{X \in \mathcal{K} | \mathcal{N}(X) = H_2\}. \\
\mathcal{B} &:= \{Y \in \mathrm{Herm}(\mathcal{H}^B) | H_1 - \mathcal{N}^*(Y)\}.
\end{aligned} \tag{3.22}$$

Elements $X \in \mathcal{A}$ and $Y \in \mathcal{B}$ are called primal feasible plan and dual feasible plan, respectively. Feasible region is the region of vectors that satisfies all the constrains of primal or dual problem based on which it is called primal or dual feasible plan. A conic optimization problem is primal feasible if the primal feasible set is non-empty and dual feasible if the dual feasible set is non-empty.

The values α and β in primal and dual problems are called primal and dual optimal

values respectively

$$\begin{aligned} \alpha &= \{\inf \mathrm{Tr}[AH_1] \,|X \in \mathcal{A}\}. \\ \beta &= \{\sup \mathrm{Tr}[YH_2] \,|Y \in \mathcal{B}\}. \end{aligned} \tag{3.23}$$

The advantage of writing dual of optimization problem is that sometimes dual problem is much easier to solve compared to primal problem. Weak duality theorem states that dual optimal value provides lower bound for the primal optimal value, $\mathrm{Tr}[XH_1] \geq \alpha \geq \beta \geq \mathrm{Tr}[YH_2]$. For any conic program, weak duality always holds.

$$\begin{aligned} \langle H_2|Y\rangle &= \langle \mathcal{N}(X)|Y\rangle, \\ &= \langle \mathcal{N}^*(Y)|X\rangle, \\ &= -\big(\langle X|H_1 - \mathcal{N}^*(Y)\rangle\big) + \langle X|H_1\rangle, \\ &\leq \langle X|H_1\rangle, \end{aligned} \tag{3.24}$$

where $\langle X|H_1 - \mathcal{N}^*(Y)\rangle \geq 0$ follows from $H_1 - \mathcal{N}^*(Y) \in \mathcal{K}^*$.

As already mentioned, weak duality always exists, but sometimes in applications, especially in quantum information, the primal optimal value is equal to the dual optimal value. Whenever this is true, we say strong duality holds, $\alpha = \beta$. Unlike linear programming, strong duality does not always hold in conic programming.

Now we are going to discuss sufficient conditions for strong duality to hold. Consider a conic program $(\mathcal{N}, H_1, H_2, \mathcal{K})$, the primal problem is strictly feasible if primal feasible plan X lies in the interior of cone $\mathcal{K}$ ($\mathcal{A} \cap \mathrm{int}(\mathcal{K}) \neq \varnothing$). Similarly, dual problem is strictly feasible if there exist a dual feasible plan Y when $H_1 - \mathcal{N}^*(Y)$ lies in the interior of cone $\mathcal{K}^*$ i.e. $(H_1 - \mathcal{N}^*(Y)) \cap \mathrm{int}(\mathcal{K}^*) \neq \varnothing$. If primal and dual plan both are feasible and one of these is strictly feasible then strong duality holds.

In upcoming chapters, we will see that problems we solved can be expressed in conic linear programming form. It will become evident that conic linear programming can assist

in solving problems of state conversion in quantum information.

Chapter 4

Complete Characterization of Static-Resources

A fundamental problem studied in quantum resource theories is inter-convertibility of states. In several scenarios, it has already been extensively studied: for the case of pure state entanglement theory, convertibility conditions of states were introduced in Ref. (Nielsen, 1999). Similarly, families of monotones that give transition conditions for states in different cases are discussed in Refs. (Gour, 2017; Liu, Bu, and Takagi, 2019; Gour, 2019; Chitambar, Vicente, et al., 2020; Takagi and Regula, 2019). This chapter introduces a complete family of conversion resource monotones for generic static convex quantum resource theories. A more generalized proof of this theorem for dynamical resource theories is provided in Ref. (Gour and Scandolo, 2020). "Complete family" means that it provides necessary and sufficient conditions for the convertibility of states. It fully characterizes the resourcefulness of static resources. These monotones, in some cases, can be computed via conic linear programming. In subsequent chapters, we will provide applications of this theorem to different cases. In most scenarios, the proofs of significant theorems substantially simplify using the resource theoretic framework.

4.1 Background

Most of background knowledge needed to understand the concept and derivation of main theorem in this chapter was already discussed in last two chapters. In this section, we will present some other details that were not covered previously.

A monotonic function that can potentially provide necessary and sufficient conditions for state transformation for generic convex quantum resource theories as proved in the next section, has a form of support function. In a generic sense, a support function gives the distance from the origin to supporting hyperplanes of the convex and closed set U. The significance of the support function is that any non-empty closed and convex set can be characterized uniquely by support function and support function is compatible with operations like rotation, translation etc. Now we present the formal mathematical definition of a support function.

Support Function

The support function $f_U : \mathbb{R}^n \to \mathbb{R}$ for a non-empty closed and convex set U is

$$f_U(z) := \sup \langle x|z\rangle , \quad \forall x \in U \text{ and } z \in \mathbb{R}^n.$$

We already know that when a supporting hyperplane to a closed convex set is drawn, it divides the space into two half-spaces, such that closed convex set is fully contained in one of the half-spaces formed, this half-space is defined as

$$\{y \in \mathbb{R}^n | \langle y|x\rangle \leq f_U(x), \forall x \in U\}.$$

There is at-least one boundary point x' of U contained in the supporting hyperplane,

$$\{y \in \mathbb{R}^n | \langle y|x'\rangle = f_U(x')\}.$$

Consider an example of singleton set $U = \{u\}$, then for this case support function has

the form $f_U(x) = \langle x|u\rangle$.

4.2 A complete family of static monotones

This chapter will introduce a complete family of resource monotones for static convex quantum resource theories. A generalization of the following result to convex dynamical resource theories is provided in Ref. (Gour and Scandolo, 2020). The family of resource monotones for convex QRTs, in some cases, can be computed via semi-definite programming. Each member of the family (discussed in this chapter) is convex.

For the entanglement theory of pure states, necessary and sufficient conditions for conversion of one state into another via free operations (local operations and classical communication) were derived making use of Nielsen majorization theorem in terms of Ky-Fan norms Ref. (Nielsen, 1999). For entanglement theory of pure states, the number of conversion conditions is finite, but it is not always the case. In general, the number of conditions that provide the necessary and sufficient conditions for states' conversion need not be finite. It is already known that for mixed state case, as we go to four dimensions, a finite number of conditions are no longer sufficient to quantify the conversion fully Ref. (Gour, 2005). So the number of monotones for a generic quantum resource theory case discussed in this thesis is not expected to be finite.

Theorem

Let $\mathfrak{F}$ be a static QRTs, such that for every two systems A and B, the set $\mathfrak{F}(A \to B) \subset \mathrm{CPTP}(A \to B)$ is convex and topologically closed. For any quantum state $\omega \in \mathfrak{D}(B)$ define

$$f_\omega(\rho_A) := \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)], \qquad \forall\ \rho \in \mathfrak{D}(A). \tag{4.1}$$

Let $\rho \in \mathfrak{D}(A)$ and $\sigma \in \mathfrak{D}(B)$ be two quantum states. Then, $\sigma_B = \mathcal{E}_{A\to B}(\rho_A)$, for

some channel $\mathcal{E} \in \mathfrak{F}(A \to B)$ if and only if

$$f_\omega(\rho_A) \geqslant f_\omega(\sigma_B), \qquad \forall\, \omega \in \mathfrak{D}(B). \tag{4.2}$$

Proof: For $\rho \in \mathfrak{D}(A)$, denote the set of states obtained by the application of free operations on the state ρ as

$$\mathfrak{M}_\rho := \{\mathcal{E}(\rho) \ : \mathcal{E} \in \mathfrak{F}(A \to B)\}. \tag{4.3}$$

As already mentioned, we consider only convex static quantum resource theories, so $\mathfrak{F}$ is convex and closed implying that $\mathfrak{M}_\rho$ is also closed and convex. For convex QRTs, the supporting hyperplane theorem ensures the existence of at least one conversion witness. Now by the application of supporting hyperplane theorem, if $\sigma_B \notin \mathfrak{M}_\rho$ then hyperplane can be drawn so that it separates the convex and closed set $\mathfrak{M}_\rho$ and σ_B. Hence for $\omega \in \mathfrak{D}(B)$ and $\sigma_B \notin \mathfrak{M}_\rho$, the supporting hyperplane theorem states that

$$\mathrm{Tr}[\omega_B \sigma_B] > \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)]. \tag{4.4}$$

The supporting hyperplane theorem indicates $\sigma_B \in \mathfrak{M}_\rho$, if and only if

$$\mathrm{Tr}[\omega_B \sigma_B] \leqslant \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)], \tag{4.5}$$

for all Hermitian matrix $\omega \in \mathfrak{D}(B)$.

We first prove the inequality in Eq. 4.5 holds for all $\omega \in \mathfrak{D}(B)$ if and only if

$$\begin{aligned} f_\omega(\sigma_B) &= \max_{\mathcal{E}' \in \mathfrak{F}(B \to B)} \mathrm{Tr}[\omega_B \mathcal{E}'(\sigma_B)], \\ &\leq \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)] \\ &= f_\omega(\rho_A) \end{aligned} \tag{4.6}$$

The Eq. 4.5 can be obtained from Eq. 4.6 when $\mathcal{E}'$ is identity map as in this case,

$$\mathrm{Tr}[\omega_B \sigma_B] \leqslant \max_{\mathcal{E}' \in \mathfrak{F}(B \to B)} \mathrm{Tr}[\omega_B \mathcal{E}'(\sigma_B)]. \tag{4.7}$$

Hence,

$$\mathrm{Tr}[\omega_B \sigma_B] \leqslant \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)]. \tag{4.8}$$

Now to prove the converse (Eq. (4.5) $\implies$ Eq. (4.6)), suppose that Eq. (4.5) holds, for $\mathcal{E}' \in \mathfrak{F}(B \to B)$ we get

$$\begin{aligned} \mathrm{Tr}[\omega_B \mathcal{E}'(\sigma_B)] &= \mathrm{Tr}[\mathcal{E}'^*(\omega_B)\sigma_B], \\ &\leqslant \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\mathcal{E}'^*(\omega_B)\mathcal{E}(\rho_A)]. \end{aligned} \tag{4.9}$$

Where we made use of Eq. (4.5) to obtain the above mentioned inequality. We can further proceed as follows;

$$\begin{aligned} \mathrm{Tr}[\omega_B \mathcal{E}'(\sigma_B)] &\leqslant \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\mathcal{E}'^*(\omega_B)\mathcal{E}(\rho_A)], \\ &= \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B (\mathcal{E}' \circ \mathcal{E})(\rho_A)], \\ &\leqslant \max_{\mathcal{E} \in \mathfrak{F}(A \to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)]. \end{aligned} \tag{4.10}$$

The last inequality is proved by using the innate structure of QRTs, as the definition of QRTs states that free operations can be applied any number of times and in any sequence. If two operations are free, then composition of those two operations should be free too. As $\mathcal{E}$ and $\mathcal{E}'$ are both free, then $(\mathcal{E}' \circ \mathcal{E})$ is also free. We proved that if Eq. (4.5) holds then Eq. (4.6) holds immediately.

We will now proceed to prove that monotonic conditions derived above are also sufficient. This can be done by proving that it is sufficient to take ω_B to be a density matrix. Consider a density matrix α_B, where $\mu_B = \frac{1}{|B|} I_B$ is a maximally mixed state.

$$\alpha_B = (1 - \varepsilon)\mu_B + \varepsilon(\omega_B + (1 - \mathrm{Tr}[\omega_B])\mu_B), \tag{4.11}$$

where $\varepsilon > 0$ is small enough such that $\alpha_B \geqslant 0$. Also $\mathrm{Tr}[\alpha_B] = 1$; hence, α_B is density matrix. Now, observe that for any arbitrary Hermitian matrix ω_B, we get

$$\max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\alpha_B \mathcal{E}(\rho_A)] = \frac{(1-\varepsilon \mathrm{Tr}[\omega_B])}{|B|} + \varepsilon \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)], \tag{4.12}$$

$$f_\alpha(\rho_A) = \frac{(1-\varepsilon \mathrm{Tr}[\omega_B])}{|B|} + \varepsilon f_\omega(\rho_A). \tag{4.13}$$

$\frac{(1-\varepsilon \mathrm{Tr}[\omega_B])}{|B|}$ is just a constant terms; hence, we can conclude that Eqs. (4.5) (4.6) hold for any arbitrary Hermitian matrix ω_B only if it holds for α_B. Thus it is sufficient to consider ω_B to be density matrix.

$$f_\alpha(\rho_A) \geqslant f_\alpha(\sigma_B) \iff f_\omega(\rho_A) \geqslant f_\omega(\sigma_B) \qquad \forall\, \alpha \in \mathfrak{D}(B), \quad \forall\, \omega \in \mathrm{Herm}(B). \tag{4.14}$$

The construction of f_ω enables us to express it in the form of conic linear program. As any quantum channel can be characterized in terms of a matrix using Choi notation, we represent the set of Choi matrices of all free operations as follows;

$$\mathfrak{J} = \{J^{\mathcal{E}}_{AB} = \mathrm{id}^A \otimes \mathcal{E}(\phi^{\tilde{A}A}) : \mathcal{E} \in \mathfrak{F}(A \to B)\}. \tag{4.15}$$

As we are considering only convex QRTs, so the set of free operations $\mathfrak{F}(A \to B)$ is closed and convex, will remain so independent of the notation of free operations that we may use. So the set $\mathfrak{J}$ is also closed and convex. Since;

$$\mathcal{E}(\rho_A) = \mathrm{Tr}_A[J^{\mathcal{E}}_{AB}(\rho_A^T \otimes I_B)].$$

Monotones f_ω can be rewritten as

$$\begin{aligned} f_\omega(\rho_A) &= \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)], \\ &= \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}_B[\omega_B \mathrm{Tr}_A[J^{\mathcal{E}}_{AB}(\rho_A^T \otimes I_B)]], \end{aligned} \tag{4.16}$$

$$= \max_{J^{\mathcal{E}}_{AB} \in \mathfrak{J}} \mathrm{Tr}[J^{\mathcal{E}}_{AB}(\rho_A^T \otimes \omega_B)].$$

Inherently, $f_\omega(\rho_A)$ is the support function of $\mathfrak{M}_\rho$. By changing the notation, we have expressed it as support function of $\mathfrak{J}$ evaluated over $\rho_A^T \otimes \omega_B$. As $\mathfrak{J}$ is closed and convex, we can get the convex cone from this set by taking the conic hull, that can be obtained by multiplying its elements by a non-negative number, i.e. $\mathcal{K} := \mathbb{R}_+\mathfrak{J}$. The monotonic function $f_\omega(\rho_A)$ can be written in term of conic linear program,

$$f_\omega(\rho_A) = \max_{\substack{J_{AB} \in \mathcal{K} \\ \mathrm{Tr}[J_{AB}] = |A|}} \mathrm{Tr}\Big[J_{AB}\big((\rho_A)^T \otimes \omega_B\big)\Big]. \tag{4.17}$$

Making use of the duality theorem, the dual problem can be written as follows;

$$f_\omega(\rho_A) = \min_{\substack{X \otimes I_B - (\rho^T \otimes \omega) \in \mathcal{K}^* \\ X \in \mathrm{Herm(A)}}} \mathrm{Tr}[X], \tag{4.18}$$

where $\mathcal{K}^*$ is a dual cone

$$\mathcal{K}^* = \{N \in \mathrm{Herm(AB)} : \mathrm{Tr}[NM] \geq 0 \quad \forall M \in \mathcal{K}\}. \tag{4.19}$$

Since $\mathfrak{F}(A \to B) \subset \mathrm{CPTP}(A \to B)$ and Choi matrix of CPTP map is a positive semi-definite matrix; hence, the cone $\mathcal{K}$ consists of only positive semi-definite matrices. The cone of positive semi-definite matrices is self-dual, so $\mathcal{K}^*$ is also a cone of positive semi-definite matrices.

The functions f_ω behave monotonically under free channels, and therefore also under channels that replace any input state with a fixed free state. This in turn implies that, for every ω, f_ω take the same value on all free states $\rho \in \mathfrak{D}(A)$. If $\rho \in \mathfrak{D}(A)$ is free state then we have

$$
\begin{aligned}
f_\omega(\rho_A) &= \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\omega_B \mathcal{E}(\rho_A)] \\
&= \max_{\mathcal{E}\in\mathfrak{F}(A\to B)} \mathrm{Tr}[\omega_B \gamma_B] \\
&= g(\omega_B)
\end{aligned}
\tag{4.20}
$$

Therefore, if we want monotones that vanish on free states, for any $\omega \in \mathfrak{D}(B)$, define

$$
\mathcal{G}_\omega(\rho_A) := f_\omega(\rho_A) - g(\omega_B) \tag{4.21}
$$

In this way, $\{\mathcal{G}_\omega\}$ is a complete set of non-negative resource monotones that vanish on free states.

In upcoming chapters, we will derive several concepts, i.e. classical conditional majorization, f-divergences etc., by application of this single theorem. It will be observed that several critical preexisting theorems can be viewed as corollaries of this single theorem.

Chapter 5

Relative Majorization and f-Divergences

A generalization of divergence was introduced by Csisźar in Ref. (Csiszar, 1967), Morimoto Ref. (Morimoto, 1963) and Ali Silvey Ref. (Ali and Silvey, 1966) independently, now widely known as f-divergences. Alfréd Rényi also discussed these divergences in the same paper where he introduced Rényi entropies. He also proved that value of f-divergences could not increase by application of a Markov process. Other well known divergences such as KL-divergence, trace distance etc., all are special cases of this more generalized family of divergences called *f-divergences*.

f-Divergence

For $\mathbf{p}$ and $\mathbf{q}$ probability vectors with elements p_y and q_y respectively, an f-divergence is

$$D_f(\mathbf{p}\|\mathbf{q}) := \sum_y q_y f\left(\frac{p_y}{q_y}\right), \tag{5.1}$$

where f is convex on $(0,\infty)$, and $f(1)=0$. Moreover we have;

- $f(0) = \lim_{x\to 0^+} f(x)$.

- $0 f\left(\frac{0}{0}\right) = 0$.

A continuum counterpart of f-divergence is also well defined and is obtained by replacing summation with integral over dq. We are only concerned with the discrete case for scope of this thesis.

f-divergences quantifies difference between two probability vectors, or in other words, they tell us how distinguishable $\mathbf{p}$ is from $\mathbf{q}$.

As already mentioned, that other more commonly known measures of distinguishability are special cases of f-divergences. We will now present the f function to get the forms of some of these special cases. Many such examples were discussed in Ref. (Liese and Vajda, 2006).

- **Kullback-Leibler (KL) divergence:** Kullback-Leibler (KL) divergence can be produced from the f-divergence by taking $f(x) = x \log x$.

- **Trace Distance:** Trace distance has the form

$$d(\mathbf{p}, \mathbf{q}) = \frac{1}{2}\|\mathbf{p} - \mathbf{q}\|_1,$$

  where $\|x\|_1 = \sum_i |x_i|$.

  We can get trace distance from f-divergence by plugging in $f(x) = \frac{1}{2}\|1 - x\|_1$.

Like KL-divergence or trace distance, f-divergences also satisfy some properties stated as follows;

- **Monotonicity or Data Processing Inequality**: If $\mathbf{p}$ and $\mathbf{q}$ probability vectors are transformed into other probability vectors $\mathbf{p}'$ and $\mathbf{q}'$ by the application of some local physical operations, i.e. $\mathbf{p}' = M\mathbf{p}$ and $\mathbf{q}' = M\mathbf{q}$, then

$$D_f(\mathbf{p}\|\mathbf{q}) \geq D_f(\mathbf{p}'\|\mathbf{q}').$$

This states that distinguishability of probability vectors cannot increase under the application of some local operations.

- **Non-Negativity**: An f-divergence never takes a negative value and is zero when $\mathbf{p}$ and $\mathbf{q}$ coincide

$$\begin{aligned} D_f(\mathbf{p}\|\mathbf{q}) &= \sum_y q_y f\Big(\frac{p_y}{q_y}\Big), \\ &\geq f\Big(\sum_y q_y\big(\frac{p_y}{q_y}\big)\Big), \\ &= f(1) = 0. \end{aligned} \tag{5.2}$$

The inequality in derivation above follows from Jensen's inequality.

- **Joint Convexity**: The convexity of f in f-divergence implies the joint convexity. For $\lambda \in [0,1]$,

$$D_f\Big(\lambda\mathbf{p}_1 + (1-\lambda)\mathbf{p}_2\|\lambda\mathbf{q}_1 + (1-\lambda)\mathbf{q}_2\Big) \leq \lambda D_f(\mathbf{p}_1\|\mathbf{q}_1) + (1-\lambda)D_f(\mathbf{p}_2\|\mathbf{q}_2)$$

These properties of f-divergence are proved in Ref. (Sason and Verdu, 2016).

5.1 Majorization

The question of when a probability vector is more uncertain than another Ref. (Littlewood and Polya, 1952) leads to the concept of majorization preorder.

Majorization

Consider two probability vectors $\mathbf{p}$ and $\mathbf{q}$, with components p_x and q_x respectively. Let the components be rearranged in the decreasing order represented as $p_x^{\downarrow}$ and $q_x^{\downarrow}$. If;

$$\sum_x p_x^{\downarrow} \geq \sum_x q_x^{\downarrow},$$

then $\mathbf{p}$ majorizes $\mathbf{q}$, denoted as $\mathbf{p} \succ \mathbf{q}$.

This notion of majorization identifies when one probability vector ($\mathbf{q}$) is more uncertain compared to other ($\mathbf{p}$). It also tells us that probability vector representing uniform distribution is the most uncertain one, which is intuitive. We may also be interested in knowing if one probability vector majorizes the other, what else we can say about it. Is there some other relation between these vectors? Are they inter-convertible in a sense if $\mathbf{q}$ can be obtained from $\mathbf{p}$ by application of some physical operation or vice versa? This notion can be well understood from the other way we can define majorization. This definition is equivalent to the one mentioned above Ref. (Littlewood and Polya, 1952).

Majorization

Given two probability vectors $\mathbf{p}$ and $\mathbf{q}$, we say that $\mathbf{p} \succ \mathbf{q}$ if $\mathbf{p}$ can be converted into $\mathbf{q}$ by the application of doubly stochastic matrix D, i.e. $\mathbf{q} = D\mathbf{p}$.

This definition tells us that the certainty does not increase by random relabelling.

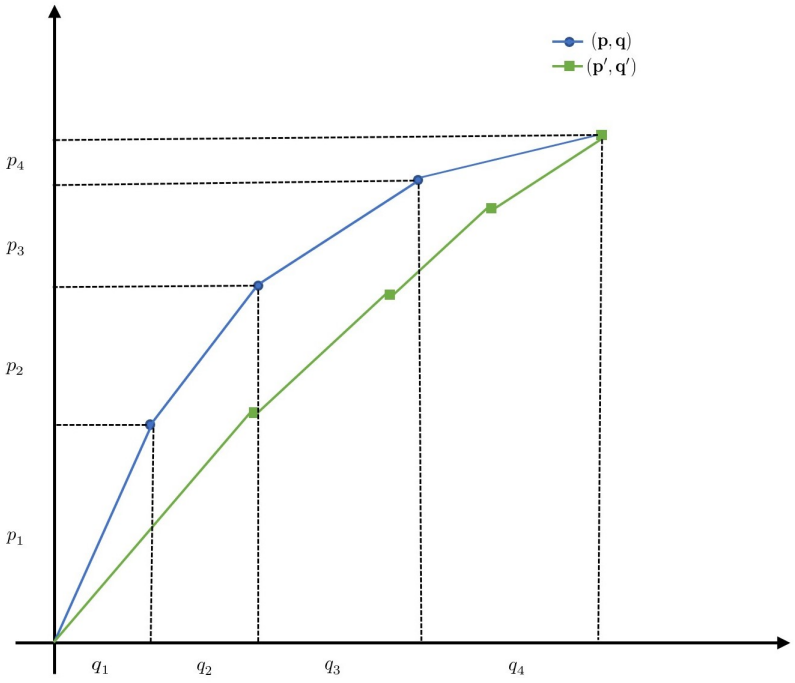
Relative majorization Refs. (Ruch and Mead, 1976; Ernst Ruch and Seligman, 1978; Ernst Ruch and Seligman, 1980; Renes, 2016a; Buscemi and Gour, 2017) is a generalization of majorization, which was historically known for its potential applications in statistics and was referred as "statistical comparison" Ref. (Blackwell, 1953). In relative majorization, we compare a pair of probability vectors rather than individual probability vectors. One pair of probability vectors relatively majorizes another when a column stochastic transformation takes the former to the latter. We now present the formal definition of relative majorization as in Ref. (Renes, 2016a).

Relative Majorization

A pair of m dimensional probability vectors $(\mathbf{p}, \mathbf{q})$ *relatively majorizes* another pair of n dimensional pair $(\mathbf{p}', \mathbf{q}')$ if and only if there exist an $n \times m$ column stochastic matrix M such that, $(\mathbf{p}', \mathbf{q}') = (M\mathbf{p}, M\mathbf{q})$ denoted as $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{p}', \mathbf{q}')$.

Lorenz curve was first introduced to give a pictorial illustration of inequality in wealth distribution Ref. (Lorenz, 1905). Lorenz curves have since been used to pictorially compare different distributions. Here it is used to fully capture the notion of relative majorization as given in Ref. (Renes, 2016a). Now we plot Lorenz curve for the pair of probability vectors $(\mathbf{p}, \mathbf{q})$ and $(\mathbf{p}', \mathbf{q}')$ when $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{p}', \mathbf{q}')$. The difference between the vertical and horizontal coordinates of elbows of curve are components of $\mathbf{p}$ and $\mathbf{q}$ respectively. If $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{p}', \mathbf{q}')$ then the Lorenz curve of $(\mathbf{p}, \mathbf{q})$ lies completely above the Lorenz curve of $(\mathbf{p}', \mathbf{q}')$. Here we assumed that probability distributions $\mathbf{p}$ and $\mathbf{q}$ are ordered in such a way that $\frac{p_x}{q_x}$ is in decreasing order.

Figure 5.1: Lorenz curve for pair of two probability vectors $(\mathbf{p}, \mathbf{q})$ and $(\mathbf{p}', \mathbf{q}')$, when $(\mathbf{p}, \mathbf{q}) \succ (\mathbf{p}', \mathbf{q}')$.



Simple majorization is just a special case of relative majorization, obtained when $n = m$ and the first or the second vector in the pairs is replaced by the uniform distribution.

Relative majorization finds extensive applications in quantum resource theories, particularly quantum resource theory of thermodynamics and pure bipartite entanglement Ref. (Renes, 2016b).

5.2 Re-derivation of RSS Theorem

In Ref. (Ruch and Mead, 1976) (RSS theorem) it was proven that $(\mathbf{p}, \mathbf{q})$ relatively majorizes $(\mathbf{p}', \mathbf{q}')$ if and only if for all f-divergences $D_f(\mathbf{p}\|\mathbf{q}) \geq D_f(\mathbf{p}'\|\mathbf{q}')$ where, $D_f(\mathbf{p}\|\mathbf{q}) := \sum_{y=1}^{n} q_y f(p_y/q_y)$ and f is a convex function, such that $f(1) = 0$. We now provide an alternative and simplified proof of the RSS theorem that follows immediately from Theorem 4.2.

Consider the classical resource theory where the objects of interest are pairs of probability vectors. The most general operations that transform n-dimensional pair of probability vectors $(\mathbf{p}, \mathbf{q})$ into pair of m-dimensional probability vectors $(\mathbf{p}', \mathbf{q}')$ are pairs of $m \times n$ column-stochastic matrices (M, N): $(\mathbf{p}', \mathbf{q}') = (M\mathbf{p}, N\mathbf{q})$. To define a resource theory for relative majorization, we consider only pairs where the two $m \times n$ column-stochastic matrices are the same, i.e. (M, M). Denote the set of free operations by $\mathfrak{C}$. Now we replace quantum state ω in Theorem 4.2 with m-dimensional pair of probability vectors $(\mathbf{r}, \mathbf{s})$ and ρ is replaced by n-dimensional pair of probability vectors $(\mathbf{p}, \mathbf{q})$. Now we replace f_ω with $D_{(\mathbf{r},\mathbf{s})}$ in original statement of Theorem 4.2. With this notation resource monotone in Eq. 4.1 takes the form

$$D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) := \max_{(M,M)} \langle (\mathbf{r}\ \mathbf{s}), (M\mathbf{p}\ M\mathbf{q}) \rangle, \tag{5.3}$$

where the maximum is over all pairs of $m \times n$ column stochastic matrices (M, M), and the inner product is the standard dot product between vectors:

$$\langle (\mathbf{r}\ \mathbf{s}), (M\mathbf{p}\ M\mathbf{q}) \rangle = \mathbf{r} \cdot M\mathbf{p} + \mathbf{s} \cdot M\mathbf{q} \tag{5.4}$$

Now Theorem 4.2 states that

$$(\mathbf{p},\mathbf{q}) \succ (\mathbf{p}',\mathbf{q}') \iff D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) \geq D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}'\|\mathbf{q}'), \tag{5.5}$$

for every pair of n-dimensional pair of probability vectors $(\mathbf{r},\mathbf{s})$. Recalling that $(\mathbf{p}',\mathbf{q}') = (M\mathbf{p}, M\mathbf{q})$, for any $m\times n$ column stochastic matrix M, we have $D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) \geq D_{(\mathbf{r},\mathbf{s})}(M\mathbf{p}\|M\mathbf{q})$ is a (classical) data-processing inequality; thus, functions $D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q})$ are divergences.

To get to f-divergence, we now simplify expression Eq. (5.3) by using the property that any $m \times n$ column-stochastic matrix can be written as convex combination of m^n matrices $\{E^x\}_{x=1}^{m^n}$, such that each column of E_x is standard basis of $\mathbb{R}^m$ ($M = \sum_{x=1}^{m^n} t_x E^x$ where $\sum_{x=1}^{m^n} t_x = 1$ and $t_x \geq 0$). For simplicity assume that all the components of $\mathbf{q}$ are strictly positive; general case can be obtained by taking appropriate limits. Hence;

$$\begin{aligned} D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) &= \max_M \{\mathbf{r}\cdot M\mathbf{p} + \mathbf{s}\cdot M\mathbf{q}\} \\ &= \max_M \sum_{y=1}^{n}\sum_{z=1}^{m}(r_z M_{zy} p_y + s_z M_{zy} q_y) \\ &= \max_{M=\sum_{x=1}^{m^n} t_x E_x} \sum_x t_x \sum_{y=1}^{n}\sum_{z=1}^{m} E^x_{zy}(r_z p_y + s_z q_y), \end{aligned} \tag{5.6}$$

where we used the fact that $M = \sum_{x=1}^{m^n} t_x E_x$, also note that

$$\sum_x t_x \sum_{y=1}^{n}\sum_{z=1}^{m} E^x_{zy}(r_z p_y + s_z q_y) \leq \max_x \sum_{y=1}^{n}\sum_{z=1}^{m} E^x_{zy}(r_z p_y + s_z q_y),$$

because t_x's are the coefficients of the convex combination. Strict equality is achieved when we have $M = E_{x^*}$, where x^* is the value of x that attains the maximum of $\sum_{y=1}^{n}\sum_{z=1}^{m} E^x_{zy}(r_z p_y + s_z q_y)$. Therefore Eq. 5.6 can be written as

$$D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) = \max_{M=\sum_{x=1}^{m^n} t_x E_x} \sum_x t_x \sum_{y=1}^{n}\sum_{z=1}^{m} E^x_{zy}(r_z p_y + s_z q_y) \tag{5.7}$$

$$
\begin{aligned}
&= \max_x \sum_{y=1}^{n} \sum_{z=1}^{m} E_{zy}^{x} (r_z p_y + s_z q_y) \\
&= \sum_{y=1}^{n} \sum_{z=1}^{m} E_{zy}^{x^*} (r_z p_y + s_z q_y) \qquad . \\
&= \sum_{y=1}^{n} q_y \sum_{z=1}^{m} \left(r_z E_{zy}^{x^*} \frac{p_y}{q_y} + s_z E_{zy}^{x^*} \right)
\end{aligned}
$$

Let us set $r_z^* := \sum_{z=1}^{m} r_z E_{zy}^{x^*}$ and $s_z^* := \sum_{z=1}^{m} s_z E_{zy}^{x^*}$; then we have

$$
\begin{aligned}
D_{(\mathbf{r},\mathbf{s})}(\mathbf{p}\|\mathbf{q}) &= \sum_{y=1}^{n} q_y \sum_{z=1}^{m} \left(r_z^* \frac{p_y}{q_y} + s_z^* \right) \\
&=: \sum_{y=1}^{n} q_y f_{(\mathbf{r},\mathbf{s})} \left(\frac{p_y}{q_y} \right).
\end{aligned} \qquad . \tag{5.8}
$$

where $f_{(\mathbf{r},\mathbf{s})}$ is a convex function defined as $f_{(\mathbf{r},\mathbf{s})}\left(\frac{p_y}{q_y}\right) = \left(r_z^* \frac{p_y}{q_y} + s_z^*\right)$. Then $D_{(\mathbf{r},\mathbf{s})}$ has the form of f-divergence. To have the property $f_{(\mathbf{r},\mathbf{s})}(1) = 0$, it is enough to redefine monotone by subtracting its maximum as in Eq. 4.21, therefore f-divergences are retrieved in relative majorization.

This application highlights the significance of resource theoretic framework. The proof of f-divergence that was first presented using another approach has been simplified by resource theoretic framework.

Chapter 6

Classical Conditional Majorization

Classical conditional majorization, discussed in Ref. (Gour, Grudka, et al., 2018), can be characterized in terms of monotonic functions. This can be derived directly from Theorem 4.2. Necessary definitions and background are first presented to understand this preorder (classical conditional majorization) and then an explicit derivation of characterization of classical conditional majorization is provided.

6.1 Classical Conditional Random Relabelling

We start by briefly describing a joint classical system, which is the object of interest to understand this preorder (classical conditional majorization). The joint classical system consists of two classical subsystems denoted as X and Y, of dimensions m and n respectively. Consider Alice holds subsystem X and Bob holds other classical register Y. The state of this joint classical system can be described as joint probability distribution, represented as an $n \times m$ joint probability matrix $\mathrm{P} = [p_{xy}]$, where p_{xy} are components of the matrix, so it must be $p_{xy} \geq 0$ and $\sum_{x,y} p_{xy} = 1$, such that $x \in [n]$ and $y \in [m]$. $[n]$ represents the set $\{1, 2, \cdots, n\}$.

For the predefined system XY, a state conversion is achieved by applying a class of operations that are a generalization of random relabeling. In this class of operations, Bob

can apply any arbitrary probabilistic operation characterized by row-substochastic maps R^j on his classical register, such that $R = \sum_j R^{(j)}$ is a row-stochastic matrix. Alice's actions are restricted in a sense that she can only do random relabelling represented by the application of $n \times n$ doubly stochastic matrix $D^{(j)}$ on her subsystem, for each of Bob's output j. These operations are called *classical-conditioned random relabeling* (CCR). In the physical setting, we can imagine Bob performing some classical experiment on his register Y, communicates his classical output to Alice. Alice in turn performs random relabeling on her system X.

Classical-Conditioned Random Relabeling

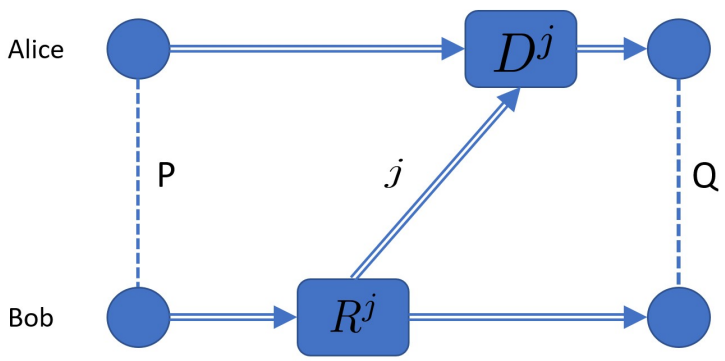
A class of operations that transforms one classical-classical state into another is called classical-conditioned random relabeling, and has the following form

$$\mathrm{P} \to \mathrm{S} = \sum_j D^j \mathrm{P} R^j,$$

where D^j is a doubly stochastic matrix and R^j is a sub-stochastic matrix such that $\sum_j R^j = R$, R represents a row stochastic matrix.

The dimensions of S and P are not necessarily same; as application of R^j can change the number of columns of P. The situation of classical conditional random relabelling is represented in Fig. 6.1;

Figure 6.1: Alice and Bob initially share a classical-classical state P. Bob can apply any arbitrary classical operations on his register. Alice performs random relabeling operations on her register conditioned on classical outputs obtained by Bob. Double line shows classical communication.



Now we proceed to the definition of *classical conditional majorization*, which is a preorder relation between two joint classical systems P and Q induced by conditional certainty non-increasing operations CCR.

Classical Conditional Majorization

A $n \times m$ joint probability matrix P conditionally majorizes $n \times \ell$ joint probability matrix Q if and only if P can be converted into Q via the application of *classical-conditioned random relabeling*

$$\mathrm{P} \to \mathrm{Q} = \sum_j D^{(j)} \mathrm{P} R^j,$$

denoted as $\mathrm{P} \succ_c \mathrm{Q}$.

6.2 Characterization of Classical Conditional Majorization

In Ref. (Gour, Grudka, et al., 2018), it was proved that convex homogeneous monotonic functions characterize classical conditional majorization. Here we show that our Theorem 4.2 produces the same results and in addition it simplifies the proof.

Theorem

Consider classical-classical systems represented by P and Q joint probability matrices of order $n \times m$ and $n \times l$. We have $\mathrm{P} \succ_c \mathrm{Q}$, if and only if

$$\sum_{y' \in [m]} p_{y'} \phi_{\mathrm{S}}(\mathbf{p}^{|y'}) \geq \sum_{x' \in [\ell]} q_{x'} \phi_{\mathrm{S}}(\mathbf{q}^{|x'}),$$

where $\phi_{\mathrm{S}}(\mathbf{p}^{|y'}) = \max_{y \leq m} \max_{\Pi} (\Pi \mathbf{s}_y)^T \mathbf{p}^{|y'}$ is a sub-linear functional.

Proof: This theorem was initially proved in Ref. (Gour, Grudka, et al., 2018), we are going to re-derive it in the context of resource theories as a corollary of Theorem 4.2, which

helps simplify the proof.

In the following application, the required version of Theorem 4.2 can be obtained by taking the set of free operations $\mathfrak{F}(A \to B)$ to be classical-conditioned random relabeling (CCR). Quantum states ω and ρ are replaced by classical-classical states S and P that are probability matrices of order $n \times \ell$ and $n \times m$ respectively. Making use of the aforementioned notation, Eq. (4.1) can be rewritten as

$$\begin{aligned} f_{\mathrm{S}}(\mathrm{P}) &= \max_{D^{(j)}, R^j} \mathrm{Tr}[\mathrm{S}^T \sum_j D^{(j)} \mathrm{P} R^j] \\ &= \max_{D^{(j)}, R^j} \sum_{j,y',y,x,k} S_{ky} D^{(j)}_{kx} P_{xy'} R_{y'y}. \end{aligned} \tag{6.1}$$

Let $\mathbf{s}_y$ be y^{th} column of S and $\mathbf{p}_{y'}$ represents y'^{th} column of P. The expression can be rewritten as

$$f_{\mathrm{S}}(\mathrm{P}) = \max_{D^{(j)}, R^j} \Big\{ \sum_{y' \in [m], y \in [\ell]} \sum_j R^j_{y'y} \big((D^{(j)})^T \mathbf{s}_y \big) \cdot \mathbf{p}_{y'} \Big\}. \tag{6.2}$$

As $(D^{(j)})^T$ is also a doubly stochastic matrix, the expression in Eq. (6.2) can be further simplified by using following notation;

$$T_{y'y} = \sum_j R^j_{y'y} \text{ and } \tilde{D}^{(y,y')} = \sum_j \frac{R^j_{y'y}}{T_{y'y}} (D^{(j)})^T,$$

where $\sum_j R^j = \mathrm{T} = [T_{y'y}]$ is a $m \times \ell$ row-stochastic matrix with entries $T_{y'y}$. Therefore we get

$$f_{\mathrm{S}}(\mathrm{P}) = \max_{\tilde{D}^{(y,y')}, \mathrm{T}} \Big\{ \sum_{y' \in [m], y \in [\ell]} T_{y'y} \big(\tilde{D}^{(y,y')} \mathbf{s}_y \big) \cdot \mathbf{p}_{y'} \Big\}.$$

Recall that

$$\max_{\tilde{D}^{(y,y')}, \mathrm{T}} \Big\{ \sum_{y' \in [m], y \in [\ell]} T_{y'y} \big(\tilde{D}^{(y,y')} \mathbf{s}_y \big) \cdot \mathbf{p}_{y'} \Big\} \leq \max_{\tilde{D}^{(y,y')}} \sum_{y' \in [m]} \max_{\mathrm{T}} \Big\{ \sum_{y \in [\ell]} T_{y'y} \big(\tilde{D}^{(y,y')} \mathbf{s}_y \big) \cdot \mathbf{p}_{y'} \Big\} \tag{6.3}$$

On the other hand, since $\sum_{y \in [\ell]} T_{y'y} \big(\tilde{D}^{(y,y')} \mathbf{s}_y \big) \cdot \mathbf{p}_{y'}$ is a convex combination (as T is a

row-stochastic matrix), we have

$$\sum_{y\in[\ell]} T_{y'y} \sum_{x\in[n]} \big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'} \leq \max_y \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\}, \tag{6.4}$$

Equality is achieved if for every choice of y', we take $T_{y'y^*}=1$, where y^* is the value of y that gives maximum value of $\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}$ and $T_{y'y}=0$ otherwise. Hence;

$$\max_{\mathrm{T}} \Big\{\sum_{y\in[\ell]} T_{y'y}\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} = \max_y \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\}. \tag{6.5}$$

With this choice of T, we achieve equality in Eq. 6.3 too. Observe that $\tilde{D}^{(y,y')}$ is still a doubly stochastic matrix, we can write it as the convex combination of permutation matrices $\tilde{D}^{(y,y')}=\sum_\pi t_\pi^{(y,y')}\Pi_\pi$, thus

$$\begin{aligned}\max_{\tilde{D}^{(y,y')}} \sum_{y'\in[m]} \max_y \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} &\leq \sum_{y'\in[m]} \max_{\tilde{D}^{(y,y')},y} \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} \\ &= \sum_{y'\in[m]} \max_{\tilde{D}^{(y,y')},y} \Big\{\sum_\pi t_\pi^{(y,y')}\big(\Pi_\pi\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\}\end{aligned} \tag{6.6}$$

Now,

$$\sum_\pi t_\pi^{(y,y')}\big(\Pi_\pi\mathbf{s}_y\big)\cdot\mathbf{p}_{y'} \leq \max_\pi \big(\Pi_\pi\mathbf{s}_y\big)\cdot\mathbf{p}_{y'} \tag{6.7}$$

We get the equality if we take $\tilde{D}^{(y,y')}=\Pi_{\pi^*}$, where π^* is the permutation for which $\big(\Pi_\pi\mathbf{s}_y\big)_x\cdot\mathbf{p}_{y'}$ attains the maximum. Then

$$\sum_{y'\in[m]} \max_{\tilde{D}^{(y,y')},y} \Big\{\sum_\pi t_\pi^{(y,y')}\big(\Pi_\pi\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} = \sum_{y'\in[m]} \max_{\Pi,y} \big(\Pi\mathbf{s}_y\big)\cdot\mathbf{p}_{y'} \tag{6.8}$$

With the choice of $\tilde{D}^{(y,y')}=\Pi$, we also have the equality in Eq. 6.6:

$$\max_{\tilde{D}^{(y,y')}} \sum_{y'\in[m]} \max_y \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} = \sum_{y'\in[m]} \max_{\tilde{D}^{(y,y')},y} \Big\{\big(\tilde{D}^{(y,y')}\mathbf{s}_y\big)\cdot\mathbf{p}_{y'}\Big\} \tag{6.9}$$

$$= \sum_{y' \in [m]} \max_{\Pi, y} \left(\Pi \mathbf{s}_y\right) \cdot \mathbf{p}_{y'}$$

This means that $f_{\mathrm{S}}(\mathrm{P}) = \sum_{y' \in [m]} \max_{\Pi, y} \left(\Pi \mathbf{s}_y\right) \cdot \mathbf{p}_{y'}$.

Consider the marginal probability on system Y: if we have a joint probability distribution P with entries p_{xy}, the marginal probability distribution is then $p_y = \sum_x p_{xy}$. Conditional probability vector can be defined as $\mathbf{p}^{|y'} := \frac{1}{p_y} \mathbf{p}_y$. Let $\phi_{\mathrm{S}}(\mathbf{p}^{|y'}) = \max_{\Pi, y} (\Pi \mathbf{s}_y)^T \mathbf{p}^{|y'}$, then the simplified expression of monotone is

$$f_{\mathrm{S}}(\mathrm{P}) = \sum_{y' \in [m]} p_{y'} \phi_{\mathrm{S}}(\mathbf{p}^{|y'}). \tag{6.10}$$

Note that $\phi_{\mathrm{S}}(\mathbf{p}^{|y'})$ is convex and positively homogeneous function, due to presence of dot product in its definition. With notation Theorem 4.2 reads that

$$\mathrm{P} \succ_c \mathrm{Q} \quad \Longleftrightarrow \quad f_{\mathrm{S}}(\mathrm{P}) \geq f_{\mathrm{S}}(\mathrm{Q}), \tag{6.11}$$

where S is a $n \times l$ probability matrix. Using the simplified form of monotone $f_{\mathrm{S}}(\mathrm{P})$ in Eq. (6.10), the monotonicity relation in Eq. (6.11) can be rewritten as

$$\sum_{y' \in [m]} p_{y'} \phi_{\mathrm{S}}(\mathbf{p}^{|y'}) \geq \sum_{x' \in [\ell]} q_{x'} \phi_{\mathrm{S}}(\mathbf{q}^{|x'}).$$

The function $\phi_{\mathrm{S}}(\mathbf{p}^{|y'})$ provides necessary and sufficient conditions to characterize classical conditional majorization.

Conditional majorization is used to derive the universal conditional uncertainty relation Ref. (Gour, Grudka, et al., 2018) in the presence of classical memory. The universal conditional uncertainty relation outperforms the entropic conditional uncertainty Refs. (Hall, 1995; Renes and Boileau, 2009) in some cases. In Ref. (Brandsen, Geng, and Gour, 2021)

operational meaning for $\phi_{\mathrm{S}}(\mathbf{p}^{|y'})$ functions was presented, where monotones reduce to pair of functions and each pair function provides the best probability to win certain game of chance.

Chapter 7

Quantum Conditional Majorization

In this chapter, for the first time, we present characterization of quantum conditional majorization. It is derived using a resource theoretic framework, which has been proved to be of adequate significance in simplifying calculations.

7.1 Classical-Quantum State

Consider an experiment discussed for the case of mixed state (see definition 2.2). There is an m faced dice and the probability that x face appears on the top when we roll the dice is p_x. When we roll it, depending on the side x that face up, we prepare state ρ_x. If after some time we forget the value x then we end up with ensemble $\{p_x, \rho_x\}_{x=1}^m$ or mixed state $\rho^A = \sum_{x=1}^m p_x \rho_x$.

Now consider the case that we did not forget the value of x, but recorded it somewhere. Then the system can be expressed in terms of the classical-quantum state $\rho^{XA} = \sum_{x=1}^n p_x |x\rangle\langle x| \otimes \rho_x^A$, where $\rho^A = \mathrm{Tr}_X[\rho^{XA}]$.

7.2 Quantum Conditional Random Relabelling

Akin to the preorder mentioned in the last chapter, a new preorder can be defined when the object of theory is classical-quantum state Refs. (Gour, Grudka, et al., 2018; Salzmann et al., 2021). In this case, Bob holds a quantum register A; Alice, on the other hand, similar the case in chapter 6, owns a classical subsystem X. The two subsystems are correlated, and the shared classical-quantum state of Alice and Bob has the form $\rho^{XA} = \sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \rho_x^A$ where, the marginal probability of Alice's output x is denoted as p_x and $|x\rangle$ represents the orthonormal basis of classical system X. The ρ_x^A is state of quantum register that Bob holds. The class of operations that define conditional majorization for this case is referred to as *quantum conditional random relabeling* (QCR).

Quantum Conditional Random Relabelling

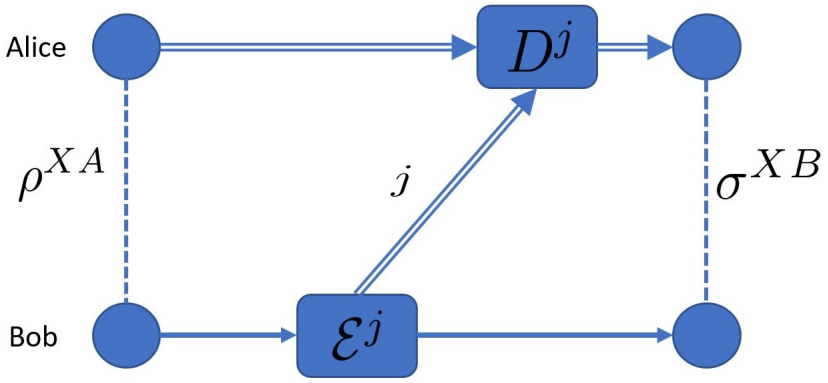
The class of operations that converts one classical-quantum state ρ^{XA} into another σ^{XB} are as follows;

$$\rho^{XA} \to \sigma^{XB} = \sum_{y,x=1}^{n} \sum_{j} p_x D_{xy}^{(j)} |y\rangle\langle y|^X \otimes [\mathcal{E}^{(j)}(\rho_x^A)]^B,$$

where $\mathcal{E}^{(j)}$ is an arbitrary trace non-increasing completely positive map such that $\sum_j \mathcal{E}^{(j)} = \mathcal{E}$ is trace preserving and $D^{(j)}$ is a doubly stochastic matrix. Then we say that ρ^{XA} conditionally majorizes σ^{XB}, denoted as $\rho^{XA} \succ_c \sigma^{XB}$.

A figurative representation of quantum conditional random relabelling is presented in Fig. 7.1.

Figure 7.1: Alice and Bob initially share a classical-quantum state. Bob preforms an arbitrary quantum operation on his subsystem which produces a classical as well as quantum output. Alice then carries out random relabeling operations on her register, possibly conditioned on classical outputs obtained by Bob. Double lines represents classical communication and a single line is used for quantum communication.



Now we can proceed to derive necessary and sufficient monotonic conditions that characterize quantum conditional majorization. As we will see in the next section, they can be written in terms of min-entropy.

7.3 Characterization of Quantum Conditional Majorization

In this section, we characterize quantum conditional majorization for the first time.

Theorem

If ρ^{XA} and σ^{XB} are two classical-quantum states, and $\rho^{XA} \succ_c \sigma^{XB}$ if and only if

$$H_{\min}(Z\tilde{B}|A)_{\Omega_\omega(\rho)} \leq H_{\min}(Z\tilde{B}|B)_{\Omega_\omega(\sigma)},$$

where

$$\Omega_{\omega}^{Z\tilde{B}A}(\rho) := \frac{1}{(n-1)!}\sum_{\pi\in[n!]}|\pi\rangle\langle\pi|\otimes\sum_{y\in[n]}q_{\pi(y)}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^{T}\otimes p_y\rho_y^A.$$
$$\Omega_{\omega}^{Z\tilde{B}B}(\sigma) := \frac{1}{(n-1)!}\sum_{\pi\in[n!]}|\pi\rangle\langle\pi|\otimes\sum_{y\in[n]}q_{\pi(y)}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^{T}\otimes p_y\sigma_y^B. \tag{7.1}$$

Proof: Suppose

$$\rho^{XA}\succ_c\sigma^{XB},$$

then

$$\rho^{XA}\to\sigma^{XB}=\mathcal{L}(\rho^{XA})=\sum_{y,x=1}^{n}\sum_j p_y D_{yx}^{(j)}|x\rangle\langle x|^X\otimes[\mathcal{E}^{(j)}(\rho_y^A)]^B,$$

for $\mathcal{L}\in$ QCR. Now we try to get the applicable form of Theorem 4.2 to proceed with the proof. For this case, set of free operations $\mathfrak{F}$ is QCR. The objects of theory are classical-quantum states like $\gamma^{\tilde{X}\tilde{B}}=\sum_{x'=1}^{n}q_{x'}|x'\rangle\langle x'|\otimes\omega_{x'}^{\tilde{B}}$ and $\rho^{XB}=\sum_{x=1}^{n}p_x|x\rangle\langle x|\otimes\rho_x^B$ which replace ω and ρ in Theorem 4.2. With this notation, the monotone in Eq. (4.1) can be rewritten as

$$\begin{aligned}f_\gamma(\rho^{XA}) &= \max_{\mathcal{L}\in\text{QCR}}\text{Tr}\big[\gamma^{\tilde{X}\tilde{B}}\mathcal{L}(\rho^{XA})\big],\\ &= \max_{D^{(j)},\mathcal{E}}\text{Tr}\Big[\Big(\sum_{x'}q_{x'}|x'\rangle\langle x'|\otimes\omega_{x'}^{\tilde{B}}\Big)\\ &\qquad\Big(\sum_{y,x}\sum_j p_y D_{yx}^{(j)}|x\rangle\langle x|^X\otimes[\mathcal{E}^{(j)}(\rho_y^A)]^B\Big)\Big].\end{aligned}$$

Every doubly stochastic matrix can be written as convex combination of permutation matrices $D^{(j)}=\sum_\pi t_{\pi|j}\Pi_\pi$ such that $\sum_\pi t_{\pi|j}=1$ and $t_{\pi|j}\geq 0$. In component form, $D_{yx}^{(j)}=\sum_\pi t_{\pi|j}\delta_{x,\pi(y)}$. Then

$$\begin{aligned}f_\gamma(\rho^{XA}) = \max_{D^{(j)},\mathcal{E}}\text{Tr}\Big[&\Big(\sum_{x'}q_{x'}|x'\rangle\langle x'|\otimes\omega_{x'}^{\tilde{B}}\Big)\\ &\Big(\sum_{y,x}\sum_j p_y D_{yx}^{(j)}|x\rangle\langle x|^X\otimes[\mathcal{E}^{(j)}(\rho_y^A)]^B\Big)\Big]\end{aligned}$$

$$
\begin{aligned}
&= \max_{D^{(j)},\mathcal{E}} \mathrm{Tr}\Big[\Big(\sum_{x'} q_{x'}|x'\rangle\langle x'| \otimes \omega_{x'}^{\tilde{B}}\Big) \\
&\quad \Big(\sum_{\pi,x,y}\sum_{j} p_y t_{\pi|j}\delta_{x,\pi(y)}|x\rangle\langle x|^X \otimes [\mathcal{E}^{(j)}(\rho_y^A)]^B\Big)\Big] \\
&= \max_{D^{(j)},\mathcal{E}} \mathrm{Tr}\Big[\Big(\sum_{x'} q_{x'}|x'\rangle\langle x'| \otimes \omega_{x'}^{\tilde{B}}\Big) \\
&\quad \Big(\sum_{\pi,y}\sum_{j} p_y t_{\pi|j}|\pi(y)\rangle\langle\pi(y)|^X \otimes [\mathcal{E}^{(j)}(\rho_y^A)]^B\Big)\Big].
\end{aligned}
\tag{7.2}
$$

Making use of notation $\tilde{\mathcal{E}}_\pi = \sum_j t_{\pi|j}\mathcal{E}^{(j)}$, we get

$$
\begin{aligned}
\mathrm{Tr}\big[\gamma^{\tilde{X}\tilde{B}}\mathcal{L}(\rho^{XA})\big] &= \mathrm{Tr}\Big[\Big(\sum_{x'} q_{x'}|x'\rangle\langle x'| \otimes \omega_{x'}^{\tilde{B}}\Big) \\
&\qquad \Big(\sum_{\pi,y} p_y|\pi(y)\rangle\langle\pi(y)| \otimes \tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big)\Big] \\
&= \sum_{\pi,x',y} q_{x'}p_y \mathrm{Tr}\Big[|x'\rangle\langle x'|\pi(y)\rangle\langle\pi(y)| \otimes \omega_{x'}^{\tilde{B}}\tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big] \\
&= \sum_{\pi,y} q_{\pi(y)}p_y \mathrm{Tr}\Big[|\pi(y)\rangle\langle\pi(y)| \otimes \omega_{\pi(y)}^{\tilde{B}}\tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big] \\
&= \sum_{\pi,y} q_{\pi(y)}p_y \mathrm{Tr}\Big[\omega_{\pi(y)}^{\tilde{B}}\tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big] \\
&= \sum_{y,\pi} q_{\pi(y)}p_y \mathrm{Tr}\Big[\Phi^{B\tilde{B}}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^T \otimes \tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big],
\end{aligned}
\tag{7.3}
$$

where $\Phi^{B\tilde{B}}$ is a maximally entangled state.

$$
\begin{aligned}
\mathrm{Tr}\big[\gamma^{\tilde{X}\tilde{B}}\mathcal{L}(\rho^{XA})\big] &= \sum_{y,\pi} q_{\pi(y)}p_y \mathrm{Tr}\Big[\Phi^{\tilde{B}B}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^T \otimes \tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\Big] \\
&= \sum_{y,\pi} q_{\pi(y)}p_y \mathrm{Tr}\Big[\Phi^{\tilde{B}B}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^T \otimes \tilde{\mathcal{E}}_\pi^{A\to B}(\rho_y^A)\delta_{\pi\pi'}\Big] \\
&= \sum_{y,\pi,\pi'} \mathrm{Tr}\Big[\big(\Phi^{\tilde{B}B} \otimes \Phi^{\tilde{Z}Z}\big)\Big(|\pi\pi'\rangle\langle\pi\pi'| \otimes q_{\pi(y)}\big(\omega_{\pi(y)}^{\tilde{B}}\big)^T \otimes p_y\tilde{\mathcal{E}}_{\pi'}^{A\to B}(\rho_y^A)\big)\Big\}\Big],
\end{aligned}
\tag{7.4}
$$

Where we have used $\mathrm{Tr}[\Phi^{\tilde{Z}Z}|\pi\pi'\rangle\langle\pi\pi'|] = \delta_{\pi'\pi}$.

$$\begin{aligned}\mathrm{Tr}\big[\gamma^{\tilde{X}\tilde{B}}\mathcal{L}(\rho^{XA})\big] = \mathrm{Tr}\Big[\big(\Phi^{\tilde{B}B}\otimes\Phi^{\tilde{Z}Z}\big)\Big\{\mathrm{id}^{Z\tilde{B}}\otimes\tilde{\mathcal{E}'}^{A\to\tilde{Z}B} \\ \Big(\sum_{\pi}|\pi\rangle\langle\pi|\otimes q_{\pi(y)}\big(\omega^{\tilde{B}}_{\pi(y)}\big)^{T}\otimes\sum_{y}p_y\rho^{A}_{y}\Big)\Big\}\Big],\end{aligned} \tag{7.5}$$

where $\tilde{\mathcal{E}}^{A\to\tilde{Z}B} = \sum_{\pi'}\tilde{\mathcal{E}}^{A\to B}_{\pi'}\otimes|\pi'\rangle\langle\pi'|$. Using the definition of $\Omega^{Z\tilde{B}A}_{\omega}(\rho)$ in Eq. (7.1), we have

$$\begin{aligned}\frac{f_\gamma(\rho^{XA})}{(n-1)!} &= \max_{\mathrm{id}^{Z\tilde{B}\to Z\tilde{B}}\otimes\tilde{\mathcal{E}'}^{A\to\tilde{Z}B}_{\pi}}\mathrm{Tr}\Big[\big(\Phi^{\tilde{B}B}\otimes\Phi^{\tilde{Z}Z}\big)\mathrm{id}^{Z\tilde{B}\to Z\tilde{B}}\otimes\tilde{\mathcal{E}'}^{A\to B\tilde{Z}}_{\pi}\big(\Omega^{Z\tilde{B}A}_{\omega}(\rho)\big)\Big] \\ &= \max_{\mathrm{id}^{Z\tilde{B}\to Z\tilde{B}}\otimes\tilde{\mathcal{E}'}^{*}_{\pi}{}^{\tilde{Z}B\to A}}\mathrm{Tr}\Big[\mathrm{id}^{Z\tilde{B}\to Z\tilde{B}}\otimes\tilde{\mathcal{E}'}^{*}_{\pi}{}^{\tilde{Z}B\to A}\big(\Phi^{\tilde{B}B}\otimes\Phi^{\tilde{Z}Z}\big)\Omega^{Z\tilde{B}A}_{\omega}(\rho)\Big] \\ &= \max_{J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}}\mathrm{Tr}\Big[J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Omega^{Z\tilde{B}A}_{\omega}(\rho)\Big].\end{aligned} \tag{7.6}$$

It can be written in the SDP form as follows;

$$\begin{aligned}&\max\mathrm{Tr}\Big[J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Omega^{Z\tilde{B}A}_{\omega}(\rho)\Big] \\ &\text{Subjected to :} \\ &\mathrm{Tr}_A\Big[J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Big] = \mathrm{id}^{Z\tilde{B}}, \\ &J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\geq 0,\end{aligned}$$

The Lagrangian associated to this primal problem is

$$\begin{aligned}L &= \mathrm{Tr}\Big[J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Omega^{Z\tilde{B}A}_{\omega}(\rho)\Big] + \mathrm{Tr}_{Z\tilde{B}}\Big[X\big(\mathrm{id}^{Z\tilde{B}} - \mathrm{Tr}_A[J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}]\big)\Big] + \mathrm{Tr}\Big[Y J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Big] \\ &= \mathrm{Tr}\Big[X\Big] + \mathrm{Tr}\Big[\big(\Omega^{Z\tilde{B}A}_{\omega}(\rho) + Y - X\otimes\mathrm{id}^{A}\big)J^{Z\tilde{B}A}_{\tilde{\mathcal{E}'}^{*}_{\pi}}\Big].\end{aligned} \tag{7.7}$$

We have introduced dual variables, i.e., Lagrange multipliers X, a Hermitian operator acting on Hilbert space $\mathcal{H}^{Z\tilde{B}}$, and Y , a semi-definite positive operator acting on Hilbert space $\mathcal{H}^{Z\tilde{B}A}$, to ensure that the Lagrangian L is always greater than the objective function whenever

the primal constraints are satisfied. Therefore, in this case, the dual SDP is obtained by minimizing over all dual variables:

$$\begin{aligned} &\min \mathrm{Tr}\Big[X\Big] \\ &\text{Subjected to :} \\ &X \otimes \mathrm{id}^A \geq \Omega_{\omega}^{Z\tilde{B}A}(\rho). \end{aligned} \tag{7.8}$$

Here, the strong duality holds since the primal SDP is finite and strictly feasible, which guarantees that the optimal value of dual coincides with the optimal value of the primal problem. The optimal value is related with the conditional min-entropy.

Min-entropy

Let $\rho \in \mathfrak{D}(AB)$ be a bipartite quantum operator. The min-entropy of A conditioned on B is defined by

$$H_{\min}(A|B)_{\rho} = -\inf_{\sigma^B} D_{\max}(\rho^{AB}|\mathrm{id}^A \otimes \sigma^B), \tag{7.9}$$

where the infimum ranges over all semi-definite positive operator σ, with

$$D_{\max}(\rho|\sigma) = \inf_{\lambda}\{\lambda \in \mathbb{R}\{\lambda : \rho \leq 2^{\lambda}\sigma\}. \tag{7.10}$$

Now it is clear from the context that the optimal value of Eq. (7.8) is $2^{-H_{\min}(Z\tilde{B}|A)}$. The monotinicity relation of Eq. (4.2) for this case will take form as follows;

$$2^{-H_{\min}(Z\tilde{B}|A)} \geq 2^{-H_{\min}(Z\tilde{B}|B)}.$$

This can be further simplified to get

$$H_{\min}(Z\tilde{B}|A) \leq H_{\min}(Z\tilde{B}|B).$$

We have proved that quantum conditional majorization can be characterized in terms of conditional min-entropic monotonic relation.

Chapter 8

Conclusion

In this thesis, we presented a framework of inter-conversion of states of physical systems for convex static quantum resource theories. The question of conversion of states in most resource theories can be formulated in terms of a feasibility of semi-definite program or more generally as a conic linear program. Choi matrix notation is extensively used to express the question of convertibility of states in terms of a conic linear program. Duality theorem allows us to write tractable conic linear programs for complete family of monotonic conditions for the convertibility of resources within certain quantum resource theories. A complete family provides necessary and sufficient conditions in the form of monotonic functions. These monotones can be computed in practice by means of a semi-definite program for the case of resource theories exhibiting a simple mathematical structure.

In this thesis, we derived a complete family of resource monotones that characterize convertibility of states for generic static convex QRTs. In the proof we used the fact that, due to convexity in QRTs, separating hyper-plane theorem ensures the presence of at least one witness for each resource state. I derived several results as the corollary of the single Theorem 4.2. My contribution is specifically work done in chapters 5,6, and 7. In chapter 5, I derived f-divergence from same theorem. The f-divergence has widely known applications in statistics, game theory etc. Ref. (Sason, 2019); this derivation shows the strength of resource

theoretic framework. In chapter 6, characterization of classical conditional majorization was done as a corollary of Theorem 4.2. Classical conditional majorization has been used to derive generalized conditional uncertainty relation in the presence of classical memory Ref. (Gour, Grudka, et al., 2018). I have provided the alternative approach that can be used to prove all the results that are derived using classical conditional majorization. In chapter 7, I presented the characterization of quantum conditional majorization in terms of the min-entropic functions for the first time. We expect that this theorem will find operational meaning in different scenarios like the classical counterpart.

Bibliography

Ali, S. M. and S. D. Silvey (1966). "A General Class of Coefficients of Divergence of One Distribution from Another". In: *Journal of the Royal Statistical Society. Series B (Methodological)* 28.1, pp. 131–142. ISSN: 00359246. URL: http://www.jstor.org/stable/2984279.

Barvinok, Alexander I. (2002). *A course in convexity*. Vol. 54. Graduate studies in mathematics. American Mathematical Society. ISBN: 978-0-8218-2968-4.

Bennett, Charles H. and Gilles Brassard (Dec. 2014). "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560, pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

Bennett, Charles H., Gilles Brassard, et al. (Mar. 1993). "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

Bennett, Charles H. and Stephen J. Wiesner (Nov. 1992). "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". In: *Phys. Rev. Lett.* 69 (20), pp. 2881–2884. DOI: 10.1103/PhysRevLett.69.2881. URL: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881.

Blackwell, David (1953). "Equivalent Comparisons of Experiments". In: *The Annals of Mathematical Statistics* 24.2, pp. 265–272. DOI: 10.1214/aoms/1177729032. URL: https://doi.org/10.1214/aoms/1177729032.

Born, Max (1926). "Zur Quantenmechanik der Stoßvorgänge". In: *Zeitschrift für Physik* 37.12, pp. 863–867.

Boyd, Stephen and Lieven Vandenberghe (2004). *Convex Optimization*. Cambridge University Press. DOI: 10.1017/CBO9780511804441.

Brandsen, Sarah, Isabelle Jianing Geng, and Gilad Gour (2021). "What is Entropy? A new perspective from games of chance".

Bromley, Thomas R et al. (July 2018). "Accessible bounds for general quantum resources". In: *Journal of Physics A: Mathematical and Theoretical* 51.32, p. 325303. DOI: 10.1088/1751-8121/aacb4a. URL: https://doi.org/10.1088/1751-8121/aacb4a.

Buscemi, Francesco and Gilad Gour (2017). "Quantum relative Lorenz curves". In: *Phys. Rev. A* 95 (1), p. 012110. DOI: 10.1103/PhysRevA.95.012110. URL: https://link.aps.org/doi/10.1103/PhysRevA.95.012110.

Chitambar, Eric and Gilad Gour (Apr. 2019). "Quantum resource theories". In: *Reviews of Modern Physics* 91.2. ISSN: 1539-0756. DOI: 10.1103/revmodphys.91.025001. URL: http://dx.doi.org/10.1103/RevModPhys.91.025001.

Chitambar, Eric, Julio I. de Vicente, et al. (2020). "Entanglement manipulation beyond local operations and classical communication". In: *Journal of Mathematical Physics* 61.4, p. 042201. DOI: 10.1063/1.5124109. eprint: https://doi.org/10.1063/1.5124109. URL: https://doi.org/10.1063/1.5124109.

Csiszar, I. (1967). "Information-type measures of difference of probability distributions and indirect observation". In: *Studia Scientiarum Mathematicarum Hungarica* 2, pp. 229–318. URL: https://ci.nii.ac.jp/naid/10028997448/en/.

Dirac, P. A. M. (Jan. 1939). "A new notation for quantum mechanics". In: *Proceedings of the Cambridge Philosophical Society* 35.3, p. 416. DOI: 10.1017/S0305004100021162.

Ernst Ruch, Rudolf Schranner and Thomas H. Seligman (1978). "The mixing distance". In: *J. Chem. Phys.* 69 (1). DOI: 10.1063/1.436364.

— (1980). "Generalization of a theorem byHardy, Littlewood, and Polya". In: *Journal of Mathematical Analysis and Applications* 76 (1), pp. 222–229. DOI: 10.1016/0022-247X(80)90075-X.

Feynman, Richard P. (June 1982). "Simulating Physics with Computers". In: *International Journal of Theoretical Physics* 21.6-7, pp. 467–488. DOI: 10.1007/BF02650179.

Girard, Mark W. (2017). "Convex Analysis in Quantum Information". PhD thesis. Calgary, Canada: University of Calgary. URL: https://www.iqst.ca/media/pdf/publications/Girard_Calgary_PhDthesis.pdf.

Gour, Gilad (Aug. 2005). "Infinite number of conditions for local mixed-state manipulations". In: *Phys. Rev. A* 72 (2), p. 022323. DOI: 10.1103/PhysRevA.72.022323. URL: https://link.aps.org/doi/10.1103/PhysRevA.72.022323.

— (June 2017). "Quantum resource theories in the single-shot regime". In: *Phys. Rev. A* 95 (6), p. 062314. DOI: 10.1103/PhysRevA.95.062314. URL: https://link.aps.org/doi/10.1103/PhysRevA.95.062314.

— (2019). "Comparison of Quantum Channels by Superchannels". In: *IEEE Transactions on Information Theory* 65.9, pp. 5880–5904. DOI: 10.1109/TIT.2019.2907989.

Gour, Gilad, Andrzej Grudka, et al. (Apr. 2018). "Conditional uncertainty principle". In: *Phys. Rev. A* 97 (4), p. 042130. DOI: 10.1103/PhysRevA.97.042130. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.042130.

Gour, Gilad and Carlo Maria Scandolo (2020). *Dynamical Resources*. arXiv: 2101.01552 [quant-ph].

Gour, Gilad and Robert W Spekkens (Mar. 2008). "The resource theory of quantum reference frames: manipulations and monotones". In: *New Journal of Physics* 10.3, p. 033023. DOI: 10.1088/1367-2630/10/3/033023. URL: https://doi.org/10.1088/1367-2630/10/3/033023.

Hall, Michael J. W. (Apr. 1995). "Information Exclusion Principle for Complementary Observables". In: *Phys. Rev. Lett.* 74 (17), pp. 3307–3311. DOI: 10.1103/PhysRevLett.74.3307. URL: https://link.aps.org/doi/10.1103/PhysRevLett.74.3307.

Horodecki, Michał, Karol Horodecki, et al. (Mar. 2003). "Local Information as a Resource in Distributed Quantum Systems". In: *Phys. Rev. Lett.* 90 (10), p. 100402. DOI: 10.1103/PhysRevLett.90.100402. URL: https://link.aps.org/doi/10.1103/PhysRevLett.90.100402.

Horodecki, Michał, Paweł Horodecki, et al. (June 2005). "Local versus nonlocal information in quantum-information theory: Formalism and phenomena". In: *Phys. Rev. A* 71 (6), p. 062307. DOI: 10.1103/PhysRevA.71.062307. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.062307.

Horodecki, Ryszard et al. (June 2009). "Quantum entanglement". In: *Rev. Mod. Phys.* 81 (2), pp. 865–942. DOI: 10.1103/RevModPhys.81.865. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.865.

Liese, F. and I. Vajda (2006). "On Divergences and Informations in Statistics and Information Theory". In: *IEEE Transactions on Information Theory* 52.10, pp. 4394–4412. DOI: 10.1109/TIT.2006.881731.

Littlewood, G. H. Hardy D. E. and G. Polya (1952). *inequalities*. 2nd ed. Cambridge Mathematical Library: Cambridge University Press. ISBN: 9780521358804.

Liu, Zi-Wen, Kaifeng Bu, and Ryuji Takagi (July 2019). "One-Shot Operational Quantum Resource Theory". In: *Phys. Rev. Lett.* 123 (2), p. 020401. DOI: 10.1103/PhysRevLett.123.020401. URL: https://link.aps.org/doi/10.1103/PhysRevLett.123.020401.

Liu, Zi-Wen, Xueyuan Hu, and Seth Lloyd (Feb. 2017). "Resource Destroying Maps". In: *Phys. Rev. Lett.* 118 (6), p. 060502. DOI: 10.1103/PhysRevLett.118.060502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.118.060502.

Lorenz, M. O. (1905). "Methods of Measuring the Concentration of Wealth". In: *Publications of the American Statistical Association* 9.70, pp. 209–219. DOI: 10.1080/15225437.1905.

10503443. eprint: https://www.tandfonline.com/doi/pdf/10.1080/15225437.1905.10503443. URL: https://www.tandfonline.com/doi/abs/10.1080/15225437.1905.10503443.

Morimoto, Tetsuzo (Mar. 1963). "Markov Processes and the H-Theorem". In: *Journal of the Physical Society of Japan* 18.3, pp. 328–331. DOI: 10.1143/JPSJ.18.328.

Nielsen, M. A. (July 1999). "Conditions for a Class of Entanglement Transformations". In: *Phys. Rev. Lett.* 83 (2), pp. 436–439. DOI: 10.1103/PhysRevLett.83.436. URL: https://link.aps.org/doi/10.1103/PhysRevLett.83.436.

Oppenheim, Jonathan et al. (Oct. 2002). "Thermodynamical Approach to Quantifying Quantum Correlations". In: *Phys. Rev. Lett.* 89 (18), p. 180402. DOI: 10.1103/PhysRevLett.89.180402. URL: https://link.aps.org/doi/10.1103/PhysRevLett.89.180402.

Raussendorf, Robert and Hans J. Briegel (May 2001). "A One-Way Quantum Computer". In: *Phys. Rev. Lett.* 86 (22), pp. 5188–5191. DOI: 10.1103/PhysRevLett.86.5188. URL: https://link.aps.org/doi/10.1103/PhysRevLett.86.5188.

Regula, Bartosz (Dec. 2017). "Convex geometry of quantum resource quantification". In: *Journal of Physics A: Mathematical and Theoretical* 51.4, p. 045303. DOI: 10.1088/1751-8121/aa9100. URL: https://doi.org/10.1088/1751-8121/aa9100.

Renes, Joseph M. (2016a). "Relative submajorization and its use in quantum resource theories". In: *Journalof Mathematical Physics* 57 (12). DOI: 10.1063/1.4972295.

— (Dec. 2016b). "Relative submajorization and its use in quantum resource theories". In: *Journal of Mathematical Physics* 57.12, p. 122202. ISSN: 1089-7658. DOI: 10.1063/1.4972295. URL: http://dx.doi.org/10.1063/1.4972295.

Renes, Joseph M. and Jean-Christian Boileau (July 2009). "Conjectured Strong Complementary Information Tradeoff". In: *Phys. Rev. Lett.* 103 (2), p. 020402. DOI: 10.1103/PhysRevLett.103.020402. URL: https://link.aps.org/doi/10.1103/PhysRevLett.103.020402.

Ruch, Ernst and Alden Mead (1976). "The principle of increasing mixing character and some of its consequences". In: *Theoret. Chim. Acta* 41. DOI: 10.1007/BF01178071.

Salzmann, Robert et al. (2021). "Symmetric distinguishability as a quantum resource".

Sason, Igal (Oct. 2019). "On Data-Processing and Majorization Inequalities for f-Divergences with Applications". In: *Entropy* 21.10, p. 1022. ISSN: 1099-4300. DOI: 10.3390/e21101022. URL: http://dx.doi.org/10.3390/e21101022.

Sason, Igal and Sergio Verdu (Nov. 2016). "f -Divergence Inequalities". In: *IEEE Transactions on Information Theory* 62.11, pp. 5973–6006. ISSN: 1557-9654. DOI: 10.1109/tit.2016.2603151. URL: http://dx.doi.org/10.1109/TIT.2016.2603151.

Sharma, Naresh (2010). "Equality conditions for the quantum f-relative entropy and generalized data processing inequalities". In: *2010 IEEE International Symposium on Information Theory*, pp. 2698–2702. DOI: 10.1109/ISIT.2010.5513655.

Takagi, Ryuji and Bartosz Regula (Sept. 2019). "General Resource Theories in Quantum Mechanics and Beyond: Operational Characterization via Discrimination Tasks". In: *Phys. Rev. X* 9 (3), p. 031053. DOI: 10.1103/PhysRevX.9.031053. URL: https://link.aps.org/doi/10.1103/PhysRevX.9.031053.

Toyoda, Toshiyuki (Mar. 1973). "Necessity of Complex Hilbert Space for Quantum Mechanics". In: *Progress of Theoretical Physics* 49.3, pp. 707–713. ISSN: 0033-068X. DOI: 10.1143/PTP.49.707. eprint: https://academic.oup.com/ptp/article-pdf/49/3/707/5261257/49-3-707.pdf. URL: https://doi.org/10.1143/PTP.49.707.

Vidal, Guifré (Oct. 2003). "Efficient Classical Simulation of Slightly Entangled Quantum Computations". In: *Phys. Rev. Lett.* 91 (14), p. 147902. DOI: 10.1103/PhysRevLett.91.147902. URL: https://link.aps.org/doi/10.1103/PhysRevLett.91.147902.