A Framework for Uncertainty Relations

Von der Fakultät für Mathematik und Informatik
der Universität Leipzig
angenommene

D I S S E R T A T I O N

zur Erlangung des akademischen Grades

DOCTOR RERUM NATURALIUM
(Dr.rer.nat.)

im Fachgebiet

Mathematik

vorgelegt

von Bachelor Yunlong Xiao
geboren am 05.07.1989 in Hubei (VR China)

Die Annahme der Dissertation wurde empfohlen von:

1. Professor Dr. Jürgen Jost (Leipzig, Deutschland)
2. Professor Dr. Gilad Gour (Calgary, Kanada)

Die Verleihung des akademischen Grades erfolgt mit Bestehen der Verteidigung am 20.02.2017 mit dem Gesamtprädikat magna cum laude.

献给我挚爱的父母和妻子！

Acknowledgements

My sincere and earnest thanks to my 'Doktorväter' Prof. Dr. Naihuan Jing and Prof. Dr. Jürgen Jost. They brought me to an interesting field of research, and have been continuously giving me valuable guidance and support. Moreover, the research leading to this thesis was carried out under the supervision of Prof. Dr. Naihuan Jing.

Thanks to my collaborators Prof. Dr. Shao-Ming Fei and Prof. Dr. Xianqing Li-Jost, from whom I have learnt a lot during discussions. I am also greatly indebted to all my collaborators for giving me the opportunity to collaborate closely with and learn from them.

A heartfelt thanks go to Dr. Yinshan Chang, Dr. Jian Wang and Mr. Ruijun Wu, who generously set aside time to answer both conceptual and technical questions and I have undoubtedly benefited a lot from these interactions.

Special thanks to Dr. Xianqing Li-Jost, not only for her guidance in mathematics and research, but also for her endless care and love—she has made a better and happier me.

Many thanks to Dr. Yinshan Chang and Mr. Ruijun Wu helping with the artwork in this thesis, and also to Dr. Yue Ma and Dr. Jian Wang for devoting their time and energy to reading drafts of the thesis and making language corrections.

I also wish to express my appreciation to the administrative staff at MIS MPG: Ms. Heike Rackwitz, Ms. Antje Vandenberg and so on. Particular thanks go to my colleagues: Dr. Wentao Cao, Dr. Yinshan Chang, Dr. Lei Liu, Dr. Yangjing Long, Mr. Ruijun Wu and Dr. Jian Wang, who gave me much valuable suggestion on both research and related questions.

I am very grateful to both IMPRS and CSC for providing a financial scholarship for my studies.

Finally, to my family and friends for their ongoing care, support and encouragement—you make my life colourful. This thesis is dedicated to my father Wenqiang Xiao, my mother Ningli Wang and my wife Lin Fan.

Abstract

Uncertainty principle, which was first introduced by Werner Heisenberg in 1927, forms a fundamental component of quantum mechanics. A graceful aspect of quantum mechanics is that the uncertainty relations between incompatible observables allow for succinct quantitative formulations of this revolutionary idea: it is impossible to simultaneously measure two complementary variables of a particle in precision. In particular, information theory offers two basic ways to express the Heisenberg's principle: variance-based uncertainty relations and entropic uncertainty relations.

We first investigate the uncertainty relations based on the sum of variances and derive a family of weighted uncertainty relations to provide an optimal lower bound for all situations. Our work indicates that it seems unreasonable to assume a priori that incompatible observables have equal contribution to the variance-based sum form uncertainty relations. We also study the role of mutually exclusive physical states in the recent work and generalize the variance-based uncertainty relations to mutually exclusive uncertainty relations.

Next, we develop a new kind of entanglement detection criteria within the framework of marjorization theory and its matrix representation. By virtue of majorization uncertainty bounds, we are able to construct the entanglement criteria which have advantage over the scalar detecting algorithms as they are often stronger and tighter.

Furthermore, we explore various expression of entropic uncertainty relations, including sum of Shannon entropies, majorization uncertainty relations and uncertainty relations in presence of quantum memory. For entropic uncertainty relations without quantum side information, we provide several tighter bounds for multi-measurements, with some of them also valid for Rényi and Tsallis entropies besides the Shannon entropy. We employ majorization theory and actions of the symmetric group to obtain an admixture bound for entropic uncertainty relations with multi-measurements. Comparisons among existing bounds for multi-measurements are also given. However,

classical entropic uncertainty relations assume there has only classical side information. For modern uncertainty relations, those who allowed for non-trivial amount of quantum side information, their bounds have been strengthened by our recent result for both two and multi-measurements.

Finally, we propose an approach which can extend all uncertainty relations on Shannon entropies to allow for quantum side information and discuss the applications of our entropic framework. Combined with our uniform entanglement frames, it is possible to detect entanglement via entropic uncertainty relations even if there is no quantum side information. With the rising of quantum information theory, uncertainty relations have been established as important tools for a wide range of applications, such as quantum cryptography, quantum key distribution, entanglement detection, quantum metrology, quantum speed limit and so on. It is thus necessary to focus on the study of uncertainty relations.

Contents

Notation

$A_{m\times n} = (a_{ij})$ denotes a matrix of size $m \times n$, with entries a_{ij}.

$\det(A)$ or $|A|$ denote the determinant of the matrix A.

$\mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ is the diagonal matrix of size $n \times n$ with diagonal elements λ_i.

A^t is the transpose of matrix A.

$\overline{A}$ or A^* is the conjugate of a matrix A, $A^* = \overline{A} = (a'_{ij})$.

$A^\dagger$ is the transposed and conjugated of matrix A.

ρ^{T_i} is the partial transpose with respect to the i-th space of a density matrix ρ.

$\mathrm{Tr}(A)$ is the trace of matrix A.

$\mathrm{Tr}_A(\rho)$ is the partial trace of a density matrix ρ with respect to the subsystem A.

Rank (A) is the rank of matrix A.

$|V\rangle$ denotes a column vector V; $\langle V| = (|V\rangle)^\dagger$.

$\langle V|W\rangle \equiv \langle V, W\rangle$ is the inner product of vectors $|V\rangle$ and $|W\rangle$.

$A \otimes B$ is the tensor product (or Kronecker product) of matrices A and B.

$\{|0\rangle = (1, 0, \cdots, 0)^t, |1\rangle = (0, 1, 0, \cdots, 0)^t, \cdots, |n-1\rangle = (0, 0, \cdots, 0, 1)^t\}$, denotes the canonical basis of an n-dimension vector space.

$\sigma_0 = I_2$, $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices.

$\langle A_i \otimes B_j\rangle_\rho \equiv \mathrm{Tr}(\rho(A_i \otimes B_j))$, where ρ is a state, A_i and B_j are Hermitian operators.

$\sigma = \begin{pmatrix} 1 & \cdots & n \\ k_1 & \cdots & k_n \end{pmatrix}$ is a permutation, $\sigma(i) = k_i$.

$span(e_1, \cdots, e_n)$ is the linear space spanned by the elements $e_1, \cdots, e_n$.

$A \geq 0$ means that the Hermitian matrix A is positive definite.

$A < 0$ means that the Hermitian matrix A is negative definite.

$\mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ denote the sets of integers, real and complex numbers, respectively.

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j \text{ ,} \\ 0 & \text{otherweise.} \end{cases}$$

List of Figures

Chapter 1

Introduction

As a first step, we start this chapter with a rather succinct introduction into quantum theory and information theory. In Sec. 1.1-1.3 , we intend to describe the basic law of quantum mechanics and attempt to give a brief overview of information theory. The remaining subsections of this chapter provide a short review of uncertainty principle and the modern representation of the uncertainty principle as a guessing game. Finally, the last subsection is detailed outline of the thesis.

1.1 Quantum Mechanics

The *Schrödinger Equation* governs the motion of particles and we can obtain the wave function, $\Psi(x,t)$, of the particle by solving the celebrated *Schrödinger Equation*:

$$i\hbar\frac{\partial\Psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + V\Psi(x,t), \tag{1.1}$$

where m is the mass of the particle and V is its potential energy. Here we restrict our attention only to non-relativistic quantum mechanics and take *Born's statistical interpretation* of the wave function.

Born's Statistical Interpretation

Born's statistical interpretation of the wave function states that the quantity $| \Psi(x,t) |^2$ describes the probability density of finding the physical particle at specific location x with specific time t, this statistical interpretation can be formulated as

$$\int_a^b | \Psi(x,t) |^2 \, dx = \left\{ \begin{matrix} \text{probability of finding the particle between} \\ \text{point } a \text{ and point } b\text{, at specific time } t \end{matrix} \right\}, \tag{1.2}$$

this law is predicatively in contrast to our intuition about the physical world. Both in classical mechanics and our daily life, any observation about a physical particle can be predicted precisely by giving the general description of the measured particle. Take a football for example, during a match every observer can measure the objective property, like position x and momentum p, of the measured football independently with the help of precise instrument. However, the statistical interpretation brings a kind of uncertainty (or so-called indeterminacy) into quantum theory. Even if you have already know all the objective information (like its wave function) about the measured particle, you can never predict both the outcome of the position x and the momentum p measurements accurately.

Due to the indeterminacy of *Born's statistical interpretation*, all quantum theory has to offer is a kind of probability distribution of the results. In both physics and philosophy, we need to face an unavoidable question: *If we measure the position of particle and find it at the position x_0, then where was the particle just before we made the measurement?* This is a rather philosophical question and the preferred answers to this question have been divided into three main kinds of thought by regarding the indeterminacy:

- The realist position: The measured particle was just at x_0. To the school of realist, probability (also known as indeterminacy or uncertainty) is not the intrinsic property of nature, but rather a lack of knowledge. And this is the interpretation that Einstein advocated. Through the celebrated paper [EPR35], *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete*, written by Einstein, Podolsky and Rosen, they believe that "the wave function does not provide a complete description of the physical reality". Moreover, some additional information (known as Local Hidden-Variable or Local realistic models [Bel66]) are needed to give the complete description of the physical particle.

- The orthodox position: The measured particle was not really anywhere but the fact is that the measurement forced the particle to appeared at position x_0. This is the "standard" interpretation of quantum mechanics, the distinguished *Copenhagen Interpretation*, which is formulated by Bohr and Heisenberg in around 1927 and it is also a natural extension of *Born's statistical interpretation* of wave functions. Note that, among all the physicists this interpretation has always been the most widely accepted rendering of quantum theory.

- All other positions: Here we take several interpretations for example. The *Many-worlds Interpretation*, introduced by Hugh Everett in around 1957 [EI56], states there is a universal wave function that obeys the deterministic laws at all time, meanwhile the phenomena related with measurements are claimed to be annotated by decoherence; In the *Stochastic Interpretation* [Nel66], introduced by Edward Nelson in around 1966, it is impossible to define the velocities of the fixed particle since the paths of motion are not smooth and continuous. Without the Markov process of the particle, we have no idea to know its motion. However, if we know the initial conditions and its Markov process of particle precisely, then the theory becomes a realistic interpretation of quantum mechanics. For simplicity, we only talk about two main interpretations here. Clearly, there are other interpretations like Louis de Broglie's *de Broglie-Bohm Interpretation*, Garrett Birkhoff's *Quantum Logic Interpretation*, John von Neumann 's *von Neumann interpretation*, Cramer's *Transactional Interpretation* and so on.

Furthermore, if the indeterminacy is not enough to confuse human's intuition, consider pair of particles (bipartite system) that are in an entangled state. Measurement, such as spin, polarization, position, momentum, performed on the entangled bipartite system are shown to be appropriately correlated. More specifically, take two electrons, e_1 and e_2, that are in a spin singlet state for example. An observer getting command of particle e_1 can accurately forecast the result of all possible spin measurements of particle e_2. On the other hand, to copy or share the quantum information inside the reduced state e_1 is unallowed in quantum information theory, and this phenomenon is the so-called *monogamy of entanglement*, or simply *no-cloning* of quantum states.

Relations between Particles

To describe the classical particle in our everyday life, two states of a classical particle are said to have the same physical nature if and only if they have the same mathematical representation. While for quantum mechanics, the situation is much more complicated. There are three main relations between particles need to be considered.

- Multiple: If two wave functions $\Psi(x,t)$ and $\Phi(x,t)$ satisfy that they are multiples of each other for some nontrivial complex number c, then this two wave functions $\Psi(x,t)$ and $\Phi(x,t)$ are said to represent the same physical

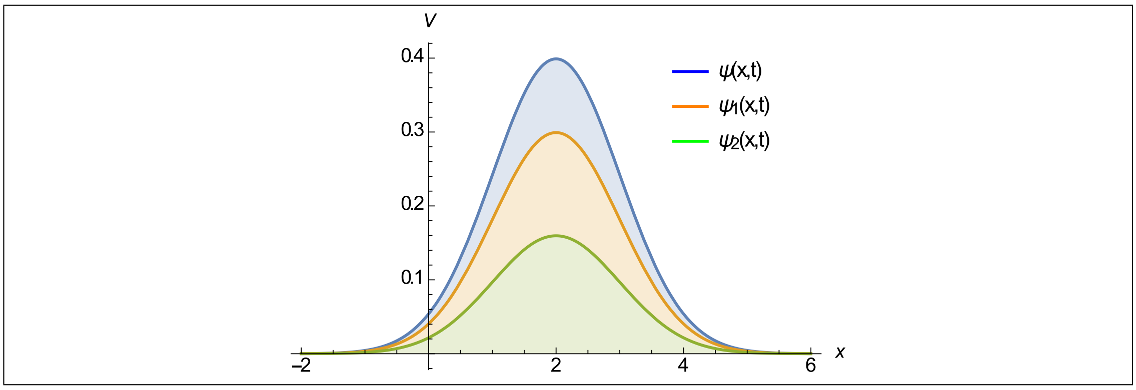

Figure 1.1: Three wave functions $\Psi(x,t)$, $\Psi_1(x,t)$ and $\Psi_2(x,t)$, which are multiples of each other, share the same physical meaning.

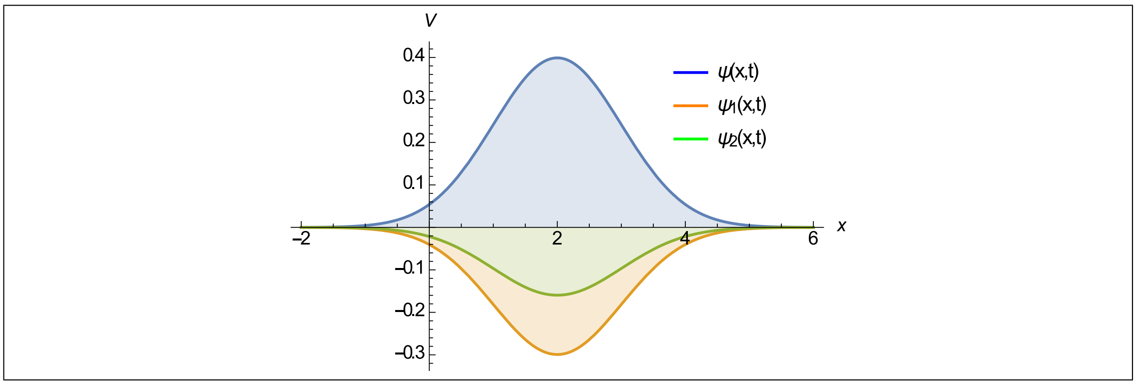

Figure 1.2: Three wave functions $\Psi(x,t)$, $\Psi_1(x,t)$ and $\Psi_2(x,t)$, which are multiples of each other, share the same physical meaning.

meaning. More specifically, their relation can be formulated as

$$\Psi(x,t) = c\Phi(x,t). \tag{1.3}$$

Hence, in FIG. 1.1 and FIG. 1.2, all wave functions share the same physical meaning. This setting is nevertheless in stark contrast with our knowledge about the classical mechanics. With the multiplying amplitude of a state in classical mechanics, the physical meaning of classical particle changes, meanwhile the physical meaning of wave functions stays the same in quantum theory.

It is now possible to introduce the *normalized wave function*

$$\overline{\Psi(x,t)} = \frac{\Psi(x,t)}{\| \Psi(x,t) \|}, \tag{1.4}$$

for any wave function $\Psi(x,t)$ with positive norm. Both $\overline{\Psi(x,t)}$ and $\Psi(x,t)$ have the same physical meaning since they are multiples of each other. In

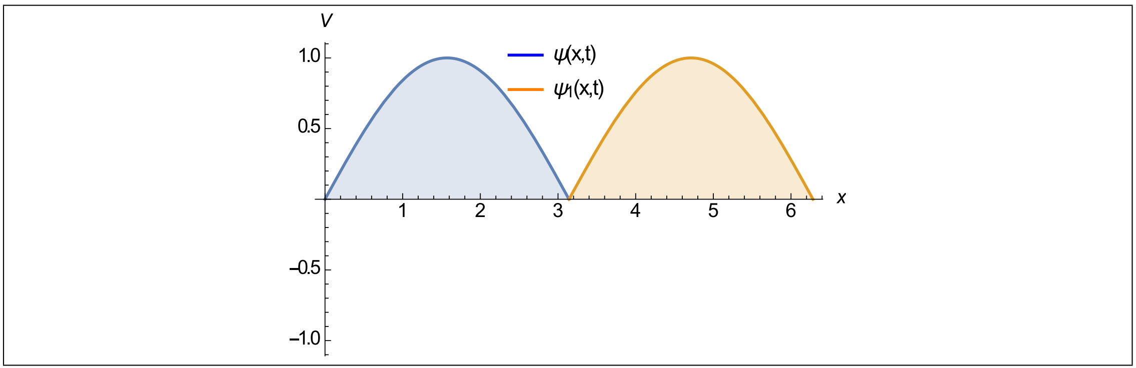

Figure 1.3: Two wave functions $\Psi(x,t)$ and $\Psi_1(x,t)$, which are mutually exclusive to each other.

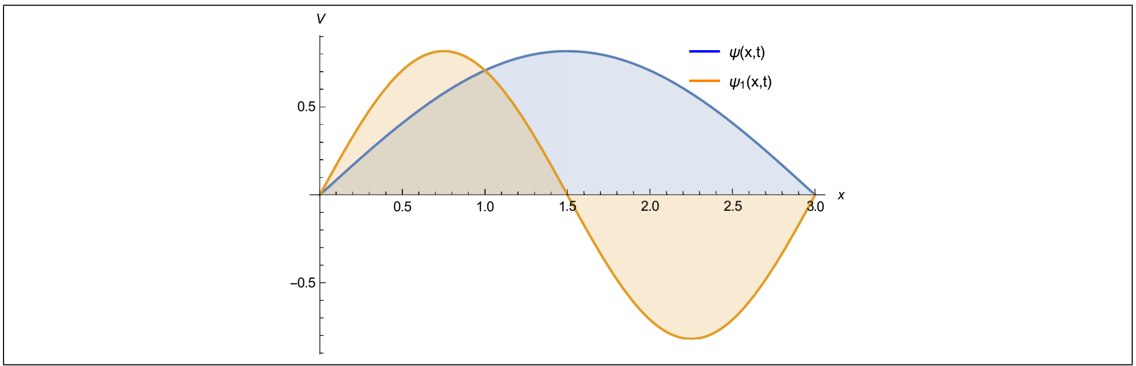

Figure 1.4: Two wave functions $\Psi(x,t)$ and $\Psi_1(x,t)$, which are mutually exclusive to each other.

physical experiment, such normalized wave function $\overline{\Psi(x,t)}$ is convenient for calculation and this is why quantum physicists usually use wave function in a normalized form.

- Mutually Exclusive: Just like in finite vector space, two vectors v_1 and v_2 are said to be orthogonal to each other if $\langle v_1|v_2\rangle = 0$. In quantum mechanics, two wave functions $\Psi(x,t)$ and $\Phi(x,t)$, which are orthogonal to each other, refer to the mutually exclusive physical states. Finally, this relation can be written as

$$\langle \Psi(x,t)|\Phi(x,t)\rangle = 0. \tag{1.5}$$

Mutually exclusive physical states play an important role in the study of variance-based uncertainty relations. Recently, Maccone and Pati obtained an amended Heisenberg-Robertson uncertainty relations based on the mutually exclusive physical states, for more detail see Chapter 3.

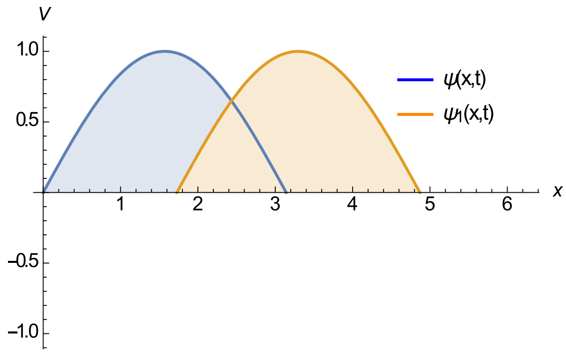

Figure 1.5: Two wave functions $\Psi(x,t)$ and $\Psi_1(x,t)$, which are incompatible to each other.

As shown in FIG. 1.3, if two different intervals do not have any overlap and these two wave functions $\Psi(x,t)$ and $\Phi(x,t)$ are located inside these intervals respectively, that is equivalent to say these wave functions vanish outside their corresponding interval. Thus, wave functions $\Psi(x,t)$ and $\Phi(x,t)$ represent the mutually exclusive possibilities.

Furthermore, the example list above is not the only situation that two physical states can be mutually exclusive. For harmonic oscillator, which has a smooth and symmetrical potential well, consider the ground state $\Psi(x,t)$ and the first excited state $\Phi(x,t)$ for a fixed physical particle at time t. Their inner product is also vanished since one of them is a odd function and the other one is a even function, while the integration is taken on the same interval. See FIG. 1.4 for detail.

- Incompatible: Two physical states $\Psi(x,t)$ and $\Phi(x,t)$ are not multiples of each other, i.e., they have different physical meaning. Meanwhile, they are also not mutually exclusive physical states, i.e., they do not represent mutually exclusive possibilities.

  In FIG. 1.5 and FIG. 1.6, physical states $\Psi(x,t)$ and $\Phi(x,t)$ are incompatible, this is a special relation exist in quantum mechanics. Indeed, the Heisenberg-Robertson uncertainty relation quantitatively formulate the impossibility of jointly sharp preparation of incompatible observables, we will discuss incompatible observables detailedly in Chapter 3 and Chapter 5. While a discernment of the laws of quantum mechanics is undoubtedly necessary in the cause of understanding the microscopic physical world surrounding us, these laws are in contrast with our intuition to some extent.

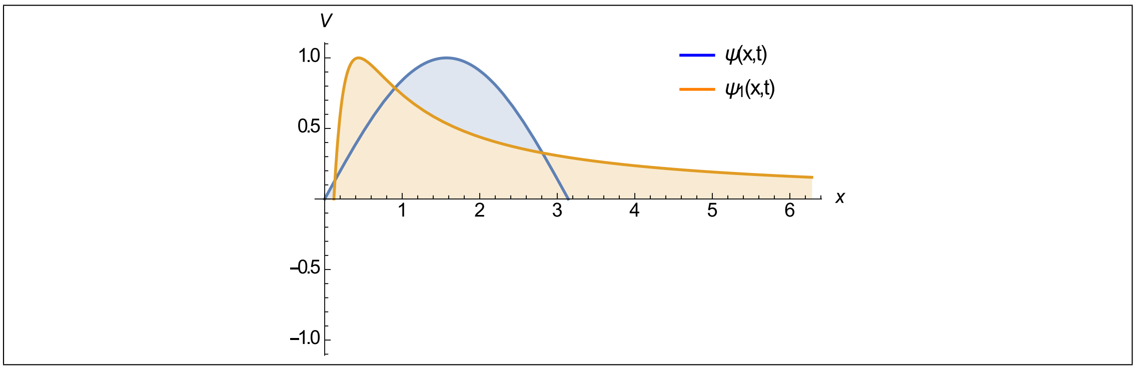

Figure 1.6: Two wave functions $\Psi(x,t)$ and $\Psi_1(x,t)$, which are incompatible to each other.

1.2 Information Theory

Claude Shannon's 1948 paper [Sha01], "Mathematical Theory of Communication", opens a door to a new field that has redefined our world. From R. Fano's words, we know "what made possible, what induced that development of loading as a theory, and the development of very complicated codes, was Shannon's theorem: he told you that is would be done, so people tried to do it". In the begining, research was primarily theoretical. Shannon studied the telegraph communication for the sake of analyzing the abilities and capacities of channels to transmit information. For example, let us first consider the famous story, *Romeo and Juliet*, written by Willian Shakespeare, there has a graceful English text:

- "*Alas that love, whose view is muffled still, Should, without eyes, see pathways to his will!– Where shall we dine?–O me! –What fray was here? Yet tell me not, for I have heard it all. Here's much to do with hate, but more with love:– Why, then, O brawling love! O loving hate! O anything, of nothing first create! O heavy lightness! serious vanity! Mis-shapen chaos of well-seeming forms! Feather of lead, bright smoke, cold fire, sick health! Still-waking sleep, that is not what it is!– This love feel I, that feel no love in this. Dost thou not laugh?*"

Obiously, different alphabet appeared above may not have the same frequency. For example, the alphabet "E" has the highest frequency, which is around 0.1268 and alphabet "T" has the second highest frequency, which is around 0.0978. Following Shannon's original idea, given alphabet E the simplest codes can reduce the complexity of communication and transmit information easily. Back to Shannon's work, who focus on information sources whose probability distribution does not vary with time, i.e. time-independent. He used the terminology "*Entropy*"

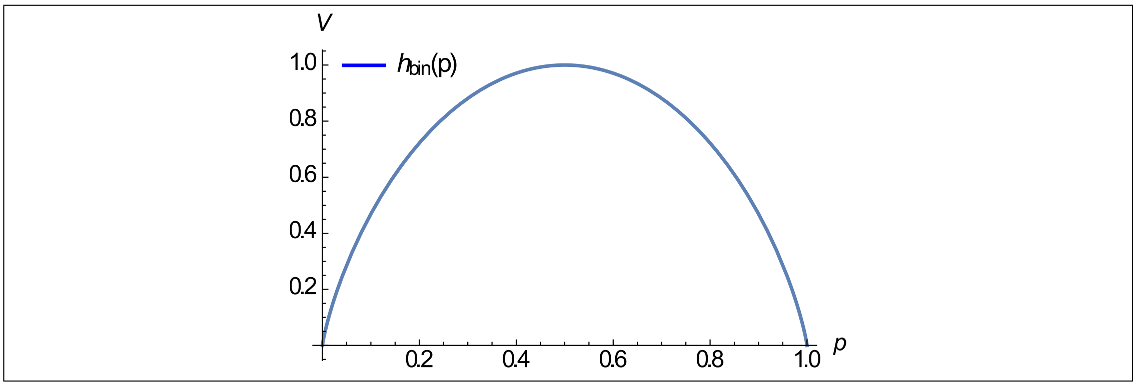

Figure 1.7: Binary Entropy.

to quantify these consideration. For each alphabet, there is a corresponding probability p and assign to them the corresponding numerical value $\log p$, which is defined as *surprisal*. Then the average surprisal of the information sources is the so-called *Shannon Entropy*. More specifically, the Shannon entropy $H(X)$ of a random variable $\mathcal{X}$ with distribution p_X is

$$H(X) := -\sum_{x\in\mathcal{X}} p_{\mathcal{X}}(x)\log p_{\mathcal{X}}(x). \tag{1.6}$$

Furthermore, if the distribution P has finite support, i.e. $P = (p_1, p_2, \cdots, p_n)$, then its Shannon entropy can be written as $H(P)$:

$$H(P) := -\sum_{i=1}^{n} p_i \log p_i, \tag{1.7}$$

which quantifies the average information content of the probability distribution P. Hence, it is a kind of measure of the uncertainty for probability distribution P. Till now, Shannon entropy is still one of the most well-known measure of uncertainty and can be employed to express uncertainty relations. Binary entropy $h_{bin}(p)$ is the simplest entropy, with $0 < p < 1$:

$$h_{bin}(p) := -p\log p - (1-p)\log(1-p), \tag{1.8}$$

and the relation between probability p and the binary entropy $h_{bin}(p)$ is shown in FIG. 1.7.

Even this simplest entropy $h_{bin}(p)$ has been widely used, in the work of optimizing the lower bound of the entropic sum for qubit states, Ghirardi et al. simplified the problem to a single parameter optimization and use binary entropy to express the final formulation.

Information theory is closely connected with a collection of pure theory and applied subject, such as: adaptive system, complex systems, complexity science, machine learning, systems sciences and so on. Consequently, information theory is a broad and deep mathematical formulation theory, it has abundant application while coding theory is one of the most important application.

1.3 Quantum Information Theory

The field of quantum information theory focus on the investigation of the representation, storing, processing and transmitting of information by quantum mechanical systems. One of the first question arises: "Can the entropic formalism of information theory be applied to quantum measurements". Since the measurement in quantum theory is a complete collection of mutually exclusive observations for a fixed quantum state, it is natural to extend *Shannon Entropy* to quantum formalism, *von Neumann Entropy*. Hence, the information theoretic tasks can also be generalized to the quantum cases. The von Neumann entropy of a fixed quantum system A can be defined as

$$S(A) := -\operatorname{Tr}(\rho_A \log \rho_A), \tag{1.9}$$

where ρ_A is the density matrix of quantum system A and the notation Tr denotes the trace of matrix.

In quantum information theory, the physical state of a quantum system can be represented as a positive semi-definite Hermitian operator with trace one in physical Hilbert space. Take an electron with its spin degree of freedom for example, this is a physical state that contains the smallest unit of quantum information–one bit, and can be formulated as a 2×2 positive semi-definite Hermitian matrix. Hence, electron is one physical implementations of the terminology "qubit" in quantum information theory. However, there are other physical supports for "qubit". Polarization is a kind of properties belonged to waves that allowed for osillating with more than one orientation. Light, which is also a kind of electromagnetic waves, has the property of polarization. So polarization encoding is another physical support for the terminology "qubit".

Aside from the von Neumann entropy, Wehrl entropy is a type of quasi-entropy in quantum information theory. Consider the Husimi Q representation $Q(x,p)$ of the phase-space quasi-probability distribution, then the *Wehrl Entropy* [Weh78]can be formulated as

$$S_Q := -\int Q(x,p) \log Q(x,p) dx dp, \tag{1.10}$$

this expression is well-defined since the Husimi Q representation $Q(x, p)$ stays non-negative.

Roughly speaking, quantum information theory is a luxuriant subject and deals with three main topics:

- Transfer of information over quantum channel: In mathematical point of view, quantum channels are completely positive trace-preserving (CPTP) map between spaces of operators. Compare with classical channels which can only transmit or store classical information like bit or mail, quantum channels can transfer both classical information and quantum information. In physical experiment, quantum channel can be realized as optical fibers or coupled spin chains. If someone transform a qubit to someone else and the transmitting procedure is not perfect: due to the perturbations coming from environment, we will call it *noisy channel* in quantum information theory.

- Tradeoff between procurement of information and disturbance of a quantum state: For example, under the quantum cryptography protocol of BB84 [BB84], developed by Charles Bennett and Gilles Brassard in 1984, Alice want to send one of four possible quantum states to Bob

$$|\uparrow_z\rangle,\ |\downarrow_z\rangle,\ |\uparrow_x\rangle,\ |\downarrow_x\rangle, \tag{1.11}$$

  while Eve tries to eavesdrop their communication, then Alice and Bob should check whether their quantum states have been perturbed by Eve's attempt to eavesdrop. And this is the connection with quantum key distribution.

- Quantum entanglement criterion: First of all, we shall know the formal definition of the terminology "entanglement": all quantum states that do not separable are called entangled. In the bipartite case, there are many separability criteria: (1). In 1996, Peres [Per96] proved the *Positive Partial Transpose Criterion* (PPT), and due to mathematical fact, PPT condition is both necessary and sufficient condition for separability if the bipartite quantum states are of form $2 \otimes 2$ or $2 \otimes 3$; (2). Positive but not completely positive map, this is the natural extension of PPT condition since PPT is a special case of P (positive) but not CP (completely positive) map; (3). Another fundamental tool is entanglement witness, and the core idea comes from geometry; (4). Entanglement detection using majorization bounds, which was first introduced by M. H. Partovi [Par12] and can be extended to a majorization-based uncertainty relations [FGG13, PRŻ13, RPŻ14, XJLJF16a].

Entanglement is also considered to be the most nonclassical (or nonlocal) feature in quantum information theory, and it plays an important role in many respects of quantum information and quantum computation, including linear optics quantum computing, measurement-based schemes and so on. Moreover, entanglement gives physicists whole new insights for the comprehension of many phenomena such as super-conductivity and super-radiance.

1.4 Uncertainty Principle and Guessing Game

Heisenberg's Uncertainty Principle [Hei27] has redefined our understanding of the physical system around us. Compare with classical mechanics, the most revolutionary change in human's cognition is that the microcosmos (world of particles like electron, photon and so on) can not be precisely predicted. Historically, while working on the mathematical foundation of quantum mechanics. Werner Heisenberg realized the uncertainty principle: incompatible observables (like the well-known position-momentum uncertainty relation) implies the uncertainty relation. This phenomena coincide with clear physical interpretation for incompatiblility and also laid the foundation for quantum mechanics. In March 1926, Heisenberg wrote:

"It can be expressed in its simplest form as follows: One can never know with perfect accuracy both of those two important factors which determine the movement of one of the smallest particles–its position and its velocity. It is impossible to determine accurately both the position and the direction and speed of a particle at the same instant."

There has two different problems we need to note, first Heisenberg uncertainty principle is different from the so-called *observer effect*. In experimental science, observer effect attempts to vary the action of observation and then will influence the result being observed. According to error estimation, it is a matter of the instruments and experimental error. Uncertainty principle and observer effect are different from each other constitutionally. Second, recently there are widely publicized postulates of a refutation of the uncertainty relation introduced by Heisenberg, these topics includes the joint measurability and measurement-disturbance. In 2013, Busch, Lahti and Werner gave the proof of Heisenberg's Error-Disturbance Relation, through their paper, measures of error and disturbance are defined as the figures of merit characteristic of measuring devices. For the imprecisions of any joint measurement of both position observable and momentum observable, their inequality (uncertainty relation) is still state independent. This debate starts from the experimental realization of Kennard-

Weyl-Robertson inequality

$$\Delta Q \Delta P \geq \frac{\hbar}{2}, \tag{1.12}$$

where ΔQ and ΔP represents the standard deviation of the position and momentum distribution for some fix quantum state and $\hbar$ is the reduced Planck constant. Meanwhile, in Heisenberg's celebrated paper "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik" [Hei27], he established expression as the minimum amount of unavoidable numerical value for the momentum disturbance caused by the observation of position and vice versa. Note that, Heisenberg never gave any precise definition for the variances of position ΔQ and the momentum ΔP, instead, he just gave some plausible estimation. For more discussion on this topic, see Busch *et al*'s remarkable paper "Proof of Heisenberg's Error-Disturbance Relation" [BLW13].

The uncertainty relation we consider above is the *preparation uncertainty relation* which states that it is impossible to prepare a quantum state that has a sharply defined result for incompatible observables, such as position and momentum measurement. To simulate the experimental operation, assume there is a source that consistently distributes copies of particles. For each of the particle, we randomly measure its position Q and momentum P, here we should mention that the incompatible observables can not be measured simultaneously. After the measurement, we observe the result and record numerical value corresponding to each observable respectively. Following Heisenberg's uncertainty principle, we know it is impossible to predict both outcome of the position measurement and the momentum measurement precisely, at least one of them is unpredictable. Moreover, quantum theory allow for mathematical formulation of Heisenberg's uncertainty principle and the corresponding quantitative expressions are the well-known uncertainty relations.

Quantitative Formulations

In 1927, the first quantitative formulation for incompatible observables (the position Q and the momentum P), which is also rigorously proven, was introduce by Kennard [Ken27] (see also the work of Weyl [Wey27]), it states that

$$\sigma_Q \sigma_P \geq \frac{\hbar}{2}, \tag{1.13}$$

where σ_Q and σ_P denotes the standard deviation of position and momentum respectively and $\hbar$ is the celebrated reduced Planck constant. More generally, Heisenberg's uncertainty principle can be applied to any pair of incompatible observables M_1 and M_2 ($[M_1, M_2] \neq 0$), Robertson showed that [Rob29], for observables with bounded spectrum, the following statement is valid,

$$\sigma_{M_1}\sigma_{M_2} \geq \frac{1}{2} \mid \langle\Psi|[M_1, M_2]|\Psi\rangle \mid, \tag{1.14}$$

for fixed quantum state $|\Psi\rangle$ and $[\cdot,\cdot]$ denotes the commutator of operators. All these formulation of uncertainty relations give us an intrinsical insight of measurement and uncertainty principle, while on the other hand, in the experimental concerning these Kennard-Weyl-Robertson inequality, no physical particle can be measured with both a position and a momentum observable. In other word, this formulation of Heisenberg's uncertainty principle has a inevitable defect. For preparation uncertainty relation, P. Busch, P. Lahti and R. F. Werner find out a method to prove the modificatory error-disturbance relation [BLW13]. From Kennard-Weyl-Robertson uncertainty relation, the standard deviation

$$\Delta_\rho(A) := [\mathrm{Tr}(\rho A^2) - (\mathrm{Tr}\,\rho A)^2]^{1/2}, \tag{1.15}$$

for position Q and momentum P are determined in experiment with the same source. Define the new quantity $\Delta(Q, Q')$ (also known as microscope resolution) as a figure of merit for the device and can be verified by a physical laboratory.

For arbitrary distribution and a fixed numerical value ξ, take the root mean square deviation from such ξ, we have

$$D(\rho, Q'; \xi) := \langle(q' - \xi)^2\rangle^{1/2}_{\rho,Q'}, \tag{1.16}$$

where $\langle\cdot,\cdot\rangle$ denotes the expectation of the indicated function of the output q', in the distribution derived by quantum state ρ with device Q' (a general positive operator valued measurement), hence the "uncertainty metrics" can be defined as

$$\Delta_C(Q, Q') := \lim_{\varepsilon\to 0} \sup \{D(\rho, Q'; \xi)|\rho, \xi : D(\rho, Q'; \xi) \leq \varepsilon\}\,. \tag{1.17}$$

With above definitions and settings, the main result of Busch-Lahti-Werner uncertainty relation can be stated as: Assume observables Q' and P' are the marginal observables of some joint measurement observable M with finite calibration error. Then following error-disturbance uncertainty relation holds

$$\Delta_C(Q, Q')\Delta_C(P, P') \geq \frac{\hbar}{2}, \tag{1.18}$$

the quality can be obtained if and only if the joint distribution (p, q) for joint measurement observable M is Husimi distribution.

Recently, with the rise of quantum information theory, quantum uncertainty can be applied to new applications such as quantum cryptography and quantum key distribution. Since both quantum cryptography and quantum key distribution have already been commercially marketed and its strong dependence on uncertainty relations promote the need for information theoretical formulation of uncertainty relation.

Aside from the variance-based uncertainty relations, like Kennard-Weyl-Robertson inequality and Busch-Lahti-Werner inequality, there are other way to formulate the uncertainty principle. Suppose we have prepared a quantum state ρ on which we can use incompatible observables M_m to measure it. By using the label x to denote the result of the measurement, we can get a probability distribution

$$P = (p(x|M_m))_{x,m}, \tag{1.19}$$

where each quantity $p(x|M_m)$ stand for the probability of deriving the outcome x with measurement M_m (may be two measurements or more).

Needless to say, information theory offers a wide variety of mathematical tool for formulating uncertainty relations based on $(p(x|M_m))_{x,m}$. Note that we should find mathematical tool from information theory, since it is the foundation of modern communication and cryptography technologies. Further, parts of the technologies of information theory has already been generalized to the quantum theory. Back to the topic, entropy is the preferred, maybe not the best, mathematical function to quantify uncertainty and formulate uncertainty relations. Among all kinds of entropies, we should pay attention to several prominent entropies. First one is the *Boltzmann Entropy*, it is a kind of statistical entropy which was first introduced by Ludwig Boltzmann in classical statistical mechanics. Its quantum generalization, von Neumann entropy, has also been widely used in quantum information theory. Based on the extension of various information-theoretic notions, new uncertainty measure, smooth min-entropy and max-entropy has also been defined.

Everett first aware of the question "Can the uncertainty principle be formulated by entropy?" in 1957 [EI57]. In the same year, Hirschman formulated the uncertainty relation for incompatible observables, position and momentum, by differential entropy [Hir57], and this is the first entropic uncertainty relation in history. Later, Hirschman's expression had been improved by Beckner and Białynicki-Birula and Mycielski [BBM75], who showed the following form

$$h(Q) + h(P) \geq \log \pi e, \tag{1.20}$$

here $\hbar = 1$ and h is the differential entropy: assume a random variable Q has been governed by a probability distribution $f(x)$, then the corresponding differential entropy can be defined as

$$h(Q) := -\int_{-\infty}^{\infty} f(x) \log f(x) dx. \tag{1.21}$$

Guessing Game

More generally, D. Deutsch [Deu83] extends the entropic uncertainty relation to arbitrary incompatible observables with finite spectrum. And the improvement for entropic uncertainty relations and variance-based uncertainty relations is the main topic of this thesis. Besides the semi-classical description of uncertainty principle, we will introduce the modern formulation of the uncertainty principle, which is the so-called guessing game (also known as the *uncertainty game*), which highlights its relevance with quantum cryptography. We can imagine there are two observers, Alice and Bob. Before the game initiates, they agree on two measurements M_1 and M_2. The guessing game proceeds as follows: Bob, can prepare an arbitrary state ρ_A which he will send to Alice. Alice then randomly chooses to perform one of measurements and records the outcome. After telling Bob the choices of her measurements, Bob can win the game if he correctly guesses Alice's outcome. Nevertheless, the uncertainty principle tells us that Bob cannot win the game under the condition of incompatible measurements.

What if Bob prepares a bipartite quantum state ρ_{AB} and sends only one particle A to Alice? Equivalently, what if Bob has nontrivial *quantum side information* about Alice's system? Or, what if all information Bob has on the particle ρ_A is beyond the classical description, for example, information on its density matrix? Berta *et al.* [BCC+10] have answered these questions and generalized Maassen and Uffink's uncertainty relation [MU88] to the case with an auxiliary quantum system B which is also known as quantum memory. It is now possible for Bob to experience no uncertainty at all when equipped himself with quantum memory. For more details see Chapter 5.

Proof of Kennard's Formulation

Before the end of this section, we want to give a rigorous proof of Kennard's formulation of uncertainty relation with the usage of *Robertson's Inequality* and the *Schrödinger Equation*. Recall the statistical interpretation of a wave function $\Psi(x,t)$, we know the expectation value of position x is

$$\langle x \rangle = \int_{-\infty}^{\infty} x \mid \Psi(x,t) \mid^2 dx, \tag{1.22}$$

the physical meaning of the expectation value is the average of repeated measurements on an ensemble of identically prepared systems. Then we can calculate the expectation value of speed–"velocity".

$$\frac{\partial \langle x \rangle}{\partial t} = \int_{-\infty}^{\infty} x \frac{\partial}{\partial t} \mid \Psi(x,t) \mid^2 dx, \tag{1.23}$$

here $\mid \Psi(x,t) \mid^2 = \Psi^*\Psi$ with Ψ^* denotes the conjugate of wave function Ψ. From *Schrödinger Equation*, we have that

$$\frac{\partial \Psi}{\partial t} = \frac{i\hbar}{2m}\frac{\partial^2 \Psi}{\partial x^2} - \frac{i}{\hbar}V\Psi. \tag{1.24}$$

On the other hand, the conjugate of wave function Ψ satisfy

$$\frac{\partial \Psi^*}{\partial t} = -\frac{i\hbar}{2m}\frac{\partial^2 \Psi^*}{\partial x^2} + \frac{i}{\hbar}V\Psi^*, \tag{1.25}$$

by the *Leibniz rule*

$$\frac{\partial \mid \Psi \mid^2}{\partial t} = \Psi^*\frac{\partial \Psi}{\partial t} + \frac{\partial \Psi^*}{\partial t}\Psi. \tag{1.26}$$

Combining with integration-by-parts, we derive

$$\frac{\partial \langle x \rangle}{\partial t} = -\frac{i\hbar}{m}\int_{-\infty}^{\infty} \Psi^* \frac{\partial}{\partial x}\Psi dx. \tag{1.27}$$

Now it is possible to write the momentum p ($p = mv$) as

$$\langle p \rangle = m\frac{\partial \langle x \rangle}{\partial t}. \tag{1.28}$$

Let us rewrite the expression for expectation of position x and momentum p:

$$\begin{aligned}\langle p \rangle &= \int_{-\infty}^{\infty} \Psi^*(\frac{\hbar}{i}\frac{\partial}{\partial x})\Psi dx;\\ \langle x \rangle &= \int_{-\infty}^{\infty} \Psi^*(x)\Psi dx,\end{aligned} \tag{1.29}$$

it is customary to use operator x denote the position and $\frac{\hbar}{i}\frac{\partial}{\partial x}$ to denote momentum. Given a test function $f(x)$, then it is obviously

$$[x,p]f(x) = x\frac{\hbar}{i}\frac{\partial}{\partial x}f(x) - \frac{\hbar}{i}\frac{\partial}{\partial x}(xf(x)) = i\hbar f(x), \tag{1.30}$$

dropping the test function we can derive

$$[x,p] = i\hbar, \tag{1.31}$$

together with *Robertson's Inequality* complete the proof.

1.5 Outline of the Thesis

The target of this thesis is to introduce the framework of uncertainty principle with both the variance-based and entropic formulations, and to delineate the improvement for the framework from our recent work, including the weighted uncertainty relations, mutually exclusive uncertainty relations, improved uncertainty relation in presence of quantum memory, strong entropic uncertainty relations for multi-measurements, uncertainty under quantum measurements and quantum memory. By the way, one of the most important recent advances concerns an extension of the uncertainty relation that allows the measured particle to be connected to its environment in a non-classical way (also known as quantum side information or quantum memory). Clearly, there has a gap between uncertainty relations in presence of quantum memory and uncertainty relations only with classical side information, not only the physical interpretation but also the mathematical expression. This work overcome this gap and generalize all uncertainty relations on Shannon entropies to allow for quantum side information. The focus of this work is thus mainly on the improvement of variance-based uncertainty relation, entropic uncertainty relation and its generalization with quantum side information.

The following is a brief outline of the main results introduced in each chapter.

In Chapter 2, the mathematical notations and the basic expressions of Hilbert space for quantum mechanics are introduced. Related formulations and results of matrix mechanics are outlined in the first half part of chapter 2. Then we briefly review the systematic presentation of the basic principle of quantum theory, along with the knowledge of linear algebra. In the rest part of chapter 2, we introduce the fundamental mathematical language of the information theory–entropy, several properties of entropies has been given and rigorously proved. Showing the foundation of matrix mechanics with linear algebra and giving a collection of properties of entropies are main topics of this chapter.

In Chapter 3, we formally show the variance-based uncertainty relations for product form and sum form. Recent result of uncertainty relations for sum of variance from L. Maccone and A. K. Pati's "Stronger Uncertainty Relations for All Incompatible Observables" [MP14] has been reviewed. In particular, we indicate that it seems unreasonable to assume a priori that both incompatible observables have equal contribution to the variance-based sum uncertainty relation and extend their original form to weighted uncertainty relations. Aside from weighted uncertainty relations, we also explore the application of mutually exclusive physical states and establish the mutually exclusive uncertainty relation.

In Chapter 4, we focus on several criteria for genuine multipartite entanglement based on majorization theory. Under non-negative Schur-concave functions, the vector-type uncertainty relation generates a family of infinitely many detectors to check genuine multipartite entanglement. We also introduce the concept of k-separable circles via geometric distance for probability vectors, which include at most $(k-1)$-separable states. The entanglement witness is also generalized to a universal entanglement witness which is able to detect the k-separable states more accurately. Due to the equivalence between majorization and double stochastic matrix, we can extend our results into matrix form.

In Chapter 5, we introduce a variety of entropic uncertainty relations that give lower bounds on the uncertainty of the outcome of two (or more) incompatible observables. Here we summarize some recent advances in the field and study entropic uncertainty relations on a finite-dimensional Hilbert space. Moreover we provide several tighter bounds for multi-measurements and in presence of quantum memory, corresponding *Information Exclusion Relations* have been also strengthened. We extend all uncertainty relations on Shannon entropies to allow for quantum side information, providing lower bounds on the uncertainties which depends on the amount of entanglement between measured particle and quantum memory. Furthermore, we detail our results to witnessing entanglement in absence of quantum side information.

The thesis ends with Chapter 6 in a short conclusion and outlook. Some potential applications and open questions are discussed.

Chapter 2

Preliminaries

This chapter contains the preliminaries of introductory notation, basic knowledge from linear algebra which will be used in quantum information theory, and some mathematical tools (such as entropy) which are needed in constructing uncertainty relations. The first section appeared in this chapter will introduce the mathematical foundations of Hilbert space in finite dimensions. For later use, we cover the fundamentals of linear algebra and a mathematical formulation of quantum mechanics in the following sections. Next, we describe the state and measurement in quantum systems. Further, we examine and discuss the entropic inequalities which is the fundamentals of later chapters. Finally, we note that this chapter is based on many well-known introductory books on linear algebra, matrix analysis and quantum information theory. For linear algebra and matrix analysis, the preliminaries mostly base on *Matrix Analysis* [HJ12] and *Topics in Matrix Analysis* [HJ91] by Roger A. Horn, *Matrix Analysis* [Bha13] and *Positive Definite Matrices* [Bha09] by Rajendra Bhatia. Moreover, John Watrous's *Theory of Quantum Information* [Wat11], Nilsen and Chuang's *Quantum Computation and Quantum Information* [NC10] and Masahito Hayashi's *Quantum Information: An Introduction* [Hay06] are invaluable books for related topics in quantum information theory.

2.1 Hilbert Spaces

Quantum information theory offers a framework that allow us to treat information-theoretic processing in quantum mechanics, in order to do so it is necessary to mathematically formulate basic concepts like quantum systems, quantum states, measurements and so on. First of all, we use Hilbert space $\mathcal{H}$ to describe the quantum system, which is also called as the representation space. Hilbert space, which is named after David Hilbert, generalizes the notion of Euclidean space.

Definition 2.1.1. (Pre-Hilbert Space). A vector space V over field $\mathbb{K}$ ($= \mathbb{R}$ or $\mathbb{C}$) together with a map (inner product)

$$\langle \cdot, \cdot \rangle : V \times V \longrightarrow \mathbb{K}, \tag{2.1}$$

satisfying (for any vectors x, y, $z \in V$ and $\lambda \in \mathbb{K}$)

1. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$,
2. $\langle \lambda x, y \rangle = \lambda \langle x, y \rangle$,
3. $\langle x, y \rangle = \overline{\langle y, x \rangle}$,
4. $\langle x, x \rangle \geq 0$ with equality $\langle x, x \rangle = 0$ if and only if $x = 0$.

For the first three properties, we can also derive:

1. $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$,
2. $\langle x, \lambda y \rangle = \overline{\lambda} \langle x, y \rangle$.

The inner product $\langle \cdot, \cdot \rangle$ on Pre-Hilbert space V gives rise to the concept of norm, which can be defined as

$$\| x \| = \sqrt{\langle x, x \rangle}. \tag{2.2}$$

Then based on the definition of the norm and the Pre-Hilbert space, we can define the concept of Hilbert space.

Definition 2.1.2. (Hilbert Space). If a Pre-Hilbert space is complete in this norm, in other words, the Cauchy sequences with respect to the given norm are convergent, then we will call it Hilbert space.

Next, we introduce some examples for Hilbert space:

1. Vector space $\mathbb{R}^n$ with the inner product

$$\langle x, y\rangle = \sum_{j=1}^{n} x_j y_j, \tag{2.3}$$

is a Hilbert space over field $\mathbb{R}$ with $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$.

2. Vector space $\mathbb{C}^n$ with the inner product

$$\langle x, y\rangle = \sum_{j=1}^{n} x_j \overline{y_j}, \tag{2.4}$$

is a Hilbert space over field $\mathbb{C}$ with $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$.

3. l^2, the space of square-summable sequences, with the inner product

$$\langle x, y\rangle = \sum_{j=1}^{\infty} x_j \overline{y_j}, \tag{2.5}$$

is a Hilbert space over field $\mathbb{C}$ with $x = \{x_j\}_{j=1}^{\infty}$ and $y = \{y_j\}_{j=1}^{\infty}$.

4. $L^2[a, b]$ is a Hilbert space with the inner product

$$\langle f, g\rangle = \int f\overline{g}dx, \tag{2.6}$$

with the integral to be taken over the appropriate domain. More generally, we consider norms defined as follow, let $1 \leq p < \infty$ and set (S, Σ, μ) as a measure space. Consider the vector space with the norm

$$\| f \|_p = (\int_S | f |^p \, d\mu)^{\frac{1}{p}} < \infty. \tag{2.7}$$

5. Another example of Hilbert space is the space of square-integrable complex-valued functions on $\mathbb{R}$, that is, $L^2(\mathbb{R})$ of all functions $f : \mathbb{R} \to \mathbb{C}$ with

$$\int_{-\infty}^{\infty} dx \, | f(x) |^2 < \infty. \tag{2.8}$$

In mathematics, the concept "Hilbert Space" is often reserved for the infinite-dimensional inner product space with the property of completeness. However, for physics the term is often used in a way that includes finite-dimensional cases. Surprisingly, the term "Hilbert Space" was first given by von Neumann, instead of David Hilbert, in order to consolidate the mathematical foundation of quantum mechanics. For more details, see [Hal73, HB82, Jam66, Lan05, Mac00, MR88].

Historically, Werner Heisenberg first formulates the quantum theory into the so-called "Matrix Mechanics". To understand the basic idea of Heisenberg, note that the physical observables for particles may depend on continuous quantities, such as position Q and momentum P, but can also rely on the discrete quantities, such as the natural numbers $n = 1, 2, \cdots$. Based on these ideas, Heisenberg replaced the functions with variables of position Q and momentum P, $f(Q, P)$, by new formulations $f(m, n)$ where both m and n are natural numbers. In classical mechanics, the multiplication rule is commutative but now it changes, $f \circ g(m, n) = \sum_l f(m, l)g(l, n)$ which is similar to the multiplication of matrices, and this is the birth of "Matrix Mechanics" for quantum theory. On the other hand, Erwin Schrödinger based his work on de Broglie's idea to construct the celebrated Schrödinger Equation with Ψ denoting the "Wave Function", and this is the formulation of "Wave Mechanics". These two alternative expressions of quantum theory looked totally different, but each of them could explain certain phenomena about the particle. For more detail, Heisenberg's formulation focus on the physical observables while Schrödinger's expression describe the quantum states lacking the description of physical observables. To fix this defect, Schrödinger introduced the well-known operators Q and P satisfying

$$\begin{aligned} Q\Psi(x) &= x\Psi(x), \\ P\Psi(x) &= \frac{\hbar}{i}\frac{\partial}{\partial x}\Psi(x). \end{aligned} \tag{2.9}$$

which had also been introduced in Chapter 1. Now it is clear that both Q and P are unbounded operators on Hilbert space $L^2(\mathbb{R}^3)$. By the way, the vectors in l^2 on which Heisenberg's matrices worked on could be seen as quantum states. In order to study the relation between Heisenberg's "Matrix Mechanics" and Schrödinger's "Wave Mechanics", von Neumann define the mathematical concept of Hilbert space. In his mathematical construction of quantum theory, Schrödinger's "Wave Function" Ψ is a unit vector from the Hilbert space $L^2(\mathbb{R}^3)$, while on the other hand, Heisenberg's observable is linear operator which acts on the Hilbert space l^2. Now the Riesz-Fischer theorem implies the equivalence between these alternative formulations of quantum theory.

Theorem 2.1.3. *(Riesz-Fischer). Given any sequence (c_k) of real (or complex) numbers and any orthonormal system (e_k) in $L^2(a, b)$, there exist a function $f \in$*

$L^2(a,b)$ for which $\langle e_k, f\rangle = c_k$ if and only if $c_k \in l^2$, in other words, if $\sum_k \mid c_k \mid^2 < \infty$.

The following two theorems are very useful:

Theorem 2.1.4. *(Cauchy-Schwarz Inequality). Let $\mathcal{H}$ be a Hilbert space with inner product $\langle\cdot,\cdot\rangle$, then for any vectors $x, y \in \mathcal{H}$, we have*

$$\mid \langle x,y\rangle \mid \leq \parallel x \parallel \parallel y \parallel, \tag{2.10}$$

where the equality holds if and only if x and y are linear dependent.

Proof. If $y = 0$, then clearly the inequality holds. Assume y is nontrivial, first consider the case $x = \alpha y$ for some $\alpha \in \mathbb{C}$, then $\langle x, y\rangle = \alpha \parallel y \parallel^2$ and thus we can derive

$$\mid \langle x,y\rangle \mid = \mid \alpha \mid \parallel y \parallel^2 = \parallel x \parallel \parallel y \parallel . \tag{2.11}$$

Next, consider the case $x \in \mathcal{H}$ is arbitrary, set $z := x - \parallel y \parallel^{-2} \langle x,y\rangle y$, then from $\parallel z \parallel^2 \geq 0$ together with the fact

$$\parallel z \parallel^2 = \parallel x \parallel^2 - \frac{\mid \langle x,y\rangle \mid^2}{\parallel y \parallel^2}, \tag{2.12}$$

implies the result with equality if and only if $x = \parallel y \parallel^{-2} \langle x,y\rangle y$ (i.e. $z = 0$). ■

Theorem 2.1.5. *(Parallelogram Law). Let $\mathcal{H}$ be a Hilbert space with inner product $\langle\cdot,\cdot\rangle$, then for any vectors $x, y \in \mathcal{H}$, we have*

$$\parallel x + y \parallel^2 + \parallel x - y \parallel^2 = 2 \parallel x \parallel^2 + 2 \parallel y \parallel^2 . \tag{2.13}$$

Proof. For simplicity, assume the Hilbert space $\mathcal{H}$ is a complex Hilbert space. Then we obtain

$$\begin{aligned}\parallel x + y \parallel^2 + \parallel x - y \parallel^2 &= \parallel x \parallel^2 + \parallel y \parallel^2 + 2Re\langle x,y\rangle + \parallel x \parallel^2 + \parallel y \parallel^2 - 2Re\langle x,y\rangle \\ &= 2 \parallel x \parallel^2 + 2 \parallel y \parallel^2 . \end{aligned} \tag{2.14}$$

Now we obtain the desired equality. ■

2.2 Density Matrix

Quantum states can be described by the state vector $|\psi\rangle$ on Hilbert space, and it can be divided into pure states and mixed states. The concept "Density Matrix" is very important for quantum information theory and it encodes all information about a quantum system into a matrix. More detailed discussion about the related topics will be shown in this section.

Probability Density

A quantum system is said to be in a pure state if we know all the information about the quantum system, in other words, we know exactly which state it is in. It is quite different from mixed states, a quantum system is in a mixed state if we only obtain part of the information about the quantum system. In terms of density matrix, mixed states mean more than one eigenvalues must be nontrivial.

Consider a quantum system in a pure state $|\psi\rangle$ with an observable A, then the physical expectation value is given by

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle, \tag{2.15}$$

hence the following definition of density matrix for pure state is straightforward:

Definition 2.2.1. (Density Matrix for Pure State). The density matrix ρ for the pure state $|\psi\rangle$ is given by

$$\rho := |\psi\rangle\langle\psi|. \tag{2.16}$$

According to the definition of density matrix for pure states, we can derive

Theorem 2.2.2. *The density matrix ρ for the pure state $|\psi\rangle$ has the following properties:*

1. *Projection:* $\rho^2 = \rho$;
2. *Positivity:* $\rho \geq 0$;
3. *Hermiticity:* $\rho^\dagger = \rho$;
4. *Normalization:* $\mathrm{Tr}\,\rho = 1$.

Proof. Write the density matrix as operator $|\psi\rangle\langle\psi|$, then it is clear

$$\rho^2 = |\psi\rangle\langle\psi||\psi\rangle\langle\psi| =\| \, |\psi\rangle \, \|^2 \, |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{2.17}$$

To prove the property of positivity, we can choose arbitrary vector $|\phi\rangle$ in Hilbert space, then the following inequality

$$\langle\phi|\rho|\phi\rangle = \langle\phi|\psi\rangle\langle\psi|\phi\rangle =| \, \langle\phi|\psi\rangle \, |^2 \geq 0, \tag{2.18}$$

implies the positivity.

The conjugate transpose of density matrix is given by

$$\overline{|\psi\rangle\langle\psi|} = |\psi\rangle\langle\psi| = \rho, \tag{2.19}$$

this equivalence yields the Hermiticity.

If $\rho = |\psi\rangle\langle\psi|$, then

$$\mathrm{Tr}(|\psi\rangle\langle\psi|) = \mathrm{Tr}(\langle\psi|\psi\rangle) = 1, \tag{2.20}$$

which completes the proof. ∎

For a quantum system, a description for the present condition of the system is called a quantum state, such as the direction of "spin" in a spin-$\frac{1}{2}$ system. Any quantum state can be described by density matrix.

Definition 2.2.3. (Density Matrix). Any Hermitian matrix ρ satisfying

1. Positivity: $\rho \geq 0$;
2. Normalization: $\mathrm{Tr}\,\rho = 1$,

is called a density matrix (or probability density).

What we still need to ensure is that the physical expectation value $\langle A\rangle_\psi$ for a quantum state $|\psi\rangle$ with observable A can be reproduced by the term of density matrix.

Theorem 2.2.4. *(Expectation Value). The physical expectation value for a density matrix ρ with an observable A is given by*

$$\langle A\rangle_\rho = \mathrm{Tr}(\rho A) = \langle A\rangle_\psi. \tag{2.21}$$

Proof. Choose an orthonormal basis $\{|e_i\rangle\}$, then we have

$$\begin{aligned}\langle A\rangle_\rho &= Tr(\rho A) = Tr(|\psi\rangle\langle\psi|A) = \sum_i \langle e_i|\psi\rangle\langle\psi|A|e_i\rangle \\ &= \sum_i \langle\psi|A|e_i\rangle\langle e_i|\psi\rangle = \langle\psi|A\sum_i |e_i\rangle\langle e_i|\psi\rangle = \langle\psi|A|\psi\rangle = \langle A\rangle_\psi.\end{aligned} \tag{2.22}$$

∎

Pure States and Mixed States

Now we focus on the concepts of pure states and mixed states, let us start with the pure state, given an ensemble of quantum states $\{|\psi_i\rangle\}$, if all objects are in the same fix state, then the quantum state is said to be in a pure state. Besides the basic definition of pure state, we also need to study the probability distribution with observable A. Note that an observable A is an Hermitian operator, we write its spectral decomposition

$$A|e_i\rangle = a_i|e_i\rangle, \qquad a_i \in \mathbb{R} \tag{2.23}$$

furthermore, we can expand the pure state $|\psi\rangle$ with respect to the observable A as

$$|\psi\rangle = \sum_i c_i|e_i\rangle. \tag{2.24}$$

Thus, it is possible to derive the expectation value of observable A by

$$\langle A\rangle_\psi = \langle\psi|A|\psi\rangle = \sum_i a_i \mid c_i \mid^2, \tag{2.25}$$

with $\mid c_i \mid^2$ denotes the probability for obtaining the eigenvalue a_i.

Next, consider an ensemble $\{|\psi_i\rangle\}$ with the probability p_i to find the quantum state $|\psi_i\rangle$ ($\sum_i p_i = 1$), thus the quantum state is mixed states and can be written as a convex sum

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{2.26}$$

Theorem 2.2.5. *The expectation value of a mixed state ρ can be given by*

$$\langle A\rangle_\rho = \mathrm{Tr}(\rho A) = \sum_i p_i\langle\psi_i|A|\psi_i\rangle. \tag{2.27}$$

Proof. Choose an orthonormal basis $\{|e_j\rangle\}$, then we have

$$\begin{aligned}
\mathrm{Tr}(\rho A) &= \mathrm{Tr}(\sum_i p_i|\psi_i\rangle\langle\psi_i|A) \\
&= \sum_j \langle e_j| \sum_i p_i|\psi_i\rangle\langle\psi_i|A|e_j\rangle \\
&= \sum_{i,j} p_i\langle e_j|\psi_i\rangle\langle\psi_i|A|e_j\rangle \\
&= \sum_{i,j} p_i\langle\psi_i|A|e_j\rangle\langle e_j|\psi_i\rangle \\
&= \sum_i p_i\langle\psi_i|A\sum_j |e_j\rangle\langle e_j|\psi_i\rangle \\
&= \sum_i p_i\langle\psi_i|A|\psi_i\rangle.
\end{aligned} \tag{2.28}$$

■

Time Evolution

Just as the *Schrödinger Equation* describes the motion of pure state $|\psi\rangle$ with time variable, the *von Neumann Equation* describes time evolution of density matrix. Moreover, the *von Neumann Equation* is the quantum formulation of classical *Liouville Equation*, so we can also call it *Liouville-von Neumann Equation.*

Theorem 2.2.6. *(Time Evolution). The time evolution of the density matrix* ρ *can be given as*

$$i\hbar\frac{\partial}{\partial t}\rho = [H,\rho], \tag{2.29}$$

which is the so-called von Neumann Equation.

Proof.

$$\begin{aligned}
i\hbar\frac{\partial}{\partial t}\rho &= i\hbar\frac{\partial}{\partial t}\left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)\\
&= i\hbar\sum_i p_i\frac{\partial}{\partial t}(|\psi_i\rangle\langle\psi_i|)\\
&= i\hbar\sum_i p_i[(\frac{\partial}{\partial t}|\psi_i\rangle)\langle\psi_i| + |\psi_i\rangle(\frac{\partial}{\partial t}\langle\psi_i|)]\\
&= \sum_i p_i[(i\hbar\frac{\partial}{\partial t}|\psi_i\rangle)\langle\psi_i| - |\psi_i\rangle(-i\hbar\frac{\partial}{\partial t}\langle\psi_i|)],
\end{aligned} \tag{2.30}$$

according to the time dependent *Schrödinger Equation*

$$i\hbar\frac{\partial}{\partial t}|\psi_i\rangle = H|\psi_i\rangle, \tag{2.31}$$

and its conjugate

$$-i\hbar\frac{\partial}{\partial t}\langle\psi_i| = \langle\psi_i|H, \tag{2.32}$$

we can obtain

$$\begin{aligned}
i\hbar\frac{\partial}{\partial t}\rho &= \sum_i p_i(H|\psi_i\rangle\langle\psi_i| - |\psi_i\rangle\langle\psi_i|H)\\
&= \sum_i p_i[H,|\psi_i\rangle\langle\psi_i|]\\
&= [H,\rho].
\end{aligned} \tag{2.33}$$

■

Qubit and Pauli Matrices

After introducing the concepts of density matrices, pure states and mixed states, it is time to describe the quantum system with a two-dimensional representation space which is also called qubit. Mathematically, the spin-$\frac{1}{2}$ system is a special case of quantum two-level system. In particular, the Hermitian matrices σ_0, σ_x, σ_y and σ_z together are called *Pauli Matrices*:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.34}$$

With the help of Pauli matrices, any density matrix of qubit can be expressed as

$$\rho = \frac{1}{2}(\sigma_0 + \overrightarrow{r} \cdot \overrightarrow{\sigma}), \tag{2.35}$$

which is called *Stokes Parameterization*. Here $\overrightarrow{\sigma}$ stands for $(\sigma_x, \sigma_y, \sigma_z)$ and $\overrightarrow{r}$ is a vector inside the unit ball of $\mathbb{R}^3$. Due to the fact that Pauli matrices can simplify calculation, it is necessary to introduce some algebraic properties of Pauli matrices.

Each one of Pauli matrices σ_x, σ_y, σ_z is involutory and traceless, with determinant -1.

- $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$;
- $\det \sigma_x = \det \sigma_y = \det \sigma_z = -1$;
- $\operatorname{Tr} \sigma_x = \operatorname{Tr} \sigma_y = \operatorname{Tr} \sigma_z = 0$.

From above algebraic properties of Pauli matrices, we find out that the eigenvalues of σ_x, σ_y and σ_z are $+1$ and -1, and the corresponding normalized eigenvectors can be listed as

$$\begin{aligned} \sigma_x e_{x+} &= e_{x+}, & \sigma_x e_{x-} &= -e_{x-}, \\ \sigma_y e_{y+} &= e_{y+}, & \sigma_y e_{y-} &= -e_{y-}, \\ \sigma_z e_{z+} &= e_{z+}, & \sigma_z e_{z-} &= -e_{z-}, \end{aligned} \tag{2.36}$$

with

$$\begin{aligned} e_{x+} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, & e_{x-} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \\ e_{y+} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, & e_{y-} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \\ e_{z+} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & e_{z-} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \end{aligned} \tag{2.37}$$

The Pauli matrices also obey the commutation and anti-commutation relations:

$$\begin{aligned} [\sigma_a, \sigma_b] &= 2i\epsilon_{abc}\sigma_c, \\ \{\sigma_a, \sigma_b\} &= 2\delta_{ab} I, \end{aligned} \tag{2.38}$$

where ϵ_{abc} is the Levi-Civita symbol and δ_{ab} is the Kronecker delta with I denotes the 2×2 identity. Combining both the commutation relation and anti-commutation relation together, we can obtain

$$\sigma_a\sigma_b = i\epsilon_{abc}\sigma_c + \delta_{ab} I, \tag{2.39}$$

and

$$(\overrightarrow{a} \cdot \overrightarrow{\sigma})(\overrightarrow{b} \cdot \overrightarrow{\sigma}) = (\overrightarrow{a} \cdot \overrightarrow{b}) I + i(\overrightarrow{a} \times \overrightarrow{b}) \cdot \overrightarrow{\sigma}. \tag{2.40}$$

In quantum information theory, the term *Generalized Pauli Matrices*, which refers to the special families of matrices that keep the algebraic property of Pauli matrices, plays an important role. Here we will focus on one of them, *Gell-Mann Matrices*.

Similar to the Pauli matrices, which are the traceless hermitian generators of the Lie algebra $su(2)$, the Gell-Mann matrices are the traceless hermitian generators of the Lie algebra $su(3)$, and can be defined as

$$\begin{aligned}
&\lambda_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\
&\lambda_4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \lambda_5 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \quad \lambda_6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\
&\lambda_7 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \quad \lambda_8 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}.
\end{aligned} \tag{2.41}$$

The Gell-Mann matrices also obey the commutation relation:

$$[\lambda_a, \lambda_b] = 2if_{abc}\lambda_c, \tag{2.42}$$

where $a, b, c \in \{1, 2, \cdots, 8\}$. Now f_{abc} are structure constants of Lie algebra $su(3)$, but much more complicated than the Levi-Civita symbol ϵ_{abc}. Note that all the f_{abc} are anti-symmetric under the action of transposition, and the nontrivial ones can be listed as

$$\begin{aligned}
&f_{123} = 1, \qquad f_{147} = \frac{1}{2}, \qquad f_{156} = -\frac{1}{2}, \\
&f_{246} = \frac{1}{2}, \qquad f_{257} = \frac{1}{2}, \\
&f_{345} = \frac{1}{2}, \qquad f_{367} = -\frac{1}{2}, \\
&f_{458} = \frac{\sqrt{3}}{2}, \\
&f_{678} = \frac{\sqrt{3}}{2}.
\end{aligned} \tag{2.43}$$

Consider the anti-commutation relation for Gell-Mann matrices:

$$\{\lambda_a, \lambda_b\} = 2d_{abc}\lambda_c + \frac{4}{3}\delta_{ab}I, \tag{2.44}$$

where $a, b, c \in \{1, 2, \cdots, 8\}$ and δ_{ab} stands for the Kronecker delta. Here d_{abc} are symmetric under the action of transposition and all the nontrivial one can be listed as

$$\begin{aligned}
&d_{118} = \frac{1}{\sqrt{3}}, \qquad d_{146} = \frac{1}{2}, \qquad d_{157} = \frac{1}{2}, \\
&d_{228} = \frac{1}{\sqrt{3}}, \qquad d_{247} = -\frac{1}{2}, \qquad d_{256} = \frac{1}{2}, \\
&d_{338} = \frac{1}{\sqrt{3}}, \qquad d_{344} = \frac{1}{2}, \qquad d_{355} = \frac{1}{2}, \qquad d_{366} = -\frac{1}{2}, \qquad d_{377} = -\frac{1}{2}, \\
&d_{448} = -\frac{1}{2\sqrt{3}}, \\
&d_{558} = -\frac{1}{2\sqrt{3}}, \\
&d_{668} = -\frac{1}{2\sqrt{3}}, \\
&d_{778} = -\frac{1}{2\sqrt{3}}, \\
&d_{888} = -\frac{1}{\sqrt{3}},
\end{aligned} \tag{2.45}$$

In Lie algebra $su(3)$, d_{abc} can also be used to construct a *cubic Casimir operator*:

$$C_3 = \frac{1}{8}d_{abc}\lambda_a\lambda_b\lambda_c, \tag{2.46}$$

where all repeated a, b, c are summed over. Thus, it is straightforward to obtain

$$[\lambda_a, C_3] = 0, \tag{2.47}$$

for any $a \in \{1, 2, \cdots, 8\}$. In other words, the cubic Casimir operator C_3 commutes with all the generators of $su(3)$. On the other hand, both f_{abc} and d_{abc} can be calculated through commutator and anti-commutator,

$$\begin{aligned} f_{abc} &= -\frac{1}{4} i \operatorname{Tr}\left(\lambda_a [\lambda_b, \lambda_c]\right), \\ d_{abc} &= \frac{1}{4} \operatorname{Tr}\left(\lambda_a \{\lambda_b, \lambda_c\}\right), \end{aligned} \tag{2.48}$$

for more information about Lie algebra, Casimir element of a representation and generators, J. E. Humphreys's book [Hum72] is an invaluable resource.

2.3 Quantum Measurement

Within the framework of non-relativistic quantum mechanics, the physical action of quantum measurement devices can be represented by self-adjoint linear operator (Hermitian). Since quantum particles (or quantum systems) are too miniature to observe, we need to perform some measurement to extract information from the quantum particles or quantum systems. Such a measurement is described by a Hermitian matrix A. In non-degenerate cases, it can be developed

$$A = \sum_{i=1}^{n} a_i P_i, \tag{2.49}$$

where P_i is the projection onto the i-th 1-dimensional eigenspace of A and can be formulate as

$$P_i = |a_i\rangle\langle a_i|, \tag{2.50}$$

with $|a_i\rangle$ denotes the eigenvector of A.

On the other hand, in degenerate cases we have

$$A = \sum_{i=1}^{r} a_i P_i, \tag{2.51}$$

where a_i are distinct eigenvalues of matrix A with multiplicity k_i satisfying

$$\sum_{i=1}^{r} k_i = n, \tag{2.52}$$

and P_i is the projection onto the i-th k_i-dimensional eigenspace of A. In both the non-degenerate cases and degenerate cases, the matrices P_i have following properties

- Hermitian: $P_i^\dagger = P_i$;
- Positive: $P_i \geq 0$;
- Complete: $\sum_i P_i = I$;
- Orthogonal: $P_i P_j = \delta_{ij} P_i$.

All these are called projective measurement. Next we will introduce the general measurement postulate.

Measurements and Quantum Systems

To explain what happens when measurements perform on quantum systems, what is the effects after the measurement and what is the state after the measurement, we introduce following postulate.

Definition 2.3.1. (Quantum Measurement). A collection of Hermitian matrices $\{M_m\}$, which represents quantum measurements, acts on the quantum state $|\psi\rangle$ of the system being measured. Then the index m stands for the outcomes that may occur in the physical experiment, and the probability p_m that outcome m occurs is given by

$$p_m = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{2.53}$$

the corresponding state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p_m}}. \tag{2.54}$$

Moreover, the measurement operators $\{M_m\}$ must satisfy the completeness condition:

$$\sum_m M_m^\dagger M_m = I. \tag{2.55}$$

From the definition of quantum measurements, we can derive the following fact about the probabilities.

Theorem 2.3.2. *The probabilities of distinct outcomes sum to one*

$$\sum_m p_m = 1. \tag{2.56}$$

Proof. According to the completeness condition of quantum measurements, we have

$$\sum_m p_m = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = 1. \tag{2.57}$$

■

Positive Operator Valued Measure

Assume the quantum measurement is repeated by a set of Hermitian matrices M_m performed on a quantum state $|\psi\rangle$. Suppose

$$E_m := M_m^\dagger M_m, \tag{2.58}$$

then from basic linear algebra and Def. 2.3.1, we know E_m is a positive operator such that

- $E_m \geq 0$;
- $\sum\limits_m E_m = I$;
- $p_m = \langle\psi|E_m|\psi\rangle$.

Hence, the description of $\{E_m\}$ can provide enough information to determine the probabilities of the measurement outcomes, and the collection of $\{E_m\}$ is known as "Positive Operator Valued Measure" (POVM). Formal definition of POVM can be shown as follows.

Definition 2.3.3. (Positive Operator Valued Measure). A collection of Hermitian matrices $\{E_m\}$ satisfying the following conditions:

1. $E_m \geq 0$,
2. $\sum\limits_m E_m = I$,

is called a Positive Operator Valued Measure (POVM).

Now, consider an example of quantum measurement which is quite simple but important. A two dimensional quantum state $|\psi\rangle$ can be formulated as

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.59}$$

with $\mid a \mid^2 + \mid b \mid^2 = 1$. Take the measurement as $\{M_0, M_1\}$ in the computational basis:

$$\begin{aligned} M_0 &= |0\rangle\langle 0|, \\ M_1 &= |1\rangle\langle 1|. \end{aligned} \tag{2.60}$$

Clearly, both M_0 and M_1 satisfy all the condition for the measurements

$$\begin{aligned} M_0^2 &= M_0 \geq 0, \\ M_1^2 &= M_1 \geq 0, \\ I &= M_0^\dagger M_0 + M_1^\dagger M_1, \end{aligned} \tag{2.61}$$

with the probabilities

$$\begin{aligned} p_0 &= \langle\psi|M_0^\dagger M_0|\psi\rangle = \mid a \mid^2, \\ p_1 &= \langle\psi|M_1^\dagger M_1|\psi\rangle = \mid b \mid^2, \end{aligned} \tag{2.62}$$

which sum to one.

The states after measurements M_0 and M_1 are

$$\begin{aligned} \frac{M_0|\psi\rangle}{\mid a \mid} &= \frac{a}{\mid a \mid}|0\rangle, \\ \frac{M_1|\psi\rangle}{\mid b \mid} &= \frac{b}{\mid b \mid}|1\rangle. \end{aligned} \tag{2.63}$$

Note that, here the vectors $\frac{a}{|a|}|0\rangle$ and $\frac{b}{|b|}|1\rangle$ are quantum states since both the multipliers $\frac{a}{|a|}$ and $\frac{b}{|b|}$ have modulus one.

By the way, we now explain why the Hermitian matrices are called as "observables". Let the eigenvalues of a Hermitian matrix A be a_i and denotes the corresponding projection to its eigenspace as P_i. Due to the spectral decomposition of A, we can have

$$A = \sum_i a_i P_i, \tag{2.64}$$

and $\{P_i\}$ forms a POVM. Moreover, since each P_i is a projection matrix, we will call it Projection Valued Measure (PVM). Therefore, we identify the Hermitain matrix A as PVM and refer to it as a measurement.

2.4 Separability and Entanglement

The most distinctive difference between classical mechanics and quantum mechanics is the correlations between composite quantum systems. In classical mechanics, the correlations between the subsystems can always be represented by the classical probability distributions, meanwhile this is not always valid for quantum theory. States that contain a non-classical correlation, is one of the key points for quantum information processing. In what follows, we first focus on finite-dimensional bipartite quantum systems, mathematically it can be described by the composed Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, and the basic correlation between subsystems are separability and entanglement.

Separable and Entangled States

Definition 2.4.1. (Separable and Entangled Pure State). A pure state $|\psi\rangle$ is called separable if and only if it can be formulated as

$$|\psi\rangle = |\psi^1\rangle \otimes |\psi^2\rangle, \tag{2.65}$$

where $|\psi^i\rangle$ is a state vector on the Hilbert space $\mathcal{H}_i$ $(i = 1, 2)$. Otherwise $|\psi\rangle$ is an entangled state.

Definition 2.4.2. (Separable and Entangled Mixed State). A mixed state ρ is called separable if and only if it can be formulated as a convex combination of pure product states

$$\rho = \sum_i p_i |\psi_i^1\rangle\langle\psi_i^1| \otimes |\psi_i^2\rangle\langle\psi_i^2| = \sum_i p_i \rho_i^1 \otimes \rho_i^2, \tag{2.66}$$

where $|\psi_i^1\rangle$ and $|\psi_i^2\rangle$ are state vectors on the Hilbert space $\mathcal{H}_1$ and $\mathcal{H}_2$, with the probabilities p_i such that

1. Positivity: $0 \leq p_i \leq 1$,
2. Completeness: $\sum_i p_i = 1$.

We should remark that in general

$$\begin{aligned} \langle\psi_i^1|\psi_j^1\rangle &\neq \delta_{ij}, \\ \langle\psi_i^2|\psi_j^2\rangle &\neq \delta_{ij}. \end{aligned} \tag{2.67}$$

Some examples need to be mentioned, the Bell states are well known entangled pure states. For qubit case, the four Bell states are maximally entangled and can form a basis for the two-qubit Hilbert space:

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2), \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 - |1\rangle_1 \otimes |1\rangle_2), \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2), \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2).
\end{aligned} \tag{2.68}$$

For simplicity, we shall use $|00\rangle$ to denote $|0\rangle_1 \otimes |0\rangle_2$ without further comments. Hence, $|\Phi^+\rangle$ can be written as $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ directly. On the other hand, an example for a mixed entangled state is the Werner state.

Now we consider the Werner state $\rho_{wer}(\lambda)$, for a bipartite system of two d-dimensional particles A and B, which defined on a d^2-dimensional Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$,

$$\rho_{wer}(\lambda) = \frac{1}{d^2}(1-\lambda)I + \lambda|\mathfrak{B}_1\rangle\langle\mathfrak{B}_1|, \tag{2.69}$$

with $|\mathfrak{B}_1\rangle$ denotes the first vector from the generalization of two-qubit Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,

$$|\mathfrak{B}_1\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} |j_A\rangle \otimes |j_B\rangle, \tag{2.70}$$

where $\{|j_A\rangle\}$ and $\{|j_B\rangle\}$ are orthonormal bases for particles A and B respectively. Moreover, the quantum state $\rho_{wer}(\lambda)$ is invariant under the unitary conjugation

$$\rho = (U \otimes U)\rho(U^\dagger \otimes U^\dagger). \tag{2.71}$$

For 2-qubit Werner state, the matrix notation of $\rho_{wer}(\lambda)$ in the standard basis is

$$\rho_{wer}(\lambda) = \begin{pmatrix} \frac{1-\lambda}{4} & 0 & 0 & 0 \\ 0 & \frac{1+\lambda}{4} & -\frac{\lambda}{2} & 0 \\ 0 & -\frac{\lambda}{2} & \frac{1+\lambda}{4} & 0 \\ 0 & 0 & 0 & \frac{1-\lambda}{4} \end{pmatrix}. \tag{2.72}$$

Note that, here we use $|\Psi^-\rangle$ instead of $|\mathfrak{B}_1\rangle$ (see Eq. 2.68).

Separability Criteria

In addition to the basic definition of separable and entangled state, we should also focus on the detection of entanglement. The simplest cases is the detection of pure state: According to the definition of separable pure state, the quantum state we considered is a product state if and only if its reduced matrices are pure state. Let us first consider the pure state $|\Psi^-\rangle$, which is one of the four Bell states, and check the entanglement of $|\Psi^-\rangle$. Take the matrix form

$$|\Psi^-\rangle\langle\Psi^-| = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.73}$$

with its reduced density matrices

$$\rho_A = \rho_B = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \tag{2.74}$$

Due to the fact that

$$\operatorname{Tr} \rho_A^2 = \operatorname{Tr} \rho_B^2 = \frac{1}{2} < 1, \tag{2.75}$$

we can conclude that the quantum state $|\Psi^-\rangle$ is entangled.

Another celebrated separability criteria for general bipartite cases is Positive Partial Transpose Criterion (PPT), which was first introduced by Asher Peres in 1996 [Per96]. For a bipartite quantum state ρ_{AB}, the PPT criterion states that if ρ_{AB} is separable, then its partial transpose $\rho_{AB}^{T_B}$ (or $\rho_{AB}^{T_A}$) is also a quantum state, hence it guarantees the positivity of $\rho_{AB}^{T_B}$ (or $\rho_{AB}^{T_A}$). We should remark that the Positive Partial Transpose Criterion can be shown stronger than entropic criteria based on Rényi entropy for $\alpha \in (0, \infty)$, for more detailed information, see Karl Gerd H. Vollbrecht and Michael M. Wolf's work [VW02].

Consider one of Bell states $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, its density matrix can be written as

$$|\Psi^+\rangle\langle\Psi^+| = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{2.76}$$

applying the partial transposition on $|\Psi^+\rangle\langle\Psi^+|$, we obtain

$$(|\Psi^+\rangle\langle\Psi^+|)^{T_B} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \tag{2.77}$$

with eigenvalues ± 1. One of the four eigenvalues for $(|\Psi^+\rangle\langle\Psi^+|)^{T_B}$ is negative, so the matrix $(|\Psi^+\rangle\langle\Psi^+|)^{T_B}$ is not positive, hence can not be a separable quantum state. Now it is clear that the state $|\Psi^+\rangle$ is entangled. We can also use the PPT criterion to investigate the Werner state, before doing so we should note that the PPT criterion is not only a necessary but also a sufficient condition for the separability of the $2\otimes 2$ and $2\otimes 3$ bipartite quantum states, thus the PPT criterion gives a essential characterization of separability and entanglement for the $2\otimes 2$ and $2\otimes 3$ cases which can be expressed as

Theorem 2.4.3. *(Positive Partial Transpose Criterion). A density matrix ρ_{AB} acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim \mathcal{H}_A = 2$ and $\dim \mathcal{H}_B = 2$ or 3 (or $\dim \mathcal{H}_A = 2$ or 3 and $\dim \mathcal{H}_B = 3$) is separable if and only if its partial transposition is a positive matrix*

$$\rho_{AB}^{T_B} = (I \otimes T)\rho_{AB} \geq 0. \tag{2.78}$$

Note that for high-dimensional case, the PPT criterion is only a necessary condition and all the quantum states satisfied above inequality are called "PPT States". To prove the sufficient condition of PPT criterion, see E. Størmer's work [Stø63] and S. L. Woronowicz's paper [Wor76].

Based on the Positive Partial Transpose Criterion, we can investigate the separability of Werner state. The partial transposition of Werner state can be expressed as

$$\rho_{wer}^{T_B}(\lambda) = \begin{pmatrix} \frac{1-\lambda}{4} & 0 & 0 & -\frac{\lambda}{2} \\ 0 & \frac{1+\lambda}{4} & 0 & 0 \\ 0 & 0 & \frac{1+\lambda}{4} & 0 \\ -\frac{\lambda}{2} & 0 & 0 & \frac{1-\lambda}{4} \end{pmatrix}, \tag{2.79}$$

with eigenvalues λ_i $(i = 1, 2, 3, 4)$

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1+\lambda}{4}, \qquad \lambda_4 = \frac{1-3\lambda}{4} \tag{2.80}$$

For all possible λ, λ_i $(i = 1, 2, 3)$ is positive. According to the PPT Criterion, $\rho_{wer}(\lambda)$ is separable if and only if λ_4 is positive, in other words, by the usage of PPT Criterion we can derive

- $\rho_{wer}(\lambda)$ is separable: $0 \leq \lambda \leq \frac{1}{3}$;
- $\rho_{wer}(\lambda)$ is entangled: $\frac{1}{3} < \lambda \leq 1$.

It is clear that, in the PPT Criterion $I\otimes T$, the transposition map T is a positive map. Before discussing the concept of positive but not completely positive map, we should introduce some definitions about C^*-algebra.

Definition 2.4.4. (*-algebra). A *-algebra $\mathcal{A}$ is a complex algebra with an algebraic involution $a \to a^*$ of $\mathcal{A}$

$$
\begin{aligned}
(a^*)^* &= a, \\
(a_1 a_2)^* &= a_2^* a_1^*, \\
(\lambda_1 a_1 + \lambda_2 a_2)^* &= \overline{\lambda_1} a_1^* + \overline{\lambda_2} a_2^*.
\end{aligned} \tag{2.81}
$$

Definition 2.4.5. (Banach-algebra). A Banach-algebra $\mathcal{B}$ is a complex algebra which is a Banach space with norm $\| \cdot \|$ such that

$$\| a_1 a_2 \| \leq \| a_1 \| \| a_2 \| \tag{2.82}$$

for all $a_i \in \mathcal{B}$ $(i = 1, 2)$.

Definition 2.4.6. (C^*-algebra). A C^*-algebra $\mathcal{C}$ is a Banach algebra which is a *-algebra and satisfies

$$\| a^* a \| = \| a \|^2 \tag{2.83}$$

for all $a \in \mathcal{C}$, and this equality is also called the C^*-condition.

Definition 2.4.7. (Positive map). Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be C^*-algebras. A linear map Λ: $\mathcal{C}_1 \to \mathcal{C}_2$ is said to be positive if

$$\Lambda(a) \geq_{\mathcal{C}_2} 0, \tag{2.84}$$

whenever $a \in \mathcal{C}_1$ and $a \geq_{\mathcal{C}_1} 0$.

In quantum information theory, a positive map maps any positive operator into a positive one. Then, it is easy to see that transposition T is a positive map, but it is not a completely positive map, i.e. $I \otimes T$ is not a positive map.

It happens that applying the positive (P) but not completely positive (CP) map Λ, one can provide a necessary and sufficient condition for separability:

Theorem 2.4.8. *(Positive but not Completely Positive map). The quantum state ρ_{AB} is separable if and only if the following condition is valid for all P but not CP maps*

$$(I \otimes \Lambda)\rho_{AB} \geq 0. \tag{2.85}$$

One can also restrict the maps to be trace preserving ones. Clearly, PPT Criterion is a special case of this general theorem. For more about C^*-algebra and operator theory, see [Mur14].

Reduction Criterion for separability [CAG99] is a special case of Theorem 2.4.8 by taking a particular positive map. The Reduction Criterion can be formulated as

Theorem 2.4.9. *(Reduction Criterion). A quantum state ρ_{AB} acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if and only if*

$$\rho_A \otimes I - \rho_{AB} \geq 0, \tag{2.86}$$

with the $2 \otimes 2$ and $2 \otimes 3$ cases.

Note that for high-dimensional case, the Reduction Criterion is only a necessary condition. In [HH99] it is shown that Reduction Criterion is equivalent to the PPT Criterion for the $2 \otimes 2$ and $2 \otimes 3$ cases.

From the P but not CP maps, we known that for a positive map Λ

$$(I \otimes \Lambda)\rho_{AB} \geq 0, \tag{2.87}$$

if the quantum state is separable. By choosing

$$\Lambda(B) = Tr(B)I - B, \tag{2.88}$$

where B stands for any quadratic matrix, we can obtain the expression of the Reduction Criterion. Here we will employ the Reduction Criterion to examine the separability of Werner state again.

Recall the Werner state in the standard basis

$$\rho_{wer}(\lambda) = \begin{pmatrix} \frac{1-\lambda}{4} & 0 & 0 & 0 \\ 0 & \frac{1+\lambda}{4} & -\frac{\lambda}{2} & 0 \\ 0 & -\frac{\lambda}{2} & \frac{1+\lambda}{4} & 0 \\ 0 & 0 & 0 & \frac{1-\lambda}{4} \end{pmatrix}, \tag{2.89}$$

with its reduced density matrix for A system

$$\rho_{wer}(\lambda)_A = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}I. \tag{2.90}$$

Then we can obtain

$$\rho_{wer}(\lambda)_A \otimes I = \frac{1}{2} I \otimes I, \tag{2.91}$$

and hence the Reduction Criterion can be formulated as

$$\rho_{wer}(\lambda)_A \otimes I - \rho_{wer}(\lambda) = \frac{1}{2} I \otimes I - \rho_{wer}(\lambda). \tag{2.92}$$

For Werner state $\rho_{wer}(\lambda)$, there exist unitary matrix M such that

$$M^\dagger \rho_{wer}(\lambda) M = \begin{pmatrix} \frac{1+\lambda}{4} & 0 & 0 & 0 \\ 0 & \frac{1+\lambda}{4} & 0 & 0 \\ 0 & 0 & \frac{1+\lambda}{4} & 0 \\ 0 & 0 & 0 & \frac{1-3\lambda}{4} \end{pmatrix}, \tag{2.93}$$

then it happens

$$M^{\dagger}(\rho_{wer}(\lambda)_A \otimes I - \rho_{wer}(\lambda))M = \begin{pmatrix} \frac{1+\lambda}{4} & 0 & 0 & 0 \\ 0 & \frac{1+\lambda}{4} & 0 & 0 \\ 0 & 0 & \frac{1+\lambda}{4} & 0 \\ 0 & 0 & 0 & \frac{1-3\lambda}{4} \end{pmatrix}. \tag{2.94}$$

Denote the eigenvalues λ_i $(i = 1, 2, 3, 4)$ as

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1+\lambda}{4}, \qquad \lambda_4 = \frac{1-3\lambda}{4} \tag{2.95}$$

Similar to the PPT Criterion, λ_i $(i = 1, 2, 3)$ is positive for all possible λ. According to the Reduction Criterion, $\rho_{wer}(\lambda)$ is separable if and only if λ_4 is positive, in other words, by the usage of Reduction Criterion we can derive

- $\rho_{wer}(\lambda)$ is separable: $0 \leq \lambda \leq \frac{1}{3}$;
- $\rho_{wer}(\lambda)$ is entangled: $\frac{1}{3} < \lambda \leq 1$.

Entanglement is a kind of resource which is as real as energy, and it can be used in many application such as quantum cryptograph, quantum teleportation and so on. For more detailed information and reviews about the characterization, detection, quantification and distillation of entanglement, see [HHHH09].

2.5 Entropy

Entropy is a fundamental concept in both physics and information theory, being one of the most important tools to measure the uncertainty. Moreover, the uncertainty relations can be formulated into entropic uncertainty relations and variance-based uncertainty relations. In thermodynamic, entropy is an elementary variable that can be employed to define the equilibrium state: From the second law of thermodynamics, equilibrium state is the one with maximal entropy for an isolated system. Furthermore, in the following chapters, we will formulate the strong entropic uncertainty relation and connect the entropic uncertainty relations in presence of quantum memory with entropic uncertainty relations in absence of quantum memory, it is necessary to introduce the basic definitions and properties of entropies here.

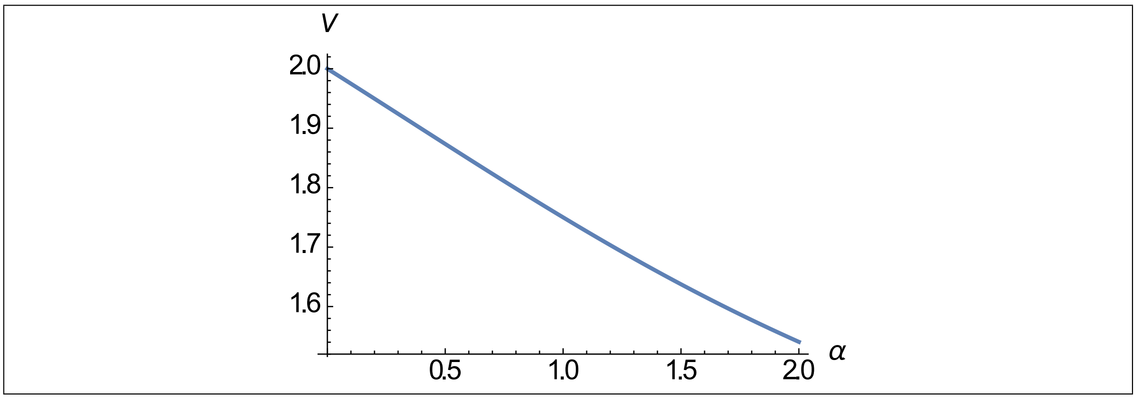

Figure 2.1: The Rényi entropy of order α.

Rényi Entropy

We start with Rényi entropy [RRN61] which has been widely used in information theory and quantum information theory. Given probabilities $p = (p_1, p_2, \cdots, p_n)$ such that

$$\sum_{i=1}^{n} p_i = 1, \tag{2.96}$$

the Rényi entropy can be defined as

Definition 2.5.1. (Rényi Entropy). The Rényi entropy of order α is formulated as

$$H_\alpha(p) = \frac{1}{1-\alpha} \log \sum_{i=1}^{n} p_i^\alpha, \tag{2.97}$$

for $\alpha \in (0, 1) \cup (1, \infty)$.

Following Shannon's idea [Sha48], we can also define the concept of surprisal.

Definition 2.5.2. (Surprisal). The surprisal of the i-th event with probability p_i is

$$-\log p_i = \log \frac{1}{p_i}. \tag{2.98}$$

Rényi entropy with $\alpha > 1$ gives more weights to the events with lower probability, in other words, with high surprisal, which leads to the monotonically decreasing as a function of α. To see this phenomena, let us consider the events with the following probabilities

$$p_1 = \frac{1}{2}, \quad p_2 = \frac{1}{4}, \quad p_3 = \frac{1}{8}, \quad p_4 = \frac{1}{8}, \tag{2.99}$$

then the functional image of Rényi entropy according to α can be shown in FIG. 2.1. On the other hand, Rényi entropy gives less weights to the events with lower probability for the cases with $\alpha < 1$.

Hence, we can conclude that the Rényi entropy for different values of α can be totally different. One of the most important properties of Rényi entropy is the Schur-concavity, which will be introduced later. Another important property for Rényi entropy is the additivity.

Theorem 2.5.3. *(Additivity). For independent variables X and Y, we have*

$$H_\alpha(X,Y) = H_\alpha(X) + H_\alpha(Y). \tag{2.100}$$

Proof.

$$\begin{aligned} H_\alpha(X,Y) &= \frac{1}{1-\alpha}\log\sum_{x,y} p^\alpha(x,y) = \frac{1}{1-\alpha}\log\sum_x p^\alpha(x)\sum_y p^\alpha(y) \\ &= \frac{1}{1-\alpha}\log\sum_x p^\alpha(x) + \frac{1}{1-\alpha}\log\sum_y p^\alpha(y) = H_\alpha(X) + H_\alpha(Y). \end{aligned} \tag{2.101}$$

■

Further properties of Rényi entropy has been comprehensively studied in [AD75, Rén76], here we will list some basic ones.

- Nonnegativity: $H_\alpha(p) \geq 0$;
- Definitiveness: $H_\alpha(p) = 0$ if $p_i = 1$ for some i;
- Concavity: For $\alpha \leq 1$, Rényi entropy $H_\alpha(p)$ is a concave function of p_i. Meanwhile, for $\alpha > 1$ the Rényi entropy $H_\alpha(p)$ is neither pure convex nor pure concave. Note that the function $(\alpha - 1)H_\alpha(p)$ is a concave function of p_i;
- Continuity: $H_\alpha(p)$ is a bounded, continuous and non-increasing function of α.

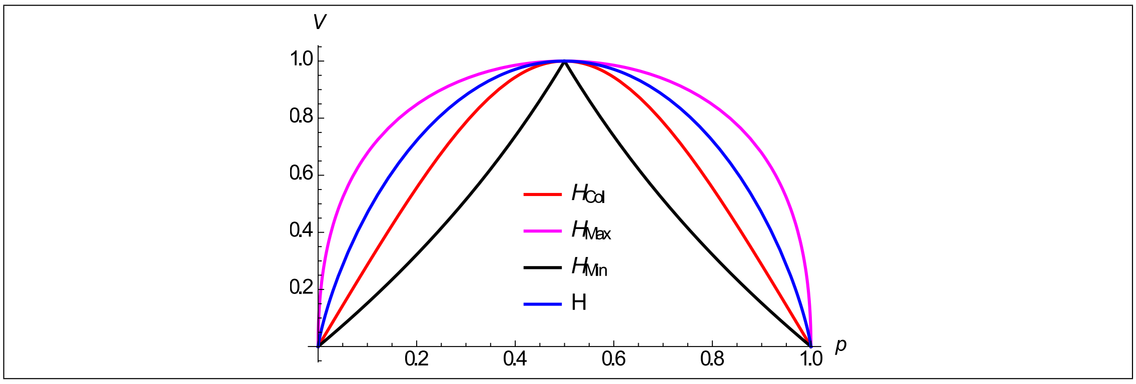

Figure 2.2: Different entropies with respect to different α.

Proof. If $p_i = 1$ for some i, then $p_j = 0$ for all $j \neq i$, hence

$$H_\alpha(p) = \frac{1}{1-\alpha} \log \sum_{i=1}^{n} p_i^\alpha = \frac{1}{1-\alpha} \log p_i = 0. \tag{2.102}$$

Since

$$\frac{\alpha-1}{\alpha} H_\alpha(p) \leq \frac{\beta-1}{\beta} H_\beta(p), \tag{2.103}$$

for $\alpha \geq \beta$, we can derive the concavity of $(\alpha-1)H_\alpha(p)$. ■

Let us consider some special cases of Rényi entropy, for different α we can obtain different kind of entropies:

Definition 2.5.4. (Collision Entropy). Collision Entropy refers to the case $H_2(p)$,

$$H_{col}(p) := H_2(p) = \frac{1}{1-2} \log \sum_{i=1}^{n} p_i^2 = -\log \sum_{i=1}^{n} p_i^2. \tag{2.104}$$

Definition 2.5.5. (Max-Entropy). Max-Entropy refers to the case $H_{\frac{1}{2}}(p)$,

$$H_{max}(p) := H_{\frac{1}{2}}(p) = \frac{1}{1-\frac{1}{2}} \log \sum_{i=1}^{n} p_i^{\frac{1}{2}} = 2\log \sum_{i=1}^{n} p_i^{\frac{1}{2}}. \tag{2.105}$$

Definition 2.5.6. (Min-Entropy). Min-Entropy refers to the case $H_\infty(p)$,

$$H_{min}(p) := H_\infty(p) = -\log \max_i p_i. \tag{2.106}$$

Definition 2.5.7. ($H_0(p)$). $H_0(p)$ is the logarithm of the support of probabilities p_i,

$$H_0(p) := \log \mid \{i : p_i > 0\} \mid . \tag{2.107}$$

Definition 2.5.8. (Shannon Entropy). Shannon Entropy refers to the case $H_1(p)$,

$$H(p) := H_1(p) = \lim_{\alpha \to 1} H_\alpha(p). \tag{2.108}$$

Applying L' Hopital's Theorem,

$$\begin{aligned} H_1(p) = \lim_{\alpha \to 1} H_\alpha(p) = \lim_{\alpha \to 1} \frac{\frac{d}{d\alpha} \log \sum_{i=1}^{n} p_i^\alpha}{\frac{d}{d\alpha}(1-\alpha)} &= - \left(\sum_{i=1}^{n} (\log p_i) p_i^\alpha \right) \left(\sum_{i=1}^{n} p_i^\alpha \right)^{-1} \Bigg|_{\alpha=1} \\ &= - \sum_{i=1}^{n} p_i \log p_i, \end{aligned} \tag{2.109}$$

which is in conformity with the definition of Shannon entropy appeared in Chapter 1. Now it is clear that the Shannon entropy quantifies the average surprisal of $p = (p_1, p_2, \cdots, p_n)$ and it is a special case of Rényi entropy.

Different entropies may emphasize on different relation between probabilities, the following example visualized in FIG. 2.2 shows the variation with respect to special α for probability distribution $(p, 1-p)$.

Back to the begining of information theory, Shannon stated that a measure I for information with probability $p = (p_1, p_2, \cdots, p_n)$ should satisfy following conditions:

1. I is a function of the probability $p = (p_1, p_2, \cdots, p_n)$ for events. If all the probabilities p_i are equally probably, in other words $p_i = \frac{1}{n}$, then $I(p)$ should be a monotonic increasing function of n;

2. $I(p)$ is a smooth function of p.

3. I should be additive: The information gained for two independent events should equal the sum of the individual information that gained from each other alone.

Shannon then proved that the information function I is

$$I(p) = -k \sum_{i=1}^{n} p_i \log p_i, \tag{2.110}$$

where k is a constant number. That is equivalent to say the information function $I(p)$ is just the Shannon entropy $H(p)$, up to a constant factor. In addition, Kendall [SO94] construct a related concept, information content, of a probability distribution $p = (p_1, p_2, \cdots, p_n)$.

Definition 2.5.9. (Information Content). The information content of the probability distribution p is

$$I_\alpha(p) = \frac{1}{\alpha - 1} - \sum_{i=1}^{n} \frac{p_i^\alpha}{\alpha - 1}. \tag{2.111}$$

The information content tends to the Shannon entropy again as α tends to 1, since

$$\begin{aligned} I_\alpha(p) &= \frac{1}{\alpha - 1} - \sum_{i=1}^{n} \frac{p_i^\alpha}{\alpha - 1} = \sum_{i=1}^{n} \frac{p_i - p_i^\alpha}{\alpha - 1} \\ &= \sum_{i=1}^{n} \frac{[1-(1-p_i)] - [1-(1-p_i)]^{(\alpha-1)+1}}{\alpha - 1} \\ &= \sum_{i=1}^{n} \frac{[1-(1-p_i)]\left(1 - [1-(1-p_i)]^{(\alpha-1)}\right)}{\alpha - 1}, \end{aligned} \tag{2.112}$$

by applying Taylor expansion, we know

$$\frac{(1-x)^a - 1}{a} = -x + (a-1)\frac{x^2}{2!} - (a-1)(a-2)\frac{x^3}{3!} + \cdots, \tag{2.113}$$

let a tends to 0, this becomes

$$\lim_{a \to 0} \frac{(1-x)^a - 1}{a} = -x - \frac{x^2}{2} - \frac{x^3}{3} + \cdots, \tag{2.114}$$

which coincides with the Taylor expansion of the logarithm, hence we can derive

$$\lim_{\alpha \to 1} \frac{p_i - p_i^\alpha}{\alpha - 1} = -p_i \log p_i, \tag{2.115}$$

thus

$$\lim_{\alpha \to 1} I_\alpha(p) = -\sum_{i=1}^{n} p_i \log p_i = H(p), \tag{2.116}$$

which is just the Shannon entropy.

Relative Entropy

For two probability distributions $p(x)$ and $q(x)$ with the same variable x, the relative entropy is a very useful entropic measure of the closeness between probability distributions $p(x)$ and $q(x)$.

Definition 2.5.10. (Relative Entropy). Given two different probability distributions $p(x)$ and $q(x)$ over the same variable x, the relative entropy of $p(x)$ to $q(x)$ is defined by

$$H(p \parallel q) = \sum_x p(x) \log \frac{p(x)}{q(x)}, \tag{2.117}$$

set $-p(x) \log 0 = +\infty$ if $p(x) > 0$, we should also note that $-0 \log 0 = 0$.

By the nonnegative of the relative entropy, we can obtain many useful entropic inequalities. Again, due to the nonnegativity of the relative entropy, it can be seen like the concept of distance measure. Based on these fact, we should give the following nonnegativity theorem.

Theorem 2.5.11. *(Nonnegativity of Relative Entropy). The relative entropy $H(p \parallel q)$ is nonnegative with equality if and only if $p(x) = q(x)$ over all variables x.*

Proof.

$$\begin{aligned} H(p \parallel q) &= \sum_x p(x) \log \frac{p(x)}{q(x)} = -\sum_x p(x) \log \frac{q(x)}{p(x)} \\ &\geq -\log \sum_x p(x) \cdot \frac{q(x)}{p(x)} = -\log \sum_x q(x) = 0. \end{aligned} \tag{2.118}$$

■

From the nonnegativity of relative entropy, we show the following corollary about entropy.

Corollary 2.5.12. *Assume $p(x)$ is a probability distribution for random variable X over n outcomes, then*

$$H(p) \leq \log n. \tag{2.119}$$

Proof. Consider the relative entropy of $p(x)$ to $q(x)$ with $q(x)$ be the uniform probability distribution over all x, that is equivalent to say

$$q(x) = \frac{1}{n}, \tag{2.120}$$

for all x. Then by nonnegativity of the relative entropy,

$$H(p \parallel q) = H(p \parallel \frac{1}{n}) = -H(p) - \sum_x p(x) \log \frac{1}{n} = \log n - H(p) \geq 0, \tag{2.121}$$

hence we can derive

$$H(p) \leq \log n, \tag{2.122}$$

which complete the proof. ■

For two random variables X and Y, we can also define the concept of joint entropy. For clarity, we now give the definition formally.

Definition 2.5.13. (Joint Entropy). The joint entropy for random variable X and Y with probability distribution $p(x, y)$ is defined as

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y). \tag{2.123}$$

Corollary 2.5.14. *(Subadditivity). The joint entropy for random variables X and Y can not exceed the sum of Shannon entropies for X and Y,*

$$H(X, Y) \leq H(X) + H(Y), \tag{2.124}$$

with equality if and only if X and Y are independent random variables.

Proof. Consider the relative entropy $H(p(x, y) \parallel p(x)p(y))$,

$$\begin{aligned} H(p(x, y) \parallel p(x)p(y)) &= \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} = H(p(x)) + H(p(y)) - H(p(x, y)) \\ &= H(X) + H(Y) - H(X, Y), \end{aligned} \tag{2.125}$$

then by the nonnegative of relative entropy we can derive

$$H(X, Y) \leq H(X) + H(Y). \tag{2.126}$$

■

This technique, finding entropic inequalities by the usage of relative entropy, is widely used in both classical information theory and quantum information theory. Before introducing the celebrated Csiszár Theorem [C+67], we should first define the concepts of f-relative entropy and stochastic matrix.

Definition 2.5.15. (f-relative Entropy). The f-relative entropy for two probability distributions p and q is defined as

$$H_f(p \parallel q) = \sum_i p_i f(\frac{q_i}{p_i}), \tag{2.127}$$

with f be a convex function.

For $f(x) = -\log x$, the f-relative entropy becomes the relative entropy $H(p \parallel q)$. For $f(x) = 1 - \sqrt{x}$, the f-relative entropy becomes the square of the Hellinger distance $d_2(p,q)$,

$$H_f(p \parallel q) = 1 - \sum_{i=1}^{n} \sqrt{p_i}\sqrt{q_i} = \frac{1}{2}\sum_{i=1}^{n}(\sqrt{p_i} - \sqrt{q_i})^2 = d_2^2(p,q), \tag{2.128}$$

and the quantity $d_2(p,q)$ satisfies the axioms of distance.

Stochastic Matrix

Next, let us consider the concept of stochastic matrix Q. When an information process converts a set of date $X = \{x_1, x_2, \cdots, x_k\}$ to another set of date $Y = \{y_1, y_2, \cdots, y_l\}$ probabilistically, in other words, there has probability Q_{ij} that converts the input x_i into the out put y_j, then $Q = (Q_{ij})_{ij}$ forms a matrix which is called stochastic matrix and satisfies

$$\sum_{j=1}^{l} Q_{ij} = 1, \tag{2.129}$$

for any i. Then we have the following fundamental property of a stochastic matrix $Q = (Q_{ij})_{ij}$ and f-relative entropy $H_f(p \parallel q)$.

Theorem 2.5.16. *(Csiszár Theorem). Let $H_f(p \parallel q)$ denote the f-relative entropy, then it satisfies the monotonicity condition,*

$$H_f(p \parallel q) \geq H_f(Q(p) \parallel Q(q)), \tag{2.130}$$

for any stochastic matrix Q.

Proof. Due to the convexity of function f, Jensen's inequality implies that

$$\sum_{i_1} \frac{Q_{i_1 j} p_{i_1}}{\sum_{i_2} Q_{i_2 j} p_{i_2}} f\left(\frac{q_{i_1}}{p_{i_1}}\right) \geq f\left(\sum_{i_1} \frac{Q_{i_1 j} p_{i_1}}{\sum_{i_2} Q_{i_2 j} p_{i_2}} \cdot \frac{q_{i_1}}{p_{i_1}}\right) = f\left(\frac{\sum_{i_1} Q_{i_1 j} q_{i_1}}{\sum_{i_2} Q_{i_2 j} p_{i_2}}\right), \tag{2.131}$$

then we can obtain

$$\begin{aligned}
&H_f(Q(p) \parallel Q(q)) \\
=&\sum_j \sum_{i_3} Q_{i_3 j} p_{i_3} f\left(\frac{\sum\limits_{i_1} Q_{i_1 j} q_{i_1}}{\sum\limits_{i_2} Q_{i_2 j} p_{i_2}}\right) \\
=&\sum_j \sum_{i_3} Q_{i_3 j} p_{i_3} f\left(\sum_{i_1} \frac{Q_{i_1 j} p_{i_1}}{\sum\limits_{i_2} Q_{i_2 j} p_{i_2}} \cdot \frac{q_{i_1}}{p_{i_1}}\right) \\
\leq&\sum_j \sum_{i_3} Q_{i_3 j} p_{i_3} \sum_{i_1} \frac{Q_{i_1 j} p_{i_1}}{\sum\limits_{i_2} Q_{i_2 j} p_{i_2}} f\left(\frac{q_{i_1}}{p_{i_1}}\right) \\
=&\sum_j \sum_{i_1} Q_{i_1 j} p_{i_1} f\left(\frac{q_{i_1}}{p_{i_1}}\right) \\
=&\sum_{i_1} (\sum_j Q_{i_1 j}) p_{i_1} f\left(\frac{q_{i_1}}{p_{i_1}}\right) \\
=&\sum_{i_1} p_{i_1} f\left(\frac{q_{i_1}}{p_{i_1}}\right) \\
=&H_f(p \parallel q),
\end{aligned} \tag{2.132}$$

therefore,

$$H_f(p \parallel q) \geq H_f(Q(p) \parallel Q(q)). \tag{2.133}$$

■

Definition 2.5.17. (Double Stochastic Matrix). If the transpose of a stochastic matrix $Q = (Q_{ij})_{ij}$ is also a stochastic matrix, we will call it double stochastic matrix, i.e.,

$$\begin{aligned}
\sum_i Q_{ij} = 1, \\
\sum_j Q_{ij} = 1.
\end{aligned} \tag{2.134}$$

Double stochastic matrix is related with majorization theory which will be widely used in following chapters. In fact, double stochastic matrix can be used to detect entanglement and improve the bound for entropic uncertainty relations. As will be shown later, with the help of double stochastic matrix, we can derive

Theorem 2.5.18. *For a probability distribution p, the double stochastic matrix $Q = (Q_{ij})_{ij}$ ensures that*

$$H(Q(p)) \geq H(p). \tag{2.135}$$

Conditional Entropy

Given two random variables X and Y, suppose we know the information about Y, i.e., we have already obtained $H(Y)$ bits of information about the whole system, then the remaining uncertainty about the whole system is related to the uncertainty about X given Y. The corresponding conditional entropy can be defined by

Definition 2.5.19. (Conditional Entropy). The conditional entropy of X given Y is

$$H(X|Y) = H(X,Y) - H(Y), \tag{2.136}$$

where $H(X,Y)$ is the joint entropy for random variables X and Y.

On the other hand, the mutual information of X and Y measures how much information X and Y have in common:

Definition 2.5.20. (Mutual Information). The mutual information of X and Y is

$$I(X:Y) = H(X) + H(Y) - H(X,Y), \tag{2.137}$$

where $H(X,Y)$ is the joint entropy for random variables X and Y. It is clear that the mutual information $I(X:Y)$ equals $H(X) - H(X|Y)$.

To prepare the later use, we now give some basic properties of Shannon entropy:

- $H(p)$ is a concave function of probability distribution $p = (p_1, p_2, \cdots, p_n)$: If $a_i \geq 0$ for all i, and $\sum_{i=1}^{n} a_i = 1$, then for random variables X_i $(i = 1, 2, \cdots, n)$, we have

$$H(\sum_{i=1}^{n} a_i X_i) \geq \sum_{i=1}^{n} a_i H(X_i); \tag{2.138}$$

- The conditional entropy is nonnegative and the joint entropy is large than the entropy of one variable (X or Y):

$$H(X|Y) \geq 0, \quad H(X,Y) \geq H(X), \qquad H(X,Y) \geq H(Y), \tag{2.139}$$

  with equality if and only if Y is a function of X.

- Strong Subadditivity:

$$H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z), \tag{2.140}$$

  with equality if and only if $Z \to Y \to X$ forms a Markov chain. And this inequality is equivalent to

$$H(X|Y,Z) \leq H(X|Y). \tag{2.141}$$

  A consequence of strong subadditivity is the following date processing inequality for Markov chain $Z \to Y \to X$

$$H(X|Z) \geq H(X|Y). \tag{2.142}$$

- Chaining rule for conditional entropy: Let $X_1, X_2, \cdots, X_n$ and Y be any random variables, then the following algebraic identity holds

$$H(X_1, X_2, \cdots, X_n|Y) = \sum_{i=1}^{n} H(X_i|Y, X_1, \cdots, X_{i-1}). \tag{2.143}$$

von Neumann Entropy

The above discussions for entropy only focus on probability distributions, now let us extend the probability distribution to density matrix ρ and consider the von Neumann entropy of the density matrix ρ.

Definition 2.5.21. (von Neumann Entropy). The von Neumann entropy of the density matrix ρ is defined by

$$H(\rho) = -\operatorname{Tr} \rho \log \rho. \tag{2.144}$$

If the density matrix ρ has a spectral decomposition

$$\rho = \sum_{i=1}^{n} p_i |u_i\rangle\langle u_i|, \tag{2.145}$$

then

$$\log \rho = \sum_{i=1}^{n} (\log p_i)|u_i\rangle\langle u_i|, \tag{2.146}$$

and hence we can written $H(\rho)$ as

$$H(\rho) = -\sum_{i=1}^{n} p_i \log p_i. \tag{2.147}$$

As an extension of relative entropy $H(p \parallel q)$ for probability distributions p and q, we can generalize to the quantum relative entropy for density matrices ρ and σ,

Definition 2.5.22. (Quantum Relative Entropy). For two density matrices ρ and σ, the quantum relative entropy $D(\rho \parallel \sigma)$ is defined as

$$D(\rho \parallel \sigma) = Tr[\rho(\log \rho - \log \sigma)]. \tag{2.148}$$

Here we will give some examples for the von Neumann entropy, for density matrices

$$\rho_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \rho_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \rho_3 = \frac{1}{3}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \rho_4 = \frac{1}{4}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \tag{2.149}$$

their von Neumann entropy can be calculated

$$H(\rho_1) = 0, \quad H(\rho_2) = 0, \quad H(\rho_3) \doteq 0.55, \quad H(\rho_4) \doteq 0.60. \tag{2.150}$$

Assume there is a quantum state ρ

$$\rho = p|0\rangle\langle 0| + (1-p)\frac{(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)}{2}, \tag{2.151}$$

where $0 \le p \le 1$, then the density matrix ρ can be written as

$$\rho = \frac{1}{2}\begin{pmatrix} 1+p & 1-p \\ 1-p & 1-p \end{pmatrix}, \tag{2.152}$$

with eigenvalues

$$p_1 = \frac{1}{2}(1 - \sqrt{1-2p+2p^2}), \quad p_2 = \frac{1}{2}(1 + \sqrt{1-2p+2p^2}). \tag{2.153}$$

The comparison between von Neumann entropy $H(\rho)$ and binary entropy $H(p)$ can be shown in FIG. 2.3.

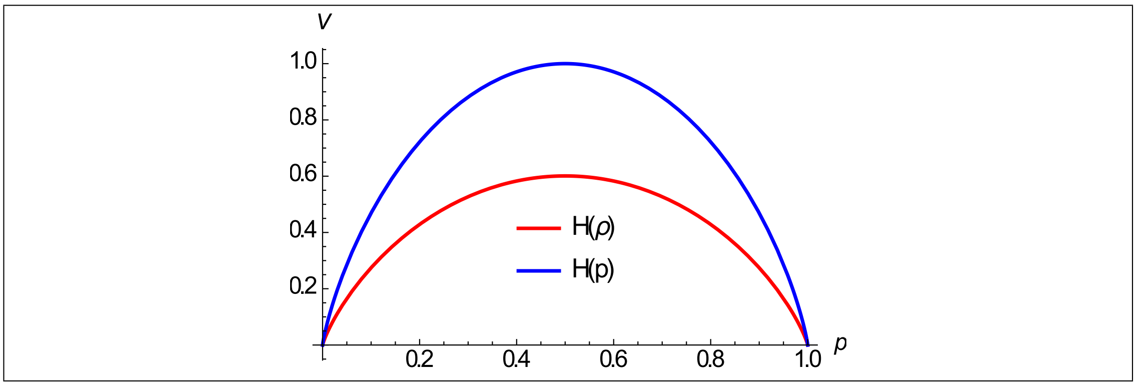

Figure 2.3: Comparison between $H(\rho)$ and $H(p)$.

We should remark that for a tripartite quantum state ρ_{ABC}, we can give definitions to the concept of entropy for reduced density matrix ρ_A, ρ_B and ρ_C by

$$H(A) = H(\rho_A), \quad H(B) = H(\rho_B), \quad H(C) = H(\rho_C), \tag{2.154}$$

where these definitions are analogous to the marginal distribution for the joint distribution $p(x, y)$. Now we can generalize the concept of quantum mutual information and quantum conditional mutual information to the tripartite case

$$\begin{aligned} &H(A|B) = H(A, B) - H(B) = H(\rho_{AB}) - H(\rho_B), \\ &I(A : B|C) = H(A, B|C) - H(B|C), \\ &I(A : B) = H(A) + H(B) - H(A, B) = H(\rho_A) + H(\rho_B) - H(\rho_{AB}), \end{aligned} \tag{2.155}$$

therefore,

$$\begin{aligned} I(A : B|C) &= H(A, C) + H(B, C) - H(A, B, C) - H(C) \\ &= H(\rho_{AC}) + H(\rho_{BC}) - H(\rho_{ABC}) - H(\rho_C). \end{aligned} \tag{2.156}$$

For some special cases, the quantum relative entropy equals the classical relative entropy.

Theorem 2.5.23. *Suppose two density matrix ρ and σ commute with each other,*

$$[\rho, \sigma] = 0, \tag{2.157}$$

where ρ has eigenvalues $p = (p_i)$ and σ has eigenvalues $q = (q_i)$, then

$$D(\rho \parallel \sigma) = H(p \parallel q). \tag{2.158}$$

Proof. Since $[\rho, \sigma] = 0$, ρ and σ have common eigenspaces, therefore we can assume

$$\begin{aligned}\rho &= \sum_{i=1}^{n} p_i |u_i\rangle\langle u_i|, \\ \sigma &= \sum_{i=1}^{n} q_i |u_i\rangle\langle u_i|. \end{aligned} \tag{2.159}$$

Hence, we can calculate the quantum relative entropy as

$$\begin{aligned} D(\rho \parallel \sigma) &= \mathrm{Tr}[\rho(\log\rho - \log\sigma)] \\ &= \sum_{i=1}^{n} p_i \log p_i - \mathrm{Tr}(\sum_{i} p_i |u_i\rangle\langle u_i| \log \sum_{j=1}^{n} q_j |u_j\rangle\langle u_j|) \\ &= \sum_{i=1}^{n} p_i \log \frac{p_i}{q_i} = H(p \parallel q). \end{aligned} \tag{2.160}$$

■

For the general case, no matter whether ρ and σ commute or not, their quantum relative entropy is nonnegative.

Theorem 2.5.24. *(Klein Inequality). Klein inequality states that*

$$D(\rho \parallel \sigma) \geq 0, \tag{2.161}$$

with equality if and only if $\rho = \sigma$.

Proof. Assume the density matrices ρ and σ have the following spectral decomposition

$$\begin{aligned}\rho &= \sum_{i} p_i |u_i\rangle\langle u_i|, \\ \sigma &= \sum_{j} q_j |v_j\rangle\langle v_j|, \end{aligned} \tag{2.162}$$

then the quantum relative entropy can be written as

$$\begin{aligned} D(\rho \parallel \sigma) &= \mathrm{Tr}[\rho(\log\rho - \log\sigma)] \\ &= \sum_{i} p_i \log p_i - \mathrm{Tr}(\sum_{i} p_i |u_i\rangle\langle u_i| \log \sum_{j} q_j |v_j\rangle\langle v_j|) \\ &= \sum_{i} p_i \log p_i - \sum_{i,j} p_i \log q_j \langle u_i|v_j\rangle\langle v_j|u_i\rangle, \end{aligned} \tag{2.163}$$

denote the quantity c_{ij} as

$$c_{ij} = \langle u_i | v_j \rangle \langle v_j | u_i \rangle, \tag{2.164}$$

and we can find out that

$$\begin{aligned} \sum_i c_{ij} &= 1, \\ \sum_j c_{ij} &= 1, \end{aligned} \tag{2.165}$$

which is equivalent to say that $(c_{ij})_{ij}$ forms a double stochastic matrix. By the convexity of log function, we obtain

$$\begin{aligned} D(\rho \parallel \sigma) &= \sum_i p_i \log p_i - \sum_{i,j} c_{ij} p_i \log q_j \\ &\geq \sum_i p_i \log p_i - \sum_i p_i \log \sum_j c_{ij} p_j, \end{aligned} \tag{2.166}$$

set $r_i = \sum_j c_{ij} p_j$, it is clear that

$$\sum_i r_i = 1, \tag{2.167}$$

and $0 \leq r_i \leq 1$. Hence

$$D(\rho \parallel \sigma) \geq \sum_i p_i \log p_i - \sum_i p_i \log r_i = H(p \parallel r) \geq 0. \tag{2.168}$$

■

Apart from the properties we discuss above, the von Neumann entropy also has other useful properties which will be used in following chapters.

- Nonnegativity: The von Neumann entropy $H(\rho)$ is nonnegative, $H(\rho) = 0$ if and only if the quantum state is pure;
- Reduced Equality: For a pure composite bipartite system ρ_{AB}, it implies $H(A) = H(B)$;
- Orthogonal Support: For different quantum states ρ_i with probabilities p_i, if their supports are orthogonal to each other, then

$$H(\sum_{i=1}^{n} p_i \rho_i) = H(p) + \sum_{i=1}^{n} p_i H(\rho_i), \tag{2.169}$$

with $p = (p_1, p_2, \cdots, p_n)$. Otherwise we obtain

$$H(\sum_{i=1}^{n} p_i \rho_i) \leq H(p) + \sum_{i=1}^{n} p_i H(\rho_i); \tag{2.170}$$

- Araki Lieb: The lower bound for the joint entropy $H(\rho_{AB})$ can be given

$$H(\rho_{AB}) \geq \mid H(\rho_A) - H(\rho_B) \mid = \mid H(A) - H(B) \mid; \tag{2.171}$$

- Joint Entropy Theorem: Support $|i\rangle\langle i|$ is projective orthonormal basis for system A and ρ_i are arbitrary density matrices for system B with probability distribution $p = (p_1, p_2, \cdots, p_n)$, then

$$H(\sum_{i=1}^{n} p_i |i\rangle\langle i| \otimes \rho_i) = H(p) + \sum_{i=1}^{n} p_i H(\rho_i), \tag{2.172}$$

which also implies that

$$H(\rho \otimes \sigma) = H(\rho) + H(\sigma). \tag{2.173}$$

- Subadditivity: The upper bound for the joint entropy $H(\rho_{AB})$ can be given

$$H(\rho_{AB}) \leq H(\rho_A) + H(\rho_B) = H(A) + H(B). \tag{2.174}$$

Chapter 3

Variance-Based Uncertainty Relations

This chapter formally introduces our results of variance-based uncertainty relations, we investigate the contribution, from individual observable, to the variance-based sum uncertainty relations and introduce the concept of *weighted uncertainty relations*. Moreover, to derive the uncertainty relations for product of variance with multi-observables, we explore the properties of mutually exclusive physical states and build the *mutually exclusive uncertainty relations*.

3.1 Weighted Uncertainty Relations

Recently, Maccone and Pati have given two stronger uncertainty relations based on the sum of variances and one of them is nontrivial when the quantum state is not an eigenstate of the sum of the observables. We derive a family of weighted uncertainty relations to provide an optimal lower bound for all situations and remove the restriction on the quantum state. Generalization to multi-observable cases is also given and an optimal lower bound for the weighted sum of the variances is obtained in general quantum situation. In Kennard's formulation [Ken27] of Heisenberg's uncertainty principle [Hei27], for any single quantum particle, the product of the uncertainties of the position and momentum measurements is at least half of the Planck constant (see also the work of Weyl [Wey27])

$$\Delta X \cdot \Delta P \geqslant \frac{\hbar}{2}. \tag{3.1}$$

Later Robertson [Rob29] derived the uncertainty relation for any pair of observables A and B with bounded spectrums:

$$\Delta A \cdot \Delta B \geqslant \frac{1}{2}|\langle [A,B]\rangle|, \tag{3.2}$$

where $\Delta A^2 = \langle A^2\rangle - \langle A\rangle^2$ is the variance of operator A over the state $|\psi\rangle$. Eq. (3.2) can be derived from a slightly strengthened inequality, the Schrödinger uncertainty relation [Sch30]

$$\Delta A^2 \cdot \Delta B^2 \geqslant |\frac{1}{2}\langle [A,B]\rangle|^2 + |\frac{1}{2}\langle \{\widehat{A},\widehat{B}\}\rangle|^2, \tag{3.3}$$

where $\widehat{A} = A - \langle A\rangle I$ and I is the identity operator.

All these inequalities [BHL07, BLW14a] can be trivial even if A and B are incompatible on the state of the system $|\psi\rangle$, for instance, when $|\psi\rangle$ is an eigenstate of either A or B. Despite of this, the variance-based uncertainty relations possess a clear physical meaning and have variety of applications in the theory of quantum information processing such as entanglement detection [Güh04, HT03], quantum spin squeezing [WZ81, WE85, WBI$^+$92, KU93, MWSN11], and quantum metrology [GLM04, GLM06, GLM11].

Maccone and Pati have presented two stronger uncertainty relations [MP14] based on the sum of variances and their inequalities are guaranteed to be nontrivial when $|\psi\rangle$ is not a common eigenstate of A and B. Though there are many formulations of the uncertainty relation in terms of the sum of entropic quantities [WW10, CBTW15], Maccone and Pati's relations capture the notion of incompatibility except when the state is an eigenstate of the sum of the operators. Their first relation for the sum of the variances is

$$\Delta A^2 + \Delta B^2 \geqslant \pm i\langle [A,B]\rangle + |\langle \psi|A \pm iB|\psi^\perp\rangle|^2 := \mathcal{L}_{MP1}, \tag{3.4}$$

which is valid for any state $|\psi^\perp\rangle$ orthogonal to the state of the system $|\psi\rangle$ while the sign should be chosen so that $\pm i\langle [A,B]\rangle$ is positive. Denote the right-hand (RHS) of Eq. (3.4) by $\mathcal{L}_{MP1}$. Their second uncertainty relation also provides a nontrivial bound even if $|\psi\rangle$ is an eigenstate of A or B:

$$\Delta A^2 + \Delta B^2 \geqslant \frac{1}{2}|\langle \psi^\perp_{A+B}|A+B|\psi\rangle|^2 := \mathcal{L}_{MP2}, \tag{3.5}$$

where $|\psi^\perp_{A+B}\rangle \propto (A+B-\langle A+B\rangle)|\psi\rangle)$ is a state orthogonal to $|\psi\rangle$. It is easy to see that the RHS $\mathcal{L}_{MP2}$ of Eq. (3.5) is nontrivial unless $|\psi\rangle$ is an eigenstate of

$A + B$. Moreover, based on the same techniques, Maccone and Pati also obtained an amended Heisenberg-Robertson inequality:

$$\Delta A \Delta B \geqslant \pm \frac{i}{2}\langle [A, B] \rangle / (1 - \frac{1}{2} \mid \langle \psi | \frac{A}{\Delta A} \pm i \frac{B}{\Delta B} | \psi^{\perp} \rangle \mid^2), \tag{3.6}$$

which reduces to Heisenberg-Robertson's uncertainty relation when minimizing the lower bound over $|\psi^{\perp}\rangle$, and the equality holds at the maximum. The goal of this paper is to give a new method of measuring the uncertainties to remove the restriction on the bounds such as $\mathcal{L}_{MP2}$.

Actually, both the entropic uncertainty relations and the sum form of variance based uncertainty do not suffer from trivial bounds. Generalizing Deutsch's entropic uncertainty relation [Deu83], Maassen and Uffink [MU88] used certain weighted entropic uncertainties to derive a tighter bound. Adopting a similar idea to the uncertainty relations based on Rényi entropy, we propose a *deformed uncertainty relation* to resolve the restriction of Maccone-Pati's variance-based uncertainty relation. i.e. the new uncertainty relation will provide a nontrivial bound even when the state is an eigenvector of $A + B$. Moreover, we show that the original Maccone-Pati's bound is a singular case in our general uncertainty relation and the usual sum of variances can be extracted from weighted sum of uncertainties. Our work indicates that it seems unreasonable to assume a priori that observables A and B have equal contribution to the variance-based sum uncertainty relation. Our family of uncertainty relations are proved to possess an optimal bound in various situations according to the state of the system. In particular, all previous important variance-based sum uncertainty relations are special cases of our weighted uncertainty relation.

We remark that there is another approach of *measurement uncertainty* [BLW13, BLW14b] to the uncertainty principle which deals with joint measurability and measurement-disturbance. Our methods can also be used to generalize the joint measurability, also known as *preparation uncertainty* [BLW13], and to obtain a tighter bound.

Two Observables

We first consider the weighted uncertainty relations based on the sum of variances for two observables, then generalize it to multi-observable cases. All observables considered in the thesis will be assumed to be non-degenerate on a finite-dimensional Hilbert space. We will show that our weighted uncertainty relations give optimal lower bounds and all previous important variance-based sum uncertainty relations are special cases of the new weighted uncertainty relation.

Theorem 3.1.1. *For arbitrary observables A, B and any positive number λ, we have the following weighted uncertainty relation:*

$$\begin{aligned}&(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2\\ \geqslant &-2i\langle[A,B]\rangle+|\langle\psi|(A-iB)|\psi_1^{\perp}\rangle|^2+\lambda^{-1}|\langle\psi|(\lambda A-iB)|\psi_2^{\perp}\rangle|^2:=\mathcal{L}_1,\end{aligned} \tag{3.7}$$

which is valid for all $|\psi_1^{\perp}\rangle$ and $|\psi_2^{\perp}\rangle$ orthogonal to $|\psi\rangle$. If $-2i\langle[A,B]\rangle$ is negative then one changes the sign in Eq. (3.7) to ensure the RHS is positive.

The equality condition for Eq. (3.7) holds if and only if $|\psi_1^{\perp}\rangle\propto(\widehat{A}+i\widehat{B})|\psi\rangle$ while $|\psi_2^{\perp}\rangle\propto(\lambda\widehat{A}+i\widehat{B})|\psi\rangle$. Denote the RHS of Eq. (3.7) by $\mathcal{L}_1$. Clearly $\mathcal{L}_{MP1}$ as a special case of $\mathcal{L}_1$, as $lim_{\lambda\to1}\mathcal{L}_1=\mathcal{L}_{MP1}$. When λ varies, one obtains a family of uncertainty relations and the lower bounds $\mathcal{L}_1$ provide infinitely many uncertainty relations with weighted contributions for measurements A and B. This will be advantageous when the ratio $\langle A\rangle/\langle B\rangle$ is not close to 1.

Proof. We start by recalling the parallelogram law in Hilbert space. Let A and B be two observables and $|\psi\rangle$ a fixed quantum state. One has that

$$2\Delta A^2+2\Delta B^2=\|\ (\widehat{A}+\alpha\widehat{B})|\psi\rangle\ \|^2+\|\ (\widehat{A}-\alpha\widehat{B})|\psi\rangle\ \|^2, \tag{3.8}$$

for any $|\alpha|=1$. Since $\Delta(A+B)=\|\ (\widehat{A}+\widehat{B})|\psi\rangle\ \|$, $\Delta(A-B)=\|\ (\widehat{A}-\widehat{B})|\psi\rangle\ \|$, we can obtain Eq. (3.4) when $\alpha=\pm i$ and Eq. (3.5) when $\alpha=1$. Note that $\mathcal{L}_{MP2}$ may be zero even if A and B are incompatible. For example this happens if $|\psi\rangle$ is an eigenstate of $A+B$. Our idea is to consider a perturbation of $A+B$, or A and B to fix this. We consider the generalized parallelogram law in Hilbert space in the following form:

$$(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2=\|\ (\widehat{A}-\alpha\widehat{B})|\psi\rangle\ \|^2+\lambda^{-1}\ \|\ (\lambda\widehat{A}+\alpha\widehat{B})|\psi\rangle\ \|^2, \tag{3.9}$$

where λ is a nonzero real number and $\alpha\in\mathbb{C}$ with modulus one. In fact, the identity can be easily verified by expanding $\Delta(A-\alpha B)^2$ and $\lambda^{-1}\Delta(\lambda A+\alpha B)^2$ using $\Delta(A)^2=\langle\psi|\widehat{A}^2|\psi\rangle$.

We now derive the *weighted uncertainty relation* in the form $(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2$. Since $\|\ (\widehat{A}-i\widehat{B})|\psi\rangle\ \|^2=-2i\langle[A,B]\rangle+\|\ (\widehat{A}+i\widehat{B})|\psi\rangle\ \|^2$, combine with Cauchy-Schwarz inequality completes the proof. ∎

Theorem 3.1.2. *For arbitrary observables A, B and any positive λ, we have the following weighted uncertainty relation:*

$$\begin{aligned}&(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2\\ \geqslant&|\langle\psi|A+B|\psi_{A+B}^{\perp}\rangle|^2+\lambda^{-1}|\langle\psi|(\lambda A-B)|\psi^{\perp}\rangle|^2:=\mathcal{L}_2,\end{aligned} \tag{3.10}$$

where the equality holds if and only if $|\psi^{\perp}\rangle\propto(\lambda\widehat{A}-\widehat{B})|\psi\rangle$.

Denote the RHS of Eq. (3.10) by $\mathcal{L}_2$. Note that the lower bound $\mathcal{L}_2$ is a nontrivial generalization of $\mathcal{L}_{MP2}$, as the latter is a proper bound unless $|\psi\rangle$ is an eigenstate of $A+B$. Even when $|\psi\rangle$ is an eigenstate of $A+B$, the new uncertainty bound $\mathcal{L}_2$ is also nonzero except for $\lambda=-1$ (Eq. (3.10) still holds for any nonzero real λ). This means that in almost all cases the lower bound provided by Eq. (3.10) is better except for $\lambda\neq-1$ and it compensates for the incompatibility of the observables. Obviously the bound $\mathcal{L}_{MP2}$ is a special case of $\mathcal{L}_2$ by canceling $|\langle\psi|(\lambda A-B)|\psi^{\perp}\rangle|^2$ when $\lambda=1$.

Proof. If we set $\alpha=-1$ in Eq. (3.9), then we get the result directly. ■

Both lower bounds of the weighted uncertainty relations can be combined in a single uncertainty relation for the sum of variances:

Theorem 3.1.3. *For arbitrary observables A, B and any positive number λ, we have the following weighted uncertainty relation:*

$$(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2\geqslant \max(\mathcal{L}_1,\mathcal{L}_2). \tag{3.11}$$

Theorems 3.1.1 and 3.1.2 provide a strengthened uncertainty relation and remove the limitation of the Maccone-Pati bounds. In fact, in the case when $|\psi\rangle$ is an eigenstate of A or B, both Heisenberg-Robertson's and Schrödinger's uncertainty relations are trivial, nevertheless our lower bound remains nonzero unless $|\psi\rangle$ is a common eigenstate of A and B, but this is essentially equivalent to the classical situation. It is also easy to see that if $|\psi\rangle$ is an eigenstate of $A\pm iB$, $|\langle\psi|A\pm iB|\psi^{\perp}\rangle|^2$ in $\mathcal{L}_{MP1}$ will vanish while the term $|\langle\psi|(A-iB)|\psi_1^{\perp}\rangle|^2+\lambda^{-1}|\langle\psi|(\lambda A-iB)|\psi_2^{\perp}\rangle|^2$ in $\mathcal{L}_1$ is still nonzero unless $\lambda=1$. Moreover, $\mathcal{L}_{MP2}$ will become null when $|\psi\rangle$ is an eigenstate of $A+B$, but at the same time $\mathcal{L}_2$ is still nontrivial.

Besides having a nontrivial bound in almost all cases, our weighted uncertainty relations can also lead to a tighter bound for the sum of variances. We give an algorithm to extract the usual uncertainty relation when one of Maccone-Pati's relations becomes trivial. Choose two λ_i: $\lambda_1>1>\lambda_2>0$ and enter our uncertainty relations Eq. (3.7). Denote $b_i=(1+\lambda_i)\Delta A^2+(1+\lambda_i^{-1})\Delta B^2$, then we have for $k=1,2$

$$\begin{aligned}\Delta A^2+\Delta B^2=&\frac{1}{\lambda_1-\lambda_2}\left(\frac{\lambda_1(1-\lambda_2)}{1+\lambda_1}b_1+\frac{\lambda_2(\lambda_1-1)}{1+\lambda_2}b_2\right)\\ \geqslant&\frac{1}{\lambda_1-\lambda_2}\left(\frac{1-\lambda_2}{1+\lambda_1^{-1}}\mathcal{L}_k(\lambda_1)+\frac{\lambda_1-1}{1+\lambda_2^{-1}}\mathcal{L}_k(\lambda_2)\right),\end{aligned} \tag{3.12}$$

which always provides a nontrivial lower bound for the sum of variances even when the state is an eigenvector of $A+B$. This clearly shows that the weighted

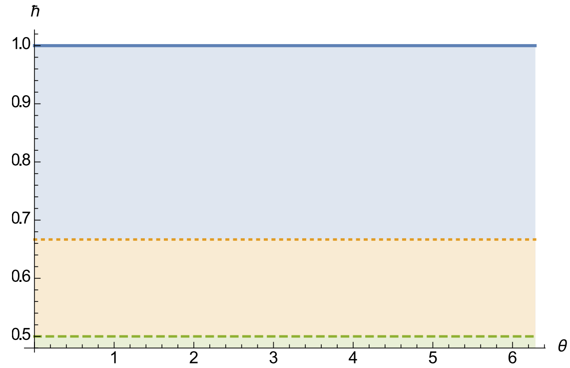

Figure 3.1: Comparison of our bound $\frac{1}{2}\mathcal{L}_2$ with Maccone-Pati's bound $\mathcal{L}_{MP2}$ for operators J_x and J_y in a spin one system. The top solid line is variance sum uncertainty $(\Delta J_x)^2+(\Delta J_y)^2$, the middle dotted line is $\frac{1}{2}\mathcal{L}_2$, and the bottom dashed one is $\mathcal{L}_{MP2}$.

uncertainty relations can help recover the uncertainties and remove the restriction placed in Maccone-Pati's uncertainty relations. Furthermore, taking the limit of $\lambda_i \to 1$ one has that for $k = 1, 2$

$$\Delta A^2 + \Delta B^2 \geqslant \frac{1}{2} lim_{\lambda\to 1}\mathcal{L}_k(\lambda). \tag{3.13}$$

For simplicity we refer to the RHS of Eq. (3.12) or the derived bound in Eq. (3.13) as *our lower bound of the sum of variances*, which usually is a multiple of our bound from the weighted sum (see FIG. 3.1). In FIG. 3.1 one will see that our bound $\frac{1}{2}\mathcal{L}_2$ derived in Eq. (3.13) is always tighter than the Maccone-Pati bound $\mathcal{L}_{MP2}$. In Eq. (3.16) we will use another method to show that our bound is tighter than Maccone-Pati's bound.

As an example to show our lower bound is tighter, we consider the spin one system with the pure state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|2\rangle$, $0 \leqslant \theta < 2\pi$. Take the angular momentum operators [RL08, CF15] with $\hbar = 1$:

$$J_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad J_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \quad J_z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \tag{3.14}$$

Direct calculation gives

$$(\Delta J_x)^2 = \frac{1}{2}(1+\sin\theta), \quad (\Delta J_y)^2 = \frac{1}{2}(1-\sin\theta), \quad (\Delta J_z)^2 = \sin^2\theta;$$

$$[\Delta(J_x+J_y)]^2 = 1, [\Delta(J_y+J_z)]^2 = \frac{1}{2}(1-\sin\theta)+\sin^2\theta, [\Delta(J_x+J_z)]^2 = \frac{1}{2}(1+\sin\theta)+\sin^2\theta;$$

$$[\Delta(J_x + J_y + J_z)]^2 = 1 + \sin^2\theta.$$

To compare Macconne-Pati's uncertainty bound $\mathcal{L}_{MP2}$ in Eq. (3.5) with our bound $\frac{1}{2}\mathcal{L}_2$ in Eq. (3.10) (see also Eq. (3.13)), setting $\lambda = 1$ we get

$$(\Delta J_x)^2 + (\Delta J_y)^2 \geqslant \frac{1}{2}\mathcal{L}_2.$$

Also we have $(\Delta J_x)^2 + (\Delta J_y)^2 = 1$ and $\mathcal{L}_{MP2} = \frac{1}{2}|\langle\psi^{\perp}_{A+B}|A+B|\psi\rangle|^2 = \frac{1}{2}$. Suppose $|\psi^{\perp}\rangle = a|0\rangle + b|1\rangle + c|2\rangle$ with $|a|^2 + |b|^2 + |c|^2 = 1$. Using $\langle\psi|\psi^{\perp}\rangle = 0$ we get

$$\frac{1}{2}\mathcal{L}_2 = \frac{1}{2} + \frac{|b|^2}{2} \geqslant \mathcal{L}_{MP2}.$$

If we choose $a = \frac{1}{\sqrt{3}}, b = \frac{1}{\sqrt{3}}, c = -\frac{1}{\sqrt{3}}$, then $\frac{1}{2}\mathcal{L}_2 = \frac{2}{3}$. Subsequently

$$(\Delta J_x)^2 + (\Delta J_y)^2 > \frac{1}{2}\mathcal{L}_2 > \mathcal{L}_{MP2}.$$

On the other hand, if we set $a = 0, b = 1, c = 0$ then $\frac{1}{2}\mathcal{L}_2 = 1 = (\Delta J_x)^2 + (\Delta J_y)^2 > \mathcal{L}_{MP2}$. Clearly our bound $\frac{1}{2}\mathcal{L}_2$ is tighter than $\mathcal{L}_{MP2}$. The comparison is shown in FIG. 3.1.

We can also consider $(\Delta J_y)^2 + (\Delta J_z)^2$, and direct computation shows $(\Delta J_y)^2 + (\Delta J_z)^2 = \frac{1}{2} + \sin^2\theta - \frac{1}{2}\sin\theta$, $\mathcal{L}_{MP2} = \frac{1}{2}(\frac{1}{2} + \sin^2\theta - \frac{1}{2}\sin\theta)$. Choose $|\psi^{\perp}\rangle = |1\rangle$ then $\frac{1}{2}\mathcal{L}_2 = \frac{1}{2} - \frac{1}{2}\sin\theta + \frac{1}{2}\sin^2\theta$. Therefore

$$(\Delta J_y)^2 + (\Delta J_z)^2 \geqslant \frac{1}{2}\mathcal{L}_2 \geqslant \mathcal{L}_{MP2}.$$

Apparently our bound $\frac{1}{2}\mathcal{L}_2$ is better than $\mathcal{L}_{MP2}$. FIG. 3.2 illustrates the comparison.

The bound $\mathcal{L}_2 = \mathcal{L}_2(\lambda)$ is a function of λ. To analyze when $\mathcal{L}_2(\lambda)$ best approximates $(1+\lambda)\Delta A^2 + (1+\lambda^{-1})\Delta B^2$, we define *the error function* $f(\lambda) = (1+\lambda)\Delta A^2 + (1+\lambda^{-1})\Delta B^2 - \mathcal{L}_2(\lambda)$. At an extremal point λ_0, the bound $\mathcal{L}_2(\lambda)$ is closest to the weighted sum and one of the following two conditions must hold. Either $f'(\lambda_0)$ does not exist or $f'(\lambda_0) = \Delta A^2 - \lambda_0^{-2}\Delta B^2 - \mathcal{L}_2'(\lambda_0) = 0$. If $\mathcal{L}_2'(1) = \Delta A^2 - \Delta B^2$, then $\lambda = 1$ is the extremal point and we call it an *equilibrium point of the uncertainty relation*. In this case both observables A and B give the same contribution to the uncertainty relation. Usually $\lambda = 1$ is not an extremal point, so in general observables A and B contribute unequally to the uncertainty relation.

To see an example of this phenomenon, let's consider again the quantum state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|2\rangle$ $(0 < \theta < 2\pi, \theta \neq \pi)$ and the angular momentum operators. Choose $|\psi^{\perp}\rangle = |1\rangle$, then

$$f(\lambda) = (1+\lambda)\Delta J_y^2 + (1+\lambda^{-1})\Delta J_z^2 - \mathcal{L}_2(\lambda) = \lambda^{-1}\sin^2\theta, \tag{3.15}$$

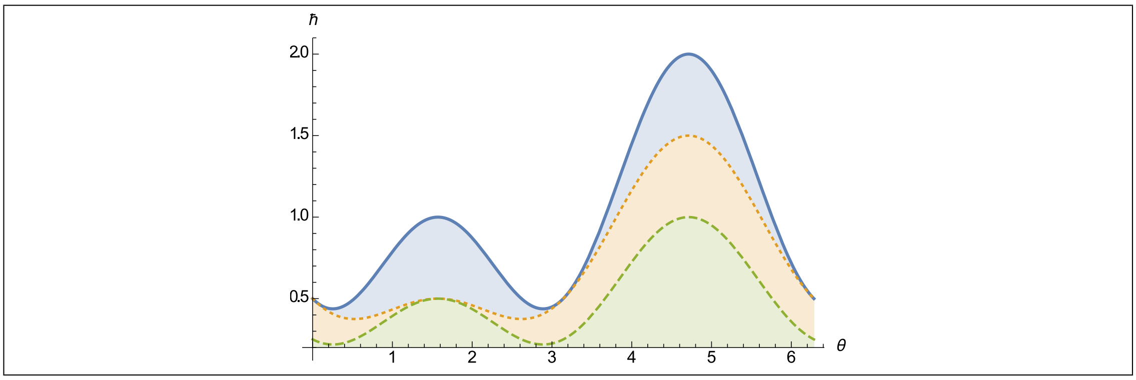

Figure 3.2: Comparison of our bound $\frac{1}{2}\mathcal{L}_2$ with Maccone-Pati's bound $\mathcal{L}_{MP2}$ for operators J_y and J_z in a spin one system. The top solid curve is variance sum uncertainty $(\Delta J_y)^2 + (\Delta J_z)^2$, the middle dotted curve is $\frac{1}{2}\mathcal{L}_2$ and the bottom dashed one is $\mathcal{L}_{MP2}$.

while $f'(\lambda) = -\lambda^{-2}\sin^2\theta < 0$, hence $f(1) > f(\lambda), \forall\lambda > 1$ (for fixed θ). So for this $|\psi\rangle$, J_y and J_z never contribute equally to the uncertainty relation, which explains the need for a weighted uncertainty relation. FIG. 3.3 shows the error function $f(\lambda)$ and $\mathcal{L}_2(\lambda)$. In general f is a function of both λ and θ, finding its extremal points involves a PDE equation. For higher dimension quantum states or multi-operator cases, the situation is more complicated.

In general, all variance-based sum uncertainty relations can mix in weights to provide an optimal lower bound. To compare the variance-based sum uncertainty relation with weighted uncertainty relation, take the lower bound $\mathcal{L}_2$ for a more detailed analysis: set $\lambda = 1$ then $\Delta A^2 + \Delta B^2 \geqslant \frac{1}{2}|\langle\psi|A+B|\psi^{\perp}_{A+B}\rangle|^2 + \frac{1}{2}|\langle\psi|(A-B)|\psi^{\perp}\rangle|^2$, it is not only a typical variance-based sum uncertainty relation, but also provides a better lower bound than Maccone-Pati's lower bound $\mathcal{L}_{MP2}$. Moreover, this lower bound can be further improved by a mixture of weights.

Corollary 3.1.4. *For arbitrary observables A, B and any positive number λ, we have the following weighted uncertainty relation:*

$$\begin{aligned}\Delta A^2 + \Delta B^2 \geqslant & \sup_{\lambda}[|\langle\psi|\frac{1}{\sqrt{1+\lambda}}A + \frac{1}{\sqrt{1+\lambda^{-1}}}B|\psi^{\perp}_{\frac{A}{\sqrt{1+\lambda}}+\frac{B}{\sqrt{1+\lambda^{-1}}}}\rangle|^2 \\ & +\lambda^{-1}|\langle\psi|(\frac{\lambda}{\sqrt{1+\lambda}}A - \frac{1}{\sqrt{1+\lambda^{-1}}}B)|\psi^{\perp}\rangle|^2] \\ \geqslant & \frac{1}{2}|\langle\psi|A+B|\psi^{\perp}_{A+B}\rangle|^2 + \frac{1}{2}|\langle\psi|(A-B)|\psi^{\perp}\rangle|^2, \end{aligned} \tag{3.16}$$

where $|\psi^{\perp}_{\frac{A}{\sqrt{1+\lambda}}+\frac{B}{\sqrt{1+\lambda^{-1}}}}\rangle \propto (\frac{A}{\sqrt{1+\lambda}}+\frac{B}{\sqrt{1+\lambda^{-1}}} - \langle\frac{A}{\sqrt{1+\lambda}}+\frac{B}{\sqrt{1+\lambda^{-1}}}\rangle)|\psi\rangle)$ is a state orthogonal to $|\psi\rangle$.

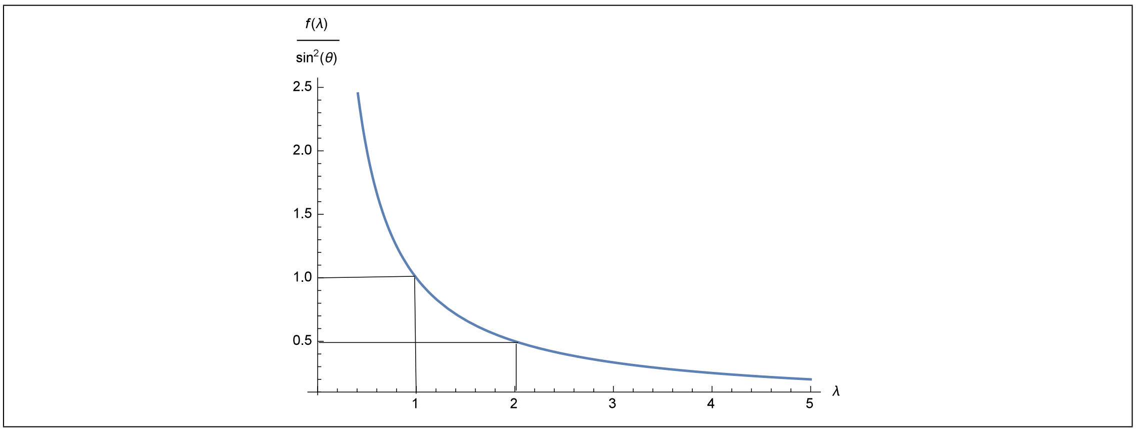

Figure 3.3: Error function Eq. (3.15) of Uncertainty Relation. The figure shows that the difference between uncertainty relation and its bound for fixed form $\mathcal{L}_2(\lambda)$ becomes less when λ increases, which means that better estimation may be obtained through larger λ.

Through Eq. (3.16), it is easy to see $\frac{1}{2}|\langle\psi|A+B|\psi^{\perp}_{A+B}\rangle|^2 + \frac{1}{2}|\langle\psi|(A-B)|\psi^{\perp}\rangle|^2$ is the special case of $\lambda = 1$ and, *a fortiori*, the lower bound with weights is tighter than the standard one.

Proof. For $\lambda > 0$, set $A^{'} = \sqrt{1+\lambda}A, B^{'} = \sqrt{1+\lambda^{-1}}B$ (see Eq. (3.32)), so

$$\begin{aligned}\mathcal{L}_2(\lambda) =& |\langle\psi|\frac{1}{\sqrt{1+\lambda}}A^{'} + \frac{1}{\sqrt{1+\lambda^{-1}}}B^{'}|\psi^{\perp}_{A+B}\rangle|^2 \\ &+\lambda^{-1}|\langle\psi|(\frac{\lambda}{\sqrt{1+\lambda}}A^{'} - \frac{1}{\sqrt{1+\lambda^{-1}}}B^{'})|\psi^{\perp}\rangle|^2,\end{aligned} \tag{3.17}$$

where the RHS $\mathcal{L}_2(\lambda, A^{'}, B^{'})$ satisfies that $\sup_\lambda \mathcal{L}_2(\lambda, A^{'}, B^{'}) \geqslant \mathcal{L}_2(1, A^{'}, B^{'})$ which implies that the weighted uncertainty relation is better than the ordinary sum: $(\Delta A^{'})^2 + (\Delta B^{'})^2 \geqslant \sup_\lambda \mathcal{L}_2(\lambda, A^{'}, B^{'}) \geqslant \mathcal{L}_2(1, A^{'}, B^{'})$. Followed by parameter transformation, we get Eq. (3.16). ■

One can study the general weighted sum of variances $x\Delta A^2 + y\Delta B^2$ based on the special weighted sum $(1+\lambda)\Delta A^2 + (1+\lambda^{-1})\Delta B^2$. Theorem 3.1.5 details the relationship between the general and special weighted sum uncertainty relations.

Theorem 3.1.5. *For arbitrary observables A, B and x, y such that $xy(x+y) > 0$, the following weighted uncertainty relation holds.*

$$x\Delta A^2 + y\Delta B^2 \geqslant \frac{xy}{x+y}\mathcal{L}_2(\frac{x}{y}). \tag{3.18}$$

Proof. For arbitrary weighted uncertainty relation $x\Delta A^2+y\Delta B^2$, denote $f(x,y)=\frac{x+y}{xy}>0$, then

$$x\Delta A^2+y\Delta B^2=\frac{1}{f(x,y)}[f(x,y)x\Delta A^2+f(x,y)y\Delta B^2]. \tag{3.19}$$

Set $\lambda=f(x,y)x-1=\frac{x}{y}$, then $\lambda^{-1}=f(x,y)y-1$. Thus

$$x\Delta A^2+y\Delta B^2=\frac{1}{f(x,y)}[(1+\lambda)\Delta A^2+(1+\lambda^{-1})\Delta B^2]\geqslant\frac{1}{f(x,y)}\mathcal{L}_2(x/y). \tag{3.20}$$

■

According to Deutsch [Deu83], uncertainty in the result of a measurement of observables A and B should be quantified as an inequality with certain lower bound. One can seek such a bound in a general form $\mathcal{U}(A,B,|\psi\rangle)$ which may not simply be a sum or product by weighted uncertainty relations. For instance, we take $\mathcal{U}(A,B,|\psi\rangle)=\frac{1}{1-\Delta A}+e^{\Delta B}$, its bound can be extracted from Theorem 3.1.5.

Remark 3.1.6. For $|\Delta A|<1$ and arbitrary observable B, $\frac{1}{1-\Delta A}+\exp(\Delta B)$ has a nonnegative lower bound:

$$\frac{1}{1-\Delta A}+e^{\Delta B}\geqslant\sum_{n=0}^{\infty}[\frac{\mathcal{L}_2(\sqrt[n]{n!})}{2(\sqrt[n]{n!}+1)}]^n. \tag{3.21}$$

Proof. Since

$$\frac{1}{1-\Delta A}+e^{\Delta B}=\sum_{n=0}^{\infty}[(\Delta A)^n+(\frac{1}{\sqrt[n]{n!}}\Delta B)^n]\geqslant\sum_{n=0}^{\infty}\frac{1}{2^n}(\Delta A+\frac{1}{\sqrt[n]{n!}}\Delta B)^n, \tag{3.22}$$

with $x=1$, $y=\frac{1}{\sqrt[n]{n!}}$, $\lambda=\sqrt[n]{n!}$ and $f(x,y)=\frac{x+y}{xy}$, we get

$$\Delta A+\frac{1}{\sqrt[n]{n!}}\Delta B=\frac{1}{f(x,y)}[(1+\lambda)\Delta A+(1+\lambda^{-1})\Delta B]\geqslant(\sqrt[n]{n!}+1)^{-1}\mathcal{L}_2(\sqrt[n]{n!}), \tag{3.23}$$

thus

$$\frac{1}{1-\Delta A}+e^{\Delta B}\geqslant\sum_{n=0}^{\infty}[\frac{\mathcal{L}_2(\sqrt[n]{n!})}{2(\sqrt[n]{n!}+1)}]^n. \tag{3.24}$$

The right-hand is a positive lower bound of uncertainty relation $\frac{1}{1-\Delta A}+\exp(\Delta B)$. ■

Multi-Observables

We now generalize the weighted uncertainty relations to multi-operator cases. To emphasize our point, we recall the trivial generalization from Maccone-Pati's lower bound.

Lemma 3.1.7. *For arbitrary observables A_i $(i = 1, \ldots, n)$, we have the following variance-based sum uncertainty relation:*

$$\sum_i \Delta A_i^2 \geqslant \frac{1}{n}\Delta S^2 = \frac{1}{n}|\langle\psi|S|\psi_S^\perp\rangle|^2, \tag{3.25}$$

where $|\psi_S^\perp\rangle \propto (S - \langle S\rangle)|\psi\rangle$ is a unit state perpendicular to $|\psi\rangle$ while $S = \sum_i A_i$. The RHS of Eq. (3.25) is nonzero unless $|\psi\rangle$ is an eigenstate of $S = \sum_i A_i$.

Proof. We recall Maccone-Pati's lower bound $\mathcal{L}_{MP2}$ using a different method. Note that $2\Delta A\Delta B \leqslant \Delta A^2 + \Delta B^2$ and $\Delta(A+B) \leqslant \Delta A + \Delta B$, therefore $\Delta A^2 + \Delta B^2 \geqslant \frac{1}{2}\Delta(A+B)^2$. The physical meaning is that the total ignorance of an ensemble of quantum states is less than or equal to the sum of individual ignorance. This means that the sum of uncertainties obeys the convexity property [PS07]:

$$\Delta(\sum_{i=1}^n A_i) \leqslant \sum_{i=1}^n \Delta A_i. \tag{3.26}$$

Let $S = \sum_i A_i$. It follows from Eq. (3.26) that

$$\sum_i \Delta A_i^2 \geqslant \frac{1}{n}\Delta S^2 = \frac{1}{n}|\langle\psi|S|\psi_S^\perp\rangle|^2, \tag{3.27}$$

where $|\psi_S^\perp\rangle \propto (S - \langle S\rangle)|\psi\rangle$ is a unit state perpendicular to $|\psi\rangle$. ■

Notice that $|\psi\rangle$ can be an eigenstate of $\sum_i A_i$ without being that of any A_i, in which case the lower bound is still trivial. However, the bound is not optimal and sometimes becomes trivial when the observables are incompatible in the general situation. We now introduce *generalized weighted uncertainty relations* to deal with these drawbacks.

Theorem 3.1.8. *For arbitrary n observables A_i and positive numbers λ_i, we have following sum uncertainty relation:*

$$\sum_{i,j=1}^n \frac{\lambda_i}{\lambda_j}\Delta A_i^2 \geqslant |\langle\psi|S|\psi_0^\perp\rangle|^2 + \sum_{1\leqslant i<j\leqslant n} |\langle\psi|(\sqrt{\frac{\lambda_i}{\lambda_j}}A_i - \sqrt{\frac{\lambda_j}{\lambda_i}}A_j)|\psi_{ij}^\perp\rangle|^2, \tag{3.28}$$

where $|\psi_{ij}^\perp\rangle \propto (\sqrt{\frac{\lambda_i}{\lambda_j}}\widehat{A}_i - \sqrt{\frac{\lambda_j}{\lambda_i}}\widehat{A}_j)|\psi\rangle$ and $|\psi_0^\perp\rangle$ is any unit state $\perp |\psi\rangle$.

Proof. Using the generalized parallelogram law and Bohr's inequality [Eğe95, HKSM10, KAT86, Zen82, Mos10, Zha07], we obtain the following relation:

$$\sum_{i,j=1}^{n} \frac{\lambda_i}{\lambda_j} \Delta A_i^2 = \| \widehat{S}|\psi\rangle \|^2 + \sum_{1\leqslant i<j\leqslant n} \| (\sqrt{\frac{\lambda_i}{\lambda_j}} \widehat{A}_i - \sqrt{\frac{\lambda_j}{\lambda_i}} \widehat{A}_j)|\psi\rangle \|^2, \tag{3.29}$$

where $S = \sum_{i}^{n} A_i$, $\widehat{S} = S - \langle S \rangle$ and $\lambda_1, \ldots, \lambda_n$ are positive real numbers. Combining with Cauchy-Schwarz inequality, we derive Eq. (3.28). ■

The RHS $\mathcal{L}_0$ of Eq. (3.28) depends on the choice of λ_i. By the same trick and fixing the (i, j)-term of Eq. (3.28), we arrive at

Theorem 3.1.9. *For arbitrary n observables A_i and positive numbers λ_i, we have following sum uncertainty relation:*

$$\begin{aligned} \sum_{i,j=1}^{n} \frac{\lambda_i}{\lambda_j} \Delta A_i^2 \geqslant & |\langle\psi|S|\psi_S^{\perp}\rangle|^2 + |\langle\psi|(\sqrt{\frac{\lambda_i}{\lambda_j}} A_i - \sqrt{\frac{\lambda_j}{\lambda_i}} A_j)|\psi_{ij}^{\perp}\rangle|^2 \\ & + \sum_{1\leqslant k\neq i<l\neq j\leqslant n} |\langle\psi|(\sqrt{\frac{\lambda_k}{\lambda_l}} A_k - \sqrt{\frac{\lambda_l}{\lambda_k}} A_l)|\psi_{kl}^{\perp}\rangle|^2, \end{aligned} \tag{3.30}$$

where $|\psi_{ij}^{\perp}\rangle$ is orthogonal to $|\psi\rangle$, $|\psi_S^{\perp}\rangle \propto (S - \langle S\rangle)|\psi\rangle$, and $|\psi_{kl}^{\perp}\rangle \propto (\sqrt{\frac{\lambda_k}{\lambda_l}} \widehat{A}_k - \sqrt{\frac{\lambda_l}{\lambda_k}} \widehat{A}_l)|\psi\rangle$.

Clearly, $\mathcal{L}_0$ and all the RHS $\mathcal{L}_{ij}$ of Eq. (3.30) comes form Theorem 3.1.8 and Theorem 3.1.9 respectively can be combined into a single uncertainty relation for variances:

Theorem 3.1.10. *For arbitrary n observables A_i and any positive numbers λ_i, we have the following sum uncertainty relation:*

$$\sum_{i,j=1}^{n} \frac{\lambda_i}{\lambda_j} \Delta A_i^2 \geqslant \max_{1\leqslant i<j\leqslant n} (\mathcal{L}_{ij}, \mathcal{L}_0). \tag{3.31}$$

When setting $\lambda_i = \lambda_j$, the RHS of Eq. (3.31) is still stronger than Eq. (3.25), since it keeps all the terms $\sum_{1\leqslant i<j\leqslant n} \| (\sqrt{\frac{\lambda_i}{\lambda_j}} \widehat{A}_i - \sqrt{\frac{\lambda_j}{\lambda_i}} \widehat{A}_j)|\psi\rangle \|^2$ appearing in Eq. (3.28). We remark that a default choice of $|\psi^{\perp}\rangle$ in Eq. (3.30) is by Vaidman's formula [Vai92, GV96]: $|\psi_S^{\perp}\rangle = (S - \langle S\rangle)|\psi\rangle/\Delta S$. We can select suitable λ_i such that $\max(\mathcal{L}_{ij}, \mathcal{L}_0)$ is nontrivial. They are zero if and only if $|\psi\rangle$ is a common

eigenstate of all observables, which happens only when the system is equivalent to the classical situation. In this sense our weighted uncertainty relation can handle all possible quantum situations.

If two or more terms in the RHS of these equality are replaced by the Cauchy-Schwarz's inequality simultaneously, the corresponding lower bound can not be bigger than the one by replacing just one term. In other words, $\max(\mathcal{L}_{ij}, \mathcal{L}_0)$ is better than the lower bounds by changing more than one term. The LHS of Eq. (3.31) has only positive coefficients since λ_i are positive.

Physical Motivations and Mathematical Considerations

There are several physical motivations and mathematical considerations behind our method. First, to remove the restriction of one of Macconne-Pati's uncertainty relations (i.e. when ψ is an eigenstate of $A+B$) and recover the lower bound for $\Delta(A)^2+\Delta(B)^2$, we consider a perturbation of A and B, or rather, $A' = \sqrt{1+\lambda}A$, $B' = \sqrt{1+\lambda^{-1}}B$ ($\lambda > 0$). Then

$$\Delta(A')^2 + \Delta(B')^2 = (1+\lambda)\Delta(A)^2 + (1+\lambda^{-1})\Delta(B)^2. \tag{3.32}$$

This means that the lower bound of the sum of variances can be obtained by scaled observables. Actually with the given measurement data of the variances, it is easy to compute the lower bound using our new formula. This is in line with the general strategy of perturbation method, just as many singular properties can be better studied through deformation.

Secondly, the idea of the weighted sum or average is similar to well-known techniques used in both statistical mechanics and mathematical physics. Through the weighted averages one may know better about the whole picture in an unbiased way.

Thirdly, the weighted sum is actually a q-deformation of the original sum of variances. In fact, the sum $2\Delta(A)^2 + 2\Delta(B)^2$ is deformed to

$$[2]\lambda^{1/2}\Delta(A)^2 + [2]\lambda^{-1/2}\Delta(B)^2,$$

where $[2] = \lambda^{1/2}+\lambda^{-1/2}$ is the quantum integer of 2 used widely in quantum groups, Yang-Baxter equations, and quantum integrable systems or statistical mechanics. The opposite phase factors $\lambda^{\pm 1/2}$ in front of the variances reflect a balance of the weighted distribution.

Last but not the least, the usual sum of variances can be solved from our weighted sums (see Eqs. (3.12-3.13)), and the derived bound is proved to be tighter than the original Maccone-Pati's bound.

The Heisenberg-Robertson and Schrödinger uncertainty relations have been skillfully generalized by Maccone and Pati in order to capture the concept of incompatibility of the observables A and B on the quantum system $|\psi\rangle$. Although other generalizations of Maccone-Pati's relations have been considered [YXWS15] by refining the RHS, our generalization provides a non-trivial lower bound in all quantum situations. One of Maccone-Pati's relations becomes trivial when $|\psi\rangle$ is an eigenstate of $A+B$. To remove the restriction of their relation, we have proposed a weighted uncertainty relation to obtain a better lower bound for the sum of the variances. The parametric uncertainty relations form a family of Bohr-type inequalities and take into account of individual contribution from the observables so that they are nontrivial in almost all cases except when $|\psi\rangle$ is a common eigenstate of all observables. In particular, Maccone-Pati's uncertainty relations are special cases of our deformed weighted uncertainty relations. Furthermore, we have shown that the sum of variances can be extracted from our weighted sums and our derived bound is always tighter than Maccone-Pati bound $\mathcal{L}_{MP2}$ (see discussion before Eq. (3.13)). We have also derived weighted uncertainty relations for multi-observables and the lower bound has been proved to be optimal in all quantum cases.

3.2 Mutually Exclusive Uncertainty Relations

The uncertainty principle is one of the characteristic properties of quantum theory based on incompatibility. Apart from the incompatible relation of quantum states, mutually exclusiveness is another remarkable phenomenon in the information-theoretic foundation of quantum theory. We investigate the role of mutual exclusive physical states in the recent work of [Phys. Rev. Lett **113**, 260401 (2014)] [MP14] and generalize the weighted uncertainty relation [Sci. Rep. **6**, 23201 (2016)] [XJLJF16b] to the product form as well as their multi-observable analogues. The new bounds capture both incompatibility and mutually exclusiveness, and are tighter compared with the existing bounds.

While the early form of variance-based uncertainty relations are vital to the foundation of quantum theory, there are two problems still need to be addressed: (i) Homogeneous product of variances may not fully capture the concept of incompatibility. In other words, a weighted relation may produce a better approximation (e.g., the uncertainty relation with Rényi entropy and variance-based uncertainty relation for a weighted sum), for more details and examples, see [XJLJF16b]; (ii) The existing variance-based uncertainty relations are far from being tight, so improvement is needed. One also needs to know how to generalize the product form to the case of multi-observables for practical applications.

In Sec. 3.1 (see also [XJLJF16b]), we have proposed weighted uncertainty relations to answer the first question and succeeded in improving the uncertainty relation. Let's recall the weighted uncertainty relation for the sum of variances. For arbitrary two incompatible observables A, B and any real number λ, the following inequality holds

$$(1+\lambda)\Delta A^2 + (1+\lambda^{-1})\Delta B^2 \geqslant \max(\mathcal{L}_1, \mathcal{L}_2), \tag{3.33}$$

with

$$\mathcal{L}_1 := -2i\langle [A,B]\rangle + |\langle\psi|(A-iB)|\psi_1^{\perp}\rangle|^2 + \lambda^{-1}|\langle\psi|(\lambda A - iB)|\psi_2^{\perp}\rangle|^2, \tag{3.34}$$

and

$$\mathcal{L}_2 := |\langle\psi|A+B|\psi_{A+B}^{\perp}\rangle|^2 + \lambda^{-1}|\langle\psi|(\lambda A - B)|\psi^{\perp}\rangle|^2, \tag{3.35}$$

where $|\psi_1^{\perp}\rangle$, $|\psi_2^{\perp}\rangle$, $|\psi_{A+B}^{\perp}\rangle$ and $|\psi^{\perp}\rangle$ are orthogonal to $|\psi\rangle$. In information-theoretic context, it is also natural to quantify the uncertainty by weighted products of variances, which also help to estimate individual variance as in [XJLJF16b].

On the other hand, Maccone and Pati obtained an amended Heisenberg-Robertson inequality [MP14]:

$$\Delta A \Delta B \geqslant \pm\frac{i}{2}\langle [A,B]\rangle / (1 - \frac{1}{2} \mid \langle\psi|\frac{A}{\Delta A} \pm i\frac{B}{\Delta B}|\psi^{\perp}\rangle \mid^2), \tag{3.36}$$

which is reduced to Heisenberg-Robertson's uncertainty relation when minimizing the lower bound over $|\psi^{\perp}\rangle$, and the equality holds at the maximum. This amended inequality gives rise to stronger uncertainty relations for almost all incompatible observables, and the improvement is due to the special vector $|\psi^{\perp}\rangle$ perpendicular to the quantum state $|\psi\rangle$. We notice that this can be further improved by using the mutually exclusive relation between $|\psi^{\perp}\rangle$ and $|\psi\rangle$. Moreover, this idea can be generalized to the case of multi-observables. For this reason the strengthen uncertainty relation thus obtained will be called a *mutually exclusive uncertainty relation*.

The goal of this section is to answer the aforementioned two questions to derive the product form of the weighted uncertainty relation, and investigate the physical meaning and applications of the mutual exclusive physical states in variance-based uncertainty relations. Moreover, we will generalize the product form to multi-observables to give tighter lower bounds.

This section is organized as follows. After reviewing recent work on variance-based uncertainty relations, we generalize the weighted uncertainty relations from the sum form [XJLJF16b] to the product form in Sec. 3.2.1. In Sec. 3.2.2 we introduce *mutually exclusive uncertainty relations* and derive a couple of lower bounds based on *mutually exclusive physical states* (MEPS), further we show that they outperform the bound in [MP14]. Finally generalization to multi-observables is also given.

Weighted Relations

The sum form of the uncertainty relation takes equal contribution of the variance from each observable. However, almost all variance-based uncertainty relations do not work for the general situation of incompatible observables, and they often exclude important cases. Sec. 3.1 (see also [XJLJF16b]), we solved this degeneracy problem by considering weighted uncertainty relations to measure the uncertainty in all cases of incompatible observables. Using the same idea, we will study the product form of weighted uncertainty relations to give a new and alternative uncertainty relation in the general situation. The corresponding mathematical tool is the famous *Young's inequality*. The new weighted uncertainty is expected to reveal the lopsided influence from observables. They contain the usual homogeneous relation of $\Delta A^2 \Delta B^2$ as a special case.

Theorem 3.2.1. *Let A, B be two observables such that $\Delta A \Delta B > 0$, and p, q two real numbers such that $\frac{1}{p} + \frac{1}{q} = 1$. Then the following weighted uncertainty relation for the product of variances holds.*

$$(\Delta A^2)^{1/p} (\Delta B^2)^{1/q} \geqslant \frac{1}{p} \Delta A^2 + \frac{1}{q} \Delta B^2, \tag{3.37}$$

where $p < 1$. and the equality holds if and only if $\Delta A = \Delta B$. If $p > 1$, then $\frac{1}{p}\Delta A^2 + \frac{1}{q}\Delta B^2$ becomes a upper bound.

Proof. To prove this, we recall *Young's inequality* [Vla04]: for $\frac{1}{p} + \frac{1}{q} = 1$ and $p < 1$ one has that

$$(\Delta A^2)^{1/p} (\Delta B^2)^{1/q} \geqslant \frac{1}{p} \Delta A^2 + \frac{1}{q} \Delta B^2. \tag{3.38}$$

Note that the right-hand side (RHS) may be negative if $p < 1$. But this can be avoided by using the symmetry of Young's inequality to get

$$(\Delta A^2)^{1/q} (\Delta B^2)^{1/p} \geqslant \frac{1}{q} \Delta A^2 + \frac{1}{p} \Delta B^2 > 0.$$

Thus our bound is nontrivial. We remark that if $p > 1$, it is directly from the *Young's inequality* [Vla04]

$$(\Delta A^2)^{1/p} (\Delta B^2)^{1/q} \leqslant \frac{1}{p} \Delta A^2 + \frac{1}{q} \Delta B^2, \tag{3.39}$$

and equality holds in (3.38) and (3.39) only when $\Delta A = \Delta B$. ∎

The weighted uncertainty relations for the product of variances have a desirable feature: our measurement of incompatibility is weighted, which fits well with the reality that observables usually don't always reach equilibrium, i.e., in physical experiments their contributions may not be the same (cf. [XJLJF16b]). As an illustration, let us consider the *relative error function* between the uncertainty and the weighted bound, which is defined by

$$f(p) = \frac{(\Delta A^2)^{1/p}(\Delta B^2)^{1/q} - \frac{1}{p}\Delta A^2 - \frac{1}{q}\Delta B^2}{(\Delta A^2)^{1/p}(\Delta B^2)^{1/q}}.$$

In general f is a function of both p and $|\psi\rangle$. It is hard to find its extremal points as it involves in partial differential equations. In general the extremal points hardly occurred at homogeneous weights, so incompatible observables usually don't contribute equally to the uncertainty relation, which explains the need for a weighted uncertainty relation in the product form.

Mutually Exclusive Relations

In this subsection, we show how to tighten Maccone and Pati's amended Heisenberg-Robertson uncertainty relation [MP14] by regarding mutually exclusive physical states as another information resource, and then generalize the variance-based uncertainty relation to the case of multi-observables.

The amended Heisenberg-Robertson inequality [MP14] gives that for two incompatible observables A and B,

$$\Delta A \Delta B \geqslant \frac{\pm \frac{i}{2}\langle [A, B]\rangle}{1 - \frac{1}{2}\mid \langle \psi | \frac{A}{\Delta A} \pm i \frac{B}{\Delta B} | \psi^{\perp}\rangle \mid^2}, \tag{3.40}$$

for any unit vector $|\psi^{\perp}\rangle$ orthogonal to $|\psi\rangle$, and the sign is chosen to ensure positivity. Eq. (3.40) reduces to Heisenberg-Robertson's uncertainty relation when minimizing the RHS over $|\psi^{\perp}\rangle$, and recovers the equality when maximizing the RHS over $|\psi^{\perp}\rangle$.

We will refer to (3.40) as a *mutually exclusive uncertainty relation* since the states $|\psi\rangle$ and $|\psi^{\perp}\rangle$ represent two mutual exclusive states in quantum mechanics, which is the main reason for improving the tightness of the bound. Next we move further to improve the bound by combining mutually exclusive relations and the weighted relations.

Maccone and Pati's uncertainty relation can be viewed as a singular case in a family of uncertainty relations parameterized by positive variable λ, which corresponds to our recent work on weighted sum of uncertainty relations [XJLJF16b]. We proceed similarly as the case of the amended Heisenberg-Robertson uncertainty relation by considering a modified square-modulus and Holevo inequalities in Hilbert space [Hol73b] in the following result.

Theorem 3.2.2. *Let A and B be two incompatible observables and* $|\psi\rangle$ *a fixed quantum state. Then the mutually exclusive uncertainty relation holds:*

$$\Delta A \Delta B \geq \frac{\pm i\langle [A,B]\rangle \sqrt{\lambda}}{(1+\lambda)- \mid \langle \psi | \frac{A}{\Delta A} \pm i\frac{\sqrt{\lambda}B}{\Delta B} |\psi^{\perp}\rangle \mid^{2}}, \tag{3.41}$$

for any unit vector $|\psi^{\perp}\rangle$ *perpendicular to* $|\psi\rangle$ *and arbitrary parameter* $\lambda > 0$.

Proof. Here we provide two proofs of the proposed mutually exclusive uncertainty relation (3.41). The first one, based on weighted relations [XJLJF16b], is a natural deformation of [MP14] and is sketched as follows. Using the square-modulus inequality and follow a procedure analogous to the one employed by [MP14], we arrive at (3.41). By maximizing the RHS of (3.41), we see that the maximum $\Delta A \Delta B$ is achieved when the *mutually exclusive physical state* (MEPS) $|\psi^{\perp}\rangle \propto (\frac{\widehat{A}}{\Delta A} \mp i\frac{\sqrt{\lambda}\widehat{B}}{\Delta B})|\psi\rangle$. Clearly our uncertainty relation contains (3.40) as a special case of $\lambda = 1$.

The second proof uses geometric property and is preferred because of its mathematical simplicity and also working for the amended Heisenberg-Robertson uncertainty relation [MP14]. In fact, the RHS of (3.40), denoted by $\mathcal{L}(\lambda, |\psi^{\perp}\rangle)$, is a continuous function of λ and the unit MEPS $|\psi^{\perp}\rangle$. By the vector projection, the maximum value $\Delta A \Delta B$ of $\mathcal{L}(\lambda, |\psi^{\perp}\rangle)$ over the hyperplane of $|\psi^{\perp}\rangle$ is attained when $|\psi^{\perp}\rangle \propto (\frac{\widehat{A}}{\Delta A} \mp i\frac{\sqrt{\lambda}\widehat{B}}{\Delta B})|\psi\rangle$. Therefore for any $\lambda > 0$

$$\max_{|\psi^{\perp}\rangle} \mathcal{L}(\lambda, |\psi^{\perp}\rangle) = \max_{|\psi^{\perp}\rangle} \mathcal{L}(1, |\psi^{\perp}\rangle) = \Delta A \Delta B,$$

where $\mathcal{L}(1, |\psi^{\perp}\rangle)$ is the RHS of (3.40). Similarly

$$\min_{|\psi^{\perp}\rangle} \mathcal{L}(\lambda, |\psi^{\perp}\rangle) = \frac{\pm i\langle [A,B]\rangle \sqrt{\lambda}}{1+\lambda} \leqslant \frac{\pm i\langle [A,B]\rangle}{2},$$

for any $\lambda > 0$ and the equality holds if $\lambda = 1$, which implies (3.41) and completes the second proof. ■

The obtained variance-based uncertainty relation is stronger than Maccone and Pati's amended uncertainty relation. In fact, when the maximal value $\mathcal{L}(\lambda_0, |\psi^{\perp}\rangle)$ is reached at a point $\lambda_0 \neq 1$, the new bound is stronger than that of Maccone-Pati's amended uncertainty relation. Let $\mathcal{L}(\lambda_i, |\psi_i^{\perp}\rangle)$ $(i = 1, 2)$ be two lower bounds given in the RHS of (3.41), define the *tropical sum*

$$\mathcal{L}(|\psi^{\perp}\rangle) = \max\{\mathcal{L}(\lambda_1, |\psi^{\perp}\rangle), \mathcal{L}(\lambda_2, |\psi^{\perp}\rangle)\}. \tag{3.42}$$

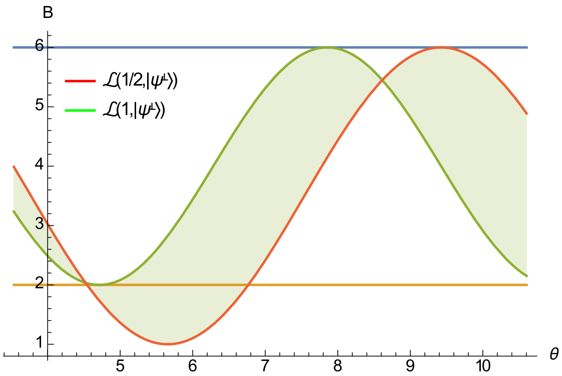

Figure 3.4: Schematic comparison of bounds: Top and middle line are $\Delta A \Delta B$ and $\pm\frac{i}{2}\langle[A,B]\rangle$ resp. Tropical sum $\max(\mathcal{L}(1,|\psi^{\perp}\rangle),\mathcal{L}(\frac{1}{2},|\psi^{\perp}\rangle))$ is the upper boundary above the shadow, and the red and green ones are $\mathcal{L}(\frac{1}{2},|\psi^{\perp}\rangle)$ and Maccone-Pati's bound $\mathcal{L}(1,|\psi^{\perp}\rangle)$ resp.

This gives a tighter lower bound when the maximal value of $\mathcal{L}(\lambda_i,|\psi_i^{\perp}\rangle)$ is reached at different direction in H_ψ (hyperplane that orthogonal to $|\psi\rangle$) for $|\psi_i^{\perp}\rangle$. In other words, the new lower bound is a piecewise defined function of MEPS $|\psi^{\perp}\rangle \in H_\psi$ taking the maximum of the two bounds. In particular, for $\lambda_0 \neq 1$, the tropical sum $\max\{\mathcal{L}(1,|\psi^{\perp}\rangle),\mathcal{L}(\lambda_0,|\psi^{\perp}\rangle)\}$ offers a better lower bound than $\mathcal{L}(1,|\psi^{\perp}\rangle)$, the Maccone-Pati's lower bound. Note that $\mathcal{L}(\lambda,|\psi^{\perp}\rangle)$ may have a smaller minimum value than $\mathcal{L}(1,|\psi^{\perp}\rangle)$ when $\lambda \neq 1$, as $\frac{2\sqrt{\lambda}}{1+\lambda} \leqslant 1$, while the minimum value of $\mathcal{L}(1,|\psi^{\perp}\rangle)$ is just the bound for Heisenberg-Robertson's uncertainty relation. Because we only consider the maximum, it does not affect our result.

For example, consider a 4-dimensional system with state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$, $0 \le \theta < \frac{\pi}{2}$ and take the following observables

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & -i & 0 & 0 \\ i & -1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}. \tag{3.43}$$

Direct calculation gives

$$\Delta A = \cos\theta, \Delta B = \sqrt{2-\cos^2\theta};$$

and

$$\langle A\rangle = \sin\theta, \langle B\rangle = \cos\theta.$$

For $\theta = \frac{\pi}{3}$ and $\lambda = \frac{1}{2}$, set

$$|\psi_1^{\perp}\rangle \propto (2-\sqrt{7}+\sqrt{3}i)|0\rangle + (\sqrt{21}-2\sqrt{3}-3i)|1\rangle,$$

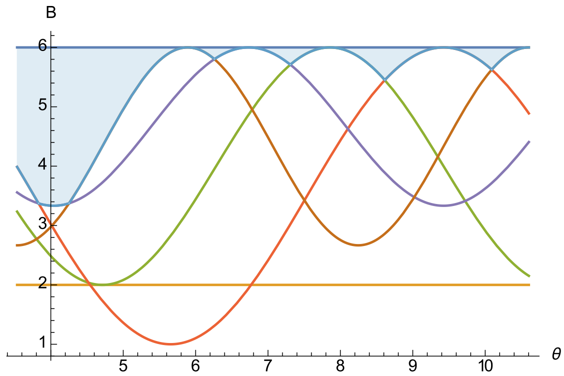

Figure 3.5: Schematic comparison: Top line is $\Delta A\Delta B$. Blue curve is our bound $\max_\lambda(\mathcal{L}(\lambda,|\psi^\perp\rangle))$, the shadow region is the difference between $\Delta A\Delta B$ and our bound $\max_\lambda(\mathcal{L}(\lambda,|\psi^\perp\rangle))$. Other bounds are shown in different colors.

and

$$|\psi_2^\perp\rangle \propto (2-\sqrt{14}+\sqrt{3}i)|0\rangle + (\sqrt{42}-2\sqrt{3}-3i)|1\rangle,$$

both of them have modulus one, then

$$\mathcal{L}(1,|\psi_1^\perp\rangle\rangle = \mathcal{L}(\frac{1}{2},|\psi_2^\perp\rangle\rangle = \Delta A\Delta B = \frac{\sqrt{7}}{4},$$

meanwhile

$$\mathcal{L}(1,|\psi_2^\perp\rangle) \approx 0.567628 < \mathcal{L}(\frac{1}{2},|\psi_2^\perp\rangle\rangle = \frac{\sqrt{7}}{4},$$

so

$$\max\{\mathcal{L}(1,|\psi^\perp\rangle),\mathcal{L}(\frac{1}{2},|\psi^\perp\rangle)\} \geqslant \mathcal{L}(1,|\psi^\perp\rangle). \tag{3.44}$$

Both the lower bounds $\max\{\mathcal{L}(1,|\psi^\perp\rangle),\mathcal{L}(\frac{1}{2},|\psi^\perp\rangle)\}$ and $\mathcal{L}(1,|\psi^\perp\rangle)$ are functions of MEPS $|\psi^\perp\rangle$. However, for each $|\psi^\perp\rangle$, $\max\{\mathcal{L}(1,|\psi^\perp\rangle),\mathcal{L}(\frac{1}{2},|\psi^\perp\rangle)\}$ gives a better approximation of $\Delta A\Delta B$ than $\mathcal{L}(1,|\psi^\perp\rangle)$. FIG. 3.4 is a schematic diagram of these two lower bounds. It is clear that $\max_\lambda\{\mathcal{L}(\lambda,|\psi^\perp\rangle)\}(\lambda > 0)$ provides a closer estimate to $\Delta A\Delta B$:

$$\Delta A\Delta B \geq \max_\lambda\{\mathcal{L}(\lambda,|\psi^\perp\rangle)\}, \tag{3.45}$$

for any unit MEPS $|\psi^\perp\rangle$ orthogonal to $|\psi\rangle$. This is due to the fact that the bound $\max_\lambda\{\mathcal{L}(\lambda,|\psi^\perp\rangle)\}$ is continuous on both MEPS $|\psi^\perp\rangle$ and λ, which shows an advantage of our mutually exclusive uncertainty principle. The shadow region in FIG. 3.5. illustrates the outline of $\Delta A\Delta B$ and our bound $\max_\lambda\{\mathcal{L}(\lambda,|\psi^\perp\rangle)\}$.

Mutually exclusive physical states with different directions in H_ψ offer different kinds of mutually exclusive information and improvement of the uncertainty relation. When such an experiment of the mutually exclusive uncertainty relation is performed, one is expected to have infinitely many strong lower bounds of the variance-based uncertainty relation.

Now we further generalize the uncertainty relations to multi-observables cases. For simplicity, write $\mathcal{L}(\lambda, |\psi^\perp\rangle)$ as $\pm\frac{i}{2}\langle[A,B]\rangle f(\lambda, |\psi^\perp\rangle; A, B)$. So

$$f(\lambda, |\psi^\perp\rangle; A, B) = \frac{2\sqrt{\lambda}}{(1+\lambda) - |\langle\psi|\frac{A}{\Delta A} \pm i\frac{\sqrt{\lambda}B}{\Delta B}|\psi^\perp\rangle|^2}, \tag{3.46}$$

is continuous on both MEPS $|\psi^\perp\rangle$ and λ. Repeatedly using (3.41) for $|\psi_{jk}^\perp\rangle$ and λ_{jk}, we obtain the following relation.

Theorem 3.2.3. *Let A_1, A_2, $\cdots$, A_n be n incompatible observables and $|\psi\rangle$ a fixed quantum state with positive real numbers λ_{jk}, we have*

$$\Delta A_1 \Delta A_2 \cdots \Delta A_n \geq (-\frac{i}{2})^{\frac{n}{2}} \max_{\lambda_{jk}} [\prod_{j>k} (f(\lambda_{jk}, |\psi_{jk}^\perp\rangle; A_j, A_k)) \langle [A_j, A_k] \rangle]^{\frac{1}{n-1}}, \tag{3.47}$$

for any MEPS $|\psi_{jk}^\perp\rangle$ orthogonal to $|\psi\rangle$ with modulus one, and the sign is chosen to ensure positivity. The equality holds if and only if MEPS $|\psi_{jk}^\perp\rangle \propto (\frac{\widehat{A}_j}{\Delta A_j} \mp i\frac{\sqrt{\lambda_{jk}}\widehat{A}_k}{\Delta A_k})|\psi\rangle$ for all $j > k$.

As a corollary, Theorem 3.2.3 leads to a simply bound for multi-observables uncertainty relations

Corollary 3.2.4. *Let A_1, A_2, $\cdots$, A_n be n incompatible observables, the following uncertainty relation holds*

$$\Delta A_1 \Delta A_2 \cdots \Delta A_n \geq (-\frac{i}{2})^{\frac{n}{2}} [\prod_{j>k} \langle [A_j, A_k] \rangle]^{\frac{1}{n-1}}. \tag{3.48}$$

Proof. Obviously, taking the minimum of (3.47) over MEPS $|\psi_{jk}^\perp\rangle$ implies that

$$\begin{aligned}
&\Delta A_1 \Delta A_2 \cdots \Delta A_n \\
\geq &(-\frac{i}{2})^{\frac{n}{2}} \max_{\lambda_{jk}} [\prod_{j>k} \frac{2\sqrt{\lambda_{jk}}}{1+\lambda_{jk}} \langle [A_j, A_k] \rangle]^{\frac{1}{n-1}} \\
= &(-\frac{i}{2})^{\frac{n}{2}} [\prod_{j>k} \langle [A_j, A_k] \rangle]^{\frac{1}{n-1}}.
\end{aligned} \tag{3.49}$$

When $\lambda_{jk} = 1$ for all $j > k$, the minimum is $(-\frac{i}{2})^{\frac{n}{2}}[\prod_{j>k}\langle[A_j, A_k]\rangle]^{\frac{1}{n-1}}$. Meanwhile if λ_{jk} and MEPS $|\psi_{jk}^{\perp}\rangle$ vary, Eq. (3.47) provides a family of mutually exclusive uncertainty relations for arbitrary n observables with Eq. (3.49) as the lower bound. ■

In what follows we provide yet another mutually exclusive uncertainty relation. Let g be the function

$$g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) = \frac{|\frac{1}{2}\langle[A, B]\rangle|^2}{(1 - \frac{1}{2}|\langle|\psi|\frac{A}{\Delta A} + i\frac{B}{\Delta B}|\psi_1^{\perp}\rangle|^2)^2} + \frac{|\frac{1}{2}\langle\{A, B\}\rangle - \langle A\rangle\langle B\rangle|^2}{(1 - \frac{1}{2}|\langle|\psi|\frac{A}{\Delta A} + \frac{B}{\Delta B}|\psi_2^{\perp}\rangle|^2)^2}, \tag{3.50}$$

where MEPS $|\psi_i^{\perp}\rangle$ are unit vectors in H_{ψ_i}. By the same method used in deriving Eq. (3.41) it follows that $\max_{|\psi_i^{\perp}\rangle} g = 2\Delta A^2\Delta B^2$, and $\min_{|\psi_i^{\perp}\rangle} g$ is

$$s = |\frac{1}{2}\langle[A, B]\rangle|^2 + |\frac{1}{2}\langle\{A, B\}\rangle - \langle A\rangle\langle B\rangle|^2, \tag{3.51}$$

which equals to the lower bound of the Schrödinger uncertainty (3.3). We can modify g into a function with the same maximum and the lower bound as Schrödinger uncertainty relation. Note that $s \leq \Delta A^2\Delta B^2$, then

$$\Delta A^2\Delta B^2 \geq (g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) - s)\frac{\Delta A^2\Delta B^2 - s}{2\Delta A^2\Delta B^2 - s} + s, \tag{3.52}$$

which is equivalent to (by solving $\Delta A^2\Delta B^2$)

$$\Delta A^2\Delta B^2 \geq \frac{(g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) + 2s) + |g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) - 2s|}{4}, \tag{3.53}$$

for any unit MEPS $|\psi_i^{\perp}\rangle (i = 1, 2)$ orthogonal to $|\psi\rangle$. In fact, let $h(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle)$ be the RHS of Eq. (3.53). It is easy to see that $\max_{|\psi_i^{\perp}\rangle} h = \Delta A^2\Delta B^2$ and

$$\min_{|\psi_i^{\perp}\rangle} h = |\frac{1}{2}\langle[A, B]\rangle|^2 + |\frac{1}{2}\langle\{\hat{A}, \hat{B}\}\rangle|^2 = s.$$

Hence (3.53) can be seen as an *amended Schrödinger inequality* and also offers a better bound than (3.3) and Maccone-Pati's relation (3.40). FIG. 3.6 illustrates the schematic comparison. Hence we have following mutually exclusive uncertainty relation.

Theorem 3.2.5. *Let A and B be two incompatible observables and $|\psi\rangle$ a fixed quantum state. Then*

$$\Delta A^2\Delta B^2 \geq \frac{(g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) + 2s) + |g(|\psi_1^{\perp}\rangle, |\psi_2^{\perp}\rangle) - 2s|}{4}, \tag{3.54}$$

for any unit MEPS $|\psi_i^{\perp}\rangle (i = 1, 2)$ orthogonal to $|\psi\rangle$.

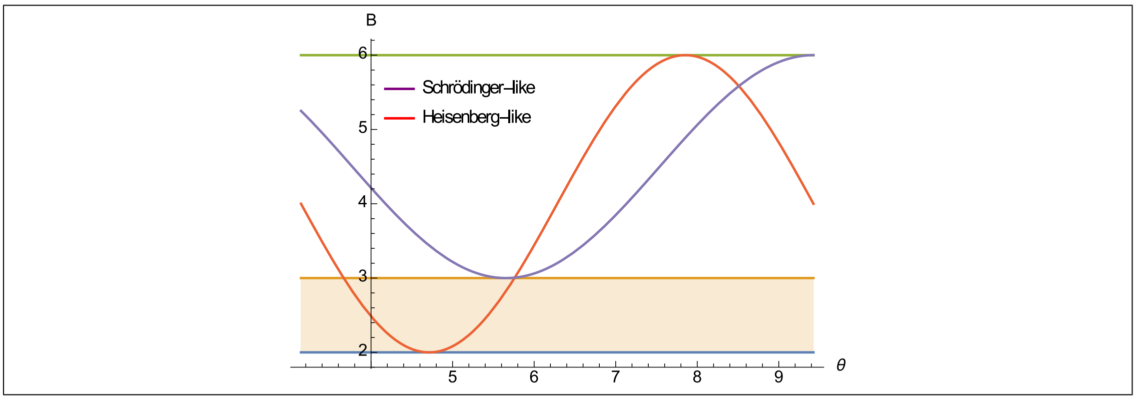

Figure 3.6: Schematic comparison of uncertainty relations: Top, middle and bottom line is $\Delta A^2 \Delta B^2$, Schrödinger bound and the square of Heisenberg bound resp. Orange and purple curve is the square of Maccone and Pati's amended Heisenberg bound and our amended Schrödinger bound resp.

In general, if there exists an operator M for A and B such that $\langle M \rangle = 0$, $\langle MM^\dagger \rangle = 2 \pm 2\frac{\langle \widehat{A}\widehat{B} \rangle}{\Delta A \Delta B}$, then we have the following:

Remark 3.2.6. Let A and B be two incompatible observables and $|\psi\rangle$ a fixed quantum state. We claim that the following mutually exclusive uncertainty relation holds:

$$\Delta A^2 \Delta B^2 \geq \frac{|\ \frac{1}{2}\langle [A, B] \rangle\ |^2 + |\ \frac{1}{2}\langle \{\widehat{A}, \widehat{B}\} \rangle |^2}{(1 - \frac{1}{2}\ |\ \langle \psi | M | \psi^\perp \rangle\ |^2)^2}, \tag{3.55}$$

Eq. (3.55) also give a generalized Schrödinger uncertainty relation. Here as usual MEPS $|\psi^\perp\rangle$ is any unit vector perpendicular to $|\psi\rangle$. The proof of Theorem 3.2.5 and Remark 3.2.6 are similar to that of Theorem 3.2.2, so we sketch it here. It is easy to see that the RHS of (3.55) reduces to the lower bound of Schrödinger's uncertainty relation (3.3) when minimizing over $|\psi^\perp\rangle$, and the equality holds at the maximum. The corresponding uncertainty relation for arbitrary n observables is the following result.

Theorem 3.2.7. *Let A_1, A_2, ..., A_n be n incompatible observables, $|\psi\rangle$ a fixed quantum state and λ_{jk} positive real numbers. Then we have that*

$$\Delta A_1^2 \Delta A_2^2 \cdots \Delta A_n^2 \geq [\prod_{j>k} \frac{|\ \frac{1}{2}\langle [A_j, A_k] \rangle\ |^2 + |\ \frac{1}{2}\langle \{\widehat{A}_j, \widehat{A}_k\} \rangle\ |^2}{(1 - \frac{1}{2}\ |\ \langle \psi | M_{jk} | \psi_{jk}^\perp \rangle\ |^2)^2}]^{\frac{1}{n-1}}, \tag{3.56}$$

where M_{jk} satisfy $\langle M_{jk} \rangle = 0$, $\langle M_{jk} M_{jk}^\dagger \rangle = 2 \pm 2\frac{\langle \widehat{A_j}\widehat{A_k} \rangle}{\Delta A_j \Delta A_k}$ and MEPS $|\psi_{jk}^\perp\rangle$ orthogonal *to $|\psi\rangle$ with modulus one. The RHS of Eq. (3.56) has the minimum value*

$$[\prod_{j>k}(|\ \frac{1}{2}\langle[A_j, A_k]\rangle\ |^2 + |\ \frac{1}{2}\langle\{\widehat{A}_j, \widehat{A}_k\}\rangle\ |^2)]^{\frac{1}{n-1}},$$

and the equality holds at the maximal.

Therefore one obtains the following corollary.

Corollary 3.2.8. *Let A_1, A_2, $\cdots$, A_n be n incompatible observables, the following uncertainty relation holds*

$$\Delta A_1 \Delta A_2 \cdots \Delta A_n \geq [\prod_{j>k}(|\ \frac{1}{2}\langle[A_j, A_k]\rangle\ |^2 + |\ \frac{1}{2}\langle\{\widehat{A}_j, \widehat{A}_k\}\rangle\ |^2)]^{\frac{1}{n-1}}. \tag{3.57}$$

We note that our enhanced Schrödinger uncertainty relations offer significantly tighter lower bounds than that of Maccone-Pati's uncertainty relations for multi-observables, as our lower bound contains an extra term of $|\frac{1}{2}\langle\{\widehat{A}, \widehat{B}\}\rangle|^2$ (compare Eq. (3.2) and Eq. (3.3)).

Finally, we remark that we can also replace the non-hermitian operator $\frac{A}{\Delta A} \pm i\frac{B}{\Delta B}$ in Eq. (3.40) by a hermitian one. A natural consideration is the amended uncertainty relation

$$\Delta A \Delta B \geq \frac{\frac{1}{2}\ |\ \langle\{A, B\}\rangle - \langle A\rangle\langle B\rangle\ |}{1 - \frac{1}{2}\ |\ \langle|\psi|\frac{A}{\Delta A} + \frac{B}{\Delta B}|\psi^{\perp}\rangle\ |^2}, \tag{3.58}$$

for any unit MEPS $|\psi^{\perp}\rangle$ perpendicular to $|\psi\rangle$. The corrresponding uncertainty relation for multi-observables can also be generalized.

The minimum of Maccone and Pati's amended bound $\mathcal{L}(1, |\psi^{\perp}\rangle)$ in the RHS of Eq. (3.40) agrees with the bound in Heisenberg-Robertson's uncertainty relation, which is weaker than Schrödinger's bound in Eq. (3.3). We point out that the bound given as a continuous function of MEPS will always produce a better lower bound. In fact, the continuity of $\mathcal{L}(1, |\psi^{\perp}\rangle)$ in MEPS $|\psi^{\perp}\rangle$ implies that there exists suitable $|\psi_0^{\perp}\rangle$ such that $\mathcal{L}(1, |\psi_0^{\perp}\rangle)$ is tighter than the bound of Heisenberg-Robertson's uncertainty relation. Similarly our lower bound given in Eq. (3.53) or more generally in Eq. (3.55) provides a tighter lower bound than the enhanced Schrödinger's uncertainty relation (3.3). This shows the advantage of lower bounds with MEPS. Furthermore, lower bounds with more variables give better estimates for the product of variances of observables, as in Eq. (3.56).

The Heisenberg-Robertson uncertainty relation is a fundamental principle of quantum theory. It has been recently generalized by Maccone and Pati to an enhanced uncertainty relation for two observables via mutually exclusive physical states. Based on these and weighted uncertainty relations [XJLJF16b], we have derived uncertainty relations for the product of variances from mutually exclusive physical states (MEPS) and offered tighter bounds.

In summary, we have proposed generalization of variance-based uncertainty relations. By virtue of MEPS, we have introduced a family of infinitely many Schrödinger-like uncertainty relations with tighter lower bounds for the product of variances. Indeed, our mutually exclusive uncertainty relations can be degenerated to the classical variance-based uncertainty relations by fixing MEPS and the weight. Also, our study further shows that the mutually exclusiveness between states is a promising information resource.

Chapter 4

Uniform Entanglement Frames

Before introducing our main results of entropic uncertainty relations based on majorization theory, we will utilize majorization method to construct several criteria for genuine multipartite entanglement. Under non-negative Schur-concave functions, the vector-type uncertainty relation generates a family of infinitely many detectors to check genuine multipartite entanglement. We also introduce the concept of k-separable circles via geometric distance for probability vectors, which include at most $(k-1)$-separable states. The entanglement witness is also generalized to a universal entanglement witness which is able to detect the k-separable states more accurately.

Entanglement is spotted as a salient feature of quantum theory, which has been a source for new computational methods and algorithms in quantum information theory. Numerous criteria of entanglement have been discovered for pure and mixed quantum states, and many of them are devoted to entanglement of bipartite states. For a multipartite system, separability can be classified into k-separability [GHH10] and the quantum state is called genuinely entangled if it is not separable with respect to any tensor bipartition of its space (see Sec. 4.2 for detailed definition). Due to the importance of genuine entanglement, numerous approaches have been devoted to detecting genuinely multipartite entanglement. Among the influential ones, the methods using entanglement witness [HS14, HMGH10, WKB+12, HPLdV13, SV13, JMG11, MLPŻ13, dVH11], generalized concurrence [MCC+11, CMCS12, HGY12, GYvE14, LFLJF15], and Bell-inequality [BGLP11] are very useful. Nevertheless, the problem of detecting genuinely entanglement is far from being solved.

The principle behind the entanglement witnesses is that entanglement of multiparity quantum states gives rise to nonlocal correlations of measurement observers, whose measurement outcomes obey certain bounds. In particular the lower bound of the uncertainty relation is expected to provide better entanglement witnesses. In this paper, we use the universal uncertainty relation and majorization theory to derive further criteria for k-separability and genuine entanglement.

We take mixed three-qubit states as an example to explain our approach to entanglement using majorization. In [ABLS01], mixed three-qubit states have been classified into three classes of genuine three-qubit entanglement (W-type, GHZ-type), biseparable and fully separable states. Our approach not only gives a new method to detect entanglement, but also provides a fine tuned devise to further classify biseparable states into three subclasses of $AB-C$, $A-BC$, and $AC-B$ types. Furthermore, we introduce the notion of a *universal entanglement witness* and derive its canonical form, which can be used to picture layers of k-separability [GHH10] as concentric circles.

In this chapter, we propose a general framework for constructing genuine entanglement criteria that are based on uncertainty relations. In the original Heisenberg-Robertson [Hei27, Rob29] uncertainty relation, the lower bound of the product of standard deviations of two incompatible observables A and B is given by

$$\Delta A \cdot \Delta B \geqslant \frac{1}{2}|\langle[A,B]\rangle|, \tag{4.1}$$

where ΔA is the standard deviation of A respect to the quantum state $|\psi\rangle$. Usually the uncertainty relations in terms of standard deviations is state-dependent (but see [XJLJF16b]).

Entropy has also been used as a measure [Hir57] for the uncertainty principle. Deutsch [Deu83] showed that the lower bound of the entropy uncertainty relation (EUR) in a finite dimensional Hilbert space is

$$H(p) + H(q) \geqslant -2\ln C, \tag{4.2}$$

where $C = (1+\sqrt{c_1})/2$ and $c_1 = max_{i,j}|\langle a_i|b_j\rangle|^2$ is the maximal overlap between the bases $|a_i\rangle$ and $|b_j\rangle$, p and q are the probability distributions in the usual manner. In this form the lower bound is independent on the state. Other uncertainty relations and improvements have been given in [MU88] and [CP14], where the lower bound are mostly state-independent and computable from two probability vectors. Good surveys for these bounds can be found in [WW10, BP85, DHL+04, OW10, Güh04, BVL05, CBTW15].

The universality of the information-based uncertainty principle gives a unbreakable lower bound that holds in general. In fact, the uncertainty relations can be quantified by majorization [Par11], which has numerous advantages over previous formulations. The *universal uncertainty relation* (UUR) based on majorization can be formulated as [FGG13, PRŻ13]

$$p(\rho) \otimes q(\rho) \prec \omega, \quad \forall\ \rho, \tag{4.3}$$

where ρ is any mixed state on a finite dimensional Hilbert space and ω is a certain probability vector independent of ρ. Here the *majorization* '$\prec$ ' is certain partial order among real vectors [AMO11] (see Sec. 4.1 for definition). In what follows, we will also generalize the UUR principle to other situations and use them to give new entanglement tests for k-separability.

This chapter is roughly organized as follows. First we review some basic backgrounds of majorization theory and the UUR in Sec. 4.1. Then we prove a universal lower bound for partial separable states and use the lower bound to give criteria for genuine entanglement and k-separability in Sec. 4.2. Finally, in Sec. 4.3 we discuss the matrix form of majorization and show how it is used to provide better tests for entanglement of multipartite mixed states.

4.1 Background Materials

We review some basic materials of majorization theory [AMO11], the UUR, and the elementary classification of mixed three-qubit states following mostly [ABLS01].

A real vector $x \in \mathbb{R}^d$ is *majorized by* (denoted as $\prec$) another real vector $y \in \mathbb{R}^d$ provided that $\sum_{j=1}^{k} x_j^{\downarrow} \leqslant \sum_{j=1}^{k} y_j^{\downarrow}$ for all $1 \leqslant k \leqslant d-1$ and $\sum_{j=1}^{d} x_j^{\downarrow} = \sum_{j=1}^{d} y_j^{\downarrow}$. The down-arrow means to rearrange the components of the vector in the decreasing order: $x_1^{\downarrow} \geqslant x_2^{\downarrow} \geqslant \cdots \geqslant x_d^{\downarrow}$. If $x \prec y$ but $x \neq y$, then x is said to be strictly majorized by y and written as $x \prec\prec y$. In general, any probability vectors $x \in \mathbb{R}^d$ satisfies that $(\frac{1}{d}, \frac{1}{d}, \cdots, \frac{1}{d}) \prec x \prec (1, 0, \cdots, 0)$.

Consider an n-partite density matrix ρ ($n \geqslant 2$) with positive operator valued measures (POVMs). Let $\{X_l, E_{\alpha_l}^{X_l}\}_{\alpha_l=1}^{N_l}$ be the l-th POVM, where $1 \leqslant l \leqslant n$ and N_l is the number of elements of the l-th POVM. A measurement of ρ with the l-th POVM X_l induces a probability distribution vector $p^l(\rho) = (p_1^l(\rho), p_2^l(\rho), \cdots, p_{N_l}^l(\rho))$, where $p_j^l(\rho) = tr(\rho E_{\alpha_j}^{X_l})$. Then a uncertainty of the form

$$\bigotimes_{l=1}^{n} p^l(\rho) \prec \omega, \quad \forall\ \rho, \tag{4.4}$$

holds, where the LHS represents the joint probability distribution induced by measuring ρ with each POVM X_l. The multitensor product is defined by associativity as follows. Suppose $a \in \mathbb{R}^m$ and $b \in \mathbb{R}^n$, then the tensor product $a \otimes b$ is the vector $(a_1 b_1, \cdots, a_1 b_n, \cdots, a_m b_n)$ in $\mathbb{R}^{mn}$.

The vector ω is independent of ρ. If the measurement elements X_l do not have a common eigenstate, then $\omega \prec\prec (1, 0, \cdots, 0)$. Moreover for any uncertainty measure Φ, a nonnegative Schur-concave function, one has that

$$\Phi[\bigotimes_{l=1}^{n} p^l(\rho)] \geqslant \Phi(\omega), \quad \forall\ \rho. \tag{4.5}$$

For example, let ρ be any bipartite density matrix and $|a_m\rangle$, $|b_m\rangle$ $(m = 1, \ldots, d)$ be two orthonormal bases of the underlying Hilbert space. Let $p_m(\rho) = \langle a_m|\rho|a_m\rangle$ and $q_n(\rho) = \langle b_n|\rho|b_n\rangle$ be the measurements of ρ given by the basis elements, then they form two probability distribution vectors $\mathbf{p}(\rho)$ and $\mathbf{q}(\rho)$ respectively. It can be shown that the realignment vector of the Kronecker tensor product of the two probability vectors $\mathbf{p}(\rho)$ and $\mathbf{q}(\rho)$ is majored by a vector ω independent of ρ:

$$\mathbf{p}(\rho) \otimes \mathbf{q}(\rho) \prec \omega, \quad \forall\ \rho, \tag{4.6}$$

where $\omega \in \mathbb{R}^{d^2}$ is given by

$$\omega = (\Omega_1, \Omega_2 - \Omega_1, \ldots, \Omega_d - \Omega_{d-1}, 0, \ldots, 0), \tag{4.7}$$

and

$$\Omega_k = \max_{I_k} \max_{\rho} \sum_{(m,n)\in I_k} p_m(\rho)\, q_n(\rho). \tag{4.8}$$

Here I_k are k-element subsets of $[d] \times [d]$ and $[d] = \{1, 2, \ldots, d\}$. The outer maximum is over all subsets I_k and the inner maximum runs over all density matrices.

Mixed states of three-qubit systems can be classified by the following: (1) the convex hull S of separable states; (2) the convex hull B of biseparable states (AB-C, AC-B and BC-A); (3) the convex hull of all states, including S, B and genuinely entangled states (W-states and GHZ-states). All these sets are compact and convex, satisfy $S \subset B \subset W \subset GHZ$ (see FIG. 4.1). Examples of GHZ witness and W witness had been given in [ABLS01].

4.2 Entanglement Detection

As shown in [Par11], the universal uncertainty relation can reach its bound on pure states. One can use this to establish an entanglement detector to check whether a density matrix is separable by proving a condition satisfied by all separable states. The method of using universal uncertainty relations, however, has a limit to detect genuine entanglement. In this section, we utilize the Lagrange multiplier to show that the universal uncertainty bound of $\rho = \sum p_i \rho^i_{AB} \otimes \rho^i_C$ can also be reached by

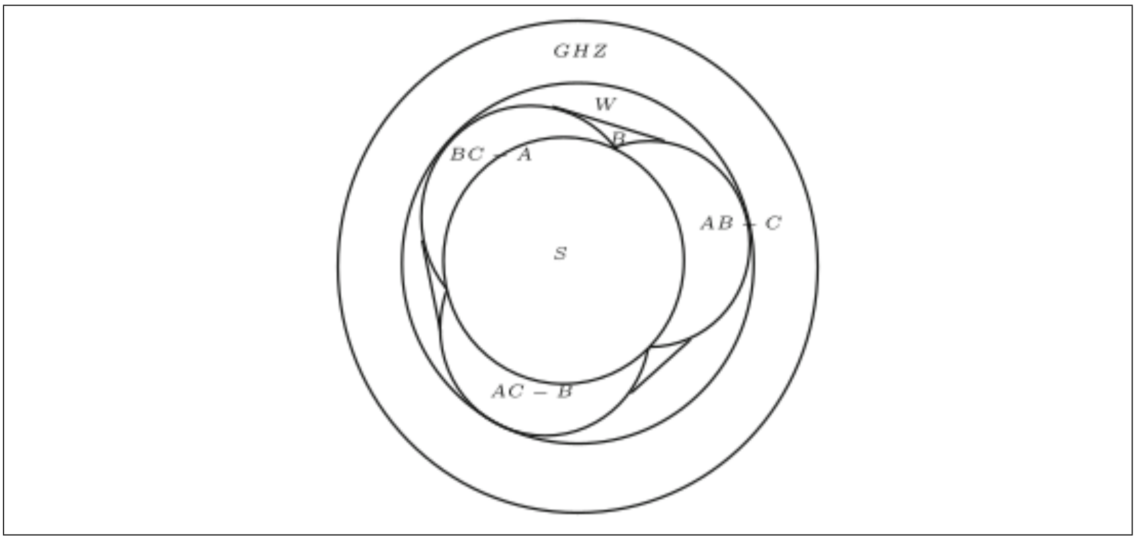

Figure 4.1: Schematic picture of mixed states for three qubits. S: Fully separable class; B: Biseparable class (convex hull of biseparable states under three different partitions); W and GHZ: genuine tripartite entangled.

the pure state of the form $\rho_{AB} \otimes \rho_C$, which provides a AB-C biseparable detector. This establishes a biseparable detector of all tripartite states in AB-C, AC-B or BC-A, and more generally, it can be generalized to give a k-separable detector for all n-partite states.

Universal Uncertainty Bounds on Pure States

For simplicity we limit ourselves to three measurements $(X, \{E_\alpha^X\})$, $(Y, \{E_\beta^Y\})$, and $(Z, \{E_\gamma^Z\})$ that have no common eigenstate. The measurements are performed on a given state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. Let $\mathcal{P}^X(\rho) = (tr(\rho E_\alpha^X)), \mathcal{P}^Y(\rho) = (tr(\rho E_\beta^Y)), \mathcal{P}^Z(\rho) = (tr(\rho E_\gamma^Z))$ and $\mathcal{P}^{X\oplus Y\oplus Z}(\rho) = \mathcal{P}^X(\rho) \otimes \mathcal{P}^Y(\rho) \otimes \mathcal{P}^Z(\rho)$.

We recall the uncertainty bound given in [Par12]. The tensor product of the probability distribution vectors satisfies that

$$\mathcal{P}^X(\rho) \otimes \mathcal{P}^Y(\rho) \otimes \mathcal{P}^Z(\rho) \prec \omega, \tag{4.9}$$

where the bound is reached on pure states ρ_0:

$$\omega = \sup_{\rho_0}[\mathcal{P}^{X\oplus Y\oplus Z}\rho_0)] \prec\prec (1, 0, \cdots, 0). \tag{4.10}$$

If $\rho = \sum p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i$, then

$$\mathcal{P}^X(\rho) \otimes \mathcal{P}^Y(\rho) \otimes \mathcal{P}^Z(\rho) \prec \omega_{A,B,C} = \sup_{\rho_A\otimes\rho_B\otimes\rho_C}[\mathcal{P}^{X\oplus Y\oplus Z}(\rho_A \otimes \rho_B \otimes \rho_C)], \tag{4.11}$$

where $\rho_A \otimes \rho_B \otimes \rho_C$ are fully separable pure state. Now we want to prove that if the density matrix of a tripartite states has the form of $\rho = \sum p_i \rho^i_{AB} \otimes \rho^i_C$, then

$$\mathcal{P}^X(\rho) \otimes \mathcal{P}^Y(\rho) \otimes \mathcal{P}^Z(\rho) \prec \omega_{AB,C} = \sup_{\rho_{AB}\otimes\rho_C} [\mathcal{P}^{X\oplus Y\oplus Z}(\rho_{AB} \otimes \rho_C)], \tag{4.12}$$

where $\rho_{AB} \otimes \rho_C$ is biseparable pure state of type AB-C. To prove this, it is sufficient to show that the maximum value of the sum of i different components of $\mathcal{P}^{X\oplus Y\oplus Z}(\sum p_i \rho^i_{AB} \otimes \rho^i_C)$ is realized on pure states of same type.

Suppose $\rho = \sum\limits_a q_a |\phi^{AB}_a\rangle\langle\phi^{AB}_a| \otimes |\phi^C_a\rangle\langle\phi^C_a|$. To maximize $\mathcal{P}^{X\oplus Y\oplus Z}(\rho)$ we apply the method of the Lagrange multipliers:

$$\begin{aligned}\sum_{a,b,c} q_a q_b q_c [&\langle\phi^{AB}_a|\langle\phi^C_a|E^X_{\alpha_1}|\phi^C_a\rangle|\phi^{AB}_a\rangle\langle\phi^{AB}_b|\langle\phi^C_b|E^Y_{\beta_1}|\phi^C_b\rangle|\phi^{AB}_b\rangle\langle\phi^{AB}_c|\langle\phi^C_c|E^Z_{\gamma_1}|\phi^C_c\rangle|\phi^{AB}_c\rangle + \\ &\langle\phi^{AB}_a|\langle\phi^C_a|E^X_{\alpha_2}|\phi^C_a\rangle|\phi^{AB}_a\rangle\langle\phi^{AB}_b|\langle\phi^C_b|E^Y_{\beta_2}|\phi^C_b\rangle|\phi^{AB}_b\rangle\langle\phi^{AB}_c|\langle\phi^C_c|E^Z_{\gamma_2}|\phi^C_c\rangle|\phi^{AB}_c\rangle + \cdots + \\ &\langle\phi^{AB}_a|\langle\phi^C_a|E^X_{\alpha_i}|\phi^C_a\rangle|\phi^{AB}_a\rangle\langle\phi^{AB}_b|\langle\phi^C_b|E^Y_{\beta_i}|\phi^C_b\rangle|\phi^{AB}_b\rangle\langle\phi^{AB}_c|\langle\phi^C_c|E^Z_{\gamma_i}|\phi^C_c\rangle|\phi^{AB}_c\rangle] + \\ &\sum_a \eta^{AB}_{i,a}(1 - \langle\phi^{AB}_a|\phi^{AB}_a\rangle) + \sum_a \eta^C_{i,a}(1 - \langle\phi^C_a|\phi^C_a\rangle) + \xi_i(1 - \sum_a q_a).\end{aligned} \tag{4.13}$$

where $\eta^{AB}_{i,a}, \eta^C_{i,a}, \xi_i$ are the Lagrange multipliers.

Denote that

$$\begin{aligned}\varepsilon^X_i &= \sum_{k=1}^{i} \mathcal{P}^Y_{\beta_k}(\rho)\mathcal{P}^Z_{\gamma_k}(\rho)E^X_{\alpha_k}, \\ \varepsilon^Y_i &= \sum_{k=1}^{i} \mathcal{P}^X_{\alpha_k}(\rho)\mathcal{P}^Z_{\gamma_k}(\rho)E^Y_{\beta_k}, \\ \varepsilon^Z_i &= \sum_{k=1}^{i} \mathcal{P}^X_{\alpha_k}(\rho)\mathcal{P}^Y_{\beta_k}(\rho)E^Z_{\gamma_k}, \\ \varepsilon_i &= \varepsilon^X_i + \varepsilon^Y_i + \varepsilon^Z_i.\end{aligned} \tag{4.14}$$

Variations with respect to $\langle\phi^{AB}_s|$ give

$$q_s[\langle\phi^c_s|\varepsilon_i|\phi^C_s\rangle]|\phi^{AB}_s\rangle = \eta^{AB}_{i,s}|\phi^{AB}_s\rangle. \tag{4.15}$$

Similarly with respect to $\langle\phi^C_s|$ we have that

$$q_s[\langle\phi^{AB}_s|\varepsilon_i|\phi^{AB}_s\rangle]|\phi^C_s\rangle = \eta^C_{i,s}|\phi^C_s\rangle, \tag{4.16}$$

which implies $\eta^{AB}_{i,s} = \eta^C_{i,s}$. Denote $\Omega_{AB,C;i}$ as the sum of i different components, and $\langle\phi^{AB}_s|\langle\phi^C_s|\varepsilon_i|\phi^C_s\rangle|\phi^{AB}_s\rangle = \varepsilon_{i,ss}$, then $\Omega_{AB,C;i} = \frac{1}{3}\sum\limits_s q_s \varepsilon_{i,ss} = \frac{1}{3}tr(\varepsilon_i \rho)$. Finally, variation with respect to q_s leads to $\langle\phi_s^{AB}|\langle\phi_s^C|\varepsilon_i|\phi_s^C\rangle|\phi_s^{AB}\rangle = \xi_i$ which means that $\varepsilon_{i,ss}$ do not depend on s, and $\omega_{AB,C}$ can be reached by pure biseparable states of form $\rho_{AB} \otimes \rho_C$.

It is clear that the above argument works for any multipartite state, and the bound for the tensor product of multipartite state can be reached by pure states with the same type. This implies that majorization uncertainty relations can be used to detect genuine entanglement in multipartite and distinguish different types at the same level of entanglement (for example, triseparable ABC-D vs. quartistate system).

Entanglement Detection in Tripartite States

Let $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be a tripartite state with a measurement $\{X, E_\alpha^X\}$. Then the probability vector $\mathcal{P}^X(\rho)$ is majorized by a bound vector ω independent of ρ. The following results are clear from our discussion.

Lemma 4.2.1. *Let $\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i$ be a mixed tripartite state. The probability density vector $\mathcal{P}^X(\rho)$ associated with the measurement X is majorized by a bound vector $\omega_{A,B,C}$ independent from ρ and reachable by a pure tripartite state:*

$$\mathcal{P}^X(\rho) \prec \omega_{A,B,C}. \tag{4.17}$$

If the probability vector of ρ violates the majorization relation, then ρ is entangled.

Lemma 4.2.2. *If $\rho = \sum_i p_i \rho_{AB}^i \otimes \rho_C^i$, then the probability vector $\mathcal{P}^X(\rho)$ resulting from the measurement X on ρ is majorized by $\omega_{AB,C}$ which is state-independent and reachable by some pure biseparable state of type AB-C:*

$$\mathcal{P}^X(\rho) \prec \omega_{AB,C}. \tag{4.18}$$

If the probability vector of ρ violates the majorization relation, then ρ is entangled but not biseparable of type AB-C.

If the dimensions of $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ are different, then the majorization uncertainty bounds $\omega_{AB,C}$, $\omega_{AC,B}$ and $\omega_{BC,A}$ are all different under a suitable measurement $\{X, E_\alpha^X\}$. These probability vectors and that of the whole space form a lattice (see FIG. 4.2), which leads to a majorization uncertainty bound to control any two of $\omega_{AB,C}$, $\omega_{AC,B}$ and $\omega_{BC,A}$.

Proposition 4.2.3. *If $\omega_{AB,C} \neq \omega_{AC,B}$ and both $\prec\prec (1, 0, \cdots, 0)$, then there exists*

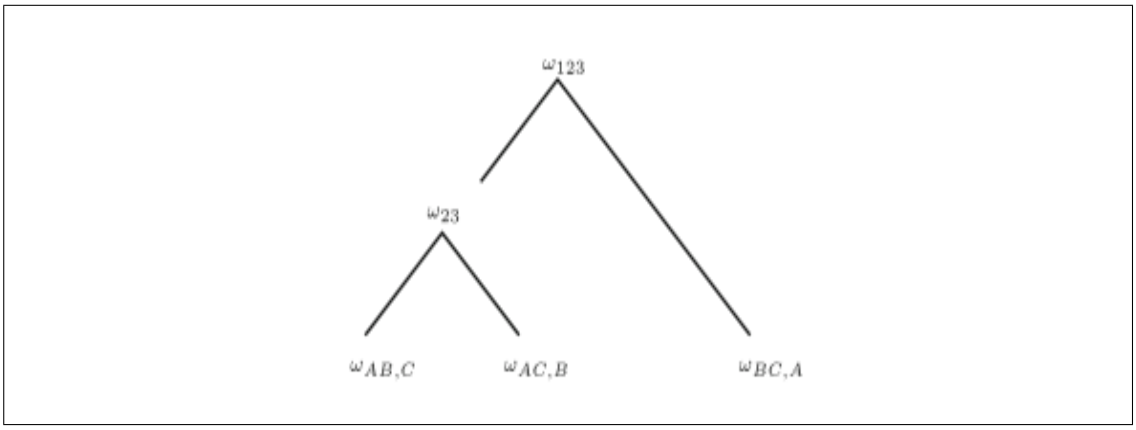

Figure 4.2: Preordering of $\omega_{AB,C}$, $\omega_{AC,B}$ and $\omega_{BC,A}$.

a unique probability vector ω_{23} such that

$$\begin{aligned} \omega_{AB,C} &\prec \omega_{23}, \\ \omega_{AC,B} &\prec \omega_{23}, \\ \omega_{23} &\prec\prec (1, 0, \cdots, 0), \end{aligned} \tag{4.19}$$

and majorizied by any other vector with property Eq. (4.19). This vector is also denoted by $\max\{\omega_{AB,C}, \omega_{AC,B}\}$.

With these results in hand, we can give an entanglement criterion to analyze biseparable states.

Theorem 4.2.4. *If the probability vector of tripartite state ρ under measurement $\{X, E_\alpha^X\}$ is not majorized by ω_{23}:*

$$\mathcal{P}^X(\rho) \not\prec \max\{\omega_{AB,C}, \omega_{AC,B}\}, \tag{4.20}$$

then ρ can not be of the form $\rho = \sum_i p_i \rho^i_{AB} \otimes \rho^i_C + \sum_j q_j \rho^i_{AC} \otimes \rho^i_B$.

To study genuine entanglement, we consider both ω_{23} and $\omega_{BC,A}$ and denote the unique probability vector $\max\{\omega_{23}, \omega_{BC,A}\}$ by ω_{123}. The following result gives a criterion for genuine entanglement.

Theorem 4.2.5. *If*

$$\mathcal{P}^X(\rho) \not\prec \omega_{123}, \tag{4.21}$$

then ρ can not be biseparable, and ρ is genuinely entangled.

For any measurement Φ of uncertainty (non-negative Schur-concave function), it follows from $\mathcal{P}^X(\rho) \prec \omega_{123}$ that

$$\Phi(\mathcal{P}^X(\rho)) \geqslant \Phi(\omega_{123}). \tag{4.22}$$

One can use uncertainty measurements to give numerical criteria for genuine entanglement.

Corollary 4.2.6. *If there is an uncertainty measurement Φ such that*

$$\Phi(\mathcal{P}^X(\rho)) < \Phi(\omega_{123}), \tag{4.23}$$

then ρ is not a biseparable state, and ρ is genuinely entangled.

If $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ have the same dimension, then $\omega_{AB,C} = \omega_{AC,B} = \omega_{BC,A} = \omega_{123}$ by the symmetry property of the superior over pure biseparable states. Although one can not use the above result to detect if a tripartite state has the form $\rho = \sum_i p_i \rho^i_{AB} \otimes \rho^i_C + \sum_j q_j \rho^i_{AC} \otimes \rho^i_B$, one still has the following result for genuine entanglement.

Theorem 4.2.7. *For $\dim \mathcal{H}_A = \dim \mathcal{H}_B = \dim \mathcal{H}_C$, if*

$$\mathcal{P}^X(\rho) \not\prec \omega_{AB,C}, \tag{4.24}$$

then ρ is not a biseparable state, and ρ is genuinely entangled.

Combining with non-negative Schur-concave functions, one immediately gets the following criterion of genuine entanglement.

Corollary 4.2.8. *If there is a non-negative Schur-concave function Φ such that*

$$\Phi(\mathcal{P}^X(\rho)) < \Phi(\omega_{AB,C}), \tag{4.25}$$

then ρ is not biseparable state, and the state ρ is genuinely entangled.

Entanglement Detection in Multipartite States

The majorization method can be generalized to characterize entanglement for multipartite quantum states. In this subsection, we present a general and systematic scheme to study k-separable and n-partite genuinely entangled states.

Following [HMGH10], we say a pure n-partite quantum state $|\Psi\rangle$ is k-separable if it can be written as

$$|\Psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_k\rangle, \tag{4.26}$$

where $|\phi_i\rangle$ is a single subsystem or a group of subsystems. If such as decomposition is not possible, $|\Psi\rangle$ is called genuinely n-partite entangled. For a mixed state ρ: a state is genuinely k-partite entangled if any decomposition into pure states

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{4.27}$$

with probabilities $p_i > 0$ contains at least one genuinely k-partite entangled component. It is called k-separable if any decomposition into pure states $|\psi_i\rangle$ is at least k-separable. All $(k+1)$-separable states form a compact and convex subset of the set of k-separable states. This hierarchical structure is usually referred to as a *uniform entanglement frame*. Our main idea is to construct criteria to detect k-separability by majorization uncertainty relations and find the principle behind these criteria.

Statistical mixture of biseparable states for tripartite states has been considered, we now focus on k-separable states for multipartite states. For any k-separable state $\rho_{kse} = \sum_i p_i \rho_{kse}^i$, if all ρ_{kse}^i have the same form (for example, systems 1 to $n-k+1$ are entangled and the rest are separable), then by the majorization method there exists a bound vector $\omega_{k,l}$ reachable by pure states with the same form as ρ_{kse}^i for each i. Moreover,

$$\mathcal{P}^X(\rho_{kse}) \prec \omega_{k,l}, \tag{4.28}$$

where there are $\mathbb{C}_n^k$ possibilities for l. If $\dim \mathcal{H}_1 = \dim \mathcal{H}_2 = \cdots = \dim \mathcal{H}_n$, then

$$\omega_{k,1} = \omega_{k,2} = \cdots = \omega_{k,\mathbf{C}_n^k} := \omega_k.$$

Under this assumption we have

Theorem 4.2.9. *For any k-separable state ρ_{kse} and measurement $\{X, E_{\alpha_i}^X\}$, the following majorization uncertainty relation holds:*

$$\mathcal{P}^X(\rho_{kse}) \prec \omega_k, \tag{4.29}$$

where ω_k can be reached by pure k-separable state.

Corollary 4.2.10. *For any n-partite state ρ, if there exists a measurement $\{X, E_{\alpha_i}^X\}$ such that the probability vector is not majorized by ω_k:*

$$\mathcal{P}^X(\rho) \not\prec \omega_k, \tag{4.30}$$

then ρ is at most $(k-1)$-separable.

One can generalize Corollary 4.2.10 to derive a criterion for genuinely n-partite entangled states.

Corollary 4.2.11. *For any n-partite state ρ, if there exists a probability vector under measurement $\{X, E^X_{\alpha_i}\}$ such that*

$$\mathcal{P}^X(\rho) \not\prec \omega_2, \tag{4.31}$$

then ρ is genuinely n-partite entangled.

Under non-negative Schur-concave functions Φ, the majorization uncertainty bound ω_2 becomes a real number $\Phi(\omega_2)$, then Eq. (4.31) generates in fact infinite family of genuinely n-partite entangled criteria.

Corollary 4.2.12. *For any n-partite state ρ and non-negative Schur-concave functions Φ, if the following equality holds under measurement $\{X, E^X_{\alpha_i}\}$:*

$$\Phi(\mathcal{P}^X(\rho)) < \Phi(\omega_2), \tag{4.32}$$

then ρ is genuinely n-partite entangled.

Entangled states are characterized well under the majorization uncertainty relations as the universal uncertainty bounds are independent from the state ρ. This is particularly so when one applies the uncertainty relations given in Eq. (4.2). We discuss some examples to show how these are applied.

Consider the Werner state $\rho^{wer}_d(q)$ [Par12] defined on the tensor product of two d-dimensional Hilbert spaces:

$$\rho^{wer}_d(q) = \frac{1}{d^2}(1-q)I + q|\mathfrak{B}_1\rangle\langle\mathfrak{B}_1|, \tag{4.33}$$

where I is the identity matrix in $\mathbb{C}^{d\times d}$ and

$$|\mathfrak{B}_1\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j_A\rangle\otimes|j_B\rangle, \tag{4.34}$$

is the first of the generalized Bell states $\{|\mathfrak{B}_\alpha\rangle\}_{\alpha=1}^{d^2}$, which form a basis of orthonormal eigenstates for $\rho^{wer}_d(q)$. Let the measurement $\{X, E^X_\alpha\}$ be $E^X_\alpha = |\mathfrak{B}_\alpha\rangle\langle\mathfrak{B}_\alpha|$, $\alpha = 1, 2, \cdots, d^2$. The probability vector is then

$$\mathcal{P}^X(\rho^{wer}_d(q)) = (q + d^{-2}(1-q), d^{-2}(1-q), d^{-2}(1-q), \cdots, d^{-2}(1-q)). \tag{4.35}$$

As shown in [BEK+04], the maximum overlap of every generalized Bell states with the set of pure, product states is given by $1/\sqrt{d}$, we get that

$$\omega_{A,B} = (1/d, 1/d, \cdots, 1/d, 0, 0, \cdots, 0). \tag{4.36}$$

Using our Theorem 4.2.4, the Werner state is separable if $\mathcal{P}^X(\rho_d^{wer}(q))$ is majorized by $\omega_{A,B}$, i.e., $q \leqslant (1+d)^{-1}$. This inequality agrees with the well-known separability condition for the Werner state.

Clearly, the efficiency of uncertainty bounds in judging entanglement depends on the choice of the measurement $\{X, E_\alpha^X\}$. The calculation of ω will be easy if the measurement is optimal in some sense.

Next we will take the quantum state to be $\rho_d^{wer}(q) \otimes \frac{1}{d}I$ and the measurement to be $\{X, E_{\alpha,j}^X\}$, where $E_{\alpha,j}^X = |\mathfrak{B}_\alpha\rangle \otimes |j\rangle$, $\alpha = 1, 2, \cdots, d^2$; $j = 0, 1, \cdots, d-1$. It is easy to see that

$$
\begin{aligned}
&\mathcal{P}^X(\rho_d^{wer}(q) \otimes \frac{1}{d}I) \\
=&(\underbrace{q + d^{-2}(1-q), \cdots, q + d^{-2}(1-q)}_{d-times}, d^{-2}(1-q), d^{-2}(1-q), \cdots, d^{-2}(1-q)).
\end{aligned}
$$

The maximum overlap of every measurement element $E_{\alpha,j}^X = |\mathfrak{B}_\alpha\rangle \otimes |j\rangle$ with the set of pure, biseparable state is given by 1. Thus we conclude that

$$
\omega_{AB,C} = (1, 0, \cdots, 0). \tag{4.37}
$$

It is easy to see that $\mathcal{P}^X(\rho_d^{wer}(q) \otimes \frac{1}{d}I) \prec \omega_{AB,C}$ is always ture, and no violation happens, which means that $\rho_d^{wer}(q) \otimes \frac{1}{d}I$ is always biseparable of form AB-C. This coincides with the fact that for any value q, $\rho_d^{wer}(q) \otimes \frac{1}{d}I$ is always biseparable and can only be entangled in the AB system.

4.3 Matrix Forms of Majorization

Majorization was first studied by Schur [Sch23] in relation with Hadamard inequalities and it was proved that two probability vectors $x \prec y$ if and only if $y = Q(x)$ for a bistochastic matrix Q. A matrix $Q = (q_{ij}) \in \mathbb{R}_+^{n\times n}$ is bistochastic if

$$
\sum_i q_{ij} = \sum_j q_{ij} = 1.
$$

Birkkhoff proved that the set of all bistochastic matrices is the convex hull of permutation matrices [And89]. The geometric and combinatoric principle behind majorization and bistochastic matrix is that the relation fully characterizes the convexity of the set of all k-separable states. It is a convex and compact subset of $(k-1)$-separable states, which enables one to construct criteria to detect k-separable states. The majorization method to detect states is relied on the "interior" of the convex set of k-separable states based on Brikhoff's theorem.

We list the equivalent forms of majorization as follows.

- $x \prec y$;
- $y = Q(x)$ for some bistochastic matrix Q;
- $\Phi(x) \geqslant \Phi(y)$ for any non-negative Schur-concave functions Φ;
- x can be derived from y by successive applications of finitely many T-transformations:
$$T = \lambda I + (1-\lambda)P, \tag{4.38}$$
where $0 \leqslant \lambda \leqslant 1$ and P is a permutation matrix that interchanges two coordinates;
- x is in the convex hull of the $n!$ permutations of y.

We now give the matrix form of the k-separable criterion.

Theorem 4.3.1. *Let ρ be an n-partite quantum state on $\mathcal{H}^{\otimes n}$ ($\dim(\mathcal{H}) = d$), and let $\{X, E_\alpha^X\}$ be a measurement with the probability vector $\mathcal{P}^X(\rho) = (p_1, p_2, \cdots, p_m)$, where $m = d^n$. Suppose the k-separable uncertainty bound is $\omega_k = (\Omega_1, \Omega_2 - \Omega_1, \ldots, \Omega_m - \Omega_{m-1})$. If there does not exist a bistochastic matrix $Q = (q_{ij})$ such that*

$$\Omega_j - \Omega_{j-1} = \sum_{i=1}^{m} q_{ij} p_i, \quad j = 1, 2, \cdots, m.$$

then ρ is at most $(k-1)$-separable.

This result follows from the fact that violation of $\mathcal{P}^X(\rho) \prec \omega_k$ is equivalent to there does not exist a bistochastic matrix Q such that $\omega_k = Q(\mathcal{P}^X(\rho))$.

We now consider an information quantity called f-relative entropy to express the closeness between two probability vectors and helps describe k-separability. The f-relative entropy is also called f-divergence in information theory.

Lemma 4.3.2. *Let f be a convex function. Then the information quantity $D_f(x \parallel y) = \sum_i x_i f(\frac{y_i}{x_i})$ for probability vectors $x = (x_i)$ and $y = (y_i)$ is monotonic:*

$$D_f(x \parallel y) \geqslant D_f(Q(x) \parallel Q(y)), \tag{4.39}$$

where Q is stochastic matrix.

It follows from Lemma 4.3.2 that $D_f(x \parallel y)$ is an f-relative entropy. This monotonicity condition (4.39) also holds if Q is replaced by a bistochastic matrix.

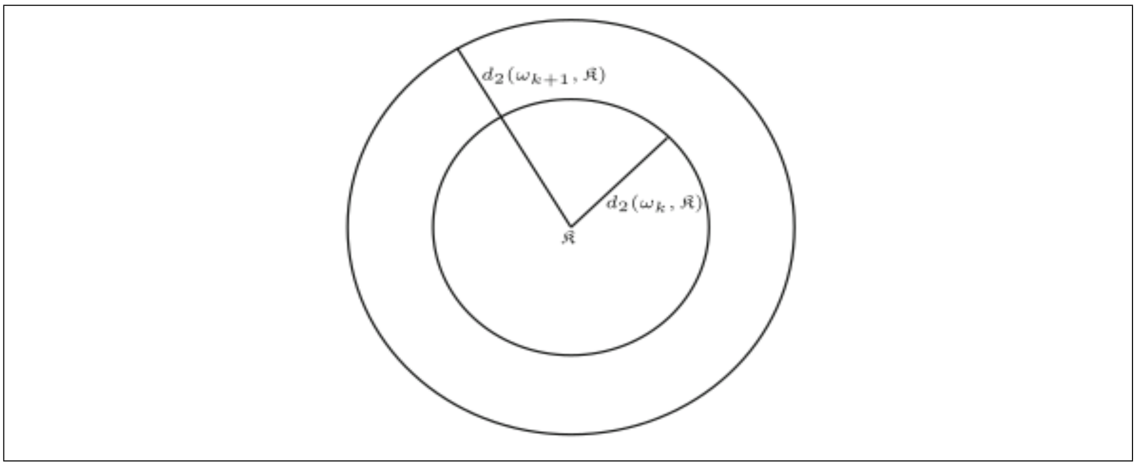

Figure 4.3: k-separable radius corresponds to ' k-circle '.

Note that $Q(1/m, 1/m, \cdots, 1/m) = (1/m, 1/m, \cdots, 1/m)$ for any bistochastic matrix. Plugging $y = \mathfrak{K} = (1/m, 1/m, \cdots, 1/m)$ and $x = \mathcal{P}^X(\rho)$ associated with a measurement $\{X, E_\alpha^X\}$ in Eq. (4.39), one immediately gets that

$$D_f(\mathcal{P}^X(\rho) \parallel \mathfrak{K}) \geqslant D_f(\omega_k \parallel \mathfrak{K}), \tag{4.40}$$

This gives the following criterion of relevant entanglement.

Theorem 4.3.3. *If there exists a convex function and a measurement $\{X, E_\alpha^X\}$ such that*

$$D_f(\mathcal{P}^X(\rho) \parallel \mathfrak{K}) < D_f(\omega_k \parallel \mathfrak{K}), \tag{4.41}$$

then the state ρ is at most $(k-1)$-separable.

The f-relative entropy $D_f(\mathcal{P}^X(\rho) \parallel \mathfrak{K})$ expresses the closeness between $\mathcal{P}^X(\rho)$ and a fixed point $\mathfrak{K}$, but it does not satisfy the axioms of a distance. To get a "distance" to characterize k-separability one needs special convex functions such as $f(x) = 1 - \sqrt{x}$, its square root is called Hellinger distance and denoted by $d_2(x, y)$. It is known that $d_2(x, y)$ satisfies the axioms of a distance. With $\mathfrak{K}$ as the center of the circle, $d_2(\omega_k, \mathfrak{K})$ can be viewed as the radius of a k-separable circle, or simply the k-circle (see FIG. 4.3).

Corollary 4.3.4. *If ρ is at most $(k-1)$-separable, then*

$$d_2(\mathcal{P}^X(\rho), \mathfrak{K}) < d_2(\omega_k, \mathfrak{K}). \tag{4.42}$$

The vector $\mathcal{P}^X(\rho) \in \mathbb{R}^m$ is a point inside the k-separable circle.

Consider again the Werner state $\rho_d^{wer}(q)$. Both the probability $\mathcal{P}^X(\rho_d^{wer}(q))$ under measurement $E_\alpha^X = |\mathfrak{B}_\alpha\rangle\langle\mathfrak{B}_\alpha|$ and the uncertainty bound $\omega_{A,B}$ are given as follows.

$$\mathcal{P}^X(\rho_d^{wer}(q)) = (q + d^{-2}(1-q), d^{-2}(1-q), d^{-2}(1-q), \cdots, d^{-2}(1-q)), \quad (4.43)$$

while

$$\omega_{A,B} = (1/d, 1/d, \cdots, 1/d, 0, 0, \cdots, 0), \quad (4.44)$$

It is easy to calculate that $d_2^2(\omega_{A,B}, \mathfrak{K}) = 1 - \sqrt{\frac{1}{d}}$. Then $d_2(\mathcal{P}^X(\rho_d^{wer}(q)), \mathfrak{K}) < d_2(\omega_{A,B}, \mathfrak{K})$ implies $q > (1+d)^{-1}$, which coincides with the necessary and sufficient condition for inseparability of the Werner state.

Hellinger distance is useful to detect entanglement based on the monotonicity condition. However, only the monotonicity property is not good enough for entanglement detection, which is shown by the following example.

Consider the variational distance given by

$$d_1(x, y) = \frac{1}{2}\sum_i |x_i - y_i|. \quad (4.45)$$

It is not an f-relative entropy, but it satisfies the monotonicity property

$$d_1(x, y) \geqslant d_1(Q(x), Q(y)). \quad (4.46)$$

If we take y as $\mathfrak{K} = (1/m, \cdots, 1/m)$ then $d_1(x, y) = d_1(Q(x), Q(y))$. Thus d_1 fails to detect entanglement.

Finally we would like to discuss how entanglement witness is used to detect entanglement. A *witness for genuine k-partite entanglement* is an observable that has a positive expectation value on states with $(k-1)$-partite entanglement and a negative expectation value on some k-partite entangled states. Entanglement witness is a useful tool for analyzing entanglement in experiments [BEK+04]. Usual entanglement witness does have its limit in dealing with the type of k-partite separable state. We now give a universal entanglement witness which can detect the type. We take tripartite states to illustrate the idea. Suppose $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ and $\dim \mathcal{H}_A \neq \dim \mathcal{H}_B \neq \dim \mathcal{H}_C$. By choosing a suitable measurement $\{X, E_\alpha^X\}$, the bounds $\omega_{AB,C}$, $\omega_{AC,B}$ and $\omega_{BC,A}$ are all different. Write $\omega_{AB,C}$ as $(\Omega_1, \Omega_2 - \Omega_1, \ldots, \Omega_m - \Omega_{m-1})$, $m = \dim \mathcal{H}_A \cdot \dim \mathcal{H}_B \cdot \dim \mathcal{H}_C$.

A universal witness operator can be written in the canonical form

$$\mathcal{W}_k = \Omega_k I - \sum_{i=1}^{k} E_{\alpha_i}^X, k = 1, 2, \cdots, m, \quad (4.47)$$

where I is the identity operator and $E^X_{\alpha_i}$ are from the measurement $\{X, E^X_\alpha\}$. Then for any biseparable state $\rho = \sum_i p_i \rho^i_{AB} \otimes \rho^i_C$ in type AB-C, we have

$$Tr(\mathcal{W}_k \rho) \geqslant 0, k = 1, 2, \cdots, m. \tag{4.48}$$

If there is

$$Tr(\mathcal{W}_k \rho) < 0, \tag{4.49}$$

for some k, then ρ can not be of type AB-C. We remark that the universal entanglement witness can be used to analyze the complement of the compact convex subset inside another one.

In this chapter, we have developed entanglement criteria based on both majorization and universal uncertainty relations. These criteria have advantage over the scalar detecting algorithms as they are often stronger and tighter due to specific formulas for the bound ω of the uncertainty relation. They are tight enough to detect k-separable n-partite states and their types by choosing a suitable measurement $\{X, E^X_\alpha\}$ when the underlying particles have different dimensions.

We have also presented the matrix form of majorization. One feature in this approach is by choosing a suitable monotonic function one can define a distance in the set of entangled states, where k-separable states form concentric circles. In this regard, viable functions are non-negative Schur-concave functions such as Shannon, Rényi and Tsallis entropies. We have also generalized the entanglement witness to detect the type of a k-separable state, and indicate how they can be implemented in experiments.

Chapter 5

Entropic Uncertainty Relations

The goal of this thesis is to construct the framework for uncertainty principle, which can be formulated by variance-based uncertainty relations and entropic uncertainty relations. In this chapter we will focus on entropic uncertainty relations, both two observables and multi-observables have been considered. Furthermore, we also investigate the relation between entropic uncertainty relations in absence of quantum memory and in presence of quantum memory. I hope this work can provide a reference for researchers who are interested in uncertainty relations.

5.1 Strong Entropic Uncertainty Relation for Multi-Measurements

In this section, we study entropic uncertainty relations on a finite-dimensional Hilbert space and provide several tighter bounds for multi-measurements, with some of them also valid for Rényi and Tsallis entropies besides the Shannon entropy. We employ majorization theory and actions of the symmetric group to obtain an *admixture bound* of entropic uncertainty relations for multi-measurements. Comparisons among bounds for multi-measurements are given in two figures.

The most revolutionary departure of quantum mechanics from classical mechanics is that it is impossible to simultaneously measure two complementary variables of a particle in precision. Kennard's form of the Heisenberg uncertainty principle [Hei27] displays vividly such an inequality for the standard deviation of position and momentum of a particle: $\sigma_Q\sigma_P \geqslant \frac{1}{2}$, where the Planck constant is taken as $\hbar = 1$. The corresponding entropic uncertainty of Białynicki-Birula and Mycielski [BBM75] says that $h(Q) + h(P) \geqslant \log(e\pi)$, where Q and P stand for position and momentum respectively while h is the differential entropy: $h(Q) = -\int_{-\infty}^{\infty} f(x)\log f(x)dx$ with $f(x)$ being the probability density corresponding to Q.

In the seminal paper [Deu83], Deutsch studied the entropic uncertainty relations on finite d-dimensional Hilbert spaces in terms of the Shannon entropy for any two measurements M_1 and M_2 (base 2 log is used unless stated otherwise):

$$H(M_1) + H(M_2) \geqslant -2\log\frac{1+\sqrt{c_1}}{2}, \tag{5.1}$$

where c_1 is the largest element in the overlap matrix $c(M_1, M_2)$ of the two measurements. Later Maassen and Uffink [MU88, BCC$^+$10] derived the influential generalized quantum mechanical uncertainty relation which amounts to a tighter lower bound than Eq. (5.1). Recently Coles and Piani [CP14] proved that, for any two measurements $M_j = \{|u^j_{i_j}\rangle\}$ on a quantum state ρ over a finite dimensional Hilbert space

$$H(M_1) + H(M_2) \geqslant -\log c_1 + \frac{1-\sqrt{c_1}}{2}\log\frac{c_1}{c_2}, \tag{5.2}$$

where c_2 is the second largest value among all overlaps $c(u^1_{i_1}, u^2_{i_2}) = |\langle u^1_{i_1}|u^2_{i_2}\rangle|^2$. Then Maassen-Uffink's bound is simply obtained by dropping the second term in RHS of Eq. (5.2).

More recently, S. Liu *et al.* [LMF15] generalized Coles and Piani's method to give a lower bound for N measurements M_i:

$$\sum_{m=1}^{N} H(M_m) \geqslant -\log b + (N-1)S(\rho), \tag{5.3}$$

where

$$b = \max_{i_N}\left\{\sum_{i_2\sim i_{N-1}} \max_{i_1}[c(u^1_{i_1}, u^2_{i_2})]\prod_{m=2}^{N-1} c(u^m_{i_m}, u^{m+1}_{i_{m+1}})\right\}. \tag{5.4}$$

and $S(\rho)$ is the *von Neumann entropy* of the quantum state ρ. Thus the state-independent uncertainty relation for multi-measurements is the corresponding inequality by ignoring $S(\rho)$. In fact, the state-independent inequality generalizes Maassen-Uffink's bound, which suggests that there are rooms for improvement in regards to Coles-Piani's bound. Such an improvement will be useful for further applications in quantum information processing, especially in quantum cryptography when several measurements are present. For the importance of entropic uncertainty relations and other applications, the reader is referred to [Tom15, CBTW15].

The aim of this section is to find several tighter bounds for multi-measurements in comparison with the bound of Eq.(5.3) by using majorization theory and symmetry. Of course it is a combinatorial or mathematical exercise to obtain bounds for multi-measurements based on the usual entropic sum of two measurements. However, what we will show is that deeper analysis is needed for nontrivial and tighter bounds for multi-measurements, and applications of majorization theory and symmetry inside the physical construction help to obtain true generalization for multi-measurements.

Indeed, from the construction of the universal uncertainty relation [FGG13, RPŻ14], the joint probability distribution in vector $P^1 \otimes P^2$, with respect to the measurement M_1 and M_2, should be controlled by a bound ω that quantifies its uncertainty in terms of majorization and is also independent of the state ρ (see chapter 4). Thus, $H(P^1) + H(P^2) \geqslant H(\omega)$ for any nonnegative Schur concave function H such as the Shannon entropy. Therefore, the generalized universal uncertainty relation for N measurements

$$\bigotimes_{m=1}^{N} P^m \prec \omega$$

can imply that $\sum_{m=1}^{N} H(P^m) \geqslant H(\omega)$ for multi-measurements. In Sec. 5.1.1, we first give a precise formula of majorization bound for N probability distributions, and discuss two simple forms of the majorization bounds for multi-measurements in connection with Eq. (5.3). Comparison of our bounds with previously ones in FIG. 5.1 shows that our bounds are tighter.

Further study shows that the simple sum of the uncertainties does not completely reveal the physical meaning of the entropic bounds. The reason is that when one computes the sum of the entropies such as Eq. (5.3), the mathematical summation does not really provide physically correct answer, as the measurement outcomes clearly do not know which order we perform the measurements, and the bound for N-measurement should be independent from the order of measuring. Therefore one should consider the average of all possible orders of measurements. But this average is cumbersome and does not provide good enough result.

In order to solve this and get operational formulas for the entropic uncertainty relation of multi-measurements, we study the effects of symmetry on majorization bounds in Sec. 5.1.2 and find that there is a large invariant subgroup of the full symmetry group under the action on certain products of probability distribution vectors and logarithms of remaining distributions. After factoring out this invariant factor we obtain a simple average to give our main result in Sec. 5.1.2:

$$\sum_{m=1}^{N} H(M_m) + (1-N)S(\rho) \geqslant -\frac{1}{N}\omega\mathfrak{B}, \tag{5.5}$$

where ω is the universal majorization bound of N-measurements and $\mathfrak{B}$ is certain vector of logarithmic distributions (cf. Theorem 5.1.3). We call this bound an *admixture bound*, since it is obtained by mixing the universal bound from tensor products and factoring out the action of the invariant subgroup of the symmetric group. We then show that this admixture bound is tighter than all previously known bounds in the last part of this section. The exact comparison is charted in FIG. 5.2.

Universal Bounds of Majorization

Majorization characterizes a balanced partial relationship between two vectors that are comparable and was studied long ago in algebra and analysis. It has been used to study entropic uncertainty relations [Par11, Par12] and played an important role in formulation of state-independent entropic uncertainty relations [FGG13, PRŻ13, RPŻ14]. A vector x is majorized by another vector y in $\mathbb{R}^d$: $x \prec y$ if $\sum_{i=1}^{k} x_i^{\downarrow} \leqslant \sum_{i=1}^{k} y_i^{\downarrow} (k = 1, 2, \cdots, d-1)$ and $\sum_{i=1}^{d} x_i^{\downarrow} = \sum_{i=1}^{d} y_i^{\downarrow}$, where the down-arrow denotes that the components are ordered in decreasing order $x_1^{\downarrow} \geqslant \cdots \geqslant x_d^{\downarrow}$. A nonnegative Schur concave function Φ on $\mathbb{R}^d$ preserves the partial order in the sense that $x \prec y$ implies that $\Phi(x) \geqslant \Phi(y)$. We adopt the convention to write a probability distribution vector in a short form by omitting the string of zeroes at the end, for example, $(0.6, 0.4, 0, \cdots, 0) = (0.6, 0.4)$ and the actual dimension of the vector should be clear from the context.

The tensor product $x \otimes y$ of two vectors $x = (x_1, \cdots, x_{d_1})$ and $y = (y_1, \cdots, y_{d_2})$ is defined as $(x_1y_1, \cdots, x_1y_{d_2}, \cdots, x_{d_1}y_1, \cdots, x_{d_1}y_{d_2})$, and multi-tensors are defined by associativity. It is well-known that Shannon, Rényi and Tsallis entropies are nonnegative Schur-concave, thus for probability distributions P^1 and P^2 with $P^1 \otimes P^2 \prec \omega$ implies that $\Phi(P^1 \otimes P^2) \geqslant \Phi(\omega)$ for any of the entropies Φ.

A majorization uncertainty relation for two measurements was well studied in [FGG13, PRŻ13]. We now construct the analogous universal upper bound for multi-measurements. Let ρ be a mixed quantum state on a d-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^d$, and let M_m $(m = 1, 2, \cdots, N)$ be N measurements. Assume that M_m has a set of orthonormal eigenvectors $\{|u_{i_m}^m\rangle\}$ $(i_m = 1, 2, \cdots, d)$, and denote by $P^m = (p_{i_m}^m)$, where $p_{i_m}^m = \langle u_{i_m}^m|\rho|u_{i_m}^m\rangle$ the probability distributions obtained by measuring ρ with respect to bases $\{|u^m_{i_m}\rangle\}$. We can derive a state-independent bound of $\bigotimes_m P^m$ under majorization

$$\bigotimes_{m=1}^{N} P^m \prec \omega, \tag{5.6}$$

where the quantity on the left-hand side represents the joint probability distribution induced by measuring ρ with measurements M_m $(m = 1, 2, \cdots, N)$.

For subsets $\{|u^1_{i_1}\rangle, \cdots, |u^1_{i_{S_1}}\rangle\}$, $\{|u^2_{j_1}\rangle, \cdots, |u^2_{j_{S_2}}\rangle\}$, $\cdots$, $\{|u^N_{l_1}\rangle, \cdots, |u^N_{l_{S_N}}\rangle\}$ of the orthonormal bases of $M^1, M^2, \cdots M^N$ respectively such that $S_1 + S_2 + \cdots + S_N = k + N - 1$, we define the matrices $U_{ij}(S_i, S_j)$

$$\begin{aligned} U_{12}(S_1, S_2) &= \begin{pmatrix} \langle u^1_{i_1}| \\ \langle u^1_{i_2}| \\ \vdots \\ \langle u^1_{i_{S_1}}| \end{pmatrix} \cdot \Big(|u^2_{j_1}\rangle, |u^2_{j_2}\rangle, \cdots, |u^2_{j_{S_2}}\rangle \Big) \\ &= \begin{pmatrix} \langle u^1_{i_1}|u^2_{j_1}\rangle & \langle u^1_{i_1}|u^2_{j_2}\rangle & \cdots & \langle u^1_{i_1}|u^2_{j_{S_2}}\rangle \\ \langle u^1_{i_2}|u^2_{j_1}\rangle & \langle u^1_{i_2}|u^2_{j_2}\rangle & \cdots & \langle u^1_{i_2}|u^2_{j_{S_2}}\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle u^1_{i_{S_1}}|u^2_{j_1}\rangle & \langle u^1_{i_{S_1}}|u^2_{j_2}\rangle & \cdots & \langle u^1_{i_{S_1}}|u^2_{j_{S_2}}\rangle \end{pmatrix}. \end{aligned} \tag{5.7}$$

For simplicity we abbreviate $U_{12}(S_1, S_2)$ by U_{12}. Then U_{13}, $U_{14}, \cdots U_{N-1,N}$ are constructed similarly. We define the block matrix

$$U(S_1, S_2, \cdots, S_N) = \begin{pmatrix} I_{S_1} & U_{12} & \cdots & U_{1N} \\ U_{21} & I_{S_2} & \cdots & U_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ U_{N1} & U_{N2} & \cdots & I_{S_N} \end{pmatrix}. \tag{5.8}$$

Since the eigenvalues of a Hermitian matrix are real, we adopt the convention to label the eigenvalues in decreasing order. Let $\lambda_1(\bullet)$ and $\sigma_1(\bullet)$ denote the maximal eigenvalue and singular value of a matrix respectively. Generalizing the idea of [PRŻ13, RPŻ14], we introduce the elements s_k by

$$s_k = \max_{\sum_{x=1}^{N} S_x = k+N-1} \{\lambda_1(U(S_1, S_2, \cdots, S_N))\}. \tag{5.9}$$

We remark that when $N = 2$, Eq. (5.9) will degenerate to the s_k defined in [PRŻ13]. Write

$$\Omega_k = (\frac{s_k}{N})^N, \tag{5.10}$$

then we have $\Omega_1 \leqslant \Omega_2 \leqslant \cdots \leqslant \Omega_a < 1$ for some integer $a \leqslant d^N - 1$ with $\Omega_{a+1} = 1$. With this preparation we can state our universal upper bound for multi-measurements:

Theorem 5.1.1. *For any d-dimensional quantum state ρ and N measurements M_m with their probability distributions P^m, we have*

$$\bigotimes_{m=1}^{N} P^m \prec \omega, \tag{5.11}$$

where

$$\omega = (\Omega_1, \Omega_2 - \Omega_1, \cdots, 1 - \Omega_a). \tag{5.12}$$

with a being the smallest index such that $\Omega_{a+1} = 1$. Here we have used the short form of the d^N-dimensional vector ω

Theorem 5.1.1 is a generalization of the majorization bound for a pair of two measurements [FGG13, PRŻ13]. Due to its key role in our discussion, we include a detailed proof.

Proof. Consider sums of k elements from the vector $\bigotimes_{m=1}^{N} P^m$, then they are bounded as follows.

$$(p^1_{i_1} p^2_{j_1} \cdots p^N_{l_1}) + \cdots + (p^1_{i_k} p^2_{j_k} \cdots p^N_{l_k}) \leqslant \max_{S_1 + \cdots + S_N = k+N-1} (\sum_{x=1}^{S_1} \widetilde{p}^1_x)(\sum_{x=1}^{S_2} \widetilde{p}^2_x) \cdots (\sum_{x=1}^{S_N} \widetilde{p}^N_x), \tag{5.13}$$

where $\widetilde{p}^i_1$, $\widetilde{p}^i_2$, $\cdots$, $\widetilde{p}^i_{S_i}$ are the greatest S_i elements of p^i_x.

Since the arithmetic mean is at least as large as the geometric mean, we derive that

$$(\sum_{x=1}^{S_1} \widetilde{p}^1_x)(\sum_{x=1}^{S_2} \widetilde{p}^2_x) \cdots (\sum_{x=1}^{S_N} \widetilde{p}^N_x) \leqslant (\frac{\sum_{x=1}^{S_1} \widetilde{p}^1_x + \cdots + \sum_{x=1}^{S_N} \widetilde{p}^N_x}{N})^N, \tag{5.14}$$

On the other hand,

$$\sum_{x=1}^{S_1} \widetilde{p}^1_x + \cdots + \sum_{x=1}^{S_N} \widetilde{p}^N_x \leqslant \max_{\sum_{x=1}^{N} S_x = k+N-1} \{\lambda_1(U(S_1, S_2, \cdots, S_N))\} = s_k, \tag{5.15}$$

so we finally get the following estimate:

$$\bigotimes_{m=1}^{N} P^m \prec (\Omega_1, \Omega_2 - \Omega_1, \cdots, 1 - \Omega_a), \tag{5.16}$$

where $\Omega_k = (\frac{s_k}{N})^N$ and Ω_{a+1} is the first component equal to 1, and this gives the desired majorization bound for multi-measurements. ■

In the case of higher dimensional quantum state ρ, $\lambda_1(U(S_1, S_2, \cdots, S_N))$ becomes hard to calculate. However, one can approximate $\lambda_1(U(S_1, S_2, \cdots, S_N))$ by the numerical calculation

$$\lambda_1(U(S_1, S_2, \cdots, S_N)) = \max_{|u\rangle} \langle u|U(S_1, S_2, \cdots, S_N)|u\rangle, \tag{5.17}$$

where the maximum runs over unit vectors $|u\rangle$, then the right-hand side of Eq. (5.17) is a deformation of the well-known *Rayleigh-Ritz ratio*. As the unit ball formed by the vectors is compact, *Weierstraß Theorem* ensures the existence of λ_1. Here we will give two simple estimates of the majorization bound for multi-measurements. To give the first simple estimation, define $CU(1, 2)$ as

$$CU(S_1, S_2) = \begin{pmatrix} 0 & U_{12} & \cdots & 0 \\ U_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{5.18}$$

Similarly, we can define $CU(S_i, S_j)$ for any pair of i, j such that $1 \leqslant i, j \leqslant d$. Then

$$U(S_1, S_2, \cdots, S_N) = I_{N+k-1} + CU(S_1, S_2) + \cdots + CU(S_{N-1}, S_N). \tag{5.19}$$

Using *Weyl's Theorem* on eigenvalues of hermitian matrices, we get that

$$\begin{aligned} &\lambda_1(U(S_1, S_2, \cdots, S_N)) \\ =&1 + \lambda_1(CU(S_1, S_2) + \cdots + CU(S_{N-1}, S_N)) \\ \leqslant&1 + \lambda_1(CU(S_1, S_2)) + \cdots + \lambda_1(CU(S_{N-1}, S_N)) \\ =&1 + \sigma_1(U_{12}) + \cdots + \sigma_1(U_{N-1,N}), \end{aligned} \tag{5.20}$$

then we define $\widehat{\Omega}_k$ by

$$\widehat{\Omega}_k = (\frac{1 + \widehat{s}_k}{N})^N, \tag{5.21}$$

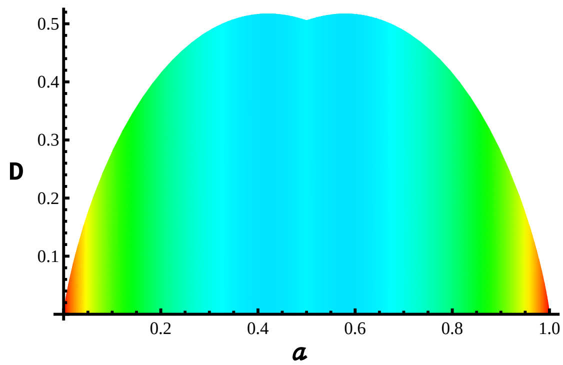

Figure 5.1: Difference (D) of $\log \frac{1}{b}$ from $H(\Omega_1, 1-\Omega_1)$ for $\phi = \pi/2$ with respect to a. The upper curve shows the value of $H(\Omega_1, 1-\Omega_1) + \log b$ and it is always nonnegative over $0 \leqslant a \leqslant 1$.

where

$$\widehat{s}_k = \max_{\sum_{x=1}^{N} S_x = k+N-1} \{\sigma_1(U_{12}) + \cdots + \sigma_1(U_{N-1,N})\}. \tag{5.22}$$

Therefore we arrive at the following result, which was essentially known in [FGG13].

Theorem 5.1.2. *For any d-dimensional quantum state ρ and the probability distributions P^m associated to N measurements M_m, we have that*

$$\bigotimes_{m=1}^{N} P^m \prec \widehat{\omega}, \tag{5.23}$$

It is obvious from the construction of $\widehat{\omega}$ that the bound is weaker than that of Theorem 5.1.1: $\omega \prec \widehat{\omega}$.

As for the second approximation, note that the universal bound $\omega \prec (\Omega_1, 1-\Omega_1)$, which therefore serves as a simple approximation of ω for general N probability distributions. Yet even the bound given by $H(\omega_0)$ with $\omega_0 = (\Omega_1, 1-\Omega_1)$ outperforms $-\log b$ appeared in Eq. (5.3). For example, consider three measurements M_i ($i = 1, 2, 3$) in a three-dimensional Hilbert space with eigenvectors $u_1^1 = (1,0,0)$, $u_2^1 = (0,1,0)$, $u_3^1 = (0,0,1)$; $u_1^2 = (\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}})$, $u_2^2 = (0,1,0)$, $u_3^2 = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$; $u_1^3 = (\sqrt{a}, e^{i\phi}\sqrt{1-a}, 0)$, $u_2^3 = (\sqrt{1-a}, -e^{i\phi}\sqrt{a}, 0)$ and $u_3^3 = (0,0,1)$. With the choice of $\phi = \pi/2$, we see that the simplest majorization bound $\omega_0 = (\Omega_1, 1-\Omega_1)$ under the Shannon entropy is superior to $-\log b$ over the whole range $0 \leqslant a \leqslant 1$, where $b = \max_{i_3}\{\sum_{i_2} \max_{i_1}[c(u_{i_1}^1, u_{i_2}^2)]c(u_{i_2}^2, u_{i_3}^3)\}$.

The difference between our second estimation bound $H(\omega_0)$ and Eq. (5.3), namely $H(\Omega_1, 1-\Omega_1) + \log b$, is shown in FIG. 5.1.

Admixture Bounds via Symmetry

As we discussed in the begining of Sec. 5.1, using Coles and Piani's method, S. Liu *et al.* have given an entropic uncertainty bound for multi-measurements by quantum channels [LMF15]:

$$\sum_{m=1}^{N} H(M_m) \geqslant -\log b + (N-1)S(\rho), \tag{5.24}$$

where

$$b = \max_{i_N} \left\{ \sum_{i_2 \sim i_{N-1}} \max_{i_1}[c(u^1_{i_1}, u^2_{i_2})] \prod_{m=2}^{N-1} c(u^m_{i_m}, u^{m+1}_{i_{m+1}}) \right\}. \tag{5.25}$$

We now use the method of symmetry to significantly strengthen the bound. We note that the above bound depends on the order of the measurements, so it is natural to denote the bound as $b(M_1, M_2, \cdots, M_N)$ or simply $b(1, 2, \cdots, N)$ to specify the order of the measurements $M_1, \cdots, M_N$. Using the apparent symmetry of the measurements, we can define the action of the symmetric group on the bounds. For each permutation $\alpha \in \mathfrak{S}_N$ we define

$$\alpha b(1, \cdots, N) = b(\alpha(1), \alpha(2), \cdots, \alpha(N)). \tag{5.26}$$

and observe that $\mathfrak{S}_N$ leaves the second term $(N-1)S(\rho)$ of Eq. (5.24) invariant. This immediately implies the following entropic uncertainty relation:

$$\sum_{m=1}^{N} H(M_m) + (1-N)S(\rho) \geqslant -\log b_{min}, \tag{5.27}$$

where

$$b_{min} = \min_{\alpha \in \mathfrak{S}_N} \{b(\alpha(1), \alpha(2), \cdots, \alpha(N))\}. \tag{5.28}$$

Apparently $-\log b_{min} \geqslant -\log b$, so this new bound $-\log b_{min} + (N-1)S(\rho)$ is tighter than the bound appeared in [LMF15]. This shows that the action of the symmetry group can significantly improve the bound. We remark that a similar consideration has been discussed in [ZZY15]. Our treatment has clarified how the symmetric group acts on the measurements, which plays an important role in our further investigation.

Now we discuss how to blend the $\mathfrak{S}_N$-symmetry and the method of quantum channels to derive a tighter bound than we did in the above.

Suppose we are given N measurements $M_1, \cdots, M_N$ with orthonormal bases $\{|u^j_{i_j}\rangle\}$. For a multi-index $(i_1, \cdots, i_N)$, where $1 \leqslant i_j \leqslant d$, we define the multi-overlap

$$c^{1,\cdots,N}_{i_1,\cdots,i_N} = c(u^1_{i_1}, u^2_{i_2})c(u^2_{i_2}, u^3_{i_3}) \cdots c(u^{N-1}_{i_{N-1}}, u^N_{i_N}).$$

Then we have that (cf. [LMF15])

$$\begin{aligned}(1-N)S(\rho) + \sum_{m=1}^{N} H(M_m) \geqslant& - \operatorname{Tr}(\rho \log \sum_{i_1,i_2,\cdots,i_N} p^1_{i_1} c^{1,\cdots,N}_{i_1,\cdots,i_N} [u^N_{i_N}]) \\ =& - \sum_{i_N} p^N_{i_N} \log \sum_{i_1,i_2,\cdots,i_{N-1}} p^1_{i_1} c^{1,\cdots,N}_{i_1,\cdots,i_N} \\ :=& I(1,2,\cdots,N),\end{aligned} \tag{5.29}$$

where $[u]$ stands for $|u\rangle\langle u|$. Note that the above inequality is obtained by a fixing order of $M_1, \cdots, M_N$ which explains why we can denote the last expression as $I(1, 2, \cdots, N)$. Therefore for any permutation $\alpha \in \mathfrak{S}_N$, one has that

$$(1-N)S(\rho) + \sum_{m=1}^{N} H(M_m) \geqslant I(\alpha(1), \alpha(2), \cdots, \alpha(N)), \tag{5.30}$$

Taking the average of all permutations, we arrive at the following relation

$$(1-N)S(\rho) + \sum_{m=1}^{N} H(M_m) \geqslant \frac{\sum_{\alpha\in\mathfrak{S}_N} I(\alpha(1), \cdots, \alpha(N))}{N!}. \tag{5.31}$$

Further analysis of the action of the symmetric group on the bound

$$I(\alpha(1), \cdots, \alpha(N)),$$

shows that only the first and the last indices matter in the formula, as the bound is invariant under the action of any permutation from $\mathfrak{S}_{2,\cdots,N-1}$. Among the remaining $N(N-1)$ permutations, it is enough to consider the cyclic group of N permutations. Therefore the above average can be simplified to the following form:

$$(1-N)S(\rho) + \sum_{m=1}^{N} H(M_m) \geqslant \frac{\sum_{\text{cyclic } \alpha} I(\alpha(1), \cdots, \alpha(N))}{N}, \tag{5.32}$$

where the sum runs through all N cyclic permutations

$$(12\cdots N), (23\cdots 1), \cdots, (N1\cdots N-1).$$

Let's consider the case of three measurements M_m in detail. By using Eq. (5.29), we get that

$$-2S(\rho) + \sum_{m=1}^{3} H(M_m) \geqslant -\alpha\Big(\sum_{i_3} p_{i_3}^3 \log \sum_{i_1,i_2} p_{i_1}^1 c_{i_1 i_2 i_3}^{123}\Big) := \alpha(I(1,2,3)), \tag{5.33}$$

for any $\alpha \in \mathfrak{S}_3$, thus

$$\begin{aligned}-2S(\rho) + \sum_{m=1}^{3} H(M_m) \geqslant& \frac{1}{3}(I(1,2,3) + I(2,3,1) + I(3,1,2)) \\ =& \frac{\sum\limits_{i_1,i_2,i_3} p_{i_1}^1 p_{i_2}^2 p_{i_3}^3 \log \sum p_{k_1}^1 p_{k_2}^2 p_{k_3}^3 c_{k_1 j_2 i_3}^{123} c_{k_2 j_3 i_1}^{231} c_{k_3 j_1 i_2}^{312}}{-3}\end{aligned} \tag{5.34}$$

where the sum inside logarithm runs over $j_1, j_2, j_3,\ k_1, k_2, k_3$. For multi-index (i_1, i_2, i_3) we define the d^3-dimensional vector $\mathfrak{A}_{i_1,i_2,i_3}$ given by the elements

$$\sum_{j_1,j_2,j_3} c_{k_1 j_2 i_3}^{123} c_{k_2 j_3 i_1}^{231} c_{k_3 j_1 i_2}^{312}, \tag{5.35}$$

and sorted in decreasing order with respect to multi-indices (k_1, k_2, k_3) (lexicographic order). Combined with the majorization bound $\omega \in \mathbb{R}^{d^3}$ formulated in Sec. 5.1.1, we immediately get that

$$-\log \sum p_{k_1}^1 p_{k_2}^2 p_{k_3}^3 c_{k_1 j_2 i_3}^{123} c_{k_2 j_3 i_1}^{231} c_{k_3 j_1 i_2}^{312} \geqslant -\log(\omega \cdot \mathfrak{A}_{i_1,i_2,i_3}). \tag{5.36}$$

Then we introduce another d^3-dimensional vector $\mathfrak{B}$ defined by $\mathfrak{B}_{i_1,i_2,i_3} = \log(\omega \cdot \mathfrak{A}_{i_1,i_2,i_3})$ and sorted in decreasing order with respect to multi-indices (i_1, i_2, i_3) in the lexicographic order. Therefore we obtain the following *admixture* bound for 3 measurements

$$-2S(\rho) + \sum_{m=1}^{3} H(M_m) \geqslant -\frac{1}{3}\omega\mathfrak{B}. \tag{5.37}$$

The new bound provides an improved lower bound for the uncertainty relation. In Fig. 5.2 we give an example to show that the admixture bound completely outperforms the other bounds that we have known so far for multi-measurements. Moreover, this admixture bound can be easily extended to multi-measurements.

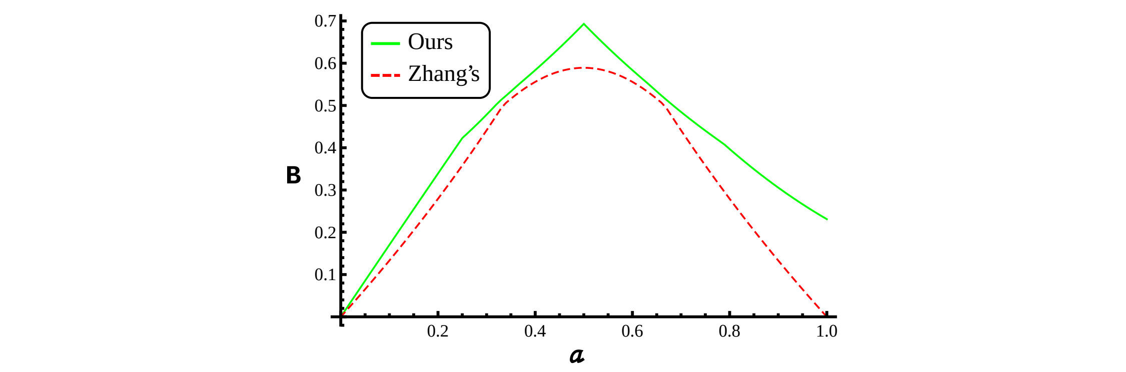

Figure 5.2: Comparison of the admixture bound with Zhang *et al.*'s bound for $\phi = \pi/2$ with $a \in [0,1]$. Our bound in green is shown as the top curve and always tighter. Here ln is used on the bound axis (B).

Let $M_i = \{|u^i_{i_j}\rangle\}$ be N measurements, where $i = 1, 2, \cdots, N$ and $j = 1, 2, \cdots, d$. For each multi-index $(i_1, i_2, \cdots, i_N)$ we introduce a d^N-dimensional vector $\mathfrak{A}_{i_1,i_2,\cdots,i_N}$ with the entries

$$\sum_{\hat{\mathbf{i}}\mathbf{j}\cdots\hat{\mathbf{k}}} c^{12\cdots N}_{k_1 j_2 \cdots i_N} c^{23\cdots 1}_{k_2 j_3 \cdots i_1} \cdots c^{N1\cdots N-1}_{k_N j_1 \cdots i_{N-1}}$$

where the sum runs over all indices except $\mathbf{i} = (i_1 \cdots i_N)$ and $\mathbf{k} = (k_1 \cdots k_N)$, and then sorted in decreasing order with respect to lexicographic order of multi-indices $(k_1, \cdots, k_N)$. Set $log(\omega \cdot \mathfrak{A}_{i_1,i_2,\cdots,i_N}) := \mathfrak{B}_{i_1,i_2,\cdots,i_N}$ as the next d^N-dimensional vector with ω being the majorization bound for N measurements formulated in Sec. 5.1.1. Here $\mathfrak{B}_{i_1,i_2,\cdots,i_N}$ is assumed to be arranged in decreasing order with respect to the multi-indices $(i_1, i_2, \cdots, i_N)$ lexicographically. The following result is then proved similarly as before.

Theorem 5.1.3. *The following entropic uncertainty relation holds,*

$$\sum_{m=1}^{N} H(M_m) + (1-N)S(\rho) \geqslant -\frac{1}{N}\omega\mathfrak{B}. \tag{5.38}$$

The admixture bound is tighter than the previously known bounds. In fact, Fig. 5.2 depicts a comparison of our bound with that of J. Zhang *et al.* [ZZY15], while the latter is known to be tighter than the bound appeared in [LMF15].

In this section, we have derived several tighter bounds for entropic uncertainty relations of multi-measurements and in particular an admixture bound is obtained and proved to be tighter than all previously known bounds. Inspired by the recent work [CP14, LMF15, FGG13, PRŻ13, RPŻ14] we have taken the advantage of unitary matrix $U(S_1, S_2, \cdots, S_N)$ and come up with the universal bound for the multi-tensor products of distribution vectors. To derive a deeper and better bound for N measurements, we have studied the action of the symmetric group $\mathfrak{S}_N$ in combination with the universal vector bound of the distribution vectors and quantum channels. The derived admixture bound turns out to be non-trivial bound for the uncertainties of N measurements. Detailed comparisons with previously known bounds are given in figures, and our admixture bound seems to outperform the other bounds most of the time.

Entropy characterizes and quantifies the physical essence of information resources in a mathematical manner. The computational and operational properties of entropy make entropic uncertainty relations useful for quantum key distributions and other quantum cryptography tasks, which can be performed relatively easy in a physical laboratory. Our new bounds are expected to be useful in handling large data for these and further quantum information processings.

5.2 Enhanced Information Exclusion Relations

In Hall's reformulation of the uncertainty principle, the entropic uncertainty relation occupies a core position and provides the first nontrivial bound for the information exclusion principle. Based upon recent developments on the uncertainty relation, we present new bounds for the information exclusion relation using majorization theory and combinatoric techniques, which reveal further characteristic properties of the overlap matrix between the measurements.

Mutual information is a measure of correlations and plays a central role in communication theory [CT06, Hol73a, YO93] . While the entropy describes uncertainties of measurements [WW10, BPP12, Deu83, MU88] , mutual information quantifies bits of gained information. Further, information is a more natural quantifier than entropy except in applications like transmission over quantum channels[DST14] . The sum of information corresponding to measurements of position and momentum is bounded by the quantity $\log 2\Delta X \Delta P_X/\hbar$ for a quantum system with uncertainties for complementary observables ΔX and ΔP_X, and this is equivalent to a formalization of Heisenberg uncertainty principle [Hei27] . Both the uncertainty relation and information exclusion relation [Hal95, Hal97, CYGG11] have been used to study the complementarity of obervables such as position and momentum. The standard deviation has also been employed to quantify uncertainties, and it has been recognized later that the entropy seems more suitable in studying certain aspects of uncertainties.

As one of the well-known entropic uncertainty relations, Maassen and Uffink's formulation [MU88] states that

$$H(M_1) + H(M_2) \geqslant -\log c_{max}, \tag{5.39}$$

where $H(M_k) = H(M_k, \rho) = -\sum_j p_j^k \log_2 p_j^k$ with $p_j^k = \langle u_j^k|\rho|u_j^k\rangle$ $(k = 1, 2; j = 1, 2, \ldots, d)$ for a given density matrix ρ of dimension d, while $c_{max} = \max_{i_1,i_2} c(u_{i_1}^1, u_{i_2}^2)$, and $c(u_{i_1}^1, u_{i_2}^2) = |\langle u_{i_1}^1|u_{i_2}^2\rangle|^2$ for two orthonormal bases $M_1 = \{|u_{i_1}^1\rangle\}$ and $M_2 = \{|u_{i_2}^2\rangle\}$ of d-dimensional Hilbert space $\mathcal{H}$.

Hall [Hal95] generalized Eq.(5.39) to give the first bound of the *Information Exclusion Relation* on accessible information about a quantum system represented by an ensemble of states. Let M_1 and M_2 be as above on system A, and let B be another classical register (which may be related to A), then

$$I(M_1 : B) + I(M_2 : B) \leqslant r_H, \tag{5.40}$$

where $r_H = \log_2(d^2 c_{max})$ and $I(M_i : B) = H(M_i) - H(M_i|B)$ is the *mutual information* [Rez61] corresponding to the measurement M_i on system A. Here $H(M_i|B)$ is the conditional entropy relative to the subsystem B. Moreover, if system B is quantum memory, then $H(M_i|B) = H(\rho_{M_iB}) - H(\rho_B)$ with $\rho_{M_iB} = (\mathcal{M}_i \otimes I)(\rho_{AB})$, while $\mathcal{M}_i(\cdot) = \sum_{k_i} |u_{k_i}^i\rangle\langle u_{k_i}^i|(\cdot)|u_{i_k}^i\rangle\langle u_{k_i}^i|$. Eq. (5.40) depicts that it is impossible to probe the register B to reach complete information about observables M_1 and M_2 if the maximal overlap c_{max} between measurements is small. Unlike the entropic uncertainty relations, the bound r_H is far from being tight. Grudka *et al.* [GHH$^+$13] conjectured a stronger information exclusion relation based on numerical evidence (proved analytically only in some special cases)

$$I(M_1 : B) + I(M_2 : B) \leqslant r_G, \tag{5.41}$$

where $r_G = \log_2 \left(d \cdot [\sum_{d\ largest} c(u_{i_1}^1, u_{i_2}^2)] \right)$. As the sum runs over the d largest $c(u_i^1, u_j^2)$, we get $r_G \leqslant r_H$, so Eq. (5.41) is an improvement of Eq. (5.41). Recently Coles and Piani [CP14] obtained a new information exclusion relation stronger than Eq. (5.41) and can also be strengthened to the case of quantum memory [BCC$^+$10]

$$I(M_1 : B) + I(M_2 : B) \leqslant r_{CP} - H(A|B), \tag{5.42}$$

where

$$r_{CP} = \min\{r_{CP}(M_1, M_2), r_{CP}(M_2, M_1)\},$$

$$r_{CP}(M_1, M_2) = \log_2 \left(d \sum_{i_1} \max_{i_2} c(u_{i_1}^1, u_{i_2}^2) \right),$$

and $H(A|B) = H(\rho_{AB}) - H(\rho_B)$ is the conditional von Neumann entropy with $H(\varrho) = -\operatorname{Tr}(\varrho \log_2 \varrho)$ the von Neumann entropy, while ρ_B represents the reduced state of the quantum state ρ_{AB} on subsystem B. It is clear that $r_{CP} \leqslant r_G$.

As pointed out in Ref. [Hal95] , the general information exclusion principle should have the form

$$\sum_{m=1}^{N} I(M_m : B) \leqslant r(M_1, M_2, \ldots, M_N, B), \tag{5.43}$$

for observables $M_1, M_2, \ldots, M_N$, where $r(M_1, M_2, \ldots, M_N, B)$ is a nontrivial quantum bound. Such a quantum bound is recently given by Zhang *et al.* [ZZY15] for the information exclusion principle of multi-measurements in the presence of the quantum memory. However, almost all available bounds are not tight even for the case of two observables.

Our goal in this section is to give a general approach for the information exclusion principle using new bounds for two and more observables of quantum systems of any finite dimension by generalizing Coles-Piani's uncertainty relation and using majorization techniques. In particular, all of our results can be reduced to the case without quantum memory.

The close relationship between the information exclusion relation and the uncertainty principle has promoted mutual developments. In the applications of the uncertainty relation to the former, there have been usually two available methods: either through subtraction of the uncertainty relation in the presence of quantum memory or utilizing the concavity property of the entropy together with combinatorial techniques or certain symmetry. Our second goal in this work is to analyze these two methods and in particular, we will show that the second method together with a special combinatorial scheme enables us to find tighter bounds for the information exclusion principle. The underlined reason for effectiveness is due to the special composition of the mutual information. We will take full advantage of this phenomenon and apply a distinguished symmetry of cyclic permutations to derive new bounds, which would have been difficult to obtain without consideration of mutual information.

We also remark that the recent result [XJF+16] for the sum of entropies is valid in the absence of quantum side information and cannot be extended to the cases with quantum memory by simply adding the conditional entropy between the measured particle and quantum memory. To resolve this difficulty, we use a different method in this paper to generalize the results of Ref. [XJF+16] in Lemma 5.2.2 and Theorem 5.2.3 to allow for quantum memory.

Two Observables

We first consider the information exclusion principle for two observables, and then generalize it to multi-observables cases. After that we will show that our information exclusion relation gives a tighter bound, and the bound not only involves the d largest $c(u^1_{i_1}, u^2_{i_2})$ but contains all the overlaps $c(u^1_{i_1}, u^2_{i_2})$ between bases of measurements.

We start with a qubit system to show our idea. The bound offered by Coles and Piani for two measurements does not improve the previous bounds for qubit systems. To see these, set $c_{i_1i_2} = c(u^1_{i_1}, u^2_{i_2})$ for brevity, then the unitarity of overlaps between measurements implies that $c_{11}+c_{12} = 1$, $c_{11}+c_{21} = 1$, $c_{21}+c_{22} = 1$ and $c_{12} + c_{22} = 1$. Assuming $c_{11} > c_{12}$, then $c_{11} = c_{22} > c_{12} = c_{21}$, thus

$$\begin{aligned} r_H &= \log_2(d^2 c_{max}) = \log_2(4c_{11}), \\ r_G &= \log_2(d \sum_{d\ largest} c(u^1_{i_1}, u^2_{i_2})) = \log_2(2(c_{11} + c_{22})), \\ r_{CP} &= \min\{r_{CP}(M_1, M_2), r_{CP}(M_2, M_1)\} = \log_2(2(c_{11} + c_{22})), \end{aligned} \tag{5.44}$$

hence we get $r_H = r_G = r_{CP} = \log_2(4c_{11})$ which says that the bounds of Hall, Grudka *et al*, and Coles and Piani coincide with each other in this case.

Our first result already strengthens the bound in this case. Recall the implicit bound from the tensor-product majorization relation [FGG13, PRŻ13, RPŻ14] is of the form

$$H(M_1|B) + H(M_2|B) \geqslant -\frac{1}{2}\omega\mathfrak{B} + H(A) - 2H(B), \tag{5.45}$$

where the vectors $\mathfrak{B} = (\log_2(\omega \cdot \mathfrak{A}_{i_1i_2}))^{\downarrow}$ and $\mathfrak{A}_{i_1,i_2} = (c(u^1_{i_1}, u^2_{i})c(u^1_{j}, u^2_{i_2}))^{\downarrow}_{ij}$ are of size d^2. The symbol $\downarrow$ means re-arranging the components in descending order. The majorization vector bound ω for probability tensor distributions $(p^1_{i_1}p^2_{i_2})_{i_1i_2}$ of state ρ is the d^2-dimensional vector $\omega = (\Omega_1, \Omega_1 - \Omega_2, \ldots, \Omega_d - \Omega_{d-1}, 0, \ldots, 0)$, where

$$\Omega_k = \max_{\rho} \sum_{|\{(i_1,i_2)\}|=k} p^1_{i_1}p^2_{i_2}.$$

The bound means that

$$(p^1_{i_1}p^2_{i_2})_{i_1i_2} \prec \omega,$$

for any density matrix ρ and $\prec$ is defined by comparing the corresponding partial sums of the decreasingly rearranged vectors. Therefore ω only depends on $c_{i_1i_2}$ [RPŻ14] . We remark that the quantity $H(A) - 2H(B)$ assumes a similar role as that of $H(A|B)$, which will be clarified in Theorem 5.2.3. As for more general case of N measurements, this quantity is replaced by $(N-1)H(A) - NH(B)$ in the place of $NH(A|B)$. A proof of this relation will be given. The following is our first improved information exclusion relation in a new form.

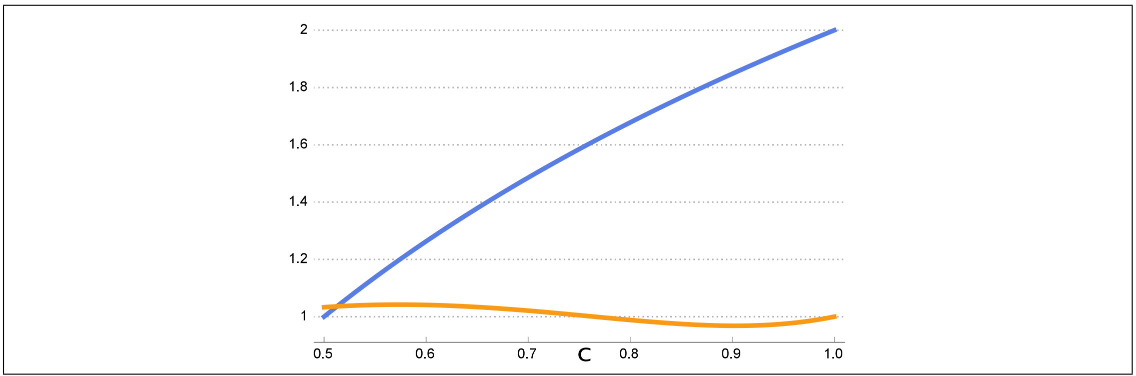

Figure 5.3: First comparison with Hall's bound. The lower orange curve (our bound $2+\frac{1}{2}\omega\mathfrak{B}$) is tighter than the upper blue one (Hall's bound r_H) almost everywhere.

Theorem 5.2.1. *For any bipartite state ρ_{AB}, let M_1 and M_2 be two measurements on system A, and let B be the quantum memory correlated to A, then*

$$I(M_1:B)+I(M_2:B)\leqslant 2+\frac{1}{2}\omega\mathfrak{B}+2H(B)-H(A), \tag{5.46}$$

where ω is the majorization bound and $\mathfrak{B}$ is defined in the paragraph under Eq. (5.45).

Proof. Recall that the quantum relative entropy $D(\rho||\sigma)=\mathrm{Tr}(\rho\log_2\rho)-\mathrm{Tr}(\rho\log_2\sigma)$ satisfies that $D(\rho||\sigma)\geqslant D(\tau\rho||\tau\sigma)\geqslant 0$ under any quantum channel τ. Denote by $\rho_{AB}\to\rho_{M_1B}$ the quantum channel $\rho_{AB}\to\sum_i|u_i^1\rangle\langle u_i^1|\rho_{AB}|u_i^1\rangle\langle u_i^1|$, which is also $\rho_{M_1B}=\sum_i|u_i^1\rangle\langle u_i^1|\otimes\mathrm{Tr}_A(\rho_{AB}|u_i^1\rangle\langle u_i^1|)$. Note that both $M^i=\{|u_j^i\rangle\}(i=1,2)$ are measurements on system A, we have that for a bipartite state ρ_{AB}

$$\begin{aligned}H(M_1|B)-H(A|B)&=H(\rho_{M_1B})-H(\rho_{AB})\\&=\mathrm{Tr}(\rho_{AB}\log_2\rho_{AB})-\mathrm{Tr}(\rho_{M_1B}\log_2\rho_{M_1B})\\&=D(\rho_{AB}||\sum_{i_1}|u_{i_1}^1\rangle\langle u_{i_1}^1|\otimes\mathrm{Tr}_A(\rho_{AB}|u_{i_1}^1\rangle\langle u_{i_1}^1|)).\end{aligned}$$

Note that $\mathrm{Tr}_B\,\mathrm{Tr}_A(\rho_{AB}|u_i^1\rangle\langle u_i^1|)=p_i^1$, the probability distribution of the reduced state ρ_A under the measurement M_1, so $\sigma_{B_i}=\mathrm{Tr}_A(\rho_{AB}|u_i^1\rangle\langle u_i^1|)/p_i^1$ is a density matrix on the system B. Then the last expression can be written as

$$\begin{aligned}&D(\rho_{AB}||\sum_{i_1}p_{i_1}^1|u_{i_1}^1\rangle\langle u_{i_1}^1|\otimes\sigma_{B_{i_1}})\\\geqslant&D(\rho_{M_2B}||\sum_{i_1,i_2}p_{i_1}^1C_{i_1i_2}|u_{i_2}^2\rangle\langle u_{i_2}^2|\otimes\sigma_{B_{i_1}})).\end{aligned}$$

If system B is a classical register, then we can obtain

$$H(M_1) + H(M_2) \geqslant H(A) - \sum_{i_2} p^2_{i_2} \log \sum_{i_1} p^1_{i_1} c(u^1_{i_1}, u^2_{i_2}), \tag{5.47}$$

by swapping the indices i_1 and i_2, we get that

$$H(M_2) + H(M_1) \geqslant H(A) - \sum_{i_1} p^1_{i_1} \log \sum_{i_2} p^2_{i_2} c(u^2_{i_2}, u^1_{i_1}). \tag{5.48}$$

Their combination implies that

$$\begin{aligned} &H(M_1) + H(M_2) \\ \geqslant &H(A) - \frac{1}{2}\left(\sum_{i_2} p^2_{i_2} \log \sum_{i_1} p^1_{i_1} c(u^1_{i_1}, u^2_{i_2}) + \sum_{i_1} p^1_{i_1} \log \sum_{i_2} p^2_{i_2} c(u^2_{i_2}, u^1_{i_1})\right), \end{aligned} \tag{5.49}$$

thus it follows from Ref. [NC10] that

$$\begin{aligned} &H(M_1|B) + H(M_2|B) \\ \geqslant &H(A) - 2H(B) - \frac{1}{2}\left(\sum_{i_2} p^2_{i_2} \log \sum_{i_1} p^1_{i_1} c(u^1_{i_1}, u^2_{i_2}) + \sum_{i_1} p^1_{i_1} \log \sum_{i_2} p^2_{i_2} c(u^2_{i_2}, u^1_{i_1})\right), \end{aligned} \tag{5.50}$$

hence

$$\begin{aligned} I(M_1|B) + I(M_2|B) &= H(M_1) + H(M_2) - (H(M_1|B) + H(M_2|B)) \\ &\leqslant H(M_1) + H(M_2) \\ &\quad + \frac{1}{2}\left(\sum_{i_2} p^2_{i_2} \log \sum_{i_1} p^1_{i_1} c(u^1_{i_1}, u^2_{i_2}) + \sum_{i_1} p^1_{i_1} \log \sum_{i_2} p^2_{i_2} c(u^2_{i_2}, u^1_{i_1})\right) \\ &\quad + 2H(B) - H(A) \\ &\leqslant H(M_1) + H(M_2) \\ &\quad + \frac{1}{2} \sum_{i_1, i_2} p^1_{i_1} p^2_{i_2} \log_2 \left(\sum_{i,j} p^1_i p^2_j c(u^1_i, u^2_{i_2}) c(u^2_j, u^1_{i_1}) \right) \\ &\quad + 2H(B) - H(A) \\ &\leqslant 2 + \frac{1}{2}\omega \mathfrak{B} + 2H(B) - H(A), \end{aligned} \tag{5.51}$$

where the last inequality has used $H(M_i) \leqslant \log_2 d$ $(i = 1, 2)$ and the vector $\mathfrak{B}$ of length d^2, whose entries $\mathfrak{B}_{i_1 i_2} = \log_2(\omega \cdot \mathfrak{A}_{i_1 i_2})$ are arranged in decreasing order

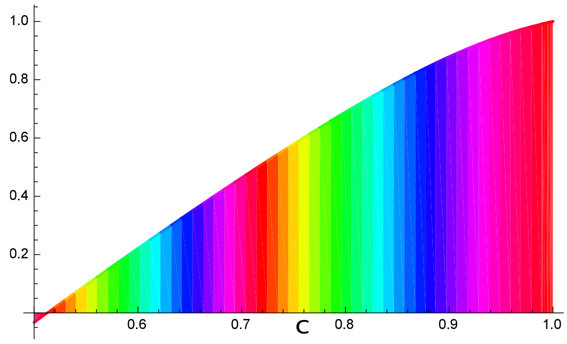

Figure 5.4: First comparison with Hall's bound. The difference $r_H - 2 - \frac{1}{2}\omega\mathfrak{B}$ of our bound from Hall's bound r_H for $a \in [0.5, 1]$ is shown.

with respect to (i_1, i_2). Here the vector $\mathfrak{A}$ is defined by $\mathfrak{A}_{i_1 i_2} = c(u_i^1, u_{i_2}^2)c(u_j^2, u_{i_1}^1)$ for each (i_1, i_2) and also sorted in decreasing order. Note that the extra term $2H(B) - H(A)$ is another quantity appearing on the right-hand side that describes the amount of entanglement between the measured particle and quantum memory besides $-H(A|B)$.

We now derive the *information exclusion relation* for qubits in the form of $I(M_1 : B) + I(M_2 : B) \leqslant 2 + \frac{1}{2}\omega\mathfrak{B} + 2H(B) - H(A)$, and this completes the proof. ■

Eq. (5.46) gives an implicit bound for the information exclusion relation, and it is tighter than $\log_2(4c_{max}) + 2H(B) - H(A)$ as our bound not only involves the maximal overlap between M_1 and M_2, but also the second largest element based on the construction of the universal uncertainty relation ω [FGG13, PRŻ13] . Majorization approach [FGG13, PRŻ13] has been widely used in improving the lower bound of entropic uncertainty relation. The application in the information exclusion relation offers a new aspect of the majorization method. The new bound not only can be used for arbitrary nonnegative Schur-concave function [AMO11] such as Rényi entropy and Tsallis entropy [HC67] , but also provides insights to the relation among all the overlaps between measurements, which explains why it offers a better bound for both entropic uncertainty relations and information exclusion relations. We also remark that the new bound is still weaker than the one based on the optimal entropic uncertainty relation for qubits [GMR03] .

As an example, we consider the measurements $M_1 = \{(1,0), (0,1)\}$ and $M_2 = \{(\sqrt{a}, e^{i\phi}\sqrt{1-a}), (\sqrt{1-a}, -e^{i\phi}\sqrt{a})\}$. Our bound and $\log_2 4c_{max}$ for $\phi = \pi/2$ with respect to a are shown in FIG. 5.3.

FIG. 5.3 shows that our bound for qubit is better than the previous bounds $r_H = r_G = r_{CP}$ almost everywhere. Using symmetry we only consider a in $[\frac{1}{2}, 1]$. The common term $2H(B) - H(A)$ is omitted in the comparison. Further analysis

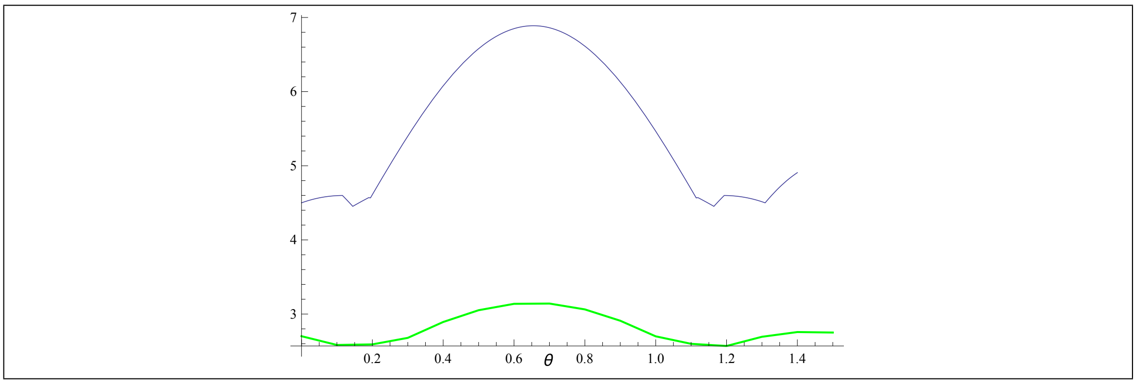

Figure 5.5: Comparison of our bound with that of Coles and Piani. Our bound $2+\frac{1}{2}\omega\mathfrak{B}$ (lower in green) is better than Coles-Piani's bound r_{CP} (upper in purple) everywhere.

of the bounds is given in FIG. 5.4.

Theorem 5.2.1 holds for any bipartite system and can be used for arbitrary two measurements M_i $(i=1,2)$. For example, consider the qutrit state and a family of unitary matrices $U(\theta)=M(\theta)O_3M(\theta)^\dagger$ [CP14, RPŻ14] where

$$M(\theta)=\begin{pmatrix}1&0&0\\0&\cos\theta&\sin\theta\\0&-\sin\theta&\cos\theta\end{pmatrix},$$

$$O_3=\frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{2}&\sqrt{2}&\sqrt{2}\\\sqrt{3}&0&-\sqrt{3}\\1&-2&1\end{pmatrix}. \tag{5.52}$$

Upon the same matrix $U(\theta)$, comparison between our bound $2+\frac{1}{2}\omega\mathfrak{B}$ and Coles-Piani's bound r_{CP} is depicted in FIG. 5.5.

Multi-Observables

In order to generalize the information exclusion relation to multi-measurements, we recall that the universal bound of tensor products of two probability distribution vectors can be computed by optimization over minors of the overlap matrix [FGG13, PRŻ13] . More generally for the multi-tensor product $(p^1_{i_1}p^2_{i_2}\cdots p^N_{i_N})$ corresponding to measurement M_m on a fixed quantum state, there exists similarly a universal upper bound ω: $(p^1_{i_1}p^2_{i_2}\cdots p^N_{i_N})\prec\omega$. Then we have the following lemma, which generalizes Eq. (5.45).

Lemma 5.2.2. *For any bipartite state ρ_{AB}, let M_m $(m=1,2,\ldots,N)$ be N measurements on system A, and B the quantum memory correlated to A, then the* *following entropic uncertainty relation holds,*

$$\sum_{m=1}^{N} H(M_m|B) \geqslant -\frac{1}{N}\omega\mathfrak{B} + (N-1)H(A) - NH(B), \tag{5.53}$$

where ω *is the* d^N*-dimensional majorization bound for the* N *measurements* M_m *and* $\mathfrak{B}$ *is the* d^N*-dimensional vector* $(log(\omega \cdot \mathfrak{A}_{i_1,i_2,\ldots,i_N}))^{\downarrow}$ *defined as follows. For each multi-index* $(i_1, i_2, \ldots, i_N)$*, the* d^N*-dimensional vector* $\mathfrak{A}_{i_1,i_2,\ldots,i_N}$ *has entries of the form* $c(1,2,\ldots,N)c(2,3,\ldots,1)\cdots c(N,1,\ldots,N-1)$ *sorted in decreasing order with respect to the indices* $(i_1, i_2, \ldots, i_N)$ *where* $c(1,2,\ldots,N) = \sum_{i_2,\ldots,i_{N-1}} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) \cdots c(u^{N-1}_{i_{N-1}}, u^N_{i_N})$ *.*

Proof. Suppose we are given N measurements $M_1, \ldots, M_N$ with orthonormal bases $\{|u^j_{i_j}\rangle\}$. To simplify presentation we denote that

$$c^{1,\ldots,N}_{i_1,\ldots,i_N} = c(u^1_{i_1}, u^2_{i_2})c(u^2_{i_2}, u^3_{i_3}) \cdots c(u^{N-1}_{i_{N-1}}, u^N_{i_N}).$$

Then we have that [LMF15]

$$\begin{aligned} &(1-N)H(A) + \sum_{m=1}^{N} H(M_m) \\ \geqslant &-\mathrm{Tr}(\rho \log \sum_{i_1,i_2,\ldots,i_N} p^1_{i_1} c^{1,\ldots,N}_{i_1,\ldots,i_N} |u^N_{i_N}\rangle\langle u^N_{i_N}|) \\ = &-\sum_{i_N} p^N_{i_N} \log \sum_{i_1,i_2,\ldots,i_{N-1}} p^1_{i_1} c^{1,\ldots,N}_{i_1,\ldots,i_N}. \end{aligned} \tag{5.54}$$

Then consider the action of the cyclic group of N permutations on indices $1, 2, \cdots, N$, and take the average can obtain the following inequality:

$$\sum_{m=1}^{N} H(M_m) \geqslant -\frac{1}{N}\omega\mathfrak{B} + (N-1)H(A), \tag{5.55}$$

where the notations are the same as appeared in Eq. (5.53). Thus it follows from Ref. [NC10] that

$$\sum_{m=1}^{N} H(M_m|B) \geqslant -\frac{1}{N}\omega\mathfrak{B} + (N-1)H(A) - NH(B). \tag{5.56}$$

The proof is finished. ∎

We remark that the *admixture bound* introduced in Ref. [XJF+16] was based upon the majorization theory with the help of the action of the symmetric group, and it was shown that the bound outperforms previous results. However, the admixture bound cannot be extended to the entropic uncertainty relations in the presence of quantum memory for multiple measurements directly. Here we first use a new method to generalize the results of Ref. [XJF+16] to allow for the quantum side information by mixing properties of the conditional entropy and Holevo inequality in Lemma 5.2.2. Moreover, by combining Lemma 5.2.2 with properties of the entropy we are able to give an enhanced information exclusion relation (see Theorem 5.2.3 for details).

The following theorem is obtained by subtracting the entropic uncertainty relation from the above result.

Theorem 5.2.3. *For any bipartite state ρ_{AB}, let M_m $(m = 1, 2, \ldots, N)$ be N measurements on system A, and B the quantum memory correlated to A, then*

$$\sum_{m=1}^{N} I(M_m : B) \leqslant \log_2 d^N + \frac{1}{N}\omega\mathfrak{B} + NH(B) - (N-1)H(A) := r_x, \tag{5.57}$$

where $\frac{1}{N}\omega\mathfrak{B}$ is defined in Eq. (5.53).

Proof. Similar to the proof of Theorem 5.2.1, due to $I(M_m : B) = H(M_m) - H(M_m|B)$, thus we get

$$\begin{aligned}\sum_{m=1}^{N} I(M_m : B) &= \sum_{m=1}^{N} H(M_m) - \sum_{m=1}^{N} H(M_m|B)\\ &\leqslant \sum_{m=1}^{N} H(M_m) + \frac{1}{N}\omega\mathfrak{B} + NH(B) - (N-1)H(A)\\ &\leqslant \log_2 d^N + \frac{1}{N}\omega\mathfrak{B} + NH(B) - (N-1)H(A),\end{aligned} \tag{5.58}$$

with the product $\frac{1}{N}\omega\mathfrak{B}$ the same in Eq. (5.53). ■

Throughout this section, we take $NH(B) - (N-1)H(A)$ instead of $-(N-1)H(A|B)$ as the variable that quantifies the amount of entanglement between measured particle and quantum memory since $NH(B) - (N-1)H(A)$ can outperform $-(N-1)H(A|B)$ numerically to some extent for entropic uncertainty relations.

Our new bound for multi-measurements offers an improvement than the bound recently given in Ref. [ZZY15] . Let us recall the information exclusion relation

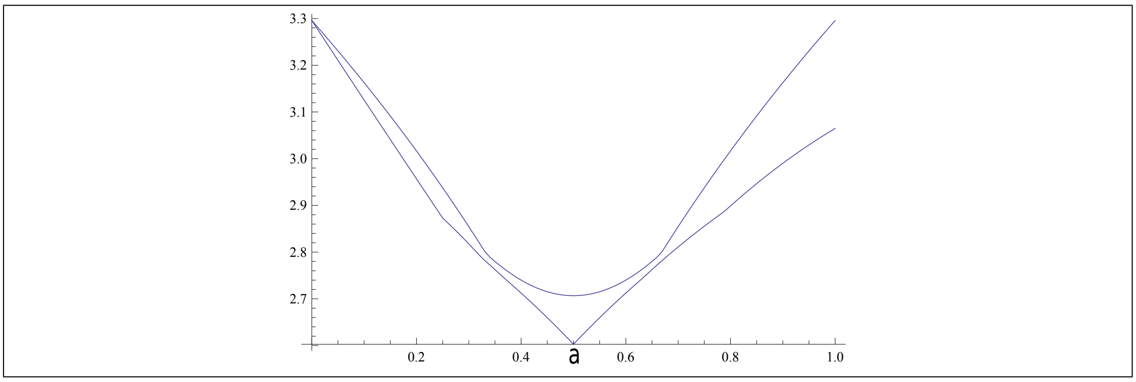

Figure 5.6: Comparison of our bound with that of Zhang et al. Our bound r_x in the bottom is tighter than the top curve of Zhang's bound $\widetilde{\mathfrak{U}}_1$.

bound [ZZY15] for multi-measurements (state-independent):

$$\sum_{m=1}^{N} I(M_m : B) \leqslant \min\left\{\widetilde{\mathfrak{U}}_1, \widetilde{\mathfrak{U}}_2, \widetilde{\mathfrak{U}}_3\right\} \tag{5.59}$$

with the bounds $\widetilde{\mathfrak{U}}_1$, $\widetilde{\mathfrak{U}}_2$ and $\widetilde{\mathfrak{U}}_3$ are defined as follows:

$$\begin{aligned}
\widetilde{\mathfrak{U}}_1 &= N\log_2 d + NH(B) - (N-1)H(A) \\
&\quad + \min_{(i_1\ldots i_N)\in\mathfrak{S}_N}\left\{\log\max_{i_N}\{\sum_{i_2\ldots i_{N-1}}\max_{i_1}\prod_{n=1}^{N-1} c(u^n_{i_n}, u^{n+1}_{i_{n+1}})\}\right\}, \\
\widetilde{\mathfrak{U}}_2 &= (N-1)\log_2 d + NH(B) - (N-1)H(A) \\
&\quad + \min_{(i_1\ldots i_N)\in\mathfrak{S}_N}\left\{\log\sum_{i_2\ldots i_N}\max_{i_1}\prod_{n=1}^{N-1} c(u^n_{i_n}, u^{n+1}_{i_{n+1}})\right\}, \\
\widetilde{\mathfrak{U}}_3 &= N\log_2 d + \frac{N}{2}(2H(B) - H(A)) \\
&\quad + \frac{1}{|I_2|}\sum_{(k,l)\in I_2}\left\{\min\{\log\max_{i_k} c(u^k_{i_k}, u^l_{i_l}), \log\max_{i_l} c(u^k_{i_k}, u^l_{i_l})\}\right\}.
\end{aligned}$$

Here the first two maxima are taken over all permutations $(i_1 i_2 \ldots i_N) : j \to i_j$, and the third is over all possible subsets $I_2 = \{(k_1, l_1), \ldots, (k_{|I_2|}, l_{|I_2|})\}$ such that $(k_1, l_1, \ldots, k_{|I_2|}, l_{|I_2|})$ is a $|I_2|$-permutation of $1, \ldots, N$. For example, (12), (23), …, $(N-1, N)$, $(N1)$ are 2-permutations of $1, \ldots, N$. Clearly, $\widetilde{\mathfrak{U}}_3$ is the average value of all potential two-measurement combinations.

Using the permutation symmetry, we have the following Theorem which improves the bound $\widetilde{\mathfrak{U}}_3$.

Theorem 5.2.4. *Let ρ_{AB} be the bipartite density matrix with measurements M_m ($m = 1, 2, \ldots, N$) on the system A with a quantum memory B as in Theorem 5.2.3, then*

$$\sum_{m=1}^{N} I(M_m : B) \leqslant N \log_2 d + \frac{N}{2}(2H(B) - H(A))$$
$$+ \frac{1}{|I_L|} \sum_{(k_1,k_2,\ldots,k_L)\in I_L} \left\{ \min_{(k_1,k_2,\ldots,k_L)} \{\log \max_{i_L} \sum_{k_2,\ldots,k_{L-1}} \max_{k_1} \prod_{n=1}^{L-1} c(u^n_{k_n}, u^{n+1}_{k_{n+1}})\} \right\} := r_{opt}, \tag{5.60}$$

where the minimum is over all L-permutations of $1, \ldots, N$ for $L = 2, \ldots, N$.

In the above we have explained that the bound $\widetilde{\mathfrak{U}}_3$ is obtained by taking the minimum over all possible 2-permutations of $1, 2, \ldots, N$, naturally our new bound r_{opt} in Theorem 5.2.4 is sharper than $\widetilde{\mathfrak{U}}_3$ as we have considered all possible multi-permutations of $1, 2, \ldots, N$.

Now we compare $\widetilde{\mathfrak{U}}_1$ with r_x. As an example in three-dimensional space, one chooses three measurements as follows [LMF15] :

$$u^1_1 = (1, 0, 0), u^1_2 = (0, 1, 0), u^1_3 = (0, 0, 1);$$

$$u^2_1 = (\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}), u^2_2 = (0, 1, 0), u^2_3 = (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}});$$

$$u^3_1 = (\sqrt{a}, e^{i\phi}\sqrt{1-a}, 0), u^3_2 = (\sqrt{1-a}, -e^{i\phi}\sqrt{a}, 0), u^3_3 = (0, 0, 1).$$

FIG. 5.6 shows the comparison when a changes and $\phi = \pi/2$, where it is clear that r_x is better than $\widetilde{\mathfrak{U}}_1$.

The relationship between r_{opt} and r_x is sketched in FIG. 5.7. In this case r_x is better than r_{opt} for three measurements of dimension three, therefore $\min\{r_{opt}, r_x\} = \min\{r_x\}$. Rigorous proof that r_x is always better than r_{opt} is nontrivial, since all the possible combinations of measurements less than N must be considered.

On the other hand, we can give a bound better than $\widetilde{\mathfrak{U}}_2$. Recall that the concavity has been utilized in the formation of $\widetilde{\mathfrak{U}}_2$, together with all possible combinations we will get following lemma (in order to simplify the process, we first consider three measurements, then generalize it to multiple measurements).

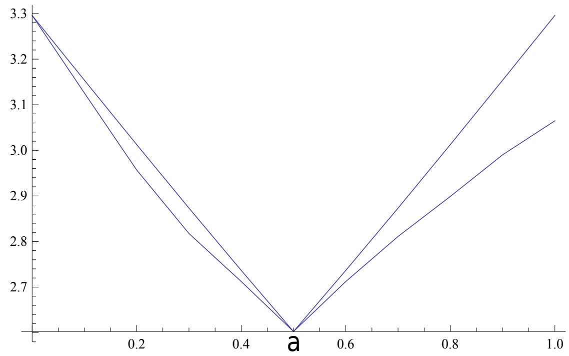

Figure 5.7: Comparison of our two bounds via combinatorial and majorization methods: the top curve is r_{opt} (combinatorial), while the lower curve is r_x (majorization).

Lemma 5.2.5. *For any bipartite state ρ_{AB}, let M_1, M_2, M_3 be three measurements on system A in the presence of quantum memory B, then*

$$\sum_{m=1}^{3} I(M_m : B) \leqslant -2H(A|B) + \sum_{cyclic\ perm} \log_2 \left[\sum_{i_3} \left(\sum_{i_2} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) c(u^2_{i_2}, u^3_{i_3}) \right)^{\frac{1}{3}} \right], \quad (5.61)$$

where the sum is over the three cyclic permutations of $1, 2, 3$.

Proof. First recall that for $\sum_{i_3} p^3_{i_3} \log_2[\sum_{i_2} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) c(u^2_{i_2}, u^3_{i_3})]$ we have

$$\begin{aligned}
&H(M_3) + \sum_{i_3} p^3_{i_3} \log_2[\sum_{i_2} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) c(u^2_{i_2}, u^3_{i_3})] \\
&= \sum_{i_3} p^3_{i_3} \log_2 \frac{1}{p^3_{i_3}} + \sum_{i_3} p^3_{i_3} \log_2[\sum_{i_2} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) c(u^2_{i_2}, u^3_{i_3})] \\
&\leqslant \log_2 \sum_{i_3} [\sum_{i_2} \max_{i_1} c(u^1_{i_1}, u^2_{i_2}) c(u^2_{i_2}, u^3_{i_3})],
\end{aligned}$$

where we have used concavity of log. By the same method we then get

$$
\begin{aligned}
\sum_{m=1}^{3} I(M_m:B) \leqslant & \sum_{m=1}^{3} H(M_m) + 3H(B) - 2H(A) + \frac{1}{3}\sum_{i_3} p^3_{i_3}\log_2[\sum_{i_2}\max_{i_1} c(1,2,3)] \\
& + \frac{1}{3}\sum_{i_2} p^2_{i_2}\log_2[\sum_{i_1}\max_{i_3} c(3,1,2)] + \frac{1}{3}\sum_{i_1} p^1_{i_1}\log_2[\sum_{i_3}\max_{i_2} c(2,3,1)] \\
& = \sum_{m=1}^{3} H(M_m) + 3H(B) - 2H(A) + \sum_{i_3} p^3_{i_3}\log_2[\sum_{i_2}\max_{i_1} c(1,2,3)]^{\frac{1}{3}} \\
& + \sum_{i_2} p^2_{i_2}\log_2[\sum_{i_1}\max_{i_3} c(3,1,2)]^{\frac{1}{3}} + \sum_{i_1} p^1_{i_1}\log_2[\sum_{i_3}\max_{i_2} c(2,3,1)]^{\frac{1}{3}} \\
& \leqslant 3H(B) - 2H(A) \\
& + \log_2\sum_{i_3}[\sum_{i_2}\max_{i_1} c(1,2,3)]^{\frac{1}{3}} + \log_2\sum_{i_2}[\sum_{i_1}\max_{i_3} c(3,1,2)]^{\frac{1}{3}} \\
& + \log_2\sum_{i_1}[\sum_{i_3}\max_{i_2} c(2,3,1)]^{\frac{1}{3}} \\
& = 3H(B) - 2H(A) \\
& + \log_2\left\{\left[\sum_{i_3}\left(\sum_{i_2}\max_{i_1} c(1,2,3)\right)^{\frac{1}{3}}\right]\left[\sum_{i_2}\left(\sum_{i_1}\max_{i_3} c(3,1,2)\right)^{\frac{1}{3}}\right]\right. \\
& \quad \cdot \left.\left[\sum_{i_1}\left(\sum_{i_3}\max_{i_2} c(2,3,1)\right)^{\frac{1}{3}}\right]\right\},
\end{aligned} \tag{5.62}
$$

with $c(1,2,3)$, $c(2,3,1)$ and $c(3,1,2)$ the same as in Eq. (5.61) and this completes the proof. ■

Observe that the right hand side of Eq. (5.61) adds the sum of three terms

$$
\begin{aligned}
& \frac{1}{3}\sum_{i_3} p^3_{i_3}\log_2[\sum_{i_2}\max_{i_1} c(1,2,3)], \\
& \frac{1}{3}\sum_{i_1} p^1_{i_1}\log_2[\sum_{i_3}\max_{i_2} c(2,3,1)], \\
& \frac{1}{3}\sum_{i_2} p^2_{i_2}\log_2[\sum_{i_1}\max_{i_3} c(3,1,2)].
\end{aligned} \tag{5.63}
$$

Naturally, we can also add

$$
\frac{1}{2}\sum_{i_3} p^3_{i_3}\log_2[\sum_{i_2}\max_{i_1} c(1,2,3)]
$$

and

$$\frac{1}{2}\sum_{i_1} p^1_{i_1} \log_2[\sum_{i_3} \max_{i_2} c(2,3,1)]$$

. By the same method, consider all possible combination and denote the minimal as r_{3y}. Similar for N-measurements, set the minimal bound under the concavity of logarithm function as r_{Ny}, moreover let $r_y = \min_m\{r_{my}\}$ $(1 \leqslant m \leqslant N)$, hence $r_y \leqslant \widetilde{\mathfrak{U}}_2$, finally we get

Theorem 5.2.6. *For any bipartite state ρ_{AB}, let M_m $(m = 1, 2, \ldots, N)$ be N measurements on system A, and let B be the quantum memory correlated to A, then*

$$\sum_{m=1}^{N} I(M_m : B) \leqslant \min\{r_x, r_y\} \tag{5.64}$$

with $\frac{1}{N}\omega\mathfrak{B}$ the same in Eq. (5.53). Since $\min\{r_x, r_y\} \leqslant \min\{\widetilde{\mathfrak{U}}_1, \widetilde{\mathfrak{U}}_2, \widetilde{\mathfrak{U}}_{opt}\}$ and all figures have shown our newly construct bound $\min\{r_x, r_y\}$ is tighter. Note that there is no clear relation between r_x and r_y, while the bound r_y cannot be obtained by simply subtracting the bound of entropic uncertainty relations in the presence of quantum memory. Moreover, if r_y outperforms r_x, then we can utilize r_y to achieve new bound for entropic uncertainty relations stronger than $-\frac{1}{N}\omega\mathfrak{B}$.

We have derived new bounds of the information exclusion relation for multi-measurements in the presence of quantum memory. The bounds are shown to be tighter than recently available bounds by detailed illustrations. Our bound is obtained by utilizing the concavity of the entropy function. The procedure has taken into account of all possible permutations of the measurements, thus offers a significant improvement than previous results which had only considered part of 2-permutations or combinations. Moreover, we have shown that majorization of the probability distributions for multi-measurements offers better bounds. In summary, we have formulated a systematic method of finding tighter bounds by combining the symmetry principle with majorization theory, all of which have been made easier in the context of mutual information. We remark that the new bounds can be easily computed by numerical computation.

5.3 Uncertainty Relation with Quantum Memory

Berta *et al*'s uncertainty principle in the presence of quantum memory [M. Berta *et al.*, Nat. Phys. **6**, 659 (2010)] [BCC+10] reveals uncertainties with quantum side information between the observers. In the recent important work of Coles and Piani [P. Coles and M. Piani, Phys. Rev. A. **89**, 022112 (2014)] [CP14], the entropic sum is controlled by the first and second maximum overlaps between the two projective measurements. We generalize the entropic uncertainty relation in the presence of quantum memory and find the exact dependence on all d largest overlaps between two measurements on any d-dimensional Hilbert space. Our bound is rigorously shown to be strictly tighter than previous entropic bounds in the presence of quantum memory, which have potential applications to quantum cryptography with entanglement witnesses and quantum key distributions.

In the context of both classical and quantum information sciences, it is more natural to use entropy to quantify uncertainties. The first entropic uncertainty relation for position and momentum was given in [BBM75] (which can be shown to be equivalent to Heisenberg's original relation). Later Deutsch [Deu83] found an entropic uncertainty relation for any pair of observables. An improvement of Deutsch's entropic uncertainty relation was subsequently conjectured by Kraus [Kra87] and later proved by Maassen and Uffink [MU88] (we use base 2 log throughout this paper),

$$H(R) + H(S) \geqslant \log \frac{1}{c_1}, \tag{5.65}$$

where $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ are two orthonormal bases on d-dimensional Hilbert space $\mathcal{H}_A$, and $H(R) = -\sum_j p_j \log p_j$ is the Shannon entropy of the probability distribution $\{p_j = \langle u_j|\rho_A|u_j\rangle\}$ for state ρ_A of $\mathcal{H}_A$ (similarly for $H(S)$ and $\{q_k = \langle v_k|\rho_A|v_k\rangle\}$). The number c_1 is the largest overlap among all $c_{jk} = |\langle u_j|v_k\rangle|^2$ ($\leqslant 1$) between the projective measurements R and S.

One of the important recent advances on uncertainty relations is to allow the measured quantum system to be correlated with its environment in a non-classical way, for instance, picking up quantum correlations such as entanglement in quantum cryptography. Berta *et al.* [BCC$^+$10] derived this landmark uncertainty relation for measurements R and S in the presence of quantum memory B:

$$H(R|B) + H(S|B) \geqslant \log \frac{1}{c_1} + H(A|B), \tag{5.66}$$

where $H(R|B) = H(\rho_{RB}) - H(\rho_B)$ is the conditional entropy with $\rho_{RB} = \sum_j (|u_j\rangle\langle u_j| \otimes I)(\rho_{AB})(|u_j\rangle\langle u_j| \otimes I)$ (similarly for $H(S|B)$), and d is the dimension of the subsystem A. The term $H(A|B) = H(\rho_{AB}) - H(\rho_B)$ appearing on the right-hand side is related to the entanglement between the measured particle A and the quantum memory B.

The bound of Berta *et al.* has recently been upgraded by Coles and Piani

[CP14], who have shown a remarkable bound in the presence of quantum memory

$$H(R|B) + H(S|B) \geqslant \log \frac{1}{c_1} + \frac{1-\sqrt{c_1}}{2} \log \frac{c_1}{c_2} + H(A|B), \tag{5.67}$$

where c_2 is the second largest overlap among all c_{jk} (counting multiplicity) and other notations are the same as in Eq.(5.39). As $1 \geqslant c_1 \geqslant c_2$, the second term in Eq.(5.67) shows that the uncertainties depend on more detailed information of the transition matrix or overlaps between the two bases. The Coles-Piani bound offers a strictly tighter bound than the bound of Berta *et al.* as long as $1 > c_1 > c_2$. The goal of this paper is to report a more general and tighter bound for the entropic uncertainty relation with quantum side information.

As reported in [RPŻ14], there are some examples where the bounds such as B_{Maj} and B_{RPZ} based on majorization approach outperform the degenerate form of Coles and Piani's new bound in the special case when quantum memory is absent. However, it is unknown if this approach can be extended to allow for quantum side information. Therefore Coles and Piani's remarkable bound Eq. (5.67) is still the strongest lower bound for the entropic sum in the presence of quantum memory. In this paper, we improve the bound by Coles and Piani in the most general situation with quantum memory. Moreover, our general bound is proven stronger by rigorous mathematical arguments.

To state our result, we first recall the majorization relation between two probability distributions $P = (p_1, \cdots, p_d)$, $Q = (q_1, \cdots, q_d)$. The partial order $P \prec Q$ means that $\sum_{j=1}^{i} p_j^{\downarrow} \leqslant \sum_{j=1}^{i} q_j^{\downarrow}$ for all $i = 1, \cdots, d$. Here $^{\downarrow}$ denotes rearranging the components of p or q in descending order. Any probability distribution vector P is bounded by $(\frac{1}{d}, \cdots, \frac{1}{d}) \prec P \prec (1, 0, \cdots, 0) = \{1\}$. For any two probability distributions $P = (p_j)$ and $Q = (q_k)$ corresponding to measurements R and S of the state ρ, there is a state-independent bound of direct-sum majorization [RPŻ14]: $P \oplus Q \prec \{1\} \oplus W$, where $P \oplus Q = (p_1 \cdots, p_d, q_1, \cdots, q_d)$ and $W = (s_1, s_2 - s_1, \cdots, s_d - s_{d-1})$ is a special probability distribution vector defined exclusively by the overlap matrix related to R and S. Let $U = (\langle u_j | v_k \rangle)_{jk}$ be the overlap matrix between the two bases given by R and S, and define the subset $\mathrm{Sub}(U, k)$ to be the collection of all size $r \times s$ submatrices M such that $r + s = k + 1$. Following [RPŻ14] we define $s_k = \max\{\|M\| : M \in \mathrm{Sub}(U, k)\}$, where $\|M\|$ is the maximal singular value of M. Denote the sum of the largest k terms in $\{1\} \oplus W$ as $\Omega_k = 1 + s_{k-1}$, while $s_0 = 0$, $s_1 = \sqrt{c_1}$ and $s_d = 1$. It is clear that

$$1 = \Omega_1 \leqslant \Omega_2 \leqslant \cdots \leqslant \Omega_{d+1} = \cdots = \Omega_{2d} = 2,$$

where we already noted that $\Omega_2 = 1 + \sqrt{c_1}$.

Our main result is the following entropic uncertainty relation that, much like Coles-Piani's bound, accounts for the possible use of a quantum side information due to the entanglement between the measured particle and quantum memory. For a bipartite quantum state ρ_{AB} on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, without confusion, we still use H to denote the von Neumann entropy, $H(\rho_{AB}) = -\mathrm{Tr}(\rho_{AB} \log \rho_{AB})$.

Theorem 5.3.1. *Let $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ be arbitrary orthonormal bases of the subsystem A of a bipartite state ρ_{AB}. Then we have that*

$$\begin{aligned} &H(R|B) + H(S|B) \\ \geqslant &\log \frac{1}{c_1} + \frac{1-\sqrt{c_1}}{2} \log \frac{c_1}{c_2} + \frac{2-\Omega_4}{2} \log \frac{c_2}{c_3} + \cdots + \frac{2-\Omega_{2(d-1)}}{2} \log \frac{c_{d-1}}{c_d} + H(A|B), \end{aligned} \tag{5.68}$$

where $H(R|B) = H(\rho_{RB}) - H(\rho_B)$ is the conditional entropy with $\rho_{RB} = \sum_j (|u_j\rangle\langle u_j| \otimes I)(\rho_{AB})(|u_j\rangle\langle u_j| \otimes I)$ (similarly for $H(S|B)$), and d is the dimension of the subsystem A. The term $H(A|B) = H(\rho_{AB}) - H(\rho_B)$ appearing on the right-hand side is related to the entanglement between the measured particle A and the quantum memory B. Also $\Omega_k = 1 + s_{k-1} \leqslant 2$ and c_i is the i-th largest overlap among c_{jk}: $c_1 \geqslant c_2 \geqslant c_3 \geqslant \cdots \geqslant c_{d^2}$.

We remark that due to $\Omega_{d+1} = \cdots \Omega_{2d} = 2$, the last (non-zero) term of formula (5.80) can be fine-tuned according to the parity of d. If $d = 2n$, it is $\frac{2-\Omega_d}{2} \log \frac{c_n}{c_{n+1}}$; if $d = 2n+1$, it is $\frac{2-\Omega_{d-1}}{2} \log \frac{c_n}{c_{n+1}}$.

Proof. For completeness we start from the derivation of the Coles-Piani inequality. Observe that the quantum channel $\rho \to \rho_{SB}$ is in fact $\rho_{SB} = \sum_k |v_k\rangle\langle v_k| \otimes \mathrm{Tr}_A((|v_k\rangle\langle v_k| \otimes I)\rho_{AB})$. As the relative entropy $D(\rho\|\sigma) = \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma)$ is monotonic under a quantum channel it follows that

$$\begin{aligned} &H(S|B) - H(A|B) \\ =&D(\rho_{AB}\| \sum_k (|v_k\rangle\langle v_k| \otimes I)|\rho_{AB}(|v_k\rangle\langle v_k| \otimes I)) \\ \geqslant&D(\rho_{RB}\| \sum_{j,k} c_{jk}|u_j\rangle\langle u_j| \otimes \mathrm{Tr}_A((|v_k\rangle\langle v_k| \otimes I)\rho_{AB})) \\ \geqslant&D(\rho_{RB}\| \sum_j \max_k c_{jk}|u_j\rangle\langle u_j| \otimes \rho_B) \\ =&-H(R|B) - \sum_j p_j \log \max_k c_{jk}, \end{aligned} \tag{5.69}$$

where the first equation is a basic identity of the quantum relative entropy (cf. [CYGG11, Col12]). So the state-dependent bound under a quantum memory follows:

$$H(R|B) + H(S|B) \geqslant H(A|B) - \sum_j p_j \log \max_k c_{jk}. \tag{5.70}$$

Interchanging R and S we also have

$$H(R|B) + H(S|B) \geqslant H(A|B) - \sum_k q_k \log \max_j c_{jk}. \tag{5.71}$$

We arrange the numbers $\max_k c_{jk}$, $j = 1, \cdots, d$, in descending order:

$$\max_k c_{j_1 k} \geqslant \max_k c_{j_2 k} \geqslant \cdots \geqslant \max_k c_{j_d k}, \tag{5.72}$$

where $j_1 j_2 \cdots j_d$ is a permutation of $12 \cdots d$. Clearly $c_1 = \max_k c_{j_1 k}$ and in general $c_i \geqslant \max_k c_{j_i k}$ for all i. Therefore

$$\begin{aligned}
&- \sum_{j=1}^{d} p_j \log \max_k c_{jk} = - \sum_{i=1}^{d} p_{j_i} \log \max_k c_{j_i k} \\
\geqslant &- p_{j_1} \log c_1 - p_{j_2} \log c_2 - \cdots - p_{j_d} \log c_d \\
= &- (1 - p_{j_2} - \cdots - p_{j_d}) \log c_1 - p_{j_2} \log c_2 - \cdots - p_{j_d} \log c_d \\
= &- \log c_1 + p_{j_2} \log \frac{c_1}{c_2} + \cdots + p_{j_d} \log \frac{c_1}{c_d}.
\end{aligned} \tag{5.73}$$

Similarly we also have

$$- \sum_k q_k \log \max_j c_{jk} \geqslant - \log c_1 + q_{k_2} \log \frac{c_1}{c_2} + \cdots + q_{k_d} \log \frac{c_1}{c_d}, \tag{5.74}$$

for some permutation $k_1 k_2 \cdots k_d$ of $12 \cdots d$. Taking the average of Eq. (5.70) and Eq. (5.71) and plugging in Eq. (5.73-5.74) we have that

$$H(R|B) + H(S|B) \geqslant H(A|B) + \log \frac{1}{c_1} + \frac{p_{j_2} + q_{k_2}}{2} \log \frac{c_1}{c_2} + \cdots + \frac{p_{j_d} + q_{k_d}}{2} \log \frac{c_1}{c_d}. \tag{5.75}$$

Using $p_{j_2} + q_{k_2} = \sum_{i=2}^{d} (p_{j_i} + q_{k_i}) - \sum_{i=3}^{d} (p_{j_i} + q_{k_i})$ we see that Eq. (5.75) can be written equivalently as

$$\begin{aligned}
H(R|B) + H(S|B) \geqslant & H(A|B) + \log \frac{1}{c_1} + \frac{1}{2} \sum_{i=2}^{d} (p_{j_i} + q_{k_i}) \log \frac{c_1}{c_2} + \frac{p_{j_3} + q_{k_3}}{2} \log \frac{c_2}{c_3} \\
& + \cdots + \frac{p_{j_d} + q_{k_d}}{2} \log \frac{c_2}{c_d}.
\end{aligned} \tag{5.76}$$

The above transformation from Eq.(5.75) to Eq.(5.76) adds all later coefficients of $\log\frac{c_1}{c_3},\cdots,\log\frac{c_1}{c_d}$ into that of $\log\frac{c_1}{c_2}$ and modify the argument of each log to $\log\frac{c_2}{c_3},\cdots,\log\frac{c_2}{c_d}$. Continuing in this way, we can write Eq.(5.76) equivalently as

$$\begin{aligned}&H(R|B)+H(S|B)\\=&H(A|B)-\log c_1+\frac{2-(p_{j_1}+q_{k_1})}{2}\log\frac{c_1}{c_2}+\frac{2-(p_{j_1}+q_{k_1}+p_{j_2}+q_{k_2})}{2}\log\frac{c_2}{c_3}\\&+\cdots+\frac{2-\sum_{i=1}^{d-1}(p_{j_i}+q_{k_i})}{2}\log\frac{c_{d-1}}{c_d}.\end{aligned}\tag{5.77}$$

Since $P\oplus Q\prec\{1\}\oplus W$, we have $p_{j_1}+q_{k_1}\leqslant\Omega_2,\cdots,p_{j_1}+q_{k_1}+\cdots+p_{j_{d-1}}+q_{k_{d-1}}\leqslant\Omega_{2(d-1)}$. Plugging these into Eq.(5.75) completes the proof. ■

We remark that the most possible condition which can force our new bound Eq.(5.68) degenerates to Eq.(5.66) is when two orthonormal bases are mutually unbiased.

As an example, consider the following 2×4 bipartite state,

$$\rho_{AB}=\frac{1}{1+7p}\begin{pmatrix}p&0&0&0&0&p&0&0\\0&p&0&0&0&0&p&0\\0&0&p&0&0&0&0&p\\0&0&0&p&0&0&0&0\\0&0&0&0&\frac{1+p}{2}&0&0&\frac{\sqrt{1-p^2}}{2}\\p&0&0&0&0&p&0&0\\0&p&0&0&0&0&p&0\\0&0&p&0&\frac{\sqrt{1-p^2}}{2}&0&0&\frac{1+p}{2}\end{pmatrix},\tag{5.78}$$

which is known to be entangled for $0<p<1$. We take system A as the quantum memory, consider the following two projective measurements: $\{|v_k\rangle\}$ are the standard orthonormal basis on $\mathcal{H}_B$ and $\{|u_j\rangle\}$ are given by

$$\begin{aligned}|u_1\rangle&=(\frac{12}{\sqrt{205}},\frac{6}{\sqrt{205}},\frac{4}{\sqrt{205}},\frac{3}{\sqrt{205}})^T,\\|u_2\rangle&=(-\frac{66}{29\sqrt{205}},\frac{172}{29\sqrt{205}},\frac{183}{29\sqrt{205}},-\frac{324}{29\sqrt{205}})^T,\\|u_3\rangle&=(-\frac{11}{29\sqrt{298}},\frac{309}{29\sqrt{298}},-\frac{195\sqrt{\frac{2}{149}}}{29},-\frac{27\sqrt{\frac{2}{149}}}{29})^T,\\|u_4\rangle&=(\frac{9}{\sqrt{298}},-\frac{9}{\sqrt{298}},-3\sqrt{\frac{2}{149}},-5\sqrt{\frac{2}{149}})^T.\end{aligned}$$

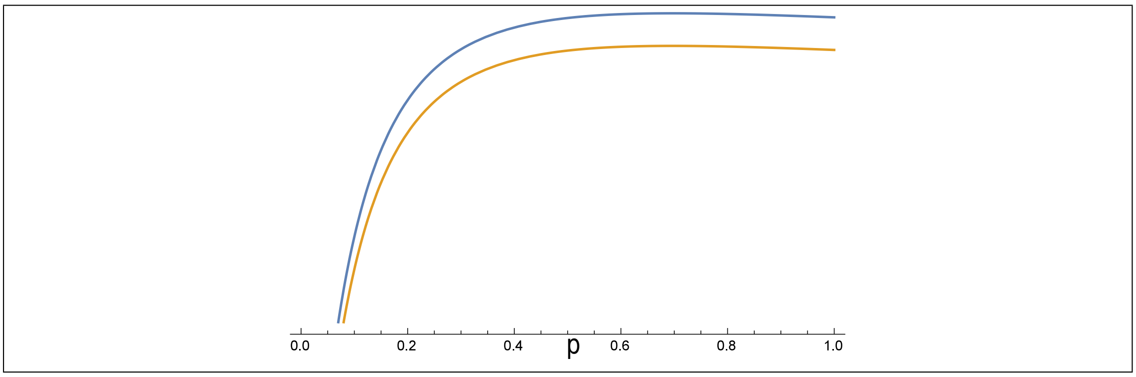

Figure 5.8: Comparison of bounds for entangled ρ_{AB}. The blue curve is the new bound Eq. (5.68) and the yellow curve is Coles-Piani's bound.

Then the overlap matrix $(|\langle u_j|v_k\rangle|^2)_{jk}$ has the form

$$\begin{pmatrix} \frac{144}{205} & \frac{36}{205} & \frac{16}{205} & \frac{9}{205} \\ \frac{4356}{172405} & \frac{29584}{172405} & \frac{33489}{172405} & \frac{104976}{172405} \\ \frac{121}{250618} & \frac{95481}{250618} & \frac{76050}{125309} & \frac{1458}{125309} \\ \frac{81}{298} & \frac{81}{298} & \frac{18}{149} & \frac{50}{149} \end{pmatrix}. \tag{5.79}$$

Thus $\Omega_4 \neq 2$ and $c_2 \neq c_3$. The comparison between Coles-Piani's bound and Eq. (5.68) in the presence of quantum memory is displayed in FIG. 5.8, which shows that our new bound is strictly tighter for all $p \in (0, 1)$.

After presenting the general result, we now turn to its special situation for a state-independent bound in the absence of quantum memory. As many state-independent bounds can not be extended to the general situation, a separate treatment is needed and one will see that our new bound fares reasonably well even at the absence of quantum memory.

Corollary 5.3.2. *Let $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ be any two orthonormal bases on d-dimensional Hilbert space $\mathcal{H}_A$. Then for any state ρ_A over $\mathcal{H}_A$, we have the following inequality,*

$$H(R) + H(S) \geqslant \log\frac{1}{c_1} + \frac{1-\sqrt{c_1}}{2}\log\frac{c_1}{c_2} + \frac{2-\Omega_4}{2}\log\frac{c_2}{c_3} + \frac{2-\Omega_6}{2}\log\frac{c_3}{c_4} + \cdots + \frac{2-\Omega_{2(d-1)}}{2}\log\frac{c_{d-1}}{c_d}, \tag{5.80}$$

Notations Ω_k and c_i are the same as in Eq.(5.68).

Proof. The corollary 5.3.2 can be similarly proved due to the following simple observation. When measurements are performed on system A, $H(R) + H(S) \geqslant -\sum_j p_j \log\sum_k q_k c_{jk} + H(A) \geqslant -\sum_j p_j \log\max_k c_{jk} + H(A)$. Then the corollary follows directly from the proof of the theorem 5.3.1. ∎

Noted that the overlaps, which are commonly used in entropic uncertainty relations, are noneffective measures so we can only consider them when the experimental device is trusted. For *device-independent uncertainty* based on effective and incompatible measures, see [KTW14]. There seems no clear relation between our bound and the bound based on effective anticommutators, and it is still open whether the approach of [KTW14] based on effective measures can be extended to allow the quantum side information. On the other hand, our result holds for the general case with the quantum side information.

We have found new lower bounds for the sum of the entropic uncertainties in the presence of quantum memory. Our new bounds have formulated the complete dependence on all d largest entries in the overlap matrix between two measurements on a d-dimensional Hilbert space, while the previously best-known bound depends on the first two largest entries. We have shown that the new bounds are strictly tighter than previously known entropic uncertainty bounds with quantum side information by mathematical argument in the general situation. In the special case without quantum memory, our bound also offer significant new information as it is complementary to some of the best known bounds in this situation.

5.4 Quantum Measurements and Quantum Memory

The uncertainty principle restricts potential information one gains about the physical properties of the measured particle. However, if the particle is prepared in entanglement with a quantum memory, the corresponding entropic uncertainty relation will vary. Based on the knowledge of correlations between the measured particle and quantum memory, we investigate the entropic uncertainty relations for two and multiple measurements, and generalize the lower bounds on the sum of Shannon entropies without quantum side information to those that allow quantum memory. In particular, we obtain generalization of Kaniewski-Tomamichel-Wehner's bound for effective measures and majorization bounds for noneffective measures to allow quantum side information. Furthermore, we derive several strong bounds for the entropic uncertainty relations in the presence of quantum memory for two and multiple measurements. Potential applications of our result to entanglement detection and entanglement witnesses are discussed via the entropic uncertainty relation even in the absence of quantum memory.

Heisenberg's uncertainty principle [Hei27] bounds the limit of measurement outcomes of two incompatible observables, thus reveals a fundamental difference between the classical and quantum mechanics. After intensive studies of the principle in terms of standard deviations of the measurements, entropies have stood out to be a natural and important alternative formulation of the uncertainty principle [CBTW15].

The first entropic uncertainty relation of observables with finite spectrum was given by Deutsch [Deu83] and then improved by Maassen and Uffink [MU88] who gave the celebrated MU bound: if two incompatible measurements $M_1 = \{|u^1_{i_1}\rangle\}$ and $M_2 = \{|u^2_{i_2}\rangle\}$ are chosen on the particle A, then the uncertainty is bounded by

$$H(M_1) + H(M_2) \geqslant \log_2 \frac{1}{c_1}, \tag{5.81}$$

where $H(M_i)$ is the *Shannon entropy* of the probability distribution induced by measurement M_i and $c_1 = \max_{i_1,i_2} \mid \langle u^1_{i_1}|u^2_{i_2}\rangle \mid^2$ denotes the largest overlap between observables. On the other hand, a mixed state is excepted to have more uncertainty, as Eq. (5.81) can be reinforced by adding a complementary term of the *von Neumann entropy* $H(A) = S(\rho_A)$:

$$H(M_1) + H(M_2) \geqslant \log_2 \frac{1}{c_1} + H(A). \tag{5.82}$$

The entropy $H(A)$ measures the amount of uncertainty induced by the mixing status of the state ρ_A: if the state is pure, then $H(A) = 0$, and if the state is a mixed state, then $H(A) > 0$. Therefore the corresponding bound Eq. (5.82) is stronger than Eq. (5.81) even though there is no auxiliary quantum system such as a quantum memory. We refer to $\log_2 \frac{1}{c_1}$ as the classical part B_{MU} and call $H(A)$ the mixing part of the bound for the entropic uncertainty relation since it measures the mixing status of the particle.

Most of the bounds for entropic uncertainty relations in the absence of quantum memory contain two parts: (i) the classical part B_C, for instance, Maassen and Uffink's bound [MU88], Coles and Piani's bound [CP14], or our recent bound [XJFLJ16]; (ii) the mixing part $H(A)$ describes information pertaining to the mixing status of the particle ρ_A. We note that both the Kaniewski-Tomamichel-Wehner bound [KTW14] based on effective anti-commutator and the direct-sum majorization bound [RPŻ14] only involve with the classical part and have no mixing parts. For more details, see Sec. 5.4.2. Obviously, not all bounds $B_C + H(A)$ (or B_C) can be generalized to the case with quantum memory by adding an extra term $H(A|B)$. It is an interesting problem to extend the entropic uncertainty relations in the absence of quantum memory to those with quantum memory.

In this section, we will solve the extension problem and answer three questions: (i) Can the uncertainty relation in the absence of quantum memory be generalized to the case with quantum side information? (ii) Are there other indices besides

$H(A|B)$ to quantify the amount of entanglement between the measured particle and quantum memory? (iii) Can two pairs of observables sharing the same overlaps between bases have different entropic uncertainty relations? Besides answering these questions in details we will give a couple of strong entropic uncertainty relations in the presence of quantum memory.

Generalized Entropic Uncertainty Relations

Strengthening the bound for the entropic uncertainty relation is an interesting problem arising from quantum theory. One of the main issues in this direction is how to extend the entropic uncertainty relation to allow for quantum side information. Several approaches have been devoted to seek for strong bounds for the entropic uncertainty relations (e.g. majorization-based uncertainty relations, direct-sum majorization relations, uncertainty relations based on effective anti-commutators and so on). However it is still not clear how to implement these methods to allow for quantum side information. In this section we will show that it is possible to generalize all entropic uncertainty relations to allow quantum side information by using the *Holevo inequality*.

Before analyzing our main techniques and results, let us first discuss the modern formulation of the uncertainty principle, the so-called *guessing game* (also known as the *uncertainty game*), which highlights its relevance with quantum cryptography. We can imagine there are two observers, Alice and Bob. Before the game initiates, they agree on two measurements M_1 and M_2. The guessing game proceeds as follows: Bob, can prepare an arbitrary state ρ_A which he will send to Alice. Alice then randomly chooses to perform one of measurements and records the outcome. After telling Bob the choices of her measurements, Bob can win the game if he correctly guesses Alice's outcome. Nevertheless, the uncertainty principle tells us that Bob cannot win the game under the condition of incompatible measurements.

What if Bob prepares a bipartite quantum state ρ_{AB} and sends only the particle A to Alice? Equivalently, what if Bob has nontrivial *quantum side information* about Alice's system? Or, what if all information Bob has on the particle ρ_A is beyond the classical description, for example, information on its density matrix? Berta *et al.* [BCC+10] answered these questions and generalized the uncertainty relation Eq. (5.82) to the case with an auxiliary quantum system B known as quantum memory.

It is now possible for Bob to experience no uncertainty at all when equipped himself with quantum memory, and Bob's uncertainty about the result of measurements on Alice's system is bounded by

$$H(M_1|B) + H(M_2|B) \geqslant \log_2 \frac{1}{c_1} + H(A|B), \tag{5.83}$$

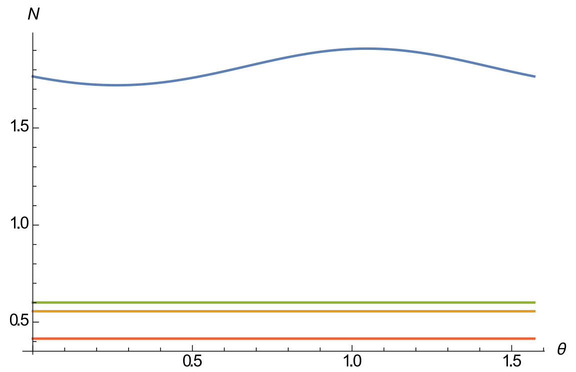

Figure 5.9: Comparison of bounds for entangled quantum state ψ. The blue curve is the entropic sum $H(M_1)+H(M_2)$, the green line is the entropic bound B_{ac}, the orange line is the entropic bound B_{maj} and the red line is Maassen and Uffink's bound B_{MU}.

where $H(M_1|B) = H(\rho_{M_1B}) - H(\rho_B)$ is the conditional entropy with $\rho_{M_1B} = \sum_j(|u_j\rangle\langle u_j| \otimes I)(\rho_{AB})(|u_j\rangle\langle u_j| \otimes I)$ (similarly for $H(M_2|B)$), and the term $H(A|B) = H(\rho_{AB}) - H(\rho_B)$ is related to the entanglement between the measured particle A and the quantum memory B.

Entropic uncertainty relation without quantum memory can be roughly divided into two categories. If the measure of incompatibility is effective, one can follow Kaniewski, Tomamichel and Wehner's approach to obtain bounds (e.g. B_{ac}) based on effective anticommutators. Otherwise one can derive strong bounds (e.g. B_{Maj1}, B_{Maj2}, B_{RPZ1}, B_{RPZ2}, B_{RPZ3}) based on majorization, or bounds (e.g. B_{CP}) constructed by the monotonicity of relative entropy under quantum channels. Note that Maassen and Uffink's bound B_{MU}, Coles and Piani's bound B_{CP} are still valid in the presence of quantum memory by adding an extra term $H(A|B)$. All these bounds can be generalized to allow for quantum side information.

Suppose we are given a quantum state ρ_{AB} and a pair of observables, M_m ($m = 1, 2$). Define the *classical correlation* of state ρ_{AB} with respect to the measurement M_m by

$$H(\rho_B) - S_m \tag{5.84}$$

with

$$S_m = \sum_{i_m} p^m_{i_m} H(\rho_{B_{i_m}})$$

where $\rho^m_{B_{i_m}} = Tr_A(|u^m_{i_m}\rangle\langle u^m_{i_m}|\rho_{AB})/p^m_{i_m}$ and $(p^m_{i_m})_{i_m}$ is the probability vector according to the measurement M_m.

It follows from definition and *Holevo's inequality* that the entropic uncertainty

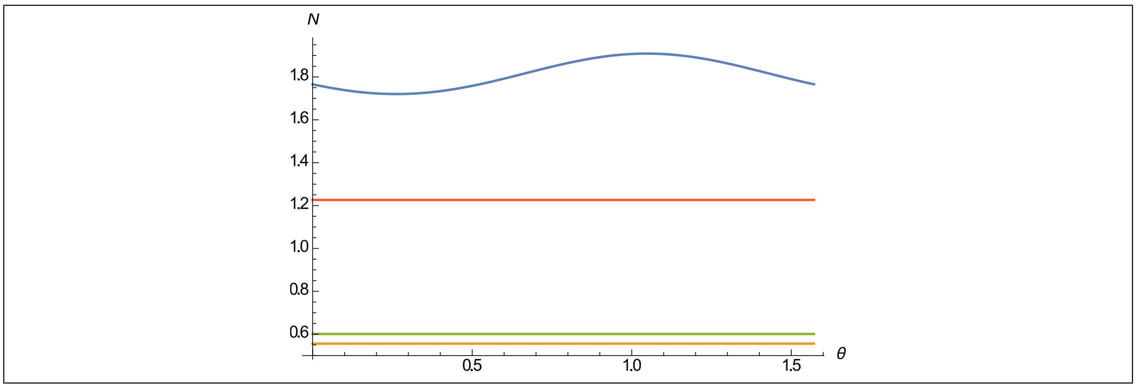

Figure 5.10: Comparison of bounds for entangled quantum state ψ. The blue curve is the entropic sum $H(M_1) + H(M_2)$, the green line is the entropic bound B_{ac}, the orange line is the entropic bound B_{maj} and the red line is Maassen and Uffink's bound $B_{MU} + H(A)$.

relation in the presence of quantum memory can be written as

$$H(M_1|B) + H(M_2|B) = H(M_1) + H(M_2) - 2H(\rho_B) + S_1 + S_2, \tag{5.85}$$

where $H(M_1), H(M_2)$ are the Shannon entropies of the state ρ_A. Suppose B_C is a lower bound of the entropic sum $H(M_1) + H(M_2)$, then

$$H(M_1|B) + H(M_2|B) \geqslant B_C - 2H(B) + S_1 + S_2. \tag{5.86}$$

We analyze the lower bound according to various types of B_C as follows.

(i) Bounds [MU88, CP14, RPŻ14] that contain a nonnegative state-dependent term $H(A) = S(\rho_A)$, the *von Neumann* entropy (*mixing part*):

$$\begin{aligned} &H(M_1) + H(M_2) \geqslant B_{MU} + H(A); \\ &H(M_1) + H(M_2) \geqslant B_{CP} + H(A); \\ &H(M_1) + H(M_2) \geqslant B_{RPZm} + H(A). \ (m = 1, 2, 3) \end{aligned} \tag{5.87}$$

(ii) Bounds [KTW14, RPŻ14, FGG13, PRŻ13] without the mixing term $H(A)$:

$$\begin{aligned} &H(M_1) + H(M_2) \geqslant B_{ac}, \\ &H(M_1) + H(M_2) \geqslant B_{Majm}. \ (m = 1, 2) \end{aligned} \tag{5.88}$$

Although both effective anticommutators and majorization approach play an important role in improving the bound for entropic uncertainty relations, even the strengthened Maassen and Uffink's bound $B_{MU} + H(A)$ can be tighter than the

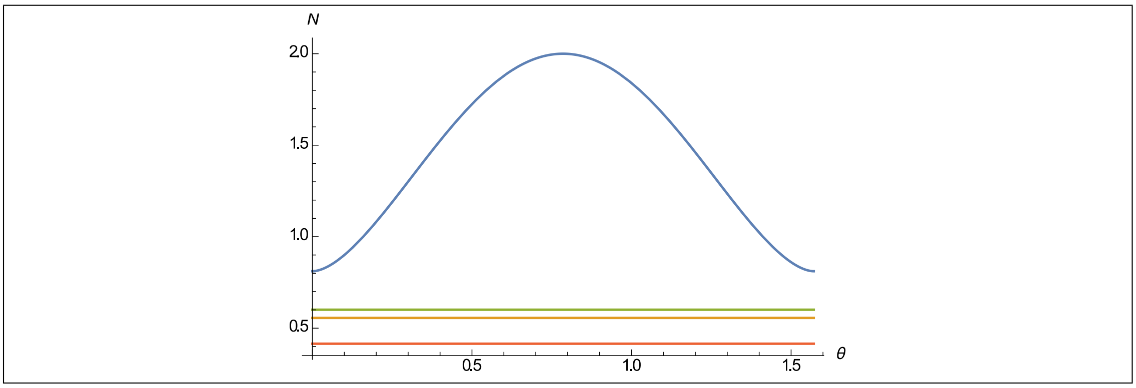

Figure 5.11: Comparison of bounds for entangled quantum state ψ. The blue curve is the entropic sum $H(M_1) + H(M_2)$, the green line is the entropic bound B_{ac}, the orange line is the entropic bound B_{maj} and the red line is Maassen and Uffink's bound B_{MU}.

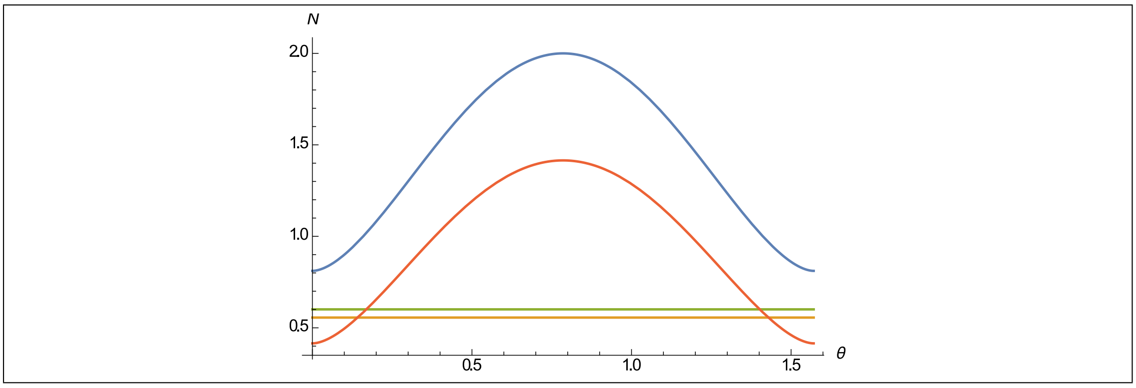

Figure 5.12: Comparison of bounds for entangled quantum state ψ. The blue curve is the entropic sum $H(M_1) + H(M_2)$, the green line is the entropic bound B_{ac}, the orange line is the entropic bound B_{maj} and the red line is Maassen and Uffink's bound $B_{MU} + H(A)$.

majorization bound B_{Maj1} and Kaniewski-Tomamichel-Wehner's bound B_{ac} if the mixing part is absent. To see this, we consider a family of quantum states

$$\rho_A = \frac{1}{2}\begin{pmatrix} \cos^2\theta + \frac{1}{2} & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta + \frac{1}{2} \end{pmatrix}, \tag{5.89}$$

where $0 \leqslant \theta \leqslant \pi/2$ with the measurements $M_1 = \{(1,0),(0,1)\}$ and $M_2 = \{(1/2, -\sqrt{3}/2), (\sqrt{3}/2, 1/2)\}$. The relations among $H(M_1) + H(M_2)$, B_{Maj}, B_{ac} and B_{MU} are shown in FIG. 5.9. The maximum overlap is $c_1 = 3/4$, and it is known [KTW14] that the bound B_{ac} outperforms B_{Maj}. The relations among $H(M_1) + H(M_2)$, B_{Maj}, B_{ac} and $B_{MU} + H(A)$ are shown in FIG. 5.10. Clearly the quantity $B_{MU} + H(A)$ is tighter than the bounds B_{Maj} or B_{ac}.

In the above discussion the value $H(A)$ is a constant, so all the bounds appeared in both FIG. 5.9 and FIG. 5.10 are lines. Now let's turn the quantum states given by

$$\rho_A = \frac{1}{2}\begin{pmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{pmatrix}, \tag{5.90}$$

where $0 \leqslant \theta \leqslant \pi/2$ with the same measurements as above. The relations among $H(M_1) + H(M_2)$, B_{Maj}, B_{ac} and B_{MU} are depicted in FIG. 5.11, again the strengthened Maassen-Uffink's bound $B_{MU} + H(A)$ outperforms B_{Maj} and B_{ac}. In FIG. 5.12 we compare them again in the neighborhood of $\theta = \pi/4$ where the bound $B_{MU} + H(A)$ gives the best estimate.

Quantum Indices

The existence of quantum memory translates into additional information on the uncertainty relation. We introduce the notion of *quantum index* to describe the relationship between measured particle and quantum memory. There are two types of quantum indices.

The first quantum index on entropic uncertainty relations is the mutual information between measured particle A and quantum memory B, which comes from the conditional von Neumann entropy [BCC+10]

$$H(A|B) = H(A) - I(A:B). \tag{5.91}$$

Let $Q_1 = -I(A:B)$ be the *first quantum index*, as $H(A)$ counts for the mixing level for measured particle A. Then the bounds for the entropic uncertainty relation in the presence of quantum memory consist of three parts: the bound B_C for the sum of Shannon entropies, the *mixing part* $H(A)$ and the first quantum index Q_1

$$\begin{aligned} H(M_1|B) + H(M_2|B) &\geqslant B_{MU} + H(A) + Q_1, \\ H(M_1|B) + H(M_2|B) &\geqslant B_{CP} + H(A) + Q_1, \end{aligned} \tag{5.92}$$

where $B_{MU} = -\log c_1$, $B_{CP} = -\log c_1 + \frac{1-\sqrt{c_1}}{2}\log\frac{c_1}{c_2}$ with c_2 is the second largest entry of the matrix $(|\langle u^1_{i_1}|u^2_{i_2}\rangle|^2)_{i_1 i_2}$.

A more natural and less restrictive *quantum index* is $-2H(B)+S_1+S_2$ discussed in Sec. 5.4.1. Let $Q_2 := -2H(B) + S_1 + S_2$ be the *second quantum index*, then we can generalize all bounds for the entropic uncertainty relation to allow for quantum side information. Namely we have

$$\begin{aligned} H(M_1|B) + H(M_2|B) &\geqslant B_{MU} + H(A) + Q_2, \\ H(M_1|B) + H(M_2|B) &\geqslant B_{CP} + H(A) + Q_2, \end{aligned} \tag{5.93}$$

Table 5.1: Bounds for entropic uncertainty relations without quantum memory

Entropic uncertainty relations without quantum memory
$H(M_1) + H(M_2) \geqslant B_{MU} + H(A)$
$H(M_1) + H(M_2) \geqslant B_{CP} + H(A)$
$H(M_1) + H(M_2) \geqslant B + H(A)$
$H(M_1) + H(M_2) \geqslant B_{ac}$
$H(M_1) + H(M_2) \geqslant B_{Maj1}$
$H(M_1) + H(M_2) \geqslant B_{Maj2}$
$H(M_1) + H(M_2) \geqslant B_{RPZ1} + H(A)$
$H(M_1) + H(M_2) \geqslant B_{RPZ2} + H(A)$
$H(M_1) + H(M_2) \geqslant B_{RPZ3} + H(A)$

Table 5.2: Bounds for entropic uncertainty relations with quantum memory

Entropic uncertainty relations under quantum memory
$H(M_1\|B) + H(M_2\|B) \geqslant B_{MU} + H(A) + Q_1$ (or Q_2)
$H(M_1\|B) + H(M_2\|B) \geqslant B_{CP} + H(A) + Q_1$ (or Q_2)
$H(M_1\|B) + H(M_2\|B) \geqslant B + H(A) + Q_1$ (or Q_2)
$H(M_1\|B) + H(M_2\|B) \geqslant B_{ac} + Q_2$
$H(M_1\|B) + H(M_2\|B) \geqslant B_{Maj1} + Q_2$
$H(M_1\|B) + H(M_2\|B) \geqslant B_{Maj2} + Q_2$
$H(M_1\|B) + H(M_2\|B) \geqslant B_{RPZ1} + H(A) + Q_2$
$H(M_1\|B) + H(M_2\|B) \geqslant B_{RPZ2} + H(A) + Q_2$
$H(M_1\|B) + H(M_2\|B) \geqslant B_{RPZ3} + H(A) + Q_2$

Clearly, both Maassen and Uffink's bound B_{MU} and Coles and Piani's bound B_{CP} are valid with or without quantum side information, with the mixing part $H(A)$ in the former case or the conditional entropy $H(A|B)$ in the latter. Mathematically, the relation says that

$$\begin{aligned} H(M_1) + H(M_2) &\geqslant B_{CC} + H(A), \\ H(M_1|B) + H(M_2|B) &\geqslant B_{CC} + H(A|B), \end{aligned} \tag{5.94}$$

where $B_{CC} = B_{MU}$ or B_{CP}. The term B_{CC} will be referred as the *consistent classical part* of the bound for the entropic uncertainty relation. In place of B_{MU} and B_{CP} in (5.94), we have recently given a new consistent classical part B, which is a tighter bound depending on all overlaps between incompatible observables

[XJFLJ16]:

$$B := \log_2 \frac{1}{c_1} + \frac{1-\sqrt{c_1}}{2} \log_2 \frac{c_1}{c_2} + \frac{2-\Omega_4}{2} \log_2 \frac{c_2}{c_3} + + \cdots + \frac{2-\Omega_{2(d-1)}}{2} \log_2 \frac{c_{d-1}}{c_d}, \tag{5.95}$$

where c_i is the i-th largest overlap among c_{jk}: $c_1 \geqslant c_2 \geqslant c_3 \geqslant \cdots \geqslant c_{d^2}$, and Ω_k is the k-th element of majorization bound for measurements M_1 and M_2 [XJFLJ16]. In general the bound B is always tighter than B_{MU}, except possibly when two orthonormal bases are mutually unbiased.

We continue discussing the quantum index of the entropic uncertainty relation with a consistent classical part. When quantum memory is present, there are infinitely many quantum indices. For any $\lambda \in [0, 1]$ one has that

$$H(M_1|B) + H(M_2|B) \geqslant B_{CC} + H(A) + Q(\lambda), \tag{5.96}$$

where

$$Q(\lambda) := -\lambda I(A : B) + (1-\lambda)(-2H(B) + S_1 + S_2) \tag{5.97}$$

is the quantum index for the entropic uncertainty relation. Here we have used a weighted sum of quantum indices similar to [XJLJF16b]. Note that the weight is performed on the quantum indices instead of the uncertainty relations. By this simple process, we can always get a better lower bound without worrying which quantum index is tighter than the other.

The quantum index Q_2 has two desirable features. First, with the help of the *second quantum index* we can extend all previous bounds of the entropic sum (Shannon entropy) to allow for the quantum side information without restrictive constraints. The comparison of some of the existing results is given together with their extensions in the presence of quantum side information in TABLE. 5.1 and TABLE. 5.2. Second, Q_2 can sometimes outperform Q_1 to give tighter bounds for the entropic uncertainty relation in the presence of quantum memory. For more details, see Sec. 5.4.3.

Moreover, by taking the maximum over $Q_2 - Q_1$ and zero, we derive that

$$\max\{0, Q_2 - Q_1\} = \delta, \tag{5.98}$$

where δ is the main quantity used in the recent paper [ASH16] for a strong uncertainty relation in the presence of quantum memory. Our result is more general by using $\max\{0, Q_2 - Q_1\}$. In fact $B + H(A) + \max\{Q_1, Q_2\}$ is tighter than the outcomes from [ASH16]. In [XJFLJ16] we have given a detailed and rigourous proof on the lower bound.

Influence of Incompatible Observables

Let us consider two pairs of incompatible observables M_1, M_2 and M_3, M_4 with the same overlaps c_{jk}. Then the bounds for the Shannon entropic sum $H(M_1) + H(M_2)$ on measured particle A will coincide with that of $H(M_3) + H(M_4)$, since their bounds only depend on the overlaps c_{jk}. If there is quantum memory B present, the same relation holds for the bounds with the first quantum index Q_1, since their bounds also only depend on c_{jk} and $H(A|B)$. However, the situation is quite different by utilizing the *second quantum index*. Even when two pairs of incompatible observables M_1, M_2 and M_3, M_4 share the same overlaps, the corresponding bounds may differ. This interesting phenomenon may be useful in physical experiments: the total uncertainty can be decreased by choosing suitable incompatible observables.

As an example, consider the following 2×4 bipartite state,

$$\rho_{AB} = \frac{1}{1+7p}\begin{pmatrix} p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & 0 & 0 & 0 & p \\ 0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+p}{2} & 0 & 0 & \frac{\sqrt{1-p^2}}{2} \\ p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & \frac{\sqrt{1-p^2}}{2} & 0 & 0 & \frac{1+p}{2} \end{pmatrix}, \tag{5.99}$$

which is known to be entangled for $0 < p < 1$. We take system A as the quantum memory and measurements are performed on system B. Choose the incompatible observables $M_1 = \{|u_i^1\rangle\}$ and $M_2 = \{|u_i^2\rangle\}$ as the first pair of measurements

$$\begin{aligned} |u_1^1\rangle &= (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0, 0)^\dagger, |u_2^1\rangle = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0)^\dagger, \\ |u_3^1\rangle &= (0, 0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})^\dagger, |u_4^1\rangle = (0, 0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})^\dagger; \\ |u_1^2\rangle &= \frac{1}{\sqrt{6}}(\sqrt{2}, \sqrt{2}, \sqrt{2}, 0)^\dagger, |u_2^2\rangle = \frac{1}{\sqrt{6}}(\sqrt{3}, 0, -\sqrt{3}, 0)^\dagger, \\ |u_3^2\rangle &= \frac{1}{\sqrt{6}}(1, -2, 1, 0)^\dagger, |u_4^2\rangle = (0, 0, 0, 1)^\dagger, \end{aligned} \tag{5.100}$$

then take $M_3 = M_2$ and $M_4 = \{|u_i^3\rangle\}$ such that

$$\begin{aligned} |u_j^1\rangle &\neq |u_j^3\rangle, \\ |\ \langle u_j^2|u_k^3\rangle\ |^2 &= |\ \langle u_j^1|u_k^2\rangle\ |^2\ . \end{aligned} \tag{5.101}$$

Let

$$\mathcal{B}_c = \log_2 \frac{1}{c_1} + \frac{1-\sqrt{c_1}}{2} \log_2 \frac{c_1}{c_2} + \frac{2-\Omega_4}{2} \log_2 \frac{c_2}{c_3} + + \cdots + \frac{2-\Omega_{2(d-1)}}{2} \log_2 \frac{c_{d-1}}{c_d}, \tag{5.102}$$

where $c_1 \geqslant c_2 \geqslant \cdots \geqslant c_d$ are the largest terms among the overlaps $c_{jk} = |\langle u_j^1 | u_k^2 \rangle|^2$, and Ω_i are given below Eq. (5.95). Set $\mathcal{B}_1 = H(B)$, $\mathcal{B}_2 = H(B|A)$, $\mathcal{B}_3 = H(B) - 2H(A) + S_1 + S_2$ and $\mathcal{B}_4 = H(B) - 2H(A) + S_2 + S_3$. If there is no quantum memory, we have that

$$\begin{aligned} H(M_1) + H(M_2) &\geqslant \mathcal{B}_c + \mathcal{B}_1, \\ H(M_3) + H(M_4) &\geqslant \mathcal{B}_c + \mathcal{B}_1, \end{aligned} \tag{5.103}$$

where the bounds are the same due to identical overlaps between the bases. In the presence of quantum memory, using the *first quantum index* $H(B|A)$ as the extra term to describe the amount of correlations between measured particle and quantum memory, we have that

$$\begin{aligned} H(M_1|A) + H(M_2|A) &\geqslant \mathcal{B}_c + \mathcal{B}_2, \\ H(M_3|A) + H(M_4|A) &\geqslant \mathcal{B}_c + \mathcal{B}_2, \end{aligned} \tag{5.104}$$

so their bounds coincide again. Finally, choose the *second quantum index* for the correlations between measured particle and quantum memory, we derive that

$$\begin{aligned} H(M_1|A) + H(M_2|A) &\geqslant \mathcal{B}_c + \mathcal{B}_3, \\ H(M_3|A) + H(M_4|A) &\geqslant \mathcal{B}_c + \mathcal{B}_4, \end{aligned} \tag{5.105}$$

and this time their bounds are different from each other. Therefore when the measured particle and quantum memory are entangled, the uncertainty is decreased through suitable incompatible observables. Since all the bounds contain $\mathcal{B}_c$, we only need to compare $\mathcal{B}_1 = H(B)$, $\mathcal{B}_2 = H(B|A)$, $\mathcal{B}_3 = H(B) - 2H(A) + S_1 + S_2$ and $\mathcal{B}_4 = H(B) - 2H(A) + S_2 + S_3$ for two pairs of measurements.

In FIG. 5.13, the comparison is done for $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ and $\mathcal{B}_4$, which shows how the *second quantum index* works for selected pairs of incompatible observables. The bound $\mathcal{B}_3$ (with the *second quantum index*) provides the best estimation for the entropic sum in the presence of quantum memory, while the bound $\mathcal{B}_2$ (with the *first quantum index*) gives a weaker approximation. The *second quantum index* does not always outperform the *first quantum index*, since $\mathcal{B}_4$ is typically worse than $\mathcal{B}_2$. However, comparing the bound $\mathcal{B}_3$ with $\mathcal{B}_4$, we find that the uncertainty from measurements can be weaken by selecting appropriate measurements even if each pair of incompatible observables share the same overlaps.

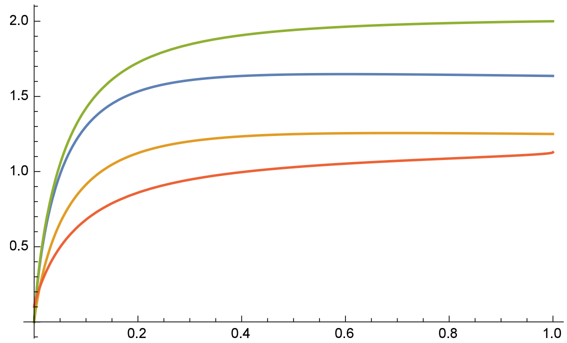

Figure 5.13: Comparison of bounds for entangled quantum state ρ_{AB}. The green curve is the entropic bound $\mathcal{B}_1$, the blue curve is the entropic bound $\mathcal{B}_3$, the orange curve is the entropic bound $\mathcal{B}_2$ and the red curve is the entropic bound $\mathcal{B}_4$.

To illustrate improvement of the bound in the presence of quantum memory, we compare the bound based on the *second quantum index* with that depended on the *first quantum index*. As a first step, choosing the initial state to be *Werner State* $\rho_{AB} = \frac{1}{4}(1-p)I + p|\mathfrak{B}_1\rangle\langle\mathfrak{B}_1|$ with $0 < p < 1$, and $|\mathfrak{B}_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ the *Bell State*. Take $|u_1^1\rangle = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$, $|u_2^1\rangle = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$; $|u_1^2\rangle = (\cos\theta, -\sin\theta)$, $|u_2^2\rangle = (\sin\theta, \cos\theta)$ with $0 < \theta < 2\pi$, then the difference between the bound with *second quantum index* and the bound with the *first quantum index* is illustrated in FIG. 5.14. The nonnegativity of the surface shows that our newly construct bound with the *second quantum index* can outperform bound with the *first quantum index* everywhere in this case.

Using quantum indices we have shown that it is possible to reduce the total uncertainties coming from incompatibility of the observables by appropriate choice. However, when the measured particle and quantum memory are maximally entangled, both the first and the second *quantum index* equal to $-\log_2 d$. We sketch a proof as

Proof. Let ρ_{AB} be a bipartite quantum state, and M_1, M_2 a pair of incompatible observables. Suppose that the measured particle A and quantum memory B are maximally entangled. We will show that both the first and second quantum indices coincide with each other. Recall that the first quantum index Q_1 was defined in Sec. 5.4.2 and the combination of the quantum index and mixing part is $H(A) + Q_1 = H(A|B) = -\log_2 d$.

Recall that the second quantum index is given by $Q_2 = -2H(B) + S_1 + S_2$,

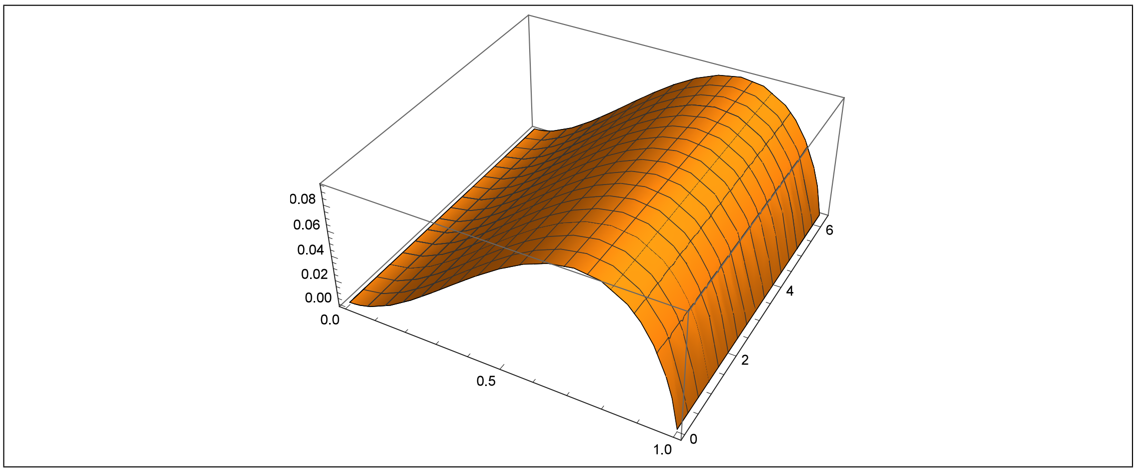

Figure 5.14: The difference between the bound of entropic uncertainty relations in the presence of quantum memory with *second quantum index* and the bound of entropic uncertainty relations in the presence of quantum memory with the *first quantum index* $H(A|B)$.

where

$$S_1 = \sum_{i_1} p^1_{i_1} H(\rho^1_{B_{i_1}}), \tag{5.106}$$

$$S_2 = \sum_{i_2} p^2_{i_2} H(\rho^1_{B_{i_2}}). \tag{5.107}$$

From $p^m_{i_m} = \langle u^m_{i_m}|\rho_A|u^m_{i_m}\rangle$ and $[u^m_{i_m}] \equiv |u^m_{i_m}\rangle\langle u^m_{i_m}|$ $(m = 1, 2)$, it follows that

$$\rho^1_{B_{i_1}} = \frac{Tr_A([u^1_{i_1}]\rho_{AB})}{p^1_{i_1}}, \tag{5.108}$$

$$\rho^2_{B_{i_2}} = \frac{Tr_A([u^2_{i_2}]\rho_{AB})}{p^2_{i_2}}. \tag{5.109}$$

One can use the formula to compute the second quantum index Q_2 if the state is the maximally entangled quantum state $\rho_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$. For simplicity, we only consider the case $d = 3$ while the high dimensional case can be similarly done. For the projective rank-1 measurements on system A, set $|u^1_{i_1}\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$, then

$$[u^1_{i_1}] = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* & \alpha\gamma^* \\ \beta\alpha^* & |\beta|^2 & \beta\gamma^* \\ \gamma\alpha^* & \gamma\beta^* & |\gamma|^2 \end{pmatrix}, \tag{5.110}$$

and

$$\rho_{B_{i_1}}^1 = \begin{pmatrix} |\alpha|^2 & \beta\alpha^* & \gamma\alpha^* \\ \alpha\beta^* & |\beta|^2 & \gamma\beta^* \\ \alpha\gamma^* & \beta\gamma^* & |\gamma|^2 \end{pmatrix}. \tag{5.111}$$

Since the density matrix $\rho_{B_{i_1}}^1$ is rank 1, it follows that

$$H(\rho_{B_{i_1}}^1) = 0, \tag{5.112}$$

which implies that $S_1 = S_2 = 0$. Therefore

$$H(A) + Q_1 = H(A) + Q_2 = -\log_2 d,$$

where the last equality implies that the first quantum index coincide with the second index when the measured particle and quantum memory are maximally entangled. ■

Strong Entropic Uncertainty Relations with quantum memory

In this subsection, we derive several strong entropic uncertainty relations in the presence of quantum memory by utilizing both the relevant bounds for the sum of Shannon entropies and optimal selection of quantum indices. Recall that the bounds of entropic uncertainty relations in the presence of quantum memory contain three ingredients: the classical part B_C, the mixing part $H(A)$ (which is not necessarily existent, e.g., the Maj bounds [RPŻ14, FGG13, PRŻ13] and B_{ac} [KTW14]), and the quantum indices Q_i $(i = 1, 2)$.

Let ρ_{AB} be a bipartite quantum state, and M_i $(i = 1, 2)$ two nondegenerate incompatible observables on the system A. We take system B as the quantum memory. A simple lower bound for the entropic sum in the presence of quantum memory can be obtained as follows. Note that the *consistent classical part* B_{CC} is valid with both quantum indices Q_i, therefore for $i = 1, 2$

$$H(M_1|B) + H(M_2|B) \geqslant B_{CC} + H(A) + Q_i.$$

As the bound B in Eq. (5.95) is the tightest, so the strongest lower bound for the entropic sum in the presence of quantum memory with *consistent classical part* is given by

$$\mathfrak{B}_{CC} := B + H(A) + \max\{Q_1, Q_2\}. \tag{5.113}$$

Without the help of the consistent classical part, all other classical part B_C can be estimated in the same way.

$$H(M_1|B) + H(M_2|B) \geqslant \mathcal{B}_C + H(A) + Q_2. \tag{5.114}$$

Note that for $B_C = B_{ac}$ or B_{Maj}, there is no mixing part $H(A)$ on the right-hand side of Eq. (5.114). Taking maximum over all possible B_C's we obtain a lower bound

$$\begin{aligned}\mathfrak{B}_C := \max\{&B_{ac}, B_{Maj1}, B_{Maj2}, B_{RPZ1} + H(A),\\ &B_{RPZ2} + H(A), B_{RPZ3} + H(A)\} + Q_2,\end{aligned} \tag{5.115}$$

Clearly both the lower bounds $\mathfrak{B}_C$ and $\mathfrak{B}_{CC}$ can be combined into a hybrid bound for the uncertainty relation in the presence of quantum memory:

$$H(M_1|B) + H(M_2|B) \geqslant \max\{\mathfrak{B}_C, \mathfrak{B}_{CC}\}, \tag{5.116}$$

where $\mathfrak{B}_C$ and $\mathfrak{B}_{CC}$ are given by (5.113) and (5.114) respectively.

We now extend our results to the general case of L-partite particles ($L \geqslant 3$) with N incompatible observables ($N \geqslant 3$). Assume the measured system is the l_1-partite subsystem and the quantum memory is the remaining l_2-partite subsystem, where $l_2 = L - l_1$ and $l_1 \geqslant 2$.

Suppose that the N measurements M_1, M_2, ..., M_N are given by the bases $M_m = \{|u^m_{i_m}\rangle\}$. Let system A be the measured particle (l_1-partite) and B the quantum memory (l_2-partite). The probability distributions

$$p^m_{i_m} = \langle u^m_{i_m}|\rho_A|u^m_{i_m}\rangle,$$

have a majorization bound [Par12]:

$$(p^m_{i_m}) \prec \omega = \sup_{M_m}(p^m_{i_m}), \tag{5.117}$$

which is state-independent. For different correlations between particles, there may exist different kind of state-independent ω called *uniform entanglement frames* [XJLJF16a]. In fact, if the majorization bound is written as $\omega = (\Omega_1, \Omega_2 - \Omega_1, \cdots, 1 - \Omega_{d-1})$, then we have

$$\begin{aligned}\sum_{m=1}^{N} H(M_m|B) &\geqslant (N-1)H(A|B) - \log_2 b_1\\ &+(1-\Omega_1)\log_2\frac{b_1}{b_2} + \cdots + (1-\Omega_{d-1})\log_2\frac{b_{d-1}}{b_d},\end{aligned} \tag{5.118}$$

where b_i is the i-th largest element among all

$$\left\{ \sum_{i_2 \cdots i_{N-1}} \max_{i_1}[c(u^1_{i_1}, c(u^2_{i_2})] \prod_{m=2}^{N-1} c(u^m_{i_m}, c(u^{m+1}_{i_{m+1}}) \right\}$$

over the indices i_N and $c(u^m_{i_m}, u^{m+1}_{i_{m+1}}) =| \langle u^m_{i_m} | u^{m+1}_{i_{m+1}} \rangle |^2$. We emphasize that our bound (5.118) has a high rate of validity $(2^L - 2 - L)/(2^L - 2)$ among all possibilities. A complete proof of the relation (5.118) is given as

Proof. For an L-partite state ρ, divide the whole system into two parts: the measured subsystem A and the remaining subsystem as quantum memory B, then we can still denote the quantum state as ρ_{AB}. Given N measurements $M_1, M_2, \cdots, M_N$, to find a lower bound for the entropic uncertainty relations in the presence of quantum memory we use basic properties of the relative entropy as follows:

$$\begin{aligned} & S(\rho_{AB} \parallel \sum_{i_1} [u^1_{i_1}] \rho_{AB} [u^1_{i_1}]) \\ \geqslant & S([u^2_{i_2}] \rho_{AB} [u^2_{i_2}] \parallel \sum_{i_1, i_2} c(u^1_{i_1}, u^2_{i_2}) [u^2_{i_2}] \otimes Tr_A([u^1_{i_1}] \rho_{AB})) \\ = & S(\rho_{AB} \parallel \sum_{i_1, i_2} c(u^1_{i_1}, u^2_{i_2}) [u^2_{i_2}] \otimes Tr_A([u^1_{i_1}] \rho_{AB})) + H(A|B) - H(M_2|B), \end{aligned} \quad (5.119)$$

where $c(u^1_{i_1}, u^2_{i_2}) =| \langle u^1_{i_1} | u^2_{i_2} \rangle |^2$ and $[u^m_{i_m}] = |u^m_{i_m}\rangle\langle u^m_{i_m}|$. Inductively the generalized lower bound is given as follows

$$-NH(A|B) + \sum_{m=1}^{N} H(M_m|B) \geqslant S(\rho_{AB} \parallel \sum_{i_N} [u^N_{i_N}] \otimes \beta^N_{i_N}), \quad (5.120)$$

where $p^1_{i_1} \rho^1_{B_{i_1}} = Tr_A([u^1_{i_1}] \rho_{AB})$ and

$$\beta^N_{i_N} = \sum_{i_1, \cdots, i_{N-1}} p^1_{i_1} \rho^1_{B_{i_1}} \prod_{m=1}^{N-1} c(u^m_{i_m}, u^{m+1}_{i_{m+1}})$$

Taking maximum over indices $i_2, \ldots, i_{N-1}$ and writing

$$\sum_{i_2, \cdots, i_{N-1}} \max_{i_1}[c(u^1_{i_1}, u^2_{i_2})] \prod_{m=2}^{N-1} c(u^m_{i_m}, u^{m+1}_{i_{m+1}}) = b(i_N), \quad (5.121)$$

we have that

$$S(\rho_{AB} \parallel \sum_{i_N}[u^N_{i_N}] \otimes \beta^N_{i_N}) \geqslant -H(A|B) - \sum_{i_N} p^N_{i_N} \log_2 b(i_N), \tag{5.122}$$

where $p^N_{i_N} = Tr([u^N_{i_N}]\rho_A)$. We arrange the numerical values $b(i_N)$ in descending order:

$$b_1 \geqslant b_2 \geqslant \cdots \geqslant b_d, \tag{5.123}$$

so b_i is the i-th largest element among all $b(i_N)$ (counting multiplicity). Denote by p^N_i the corresponding probability. Therefore

$$\begin{aligned} &S(\rho_{AB} \parallel \sum_{i_N}[u^N_{i_N}] \otimes \beta^N_{i_N}) \\ \geqslant &- H(A|B) - \log_2 b_1 + (1-p_1)\log_2 \frac{b_1}{b_2} + \cdots + (1-p_1-\cdots-p_{d-1})\log_2 \frac{b_{d-1}}{b_d}. \end{aligned} \tag{5.124}$$

If the measured particle is l_1-partite and the quantum memory is a l_2-partite particle such that $l_1 + l_2 = L, l_1 \geqslant 2$, then there exists a state-independent majorization bound [XJLJF16a] $\omega = (\Omega_1, \Omega_2 - \Omega_1, \cdots, 1 - \Omega_{d-1})$ corresponding to the structure of the measured particle. Note that

$$\begin{aligned} 1 - p_1 &\geqslant 1 - \Omega_1, \\ 1 - p_1 - p_2 &\geqslant 1 - \Omega_2, \\ &\cdots\cdots \\ 1 - p_1 - \cdots - p_{d-1} &\geqslant 1 - \Omega_{d-1}, \end{aligned}$$

which imply that

$$\begin{aligned} &S(\rho_{AB} \parallel \sum_{i_N}[u^N_{i_N}] \otimes \beta^N_{i_N}) \\ \geqslant &- H(A|B) - \log_2 b_1 + (1-\Omega_1)\log_2 \frac{b_1}{b_2} + \cdots + (1-\Omega_{d-1})\log_2 \frac{b_{d-1}}{b_d}. \end{aligned} \tag{5.125}$$

Hence the entropic uncertainty relation is written as

$$\begin{aligned} \sum_{m=1}^{N} H(M_m|B) \geqslant &(N-1)H(A|B) - \log_2 b_1 \\ &+ (1-\Omega_1)\log_2 \frac{b_1}{b_2} + \cdots + (1-\Omega_{d-1})\log_2 \frac{b_{d-1}}{b_d}, \end{aligned} \tag{5.126}$$

which provides a substantial improvement over $(N-1)H(A|B) - \log_2 b_1$, the term contained in the presence of quantum memory. Therefore, the new bound is the tightest one with *consistent classical part* till now. ■

By taking all permutations on the index of Eq. (5.126) first, and computing the maximum over all possibilities, we obtain an optimal lower bound in the presence of quantum memory. One can also use uniform entanglement frames [XJLJF16a] to give a degenerate uncertainty inequality in the absence of quantum memory.

Besides giving theoretical improvement of the uncertainty relation, our result has potential applications in other areas of quantum theory. For example, it can be utilized in designing new entanglement detector. To witness entanglement, one considers a source that emits a bipartite state ρ_A. One defines the probability distributions of incompatible observables M_m $(m = 1, \cdots, N)$ as usual:

$$p_{i_m}^m = \langle u_{i_m}^m | \rho_A | u_{i_m}^m \rangle.$$

If the bipartite state ρ_A is separable, then there exists a vector $\omega^{sep} = (\Omega_1^{sep}, \Omega_2^{sep} - \Omega_1^{sep}, \cdots, 1 - \Omega_{d-1}^{sep})$ such that

$$(p_{i_m}^m) \prec \omega^{sep}. \tag{5.127}$$

Subsequently we have

$$\begin{aligned} \sum_{m=1}^{N} H(M_m) \geqslant (N-1)H(A) - \log_2 b_1 \\ +(1-\Omega_1^{sep}) \log_2 \frac{b_1}{b_2} + \cdots + (1-\Omega_{d-1}^{sep}) \log_2 \frac{b_{d-1}}{b_d}, \end{aligned} \tag{5.128}$$

with other notations are the same with Eq. (5.118). If there exists another quantum state ρ_A' with

$$\begin{aligned} \sum_{m=1}^{N} H(M_m) < (N-1)H(A') - \log_2 b_1 \\ +(1-\Omega_1^{sep}) \log_2 \frac{b_1}{b_2} + \cdots + (1-\Omega_{d-1}^{sep}) \log_2 \frac{b_{d-1}}{b_d}, \end{aligned} \tag{5.129}$$

where $H(A') = S(\rho_A')$, then state ρ_A' must be entangled since it violates the majorization bound for separable states. As this method is based on *uniform entanglement frames* and the entropic uncertainty relations, the witnessed entanglement does not involve with quantum memory.

Similarly, the second quantum index enables us to generalize the *admixture bound* [XJF+16] of entropic uncertainty relations for multiple measurements to allow for quantum side information. By taking maximum over Eq. (5.118) and the *admixture bound* in the presence of quantum memory, we obtain a strong entropic uncertainty relation with quantum memory for multi-measurements which will be useful in handling quantum cryptography tasks and general quantum information processings.

In this section we have extended all entropic uncertainty relations to allow for quantum side information, first in the case of two incompatible observables and then for multi-observables. Using the *second quantum index* we have characterized the correlations between measured particle and quantum memory. Our uncertainty relations are universal and capture the intrinsic nature of the uncertainty in the presence of quantum memory. Moreover, we have observed that the uncertainties in the presence of quantum memory decrease under appropriate selection of incompatible observables. Finally, we have derived several strong bounds for the entropic uncertainty relation in the presence of quantum memory. We have also discussed applications of our result to entanglement witnesses with or without quantum memory.

Chapter 6

Conclusions and Outlook

The aim of this thesis is to strengthen the bounds for uncertainty relations, including the variance-based uncertainty relations, mutually exclusive uncertainty relations and entropic framework of uncertainty principle, and to generalize all entropic uncertainty relations to allow for quantum side information. The concept of *quantum index* has been given to consolidate the framework for uncertainty principle in presence of quantum memory.

6.1 Applications

The uncertainty relations has aleardy found a wide range of applications, especially entropic uncertainty relations.

Quantum key distribution (QKD) is one of the main applications for entropic uncertainty relations. Traditionally, two parties Alice and Bob agree on a shared key by communicating through a public information channel. The key is safe from any potential eavesdropper, Eve. Unfortunately, it is clear that if only the classical information has been considered by Alice and Bob, the key distribution becomes impossible. On the other hand, the impossiblity statement fails to hold when two parties Alice and Bob allow to communicate via a quantum channel instead of classical information channel, since quantum information can not be copied or cloned. Historically, quantum key distribution was first introduced by Bennett and Brassard [BB84] and Ekert [Eke91]. Further, the entropic framework for uncertainty relations have became a standard tool to analyze security in cryptography.

The entanglement detection are crucial for quantum information theory, since entanglement between particles is a central resource in quantum information processing. A common idea in entanglement detection is to build a mathematical restriction that all separable states must satisfy, and once this restriction has been violated will then guarantee the entanglement. Combine this idea with majorization theory, we propose the *Uniform Entanglement Frames* which can detect the correlations of multi-partite quantum system more effectively.

Finally, it has been shown [XJLJF16a] that based on uniform entanglement frames and the entropic uncertainty relations, the bounds of uncertainty relation can be used to witness entanglement and this method does not involve with quantum memory.

6.2 Outlook and Open Questions

Some of the technical results appeared in this thesis are novel and their applications remain unexplored. The lower bound of the entropic uncertainty relations has been improved and our results have applications in quantum cryptography, entanglement detection and quantum communication. Investigating these potential applications is one of the most interesting future research arising from our results. Another more foundational direction of our research could be whether our results can be extend to smooth entropies or smooth mutual information which are closely related to nonasymptotic quantum information theory.

The entropic uncertainty relations in presence of quantum memory is one of the important recent advances on uncertainty principle, and it allows the measured quantum system to be correlated with its environment in a non-classical way. From D. Deutsch's expression of uncertainty principle [Deu83]

- "*It is logically possible that the bound could also depend on the initial state of the system, but this could not be the case in quantum theory where there always exists a dynamical evolution which transforms any initial state into any other.*"

in other words, in order to represent a quantitative physical concept of "uncertainty", the lower bound should be state independent (or measured particle independent). For entropic formulation of uncertainty principle with quantum memory, it remains an open question whether we can derive a measured particle independent lower bound.

Finally, my sincerest hope is that the results of this thesis could do a little help in consolidating the framework of uncertainty relations and providing a reference for researchers who are interested in uncertainty relations.

References

[ABLS01] Antonio Acin, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera, *Classification of mixed three-qubit states*, Physical Review Letters **87** (2001), no. 4, 040401. 86, 87, 88

[AD75] János Aczél and Zoltán Daróczy, *On measures of information and their characterizations*, New York (1975). 43

[AMO11] BC Arnold, AW Marshall, and I Olkin, *Inequalities: Theory of majorization and its applications*, 2011. 87, 119

[And89] Tsuyoshi Ando, *Majorization, doubly stochastic matrices, and comparison of eigenvalues*, Linear Algebra and Its Applications **118** (1989), 163–248. 96

[ASH16] F Adabi, S Salimi, and S Haseli, *Tightening the entropic uncertainty bound in the presence of quantum memory*, arXiv preprint arXiv:1602.04296 (2016). 142

[BB84] Charles H Bennett and Gilles Brassard, *Advances in cryptology: Proceedings of crypto'84, august 1984*, 1984. 10, 153

[BBM75] Iwo Białynicki-Birula and Jerzy Mycielski, *Uncertainty relations for information entropy in wave mechanics*, Communications in Mathematical Physics **44** (1975), no. 2, 129–132. 14, 102, 128

[BCC+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner, *The uncertainty principle in the presence of quantum memory*, Nature Physics **6** (2010), no. 9, 659–662. 15, 102, 114, 127, 128, 136, 140

[BEK+04] Mohamed Bourennane, Manfred Eibl, Christian Kurtsiefer, Sascha Gaertner, Harald Weinfurter, Otfried Gühne, Philipp Hyllus, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera, *Experimental detection of multipartite entanglement using witness operators*, Physical review letters **92** (2004), no. 8, 087902. 95, 99

[Bel66] John S Bell, *Physics 1, 195 (1964)*, Rev. Mod. Phys **38** (1966), 447. 2

[BGLP11] Jean-Daniel Bancal, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio, *Device-independent witnesses of genuine multipartite entanglement*, Physical Review Letters **106** (2011), no. 25, 250404. 85

[Bha09] Rajendra Bhatia, *Positive definite matrices*, Princeton university press, 2009. 19

[Bha13] ______, *Matrix analysis*, vol. 169, Springer Science & Business Media, 2013. 19

[BHL07] Paul Busch, Teiko Heinonen, and Pekka Lahti, *Heisenberg's uncertainty principle*, Physics Reports **452** (2007), no. 6, 155–176. 60

[BLW13] Paul Busch, Pekka Lahti, and Reinhard F Werner, *Proof of heisenberg's error-disturbance relation*, Physical review letters **111** (2013), no. 16, 160405. 12, 13, 61

[BLW14a] ______, *Colloquium: Quantum root-mean-square error and measurement uncertainty relations*, Reviews of Modern Physics **86** (2014), no. 4, 1261. 60

[BLW14b] ______, *Heisenberg uncertainty for qubit measurements*, Physical Review A **89** (2014), no. 1, 012129. 61

[BP85] Richard Blankenbecler and M Hossein Partovi, *Uncertainty, entropy, and the statistical mechanics of microscopic systems*, Physical review letters **54** (1985), no. 5, 373. 86

[BPP12] GM Bosyk, M Portesi, and A Plastino, *Collision entropy and optimal uncertainty*, Physical Review A **85** (2012), no. 1, 012108. 113

[BVL05] Samuel L Braunstein and Peter Van Loock, *Quantum information with continuous variables*, Reviews of Modern Physics **77** (2005), no. 2, 513. 86

[C+67] I Csisz et al., *Information-type measures of difference of probability distributions and indirect observations*, Studia Sci. Math. Hungar. **2** (1967), 299–318. 49

[CAG99] NJ Cerf, C Adami, and RM Gingrich, *Reduction criterion for separability*, Physical Review A **60** (1999), no. 2, 898. 39

[CBTW15] Patrick J Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner, *Entropic uncertainty relations and their applications*, arXiv preprint arXiv:1511.04857 (2015). 60, 86, 103, 135

[CF15] Bin Chen and Shao-Ming Fei, *Sum uncertainty relations for arbitrary n incompatible observables*, Scientific reports **5** (2015). 64

[CMCS12] Zhi-Hua Chen, Zhi-Hao Ma, Jing-Ling Chen, and Simone Severini, *Improved lower bounds on genuine-multipartite-entanglement concurrence*, Physical Review A **85** (2012), no. 6, 062320. 85

[Col12] Patrick J Coles, *Unification of different views of decoherence and discord*, Physical Review A **85** (2012), no. 4, 042103. 130

[CP14] Patrick J Coles and Marco Piani, *Improved entropic uncertainty relations and information exclusion relations*, Physical Review A **89** (2014), no. 2, 022112. 86, 102, 112, 114, 120, 128, 129, 135, 138

[CT06] Thomas M Cover and Joy A Thomas, *Elements of information theory 2nd edition*. 113

[CYGG11] Patrick J Coles, Li Yu, Vlad Gheorghiu, and Robert B Griffiths, *Information-theoretic treatment of tripartite systems and quantum channels*, Physical Review A **83** (2011), no. 6, 062338. 113, 130

[Deu83] David Deutsch, *Uncertainty in quantum measurements*, Physical Review Letters **50** (1983), no. 9, 631. 15, 61, 68, 86, 102, 113, 128, 135, 154

[DHL+04] David P DiVincenzo, Michał Horodecki, Debbie W Leung, John A Smolin, and Barbara M Terhal, *Locking classical correlations in quantum states*, Physical Review Letters **92** (2004), no. 6, 067902. 86

[DST14] Frédéric Dupuis, Oleg Szehr, and Marco Tomamichel, *A decoupling approach to classical data transmission over quantum channels*, IEEE Transactions on Information Theory **60** (2014), no. 3, 1562–1572. 113

[dVH11] Julio I de Vicente and Marcus Huber, *Multipartite entanglement detection from correlation tensors*, Physical Review A **84** (2011), no. 6, 062306. 85

[Eğe95] Ömer Eğecioğlu, *Parallelogram-law-type identities*, Linear algebra and its applications **225** (1995), 1–12. 70

[EI56] Hugh Everett III, *The many-worlds interpretation of quantum mechanics. the theory of the universal wavefunction*, Ph.D. thesis, Thesis, Princeton University,(1956, 1973), 1956. 3

[EI57] ———, *relative stateformulation of quantum mechanics*, Reviews of modern physics **29** (1957), no. 3, 454. 14

[Eke91] Artur K Ekert, *Quantum cryptography based on bell's theorem*, Physical review letters **67** (1991), no. 6, 661. 153

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Physical review **47** (1935), no. 10, 777. 2

[FGG13] Shmuel Friedland, Vlad Gheorghiu, and Gilad Gour, *Universal uncertainty relations*, Physical review letters **111** (2013), no. 23, 230401. 10, 87, 103, 104, 106, 108, 112, 116, 119, 120, 138, 147

[GHH10] Andreas Gabriel, Beatrix C Hiesmayr, and Marcus Huber, *Criterion for k-separability in mixed multipartite systems*, arXiv preprint arXiv:1002.2953 (2010). 85, 86

[GHH+13] Andrzej Grudka, Michał Horodecki, Paweł Horodecki, Ryszard Horodecki, Waldemar Kłobus, and Łukasz Pankowski, *Conjectured strong complementary-correlations tradeoff*, Physical Review A **88** (2013), no. 3, 032106. 114

[GLM04] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone, *Quantum-enhanced measurements: beating the standard quantum limit*, Science **306** (2004), no. 5700, 1330–1336. 60

[GLM06] ———, *Quantum metrology*, Physical review letters **96** (2006), no. 1, 010401. 60

[GLM11] ———, *Advances in quantum metrology*, Nature Photonics **5** (2011), no. 4, 222–229. 60

[GMR03] GianCarlo Ghirardi, Luca Marinatto, and Raffaele Romano, *An optimal entropic uncertainty relation in a two-dimensional hilbert space*, Physics Letters A **317** (2003), no. 1, 32–36. 119

[Güh04] Otfried Gühne, *Characterizing entanglement via uncertainty relations*, Physical review letters **92** (2004), no. 11, 117903. 60, 86

[GV96] Lior Goldenberg and Lev Vaidman, *Applications of a simple quantum mechanical formula*, American Journal of Physics **64** (1996), no. 8, 1059–1060. 70

[GYvE14] Ting Gao, Fengli Yan, and SJ van Enk, *Permutationally invariant part of a density matrix and nonseparability of n-qubit states*, Physical review letters **112** (2014), no. 18, 180501. 85

[Hal73] Paul R Halmos, *The legend of john von neumann*, The American Mathematical Monthly **80** (1973), no. 4, 382–394. 22

[Hal95] Michael JW Hall, *Information exclusion principle for complementary observables*, Physical review letters **74** (1995), no. 17, 3307. 113, 114, 115

[Hal97] ______, *Quantum information and correlation bounds*, Physical Review A **55** (1997), no. 1, 100. 113

[Hay06] Masahito Hayashi, *Quantum information*, Springer, 2006. 19

[HB82] Steve J Heims and Duane W Bailey, *John von neumann and norbert wiener, from mathematics to the technologies of life and death*, American Journal of Physics **50** (1982), no. 4, 383–383. 22

[HC67] Jan Havrda and František Charvát, *Quantification method of classification processes. concept of structural a-entropy*, Kybernetika **3** (1967), no. 1, 30–35. 119

[Hei27] Werner Heisenberg, *Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik*, Zeitschrift für Physik **43** (1927), no. 3-4, 172–198. 11, 12, 59, 86, 102, 113, 134

[HGY12] Yan Hong, Ting Gao, and Fengli Yan, *Measure of multipartite entanglement with computable lower bounds*, Physical Review A **86** (2012), no. 6, 062323. 85

[HH99] Michał Horodecki and Paweł Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols*, Physical Review A **59** (1999), no. 6, 4206. 40

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki, *Quantum entanglement*, Reviews of modern physics **81** (2009), no. 2, 865. 41

[Hir57] Isidore I Hirschman, *A note on entropy*, American journal of mathematics **79** (1957), no. 1, 152–156. 14, 86

[HJ91] Roger A Hom and Charles R Johnson, *Topics in matrix analysis*, Cambridge UP, New York (1991). 19

[HJ12] Roger A Horn and Charles R Johnson, *Matrix analysis*, Cambridge university press, 2012. 19

[HKSM10] Omar Hirzallah, Fuad Kittaneh, and Mohammad Sal Moslehian, *Schatten p–norm inequalities related to a characterization of inner product spaces*, Mathematical Inequalities and Applications **13** (2010). 70

[HMGH10] Marcus Huber, Florian Mintert, Andreas Gabriel, and Beatrix C Hiesmayr, *Detection of high-dimensional genuine multipartite entanglement of mixed states*, Physical review letters **104** (2010), no. 21, 210501. 85, 93

[Hol73a] Alexander Semenovich Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel*, Problemy Peredachi Informatsii **9** (1973), no. 3, 3–11. 113

[Hol73b] ______, *A generalization of the rao-cramér inequality*, Teoriya Veroyatnostei i ee Primeneniya **18** (1973), no. 2, 371–375. 76

[HPLdV13] Marcus Huber, Martí Perarnau-Llobet, and Julio I de Vicente, *Entropy vector formalism and the structure of multidimensional entanglement in multipartite systems*, Physical Review A **88** (2013), no. 4, 042328. 85

[HS14] Marcus Huber and Ritabrata Sengupta, *Witnessing genuine multipartite entanglement with positive maps*, Physical review letters **113** (2014), no. 10, 100501. 85

[HT03] Holger F Hofmann and Shigeki Takeuchi, *Violation of local uncertainty relations as a signature of entanglement*, Physical Review A **68** (2003), no. 3, 032103. 60

[Hum72] James E Humphreys, *Introduction to lie algebras and representation theory*, vol. 9, Springer Science & Business Media, 1972. 31

[Jam66] Max Jammer, *The conceptual development of quantum mechanics*. 22

[JMG11] Bastian Jungnitsch, Tobias Moroder, and Otfried Gühne, *Taming multiparticle entanglement*, Physical review letters **106** (2011), no. 19, 190502. 85

[KAT86] Mikio KATo, *A note on a generalized parallelogram law and the littlewood matrices*, Bull. Kyushu Inst. Tech. Math. Natur. Sci **33** (1986), 37–39. 70

[Ken27] Earle H Kennard, *Zur quantenmechanik einfacher bewegungstypen*, Zeitschrift für Physik **44** (1927), no. 4-5, 326–352. 12, 59

[Kra87] Karl Kraus, *Complementary observables and uncertainty relations*, Physical Review D **35** (1987), no. 10, 3070. 128

[KTW14] Jędrzej Kaniewski, Marco Tomamichel, and Stephanie Wehner, *Entropic uncertainty from effective anticommutators*, Physical Review A **90** (2014), no. 1, 012332. 134, 135, 138, 139, 147

[KU93] Masahiro Kitagawa and Masahito Ueda, *Squeezed spin states*, Physical Review A **47** (1993), no. 6, 5138. 60

[Lan05] Nicolaas Pieter Landsman, *Requiem voor newton*, Amsterdam: Contact, 2005. 22

[LFLJF15] Ming Li, Shao-Ming Fei, Xianqing Li-Jost, and Heng Fan, *Genuine multipartite entanglement detection and lower bound of multipartite concurrence*, Physical Review A **92** (2015), no. 6, 062338. 85

[LMF15] Shang Liu, Liang-Zhu Mu, and Heng Fan, *Entropic uncertainty relations for multiple measurements*, Physical Review A **91** (2015), no. 4, 042133. 102, 109, 110, 112, 121, 124

[Mac00] Norman Macrae, *John von neumann: The scientific genius who pioneered the modern computer, game theory, nuclear deterrence, and much more*, American Mathematical Soc., 2000. 22

[MCC+11] Zhi-Hao Ma, Zhi-Hua Chen, Jing-Ling Chen, Christoph Spengler, Andreas Gabriel, and Marcus Huber, *Measure of genuine multipartite entanglement with computable lower bounds*, Physical Review A **83** (2011), no. 6, 062325. 85

[MLPŻ13] Marcin Markiewicz, Wiesław Laskowski, Tomasz Paterek, and Marek Żukowski, *Detecting genuine multipartite entanglement of pure states with bipartite correlations*, Physical Review A **87** (2013), no. 3, 034301. 85

[Mos10] Mohammad Sal Moslehian, *An operator extension of the parallelogram law and related norm inequalities*, arXiv preprint arXiv:1011.6605 (2010). 70

[MP14] Lorenzo Maccone and Arun K Pati, *Stronger uncertainty relations for all incompatible observables*, Physical review letters **113** (2014), no. 26, 260401. 17, 60, 72, 73, 74, 75, 76

[MR88] Jagdish Mehra and Helmut Rechenberg, *The historical development of quantum theory, vol. 6: The completion of quantum mechanics*, Part **1** (1988), 241–56. 22

[MU88] Hans Maassen and Jos BM Uffink, *Generalized entropic uncertainty relations*, Physical Review Letters **60** (1988), no. 12, 1103. 15, 61, 86, 102, 113, 114, 128, 135, 138

[Mur14] Gerald J Murphy, *C*-algebras and operator theory*, Academic press, 2014. 39

[MWSN11] Jian Ma, Xiaoguang Wang, CP Sun, and Franco Nori, *Quantum spin squeezing*, Physics Reports **509** (2011), no. 2, 89–165. 60

[NC10] Michael A Nielsen and Isaac L Chuang, *Quantum computation and quantum information*, Cambridge university press, 2010. 19, 118, 121

[Nel66] Edward Nelson, *Derivation of the schrödinger equation from newtonian mechanics*, Physical review **150** (1966), no. 4, 1079. 3

[OW10] Jonathan Oppenheim and Stephanie Wehner, *The uncertainty principle determines the nonlocality of quantum mechanics*, Science **330** (2010), no. 6007, 1072–1074. 86

[Par11] M Hossein Partovi, *Majorization formulation of uncertainty in quantum mechanics*, Physical Review A **84** (2011), no. 5, 052117. 86, 88, 104

[Par12] ______, *Entanglement detection using majorization uncertainty bounds*, Physical Review A **86** (2012), no. 2, 022309. 10, 89, 95, 104, 148

[Per96] Asher Peres, *Separability criterion for density matrices*, Physical Review Letters **77** (1996), no. 8, 1413. 10, 37

[PRŻ13] Zbigniew Puchała, Łukasz Rudnicki, and Karol Życzkowski, *Majorization entropic uncertainty relationsdedicated to iwo białynicki-birula on the occasion of his 80th birthday.*, Journal of Physics A: Mathematical and Theoretical **46** (2013), no. 27, 272002. 10, 87, 104, 105, 106, 112, 116, 119, 120, 138, 147

[PS07] AK Pati and PK Sahu, *Sum uncertainty relation in quantum theory*, Physics Letters A **367** (2007), no. 3, 177–181. 69

[Rén76] Alfréd Rényi, *Selected papers of alfréd rényi: 1948-1956*, vol. 1, Akadémiai Kiadó, 1976. 43

[Rez61] Fazlollah M Reza, *An introduction to information theory*, Courier Corporation, 1961. 114

[RL08] Ángel Rivas and Alfredo Luis, *Characterization of quantum angular-momentum fluctuations via principal components*, Physical review A **77** (2008), no. 2, 022105. 64

[Rob29] Howard Percy Robertson, *The uncertainty principle*, Physical Review **34** (1929), no. 1, 163. 13, 60, 86

[RPŻ14] Łukasz Rudnicki, Zbigniew Puchała, and Karol Życzkowski, *Strong majorization entropic uncertainty relations*, Physical Review A **89** (2014), no. 5, 052115. 10, 103, 104, 105, 112, 116, 120, 129, 135, 138, 147

[RRN61] ALFRPED RRNYI, *On measures of entropy and information.* 42

[Sch23] I Schur, *Theorie sitzungsber*, Berlin Math. Gesellschaft **22** (1923), no. 9. 96

[Sch30] Erwin Schrödinger, *Zum heisenbergschen unschärfeprinzip*, Akademie der Wissenschaften, 1930. 60

[Sha48] Claude E Shannon, *Bell system tech. j. 27 (1948) 379; ce shannon*, Bell System Tech. J **27** (1948), 623. 42

[Sha01] Claude Elwood Shannon, *A mathematical theory of communication*, ACM SIGMOBILE Mobile Computing and Communications Review **5** (2001), no. 1, 3–55. 7

[SO94] A Smart and JK Ord, *Kendall's advanced theory of statistics: Distribution theory*, 1994. 46

[Stø63] Erling Størmer, *Positive linear maps of operator algebras*, Acta Mathematica **110** (1963), no. 1, 233–278. 38

[SV13] J Sperling and W Vogel, *Multipartite entanglement witnesses*, Physical review letters **111** (2013), no. 11, 110503. 85

[Tom15] Marco Tomamichel, *Quantum information processing with finite resources: Mathematical foundations*, vol. 5, Springer, 2015. 103

[Vai92] Lev Vaidman, *Minimum time for the evolution to an orthogonal quantum state*, American journal of physics **60** (1992), no. 2, 182–183. 70

[Vla04] A Vladimir, *Zorich, mathematical analysis i*, 2004. 74

[VW02] Karl Gerd H Vollbrecht and Michael M Wolf, *Conditional entropies and their relation to entanglement criteria*, Journal of Mathematical Physics **43** (2002), no. 9, 4299–4306. 37

[Wat11] John Watrous, *Theory of quantum information*, University of Waterloo Fall **128** (2011). 19

[WBI+92] DJ Wineland, JJ Bollinger, WM Itano, FL Moore, and DJ Heinzen, *Spin squeezing and reduced quantum noise in spectroscopy*, Physical Review A **46** (1992), no. 11, R6797. 60

[WE85] K Wodkiewicz and JH Eberly, *Coherent states, squeezed fluctuations, and the su (2) am su (1, 1) groups in quantum-optics applications*, JOSA B **2** (1985), no. 3, 458–466. 60

[Weh78] Alfred Wehrl, *General properties of entropy*, Reviews of Modern Physics **50** (1978), no. 2, 221. 9

[Wey27] Hermann Weyl, *Quantenmechanik und gruppentheorie*, Zeitschrift für Physik **46** (1927), no. 1-2, 1–46. 12, 60

[WKB+12] Jun-Yi Wu, Hermann Kampermann, Dagmar Bruß, Claude Klöckl, and Marcus Huber, *Determining lower bounds on a measure of multipartite entanglement from few local observables*, Physical Review A **86** (2012), no. 2, 022319. 85

[Wor76] Stanisław Lech Woronowicz, *Positive maps of low dimensional matrix algebras*, Reports on Mathematical Physics **10** (1976), no. 2, 165–183. 38

[WW10] Stephanie Wehner and Andreas Winter, *Entropic uncertainty relations—a survey*, New Journal of Physics **12** (2010), no. 2, 025009. 60, 86, 113

[WZ81] DF Walls and P Zoller, *Reduced quantum fluctuations in resonance fluorescence*, Physical Review Letters **47** (1981), no. 10, 709. 60

[XJF+16] Yunlong Xiao, Naihuan Jing, Shao-Ming Fei, Tao Li, Xianqing Li-Jost, Teng Ma, and Zhi-Xi Wang, *Strong entropic uncertainty relations for multiple measurements*, Physical Review A **93** (2016), no. 4, 042125. 115, 122, 151

[XJFLJ16] Yunlong Xiao, Naihuan Jing, Shao-Ming Fei, and Xianqing Li-Jost, *Improved uncertainty relation in the presence of quantum memory*, arXiv preprint arXiv:1604.04944 (2016). 135, 142

[XJLJF16a] Yunlong Xiao, Naihuan Jing, Xianqing Li-Jost, and Shao-Ming Fei, *Uniform entanglement frames*, International Journal of Theoretical Physics (2016), 1–14. 10, 148, 150, 151, 154

[XJLJF16b] ———, *Weighted uncertainty relations*, Scientific Reports **6** (2016), 23201. 72, 73, 74, 75, 76, 83, 86, 142

[YO93] Horace P Yuen and Masanao Ozawa, *Ultimate information carrying limit of quantum systems*, Physical review letters **70** (1993), no. 4, 363. 113

[YXWS15] Yao Yao, Xing Xiao, Xiaoguang Wang, and CP Sun, *Implications and applications of the variance-based uncertainty equalities*, Physical Review A **91** (2015), no. 6, 062113. 72

[Zen82] WL Zeng, *An extension of the parallelogram characterization of inner product spaces*, J. Math. Res. Exposition, vol. 2, 1982, pp. 23–25. 70

[Zha07] Fuzhen Zhang, *On the bohr inequality of operators*, Journal of mathematical analysis and applications **333** (2007), no. 2, 1264–1271. 70

[ZZY15] Jun Zhang, Yang Zhang, and Chang-shui Yu, *Entropic uncertainty relation and information exclusion relation for multiple measurements in the presence of quantum memory*, Scientific reports **5** (2015). 109, 112, 115, 122, 123

Veröffentlichungen

Begutachtete Artikel

- *Geometric Global Quantum Discord of Two-qubit States*, Yunlong Xiao, Tao Li, Shao-Ming Fei, Naihuan Jing, Xianqing Li-Jost and Zhi-Xi Wang, Chin. Phys. B Vol. 25, No. 3 (2016) 030301.
- *Uniform Entanglement Frames*, Yunlong Xiao, Naihuan Jing, Xianqing Li-Jost and Shao-Ming Fei, Int. J. Theor. Phys. (2016). DOI:10.1007/s10773-016-2976-0.
- *Weighted Uncertainty Relations*, Yunlong Xiao, Naihuan Jing, Xianqing Li-Jost and Shao-Ming Fei, Scientific Reports 6, 23201 (2016).
- *Strong entropic uncertainty relations for multiple measurements*, Yunlong Xiao, Naihuan Jing, Shao-Ming Fei, Tao Li, Xianqing Li-Jost, Teng Ma and Zhi-Xi Wang, Phys. Rev. A 93, 042125 (2016).
- *Enhanced Information Exclusion Relations*, Yunlong Xiao, Naihuan Jing and Xianqing Li-Jost, Scientific Reports 6, 30440 (2016).
- *Mutually Exclusive Uncertainty Relations*, Yunlong Xiao and Naihuan Jing, Scientific Reports 6, 36616 (2016).
- *Improved Uncertainty Relation in the Presence of Quantum Memory*, Yunlong Xiao, Naihuan Jing, Shao-Ming Fei and Xianqing Li-Jost, J. Phys. A: Math. Theor. 49, 49LT01 (2016).

Eingereicht Artikel

- *Uncertainty under Quantum Measurements and Quantum Memory*, Yunlong Xiao, Naihuan Jing and Xianqing Li-Jost, preprint.
- *Strong Variance-Based Uncertainty Relations*, Yunlong Xiao, Naihuan Jing, Bing Yu, Shao-Ming Fei and Xianqing Li-Jost, preprint.

Bibliographische Daten

A Framework for Uncertainty Relations
(Ein Rahmen für Unschärferelation)
Xiao, Yunlong

Universität Leipzig, Dissertation, 2016
186 Seiten, 33 Abbildungen, 131 Referenzen

Selbstständigkeitserklärung

Hiermit erkläre ich, die vorliegende Dissertation selbständig und ohne unzulässige fremde Hilfe angefertigt zu haben. Ich habe keine anderen als die angeführten Quellen und Hilfsmittel benutzt und sämtliche Textstellen, die wörtlich oder sinngemäß aus veröffentlichten oder unveröffentlichten Schriften entnommen wurden, und alle Angaben, die auf mündlichen Auskünften beruhen, als solche kenntlich gemacht. Ebenfalls sind alle von anderen Personen bereitgestellten Materialien oder erbrachten Dienstleistungen als solche gekennzeichnet.

Leipzig, den 21. Februar, 2017

Yunlong Xiao

....

(Yunlong Xiao)

Short CV

Name:	Yunlong Xiao
Date of birth:	05.07.1989
09/2007 - 07/2011	Bachelor in School of Mathematical Sciences Shanxi University (China)
09/2011 - 07/2013	Graduate student in School of Mathematics South China University of Technology (China)
since 09/2013	PhD student in School of Mathematics South China University of Technology (China)
since 09/2014	PhD student at the Max Planck Institute for Mathematics in the Sciences (Germany)

Daten zum Autor

Name:	Yunlong Xiao
Geburtsdatum:	05.07.1989
09/2007 - 07/2011	Mathematikstudium Universität Shanxi Taiyuan
09/2011 - 07/2013	Student im Mathematikstudium Technische Universität Südchinas Guangzhou
seit 09/2013	Doktorand im Mathematikstudium Technische Universität Südchinas Guangzhou
seit 09/2014	Doktorand am Max-Planck-Institut für Matematik in den Naturwissenschaften Leipzig
Adresse:	Inselstraße 22 Max-Planck-Institut für Mathematik in den Naturwissenschaften, 04103 Leipzig