

Explicit Bounds of Uncertainty Relations for Quantum Testers

Taihei Kimoto

Abstract

Uncertainty relations represent one of the most fundamental constraints in quantum theory and have been extensively studied from the early days of quantum mechanics to the present. The importance of uncertainty relations has further increased with the emergence of innovative quantum information processing protocols and the recent advances in high-precision control of quantum-scale physical systems. In particular, the uncertainty relations derived by Xiao et al. for quantum testers, also known as process positive-operator-valued measures (PPOVMs), provide quantitative trade-offs that characterize the (im)possibility of quantum processes, and thus offer formulas of great significance from both foundational and applied perspectives. On the other hand, it is possible to obtain more practical uncertainty relations for quantum testers by restricting classes of quantum processes or by considering a formulation that allows an arbitrary number of testers. The purpose of this thesis is to present theoretical results on uncertainty relations for quantum testers obtained from these viewpoints. Specifically, the thesis addresses the following three topics:

1. derivation of an exact uncertainty relation for a simple physical system;
2. derivation of a scalable uncertainty relation applicable to an arbitrary number of testers;
3. derivation of explicit formulas characterizing uncertainty that arises from restrictions on the class of time evolutions.

Since the main results are given in explicit and directly evaluable forms, they are expected to be applicable to several tasks in quantum technologies, such as performance evaluation in quantum computation and quantum cryptography, as well as experimental verification of quantum mechanics. Indeed, applications to a quantum key distribution protocol, a certain state transformation problem, and a detection problem of a channel property are discussed, supporting the usefulness of the main contributions of this thesis.

List of Papers

This doctoral thesis is based on the following papers:

1. ([1])
T. Kimoto and T. Miyadera, “An Uncertainty Relation for Measurements of Random Unitary Channels Acting on a Qubit,” *Journal of the Physical Society of Japan*, **92**, 034005 (2023).
2. ([2])
T. Kimoto, “Fine-Grained Uncertainty Relations for Quantum Testers,” *Journal of the Physical Society of Japan*, **94**, 054001 (2025).
3. ([3])
T. Kimoto and T. Miyadera, “Upper Bounds on Probabilities in Channel Measurements on Qubit Channels and Their Applications,” *Journal of the Physical Society of Japan*, **94**, 084004 (2025).

Contents

1	Introduction	4
2	Preliminaries	7
2.1	States, POVMs, Channels, and Testers	7
2.1.1	States	7
2.1.2	POVMs	8
2.1.3	Channels	9
2.1.4	Random unitary channels	12
2.1.5	Entanglement breaking channels	13
2.1.6	Testers	15
2.2	Uncertainty Relations	18
2.2.1	Uncertainty relations for measurements of states	19
2.2.2	Uncertainty relations for measurements of channels . .	28
3	An Uncertainty Relation for Measurements of Random Unitary Channels Acting on a Qubit	31
3.1	Introduction	31
3.2	Derivation	32
3.3	Summary and Discussion	36
4	Fine-Grained Uncertainty Relations for Quantum Testers	39
4.1	Introduction	39
4.2	Generalization of the Fine-Grained Uncertainty Relation . . .	40
4.3	Estimation of the Uncertainty Bound	42
4.3.1	Case of ancilla-free testers	43
4.3.2	Case of testers with a maximally entangled input state	43
4.4	A Semidefinite Program for the Uncertainty Bound	48
4.5	Application to a Quantum Key Distribution Protocol	51

4.6	Summary and Discussion	55
5	Upper Bounds on Probabilities in Channel Measurements on Qubit Channels and Their Applications	58
5.1	Introduction	58
5.2	Estimation of Probabilities in Channel Measurements	59
5.2.1	Depolarizing channels	61
5.2.2	Unital channels	62
5.2.3	Entanglement breaking channels	62
5.2.4	Unital entanglement breaking channels	62
5.2.5	General qubit channels	63
5.2.6	Comparison of the upper bounds	63
5.2.7	Remarks on the upper bounds	65
5.3	Joint Convertibility	66
5.3.1	Depolarizing channels	67
5.3.2	Unital channels	69
5.3.3	Entanglement breaking channels	70
5.3.4	Unital entanglement breaking channels	72
5.3.5	General qubit channels	74
5.3.6	Comparison of the joint convertibility	77
5.4	Detection of a Channel	79
5.4.1	Measurement with the maximally entangled state	80
5.4.2	Ancilla-free measurements	81
5.5	Summary and Discussion	82
6	Summary	84

Chapter 1

Introduction

Uncertainty relations are at the heart of quantum theory. They impose restrictions on the probability distributions of measurements performed on a state, thereby describing a kind of impossibility in quantum systems. For instance, the inequality derived by Robertson in Ref. [4] expresses such a constraint on the probability distributions of Hermitian operators by bounding the associated standard deviations from below by a quantity which depends on the commutator of the Hermitian operators. In particular, Robertson's inequality implies that the probability distributions of a particle's position and momentum cannot be arbitrarily localized at the same time, indicating that, unlike in classical mechanics, it is not possible to assign definite values to the position and momentum in quantum mechanics.

Although Robertson's inequality demonstrates a crucial difference between the quantum and classical worlds, it is not a perfect formulation of uncertainty relations. In Ref. [5], Deutsch provided an alternative uncertainty relation by employing the Shannon entropy as the measure of uncertainty while pointing out non-negligible drawbacks of Robertson's inequality. Deutsch's uncertainty relation has had a significant impact on subsequent research. In particular, uncertainty relations formulated with information entropies, including the Shannon entropy, have been investigated from both fundamental and practical points of view, constituting a wide and deep area of study [6].

Besides entropic uncertainty relations, other formulations have been proposed and analyzed. Among them, majorization uncertainty relations and fine-grained uncertainty relations impose strong and detailed restrictions on probability distributions, respectively. The idea of using majorization, which

is a preorder comparing two real vectors, was initiated by Partovi [7], and was further developed in subsequent works [8, 9, 10]. Majorization uncertainty relations are comprised of inequalities, thereby strongly confining the probability distributions associated with measurements performed on a state. Similar to majorization-based formulations, fine-grained uncertainty relations are defined as sets of inequalities [11]. Each element of a fine-grained uncertainty relation restricts the possible probabilities associated with a combination of measurement outcomes, making it possible to quantify how large these probabilities can be at the same time. Majorization-based and fine-grained uncertainty relations can be considered more refined formulations than entropic ones, because some entropic inequalities are derived from them [7, 8, 9, 10, 11].

A large number of uncertainty relations, including those described above, are formulated in the case where several measurements are performed on a state. In contrast, in Ref. [12], Xiao et al. presented uncertainty relations for measurements that are carried out to probe a quantum channel by utilizing a mathematical framework known as the quantum tester [13] or process positive-operator-valued measure (PPOVM) [14]. Their uncertainty relations are highly interesting and innovative in that they quantify the impossibility of quantum dynamical behaviors from the perspective of uncertainty. In addition, since every state can be identified with a state-preparation channel, these uncertainty relations encompass those for measurements performed on a state as special cases.

Thus, the uncertainty relations derived by Xiao et al. extend the concept of the principle itself, shedding new light on universal constraints in quantum systems. However, when one considers applications to quantum computation, quantum cryptography, and verification of quantum mechanics, even more flexible forms of uncertainty relations are required. In particular, the majorization-based uncertainty relations of Xiao et al. involve optimization over all physically allowed quantum evolutions, making their applications to large-scale quantum information processing protocols or Avogadro-scale physical systems practically infeasible. Therefore, from a foundational perspective, it is of great importance to derive uncertainty relations that are evaluable—in particular, those that provide explicit constraints—when one aims at applications to large-scale physical systems.

This doctoral thesis presents a series of research results on uncertainty relations for quantum testers, obtained through the author’s primary contributions [1, 2, 3]. These works pursue the goal of deriving explicitly evaluable

formulas from three complementary perspectives. First, a detailed analysis of an uncertainty relation for a simple physical system is carried out, leading to an explicit closed-form expression that does not require any optimization. Second, an uncertainty relation with a relaxed bound is formulated, yielding a scalable expression that remains tractable even for large physical systems. Third, uncertainty under restricted classes of time evolutions is investigated, resulting in explicit upper bounds on the achievable probabilities for various classes of quantum channels.

The structure of this thesis is as follows. Chapter 2 provides preliminaries for later chapters. They include the introductions of state, positive-operator-valued measure (POVM), channel, and tester, each of which is a basic concept in quantum theory. A brief review of uncertainty relations is also described in this chapter. Chapters 3, 4, and 5 constitute the main parts of this thesis. Each chapter examines one of the research topics described in the previous paragraph, based on Refs. [1], [2], and [3], respectively. Most of the results are presented as mathematical lemmas, theorems, propositions, or corollaries without proofs (see Refs. [1], [2], and [3] for the details of their proofs). Chapter 6 is the summary of this thesis.

Chapter 2

Preliminaries

2.1 States, POVMs, Channels, and Testers

States, positive-operator-valued measures (POVMs), channels, and testers are building blocks in this thesis. They can be interpreted using the language of information processing as follows: states are mathematical expressions of information packed in systems, POVMs are devices for retrieving information encoded in states, channels are converters for manipulating states, and testers are devices for inspecting channels. The aim of this section is to introduce these concepts based on Refs. [15, 16, 17, 18].

2.1.1 States

Let $\mathcal{H}$ be a d -dimensional Hilbert space, and let $\mathcal{L}(\mathcal{H})$ denote the set of all linear operators on $\mathcal{H}$. Unless otherwise stated, we assume that all Hilbert spaces are finite-dimensional. A state is a positive operator on $\mathcal{H}$ with trace equal to 1. Here, the positive operator and the trace are respectively defined as follows.

Definition 2.1.1 (Positive operator). A *positive operator* is a Hermitian operator A such that all the eigenvalues are nonnegative. We write $A \geq 0$ to indicate that A is positive.

Definition 2.1.2 (Trace). The *trace* of a linear operator, denoted $\text{tr}[\cdot]$, is

the function from $\mathcal{L}(\mathcal{H})$ to $\mathbb{C}$ defined as

$$\text{tr}[A] = \sum_{i=0}^{d-1} \langle e_i | A | e_i \rangle \quad (2.1)$$

for every $A \in \mathcal{L}(\mathcal{H})$. Here, $\{|e_i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis for $\mathcal{H}$.

With these definitions, a state is formally defined as follows.

Definition 2.1.3 (State). A *state* is an operator $\rho \in \mathcal{L}(\mathcal{H})$ such that $\rho \geq 0$ and $\text{tr}[\rho] = 1$. In particular, a state ρ is said to be *pure* if its rank is 1, i.e., it is expressed as $\rho = |\psi\rangle\langle\psi|$ using a unit vector $|\psi\rangle \in \mathcal{H}$.

A state that frequently appears in this thesis is the *maximally entangled state* P_+ on $\mathcal{H} \otimes \mathcal{H}$ given by

$$P_+ := |\Psi_+\rangle\langle\Psi_+| \quad (2.2)$$

where

$$|\Psi_+\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i \otimes i\rangle, \quad (2.3)$$

and $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis for $\mathcal{H}$.

2.1.2 POVMs

As stated in the beginning of this chapter, POVMs describe devices for measuring states. Formally, a POVM is defined as follows.

Definition 2.1.4 (POVM). Let Ω be a finite set, and let $\mathbf{E}$ be a function from Ω to $\mathcal{L}(\mathcal{H})$. The function $\mathbf{E}$ is said to be a *positive-operator-valued measure* (POVM) if and only if $\mathbf{E}(x) \geq 0$ for every $x \in \Omega$ and $\sum_{x \in \Omega} \mathbf{E}(x) = I$, where I denotes the identity operator on $\mathcal{H}$.

A pair consisting of a POVM and a state induces a probability distribution. Let $\mathbf{E}$ be a POVM defined on a finite set Ω . The set Ω is interpreted as the all possible outcomes in a measurement. If the system in a state $\rho \in \mathcal{L}(\mathcal{H})$ is measured using the device described by $\mathbf{E}$, the probability of obtaining an outcome $x \in \Omega$ is given by

$$p(x|\rho) = \text{tr}[\mathbf{E}(x)\rho], \quad (2.4)$$

which is referred to as the *Born rule*. It is clear that $p(x|\rho) \geq 0$ for every $x \in \Omega$ and $\sum_{x \in \Omega} p(x|\rho) = 1$ are respectively guaranteed by the conditions $E(x) \geq 0$ for every $x \in \Omega$ and $\sum_{x \in \Omega} E(x) = I$.

A special type of POVM is projection-valued measures (PVMs) defined as follows.

Definition 2.1.5 (PVM). A POVM $P: \Omega \rightarrow \mathcal{L}(\mathcal{H})$ is referred to as a *projection-valued measure (PVM)* if and only if, for every $x \in \Omega$, $P(x)$ is a projection, i.e., $P(x) = P(x)^\dagger = P(x)^2$ is satisfied. In particular, a PVM is said to be *rank-1* if and only if every element of the PVM is rank-1.

For instance, let A be a Hermitian operator on $\mathcal{H}$ whose spectral decomposition is given by

$$A = \sum_a a P_a \quad (2.5)$$

where a is an eigenvalue, and P_a is the corresponding projection. It is obvious that the function P given by $P(a) := P_a$ defines a PVM. In particular, if all P_a are rank-1, or equivalently, A is nondegenerate, then P is a rank-1 PVM. Thus, every Hermitian operator induces a PVM.

2.1.3 Channels

In this subsection, we formally define channels, and then introduce several types of channels.

To define channels, we need to introduce a few preliminary concepts. Let Λ be a linear map from $\mathcal{L}(\mathcal{H}_{\text{in}})$ to $\mathcal{L}(\mathcal{H}_{\text{out}})$ where $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ are Hilbert spaces.

Definition 2.1.6 (Positive map). The linear map Λ is said to be *positive* if and only if $\Lambda(A) \geq 0$ for every $A \geq 0$.

Definition 2.1.7 (Completely positive map). The linear map Λ is said to be *completely positive* if and only if $\text{id} \otimes \Lambda: \mathcal{L}(\mathcal{H}) \otimes \mathcal{L}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{L}(\mathcal{H}) \otimes \mathcal{L}(\mathcal{H}_{\text{out}})$ is positive for every finite-dimensional Hilbert space $\mathcal{H}$. Here, id denotes the identity map on $\mathcal{L}(\mathcal{H})$.

Definition 2.1.8 (Trace-preserving map). The linear map Λ is said to be *trace-preserving* if and only if $\text{tr}[\Lambda(A)] = \text{tr}[A]$ for every $A \in \mathcal{L}(\mathcal{H}_{\text{in}})$.

Using these definitions, a channel is defined as follows.

Definition 2.1.9 (Channel). A *channel* is a linear, completely positive, and trace-preserving map.

At first glance, it seems difficult to determine whether a given linear map is a channel or not. Fortunately, two useful necessary and sufficient conditions for a linear map to be a channel are known [19].

Proposition 2.1.10. *The following statements are equivalent.*

- The linear map Λ is a channel.
- The operator $J_\Lambda := (\text{id}_{\text{in}} \otimes \Lambda)(P'_+)$ referred to as the Choi operator of Λ is positive and satisfies $\text{tr}_{\text{out}}[J_\Lambda] = I_{\text{in}}$. Here, P'_+ is defined as

$$P'_+ := \sum_{i,j=0}^{d_{\text{in}}-1} |i\rangle\langle j| \otimes |i\rangle\langle j|. \quad (2.6)$$

- There is a family of linear operators $\{K_i\}_i$ such that $\Lambda(A) = \sum_i K_i A K_i^\dagger$ for every $A \in \mathcal{L}(\mathcal{H}_{\text{in}})$, and $\sum_i K_i^\dagger K_i = I_{d_{\text{in}}}$.

The second statement indicates that the positivity of J_Λ is not only necessary but also sufficient for Λ to be a channel. Recall that a linear operator is said to be positive if and only if it is Hermitian and has nonnegative eigenvalues. Thus, the second statement is equivalent to say that Λ is a channel if and only if all of the eigenvalues of J_Λ are nonnegative and $\text{tr}_{\text{out}}[J_\Lambda] = I_{\text{in}}$.

The third statement of Proposition 2.1.10 enables us to readily show that a linear map is a channel. For instance, we can prove the following corollary as a direct consequence of the third statement.

Corollary 2.1.11. *Let $\mathcal{H}_0$, $\mathcal{H}_1$, and $\mathcal{H}_2$ be Hilbert spaces. Let Λ_0 be a channel from $\mathcal{L}(\mathcal{H}_0)$ to $\mathcal{L}(\mathcal{H}_1)$, and let Λ_1 be a channel from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$. The composition of Λ_1 and Λ_0 , defined as $(\Lambda_1 \circ \Lambda_0)(A) := \Lambda_1(\Lambda_0(A))$ for every $A \in \mathcal{L}(\mathcal{H}_0)$, is also a channel.*

Proof. From the third statement of Proposition 2.1.10, there are families of linear operators such that

$$\Lambda_0(A) = \sum_i K_i^{(0)} A (K_i^{(0)})^\dagger \quad (2.7)$$

$$\Lambda_1(B) = \sum_j K_j^{(1)} B (K_j^{(1)})^\dagger \quad (2.8)$$

for every $A \in \mathcal{L}(\mathcal{H}_0)$ and $B \in \mathcal{L}(\mathcal{H}_1)$. Therefore, it holds that

$$(\Lambda_1 \circ \Lambda_0)(A) = \sum_{i,j} K_j^{(1)} K_i^{(0)} A (K_j^{(1)} K_i^{(0)})^\dagger. \quad (2.9)$$

The family $\{K_j^{(1)} K_i^{(0)}\}_{i,j}$ satisfies $\sum_{i,j} (K_j^{(1)} K_i^{(0)})^\dagger K_j^{(1)} K_i^{(0)} = I_0$, so that $\Lambda_1 \circ \Lambda_0$ is a channel again from the third statement of Proposition 2.1.10. $\square$

The composition $\Lambda_1 \circ \Lambda_0$ of channels Λ_1 and Λ_0 physically corresponds to the transformation that applies Λ_0 to a state, and then immediately applies Λ_1 to the output state.

Having defined what channels are, we introduce several typical types of channels.

Preparation of states

An extreme type of channel is those defined on $\mathbb{C}$. Physically, each channel from $\mathbb{C}$ to $\mathcal{L}(\mathcal{H})$, where $\mathcal{H}$ denotes a Hilbert space, is identified with a device for preparing a state on $\mathcal{H}$. For instance, a channel Λ on $\mathbb{C}$ serves as the preparation of a state $\Lambda(1)$. Furthermore, we can show the following proposition, from which states can also be understood as channels on $\mathbb{C}$.

Proposition 2.1.12. *There is a channel Λ such that $\Lambda(1) = \rho$ for every state ρ on a Hilbert space $\mathcal{H}$.*

Proof. Let λ_i and $|\psi_i\rangle$ respectively denote an eigenvalue and the corresponding normalized eigenvector for each $0 \leq i \leq d-1$, where d denotes the dimension of $\mathcal{H}$. The third statement of Proposition 2.1.10 ensures that the linear map $\Lambda: \mathbb{C} \rightarrow \mathcal{L}(\mathcal{H})$ defined as

$$\Lambda(\alpha) := \sum_{i=0}^{d-1} \sqrt{\lambda_i} |\psi_i\rangle \alpha \langle \psi_i| \sqrt{\lambda_i} \quad (2.10)$$

is a channel. It holds that $\Lambda(1) = \rho$ because of $\Lambda(\alpha) = \alpha\rho$. $\square$

Trace

Another extreme type of channel is those whose output spaces are $\mathbb{C}$. Physically, each channel from $\mathcal{L}(\mathcal{H})$, where $\mathcal{H}$ is a Hilbert space, to $\mathbb{C}$ is regarded as a transformation that discards any state on $\mathcal{H}$. The trace is an example of such channels, which is clear from its definition and the third statement of Proposition 2.1.10. In fact, the trace is the only channel from $\mathcal{L}(\mathcal{H})$ to $\mathbb{C}$.

Proposition 2.1.13. *It holds that $\Lambda = \text{tr}$ for every channel $\Lambda: \mathcal{L}(\mathcal{H}) \rightarrow \mathbb{C}$.*

Proof. Let Λ be a channel from $\mathcal{L}(\mathcal{H})$ to $\mathbb{C}$. For an $A \in \mathcal{L}(\mathcal{H})$, we have $\Lambda(A) = \alpha$ for some $\alpha \in \mathbb{C}$ because of the definition of Λ . The trace-preserving property of Λ implies

$$\text{tr}[A] = \text{tr}[\Lambda(A)] = \text{tr}[\alpha] = \alpha. \quad (2.11)$$

Consequently, it holds that $\Lambda(A) = \text{tr}[A]$ for every $A \in \mathcal{L}(\mathcal{H})$. $\square$

Depolarizing channels

Corollary 2.1.11 states that the composition of the preparation of a state and the trace is also a channel. Channels of this type are referred to as *depolarizing channels*, and formally defined as follows.

Definition 2.1.14 (Depolarizing channel). A channel $\Lambda: \mathcal{L}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{L}(\mathcal{H}_{\text{out}})$, where $\mathcal{H}_{\text{in}}$ and $\mathcal{H}_{\text{out}}$ are Hilbert spaces, is referred to as a *depolarizing channel* if and only if for every $A \in \mathcal{L}(\mathcal{H}_{\text{in}})$ it acts as

$$\Lambda(A) = \text{tr}[A] \rho \quad (2.12)$$

where ρ is a state on $\mathcal{H}_{\text{out}}$.

Every depolarizing channel can be interpreted as a transformation that discards the input state, and then prepares a new state as the output.

2.1.4 Random unitary channels

Of course, unitary evolutions, which describe transformations of states in a closed system, are also channels. Such channels are referred to as *unitary channels*, and formally defined as follows.

Definition 2.1.15 (Unitary channel). A linear map Λ is said to be a *unitary channel* if and only if there is a unitary operator U on a Hilbert space $\mathcal{H}$ such that

$$\Lambda(A) = UAU^\dagger, \quad (2.13)$$

where A is a linear operator on $\mathcal{H}$.

A convex combination of unitary channels is also a channel. We call such channels *random unitary channels*, and formally define them as follows.

Definition 2.1.16 (Random unitary channel). A channel Λ is said to be a *random unitary channel* if and only if there are a probability distribution $\{p_i\}$, i.e., a family of nonnegative numbers satisfying $\sum_i p_i = 1$, and a family of unitary operators $\{U_i\}_i$, each of which acts on a Hilbert space $\mathcal{H}$, such that

$$\Lambda(A) = \sum_i p_i U_i A U_i^\dagger, \quad (2.14)$$

where A is a linear operator on $\mathcal{H}$.

Random unitary channels are representative expressions of noise in quantum information processing. For instance, the linear map Λ defined as

$$\Lambda(\cdot) := p\sigma_1(\cdot)\sigma_1 + (1-p)\text{id}(\cdot) \quad (2.15)$$

where σ_1 is the first component of the Pauli operators, i.e.,

$$\sigma_1 = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (2.16)$$

is a model of bit-flip noise, which applies a bit-flip error, represented as σ_1 , to a state with the probability p , and leaves a state alone with the remaining probability $1-p$.

2.1.5 Entanglement breaking channels

Entangled states are crucial resources for quantum information protocols like quantum teleportation [20]. Therefore, it is of great interest to know whether a channel breaks entangled states, i.e., transforms entangled states into separable states, motivating the following definition.

Definition 2.1.17 (Entanglement breaking channel). A channel $\Lambda : \mathcal{L}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{L}(\mathcal{H}_{\text{out}})$ is referred to as an *entanglement breaking channel* if and only if $(\text{id} \otimes \Lambda)(\rho)$ is separable for every state ρ on $\mathcal{H} \otimes \mathcal{H}_{\text{in}}$ and every Hilbert space $\mathcal{H}$.

It seems difficult to determine whether a channel is entanglement breaking or not because the definition requires us to check the separability of $(\text{id} \otimes \Lambda)(\rho)$ for all ρ . Fortunately, it is known that we can verify the entanglement breaking property of a channel by examining its action to the maximally entangled state. Specifically, the following proposition holds [21].

Proposition 2.1.18. *A channel $\Lambda : \mathcal{L}(\mathcal{H}_{in}) \rightarrow \mathcal{L}(\mathcal{H}_{out})$ is entanglement breaking if and only if $(\text{id} \otimes \Lambda)(P_+) = J_\Lambda/d$ is separable.*

Thanks to this proposition, it is easily proven that several types of channels are entanglement breaking. For instance, a depolarizing channel Λ , which discards the input state and output a state ρ , is entanglement breaking because of $J_\Lambda = 1 \otimes \rho$.

Another typical example of entanglement breaking channel is a measure-and-prepare channel, which is interpreted as a transformation that measures an input state using a POVM, and then outputs a state depending on the obtained measurement outcome. To be more specific, a channel $\Lambda' : \mathcal{L}(\mathcal{H}_{in}) \rightarrow \mathcal{L}(\mathcal{H}_{out})$ is referred to as a *measure-and-prepare channel* if and only if it acts as follows for any linear operator A on $\mathcal{H}_{in}$:

$$\Lambda'(A) = \sum_{x \in \Omega} \text{tr}[\mathbf{E}(x)A] \tau_x \quad (2.17)$$

where $\mathbf{E}$ is a POVM defined on a set Ω , and τ_x is a state on $\mathcal{H}_{out}$ for each $x \in \Omega$. If a state ρ on $\mathcal{H}_{in}$ is input, then Λ' outputs τ_x with the probability $\text{tr}[\mathbf{E}(x)\rho]$. The map Λ' is indeed a channel, and this fact can be shown from the following equalities:

$$\Lambda'(A) = \sum_{x,i,j} (\sqrt{\lambda_{x,j}} |\psi_{x,j}\rangle \langle i| \sqrt{\mathbf{E}(x)}) A (\sqrt{\lambda_{x,j}} |\psi_{x,j}\rangle \langle i| \sqrt{\mathbf{E}(x)})^\dagger, \quad (2.18)$$

$$\sum_{x,i,j} (\sqrt{\lambda_{x,j}} |\psi_{x,j}\rangle \langle i| \sqrt{\mathbf{E}(x)})^\dagger \sqrt{\lambda_{x,j}} |\psi_{x,j}\rangle \langle i| \sqrt{\mathbf{E}(x)} = I_{in}, \quad (2.19)$$

where $\lambda_{x,j}$ denotes an eigenvalue of τ_x for each $x \in \Omega$, $|\psi_{x,j}\rangle$ represents the corresponding normalized eigenvector, and $\{|i\rangle\}_{i=0}^{d_{in}-1}$ is an orthonormal basis for $\mathcal{H}_{in}$. It is direct to verify that Λ' is entanglement breaking, from the separability of

$$\frac{J_{\Lambda'}}{d} = \sum_{x \in \{x \in \Omega : \mathbf{E}(x) \neq 0\}} \frac{\text{tr}[\mathbf{E}(x)]}{d} \frac{\mathbf{E}(x)^T}{\text{tr}[\mathbf{E}(x)]} \otimes \tau_x, \quad (2.20)$$

where $(\cdot)^T$ represents the transpose of a linear operator with respect to the orthonormal basis $\{|i\rangle\}_{i=0}^{d_{in}-1}$.

We note that every depolarizing channel is also a measure-and-prepare channel whose POVM is defined on a singleton, i.e., a set with a single element. Hence, the set of all entanglement breaking channels encompasses the set of all depolarizing channels.

2.1.6 Testers

This subsection describes testers [13], also known as process POVMs (PPOVMs) [14]. We introduce a scheme that is designed to measure channels, and then define a tester as a mathematical expression of this scheme. After discussing a general case, we provide two special types of schemes and the associated testers.

General testers

Let Λ be a channel which transforms states on a Hilbert space $\mathcal{H}_{\text{in}}$ into states on another Hilbert space $\mathcal{H}_{\text{out}}$. Measuring Λ means gaining information about Λ . More specifically, a measurement to probe Λ is performed as the following procedure:

1. Preparation of a state ρ on $\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{in}}$, where $\mathcal{H}_{\text{anc}}$ is the Hilbert space of an ancillary system.
2. Application of $\text{id}_{\text{anc}} \otimes \Lambda$ to ρ .
3. Execution of the measurement on the composite system $\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{out}}$ described by a POVM $\mathbf{E}: \Omega \rightarrow \mathcal{L}(\mathcal{H}_{\text{anc}}) \otimes \mathcal{L}(\mathcal{H}_{\text{out}})$.

The outcome of this measurement for Λ is that produced in the third step.

The measurement procedure can be interpreted as a device having a space into which a channel can be inserted. Each time this device runs, it supplies a state ρ to the inserted channel, performs a measurement $\mathbf{E}$ for the state, which the channel outputs, and as a result displays a measurement outcome with a probability.

Let $p(x|\Lambda)$ denote the probability of obtaining an outcome $x \in \Omega$. Clearly, $p(x|\Lambda)$ is given by

$$p(x|\Lambda) = \text{tr} [\mathbf{E}(x)(\text{id}_{\text{anc}} \otimes \Lambda)(\rho)]. \quad (2.21)$$

Although all the probabilities are computed using this formula in principle, the right-hand side of Eq. (2.21) can be rewritten as a more useful expression with the following lemma.

Lemma 2.1.19. *There is a unique completely positive map $\Upsilon_\rho: \mathcal{L}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{L}(\mathcal{H}_{\text{anc}})$ such that $(\Upsilon_\rho \otimes \text{id}_{\text{in}})(P'_+) = \rho$.*

Proof. Let $|\Psi\rangle$ be a unit vector in $\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{in}}$, and let K_Ψ be the linear operator from $\mathcal{H}_{\text{in}}$ to $\mathcal{H}_{\text{anc}}$ defined as

$$K_\Psi = \sum_{a=0}^{d_{\text{anc}}} \sum_{i=0}^{d_{\text{in}}-1} |a\rangle \langle a \otimes i | \Psi \rangle \langle i|, \quad (2.22)$$

where d_{anc} and d_{in} respectively denote the dimensions of $\mathcal{H}_{\text{anc}}$ and $\mathcal{H}_{\text{in}}$. It is easy to see that

$$(\Upsilon_\Psi \otimes \text{id}_{\text{in}})(P'_+) = |\Psi\rangle \langle \Psi|, \quad (2.23)$$

where Υ_Ψ is the completely positive map defined as $\Upsilon_\Psi(A) = K_\Psi A K_\Psi^\dagger$ for every $A \in \mathcal{L}(\mathcal{H}_{\text{in}})$.

Let $\{\lambda_j\}_{j=0}^{d_{\text{anc}}d_{\text{in}}-1}$ be the eigenvalues of ρ , and let $\{|\Psi_j\rangle\}_{j=0}^{d_{\text{anc}}d_{\text{in}}-1}$ be the corresponding eigenvectors of ρ , i.e., $\rho|\Psi_j\rangle = \lambda_j|\Psi_j\rangle$. We have

$$(\Upsilon_\rho \otimes \text{id}_{\text{in}})(P'_+) = \rho, \quad (2.24)$$

where $\Upsilon_\rho := \sum_{j=0}^{d_{\text{anc}}d_{\text{in}}-1} \lambda_j \Upsilon_{\Psi_j}$. This map is uniquely determined because $\Upsilon_\rho = \Upsilon'_\rho$ is implied if a linear map Υ'_ρ satisfies $(\Upsilon'_\rho \otimes \text{id}_{\text{in}})(P'_+) = \rho$. $\square$

Consequently, the probability $p(x|\Lambda)$ can be expressed as follows.

Proposition 2.1.20. *It holds that*

$$p(x|\Lambda) = \text{tr}[S(x)J_\Lambda]. \quad (2.25)$$

Here, S is the function from Ω to $\mathcal{L}(\mathcal{H}_{\text{in}}) \otimes \mathcal{L}(\mathcal{H}_{\text{out}})$ defined as

$$S(x) = (\Upsilon_\rho^* \otimes \text{id}_{\text{out}})(E(x)) \quad (2.26)$$

where Υ_ρ^* is the dual map of Υ_ρ given by Lemma 2.1.19.

Proof. The assertion can be shown from the following equalities:

$$p(x|\Lambda) = \text{tr}[E(x)(\text{id}_{\text{anc}} \otimes \Lambda)(\rho)] \quad (2.27)$$

$$= \text{tr}[E(x)(\text{id}_{\text{anc}} \otimes \Lambda)(\Upsilon_\rho \otimes \text{id}_{\text{in}})(P'_+)] \quad (2.28)$$

$$= \text{tr}[E(x)(\Upsilon_\rho \otimes \text{id}_{\text{out}})(\text{id}_{\text{in}} \otimes \Lambda)(P'_+)] \quad (2.29)$$

$$= \text{tr}[(\Upsilon_\rho^* \otimes \text{id}_{\text{out}})(E(x))(\text{id}_{\text{in}} \otimes \Lambda)(P'_+)] \quad (2.30)$$

$$= \text{tr}[S(x)J_\Lambda]. \quad (2.31)$$

$\square$

An advantage of Eq. (2.25) is that Λ is expressed as its Choi operator J_Λ , and thereby useful tools, like the spectral decomposition of J_Λ , can be applied.

Another advantage of Eq. (2.25) is that the information about ρ and E , which are used to measure Λ , is packed into S . As stated earlier, the measurement procedure can be understood as a device, which supplies the ρ to channel and then performs a measurement E on the output state. Thus, S can be interpreted as a mathematical representation of this device.

In Eq. (2.25), S exhibits behavior analogous to the POVM in Eq. (2.4). In fact, S is called a *tester* or *process POVM (PPOVM)*. A crucial difference between a POVM and a tester (or a PPOVM) lies in the normalization conditions; while the sum of all values of a POVM coincides with the identity operator, the sum of all values of a tester is in general not equal to the identity operator. Indeed, using $\Upsilon_\rho^*(I_{\text{anc}}) = \rho_{\text{in}}^T$, where $\rho_{\text{in}} := \text{tr}_{\text{anc}} \rho$, we obtain $\sum_{x \in \Omega} S(x) = \rho_{\text{in}}^T \otimes I_{\text{out}}$, and its right-hand side is not equal to the identity operator if and only if $d_{\text{in}} > 1$. Formally, a tester or PPOVM is defined as follows.

Definition 2.1.21 (Tester). Let Ω be a finite set, and let S be a function from Ω to $\mathcal{L}(\mathcal{H}_{\text{in}}) \otimes \mathcal{L}(\mathcal{H}_{\text{out}})$. The function S is said to be a *tester* or *process POVM (PPOVM)* if and only if $S(x) \geq 0$ for every $x \in \Omega$ and $\sum_{x \in \Omega} S(x) = \rho_{\text{in}}^T \otimes I_{\text{out}}$ where ρ_{in} is a state on $\mathcal{L}(\mathcal{H}_{\text{in}})$.

Testers play central roles in this paper. In the following, we introduce typical types of testers for later chapters.

Ancilla-free testers

A tester of a measurement procedure that does not utilize the correlation induced by an ancillary system is referred to as an *ancilla-free tester*. A typical ancilla-free tester is given by choosing $\mathcal{H}_{\text{anc}} = \mathbb{C}$. In this setting, the state and POVM can be written as

$$\rho = 1 \otimes \rho_{\text{in}}, \quad (2.32)$$

$$E(x) = 1 \otimes E_{\text{out}}(x) \quad (2.33)$$

where ρ_{in} is a state on $\mathcal{H}_{\text{in}}$, and $\{E_{\text{out}}(x)\}_{x \in \Omega}$ is a POVM whose range is $\mathcal{L}(\mathcal{H}_{\text{out}})$. Equation (2.26) implies

$$S(x) = \rho_{\text{in}}^T \otimes E_{\text{out}}(x) \quad (2.34)$$

for each $x \in \Omega$.

Every measurement on states, described by a POVM, can be regarded as an ancilla-free measurement on preparation channels, i.e., channels from $\mathbb{C}$ to $\mathcal{L}(\mathcal{H}_{\text{out}})$. Indeed, if $\mathcal{H}_{\text{anc}} = \mathcal{H}_{\text{in}} = \mathbb{C}$, $S(x)$ and J_Λ become

$$S(x) = 1 \otimes E_{\text{out}}(x), \quad (2.35)$$

$$J_\Lambda = 1 \otimes \rho_{\text{out}}, \quad (2.36)$$

which are respectively identified with E_{out} and the prepared state $\rho_{\text{out}} := \Lambda(1)$. Furthermore, the probability $p(x|\Lambda)$, given by Eq. (2.25), becomes

$$p(x|\Lambda) = \text{tr}[E_{\text{out}}(x)\rho_{\text{out}}], \quad (2.37)$$

whose right-hand is equal to that of Eq. (2.4). Thus, the concept of tester generalizes that of POVM, and Eq. (2.25), a formula for calculating a probability, can be considered an extension of the Born rule, expressed as Eq. (2.4).

Testers induced by maximally entangled input states

Other typical examples of testers are those associated with measurements on channels in which maximally entangled states are employed as their input states. Let $\mathcal{H}_{\text{anc}} = \mathcal{H}_{\text{in}}$, and let $\rho = |\Psi\rangle\langle\Psi|$ where $|\Psi\rangle$ is a maximally entangled state in $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{in}}$. In this case, Eq. (2.26) implies

$$S(x) = \frac{1}{d}(U^\dagger \otimes I_{\text{out}})E(x)(U \otimes I_{\text{out}}), \quad (2.38)$$

where U is the unitary operator given by $|\Psi\rangle = (U \otimes I_{\text{in}})|\Psi_+\rangle$.

Investigating how a channel transforms maximally entangled states is a crucial task. This is because maximally entangled states play prominent roles in several quantum information schemes, like quantum teleportation [20]. Thus, measurement devices implemented by maximally entangled input states serve as basic tools for performing such investigations.

2.2 Uncertainty Relations

In this section, we describe two notions of uncertainty relation. First, uncertainty relations for measurements of states are briefly reviewed, and then those for measurements of channels, derived in Ref. [12], are presented.

2.2.1 Uncertainty relations for measurements of states

Robertson's uncertainty relation

In a nutshell, any mathematical object expressing a restriction on probability distributions is referred to as an *uncertainty relation*. First, we explain Robertson's inequality, because it is described in most textbooks on quantum mechanics and hence considered a natural starting point for the review of uncertainty relations.

Let $\mathcal{H}$ be a Hilbert space of dimension d , let A and B be Hermitian operators on $\mathcal{H}$, and let $|\psi\rangle$ be a unit vector in $\mathcal{H}$. Robertson's uncertainty relation is expressed as the following proposition [4].

Proposition 2.2.1. *The following inequality holds:*

$$\Delta_{|\psi\rangle}A \cdot \Delta_{|\psi\rangle}B \geq \frac{1}{2}|\langle\psi|[A, B]|\psi\rangle|, \quad (2.39)$$

where $\Delta_{|\psi\rangle}X$ denotes the standard deviation of a Hermitian operator X defined as $\Delta_{|\psi\rangle}X := \sqrt{\langle\psi|X^2|\psi\rangle - \langle\psi|X|\psi\rangle^2}$, and $[A, B]$ is the commutator of A and B defined as $[A, B] := AB - BA$.

Equation (2.39) induces a restriction on the probability distributions of A and B , and thereby reveals a fundamental difference between the quantum and classical worlds. Specifically, by letting $A = X$ and $B = P$, where X and P respectively denote the position and momentum of a particle, we obtain

$$\Delta_{|\psi\rangle}X \cdot \Delta_{|\psi\rangle}P \geq \frac{\hbar}{2}, \quad (2.40)$$

because X and P satisfy the canonical commutation relation, i.e., $[X, P] = i\hbar I$ (this example is the only case in this thesis that involves an infinite-dimensional Hilbert space). The standard deviation represents the spread of a probability distribution. Therefore, Eq. (2.40) provides the significant physical implication that the probability distributions of the position and momentum cannot be sharpened at the same time in the quantum world. This conflicts with a naive intuition that the position and momentum have fixed values at each point in time, on which classical mechanics relies. Thus, Robertson's uncertainty relation, expressed as Eq. (2.39), is regarded as an inequality characterizing quantum theory.

However, there is a non-negligible drawback in Robertson's inequality. Specifically, the dependency of the right-hand side of Eq. (2.39) on $|\psi\rangle$ becomes a problem if Eq. (2.39) is applied to Hermitian operators on a finite-dimensional system. For instance, let us suppose that $\mathcal{H}$ is a two-dimensional Hilbert space with an orthonormal basis $\{|0\rangle, |1\rangle\}$, and the Hermitian operators are respectively given by $A = \sigma_1$ and $B = \sigma_3$, where σ_1 and σ_3 respectively denote the first and third Pauli operators, defined as

$$\sigma_1 := |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (2.41)$$

$$\sigma_2 := (-i)|0\rangle\langle 1| + i|1\rangle\langle 0|, \quad (2.42)$$

$$\sigma_3 := |0\rangle\langle 0| - |1\rangle\langle 1|. \quad (2.43)$$

If $|\psi\rangle = |0\rangle$, which is an eigenvector of σ_3 , Eq. (2.39) becomes

$$\Delta_{|\psi\rangle}\sigma_1 \cdot \Delta_{|\psi\rangle}\sigma_3 \geq 0. \quad (2.44)$$

This inequality is trivial because the standard deviations are nonnegative by definition. Although the probability distribution of σ_1 cannot be deterministic (in fact, it is the uniform distribution), Eq. (2.44) does not reflect this restriction.

Furthermore, it is not necessary to use the standard deviation to establish uncertainty relations. In fact, the standard deviation of a probability distribution depends on the values of outcomes, and therefore cannot be considered a perfect measure of uncertainty. For instance, let us imagine a fair coin whose heads and tails are marked 1 and -1 , respectively. While the standard deviation of this coin is 1, it changes into 2 when the values of the heads and tails are rewritten as 2 and -2 , respectively. Thus, the standard deviation can change by rewriting the values assigned to the heads and tails, although the uncertainty related to a coin flip is invariant under such a relabeling.

The drawbacks of Robertson's inequality have motivated researchers to seek alternative formulations of uncertainty relations. In the following, we describe three types of uncertainty relations, each of which serves as such a contemporary formulation.

Entropic uncertainty relations

In Ref. [5], Deutsch pointed out the shortcomings of Robertson's inequality, stated above, and derived an uncertainty relation using the Shannon entropy,

which is defined for a probability distribution $\{p(x)\}_{x \in \Omega}$ as follows:

$$H(p) := - \sum_{x \in \text{supp}(p)} p(x) \ln p(x), \quad (2.45)$$

where $\text{supp}(p) := \{x \in \Omega : p(x) \neq 0\}$. As a basic property, $H(p)$ satisfies $0 \leq H(p) \leq \ln |\Omega|$, in which $H(p) = 0$ if and only if $p(x) = 1$ for some $x \in \Omega$, and $H(p) = \ln |\Omega|$ if and only if $p(x) = \frac{1}{|\Omega|}$. Furthermore, the Shannon entropy is invariant under a relabeling of outcomes, unlike the standard deviation. To see this, let $\{p'(x')\}_{x' \in \Omega'}$ be a probability distribution such that $p = p' \circ f$, where $f: \Omega \rightarrow \Omega'$ is a bijective function representing a relabeling. Clearly, it holds that $H(p') = H(p)$. Thus, the Shannon entropy is considered a suitable measure to quantify the uncertainty of a probability distribution.

Deutsch's inequality is expressed as follows [5].

Proposition 2.2.2. *Let Ω_1 and Ω_2 be finite sets respectively specified by $\Omega_1 := \{x_0, \dots, x_{d-1}\}$ and $\Omega_2 := \{y_0, \dots, y_{d-1}\}$, and let $\mathbf{P}: \Omega_1 \rightarrow \mathcal{L}(\mathcal{H})$ and $\mathbf{Q}: \Omega_2 \rightarrow \mathcal{L}(\mathcal{H})$ be rank-1 PVMs respectively given by $\mathbf{P}(x_i) = |e_i\rangle\langle e_i|$ and $\mathbf{Q}(y_j) = |f_j\rangle\langle f_j|$, where $\{|e_i\rangle\}_{i=0}^{d-1}$ and $\{|f_j\rangle\}_{j=0}^{d-1}$ are orthonormal bases for $\mathcal{H}$. Then, the following inequality holds:*

$$H(p) + H(q) \geq -2 \ln \left[\frac{1 + \max_{i,j} |\langle e_i | f_j \rangle|}{2} \right], \quad (2.46)$$

where p and q are the probability distributions of the measurements described by $\mathbf{P}$ and $\mathbf{Q}$ on a state $|\psi\rangle \in \mathcal{H}$, i.e., they are given by $p(x_i) = |\langle e_i | \psi \rangle|^2$ and $q(y_j) = |\langle f_j | \psi \rangle|^2$, respectively.

Note that the bound of Eq. (2.46) does not depend on the state $|\psi\rangle$, unlike Robertson's inequality, given by Eq. (2.39). Because of this, Eq. (2.46) implies that if $\max_{i,j} |\langle e_i | f_j \rangle| < 1$, $H(p)$ and $H(q)$ cannot be 0 simultaneously, or equivalently, p and q cannot be deterministic simultaneously. For instance, if $d = 2$ and $|\langle e_i | f_j \rangle| = \frac{1}{\sqrt{2}}$, then the right-hand side of Eq. (2.46) becomes positive, imposing a nontrivial restriction on p and q , which Robertson's inequality fails to capture.

Equation (2.46) has undergone various improvements so far. Maassen and Uffink refined Eq. (2.46) in Ref. [22], Krishna and Parthasarathy extended the Maassen–Uffink inequality in Ref. [23] so that an arbitrary pair of POVMs can be applied to it, and Rastegin generalized the Krishna–Parthasarathy inequality by employing the Rényi entropy as a measure of

uncertainty in Ref. [24]. The Rényi entropy of a probability distribution p is a function of p with a nonnegative parameter $0 \leq \alpha \leq \infty$. Specifically, it is defined as

$$H_\alpha(p) := \frac{1}{1-\alpha} \ln \left(\sum_{x \in \Omega} p(x)^\alpha \right) \quad (2.47)$$

for $\alpha \notin \{0, 1, \infty\}$ and as the limits of the right-hand side for $\alpha \in \{0, 1, \infty\}$ [25]. In particular, $H_1(p)$ coincides with $H(p)$ for all probability distributions p , indicating that the Rényi entropy is a generalization of the Shannon entropy. The uncertainty relation obtained by Rastegin is expressed as the following proposition [24].

Proposition 2.2.3. *Let Ω_1 and Ω_2 be finite sets respectively characterized by $\Omega_1 := \{x_0, \dots, x_{M-1}\}$ and $\Omega_2 := \{y_0, \dots, y_{N-1}\}$, where M and N are nonnegative integers, and let $E: \Omega_1 \rightarrow \mathcal{L}(\mathcal{H})$ and $F: \Omega_2 \rightarrow \mathcal{L}(\mathcal{H})$ be POVMs. Then, the following inequality holds:*

$$H_\alpha(p) + H_\beta(q) \geq -2 \ln \max_{i,j} \|E(x_i)^{1/2} F(y_j)^{1/2}\|. \quad (2.48)$$

Here, α and β are positive numbers such that $\alpha, \beta \neq 1$ and $\frac{1}{\alpha} + \frac{1}{\beta} = 2$, and p and q denote the probability distributions of the measurements described by E and F on a state $\rho \in \mathcal{L}(\mathcal{H})$, i.e., they are given by $p(x_i) = \text{tr}[E(x_i)\rho]$ and $q(y_j) = \text{tr}[F(y_j)\rho]$, respectively.

By taking the limit $\alpha \rightarrow 1$ in Eq. (2.48), we obtain the following corollary.

Corollary 2.2.4. *Under the hypotheses of Proposition 2.2.3, the following inequality holds:*

$$H(p) + H(q) \geq -2 \ln \max_{i,j} \|E(x_i)^{1/2} F(y_j)^{1/2}\|. \quad (2.49)$$

In particular, if $M = N = d$, $E(x_i) = |e_i\rangle\langle e_i|$ for $i \in \{0, \dots, d-1\}$, and $F(y_j) = |f_j\rangle\langle f_j|$ for all $j \in \{0, \dots, d-1\}$, where $\{|e_i\rangle\}_{i=0}^{d-1}$ and $\{|f_j\rangle\}_{j=0}^{d-1}$ are orthonormal bases, then the inequality becomes

$$H(p) + H(q) \geq -2 \ln \max_{i,j} |\langle e_i | f_j \rangle|. \quad (2.50)$$

Equations (2.49) and (2.50) are the Krishna–Parthasarathy and Maassen–Uffink inequalities, respectively. It is clear that Eq. (2.50) is stronger than Eq. (2.46).

Majorization uncertainty relations

Uncertainty relations formulated with majorization, referred to as *majorization uncertainty relations*, serve as other modern expressions for quantifying the restrictions imposed on probability distributions [7, 8, 9, 10]. Majorization is a preorder on a set of real vectors, and is defined as follows [26].

Definition 2.2.5 (Majorization). Let $\mathbf{x}$ and $\mathbf{y}$ be real vectors of dimension d , and let $\mathbf{x}^\downarrow$ and $\mathbf{y}^\downarrow$ be the real vectors given by arranging the components of $\mathbf{x}$ and $\mathbf{y}$ in decreasing order, respectively. We say that $\mathbf{x}$ is *majorized by* $\mathbf{y}$ if and only if

$$\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow \quad (2.51)$$

for every $1 \leq k \leq d-1$, and

$$\sum_{i=1}^d x_i^\downarrow = \sum_{i=1}^d y_i^\downarrow. \quad (2.52)$$

We write $\mathbf{x} \prec \mathbf{y}$ to denote that $\mathbf{x}$ is majorized by $\mathbf{y}$, and call $\mathbf{x} \prec \mathbf{y}$ a *majorization relation*.

A majorization relation $\mathbf{x} \prec \mathbf{y}$, where $\mathbf{x}$ and $\mathbf{y}$ are real vectors, indicates that $\mathbf{x}$ is flatter than $\mathbf{y}$. For instance, it follows that $(1/d, \dots, 1/d) \prec \mathbf{p} \prec (1, 0, \dots, 0)$ for all probability vectors $\mathbf{p}$ of dimension d . This relation is consistent with our intuition that $(1/d, \dots, 1/d)$ and $(1, 0, \dots, 0)$ are respectively considered the flattest and least flat probability vectors. Furthermore, majorization is closely related to information entropies through the notion of Schur-concave function. Here, a function $f: \mathbb{R}^d \rightarrow \mathbb{R}$, where d is a positive integer, is said to be *Schur-concave* if and only if $f(\mathbf{x}) \geq f(\mathbf{y})$ whenever $\mathbf{x} \prec \mathbf{y}$ for all real vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{R}^d$. For example, the Rényi entropy is a Schur-concave function, and hence each majorization relation for probability vectors induces a Rényi entropic inequality. Thus, majorization provides a stronger criterion for comparing the flatness of two real vectors than any Schur-concave functions, including the Rényi entropy.

A type of majorization uncertainty relation is given by the following proposition [7, 8, 9].

Proposition 2.2.6. *Let Ω_1 and Ω_2 be finite sets respectively specified by $\Omega_1 := \{x_1, \dots, x_M\}$ and $\Omega_2 := \{y_1, \dots, y_N\}$, where M and N are positive integers. Let ρ be a state on $\mathcal{H}$, and let $\mathbf{E}: \Omega_1 \rightarrow \mathcal{L}(\mathcal{H})$ and $\mathbf{F}: \Omega_2 \rightarrow \mathcal{L}(\mathcal{H})$ be POVMs. Then, the following majorization relation holds:*

$$\mathbf{p} \otimes \mathbf{q} \prec \mathbf{b}_\otimes \quad (2.53)$$

where $\mathbf{p}$ and $\mathbf{q}$ denote the probability vectors given by $p_i := \text{tr}[\mathbf{E}(x_i)\rho]$ and $q_j := \text{tr}[\mathbf{F}(y_j)\rho]$ for all $i \in \{1, \dots, M\}$ and $j \in \{1, \dots, N\}$, respectively. The vector $\mathbf{b}_\otimes$ in the right-hand side is a probability vector of dimension MN whose elements are defined as

$$b_{\otimes, k} := s_{\otimes, k} - s_{\otimes, k-1} \quad (2.54)$$

for all $k \in \{1, \dots, MN\}$. Here, the quantities in the right-hand side are given by $s_{\otimes, 0} := 0$, and

$$s_{\otimes, k} := \max_{\substack{\mathcal{K} \subseteq \{1, \dots, M\} \times \{1, \dots, N\} \\ |\mathcal{K}| = k}} \max_{\rho} \sum_{(i, j) \in \mathcal{K}} p_i q_j \quad (2.55)$$

for all $k \in \{1, \dots, MN\}$.

Equation (2.53) indicates that the probability vector $\mathbf{p} \otimes \mathbf{q}$ must be flatter than the state-independent vector $\mathbf{b}_\otimes$ in the sense of majorization. In particular, it implies that if $\mathbf{b}_\otimes$ is not deterministic, i.e., $\mathbf{b}_\otimes^\downarrow \neq (1, 0, \dots, 0)$, then $\mathbf{p}$ and $\mathbf{q}$ cannot be deterministic simultaneously for all states.

Another type of majorization uncertainty relation is given by the following proposition [10].

Proposition 2.2.7. *Under the same hypotheses in Proposition 2.2.6, the following majorization relation holds:*

$$\mathbf{p} \oplus \mathbf{q} \prec \mathbf{b}_\oplus \quad (2.56)$$

where $\mathbf{b}_\oplus$ is a vector of dimension $M + N$ whose elements are defined as

$$b_{\oplus, k} := s_{\oplus, k} - s_{\oplus, k-1} \quad (2.57)$$

for all $k \in \{1, \dots, M + N\}$. Here, $s_{\oplus, k}$ are given by $s_{\oplus, 0} := 0$, and

$$s_{\oplus, k} := \max_{\substack{\mathcal{I}, \mathcal{J} \\ |\mathcal{I}| + |\mathcal{J}| = k}} \max_{\rho} \left\{ \sum_{i \in \mathcal{I}} p_i + \sum_{j \in \mathcal{J}} q_j \right\} \quad (2.58)$$

for all $k \in \{1, \dots, M + N\}$.

Similar to Eq. (2.53), Eq. (2.56) implies that if $\mathbf{b}_{\oplus}^{\downarrow} \neq (1, 1, 0, \dots, 0)$ holds, then $\mathbf{p}$ or $\mathbf{q}$ must be non-deterministic for all states.

Thus, the majorization uncertainty relations, given by Eqs. (2.53) and (2.56), express the uncertainty trade-off between $\mathbf{p}$ and $\mathbf{q}$ through the state-independent vectors, like entropic uncertainty relations. Furthermore, Eqs. (2.53) and (2.56) are by definition equivalent to sets of inequalities, thereby imposing multiple restrictions on the probability vectors $\mathbf{p}$ and $\mathbf{q}$. As a consequence, Eqs. (2.53) and (2.56) induce strong entropic inequalities [7, 8, 9, 10].

Fine-grained uncertainty relations

Finally, we introduce the concept of *fine-grained uncertainty relations*. In general, some expression imposing a restriction for each combination of the probabilities associated with measurements on a state is referred to as a fine-grained uncertainty relation. Oppenheim and Wehner devised the following set of inequalities as a fine-grained uncertainty relation [11]:

$$\mathcal{U} := \left\{ \sum_{l=1}^L r_l p_l(x^{(l)}|\rho) \leq b(\mathbf{x}) : \mathbf{x} := (x^{(1)}, \dots, x^{(L)}) \in \prod_{l=1}^L \Omega_l \right\} \quad (2.59)$$

where L is a positive integer, $\{r_l\}_{l=1}^L$ is a probability distribution, and ρ is a state on $\mathcal{H}$. For each $l \in \{1, \dots, L\}$, $p_l(x^{(l)}|\rho)$ denotes the probability of obtaining an outcome $x^{(l)}$ in a subset Ω_l when the measurement described by a POVM $\mathbf{E}^{(l)} : \Omega_l \rightarrow \mathcal{L}(\mathcal{H})$ is performed on ρ . The bound is given by

$$b(\mathbf{x}) := \max_{\rho} \sum_{l=1}^L r_l p_l(x^{(l)}|\rho) \quad (2.60)$$

$$= \left\| \sum_{l=1}^L r_l \mathbf{E}^{(l)}(x^{(l)}) \right\|, \quad (2.61)$$

where $\|\cdot\|$ denotes the operator norm defined for each $A \in \mathcal{L}(\mathcal{H})$ as

$$\|A\| := \max_{\substack{|\psi\rangle \in \mathcal{H} \\ \|\psi\| \neq 0}} \frac{\|A\psi\|}{\|\psi\|}. \quad (2.62)$$

Equation (2.59) indeed forms a fine-grained uncertainty relation because each element in $\mathcal{U}$ imposes a restriction on the probabilities

$$p_1(x^{(1)}|\rho), \dots, p_L(x^{(L)}|\rho) \quad (2.63)$$

for an outcome combination $\mathbf{x} = (x^{(1)}, \dots, x^{(L)}) \in \prod_{l=1}^L \Omega_l$ through the state-independent quantity $b(\mathbf{x})$. To be more specific, if the strict inequality

$$b(\mathbf{x}) < \sum_{l=1}^L r_l \max_{\rho} p_l(x^{(l)}|\rho) \quad (2.64)$$

holds, then the probabilities in Eq. (2.63) cannot be maximized at the same time, meaning that a nontrivial restriction on the probability distributions exists [27].

Furthermore, each inequality in $\mathcal{U}$ has a clear operational meaning in the scheme where a state ρ is stochastically measured using one of the POVMs $\mathbf{E}^{(1)}, \dots, \mathbf{E}^{(L)}$ according to the probability distribution $\{r_l\}_{l=1}^L$. Specifically, the left-hand side of the inequality in Eq. (2.59) represents the probability of obtaining one of the outcomes in an $\mathbf{x} \in \prod_{l=1}^L \Omega_l$, while the right-hand side, i.e., $b(\mathbf{x})$, gives the maximum of this probability, optimized with respect to states. Thus, the fine-grained uncertainty relation, expressed as $\mathcal{U}$, is considered a reasonable formulation for expressing restrictions on the probability distributions $p_1, \dots, p_L$.

Equation (2.59) quantifies how large probabilities $p_1(x^{(1)}|\rho), \dots, p_L(x^{(L)}|\rho)$ can be at the same time for every $\mathbf{x} \in \prod_{l=1}^L \Omega_l$. For instance, if $L = 2$, $r_1 = r_2 = \frac{1}{2}$, and $\mathbf{E}^{(l)}(x_i^{(l)}) = |e_i^{(l)}\rangle\langle e_i^{(l)}|$ where $\{|e_i^{(l)}\rangle\}_{i=0}^{d-1}$ are orthonormal bases, the uncertainty bound is given by

$$b(\mathbf{x}) = \frac{1}{2} \left(1 + |\langle e_i^{(1)} | e_j^{(2)} \rangle| \right) \quad (2.65)$$

for all $\mathbf{x} \in \Omega_1 \times \Omega_2$, indicating that the probabilities $p_1(x_i^{(1)}|\rho)$ and $p_2(x_j^{(2)}|\rho)$ cannot be unity if $|\langle e_i^{(1)} | e_j^{(2)} \rangle| < 1$ [28, 29, 30]. In particular, if $\{|e_i^{(1)}\rangle\}_{i=0}^{d-1}$ and $\{|e_j^{(2)}\rangle\}_{j=0}^{d-1}$ are mutually unbiased, i.e., $|\langle e_i^{(1)} | e_j^{(2)} \rangle| = \frac{1}{\sqrt{d}}$ holds for every $i, j \in \{0, \dots, d-1\}$, then the bound becomes

$$b(\mathbf{x}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{d}} \right), \quad (2.66)$$

meaning that $p_1(x_i^{(1)}|\rho)$ and $p_2(x_j^{(2)}|\rho)$ cannot be large simultaneously and a nontrivial trade-off between $p_1(x_i^{(1)}|\rho)$ and $p_2(x_j^{(2)}|\rho)$ exists for every $i, j \in \{0, \dots, d-1\}$.

It is a significant advantage of $\mathcal{U}$ that it imposes a restriction on probabilities for each outcome combination. Thanks to this feature, $\mathcal{U}$ can express nontrivial uncertainty trade-offs that the entropic and majorization-based uncertainty relations cannot capture. For instance, let us consider the following case:

$$d = 3, \quad (2.67)$$

$$L = 2, \quad (2.68)$$

$$\mathbf{E}^{(1)}(x_i^{(1)}) = |i\rangle \langle i|, \quad (2.69)$$

$$\mathbf{E}^{(2)}(x_j^{(2)}) = |\tilde{j}\rangle \langle \tilde{j}| \quad (2.70)$$

where $\{|\tilde{j}\rangle\}_{j \in [2]}$ is defined as

$$|\tilde{j}\rangle := \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^j |1\rangle) & (j \in \{0, 1\}) \\ |2\rangle & (j = 2) \end{cases}. \quad (2.71)$$

Then, we obtain

$$b(x_i^{(1)}, x_j^{(2)}) = \begin{cases} \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}}\right) & (i, j \in \{0, 1\}) \\ \frac{1}{2} & (i = 2, j \in \{0, 1\} \text{ or } i \in \{0, 1\}, j = 2) \\ 1 & (i = j = 2) \end{cases}, \quad (2.72)$$

implying that a nontrivial upper limitation on

$$\frac{1}{2}p_1(x_i^{(1)}|\rho) + \frac{1}{2}p_2(x_j^{(2)}|\rho) \quad (2.73)$$

exists for each $(x_i^{(1)}, x_j^{(2)}) \in (\Omega_1 \times \Omega_2) \setminus \{(x_2^{(1)}, x_2^{(2)})\}$. In contrast to this, Eq. (2.48) becomes

$$H_\alpha(p_1) + H_\beta(p_2) \geq 0, \quad (2.74)$$

which is trivial because the Rényi entropies are nonnegative by definition. Similarly, the majorization uncertainty relations, given by Eqs. (2.53) and (2.56), become the following trivial expressions:

$$\mathbf{p}_1 \otimes \mathbf{p}_2 \prec (1, 0, \dots, 0), \quad (2.75)$$

$$\mathbf{p}_1 \oplus \mathbf{p}_2 \prec (2, 0, \dots, 0), \quad (2.76)$$

where $\mathbf{p}_1$ and $\mathbf{p}_2$ denote the probability vectors gained by collecting the probability distributions p_1 and p_2 , respectively. Thus, $\mathcal{U}$ possesses a unique strength, which is not found in the entropic and majorization-based uncertainty relations.

It should be noted that, if $r_l = \frac{1}{L}$ for all $l \in \{1, \dots, L\}$, then $\mathcal{U}$ is identified with the generalized Landau–Pollak uncertainty relation, which was devised in Ref. [28] before the concept of fine-grained uncertainty relations was proposed in Ref. [11].

2.2.2 Uncertainty relations for measurements of channels

We described several types of uncertainty relations in the previous subsection. They impose restrictions on probability distributions, and thereby expressing a kind of impossibility in quantum theory. However, these uncertainty relations can be applied to only measurements of states, expressed as POVMs. As stated previously, measurements of channels, including states, can be described using the concept of testers. Thus, it is natural to extend uncertainty relations for POVMs, such as those presented in the above subsection, by means of testers.

Xiao et al. pioneered this direction of study in Ref. [12], and derived three forms of uncertainty relations for testers. Let us consider two measurements for probing channels that transform states on a Hilbert space $\mathcal{H}_{\text{in}}$ into states on another Hilbert space $\mathcal{H}_{\text{out}}$. Let $\Omega_1 := \{x_1, \dots, x_M\}$ and $\Omega_2 := \{y_1, \dots, y_N\}$ respectively denote the sets of measurement outcomes with the cardinalities M and N , and let $\mathbf{S}: \Omega_1 \rightarrow \mathcal{L}(\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}})$ and $\mathbf{T}: \Omega_2 \rightarrow \mathcal{L}(\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}})$ be the associated testers satisfying the following normalization conditions:

$$\sum_{i=1}^M \mathbf{S}(x_i) = \rho_{\text{in}}^T \otimes I_{\text{out}}, \quad (2.77)$$

$$\sum_{j=1}^N \mathbf{T}(y_j) = \sigma_{\text{in}}^T \otimes I_{\text{out}}, \quad (2.78)$$

where ρ_{in} and σ_{in} are states on $\mathcal{H}_{\text{in}}$. Let Λ be a channel from $\mathcal{L}(\mathcal{H}_{\text{in}})$ to $\mathcal{L}(\mathcal{H}_{\text{out}})$, and let $\mathbf{p}$ and $\mathbf{q}$ respectively denote the probability vectors corre-

sponding to $\mathbf{S}$ and $\mathbf{T}$, i.e.,

$$p_i = p(x_i|\Lambda) = \text{tr} [\mathbf{S}(x_i)J_\Lambda], \quad (2.79)$$

$$q_j = q(y_j|\Lambda) = \text{tr} [\mathbf{T}(y_j)J_\Lambda]. \quad (2.80)$$

The uncertainty relations for testers obtained by Xiao et al. are expressed as the following propositions [12].

Proposition 2.2.8. *The following inequality holds:*

$$\begin{aligned} & H_\alpha \left(\frac{1}{d_{in}} \mathbf{p} \oplus \frac{d_{in}-1}{d_{in}} \right) + H_\beta \left(\frac{1}{d_{in}} \mathbf{q} \oplus \frac{d_{in}-1}{d_{in}} \right) \\ & \geq -2 \ln \max_{i,j} \|\mathbf{A}(x_i)^{1/2} \mathbf{B}(y_j)^{1/2}\| \end{aligned} \quad (2.81)$$

where α and β are positive numbers such that $\frac{1}{\alpha} + \frac{1}{\beta} = 2$, and $\mathbf{A}$ and $\mathbf{B}$ denote the POVMs respectively defined as

$$\mathbf{A}(x_i) := \begin{cases} \mathbf{S}(x_i) & 1 \leq i \leq M, \\ I - \rho_{in}^T \otimes I_{out} & i = M+1, \end{cases} \quad (2.82)$$

and

$$\mathbf{B}(y_j) := \begin{cases} \mathbf{T}(y_j) & 1 \leq j \leq N, \\ I - \sigma_{in}^T \otimes I_{out} & j = N+1. \end{cases} \quad (2.83)$$

Proposition 2.2.9. *The following majorization relation holds:*

$$\mathbf{p} \otimes \mathbf{q} \prec \mathbf{c}_\otimes \quad (2.84)$$

where $\mathbf{c}_\otimes$ is a probability vector of dimension MN whose elements are defined as

$$c_{\otimes,k} := t_{\otimes,k} - t_{\otimes,k-1} \quad (2.85)$$

for all $k \in \{1, \dots, MN\}$. Here, $t_{\otimes,k}$ is given by $t_{\otimes,0} := 0$ and

$$t_{\otimes,k} := \max_{\substack{\mathcal{K} \subseteq \{1, \dots, M\} \times \{1, \dots, N\} \\ |\mathcal{K}|=k}} \max_{\Lambda} \sum_{(i,j) \in \mathcal{K}} p_i q_j \quad (2.86)$$

for each $k \in \{1, \dots, MN\}$.

Proposition 2.2.10. *The following majorization relation holds:*

$$\mathbf{p} \oplus \mathbf{q} \prec \mathbf{c}_\oplus \quad (2.87)$$

where $\mathbf{c}_\oplus$ is a vector of dimension $M + N$ whose elements are defined as

$$c_{\oplus,k} = t_{\oplus,k} - t_{\oplus,k-1} \quad (2.88)$$

for all $k \in \{1, \dots, M + N\}$. Here, $t_{\oplus,k}$ is given by $t_{\oplus,0} := 0$, and

$$t_{\oplus,k} := \max_{\substack{\mathcal{I}, \mathcal{J} \\ |\mathcal{I}| + |\mathcal{J}| = k}} \max_{\Lambda} \left\{ \sum_{i \in \mathcal{I}} p_i + \sum_{j \in \mathcal{J}} q_j \right\} \quad (2.89)$$

for each $k \in \{1, \dots, M + N\}$.

It should be noted that $t_{\oplus,k}$ can be expressed using the conditional min-entropy, devised in Ref. [31], and $t_{\otimes,k}$ can be bounded from above using $t_{\oplus,k+1}$; see Ref. [12] for more details.

Equations (2.81), (2.84), and (2.87) are considered reasonable forms of uncertainty relations for measurements of channels. Their bounds are determined by the testers $\mathbf{S}$ and $\mathbf{T}$, thereby making it possible to express channel-independent restrictions imposed on the probability vectors $\mathbf{p}$ and $\mathbf{q}$. In particular, if $\max_{i,j} \|\mathbf{A}(x_i)^{1/2} \mathbf{B}(y_j)^{1/2}\| < 1$, $\mathbf{c}_\otimes^\downarrow \neq (1, 0, \dots, 0)$, or $\mathbf{c}_\oplus^\downarrow \neq (1, 1, 0, \dots, 0)$ holds, then $\mathbf{p}$ and $\mathbf{q}$ cannot be deterministic at the same time. Additionally, Eqs. (2.49), (2.53), and (2.56) can be obtained from Eqs. (2.81), (2.84), and (2.87), respectively, because measurements of states correspond to ancilla-free measurements in the case of $d_{\text{in}} = 1$. Thus, Eqs. (2.81), (2.84), and (2.87) quantify the uncertainty trade-offs in measurements of channels, including measurements of states, making it possible to capture an aspect of impossibility in quantum theory.

Chapter 3

An Uncertainty Relation for Measurements of Random Unitary Channels Acting on a Qubit

In this chapter, we establish an uncertainty relation for measurements of channels, based on Ref. [12]. Specifically, we consider a scheme where a random unitary channel acting on a qubit is stochastically measured using a pair of ancilla-free testers. Consequently, an uncertainty relation is obtained as a closed-form expression in such a specific situation.

3.1 Introduction

In the previous chapter, it was explained that uncertainty relations can be formulated not only for POVMs but also for testers. For a pair of testers, Eqs. (2.81), (2.84), and (2.87) impose restrictions on the probability distributions of a channel. These uncertainty relations apply to scenarios in which arbitrary quantum channels are allowed, thereby capturing the universal constraints inherent in quantum dynamical processes.

While this assumption regarding the preparation of channels is reasonable, it is also worth considering cases where a prepared channel is of a specific form. This is because particular transformations are of interest in some contexts; for instance, the private quantum channels, designed in Ref.

[32] as protocols for securely transmitting quantum states through classical keys, are defined using random unitary channels. Furthermore, confining the range of channels to be measured renders the problem of estimating uncertainty bounds more tractable than when no constraints are imposed, and thereby makes it possible to express uncertainty relations that reflect properties of specific quantum processes.

Random unitary channels constitute a typical class of channels because not only are they utilized in quantum information tasks, such as the private quantum channels, but also include unitary channels, fundamental transformations in quantum theory. Thus, it is considered meaningful to assume that a channel subject to measurements is random unitary.

The aim of this chapter is to derive an uncertainty relation for measurements of a random unitary channel acting on a qubit. We restrict ourselves to ancilla-free measurements because they are typical schemes for probing channels and easy to analyze thanks to the simplicity of the corresponding testers. Although restricting the system to a qubit is a strong limitation, qubits are the building blocks of quantum information processing. Thus, qubit-level formulas are expected to serve as elementary constraints for large-scale physical systems. We provide an uncertainty relation with an explicit channel-independent bound expressed as a function of the testers, which does not involve any optimization problem.

3.2 Derivation

Let $\mathcal{H}$ be a two-dimensional Hilbert space, let ρ and τ be states on $\mathcal{H}$, and let $\mathbf{E}$ and $\mathbf{F}$ be POVMs respectively defined on finite sets Ω_1 and Ω_2 . We consider the following two ancilla-free testers $\mathbf{S}$ and $\mathbf{T}$ defined as

$$\mathbf{S}(x) = \rho^T \otimes \mathbf{E}(x), \quad (3.1)$$

$$\mathbf{T}(y) = \tau^T \otimes \mathbf{F}(y) \quad (3.2)$$

for every $x \in \Omega_1$ and $y \in \Omega_2$. As described in Sect. 2, the testers $\mathbf{S}$ and $\mathbf{T}$ are respectively identified with devices that supply the states ρ and τ to a channel and perform the measurements described by the POVMs $\mathbf{E}$ and $\mathbf{F}$.

Let us consider the scheme where a random unitary channel Λ is measured using $\mathbf{S}$ with a probability r and measured using $\mathbf{T}$ with the remaining probability $1 - r$. For subsets $\mathcal{X} \subseteq \Omega_1$ and $\mathcal{Y} \subseteq \Omega_2$, an uncertainty relation

of this scheme is expressed as

$$r \sum_{x \in \mathcal{X}} p(x|\Lambda) + (1-r) \sum_{y \in \mathcal{Y}} q(y|\Lambda) \leq c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}). \quad (3.3)$$

This inequality is regarded as a translation of the generalized Landau–Pollak uncertainty relation [28], or the fine-grained uncertainty relation [11]. The right-hand side is defined as

$$c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) := \max_{\Lambda \in \mathcal{R}} \left\{ r \sum_{x \in \mathcal{X}} p(x|\Lambda) + (1-r) \sum_{y \in \mathcal{Y}} q(y|\Lambda) \right\}, \quad (3.4)$$

where $\mathcal{R}$ denotes the set of all random unitary channels on $\mathcal{L}(\mathcal{H})$. If $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ is strictly less than the trivial bound defined as

$$t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) := \max_{\Lambda \in \mathcal{R}} \left\{ r \sum_{x \in \mathcal{X}} p(x|\Lambda) \right\} + \max_{\Lambda \in \mathcal{R}} \left\{ (1-r) \sum_{y \in \mathcal{Y}} q(y|\Lambda) \right\}, \quad (3.5)$$

i.e., if $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) < t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ holds, then a nontrivial trade-off between the probabilities $\sum_{x \in \mathcal{X}} p(x|\Lambda)$ and $\sum_{y \in \mathcal{Y}} q(y|\Lambda)$ exists. Thus, we need to evaluate $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ and $t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$, defined as maximum values, to quantify such a trade-off. The following theorem provides closed-form expressions of $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ and $t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$.

Theorem 3.2.1. *The following equalities hold:*

$$\begin{aligned} c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) = & \frac{Z(\mathcal{X}, \mathcal{Y})}{2} + \frac{1}{2} \left((r\Delta\rho\Delta E(\mathcal{X}) - (1-r)\Delta\tau\Delta F(\mathcal{Y}))^2 \right. \\ & + 4r(1-r)\Delta\rho\Delta E(\mathcal{X})\Delta\tau\Delta F(\mathcal{Y}) \left(|\langle\psi|\phi\rangle| |\langle e(\mathcal{X})|f(\mathcal{Y})\rangle| \right. \\ & \left. \left. + \sqrt{(1-|\langle\psi|\phi\rangle|^2)(1-|\langle e(\mathcal{X})|f(\mathcal{Y})\rangle|^2)} \right)^2 \right)^{1/2}, \end{aligned} \quad (3.6)$$

$$t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) = \frac{Z(\mathcal{X}, \mathcal{Y})}{2} + \frac{1}{2} (r\Delta\rho\Delta E(\mathcal{X}) + (1-r)\Delta\tau\Delta F(\mathcal{Y})) \quad (3.7)$$

where

$$E(\mathcal{X}) := \sum_{x \in \mathcal{X}} E(x), \quad (3.8)$$

$$F(\mathcal{Y}) := \sum_{y \in \mathcal{Y}} F(y), \quad (3.9)$$

$$Z(\mathcal{X}, \mathcal{Y}) := \text{tr} [rE(\mathcal{X}) + (1-r)F(\mathcal{Y})], \quad (3.10)$$

and ΔA denotes the difference between the maximum and minimum eigenvalue for every positive operator A , i.e., $\Delta A := 2\|A\| - \text{tr}[A]$. The vectors $|\psi\rangle$, $|\phi\rangle$, $|e(\mathcal{X})\rangle$, and $|f(\mathcal{Y})\rangle$ represent the normalized eigenvectors corresponding the maximum eigenvalues of ρ , τ , $E(\mathcal{X})$, and $F(\mathcal{Y})$, respectively.

It is clear from this theorem that $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) = t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ holds when $r = 0$ or $r = 1$, meaning that no trade-off between the probabilities exists when the measurements are not stochastically mixed. When $0 < r < 1$, the quantity

$$Q := |\langle\psi|\phi\rangle| |\langle e(\mathcal{X})|f(\mathcal{Y})\rangle| + \sqrt{(1 - |\langle\psi|\phi\rangle|^2) (1 - |\langle e(\mathcal{X})|f(\mathcal{Y})\rangle|^2)} \quad (3.11)$$

appearing in Eq. (3.6) serves as a factor that contributes to a trade-off between the probabilities, because $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) < t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ holds if and only if $Q < 1$. This fact leads to the following proposition that provides a necessary and sufficient condition for $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) < t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ when $0 < r < 1$.

Proposition 3.2.2. *Suppose $0 < r < 1$. The strict inequality $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) < t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ holds if and only if $|\langle\psi|\phi\rangle| \neq |\langle e(\mathcal{X})|f(\mathcal{Y})\rangle|$. In other words, the equality $c_{\mathcal{R}}(\mathcal{X}, \mathcal{Y}) = t_{\mathcal{R}}(\mathcal{X}, \mathcal{Y})$ holds if and only if $|\langle\psi|\phi\rangle| = |\langle e(\mathcal{X})|f(\mathcal{Y})\rangle|$.*

It is worth considering the following extreme case:

Corollary 3.2.3. *Suppose the following settings:*

$$\Omega_1 = \{x_0, x_1\}, \quad (3.12)$$

$$\Omega_2 = \{y_0, y_1\}, \quad (3.13)$$

$$\rho = |\psi\rangle \langle\psi|, \quad (3.14)$$

$$\tau = |\phi\rangle \langle\phi|, \quad (3.15)$$

$$E(x_i) = |e_i\rangle \langle e_i|, \quad (3.16)$$

$$F(y_j) = |f_j\rangle \langle f_j| \quad (3.17)$$

where $|\psi\rangle$ and $|\phi\rangle$ are normalized vectors, and $\{|e_0\rangle, |e_1\rangle\}$ and $\{|f_0\rangle, |f_1\rangle\}$ are orthonormal bases. Then, $c_{\mathcal{R}}(\{x_i\}, \{y_j\})$ and $t_{\mathcal{R}}(\{x_i\}, \{y_j\})$ are respectively given by

$$c_{\mathcal{R}}(\{x_i\}, \{y_j\}) = \frac{1}{2} + \left(\left(r - \frac{1}{2} \right)^2 + r(1-r) \left(|\langle\psi|\phi\rangle| |\langle e_i|f_j\rangle| + \sqrt{(1-|\langle\psi|\phi\rangle|^2)(1-|\langle e_i|f_j\rangle|^2)} \right)^2 \right)^{1/2}, \quad (3.18)$$

$$t_{\mathcal{R}}(\{x_i\}, \{y_j\}) = 1 \quad (3.19)$$

for every $i, j \in \{0, 1\}$. In particular, if $r = \frac{1}{2}$, the first equality becomes

$$c_{\mathcal{R}}(\{x_i\}, \{y_j\}) = \frac{1}{2} \left(1 + |\langle\psi|\phi\rangle| |\langle e_i|f_j\rangle| + \sqrt{(1-|\langle\psi|\phi\rangle|^2)(1-|\langle e_i|f_j\rangle|^2)} \right). \quad (3.20)$$

Under the settings of this corollary, Q is expressed as

$$Q = |\langle\psi|\phi\rangle| |\langle e_i|f_j\rangle| + \sqrt{(1-|\langle\psi|\phi\rangle|^2)(1-|\langle e_i|f_j\rangle|^2)}. \quad (3.21)$$

Thanks to the pureness of the testers, the influence of Q on a trade-off between $p(x_i|\Lambda)$ and $q(y_j|\Lambda)$, i.e., the fact that $Q < 1$ implies $c_{\mathcal{R}}(\{x_i\}, \{y_j\}) < t_{\mathcal{R}}(\{x_i\}, \{y_j\})$, is even more obvious than the general case.

We finish this section by providing the following concrete example:

Example 3.2.4. Consider the following additional settings in Corollary 3.2.3:

$$|\psi\rangle = |0\rangle, \quad (3.22)$$

$$|\phi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + \sin\left(\frac{\theta}{2}\right) |1\rangle, \quad (3.23)$$

$$|e_i\rangle = |i\rangle, \quad (3.24)$$

$$|f_j\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^j |1\rangle), \quad (3.25)$$

$$r = \frac{1}{2} \quad (3.26)$$

where $0 \leq \theta \leq \pi$. Equation (3.20) implies that, for every $i, j \in \{0, 1\}$, the following equality holds:

$$c_{\mathcal{R}}(\{x_i\}, \{y_j\}) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{\theta}{2} - \frac{\pi}{4}\right), \quad (3.27)$$

whose right-hand side is equal to 1 if and only if $\theta = \frac{\pi}{2}$. Consequently, the inequality

$$\frac{1}{2}p(x_i|\Lambda) + \frac{1}{2}q(y_j|\Lambda) \leq c_{\mathcal{R}}(\{x_i\}, \{y_j\}) \quad (3.28)$$

indicates that an unavoidable trade-off between $p(x_i|\Lambda)$ and $q(y_j|\Lambda)$ exists if and only if $\theta \neq \frac{\pi}{2}$. Figure 3.1 presents $c_{\mathcal{R}}(\{x_i\}, \{y_j\})$ plotted as a function of $|\langle\psi|\phi\rangle|$.

3.3 Summary and Discussion

In this chapter, an uncertainty relation for testers was presented in a specific scheme. The uncertainty bound is explicitly provided in Theorem 3.2.1 without involving any optimization problem, revealing that Q is an important factor of a trade-off between the associated probabilities. A necessary and sufficient condition for the existence of such a trade-off was also obtained by observing the explicit formula of uncertainty bound.

Our uncertainty relation is essentially different from the uncertainty relations Eqs. (2.81), (2.84), and (2.87), which were obtained in Ref. [12]. To see this, let us consider the settings supposed in Example 3.2.4 with the additional condition that $\theta = \pi$. Equation (3.27) implies the existence of a nontrivial trade-off between the probabilities, while Eqs. (2.81), (2.84), and (2.87) become trivial in the considered case. This nontriviality is a consequence of the assumption that a channel to be measured is chosen from the set of all random unitary channels, rather than the set of all qubit channels, meaning that our uncertainty relations reflect a property of the quantum dynamics implemented by mixing unitary processes.

Finally, let us mention three possible directions for future research. The first direction is to generalize our uncertainty relations from a qubit to a qudit, i.e., a system whose Hilbert space has dimension greater than 2, with the aim of applying them to large-scale physical systems. It is not easy to obtain a closed-form expression of the uncertainty relation for an arbitrary

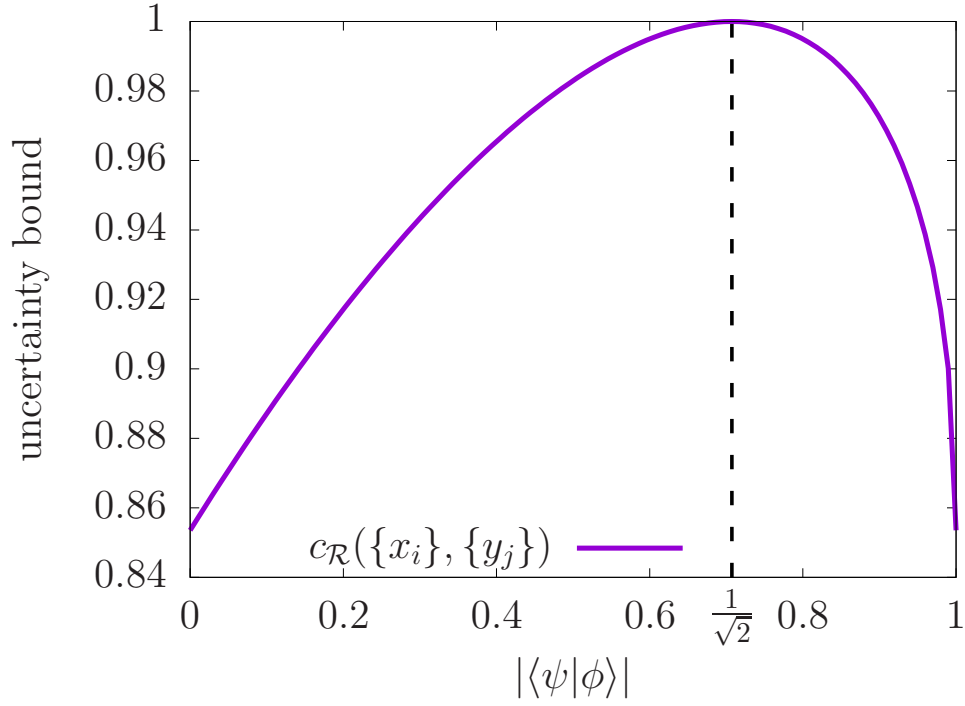


Figure 3.1: A plot of Eq. (3.27) as a function of $|\langle \psi | \phi \rangle|$. The uncertainty bound $c_{\mathcal{R}}(\{x_i\}, \{y_j\})$ is equal to 1 if and only if $|\langle \psi | \phi \rangle| = \frac{1}{\sqrt{2}}$, meaning that $p(x_i|\Lambda)$ and $q(y_j|\Lambda)$ cannot attain 1 at the same time if and only if $|\langle \psi | \phi \rangle| \neq \frac{1}{\sqrt{2}}$, i.e., $\theta \neq \frac{\pi}{4}$.

qudit system. However, if testers are given by pure input states and rank-1 PVMs, as in Corollary 3.2.3, it would be possible to estimate the uncertainty bound for a qudit from above using the same functional form as the right-hand side of Eq. (3.18).

The second direction is to explore uncertainty relations for testers other than ancilla-free ones. It is interesting to clarify the influence of the correlation between ancillary systems with input-output systems on a trade-off between probabilities. By supposing specific forms about testers, one can obtain closed-form expressions of uncertainty relations, similar to Eqs. (3.6), (3.18), and (3.20). While it seems difficult to derive explicit uncertainty relations for general testers, nevertheless, the corresponding uncertainty bounds are evaluable by utilizing their connection with the fully entangled fraction (FEF) [33]. Specifically, it is possible to compute an uncertainty bound for an arbitrary pair of testers using the analytical expressions of FEF obtained in Refs. [34] and [35].

The final direction is to apply our uncertainty relation to protocols or schemes in quantum information processing. While this kind of research is not trivial, applications of entropic uncertainty relations (e.g., see Ref. [6]) would be helpful guides for this type of future research.

Chapter 4

Fine-Grained Uncertainty Relations for Quantum Testers

In this chapter, a fine-grained uncertainty relation for testers is provided, with two methods for evaluating its uncertainty bound. One of the evaluation methods is given as an upper estimate of the uncertainty bound, leading to a closed-form expression of the fine-grained uncertainty relation in specific settings. The other evaluation method is with respect to a numerical computation, enabling us to obtain approximation values of the uncertainty bound for given testers.

4.1 Introduction

As a physical system becomes larger, its dynamics admits increasingly diverse state transitions. Consequently, for large-scale quantum processes, it is both natural and necessary to consider measurements implemented by multiple quantum testers. Since Eqs. (2.81), (2.84), and (2.87) apply only to pairs of testers, deriving *scalable uncertainty relations*, i.e., ones that hold for an arbitrary number of testers, is essential for quantifying the uncertainty inherent in large-scale quantum information processing.

As stated in Sect. 2.2.1, fine-grained uncertainty relations are considered modern expressions of uncertainty trade-offs associated with measurements on a state. Indeed, Eq. (2.59), a fine-grained uncertainty relation for POVMs, has a unique strength which the other uncertainty relations, such as Robertson's inequality, entropic uncertainty relations, and majorization

uncertainty relations, do not offer. Hence, it is natural to consider establishing fine-grained uncertainty relations even in measurements on a channel. In addition, such relations are also meaningful for other physical concepts. The fine-grained uncertainty relation Eq. (2.59) has connections with the non-locality of quantum theory [11], the second law of thermodynamics [36], and the separability of bipartite states [37]. As such, a generalization of Eq. (2.59) is expected to develop these concepts from a wider perspective, while serving as a scalable uncertainty relation for quantum testers.

In this chapter, we present a fine-grained uncertainty relation for testers. The main difficulty lies in evaluating its uncertainty bound. Specifically, while it is direct to generalize Eq. (2.59) by formally replacing POVMs and a state with testers and a Choi operator, respectively, it is not trivial to obtain the value of the generalized uncertainty bound. Thus, some methods to evaluate the uncertainty bound are required in order to quantify the involved uncertainty trade-offs for potential applications to large-scale physical systems. To address that issue, we provide a relaxed bound of the generalized fine-grained uncertainty relation, by which the calculation of the uncertainty trade-offs becomes more tractable than the one given by the original uncertainty bound. We also present a numerical method for computing the uncertainty bound based on a semidefinite program.

4.2 Generalization of the Fine-Grained Uncertainty Relation

A fine-grained uncertainty relation associated with several measurements performed on a channel can be formulated by replacing the POVMs and state in Eq. (2.59) with testers and a channel, respectively. Thus, we consider L testers $\mathsf{T}^{(1)}, \dots, \mathsf{T}^{(L)}$ that are designed to probe channels which transform states on a Hilbert space $\mathcal{H}_{\text{in}}$ into states on another Hilbert space $\mathcal{H}_{\text{out}}$. Specifically, the tester $\mathsf{T}^{(l)}$ is determined by a state $\rho^{(l)}$ on $\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{in}}$ and POVM $\mathsf{E}^{(l)}: \Omega_l \rightarrow \mathcal{L}(\mathcal{H}_{\text{anc}} \otimes \mathcal{H}_{\text{out}})$ according to Eq. (2.26) for each $l \in \{1, \dots, L\}$, where $\mathcal{H}_{\text{anc}}$ denotes an ancillary system. Therefore, we can consider the following set of inequalities:

$$\mathcal{V} := \left\{ \sum_{l=1}^L r_l p_l(x^{(l)} | \Lambda) \leq c(\mathbf{x}) : \mathbf{x} := (x^{(1)}, \dots, x^{(L)}) \in \prod_{l=1}^L \Omega_l \right\} \quad (4.1)$$

where $\{r_l\}_{l=1}^L$ is a probability distribution and Λ is a channel from $\mathcal{L}(\mathcal{H}_{\text{in}})$ to $\mathcal{L}(\mathcal{H}_{\text{out}})$. The right-hand side of the inequality is defined as

$$c(\mathbf{x}) := \max_{\Lambda} \sum_{l=1}^L r_l p_l(x^{(l)}|\Lambda), \quad (4.2)$$

where the maximization is taken over all channels from $\mathcal{L}(\mathcal{H}_{\text{in}})$ to $\mathcal{L}(\mathcal{H}_{\text{out}})$.

The set $\mathcal{V}$ is regarded as an uncertainty relation for the testers $\mathsf{T}^{(1)}, \dots, \mathsf{T}^{(L)}$ because it imposes restrictions on the probability distributions $p_1, \dots, p_L$ by bounding

$$\sum_{l=1}^L r_l p_l(x^{(l)}|\Lambda) \quad (4.3)$$

for all $\mathbf{x} \in \prod_{l=1}^L \Omega_l$. Specifically, similar to Eq. (2.59), the strict inequality

$$c(\mathbf{x}) < t(\mathbf{x}) \quad (4.4)$$

indicates that the associated probabilities, i.e.,

$$p_1(x^{(1)}|\Lambda), \dots, p_L(x^{(L)}|\Lambda), \quad (4.5)$$

cannot attain their maximum values simultaneously, and hence signifies a nontrivial restriction on the probability distributions. Here, $t(\mathbf{x})$ is referred to as a *trivial bound* and defined by

$$t(\mathbf{x}) := \sum_{l=1}^L r_l \max_{\Lambda} p_l(x^{(l)}|\Lambda). \quad (4.6)$$

As in Eq. (2.59), $\mathcal{V}$ is regarded as a reasonable form of uncertainty relation because each inequality in $\mathcal{V}$ has a clear operational meaning that the probability of obtaining one of the outcomes in an $\mathbf{x} \in \Omega$ cannot exceed $c(\mathbf{x})$.

The fine-grained uncertainty relation $\mathcal{V}$ encompasses the conventional one $\mathcal{U}$ as a special case because $\mathcal{V}$ induces $\mathcal{U}$ by choosing $\mathcal{H}_{\text{in}} = \mathcal{H}_{\text{anc}} = \mathbb{C}$. This is a natural consequence because the channel is identified with a state and the testers become POVMs in such a case.

4.3 Estimation of the Uncertainty Bound

In general, it is challenging to compute how much trade-off exists between the probabilities $p_1(x^{(1)}|\Lambda), \dots, p_L(x^{(L)}|\Lambda)$ for each $\mathbf{x} \in \prod_{l=1}^L \Omega_l$ because $c(\mathbf{x})$ is given by an optimization problem. A simple approach to address this issue is to estimate the uncertainty bound $c(\mathbf{x})$ from above in return for optimality, i.e., to derive a relaxed uncertainty bound. The following proposition provides such an upper bound for $c(\mathbf{x})$.

Proposition 4.3.1. *For an arbitrary $\mathbf{x} \in \prod_{l=1}^L \Omega_l$, the following inequality holds:*

$$c(\mathbf{x}) \leq \tilde{c}(\mathbf{x}). \quad (4.7)$$

Here, $\tilde{c}(\mathbf{x})$ is defined as

$$\tilde{c}(\mathbf{x}) := d_{in} \left\| \sum_{l=1}^L r_l \mathsf{T}^{(l)}(x^{(l)}) \right\|, \quad (4.8)$$

where $\|\cdot\|$ denotes the operator norm defined by

$$\|A\| := \max_{\substack{|\psi\rangle \\ \|\psi\| \neq 0}} \frac{\|A|\psi\rangle\|}{\|\psi\|} \quad (4.9)$$

for every linear operator A on a Hilbert space. Equation (4.7) becomes equality if $\text{tr}_{out}[|\Psi_0\rangle\langle\Psi_0|] = \frac{I_{in}}{d_{in}}$ where $|\Psi_0\rangle$ is a normalized eigenvector of $\sum_{l=1}^L r_l \mathsf{T}^{(l)}(x^{(l)})$ corresponding to the largest eigenvalue.

Similar to $c(\mathbf{x})$, $\tilde{c}(\mathbf{x})$ indicates a nontrivial trade-off between

$$p_1(x^{(1)}|\Lambda), \dots, p_L(x^{(L)}|\Lambda) \quad (4.10)$$

if $\tilde{c}(\mathbf{x}) < t(\mathbf{x})$, so that the following set of inequalities serves as an uncertainty relation for the testers:

$$\tilde{\mathcal{V}} := \left\{ \sum_{l=1}^L r_l p_l(x^{(l)}|\Lambda) \leq \tilde{c}(\mathbf{x}) : \mathbf{x} \in \prod_{l=1}^L \Omega_l \right\}. \quad (4.11)$$

The set $\tilde{\mathcal{V}}$ is a generalization of the conventional fine-grained uncertainty relation, i.e., $\mathcal{U}$, because $\mathcal{V} = \tilde{\mathcal{V}}$ holds if $d_{in} = d_{anc} = 1$. We also call $\tilde{\mathcal{V}}$ a fine-grained uncertainty relation.

4.3.1 Case of ancilla-free testers

Unfortunately, $\tilde{\mathcal{V}}$ is not useful if the testers are ancilla-free, as demonstrated by the following example.

Example 4.3.2. Suppose the following settings:

$$d_{\text{anc}} = 1, \quad (4.12)$$

$$L = 2, \quad (4.13)$$

$$r_1 = r_2 = \frac{1}{2}, \quad (4.14)$$

$$\rho^{(l)} = I_{\text{anc}} \otimes |\psi^{(l)}\rangle \langle \psi^{(l)}|, \quad (4.15)$$

$$\mathbb{E}^{(l)}(x_i^{(l)}) = I_{\text{anc}} \otimes |e_i^{(l)}\rangle \langle e_i^{(l)}| \quad (4.16)$$

where $|\psi^{(l)}\rangle$ is a unit vector in $\mathcal{H}_{\text{in}}$ for each $l \in \{1, 2\}$, and $\{|e_i^{(l)}\rangle\}_{i=0}^{d_{\text{out}}-1}$ is an orthonormal basis for $\mathcal{H}_{\text{out}}$ of dimension d_{out} for each $l \in \{1, 2\}$. Under these settings, the testers are given by

$$\mathsf{T}^{(l)}(x_i^{(l)}) = |\psi^{(l)}\rangle \langle \psi^{(l)}|^T \otimes |e_i^{(l)}\rangle \langle e_i^{(l)}|. \quad (4.17)$$

A simple computation shows that the following equalities hold for every $\mathbf{x} \in \Omega_1 \times \Omega_2$:

$$\tilde{c}(\mathbf{x}) = \frac{d_{\text{in}}}{2} \left(1 + |\langle \psi^{(1)} | \psi^{(2)} \rangle| |\langle e_i^{(1)} | e_j^{(2)} \rangle| \right), \quad (4.18)$$

$$t(\mathbf{x}) = 1. \quad (4.19)$$

If $d_{\text{in}} = 1$, the right-hand side of Eq. (4.18) coincides with that of Eq. (2.65), as expected. If $d_{\text{in}} > 1$, $\tilde{c}(\mathbf{x})$ is meaningless because the right-hand side of Eq. (4.18) is strictly greater than $t(\mathbf{x}) = 1$.

4.3.2 Case of testers with a maximally entangled input state

The upper bound $\tilde{c}(\mathbf{x})$ needs to be less than 1 at least, in order to serve as a meaningful upper bound for $c(\mathbf{x})$. The following proposition provides such a condition.

Proposition 4.3.3. *If $\text{tr}_{\text{anc}} \rho^{(l)} = \frac{I_{\text{in}}}{d_{\text{in}}}$ for all $l \in \{1, \dots, L\}$, $\tilde{c}(\mathbf{x}) \leq 1$ holds for all $\mathbf{x} \in \prod_{l=1}^L \Omega_l$.*

Proposition 4.3.3 ensures that $\tilde{c}(\mathbf{x}) \leq 1$ if the input states $\rho^{(l)}$ are maximally entangled states for all $l \in \{1, \dots, L\}$. Thus, we suppose $\mathcal{H}_{\text{in}} = \mathcal{H}_{\text{anc}} = \mathcal{H}$ where $\mathcal{H}$ is a Hilbert space of dimension d and $\rho^{(l)} = P_+$ in the remainder of this subsection. It is a typical approach in ancilla-assisted process tomography to probe an unknown channel by inputting one side of a maximally entangled state [38, 39, 14].

While $\tilde{c}(\mathbf{x}) \leq 1$ is guaranteed, $\tilde{c}(\mathbf{x}) < t(\mathbf{x})$ is required to conclude that a nontrivial trade-off between $p_1(x^{(1)}|\Lambda), \dots, p_L(x^{(L)}|\Lambda)$ exists. The following example shows that $\tilde{c}(\mathbf{x})$ is useless, i.e., $\tilde{c}(\mathbf{x}) \geq t(\mathbf{x})$ holds, if the POVMs are given by orthonormal bases consisting of product states.

Example 4.3.4. Suppose the following settings:

$$L = 2, \quad (4.20)$$

$$r_1 = r_2 = \frac{1}{2}, \quad (4.21)$$

$$\Omega_l = \{x_{i,j}^{(l)} : i \in \{0, \dots, d-1\}, j \in \{0, \dots, d_{\text{out}}-1\}\}, \quad (4.22)$$

$$\mathbb{E}^{(l)}(x_{i,j}^{(l)}) = |e_i^{(l)}\rangle \langle e_i^{(l)}| \otimes |f_j^{(l)}\rangle \langle f_j^{(l)}| \quad (4.23)$$

where $\{|e_i^{(l)}\rangle\}_{i=0}^{d-1}$ and $\{|f_j^{(l)}\rangle\}_{j=0}^{d_{\text{out}}-1}$ are orthonormal bases for $\mathcal{H}$ and $\mathcal{H}_{\text{out}}$, respectively. Under these settings, the testers are given by

$$\mathbb{T}^{(l)}(x_{i,j}^{(l)}) = \frac{1}{d} |e_i^{(l)}\rangle \langle e_i^{(l)}| \otimes |f_j^{(l)}\rangle \langle f_j^{(l)}|. \quad (4.24)$$

Thus, we have

$$\tilde{c}(x_{(i(1),j(1))}^{(1)}, x_{(i(2),j(2))}^{(2)}) = \frac{1}{2} \left(1 + |\langle e_{i(1)}^{(1)} | e_{i(2)}^{(2)} \rangle| |\langle f_{j(1)}^{(1)} | f_{j(2)}^{(2)} \rangle| \right), \quad (4.25)$$

$$t(x_{(i(1),j(1))}^{(1)}, x_{(i(2),j(2))}^{(2)}) = \frac{1}{d} \quad (4.26)$$

for every $(i(1), j(1)), (i(2), j(2)) \in \{0, \dots, d-1\} \times \{0, \dots, d_{\text{out}}-1\}$. If $d = 1$, the right-hand side of Eq. (4.25) can be identified with that of Eq. (2.65) as expected because $|\langle e_{i(1)}^{(1)} | e_{i(2)}^{(2)} \rangle| = 1$ holds in this case. If $d > 1$, $\tilde{c}(x_{(i(1),j(1))}^{(1)}, x_{(i(2),j(2))}^{(2)})$ is meaningless since it holds that $\tilde{c}(x_{(i(1),j(1))}^{(1)}, x_{(i(2),j(2))}^{(2)}) \geq t(x_{(i(1),j(1))}^{(1)}, x_{(i(2),j(2))}^{(2)})$ in this case.

This example suggests seeking testers satisfying $t(\mathbf{x}) = 1$. Testers induced by POVMs whose elements are *maximally entangled bases*, i.e., orthonormal

bases consisting of maximally entangled states, meet the condition. For instance, the Bell basis is a well-known maximally entangled basis. Thus, we suppose that $\mathcal{H}_{\text{out}} = \mathcal{H}$ and for all $l \in \{1, \dots, L\}$ the POVMs are given by

$$\mathbb{E}^{(l)}(x_i^{(l)}) = |\Psi_i^{(l)}\rangle \langle \Psi_i^{(l)}| \quad (4.27)$$

where $\{|\Psi_i^{(l)}\rangle\}_{i=0}^{d^2-1}$ is a maximally entangled basis of $\mathcal{H} \otimes \mathcal{H}$ for each $l \in \{1, \dots, L\}$. Consequently, the testers become

$$\mathbb{T}^{(l)}(x_i^{(l)}) = \frac{1}{d} |\Psi_i^{(l)}\rangle \langle \Psi_i^{(l)}| \quad (4.28)$$

for all $l \in \{1, \dots, L\}$.

Let us confirm that the testers, given by Eq. (4.28), indeed satisfy $t(\mathbf{x}) = 1$. To this end, recall that the trivial bound is given by

$$t(x_{i(1)}^{(1)}, \dots, x_{i(L)}^{(L)}) = \sum_{l=1}^L r_l \max_{\Lambda} \text{tr} \left[\mathbb{T}^{(l)}(x_{i(l)}^{(l)}) J_{\Lambda} \right] \quad (4.29)$$

$$= \sum_{l=1}^L r_l \max_{\Lambda} \langle \Psi_i^{(l)} | \frac{J_{\Lambda}}{d} | \Psi_i^{(l)} \rangle, \quad (4.30)$$

where the second equality follows by substitution of Eq. (4.28). The assumption that all $|\Psi_{i(l)}^{(l)}\rangle$ are maximally entangled states indicates that there is a unitary operator $U_{i(l)}^{(l)}$ for every $l \in \{1, \dots, L\}$ and $i(l) \in \{1, \dots, d^2 - 1\}$ such that

$$|\Psi_{i(l)}^{(l)}\rangle = (I \otimes U_{i(l)}^{(l)}) |\Psi_+\rangle. \quad (4.31)$$

Therefore, we can conclude $t(x_{i(1)}^{(1)}, \dots, x_{i(L)}^{(L)}) = 1$ because for each $l \in \{1, \dots, L\}$ the following equality holds:

$$\langle \Psi_i^{(l)} | \frac{J_{\Lambda_{i(l)}^{(l)}}}{d} | \Psi_i^{(l)} \rangle = 1 \quad (4.32)$$

where $\Lambda_{i(l)}^{(l)}$ is the unitary channel defined as $\Lambda_{i(l)}^{(l)}(A) = U_{i(l)}^{(l)} A (U_{i(l)}^{(l)})^\dagger$ for every linear operator A on $\mathcal{H}$.

Having fixed the testers, we now proceed to the calculation of $\tilde{c}(\mathbf{x})$, which is given by

$$\tilde{c}(\mathbf{x}) = \left\| \sum_{l=1}^L r_l \mathbf{T}^{(l)}(x^{(l)}) \right\|. \quad (4.33)$$

The operator norm of a linear operator A coincides with the largest singular value of A , i.e., the largest eigenvalue of $(A^\dagger A)^{1/2}$. Thus, the right-hand side of Eq. (4.33) can be analytically computed if the argument of operator norm is low rank. The following proposition provides the closed expression of $\tilde{c}(x_i^{(1)}, x_j^{(2)})$ under the additional conditions $L = 2$ and $r_1 = r_2 = \frac{1}{2}$.

Proposition 4.3.5. *The following equality holds:*

$$\tilde{c}(x_i^{(1)}, x_j^{(2)}) = \frac{1}{2} \left(1 + |\langle \Psi_i^{(1)} | \Psi_j^{(2)} \rangle| \right). \quad (4.34)$$

Consequently, the fine-grained uncertainty relation is expressed as

$$\begin{aligned} \tilde{\mathcal{V}} = \left\{ \frac{1}{2} p_1(x_i^{(1)} | \Lambda) + \frac{1}{2} p_2(x_j^{(2)} | \Lambda) \leq \frac{1}{2} \left(1 + |\langle \Psi_i^{(1)} | \Psi_j^{(2)} \rangle| \right) \right. \\ \left. : i, j \in \{0, \dots, d^2 - 1\} \right\}. \end{aligned} \quad (4.35)$$

If $|\langle \Psi_i^{(1)} | \Psi_j^{(2)} \rangle| < 1$ for a pair $i, j \in \{0, \dots, d^2 - 1\}$, the corresponding inequality in $\tilde{\mathcal{V}}$ implies that $p_1(x_i^{(1)} | \Lambda)$ and $p_2(x_j^{(2)} | \Lambda)$ cannot be 1 simultaneously, meaning that a nontrivial trade-off between these probabilities exists.

It is natural to consider how well $\tilde{c}(x_i^{(1)}, x_j^{(2)})$ approximates the optimum uncertainty bound $c(x_i^{(1)}, x_j^{(2)})$. We can show that $\tilde{c}(x_i^{(1)}, x_j^{(2)})$ coincides with $c(x_i^{(1)}, x_j^{(2)})$ if $d = 2$, as stated by the following proposition.

Proposition 4.3.6. *If $d = 2$, the following equality holds:*

$$c(x_i^{(1)}, x_j^{(2)}) = \frac{1}{2} \left(1 + |\langle \Psi_i^{(1)} | \Psi_j^{(2)} \rangle| \right), \quad (4.36)$$

i.e., $c(x_i^{(1)}, x_j^{(2)}) \leq \tilde{c}(x_i^{(1)}, x_j^{(2)})$, the inequality stated by Proposition 4.3.1, becomes equality. To be more specific, the maximum in Eq. (4.2) is achieved

by the unitary channel which is, for every linear operator A , defined as $\Lambda_{x_i^{(1)}, x_j^{(2)}}(A) = U_{x_i^{(1)}, x_j^{(2)}} A (U_{x_i^{(1)}, x_j^{(2)}})^\dagger$ where

$$U_{x_i^{(1)}, x_j^{(2)}} = \begin{cases} \frac{1}{\sqrt{2 + |\langle U_i^{(1)} | U_j^{(2)} \rangle_{HS}|}} \left(U_i^{(1)} + \frac{\langle U_j^{(2)} | U_i^{(1)} \rangle_{HS}}{|\langle U_i^{(1)} | U_j^{(2)} \rangle_{HS}|} U_j^{(2)} \right) & \langle U_i^{(1)} | U_j^{(2)} \rangle_{HS} \neq 0, \\ U_i^{(1)} & \langle U_i^{(1)} | U_j^{(2)} \rangle_{HS} = 0. \end{cases} \quad (4.37)$$

Here, $U_i^{(1)}$ and $U_j^{(2)}$ denote the unitary operators such that $|\Psi_i^{(1)}\rangle = (I \otimes U_i^{(1)}) |\Psi_+\rangle$ and $|\Psi_j^{(2)}\rangle = (I \otimes U_j^{(2)}) |\Psi_+\rangle$, and $\langle U_i^{(1)} | U_j^{(2)} \rangle_{HS}$ represents the Hilbert-Schmidt inner product between $U_i^{(1)}$ and $U_j^{(2)}$, defined as $\langle U_i^{(1)} | U_j^{(2)} \rangle_{HS} := \text{tr} [(U_i^{(1)})^\dagger U_j^{(2)}]$.

Therefore, we obtain

$$\mathcal{V} = \left\{ \frac{1}{2} p_1(x_i^{(1)} | \Lambda) + \frac{1}{2} p_2(x_j^{(2)} | \Lambda) \leq \frac{1}{2} \left(1 + |\langle \Psi_i^{(1)} | \Psi_j^{(2)} \rangle| \right) : i, j \in \{0, 1, 2, 3\} \right\}, \quad (4.38)$$

in which each inequality is tight, i.e., there exists a unitary channel such that equality is achieved. In particular, if $\{|\Psi_i^{(1)}\rangle\}_{i=0}^3$ and $\{|\Psi_j^{(2)}\rangle\}_{j=0}^3$ are mutually unbiased, then Eq. (4.38) indicates that a trade-off between $p_1(x_i^{(1)} | \Lambda)$ and $p_2(x_j^{(2)} | \Lambda)$ exists for all $i, j \in \{0, 1, 2, 3\}$. In Ref. [40], a pair of maximally entangled bases are designed for a two-qubit system; one is given by

$$\begin{aligned} & \left\{ |\Phi_0^{(1)}\rangle = \frac{1}{\sqrt{2}} (|0 \otimes x_0\rangle + |1 \otimes x_1\rangle), \right. \\ & |\Phi_1^{(1)}\rangle = \frac{1}{\sqrt{2}} (|0 \otimes x_0\rangle - |1 \otimes x_1\rangle), \\ & |\Phi_2^{(1)}\rangle = \frac{1}{\sqrt{2}} (|0 \otimes x_1\rangle + |1 \otimes x_0\rangle), \\ & \left. |\Phi_3^{(1)}\rangle = \frac{1}{\sqrt{2}} (|0 \otimes x_1\rangle - |1 \otimes x_0\rangle) \right\}, \quad (4.39) \end{aligned}$$

and the other is given by

$$\left\{ \begin{aligned} |\Phi_0^{(2)}\rangle &= \frac{1}{\sqrt{2}} (|y_0 \otimes 0\rangle + i |y_1 \otimes 1\rangle), \\ |\Phi_1^{(2)}\rangle &= \frac{1}{\sqrt{2}} (|y_0 \otimes 0\rangle - i |y_1 \otimes 1\rangle), \\ |\Phi_2^{(2)}\rangle &= \frac{1}{\sqrt{2}} (|y_0 \otimes 1\rangle + i |y_1 \otimes 0\rangle), \\ |\Phi_3^{(2)}\rangle &= \frac{1}{\sqrt{2}} (|y_0 \otimes 1\rangle - i |y_1 \otimes 0\rangle) \end{aligned} \right\}, \quad (4.40)$$

where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis, $|x_k\rangle := \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k |1\rangle)$, and $|y_k\rangle := \frac{1}{\sqrt{2}}(|0\rangle + (-1)^k i |1\rangle)$. We can show that $\{|\Phi_i^{(1)}\rangle\}_{i=0}^3$ and $\{|\Phi_j^{(2)}\rangle\}_{j=0}^3$ are indeed mutually unbiased by a direct calculation. Hence, by letting $|\Psi_i^{(1)}\rangle = |\Phi_i^{(1)}\rangle$ and $|\Psi_j^{(2)}\rangle = |\Phi_j^{(2)}\rangle$ for each $i, j \in \{0, 1, 2, 3\}$, we obtain

$$\mathcal{V} = \left\{ \frac{1}{2} p_1(x_i^{(1)}|\Lambda) + \frac{1}{2} p_2(x_j^{(2)}|\Lambda) \leq \frac{3}{4} : i, j \in \{0, 1, 2, 3\} \right\}. \quad (4.41)$$

Thus, mutually unbiased maximally entangled bases induce a typical pair of testers that yields nontrivial trade-offs between probabilities.

4.4 A Semidefinite Program for the Uncertainty Bound

We can connect the bound of the generalized fine-grained uncertainty relation with a semidefinite program. By utilizing the second statement of Proposition 2.1.10, we can rewrite $c(\mathbf{x})$, defined by Eq. (4.2), as the following form:

$$c(\mathbf{x}) = \max \left\{ \text{tr} \left[\left(\sum_{l=1}^L r_l \mathsf{T}^{(l)}(x^{(l)}) \right) J \right] : \text{tr}_{\text{out}} J = I_{\text{in}}, J \geq 0 \right\}, \quad (4.42)$$

i.e., $c(\mathbf{x})$ is given by the optimum value of the optimization problem

$$\begin{cases} \text{maximize} & \text{tr} \left[\left(\sum_{l=1}^L r_l \mathsf{T}^{(l)}(x^{(l)}) \right) J \right] \\ \text{subject to} & \text{tr}_{\text{out}} J = I_{\text{in}}, \\ & J \geq 0. \end{cases} \quad (4.43)$$

Equation (4.43) is a semidefinite program [41, 17], and thus can be numerically solved by using software packages. For instance, let us consider the same settings as in Example 4.3.2 with the following additional conditions:

$$d_{\text{in}} = d_{\text{out}} = 2, \quad (4.44)$$

$$|\psi^{(1)}\rangle = |0\rangle, \quad (4.45)$$

$$|\psi^{(2)}\rangle = |\phi(\theta)\rangle := \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle, \quad (4.46)$$

$$|e_i^{(1)}\rangle = |i\rangle, \quad (4.47)$$

$$|e_j^{(2)}\rangle = |x_j\rangle, \quad (4.48)$$

where $\theta \in [0, \pi]$. Then, Eq. (4.43) becomes

$$\begin{cases} \text{maximize} & \frac{1}{2} \text{tr} [(|0\rangle\langle 0| \otimes |i\rangle\langle i| + |\phi(\theta)\rangle\langle \phi(\theta)| \otimes |x_j\rangle\langle x_j|) J] \\ \text{subject to} & \text{tr}_{\text{out}} J = I_{\text{in}}, \\ & J \geq 0. \end{cases} \quad (4.49)$$

Figure 4.1 illustrates $c(x_0^{(1)}, x_0^{(2)})$ along with

$$\begin{aligned} & c_{\mathcal{R}}(x_0^{(1)}, x_0^{(2)}) \\ & := \max_{\Lambda \in \mathcal{R}} \left\{ \frac{1}{2} \text{tr} [(|0\rangle\langle 0| \otimes |i\rangle\langle i| + |\phi(\theta)\rangle\langle \phi(\theta)| \otimes |x_j\rangle\langle x_j|) J] \right\} \end{aligned} \quad (4.50)$$

$$= \frac{1}{2} \left(1 + \cos\left(\frac{\theta}{2} - \frac{\pi}{4}\right) \right), \quad (4.51)$$

where $\mathcal{R}$ denotes the set of all random unitary channels and the second equality is shown in Ref. [1]. The figure conforms to the fact that $c(x_0^{(1)}, x_0^{(2)})$ is strictly less than 1 if and only if $\theta < \frac{\pi}{2}$, derived in Ref. [3], and furthermore implies that $c(x_0^{(1)}, x_0^{(2)})$ coincides with $c_{\mathcal{R}}(x_0^{(1)}, x_0^{(2)})$ if $\theta < \frac{\pi}{2}$. Thus, although it is difficult to analytically compute $c(\mathbf{x})$, its numerical calculation is possible through the semidefinite program Eq. (4.43), when the testers are specified. The numerically obtained values enable us to capture the qualitative behavior of $c(\mathbf{x})$, as shown in Fig. 4.1.

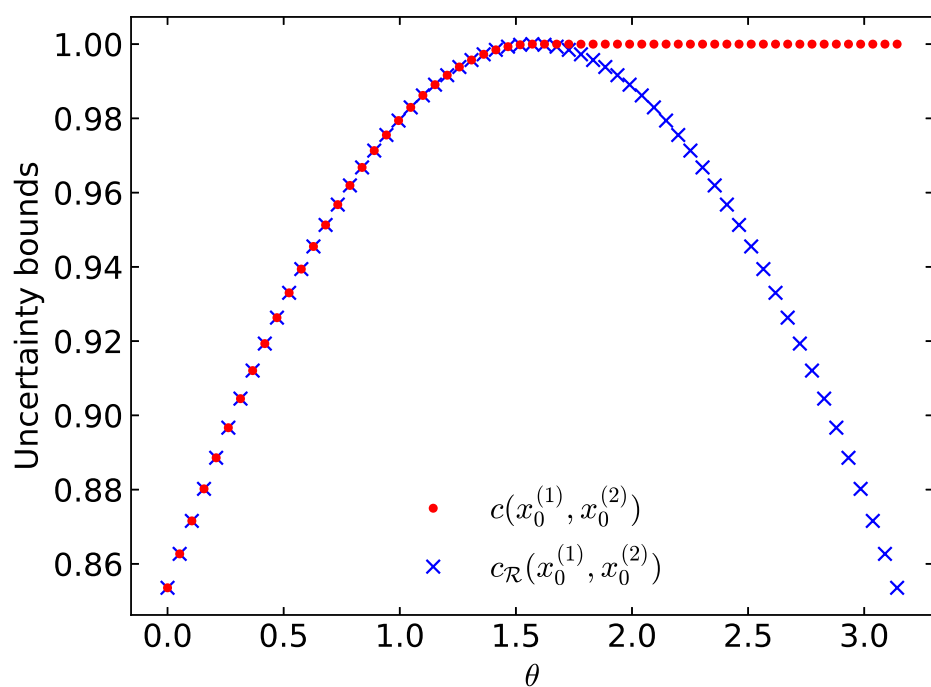


Figure 4.1: A plot of $c(x_0^{(1)}, x_0^{(2)})$ (the red dots), obtained by numerically solving Eq. (4.49), and $c_{\mathcal{R}}(x_0^{(1)}, x_0^{(2)})$ (the blue crosses), given by Eq. (4.51). The values are computed for $\theta = n\pi/60$, where $n \in \{0, 1, \dots, 60\}$. This figure is reproduced from Ref. [2].

4.5 Application to a Quantum Key Distribution Protocol

The fine-grained uncertainty relations for testers can be used to evaluate the security of a quantum key distribution protocol. Here, we treat an extended version of the BB84 protocol where a private key is distributed using a qudit system and L mutually unbiased bases [42, 43]. Consider legitimate users Alice and Bob who want to share a secret key—a sequence of d -ary symbols—to establish a secure classical communication, and an attacker Eve, who attempts to eavesdrop on the key being distributed. Since we focus on individual attacks, which are the simplest type of eavesdropping, the extended BB84 protocol can be regarded as a routine that is repeated for each symbol of the key. The procedure is as follows:

1. State preparation: Alice randomly chooses a symbol $i \in \{0, \dots, d-1\}$ and a basis label $l \in \{1, \dots, L\}$, and encodes i into the quantum state $|\psi_i^{(l)}\rangle$. She then sends this state to Bob through a quantum channel.
2. Eavesdropping (individual attack): Eve intercepts the transmitted state, lets it interact with her quantum memory, and resends a quantum system to Bob.
3. Acknowledgment: Bob notifies Alice, through an authenticated classical channel, that he has received the quantum system.
4. Basis announcement: Alice reveals, via the authenticated classical channel, the basis label l that she used for the encoding.
5. Measurement: Bob and Eve perform the projective measurement given by $\{|\psi_i^{(l)}\rangle\langle\psi_i^{(l)}|\}_{i=0}^{d-1}$ on their respective quantum systems.

Here, $\{|\psi_i^{(l)}\rangle\}_{i=0}^{d-1}$ are orthonormal bases for a d -dimensional Hilbert space such that $|\langle\psi_i^{(l)}|\psi_j^{(m)}\rangle| = \frac{1}{\sqrt{d}}$ if $l \neq m$, where $l, m \in \{1, 2, \dots, L\}$. In addition, it is assumed that Eve is able to intercept both the authenticated classical channel and quantum channel.

For a d -ary symbol i and a basis label l , Eve's success probability under an individual attack is defined as

$$p_{i,\text{success}}^{(l)} = \langle\psi_i^{(l)} \otimes \psi_i^{(l)} | \Lambda(|\psi_i^{(l)}\rangle\langle\psi_i^{(l)}|) | \psi_i^{(l)} \otimes \psi_i^{(l)} \rangle, \quad (4.52)$$

where Λ denotes Eve's interaction. This definition is justified because if $p_{i,\text{success}}^{(l)} = 1$, then Alice, Bob, and Eve all obtain the same d -ary symbol i . Since both i and l are chosen uniformly at random, Eve's overall success probability is given by the average

$$P_{\text{success}} = \frac{1}{dL} \sum_{l=1}^L p_{i,\text{success}}^{(l)}. \quad (4.53)$$

If there exists a quantum channel Λ such that $P_{\text{success}} = 1$, then Eve can extract the entire key without being detected by Alice and Bob. Conversely, if $P_{\text{success}} < 1$ for every possible Λ , then Eve cannot obtain the full key information, and her eavesdropping becomes detectable.

Proposition 4.5.1. *The success probability of Eve's eavesdropping is bounded from above as follows:*

$$P_{\text{success}} \leq \frac{1}{L} + \frac{1}{d} \left(1 - \frac{1}{L}\right). \quad (4.54)$$

Proof. The success probability P_{success} can be expressed as follows:

$$P_{\text{success}} = \frac{1}{L} \sum_{l=1}^L \text{tr} [S^{(l)} J_{\Lambda}] \quad (4.55)$$

where

$$S^{(l)} := \frac{1}{d} \sum_{i=0}^{d-1} |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}|^T \otimes |\psi_i^{(l)} \otimes \psi_i^{(l)}\rangle \langle \psi_i^{(l)} \otimes \psi_i^{(l)}|. \quad (4.56)$$

Each $S^{(l)}$ is regarded as the first element of the tester

$$\left\{ \frac{1}{d} \sum_{i=0}^{d-1} |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}|^T \otimes |\psi_i^{(l)} \otimes \psi_i^{(l)}\rangle \langle \psi_i^{(l)} \otimes \psi_i^{(l)}|, \right. \\ \left. \frac{1}{d} \sum_{i=0}^{d-1} |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}|^T \otimes (I - |\psi_i^{(l)} \otimes \psi_i^{(l)}\rangle \langle \psi_i^{(l)} \otimes \psi_i^{(l)}|) \right\}. \quad (4.57)$$

Thus, using Proposition 4.3.1, we have

$$P_{\text{success}} \leq \frac{1}{L} \left\| \sum_{l=1}^L P^{(l)} \right\|. \quad (4.58)$$

where

$$P^{(l)} := \sum_{i=0}^{d-1} |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}|^T \otimes |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}| \otimes |\psi_i^{(l)}\rangle \langle \psi_i^{(l)}|. \quad (4.59)$$

Furthermore, we can estimate the right-hand side of Eq. (4.58) from above as follows [44]:

$$P_{\text{success}} \leq \frac{1}{L} \max_{m=1}^L \sum_{l=1}^L \|P^{(l)} P^{(m)}\|. \quad (4.60)$$

For all $m \in \{1, 2, \dots, L\}$, it holds that

$$\sum_{l=1}^L \|P^{(l)} P^{(m)}\| = 1 + \frac{L-1}{d}. \quad (4.61)$$

Therefore, we obtain

$$P_{\text{success}} \leq \frac{1}{L} \max_{m=1}^L \sum_{l=1}^L \|P^{(l)} P^{(m)}\| \quad (4.62)$$

$$= \frac{1}{L} \left(1 + \frac{L-1}{d} \right) \quad (4.63)$$

$$= \frac{1}{L} + \frac{1}{d} \left(1 - \frac{1}{L} \right). \quad (4.64)$$

□

This proposition states that Eve cannot succeed in eavesdropping without being unnoticed by Alice and Bob, and furthermore large values of L and d are disadvantageous for Eve, which implies that the protocol becomes more secure. Figure 4.2 plots the right-hand side of Eq. (4.54) for $L = d + 1$, showing that the larger the dimension d is, the smaller Eve's eavesdropping success probability must become. Thus, the fine-grained uncertainty relation for testers provides an upper bound on the Eve's eavesdropping success probability, leading to a quantitative evaluation of the security of the extended BB84 protocol.

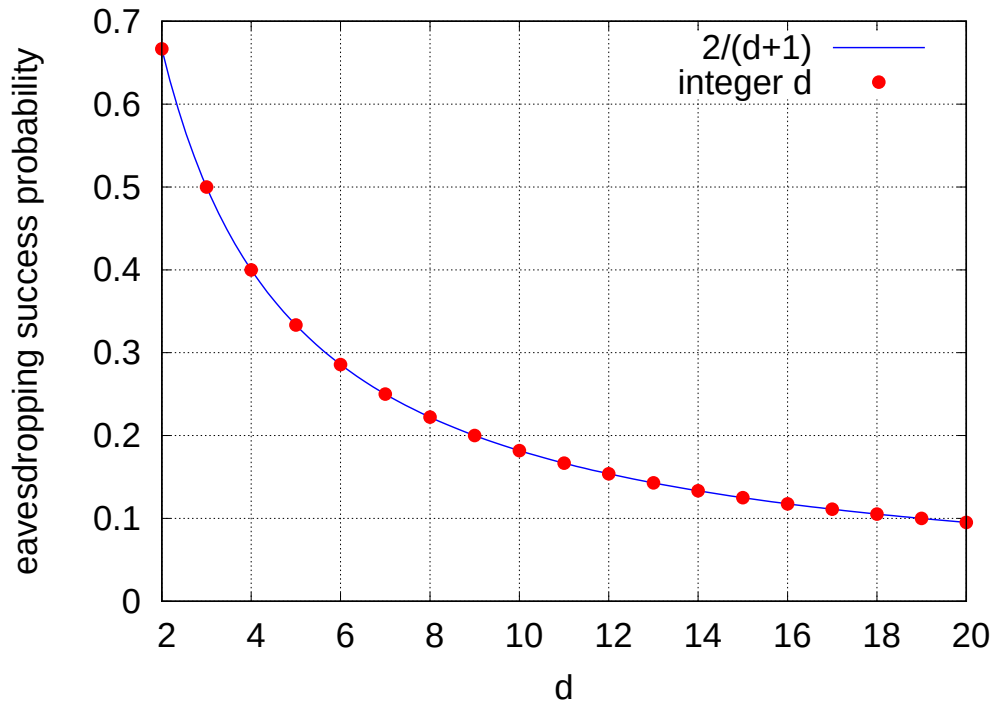


Figure 4.2: A plot of the right-hand side of Eq. (4.54) for $L = d + 1$. This choice of L is possible when d is a power of a prime number.

4.6 Summary and Discussion

In this chapter, we developed the framework of uncertainty relations for testers, pioneered in Ref. [12]. In Sect. 4.2, a fine-grained uncertainty relation is formulated as a set of inequalities for a scheme in which several measurements, described by testers, are stochastically performed on a channel. The derived expression, Eq. (4.1), is regarded as a scalable uncertainty relation. However, it is not simple to analytically compute the generalized uncertainty bound, given by Eq. (4.2), because the bound is defined as the maximum value of a probability. We gave prescriptions in Sects. 4.3 and 4.4 to address this issue. In Sect. 4.3, we provided a relaxed uncertainty bound, and investigated its effectiveness through several examples. Consequently, closed-form expressions of the fine-grained uncertainty relation, Eqs. (4.35) and (4.38), were derived for the cases where testers are given by maximally entangled bases. In Sect. 4.4, we connected the uncertainty bound with a semidefinite program to give a method for numerically computing its value. Figure 4.1 plots the values of uncertainty bound for a particular case, obtained in a numerical investigation. An application to a quantum key distribution protocol was also presented, and it was demonstrated that utilizing large-scale quantum systems is beneficial for legitimate users to securely share keys.

It should be noted that Eq. (4.35) can also be derived using Eq. (2.65), i.e., the conventional fine-grained uncertainty bound. To see this, let us rewrite the left-hand side of the inequality in Eq. (4.35) as follows:

$$\frac{1}{2}p_1(x_i^{(1)}|\Lambda) + \frac{1}{2}p_2(x_j^{(2)}|\Lambda) = \frac{1}{2}\langle\Psi_i^{(1)}|\frac{J_\Lambda}{d}|\Psi_i^{(1)}\rangle + \frac{1}{2}\langle\Psi_j^{(2)}|\frac{J_\Lambda}{d}|\Psi_j^{(2)}\rangle. \quad (4.65)$$

The right-hand side can be connected with the conventional fine-grained uncertainty relation Eq. (2.59) because $\{|\Psi_i^{(1)}\rangle\langle\Psi_i^{(1)}|\}_{i=1}^{d^2-1}$ and $\{|\Psi_j^{(2)}\rangle\langle\Psi_j^{(2)}|\}_{j=1}^{d^2-1}$ are POVMs, and $\frac{J_\Lambda}{d}$ is a state. The application of Eq. (2.65) induces the same upper bound as in Eq. (4.35). Thus, existing uncertainty relations for measurements of states can also be used to quantify uncertainty trade-offs in measurements of channels if the corresponding testers are implemented by a maximally entangled input state and POVMs given by maximally entangled bases. However, note that the formulation Eq. (4.1) is still valuable in spite of this fact because utilizing Eq. (2.59) does not necessarily induce nontrivial evaluation of the generalized uncertainty bound.

As stated previously, Fig. 4.1 implies a nontrivial relationship between

$c(x_i^{(1)}, x_j^{(2)})$ and $c_{\mathcal{R}}(x_i^{(1)}, x_j^{(2)})$, motivating us to propose the following conjecture.

Conjecture 4.6.1. *Suppose the same settings in Example 4.3.2, i.e., Eqs. (4.12) through (4.16), with the additional condition $d_{in} = d_{out} = 2$. For every $i, j \in \{0, 1\}$, if $|\langle \psi^{(1)} | \psi^{(2)} \rangle| > |\langle e_i^{(1)} | e_j^{(2)} \rangle|$, then the following equalities hold:*

$$c(x_i^{(1)}, x_j^{(2)}) = c_{\mathcal{R}}(x_i^{(1)}, x_j^{(2)}) \quad (4.66)$$

$$= \frac{1}{2} \left(1 + |\langle \psi^{(1)} | \psi^{(2)} \rangle| |\langle e_i^{(1)} | e_j^{(2)} \rangle| + \sqrt{(1 - |\langle \psi^{(1)} | \psi^{(2)} \rangle|^2)(1 - |\langle e_i^{(1)} | e_j^{(2)} \rangle|^2)} \right), \quad (4.67)$$

where

$$c_{\mathcal{R}}(x_i^{(1)}, x_j^{(2)}) := \max_{\Lambda \in \mathcal{R}} \left\{ \frac{1}{2} p_1(x_i^{(1)} | \Lambda) + \frac{1}{2} p_2(x_j^{(2)} | \Lambda) \right\} \quad (4.68)$$

and Eq. (4.67) is shown in Ref. [1].

This conjecture asserts that, for a specific case, the maximization in Eq. (4.2) is achieved within $\mathcal{R}$ (in fact, if this is true, then the maximum in Eq. (4.2) is attained by a unitary channel), and furthermore $c(x_i^{(1)}, x_j^{(2)})$ is expressed as a simple formula, i.e., Eq. (4.67).

Finally, let us mention a possible generalization of $\mathcal{V}$, given by Eq. (4.1). We can consider the following set of inequalities:

$$\mathcal{V}(\mathcal{A}) := \left\{ \sum_{l=1}^L r_l \sum_{x^{(l)} \in \mathcal{X}_l} p_l(x^{(l)} | \Lambda) \leq c_{\mathcal{A}}(\mathcal{X}) : \mathcal{X} := (\mathcal{X}_1, \dots, \mathcal{X}_L) \in \prod_{l=1}^L 2^{\Omega_l} \right\}, \quad (4.69)$$

where $\mathcal{A}$ is a subset of channels, 2^{Ω_l} denotes the power set of Ω_l for each $l \in \{1, \dots, L\}$, and $\prod_{l=1}^L 2^{\Omega_l}$ represents the Cartesian product of $2^{\Omega_1}, \dots, 2^{\Omega_L}$. For every $\mathcal{X} = (\mathcal{X}_1, \dots, \mathcal{X}_L) \in \prod_{l=1}^L 2^{\Omega_l}$, the bound is defined as

$$c_{\mathcal{A}}(\mathcal{X}) := \max_{\Lambda \in \mathcal{A}} \left\{ \sum_{l=1}^L r_l \sum_{x^{(l)} \in \mathcal{X}_l} p_l(x^{(l)} | \Lambda) \right\}, \quad (4.70)$$

i.e., it is the maximum value of the probability of obtaining an outcome in the subsets $\mathcal{X}_1, \dots, \mathcal{X}_L$, when a channel is chosen from $\mathcal{A}$. Thus, each inequality in $\mathcal{V}(\mathcal{A})$ implies a trade-off relationship between the probability distributions $p_1, \dots, p_L$ by imposing a restriction on

$$\sum_{x^{(1)} \in \mathcal{X}_1} p_1(x^{(1)}|\Lambda), \dots, \sum_{x^{(L)} \in \mathcal{X}_L} p_L(x^{(L)}|\Lambda) \quad (4.71)$$

under the constraint that a channel Λ can be prepared within $\mathcal{A}$. Clearly, $\mathcal{V}(\mathcal{A})$ serves as an extension of $\mathcal{V}$, because $\mathcal{V} \subseteq \mathcal{V}(\mathcal{A})$ holds if $\mathcal{A}$ is the set of all channels. The introduction of $\mathcal{A}$ makes the calculation of uncertainty bound more tractable. For instance, Eq. (4.67) corresponds to a case of $\mathcal{A} = \mathcal{R}$, and is expressed as a simple formula, without using an optimization problem. In addition to random unitary channels, various important types of channels, such as entanglement breaking channels [21], appear in the context of quantum information processing. Thus, investigating $\mathcal{V}(\mathcal{A})$ for such classes of channels is regarded as an interesting research direction.

Chapter 5

Upper Bounds on Probabilities in Channel Measurements on Qubit Channels and Their Applications

In this chapter, we investigate upper bounds on the probabilities associated with measurements on qubit channels. We show that, for typical subsets of channels, the probabilities are bounded from above using simple functions that are independent of a channel to be measured. Two basic problems are also considered in order to demonstrate the effectiveness of the obtained upper bounds.

5.1 Introduction

As we have seen so far, the probability distributions arising from measurements of quantum testers depend on the underlying quantum channel. Therefore, even for a single tester, uncertainty can arise when the channel to be examined is subject to certain restrictions. More concretely, two factors constitute the primary sources of such uncertainty:

1. locality constraints, where only one subsystem of a composite system undergoes time evolution; and
2. restrictions on the admissible types of time evolution.

The resulting uncertainty can thus be regarded as an interesting indicator that characterizes these constraints.

This chapter aims to provide several upper bounds on the probabilities associated with measurements performed on a qubit channel. Such upper bounds quantify the likelihood of certain events and can be regarded as one of the most fundamental measures of (un)certainty. As in Ch. 3, although restricting our attention to qubit channels is a strong limitation, these bounds are expected to serve as elementary constraints for large-scale physical systems composed of many qubits. The effectiveness of the upper bounds is demonstrated through two topics. The first one is a kind of convertibility problem defined on pairs of pure states, and the second one is a detection problem of a parametrized unital channel.

5.2 Estimation of Probabilities in Channel Measurements

Let $\mathcal{H}$ be a two-dimensional Hilbert space, let S be a positive operator on $\mathcal{H} \otimes \mathcal{H}$ such that $S \leq \rho_1^T \otimes I$ for some state ρ_1 , and let $\Lambda: \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H})$ be a channel in a subset $\mathcal{X}$ of channels. The operator S can be regarded as an element of a tester, whose normalization condition is given by $\rho_1^T \otimes I$. Hence,

$$p(\Lambda) = \text{tr}[SJ_\Lambda] \quad (5.1)$$

represents the probability of obtaining an outcome assigned to S upon the measurement of Λ . The purpose of this section is to estimate the maximum values of this probability with respect to several subsets of channels, i.e., to provide upper bounds on $\max_{\Lambda \in \mathcal{X}} p(\Lambda)$.

An upper bound on $\max_{\Lambda \in \mathcal{X}} p(\Lambda)$ has a clear physical meaning. Let us imagine a game that proceeds as follows by Alice, who has a device for measuring channels, and Bob, who has the ability to prepare a channel and knows what measurement device Alice possesses:

1. Alice chooses an outcome of the measurement device, and communicates it to Bob.
2. Bob prepares a channel based on the selected outcome and the specification of Alice's measurement device. Then, Bob sends the prepared channel to Alice.

3. Alice probes the sent channel using the measurement device.

Bob wins the game if the measurement outcome produced in the final step matches the outcome chosen by Alice in the first step. It is possible to associate S with the tester element that corresponds to the outcome selected by Alice, Λ with the channel prepared by Bob, and $p(\Lambda)$ with Bob's winning probability. Thus, an upper bound on $\max_{\Lambda \in \mathcal{X}} p(\Lambda)$ represents a limit of the maximum winning probability, when Bob is able to prepare a channel within $\mathcal{X}$; if such an upper bound is strictly less than 1, then there is a possibility of Bob's losing the game.

Instead of $\max_{\Lambda \in \mathcal{X}} p(\Lambda)$, we analyze

$$C(\tau, \mathcal{X}) := \max_{\Lambda \in \mathcal{X}} \text{tr} [\tau J_\Lambda], \quad (5.2)$$

defined for each state τ on $\mathcal{H} \otimes \mathcal{H}$, as estimating $\max_{\Lambda \in \mathcal{X}} p(\Lambda)$ is equivalent to estimating $C(\tau, \mathcal{X})$. Indeed, without loss of generality, we can assume $S \neq 0$, and therefore the probability is expressed as

$$p(\Lambda) = (\text{tr } S) \text{tr} [\tau_S J_\Lambda] \quad (5.3)$$

where $\tau_S := \frac{S}{\text{tr } S}$, meaning

$$\max_{\Lambda \in \mathcal{X}} p(\Lambda) = C(\tau_S, \mathcal{X}). \quad (5.4)$$

By employing $C(\tau, \mathcal{X})$, we can utilize quantities defined for a state. Let τ be a state on $\mathcal{H} \otimes \mathcal{H}$. The reduced state on the second Hilbert space is represented as τ_2 , i.e., $\tau_2 := \text{tr}_1 \tau$, where tr_1 denotes the partial trace with respect to the first Hilbert space. The *Bloch vector* of τ_2 is expressed as $\mathbf{b}(\tau_2)$, where $b_i(\tau_2) = \text{tr} [\sigma_i \tau_2]$ for all $i \in \{1, 2, 3\}$, and its *Euclidean norm* is written as $\|\mathbf{b}(\tau_2)\|$, i.e.,

$$\|\mathbf{b}(\tau_2)\| := \sqrt{\sum_{i=1}^3 b_i(\tau_2)^2}. \quad (5.5)$$

The expectation values $N_{ij}(\tau) := \text{tr} [(\sigma_i \otimes \sigma_j) \tau]$ compose the *correlation matrix* $N(\tau)$, i.e., $N_{ij}(\tau) := \text{tr} [(\sigma_i \otimes \sigma_j) \tau]$ for all $i, j \in \{1, 2, 3\}$. Two types of norms related to $N(\tau)$ are used later. Let $s_1(N(\tau))$, $s_2(N(\tau))$, and $s_3(N(\tau))$ be the singular values of $N(\tau)$, i.e., the eigenvalues of $\sqrt{N(\tau)^T N(\tau)}$. The

matrix norm of $N(\tau)$, induced by the Euclidean norm, is denoted as $\|N(\tau)\|$ and given by

$$\|N(\tau)\| = \max\{s_i(N(\tau)) : i \in \{1, 2, 3\}\}, \quad (5.6)$$

i.e., $\|N(\tau)\|$ is equal to the largest singular value of $N(\tau)$. The *Ky Fan norm* of $N(\tau)$ is expressed as $\|N(\tau)\|_{\text{KF}}$ and given by

$$\|N(\tau)\|_{\text{KF}} := \sum_{i=1}^3 s_i(N(\tau)), \quad (5.7)$$

i.e., $\|N(\tau)\|_{\text{KF}}$ is equal to the sum of all singular values of $N(\tau)$.

In the following subsections, we present the estimation of $C(\tau, \mathcal{X})$ for cases where $\mathcal{X}$ are given by the sets of

1. depolarizing channels,
2. unital channels,
3. entanglement breaking channels,
4. unital entanglement breaking channels, and
5. general qubit channels;

see Sect. 2 for more details about basic properties of these types of channels.

5.2.1 Depolarizing channels

A channel on $\mathcal{L}(\mathcal{H})$ is called a depolarizing channel if and only if, for every linear operator A on $\mathcal{H}$, it acts as follows:

$$\Lambda(A) = (\text{tr } A)\rho, \quad (5.8)$$

where ρ is a state on $\mathcal{H}$. Let $\mathcal{D}$ denote the set of all depolarizing channels on $\mathcal{L}(\mathcal{H})$. If $\mathcal{X} = \mathcal{D}$, the right-hand side of Eq. (5.2) can be explicitly represented as follows:

Proposition 5.2.1. *The following equality holds:*

$$C(\tau, \mathcal{D}) = \frac{1}{2} (1 + \|\mathbf{b}(\tau_2)\|). \quad (5.9)$$

5.2.2 Unital channels

A channel is said to be *unital* if and only if it preserves the identity operator. In Ref. [45], it was shown that, for qubit systems, any unital channel is also written as a random unitary channel, i.e., a convex combination of unitary channels. Thus, we can identify unital channels with random unitary channels, as $\mathcal{H}$ is two-dimensional. Let $\mathcal{R}$ denote the set of all random unitary channels on $\mathcal{L}(\mathcal{H})$. Similar to the case of $\mathcal{X} = \mathcal{D}$, a formula of $C(\tau, \mathcal{R})$ is explicitly obtained as follows by connecting $C(\tau, \mathcal{R})$ with the FEF of τ and utilizing an analytical expression of the FEF derived in Ref. [35]:

Proposition 5.2.2. *The following equality holds:*

$$C(\tau, \mathcal{R}) = \frac{1}{2} (1 + \|N(\tau)\|_{KF}). \quad (5.10)$$

5.2.3 Entanglement breaking channels

A channel Λ on $\mathcal{L}(\mathcal{H})$ is called entanglement breaking channel if and only if it transforms all states on $\mathcal{H} \otimes \mathcal{H}$ into separable states. Let $\mathcal{GE}$ be the set of all entanglement breaking channels on $\mathcal{L}(\mathcal{H})$. The quantity $C(\tau, \mathcal{GE})$ can be bounded from above using $\|\mathbf{b}(\tau_2)\|$ and $\|N(\tau)\|$ as follows:

Proposition 5.2.3. *It holds that*

$$C(\tau, \mathcal{GE}) \leq \frac{1}{2} \left(1 + \sqrt{\|\mathbf{b}(\tau_2)\|^2 + \|N(\tau)\|^2} \right) \quad (5.11)$$

$$=: \tilde{C}(\tau, \mathcal{GE}). \quad (5.12)$$

5.2.4 Unital entanglement breaking channels

Let $\mathcal{UE}$ be the set of all unital entanglement breaking channels on $\mathcal{L}(\mathcal{H})$, i.e., $\mathcal{UE} = \mathcal{R} \cap \mathcal{GE}$. The quantity $C(\tau, \mathcal{UE})$ can be bounded from above using $\|N(\tau)\|$ as follows:

Proposition 5.2.4. *It holds that*

$$C(\tau, \mathcal{UE}) \leq \frac{1}{2} (1 + \|N(\tau)\|) \quad (5.13)$$

$$=: \tilde{C}(\tau, \mathcal{UE}). \quad (5.14)$$

5.2.5 General qubit channels

Let $\mathcal{C}$ denote the set of all channels on $\mathcal{L}(\mathcal{H})$, i.e., linear, completely positive, and trace-preserving maps. The quantity $C(\tau, \mathcal{C})$ can be bounded from above using $\|\mathbf{b}(\tau_2)\|$ and $\|N(\tau)\|_{\text{KF}}$ as follows:

Proposition 5.2.5. *It holds that*

$$C(\tau, \mathcal{C}) \leq \frac{1}{2} \left(1 + \sqrt{\|\mathbf{b}(\tau_2)\|^2 + \|N(\tau)\|_{\text{KF}}^2} \right) \quad (5.15)$$

$$=: \tilde{C}(\tau, \mathcal{C}). \quad (5.16)$$

Note that while the formulas of $\tilde{C}(\tau, \mathcal{GE})$ and $\tilde{C}(\tau, \mathcal{C})$ resemble each other, the former and latter are expressed using the matrix norm $\|N(\tau)\|$ and the Ky Fan norm $\|N(\tau)\|_{\text{KF}}$, respectively.

Although the proposition provides an estimate for $C(\tau, \mathcal{C})$, it is possible to obtain the exact expression of $C(\tau, \mathcal{C})$ in a specific case as follows, by combining Eq. (5.15) with Eq. (5.10):

Corollary 5.2.6. *If $\tau_2 = \frac{I}{2}$, then it holds that*

$$C(\tau, \mathcal{C}) = \frac{1}{2} (1 + \|N(\tau)\|_{\text{KF}}). \quad (5.17)$$

For instance, it follows from this corollary that

$$C\left(\sum_x p_x |\Psi_x\rangle \langle \Psi_x|, \mathcal{C}\right) = \frac{1}{2} \left(1 + \left\| N\left(\sum_x p_x |\Psi_x\rangle \langle \Psi_x|\right) \right\|_{\text{KF}} \right) \quad (5.18)$$

where $\{p_x\}_x$ is a probability distribution and $|\Psi_x\rangle$ is a maximally entangled state for each x . Thus, if τ is a mixture of maximally entangled states, then the exact value of $C(\tau, \mathcal{C})$ can be obtained by calculating $\|N(\tau)\|_{\text{KF}}$.

5.2.6 Comparison of the upper bounds

The subsets of channels appearing in the preceding subsections can be characterized by how they treat entanglement. Therefore, a tester whose input state and output POVM measurement are both given by entangled states can be regarded as good examples for comparing the upper bounds presented so

far. Among such testers, the one that has the element given by the following operator is the simplest instance:

$$S = \frac{1}{2} |\Psi_w\rangle \langle \Psi_w| \quad (5.19)$$

where $0 \leq w \leq \frac{1}{2}$, and

$$|\Psi_w\rangle := \sqrt{w} |00\rangle + \sqrt{1-w} |11\rangle, \quad (5.20)$$

of which the degree of entanglement increases as w becomes larger. Let $p_w(0)$ be the probability associated with S upon the measurement performed on a channel Λ in a subset $\mathcal{X}$, i.e.,

$$p_w(0) = \text{tr}[S J_\Lambda] \quad (5.21)$$

$$= \frac{1}{2} \text{tr}[|\Psi_w\rangle \langle \Psi_w| J_\Lambda]. \quad (5.22)$$

Thus, the maximum probability is bounded from as follows:

$$\max_{\Lambda \in \mathcal{X}} p_w(0) = \frac{1}{2} C(|\Psi_w\rangle \langle \Psi_w|, \mathcal{X}). \quad (5.23)$$

By utilizing the upper bounds in the preceding subsections, we have

$$\max_{\Lambda \in \mathcal{D}} p_w(0) = \frac{1}{2} (1 - w), \quad (5.24)$$

$$\max_{\Lambda \in \mathcal{R}} p_w(0) = \frac{1}{2} \left(1 + 2\sqrt{w(1-w)} \right), \quad (5.25)$$

$$\max_{\Lambda \in \mathcal{GE}} p_w(0) \leq \frac{1}{4} \left(1 + \sqrt{4w^2 - 4w + 2} \right), \quad (5.26)$$

$$\max_{\Lambda \in \mathcal{UE}} p_w(0) \leq \frac{1}{2}, \quad (5.27)$$

$$\max_{\Lambda \in \mathcal{C}} p_w(0) \leq \frac{1}{4} \left(1 + \sqrt{(2w-1)^2 + (1 + 4\sqrt{w(1-w)})^2} \right). \quad (5.28)$$

Figure 5.1 plots these values as functions of w . As can be seen from this figure, all the upper limits on the maximum probabilities given by Eqs. (5.24)-(5.28) are less than 1 and take mutually different values. This demonstrates that the nontrivial nature of the upper bounds provided in the previous subsections. In addition, this figure illustrates how the effect of a

channel on an entangled state contributes to the resulting uncertainty. Since the subsets $\mathcal{R}$ and $\mathcal{C}$ contain channels that preserve entanglement, the upper bounds on the maximum probabilities are proportional to w . On the other hand, since channels in $\mathcal{D}$, $\mathcal{GE}$, and $\mathcal{UE}$ break entanglement, the upper bounds on the maximum probabilities do not scale proportionally with w . In particular, because channels in $\mathcal{D}$ discard the input state and destroy even classical correlations, the maximum probability decreases as w increases.

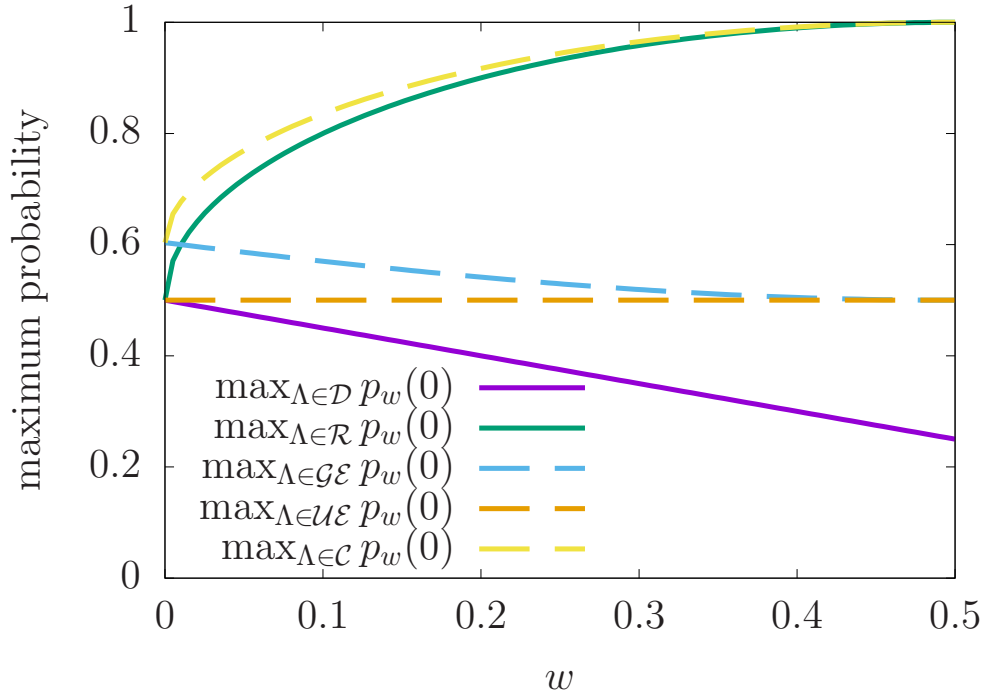


Figure 5.1: A plot of the maximum probabilities given from Eqs. (5.24)-(5.28) as functions of w . The dashed lines represent upper bounds on the maximum probabilities, while the solid lines represent the exact values.

5.2.7 Remarks on the upper bounds

The upper bounds are explicitly represented as functions of $\|\mathbf{b}(\tau_2)\|$, $\|N(\tau)\|$, or $\|N(\tau)\|_{\text{KF}}$. These representations serve as useful tools for evaluating the upper limits on probabilities, as will be described in later subsections. Note

that while the upper bounds for $\mathcal{D}$ and $\mathcal{R}$ coincide with $C(\tau, \mathcal{X})$, i.e., they are optimal, those for $\mathcal{UE}$, $\mathcal{GE}$, and $\mathcal{C}$, respectively defined as $\tilde{C}(\tau, \mathcal{GE})$, $\tilde{C}(\tau, \mathcal{UE})$, and $\tilde{C}(\tau, \mathcal{C})$, are estimates.

It seems that the estimate of $C(\tau, \mathcal{C})$, given by $\tilde{C}(\tau, \mathcal{C})$, is sufficient for bounding probabilities because $\mathcal{C}$ is by definition comprised of all channels. However, it holds that

$$\tilde{C}(\tau, \mathcal{UE}) \leq C(\tau, \mathcal{R}) \leq \tilde{C}(\tau, \mathcal{C}), \quad (5.29)$$

$$C(\tau, \mathcal{D}), \tilde{C}(\tau, \mathcal{UE}) \leq \tilde{C}(\tau, \mathcal{GE}) \leq \tilde{C}(\tau, \mathcal{C}). \quad (5.30)$$

Hence, if $\Lambda \in \mathcal{X} \subseteq \mathcal{Y}$, then $C(\tau, \mathcal{X})$ or $\tilde{C}(\tau, \mathcal{X})$ is better than $C(\tau, \mathcal{Y})$ or $\tilde{C}(\tau, \mathcal{Y})$ as an upper bound. For instance, in the game described previously, if Bob can only prepare a unital channel, then $C(\tau, \mathcal{R})$ should be used, rather than $\tilde{C}(\tau, \mathcal{C})$, to evaluate the maximum winning probability.

5.3 Joint Convertibility

The upper bounds given in the previous section can be utilized to quantify a notion of convertibility related to pairs of states. Let $\mathcal{H}$ be a two-dimensional Hilbert space, let $(|\psi\rangle, |\phi\rangle)$ and $(|e\rangle, |f\rangle)$ be pairs of pure states, and let $\mathcal{X}$ be a subset of channels on $\mathcal{L}(\mathcal{H})$.

Definition 5.3.1. We say that $(|\psi\rangle, |\phi\rangle)$ is *jointly convertible* into $(|e\rangle, |f\rangle)$ within $\mathcal{X}$ if and only if there is a channel $\Lambda \in \mathcal{X}$ such that

$$|e\rangle\langle e| = \Lambda(|\psi\rangle\langle\psi|), \quad (5.31)$$

$$|f\rangle\langle f| = \Lambda(|\phi\rangle\langle\phi|). \quad (5.32)$$

This notion of convertibility is a modification of that addressed in Ref. [46], in which the case where $\mathcal{X}$ is the set of all qubit channels was analyzed. In particular, a necessary and sufficient condition of the joint convertibility within the set of all qubit channels was derived for arbitrary pairs of mixed states in Ref. [46]. Thus, Definition 5.3.1 extends the notion of convertibility in Ref. [46] for pairs of pure states by introducing the additional constraint $\Lambda \in \mathcal{X}$. For instance, the following question is related to Definition 5.3.1: can a pair of pure states be converted into another using a specific type of channel?

The joint convertibility within $\mathcal{X}$ can be quantified by the maximum average squared fidelity given by

$$F_{\max}(\mathcal{X}) := \max_{\Lambda \in \mathcal{X}} \left\{ \frac{1}{2} \sqrt{F}(|e\rangle\langle e|, \Lambda(|\psi\rangle\langle\psi|))^2 + \frac{1}{2} \sqrt{F}(|f\rangle\langle f|, \Lambda(|\phi\rangle\langle\phi|))^2 \right\}. \quad (5.33)$$

Here, $\sqrt{F}(|\xi\rangle\langle\xi|, \rho) := \sqrt{\langle\xi|\rho|\xi\rangle}$ is a measure of closeness between states $|\xi\rangle\langle\xi|$ and ρ known as the *fidelity* between $|\xi\rangle\langle\xi|$ and ρ (cf. Refs. [15, 16, 17]). (We use the notation $\sqrt{F}$ to emphasize that the fidelity is given not by $\langle\xi|\rho|\xi\rangle$, which some works, e.g., Refs. [18, 47], employ as the definition of the fidelity, but by $\sqrt{\langle\xi|\rho|\xi\rangle}$.) For instance, $\sqrt{F}(|\xi\rangle\langle\xi|, \rho) = 1$ if and only if $|\xi\rangle\langle\xi| = \rho$. Therefore, $F_{\max}(\mathcal{X})$ expresses the maximum of the average closeness

$$F_{\text{av}}(\Lambda) := \frac{1}{2} \sqrt{F}(|e\rangle\langle e|, \Lambda(|\psi\rangle\langle\psi|))^2 + \frac{1}{2} \sqrt{F}(|f\rangle\langle f|, \Lambda(|\phi\rangle\langle\phi|))^2 \quad (5.34)$$

under the constraint that $\Lambda \in \mathcal{X}$. Thus, $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{X}$ if and only if $F_{\max}(\mathcal{X})$ is equal to 1.

The quantity $F_{\max}(\mathcal{X})$ is expressed using $C(\tau, \mathcal{X})$, defined in Eq. (5.2). A direct computation shows that the following equality holds:

$$F_{\max}(\mathcal{X}) = C(\tau_0, \mathcal{X}) \quad (5.35)$$

where

$$\tau_0 := \frac{1}{2} \left(|\psi\rangle\langle\psi|^T \otimes |e\rangle\langle e| + |\phi\rangle\langle\phi|^T \otimes |f\rangle\langle f| \right). \quad (5.36)$$

Thus, the upper bounds, provided in the previous section, serve as estimates or closed-form expressions of $F_{\max}(\mathcal{X})$. In the following subsections, we apply the upper bounds to $F_{\max}(\mathcal{X})$, and provide the condition of joint convertibility for each subset.

5.3.1 Depolarizing channels

The following equality follows from Eq. (5.9):

$$C(\tau_0, \mathcal{D}) = \frac{1}{2} (1 + \|\mathbf{b}(\tau_{0,2})\|), \quad (5.37)$$

where $\tau_{0,2} := \text{tr}_1 \tau_0$. It is easy to obtain

$$\|\mathbf{b}(\tau_{0,2})\| = |\langle e|f\rangle|. \quad (5.38)$$

Thus, we have the following corollary.

Corollary 5.3.2. *The following equality holds:*

$$F_{\max}(\mathcal{D}) = \frac{1}{2} (1 + |\langle e|f\rangle|). \quad (5.39)$$

The right-hand side is equal to 1 if and only if $|\langle e|f\rangle| = 1$. Thus, $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{D}$ if and only if $|\langle e|f\rangle| = 1$.

It is interesting to find the optimal depolarizing channels, i.e., the elements in $\mathcal{D}$ that achieve the maximization of $F_{\max}(\mathcal{D}) = \max_{\Lambda \in \mathcal{D}} F_{\text{av}}(\Lambda)$.

Proposition 5.3.3. *If $|\langle e|f\rangle| = 0$, arbitrary depolarizing channels achieve the maximization in $F_{\max}(\mathcal{D}) = \max_{\Lambda \in \mathcal{D}} F_{\text{av}}(\Lambda) = \frac{1}{2}$. If $|\langle e|f\rangle| \neq 0$, the maximization is achieved by $\Lambda \in \mathcal{D}$ that acts as follows for any linear operator A :*

$$\Lambda(A) = (\text{tr } A) |e_+\rangle \langle e_+| \quad (5.40)$$

where

$$|e_+\rangle := \frac{1}{\sqrt{2(1 + |\langle e|f\rangle|)}} \left(|e\rangle + \frac{\langle f|e\rangle}{|\langle e|f\rangle|} |f\rangle \right). \quad (5.41)$$

For later use, we introduce two normalized vectors $|u, v, \pm\rangle$ related a pair of pure states $(|u\rangle, |v\rangle)$ such that $|\langle u|v\rangle| \neq 1$. These vectors are defined as follows:

$$|u, v, \pm\rangle := \begin{cases} \frac{1}{\sqrt{2(1 \pm |\langle u|v\rangle|)}} \left(|u\rangle \pm \frac{\langle v|u\rangle}{|\langle u|v\rangle|} |v\rangle \right) & \text{if } 0 < |\langle u|v\rangle| < 1, \\ \frac{1}{\sqrt{2}} (|u\rangle \pm |v\rangle) & \text{if } |\langle u|v\rangle| = 0, \end{cases} \quad (5.42)$$

and if $|\langle u|v\rangle| = 1$

$$|u, v, +\rangle := |u\rangle, \quad (5.43)$$

$$|u, v, -\rangle := |u^\perp\rangle, \quad (5.44)$$

where $|u^\perp\rangle$ is a normalized vector orthogonal to $|u\rangle$. It is easy to verify that $\{|u, v, \pm\rangle\}$ is an orthonormal basis. In the Bloch representation, $\mathbf{b}(|u, v, \pm\rangle\langle u, v, \pm|)$ are respectively associated with the different arcs of the circle determined by $\mathbf{b}(|u\rangle\langle u|)$ and $\mathbf{b}(|v\rangle\langle v|)$ if $|\langle u|v\rangle| \neq 1$, where $\mathbf{b}(\cdot)$ denotes the Bloch vector of its argument. Specifically, $\mathbf{b}(|u, v, +\rangle\langle u, v, +|)$ points at the midpoint of the arc that is shorter than or equal to the other arc, while $\mathbf{b}(|u, v, -\rangle\langle u, v, -|)$ points at the midpoint of the other arc. If $|\langle u|v\rangle| = 1$, it clearly follows that

$$\mathbf{b}(|u, v, +\rangle\langle u, v, +|) = -\mathbf{b}(|u, v, -\rangle\langle u, v, -|) = \mathbf{b}(|u\rangle\langle u|) = \mathbf{b}(|v\rangle\langle v|). \quad (5.45)$$

Algebraically, $|u, v, +\rangle$ and $|u, v, -\rangle$ are the eigenvectors of $|u\rangle\langle u| + |v\rangle\langle v|$ corresponding to the largest and smallest eigenvalues, respectively. Thus, due to $|e_+\rangle = |e, f, +\rangle$, we can say that the maximization in $F_{\max}(\mathcal{D}) = \max_{\Lambda \in \mathcal{D}} F_{\text{av}}(\Lambda)$ is achieved by a depolarizing channel that outputs the eigenstate of $|e\rangle\langle e| + |f\rangle\langle f|$ corresponding to the largest eigenvalue.

5.3.2 Unital channels

Equation (5.10) implies

$$C(\tau_0, \mathcal{R}) = \frac{1}{2} (1 + \|N(\tau_0)\|_{\text{KF}}). \quad (5.46)$$

As stated previously, $\|N(\tau_0)\|_{\text{KF}}$ is given by the sum of all singular values of $N(\tau_0)$, calculated as follows:

Lemma 5.3.4. *The multiset of singular values of $N(\tau_0)$ is*

$$\left\{ |\langle \psi|\phi\rangle| |\langle e|f\rangle|, \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)}, 0 \right\}. \quad (5.47)$$

Thus, by utilizing this lemma, we obtain

$$\|N(\tau_0)\|_{\text{KF}} = |\langle \psi|\phi\rangle| |\langle e|f\rangle| + \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)}. \quad (5.48)$$

Consequently, the following corollary follows.

Corollary 5.3.5. *The following equality holds:*

$$\begin{aligned} F_{\max}(\mathcal{R}) &= \frac{1}{2} \left(1 + |\langle \psi|\phi\rangle| |\langle e|f\rangle| + \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)} \right). \end{aligned} \quad (5.49)$$

The right-hand side is equal to 1 if and only if $|\langle\psi|\phi\rangle| = |\langle e|f\rangle|$. Thus, $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{R}$ if and only if $|\langle\psi|\phi\rangle| = |\langle e|f\rangle|$.

Similar to the case of $\mathcal{D}$, we obtain the following proposition pertaining to the optimal random unitary channels.

Proposition 5.3.6. *The maximization in $F_{\max}(\mathcal{R}) = \max_{\Lambda \in \mathcal{R}} F_{av}(\Lambda)$ is achieved by a unitary channel $\Lambda \in \mathcal{R}$ that acts as follows on any linear operator A :*

$$\Lambda(A) = UAU^\dagger \quad (5.50)$$

where U is the unitary operator defined as

$$U := |e, f, +\rangle \langle\psi, \phi, +| + |e, f, -\rangle \langle\psi, \phi, -|. \quad (5.51)$$

In particular, if $(|\langle\psi|\phi\rangle|, |\langle e|f\rangle|) \in \{(0, 1), (1, 0)\}$, arbitrary random unitary channels achieve the maximization in $F_{\max}(\mathcal{R}) = \max_{\Lambda \in \mathcal{R}} F_{av}(\Lambda) = \frac{1}{2}$.

This proposition can be verified by utilizing the following equalities:

$$\langle u|u, v, \pm\rangle = \sqrt{\frac{1 \pm |\langle u|v\rangle|}{2}}, \quad (5.52)$$

$$\langle v|u, v, \pm\rangle = \pm \frac{\langle v|u\rangle}{|\langle u|v\rangle|} \sqrt{\frac{1 \pm |\langle u|v\rangle|}{2}} \quad (5.53)$$

where $\frac{\langle v|u\rangle}{|\langle u|v\rangle|}$ is interpreted as 1 if $|\langle u|v\rangle| = 0$. The vectors $|\psi, \phi, +\rangle$ and $|e, f, +\rangle$ are the eigenvectors of $|\psi\rangle\langle\psi| + |\phi\rangle\langle\phi|$ and $|e\rangle\langle e| + |f\rangle\langle f|$ corresponding to the largest eigenvalues, respectively. Thus, U represents a unitary operator that maps the eigenvectors of $|\psi\rangle\langle\psi| + |\phi\rangle\langle\phi|$ to those of $|e\rangle\langle e| + |f\rangle\langle f|$, and in particular, it maps the eigenvector corresponding to the largest eigenvalue of the former operator to that of the latter.

5.3.3 Entanglement breaking channels

Equation (5.11) implies

$$C(\tau_0, \mathcal{GE}) \leq \frac{1}{2} \left(1 + \sqrt{\|\mathbf{b}(\tau_{0,2})\|^2 + \|N(\tau_0)\|^2} \right). \quad (5.54)$$

As described previously, $\|N(\tau_0)\|$ is given by the largest singular value of $N(\tau_0)$, i.e., it holds that

$$\|N(\tau_0)\| = \max \left\{ |\langle \psi | \phi \rangle| |\langle e | f \rangle|, \sqrt{(1 - |\langle \psi | \phi \rangle|^2)(1 - |\langle e | f \rangle|^2)} \right\}. \quad (5.55)$$

Consequently, the following corollary is obtained by using Eqs. (5.38) and (5.47).

Corollary 5.3.7. *The following inequality holds:*

$$F_{\max}(\mathcal{GE}) \leq \frac{1}{2} \left[1 + (|\langle e | f \rangle|)^2 + \max \left\{ |\langle \psi | \phi \rangle|^2 |\langle e | f \rangle|^2, (1 - |\langle \psi | \phi \rangle|^2)(1 - |\langle e | f \rangle|^2) \right\} \right]^{1/2}. \quad (5.56)$$

This corollary provides an upper bound of $F_{\max}(\mathcal{GE})$. Note that the right-hand side of Eq. (5.56) can be greater than or equal to 1. For instance, if $|\langle \psi | \phi \rangle| = 1$, Eq. (5.56) becomes

$$F_{\max}(\mathcal{GE}) \leq \frac{1}{2} \left(1 + \sqrt{2} |\langle e | f \rangle| \right), \quad (5.57)$$

which is meaningful only when $|\langle e | f \rangle| < \frac{1}{\sqrt{2}}$. Thus, Eq. (5.56) gives a necessary condition for the joint convertibility within $\mathcal{GE}$. In other words, if the right-hand side of Eq. (5.56) is strictly less than 1, $(|\psi\rangle, |\phi\rangle)$ is not jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{GE}$.

In some cases, it is possible to obtain the exact values of $F_{\max}(\mathcal{GE})$ by finding channels in $\mathcal{GE}$ that achieve upper bounds on $F_{\max}(\mathcal{GE})$, including the right-hand side of Eq. (5.56). The inequality $F_{\max}(\mathcal{UE}) \leq F_{\max}(\mathcal{GE})$ is also useful for this task because it implies $F_{\max}(\mathcal{GE}) = F_{\max}(\mathcal{UE})$ if $F_{\max}(\mathcal{UE})$ is equal to the right-hand side of Eq. (5.56). Specifically, the following proposition holds.

Proposition 5.3.8. *The following equalities hold:*

$$F_{\max}(\mathcal{GE}) = \begin{cases} 1 & \text{if } |\langle \psi | \phi \rangle| = 0, \\ \frac{1}{2} (1 + |\langle e | f \rangle|) & \text{if } |\langle \psi | \phi \rangle| = 1, \\ \frac{1}{2} \left(1 + \sqrt{1 - |\langle \psi | \phi \rangle|^2} \right) & \text{if } |\langle e | f \rangle| = 0, \\ 1 & \text{if } |\langle e | f \rangle| = 1 \end{cases} \quad (5.58)$$

where the maximization in $F_{\max}(\mathcal{GE}) = \max_{\Lambda \in \mathcal{GE}} F_{av}(\Lambda)$ is achieved by the entanglement breaking channel of the form

$$\Lambda(\cdot) = |e\rangle \langle \psi|(\cdot)|\psi\rangle \langle e| + |f\rangle \langle \phi|(\cdot)|\phi\rangle \langle f| \quad (5.59)$$

if $|\langle \psi|\phi\rangle| = 0$, the depolarizing channel given in Eq. (5.40) if $|\langle \psi|\phi\rangle| = 1$, the unital entanglement breaking channel defined in Eq. (5.65) if $|\langle e|f\rangle| = 0$, and the depolarizing channel that outputs $|e\rangle \langle e|$ if $|\langle e|f\rangle| = 1$. In particular, if $|\langle \psi|\phi\rangle| = 1$ and $|\langle e|f\rangle| = 0$, arbitrary entanglement breaking channels achieve the maximization.

Thus, the right-hand side of Eq. (5.56) coincides with the exact value of $F_{\max}(\mathcal{GE})$ if $|\langle \psi|\phi\rangle| = 0$ or $|\langle e|f\rangle| = 0$. In addition, it is clear from the proposition that $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{GE}$ if $|\langle \psi|\phi\rangle| = 0$ or $|\langle e|f\rangle| = 1$.

5.3.4 Unital entanglement breaking channels

Similar to the previous subsections, we obtain

$$\begin{aligned} C(\tau_0, \mathcal{UE}) &\leq \frac{1}{2} (1 + \|N(\tau_0)\|) \end{aligned} \quad (5.60)$$

$$= \frac{1}{2} \left(1 + \max \left\{ |\langle \psi|\phi\rangle| |\langle e|f\rangle|, \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)} \right\} \right) \quad (5.61)$$

where the first inequality and the second equality follow from Eqs. (5.13) and (5.55), respectively. In addition, we can show that $C(\tau_0, \mathcal{UE})$ attains the right-hand side in Eq. (5.61), i.e., the following equality holds:

$$\begin{aligned} C(\tau_0, \mathcal{UE}) &= \frac{1}{2} \left(1 + \max \left\{ |\langle \psi|\phi\rangle| |\langle e|f\rangle|, \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)} \right\} \right). \end{aligned} \quad (5.62)$$

To see this, it suffices to find channels $\Lambda \in \mathcal{UE}$ such that

$$\begin{aligned} &\text{tr} [\tau_0 J_\Lambda] \\ &= \frac{1}{2} \left(1 + \max \left\{ |\langle \psi|\phi\rangle| |\langle e|f\rangle|, \sqrt{(1 - |\langle \psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)} \right\} \right), \end{aligned} \quad (5.63)$$

due to $C(\tau_0, \mathcal{UE}) = \max_{\Lambda \in \mathcal{UE}} \{\text{tr}[\tau_0 J_\Lambda]\}$, and the following channels indeed serve as such channels:

$$\Lambda_0(A) := \sum_{s=\pm} |e, f, s\rangle \langle \psi, \phi, s| A | \psi, \phi, s\rangle \langle e, f, s|, \quad (5.64)$$

$$\Lambda_1(A) := \sum_{s=\pm} |\widetilde{e, f, s}\rangle \langle \widetilde{\psi, \phi, s}| A | \widetilde{\psi, \phi, s}\rangle \langle \widetilde{e, f, s}| \quad (5.65)$$

where A is a linear operator, and $|\widetilde{u, v, \pm}\rangle$ is defined as

$$|\widetilde{u, v, \pm}\rangle := \frac{1}{\sqrt{2}} (|u, v, +\rangle \pm |u, v, -\rangle) \quad (5.66)$$

for arbitrary pure states $|u\rangle$ and $|v\rangle$. To be more specific, Eq. (5.63) is satisfied by Λ_0 when $(|\langle \psi | \phi \rangle|, |\langle e | f \rangle|) \in \mathcal{F}_0$, and Λ_1 when $(|\langle \psi | \phi \rangle|, |\langle e | f \rangle|) \in \mathcal{F}_1$, where

$$\mathcal{F}_0 := \{(x, y) \in [0, 1]^2 : x^2 + y^2 \geq 1\}, \quad (5.67)$$

$$\mathcal{F}_1 := \{(x, y) \in [0, 1]^2 : x^2 + y^2 < 1\}. \quad (5.68)$$

This fact can be easily verified from

$$F_{\text{av}}(\Lambda_0) = \frac{1}{2} (1 + |\langle \psi | \phi \rangle| |\langle e | f \rangle|), \quad (5.69)$$

$$F_{\text{av}}(\Lambda_1) = \frac{1}{2} \left(1 + \sqrt{(1 - |\langle \psi | \phi \rangle|^2)(1 - |\langle e | f \rangle|^2)} \right). \quad (5.70)$$

Furthermore, if $(|\langle \psi | \phi \rangle|, |\langle e | f \rangle|) = (1, 0)$ or $(|\langle \psi | \phi \rangle|, |\langle e | f \rangle|) = (0, 1)$, Eq. (5.63) is satisfied by any channel in $\mathcal{UE}$. Consequently, the following corollary and proposition are obtained.

Corollary 5.3.9. *The following equality holds:*

$$\begin{aligned} & F_{\max}(\mathcal{UE}) \\ &= \frac{1}{2} \left(1 + \max \left\{ |\langle \psi | \phi \rangle| |\langle e | f \rangle|, \sqrt{(1 - |\langle \psi | \phi \rangle|^2)(1 - |\langle e | f \rangle|^2)} \right\} \right). \end{aligned} \quad (5.71)$$

The right-hand side is equal to 1 if and only if $|\langle \psi | \phi \rangle| = |\langle e | f \rangle| = 1$ or $|\langle \psi | \phi \rangle| = |\langle e | f \rangle| = 0$. Thus, $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{UE}$ if and only if $|\langle \psi | \phi \rangle| = |\langle e | f \rangle| = 1$ or $|\langle \psi | \phi \rangle| = |\langle e | f \rangle| = 0$.

Proposition 5.3.10. *The maximization in $F_{\max}(\mathcal{UE}) = \max_{\Lambda \in \mathcal{UE}} F_{av}(\Lambda)$ is achieved by Λ_0 when $(|\langle\psi|\phi\rangle|, |\langle e|f\rangle|) \in \mathcal{F}_0$, Λ_1 when $(|\langle\psi|\phi\rangle|, |\langle e|f\rangle|) \in \mathcal{F}_1$, and any channel in $\mathcal{UE}$ when $(|\langle\psi|\phi\rangle|, |\langle e|f\rangle|) \in \{(1, 0), (0, 1)\}$.*

The optimal channels Λ_0 and Λ_1 are regarded as measure-and-prepare processes. For instance, Λ_0 represents a transformation that performs a measurement using the orthonormal basis $\{|\psi, \phi, s\rangle\}_{s=\pm}$, the eigenbasis of $|\psi\rangle\langle\psi| + |\phi\rangle\langle\phi|$, and then prepares the state $|e, f, s\rangle$, an eigenvector of $|e\rangle\langle e| + |f\rangle\langle f|$, if the measurement outcome corresponding to $|\psi, \phi, s\rangle$ is obtained ($s = \pm$). The channel Λ_1 can also be interpreted in a similar manner.

5.3.5 General qubit channels

Equation (5.15) implies

$$C(\tau_0, \mathcal{C}) \leq \frac{1}{2} \left(1 + \sqrt{\|\mathbf{b}(\tau_{0,2})\|^2 + \|N(\tau_0)\|_{\text{KF}}^2} \right). \quad (5.72)$$

Thus, the following corollary is obtained by substituting Eqs. (5.38) and (5.48) into this inequality.

Corollary 5.3.11. *The following inequality holds:*

$$F_{\max}(\mathcal{C}) \leq \frac{1}{2} \left\{ 1 + \left[|\langle e|f\rangle|^2 + \left(|\langle\psi|\phi\rangle| |\langle e|f\rangle| + \sqrt{(1 - |\langle\psi|\phi\rangle|^2)(1 - |\langle e|f\rangle|^2)} \right)^2 \right]^{1/2} \right\}. \quad (5.73)$$

Similar to the case of $\mathcal{GE}$, Eq. (5.73) is meaningful only when the right-hand side of Eq. (5.73) is strictly less than 1. While, in such a case, we can conclude that $(|\psi\rangle, |\phi\rangle)$ is not jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{C}$, as stated previously, a necessary and sufficient condition for the joint convertibility within $\mathcal{C}$ already exists [46]. As a consequence of this condition, the following theorem can be obtained.

Theorem 5.3.12. *The pair $(|\psi\rangle, |\phi\rangle)$ is jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{C}$ if and only if*

$$|\langle\psi|\phi\rangle| \leq |\langle e|f\rangle|. \quad (5.74)$$

Therefore, the value of Eq. (5.73) lies in enabling the estimation of $F_{\max}(\mathcal{C})$ from above, rather than in providing a necessary condition for the joint convertibility within $\mathcal{C}$. For instance, if $|\langle\psi|\phi\rangle| = \frac{1}{\sqrt{2}}$, Eq. (5.73) becomes

$$F_{\max}(\mathcal{C}) \leq \frac{1}{2} \left(1 + \sqrt{1 + \frac{1}{\sqrt{2}} \sin \left(2\theta + \frac{\pi}{4} \right)} \right) \quad (5.75)$$

where $|\langle e|f\rangle| = \cos \theta$ and $0 \leq \theta \leq \frac{\pi}{2}$. The right-hand side of this inequality is strictly less than 1 if and only if $\frac{3\pi}{8} < \theta \leq \frac{\pi}{2}$, implying that $(|\psi\rangle, |\phi\rangle)$ is not jointly convertible into $(|e\rangle, |f\rangle)$ within $\mathcal{C}$. In contrast, Theorem 5.3.12 indicates that the joint conversion within $\mathcal{C}$ is not possible if and only if $\frac{\pi}{4} < \theta \leq \frac{\pi}{2}$, meaning that Eq. (5.75) fails to estimate $F_{\max}(\mathcal{C})$ when $\frac{\pi}{4} < \theta \leq \frac{3\pi}{8}$. Thus, while Eq. (5.73) can be meaningless for some cases, it provides a nontrivial upper bound for $F_{\max}(\mathcal{C})$.

The exact values of $F_{\max}(\mathcal{C})$ can be obtained in some cases. For instance, Theorem 5.3.12 implies $F_{\max}(\mathcal{C}) = 1$ if $|\langle\psi|\phi\rangle| \leq |\langle e|f\rangle|$. In particular, $F_{\max}(\mathcal{C}) = 1$ follows if $|\langle\psi|\phi\rangle| = 0$. In addition, we can exactly calculate $F_{\max}(\mathcal{C})$ as follows, similar to Proposition 5.3.8:

Proposition 5.3.13. *The following equalities hold:*

$$F_{\max}(\mathcal{C}) = \begin{cases} \frac{1}{2} (1 + |\langle e|f\rangle|) & \text{if } |\langle\psi|\phi\rangle| = 1, \\ \frac{1}{2} \left(1 + \sqrt{1 - |\langle\psi|\phi\rangle|^2} \right) & \text{if } |\langle e|f\rangle| = 0 \end{cases} \quad (5.76)$$

where the maximization in $F_{\max}(\mathcal{C}) = \max_{\Lambda \in \mathcal{C}} F_{av}(\Lambda)$ is achieved by the depolarizing channel given in Eq. (5.40) if $|\langle\psi|\phi\rangle| = 1$, the unital entanglement breaking channel defined in Eq. (5.65) if $|\langle e|f\rangle| = 0$, and the unitary channel defined in Eq. (5.51) for both cases. In particular, if $|\langle\psi|\phi\rangle| = 1$ and $|\langle e|f\rangle| = 0$, arbitrary channels achieve the maximization.

Thus, the right-hand side of Eq. (5.73) is equal to the exact value of $F_{\max}(\mathcal{C})$ if $|\langle\psi|\phi\rangle| = 0$ or $|\langle e|f\rangle| = 0$.

It is worth clarifying what kinds of channels satisfy Eqs. (5.31) and (5.32) if Eq. (5.74) is fulfilled. If $|\langle\psi|\phi\rangle| = |\langle e|f\rangle| = 0$, Eqs. (5.31) and (5.32) are met by the channels $\Lambda_0 \in \mathcal{UE}$ and $\Lambda_1 \in \mathcal{R}$ that act for any linear operator A as follows:

$$\Lambda_0(A) := |e\rangle \langle\psi|A|\psi\rangle \langle e| + |f\rangle \langle\phi|A|\phi\rangle \langle f|, \quad (5.77)$$

$$\Lambda_1(A) := (|e\rangle \langle\psi| + |f\rangle \langle\phi|) A (|e\rangle \langle\psi| + |f\rangle \langle\phi|)^\dagger. \quad (5.78)$$

If $|\langle\psi|\phi\rangle| = |\langle e|f\rangle| = 1$, Eqs. (5.31) and (5.32) are satisfied by the following channels:

$$\Lambda_2(A) := (\text{tr } A) |e\rangle \langle e|, \quad (5.79)$$

$$\Lambda_3(A) := (|e\rangle \langle\psi| + |e^\perp\rangle \langle\psi^\perp|) A (|e\rangle \langle\psi| + |e^\perp\rangle \langle\psi^\perp|)^\dagger \quad (5.80)$$

where A is a linear operator, and $|e^\perp\rangle$ and $|\psi^\perp\rangle$ denote states orthogonal to $|e\rangle$ and $|\psi\rangle$, respectively. For the remaining case, i.e.,

$$(|\langle\psi|\phi\rangle|, |\langle e|f\rangle|) \in \{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq y \leq 1\} \setminus \{(0, 0), (1, 1)\}, \quad (5.81)$$

the following channel, belonging to the class of generalized extreme points of $\mathcal{C}$ that are discovered in Ref. [48], satisfies Eqs. (5.31) and (5.32):

$$\Lambda_4 := \Gamma_V \circ \tilde{\Lambda}_4 \circ \Gamma_U \quad (5.82)$$

where Γ_W denotes the completely positive map induced by a linear operator W , i.e., it is defined as $\Gamma_W(A) := WAW^\dagger$ for all linear operators A , and V and U are given by

$$V := |e, f, +\rangle \langle 0| + |e, f, -\rangle \langle 1|, \quad (5.83)$$

$$U := |0\rangle \langle\psi, \phi, +| + |1\rangle \langle\psi, \phi, -|. \quad (5.84)$$

The channel $\tilde{\Lambda}_4$ is determined by a matrix

$$T := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos u_1 & 0 & 0 \\ 0 & 0 & \cos u_2 & 0 \\ \sin u_1 \sin u_2 & 0 & 0 & \cos u_1 \cos u_2 \end{pmatrix} \quad (5.85)$$

through the relation $\frac{1}{2} \text{tr} [\sigma_\mu \tilde{\Lambda}_4(\sigma_\nu)] = T_{\mu\nu}$, where $\sigma_0 = I$ and the elements of T are given by

$$\cos u_1 := \sqrt{\frac{1 - |\langle e|f\rangle|^2}{1 - |\langle\psi|\phi\rangle|^2}}, \quad (5.86)$$

$$\cos u_2 := \frac{|\langle\psi|\phi\rangle|}{|\langle e|f\rangle|} \sqrt{\frac{1 - |\langle e|f\rangle|^2}{1 - |\langle\psi|\phi\rangle|^2}}, \quad (5.87)$$

$$\sin u_1 \sin u_2 := \frac{|\langle e|f\rangle|^2 - |\langle\psi|\phi\rangle|^2}{(1 - |\langle\psi|\phi\rangle|^2) |\langle e|f\rangle|}, \quad (5.88)$$

all of which are definable thanks to Eq. (5.81). In particular, Λ_4 reduces to a depolarizing channel

$$\Lambda_4(A) = (\text{tr } A) |e\rangle \langle e| \quad (5.89)$$

when $|\langle\psi|\phi\rangle| < |\langle e|f\rangle| = 1$, an entanglement breaking channel

$$\Lambda_4(A) = |e\rangle \langle\psi|A|\psi\rangle \langle e| + |f\rangle \langle\phi|A|\phi\rangle \langle f| \quad (5.90)$$

when $0 = |\langle\psi|\phi\rangle| < |\langle e|f\rangle|$, and a unitary channel

$$\Lambda_4(A) = \left(\sum_{s=\pm} |e, f, s\rangle \langle\psi, \phi, s| \right) A \left(\sum_{s=\pm} |e, f, s\rangle \langle\psi, \phi, s| \right)^\dagger \quad (5.91)$$

when $0 < |\langle\psi|\phi\rangle| = |\langle e|f\rangle| < 1$.

5.3.6 Comparison of the joint convertibility

We can compare the joint convertibility for the subsets addressed in the previous subsections through the maximum average squared fidelities. Clearly, it holds that $F_{\max}(\mathcal{X}) \leq F_{\max}(\mathcal{Y})$, if $\mathcal{X} \subseteq \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ denote subsets of channels. Thus, the pairs of subsets $(\mathcal{UE}, \mathcal{D})$, $(\mathcal{R}, \mathcal{D})$, and $(\mathcal{R}, \mathcal{GE})$ are of particular interest for comparison of the joint convertibility because each pair consists of subsets that are not comparable to one another. In the following, we compare the joint convertibility for the subsets of these pairs in two specific cases, using the previously obtained exact values or upper bounds of the maximum average squared fidelities.

As the first case, we set $|\langle\psi|\phi\rangle| = \frac{1}{\sqrt{2}}$. For instance, this condition is satisfied if $|\psi\rangle$ and $|\phi\rangle$ belong to mutually unbiased bases, such as the eigenbases of the Pauli operators. In this case, Eqs. (5.39), (5.49), (5.56), and (5.71)

imply

$$F_{\max}(\mathcal{D}) = \frac{1}{2} (1 + |\langle e|f \rangle|), \quad (5.92)$$

$$F_{\max}(\mathcal{R}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \left(|\langle e|f \rangle| + \sqrt{1 - |\langle e|f \rangle|^2} \right) \right), \quad (5.93)$$

$$F_{\max}(\mathcal{GE}) \leq \frac{1}{2} \left(1 + \sqrt{|\langle e|f \rangle|^2 + \frac{1}{2} \max \left\{ |\langle e|f \rangle|, \sqrt{1 - |\langle e|f \rangle|^2} \right\}^2} \right) \quad (5.94)$$

$$=: F'_{\max}(\mathcal{GE}), \quad (5.95)$$

$$F_{\max}(\mathcal{UE}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \max \left\{ |\langle e|f \rangle|, \sqrt{1 - |\langle e|f \rangle|^2} \right\} \right). \quad (5.96)$$

1. $(\mathcal{UE}, \mathcal{D})$. The difference $F_{\max}(\mathcal{UE}) - F_{\max}(\mathcal{D})$ is positive if and only if $0 \leq |\langle e|f \rangle| < \frac{1}{\sqrt{3}}$, zero if and only if $|\langle e|f \rangle| = \frac{1}{\sqrt{3}}$, and negative if and only if $\frac{1}{\sqrt{3}} < |\langle e|f \rangle| \leq 1$. Thus, the joint convertibility within $\mathcal{UE}$ is higher than that within $\mathcal{D}$ if and only if $0 \leq |\langle e|f \rangle| < \frac{1}{\sqrt{3}}$, and vice versa if and only if $\frac{1}{\sqrt{3}} < |\langle e|f \rangle| \leq 1$. Both joint convertibility coincide if and only if $|\langle e|f \rangle| = \frac{1}{\sqrt{3}}$.
2. $(\mathcal{R}, \mathcal{D})$. The difference $F_{\max}(\mathcal{R}) - F_{\max}(\mathcal{D})$ is positive if and only if $0 \leq |\langle e|f \rangle| < \frac{1}{\sqrt{4-2\sqrt{2}}}$, zero if and only if $|\langle e|f \rangle| = \frac{1}{\sqrt{4-2\sqrt{2}}}$, and negative if and only if $\frac{1}{\sqrt{4-2\sqrt{2}}} < |\langle e|f \rangle| \leq 1$. Thus, the joint convertibility within $\mathcal{R}$ is higher than that within $\mathcal{D}$ if and only if $0 \leq |\langle e|f \rangle| < \frac{1}{\sqrt{4-2\sqrt{2}}}$, and vice versa if and only if $\frac{1}{\sqrt{4-2\sqrt{2}}} < |\langle e|f \rangle| \leq 1$. Both joint convertibility coincide if and only if $|\langle e|f \rangle| = \frac{1}{\sqrt{4-2\sqrt{2}}}$.
3. $(\mathcal{R}, \mathcal{GE})$. The difference $F_{\max}(\mathcal{R}) - F'_{\max}(\mathcal{GE})$ is positive if and only if $0 < |\langle e|f \rangle| < \frac{1}{\sqrt{5-2\sqrt{3}}}$, and zero if and only if $|\langle e|f \rangle| = 0$ or $|\langle e|f \rangle| = \frac{1}{\sqrt{5-2\sqrt{3}}}$. Thus, the joint convertibility within $\mathcal{R}$ is higher than that within $\mathcal{GE}$ if $0 < |\langle e|f \rangle| < \frac{1}{\sqrt{5-2\sqrt{3}}}$, and not lower than that within $\mathcal{GE}$ if $|\langle e|f \rangle| = 0$ or $|\langle e|f \rangle| = \frac{1}{\sqrt{5-2\sqrt{3}}}$. No conclusions can be drawn if the difference is negative because $F'_{\max}(\mathcal{GE})$ is an upper bound on $F_{\max}(\mathcal{GE})$.

As the second case, we set $|\langle e|f\rangle| = \frac{1}{\sqrt{2}}$. In this case, Eqs. (5.39), (5.49), (5.56), and (5.71) imply

$$F_{\max}(\mathcal{D}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right), \quad (5.97)$$

$$F_{\max}(\mathcal{R}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \left(|\langle \psi|\phi \rangle| + \sqrt{1 - |\langle \psi|\phi \rangle|^2} \right) \right), \quad (5.98)$$

$$F_{\max}(\mathcal{GE}) \leq \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \sqrt{1 + \max \left\{ |\langle \psi|\phi \rangle|, \sqrt{1 - |\langle \psi|\phi \rangle|^2} \right\}^2} \right), \quad (5.99)$$

$$=: F''_{\max}(\mathcal{GE}), \quad (5.100)$$

$$F_{\max}(\mathcal{UE}) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \max \left\{ |\langle \psi|\phi \rangle|, \sqrt{1 - |\langle \psi|\phi \rangle|^2} \right\} \right). \quad (5.101)$$

1. $(\mathcal{UE}, \mathcal{D})$. The difference $F_{\max}(\mathcal{UE}) - F_{\max}(\mathcal{D})$ is negative if and only if $0 < |\langle \psi|\phi \rangle| < 1$, and zero if and only if $|\langle \psi|\phi \rangle| = 0$ or $|\langle \psi|\phi \rangle| = 1$. Thus, the joint convertibility within $\mathcal{D}$ is higher than that within $\mathcal{UE}$ if and only if $0 < |\langle \psi|\phi \rangle| < 1$. Both joint convertibility coincide if and only if $|\langle \psi|\phi \rangle| = 0$ or $|\langle \psi|\phi \rangle| = 1$.
2. $(\mathcal{R}, \mathcal{D})$. The difference $F_{\max}(\mathcal{R}) - F_{\max}(\mathcal{D})$ is positive if and only if $0 < |\langle \psi|\phi \rangle| < 1$, and zero if and only if $|\langle \psi|\phi \rangle| = 0$ or $|\langle \psi|\phi \rangle| = 1$. Thus, the joint convertibility within $\mathcal{R}$ is higher than that within $\mathcal{D}$ if and only if $0 < |\langle \psi|\phi \rangle| < 1$. Both joint convertibility coincide if and only if $|\langle \psi|\phi \rangle| = 0$ or $|\langle \psi|\phi \rangle| = 1$.
3. $(\mathcal{R}, \mathcal{GE})$. The difference $F_{\max}(\mathcal{R}) - F''_{\max}(\mathcal{GE})$ is positive if and only if $\frac{1}{\sqrt{5}} < |\langle \psi|\phi \rangle| < \frac{2}{\sqrt{5}}$, and zero if and only if $|\langle \psi|\phi \rangle| = \frac{1}{\sqrt{5}}$ or $|\langle \psi|\phi \rangle| = \frac{2}{\sqrt{5}}$. Thus, the joint convertibility within $\mathcal{R}$ is higher than that within $\mathcal{GE}$ if $\frac{1}{\sqrt{5}} < |\langle \psi|\phi \rangle| < \frac{2}{\sqrt{5}}$, and not lower than that within $\mathcal{GE}$ if $|\langle \psi|\phi \rangle| = \frac{1}{\sqrt{5}}$ or $|\langle \psi|\phi \rangle| = \frac{2}{\sqrt{5}}$. Similar to the previous case, we cannot draw any conclusion if the difference is negative because $F''_{\max}(\mathcal{GE})$ is an upper bound on $F_{\max}(\mathcal{GE})$.

5.4 Detection of a Channel

Upper bounds on probabilities can be used to reveal properties of channels. If a qubit channel Λ belongs to a subset of qubit channels $\mathcal{X}$, then the following

inequality holds:

$$p(\Lambda) \leq (\text{tr } S)C(\tau_S, \mathcal{X}), \quad (5.102)$$

where the symbols are defined in Sect. 5.2. The contraposition of this statement is as follows: if it holds that

$$p(\Lambda) > (\text{tr } S)C(\tau_S, \mathcal{X}), \quad (5.103)$$

then $\Lambda \notin \mathcal{X}$. Thus, a violation of Eq. (5.102) signifies that Λ does not possess the property characterized by $\mathcal{X}$.

In this section, we demonstrate the effectiveness of this detection method using the upper bound for $\mathcal{UE}$. Specifically, we derive the conditions under which the following unital qubit channel is not entanglement breaking:

$$\Lambda_w := w \text{id} + (1 - w)\Theta \quad (5.104)$$

where $0 \leq w \leq 1$ and Θ is the depolarizing channel that outputs $\frac{I}{2}$. The state $(\text{id} \otimes \Lambda_w)(P_+)$, where P_+ is the maximally entangled state, is called the Werner state, and separable if and only if $w \leq \frac{1}{3}$ [49]. Thus, Λ_w is an entanglement breaking channel if and only if $w \leq \frac{1}{3}$, or equivalently, Λ_w is not an entanglement breaking channel if and only if $w > \frac{1}{3}$. In the following, we consider two measurement settings for Λ_w , and compare the obtained criteria with this necessary and sufficient condition.

5.4.1 Measurement with the maximally entangled state

As the first setting, we consider the measurement on channels characterized by the maximally entangled state. Specifically, it is implemented by inputting half of the maximally entangled state P_+ on $\mathcal{H} \otimes \mathcal{H}$, where $\mathcal{H}$ denotes a two-dimensional Hilbert space, to a channel, and then performing the following POVM measurement $E: \{0, 1\} \rightarrow \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ on the output state:

$$E(0) := P_+, \quad (5.105)$$

$$E(1) := I - P_+. \quad (5.106)$$

The tester associated with this scheme is given by $S(i) := \frac{1}{2}E(i)$ for all $i \in \{0, 1\}$. It is evident that this measurement setup is designed to investigate the impact of a channel on P_+ ; a high probability of outcome 0 indicates

that measured channel behaves like the identity channel. In other words, this probability quantifies the closeness between the measured channel and the identity channel.

An upper bound on the probability associated with the outcome 0 provides a necessary condition for a channel to be entanglement breaking. Let $p(\Lambda_w)$ denote the probability of obtaining the outcome 0 when Λ_w is measured with this scheme, i.e.,

$$p(\Lambda_w) := \frac{1}{2} \text{tr} [P_+ J_{\Lambda_w}] \quad (5.107)$$

$$= \frac{1}{4} (1 + 3w). \quad (5.108)$$

If $\Lambda_w \in \mathcal{UE}$, we obtain the following chain of inequalities, as stated in the beginning of this section:

$$\frac{1}{4} (1 + 3w) \leq \frac{1}{2} C(P_+, \mathcal{UE}) \quad (5.109)$$

$$\leq \frac{1}{4} (1 + \|N(P_+)\|) \quad (5.110)$$

where the second inequality follows from Eq. (5.13). Direct calculations show $\|N(P_+)\| = 1$, and hence the following inequality is derived:

$$w \leq \frac{1}{3}. \quad (5.111)$$

In other words, if $w > \frac{1}{3}$, Λ_w does not belong to $\mathcal{UE}$. Thus, this criterion, given by Eq. (5.13), detects all Λ_w that are not entanglement breaking channels.

5.4.2 Ancilla-free measurements

As the second setting, we consider three ancilla-free measurements on channels labeled by $a \in \{1, 2, 3\}$. The a th measurement is implemented by inputting the state $|a, 0\rangle \langle a, 0|$ to a channel and then performing the POVM measurement $\mathbf{E}_a: \{(a, i) : i \in \{0, 1\}\} \rightarrow \mathcal{L}(\mathcal{H})$ defined as $\mathbf{E}_a(a, i) := |a, i\rangle \langle a, i|$ on the output state. Here, $\mathcal{H}$ denotes a two-dimensional Hilbert space, and $|a, i\rangle$ represents the eigenvector of the a th Pauli operator corresponding to the eigenvalue $(-1)^i$, i.e., $\sigma_a |a, i\rangle = (-1)^i |a, i\rangle$. The testers are given by

$$\mathbf{S}_a(a, i) := |a, 0\rangle \langle a, 0|^T \otimes |a, i\rangle \langle a, i| \quad (5.112)$$

for all $a \in \{1, 2, 3\}$ and $i \in \{0, 1\}$. We suppose that a channel is probed by randomly using these three ancilla-free measurement devices. If the identity channel is measured by this scheme, then one of the outcomes $(1, 0)$, $(2, 0)$, or $(3, 0)$ is obtained. As such, the closeness between the measured channel and the identity channel is quantified by the probability of getting an outcome in $\{(a, 0) : a \in \{1, 2, 3\}\}$.

Thus, similar to the first setting, we can derive a sufficient condition for $\Lambda_w \notin \mathcal{UE}$ by calculating an upper bound, given by $C(\tau, \mathcal{UE})$, on the following probability:

$$p(\Lambda_w) := \text{tr} [\tau J_{\Lambda_w}] \quad (5.113)$$

$$= \frac{1+w}{2} \quad (5.114)$$

where $\tau := \frac{1}{3} \sum_{a=1}^3 S_a(a, 0)$. If $\Lambda_w \in \mathcal{UE}$, we have

$$\frac{1+w}{2} \leq \frac{1}{2} (1 + \|N(\tau)\|) \quad (5.115)$$

$$= \frac{1}{2} \left(1 + \frac{1}{3} \right), \quad (5.116)$$

from Eq. (5.13) and $\|N(\tau)\| = \frac{1}{3}$. Thus, if $\Lambda_w \in \mathcal{UE}$, then $w \leq \frac{1}{3}$ must hold, meaning that if $w > \frac{1}{3}$, then $\Lambda_w \notin \mathcal{UE}$. Therefore, this criterion, provided by the three ancilla-free measurements, also detects all Λ_w that does not belong to $\mathcal{UE}$, similar to the criterion induced in the first setting. Note that the second scheme does not use entangled states, while it needs the three different types of ancilla-free measurements. This feature can be advantageous from an experimental point of view compared to the first scheme, where the maximally entangled states are utilized, because in general generating entanglement is not an easy task.

5.5 Summary and Discussion

In this chapter, several upper bounds on the probabilities associated with measurements on channels and their applications were presented. The upper bounds are explicitly represented as simple channel-independent functions characterized by the norms $\|\mathbf{b}(\tau_2)\|$, $\|N(\tau)\|$, or $\|N(\tau)\|_{\text{KF}}$ of a two-qubit state τ .

An application of the upper bounds is a notion of convertibility problem. Inspired by the problem investigated in Ref. [46], we considered the question of whether a pair of pure states can be jointly converted into another using a specific type of channel. The joint convertibility within several subsets of channels were evaluated by utilizing the fact that the maximum average squared fidelity, a figure of merit of the joint convertibility, is directly connected with the upper bounds.

Another application of the upper bounds is a detection problem of a channel's property. We obtained criteria for verifying that a unital channel with a single parameter is not entanglement breaking by applying one of the upper bounds to two contrasting measurement schemes. The criteria detect all of the unital channels that are not entanglement breaking, indicating the effectiveness of the applied upper bound. Our measurement schemes might serve as experimentally friendly tests for certifying that a unital channel does not possess the entanglement breaking property because they do not require full process tomography.

Let us mention a possible application of the upper bounds to uncertainty relations for testers. As stated in Ch. 3, an uncertainty relation for testers can be formulated by assuming that the qubit channel to be measured is selected from a specific subset of channels. It is easy to see that the bound of an uncertainty relation is given by $C(\tau_S, \mathcal{X})$, where τ_S is a two-qubit state induced by a tester element S , and $\mathcal{X}$ denotes a subset of qubit channels. Thus, the uncertainty bound can be estimated from above using the upper bounds provided in this chapter. In particular, similar to Theorem 3.2.1, if the testers are ancilla-free, then it is possible to represent the estimates of uncertainty bounds as simple formulas of input states and POVMs for the output system.

As discussed in the introduction of this chapter, our formulas for qubit channels are expected to serve as fundamental constraints for large physical systems composed of many qubits. In particular, verifying large-scale quantum circuits and characterizing high-capacity quantum channels are essential tasks for evaluating the performance of quantum information processing. Therefore, applying our upper bounds on probabilities to these tasks constitutes an engineeringly significant direction, and further developments along this line are highly desirable.

Chapter 6

Summary

Uncertainty relations for testers and related topics were investigated with emphasis on representing them by explicit formulas. The main conclusions were given in Chs. 3, 4, and 5, which are described based on Refs. [1], [2], and [3], respectively. The contents of these chapters are summarized as follows.

Chapter 3 presents an uncertainty relation for ancilla-free measurements performed on qubit random unitary channels. The bound of an uncertainty relation was provided in Theorem 3.2.1 as an explicit formula of states and POVMs, which characterize ancilla-free measurements. It was revealed from the uncertainty relation that a quantity Q , defined in Eq. (3.11), serves as an important factor contributing to an unavoidable trade-off between the probabilities associated with the scheme. In particular, a necessary and sufficient condition for the existence of such a trade-off was clarified through an observation of the qualitative behavior of Q .

Chapter 4 is devoted to a detailed investigation of a fine-grained uncertainty relation for testers. The fine-grained uncertainty relation established in Ref. [11] was generalized by considering a set of inequalities, each of which imposes a restriction on possible values of probabilities related a combination of outcomes in measurements on channels. To address the difficulty in calculating the generalized uncertainty bound, two types of prescriptions were provided. The first one is to estimate the uncertainty bound from above using the operator norm. While this approach does not work effectively in some cases, it yields nontrivial estimates of the uncertainty bound when testers are given by maximally entangled bases. In particular, it was shown that these estimates coincide with the exact values of the uncertainty bound for the

case of measurements of qubit channels. As the second prescription, we connected the generalized uncertainty bound with a semidefinite program. We presented numerically obtained values of the uncertainty bound based on the semidefinite program, and proposed a conjecture induced by these values. An application to a quantum key distribution protocol was also described in this chapter.

Chapter 5 describes upper bounds on probabilities in measurements performed on qubit channels and their applications. For typical subsets of qubit channels, upper bounds on a probability in a channel measurement were provided as simple functions by evaluating a quantity $C(\tau, \mathcal{X})$, defined in Eq. (5.2). To demonstrate the effectiveness of the upper bounds, two fundamental problems were posed. The first one pertains to the question of whether a pair of pure states is jointly convertible into another using a specific type of channel. We examined the joint convertibility within specific subsets of qubit channels in details by utilizing the connection between the upper bounds and the maximum average squared fidelity, a measure of the joint convertibility. The second one concerns the problem of verifying that a unital channel with a single parameter is not entanglement breaking. In two schemes for measuring channels, we provided sufficient conditions of the parameter under which the unital channel is not entanglement breaking, by applying one of the upper bounds. The conditions are not only sufficient but also necessary, signifying the effectiveness of the applied upper bound.

As discussed in the introduction, explicit uncertainty relations provide quantitatively evaluable constraints on the dynamics of large quantum systems. Such constraints can serve both as methods for the physical realizability of quantum operations and as criteria for determining whether a given quantum channel possesses certain properties. In particular, the uncertainty relations presented in this thesis—as well as their potential extensions—are expected to find applications in areas such as security evaluation in quantum cryptography, certification of large-scale quantum circuits, and experimental verifications of quantum mechanics. For the first two directions, Chs. 4 and 5 have already implied, albeit in special cases, that applying uncertainty relations for quantum testers yields meaningful results. As quantum technologies continue to develop rapidly, the feasibility of large-scale quantum information processing protocols is becoming increasingly realistic. It is hoped that uncertainty relations for quantum testers will serve as useful tools supporting these developments in the years to come.

Acknowledgments

I would like to express my gratitude to Takayuki Miyadera for his insightful advice. This thesis would not have been completed without his invaluable guidance. I am equally grateful to Kenzo Ogure for his constant support and helpful advice on my future career. I also want to thank the current and past members of my laboratory. My gratitude is also extended to the Kyoto University Division of Graduate Studies; this work was supported by JST SPRING, Grant Number JPMJSP2110. My acknowledgments would not be complete without thanking my friends, relatives, and family. In particular, I must express my sincere appreciation to my parents for their continued support and patience. Finally, I dedicate this thesis to the memory of my grandparents.

Bibliography

- [1] T. Kimoto and T. Miyadera, J. Phys. Soc. Jpn. **92**, 034005 (2023).
- [2] T. Kimoto, J. Phys. Soc. Jpn. **94**, 054001 (2025).
- [3] T. Kimoto and T. Miyadera, J. Phys. Soc. Jpn. **94**, 084004 (2025).
- [4] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
- [5] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
- [6] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (2017).
- [7] M. H. Partovi, Phys. Rev. A **84**, 052117 (2011).
- [8] Z. Puchała, Ł. Rudnicki, and K. Życzkowski, J. Phys. A **46**, 272002 (2013).
- [9] S. Friedland, V. Gheorghiu, and G. Gour, Phys. Rev. Lett. **111**, 230401 (2013).
- [10] L. Rudnicki, Z. Puchała, and K. Życzkowski, Phys. Rev. A **89**, 052115 (2014).
- [11] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
- [12] Y. Xiao, K. Sengupta, S. Yang, and G. Gour, Phys. Rev. Res. **3**, 023077 (2021).
- [13] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180501 (2008).
- [14] M. Ziman, Phys. Rev. A **77**, 062112 (2008).

- [15] T. Heinosaari and M. Ziman, *The mathematical language of quantum theory: from uncertainty to entanglement* (Cambridge University Press, Cambridge, U.K., 2011).
- [16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2010) 10th Anniversary Edition.
- [17] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, U.K., 2018).
- [18] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, U.K., 2017) Second Edition.
- [19] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).
- [20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [21] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).
- [22] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
- [23] M. Krishna and K. R. Parthasarathy, Sankhyā Ser. A **64**, 842 (2002).
- [24] A. E. Rastegin, J. Phys. A **43**, 155302 (2010).
- [25] A. Rényi, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, ed. J. Neyman (University of California Press, Oakland, 1961), pp. 547–561.
- [26] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications* (Springer Science+Business Media, New York, 2011) Second Edition.
- [27] A. E. Rastegin, Quantum Inf. Process. **14**, 783 (2015).
- [28] T. Miyadera and H. Imai, Phys. Rev. A **76**, 062108 (2007).
- [29] G. Sharma, S. Sazim, and S. Mal, Phys. Rev. A **104**, 032424 (2021).

- [30] X. Zhou, L.-L. Sun, and S. Yu, Phys. Rev. A **109**, 022408 (2024).
- [31] R. Renner, Dr. Thesis, ETH Zürich (2005).
- [32] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, Proc. 41st Annual Symposium on Foundations of Computer Science, 2000, p. 547.
- [33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [34] J. Grondalski, D. Etlinger, and D. James, Phys. Lett. A **300**, 573 (2002).
- [35] M. Li, S.-M. Fei, and Z.-X. Wang, Phys. Rev. A **78**, 032332 (2008).
- [36] E. Hänggi and S. Wehner, Nat. Commun. **4**, 1670 (2013).
- [37] A. E. Rastegin, Quantum Inf. Process. **15**, 2621 (2016).
- [38] G. M. D’Ariano and P. Lo Presti, Phys. Rev. Lett. **91**, 047902 (2003).
- [39] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O’Brien, M. A. Nielsen, and A. G. White, Phys. Rev. Lett. **90**, 193601 (2003).
- [40] J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).
- [41] L. Vandenbergh and S. Boyd, SIAM Rev. **38**, 49 (1996).
- [42] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
- [43] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
- [44] D. Popovici and Z. Sebestyén, J. Operator Theory **56**, 3 (2006).
- [45] L. Landau and R. Streater, Linear Algebra Appl. **193**, 107 (1993).
- [46] P. Alberti and A. Uhlmann, Rep. Math. Phys. **18**, 163 (1980).
- [47] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
- [48] M. B. Ruskai, S. Szarek, and E. Werner, Linear Algebra Appl. **347**, 159 (2002).
- [49] A. O. Pittenger and M. H. Rubin, Opt. Commun. **179**, 447 (2000).