Mathematical Studies on Quantum Systems and Locally Quantum Systems

Yuuya Yoshida

October 12, 2021

Abstract

General probabilistic theories (GPTs) are theoretical models having states, measurements, and probabilities of obtaining measurement outcomes. For example, classical probability theory and quantum theory are GPTs with probability vectors and density matrices as states, respectively. In the study of GPTs, one often describes a finite number of GPTs $A_1, \ldots, A_n$ together, as one GPT $A = A_1 \cdots A_n$. In this case, we say that A is a whole system of subsystems $A_1, \ldots, A_n$. If $A_1, \ldots, A_n$ are quantum systems, then A is called a locally quantum system. A quantum system is locally quantum, but there are many other locally quantum systems. In this thesis, we study three topics associated with quantum systems and locally quantum systems.

The first one is capacity. For a GPT, the maximum number of simultaneously and perfectly distinguishable states is called the capacity. It is known that the capacity does not really depend on the GPT. In this thesis, we propose a statement S to determine the capacities of special locally quantum systems, and prove a weaker statement WS. Statement WS is a statement associated with tensor product spaces over $\mathbb{C}$. Our proof works even if replacing the scalar field $\mathbb{C}$ with an arbitrary infinite field $\mathcal{F}$. We also show a partial result for finite fields.

The second one is differential privacy (DP). DP was born in the study to utilize private data while protecting the data (privacy-preserving data mining, PPDM). For this reason, DP has been studied by using classical probability theory, and has almost never been studied in quantum information theory. In this thesis, we define a quantum version of DP (called classical-quantum DP) and investigate its mathematical aspects. We define the set CQ_n of all classical-quantum differentially private n-tuples of quantum states and the subset EC_n of CQ_n that is essentially classical. We prove that $\mathrm{EC}_n = \mathrm{CQ}_n$ if $n = 2$ and $\mathrm{EC}_n \neq \mathrm{CQ}_n$ if $n \geq 3$.

The third one is perfect discrimination of two states. In quantum theory, orthogonality is a necessary and sufficient condition to distinguish two states perfectly (denote this equivalence by E). However, equivalence E does not hold for a general GPT. In this thesis, we construct continuous one-parameter families of locally quantum systems in a certain natural manner, and investigate perfect discrimination of two states in the framework of those locally quantum systems. These one-parameter families contain a locally quantum system sufficiently close to a quantum system. Nevertheless, we show that they violate equivalence E.

Publication list

This thesis is organized with special emphasis on the author's single-authored articles, and is based on the following papers and preprint.

1. Y. Yoshida, Maximum dimension of subspaces with no product basis, *Linear Algebra Appl.* **620**, 228–241 (2021).
2. Y. Yoshida, Classical-quantum differentially private mechanisms beyond classical ones, arXiv:2011.09960 (2020).
3. Y. Yoshida and M. Hayashi, Classical mechanism is optimal in classical-quantum differentially private mechanisms, *Proc. of 2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1991–1995 (2020).[1]
4. Y. Yoshida, H. Arai, and M. Hayashi, Perfect discrimination in approximate quantum theory of general probabilistic theories, *Phys. Rev. Lett.* **125**, 150402 (2020).[2]

The contents of this thesis have the following correspondence. My contribution to paper 4 is its mathematical parts: Definition 2, Theorems 1, 2, and their proofs. Definition 1 in paper 4 is a definition discussed together with Hayato Arai.

Section 1.1	Section 1 of paper 1
Section 1.2	Section 1 of preprint 2
Section 1.3	None
Chapter 2	Section 4 of paper 1
Chapter 3	Sections 2 and 3 of paper 1
Chapter 4 excluding Section 4.2	Sections 2–4 and Appendix of preprint 2
Section 4.2	Paper 3
Chapter 5	Paper 4
Section 6.1	None
Section 6.2	Section 5 of preprint 2
Section 6.3	None

I also wrote the following papers, which are not included in this thesis.

5. K. Saito and Y. Yoshida, Distributions of finite sequences represented by polynomials in Piatetski-Shapiro sequences, *J. Number Theory* **222**, 115–156 (2021).

[1] ©2020 IEEE
[2] ©2020 American Physical Society

6. Y. Yoshida and M. Hayashi, Asymptotic properties for Markovian dynamics in quantum theory and general probabilistic theories, *J. Phys. A* **53**, 215303 (2020).
7. H. Arai, Y. Yoshida, and M. Hayashi, Perfect discrimination of non-orthogonal separable pure states on bipartite system in general probabilistic theory, *J. Phys. A* **52**, 465304 (2019).

Acknowledgments

Firstly, I am grateful to Prof. François Le Gall for giving me some advice on my life as a graduate student and this thesis. I also thank Prof. Masahito Hayashi for discussing topics in quantum information theory and writing some papers together. I thank Hayato Arai, who is another coauthor, for his explanations about topics in physics. Finally, I express my gratitude to my colleagues Seunghoan Song and Kota Saito during my life as a graduate student. Seunghoan Song is a friend with who I often talk about topics in mathematics or quantum information theory, and gave me many helpful comments about my preprints. Kota Saito is my coauthor in number theory, and I enjoyed my life as a graduate student in mathematics thanks to him. The research in this thesis was supported by JSPS KAKENHI Grant Number JP19J20161.

Contents

Chapter 1

Introduction

General probabilistic theories.—*A general probabilistic theory (GPT)* is a theoretical model [36, 40, 41, 43, 48, 54], which is defined as a triplet $(\mathcal{V}, \mathcal{K}, u)$ of a real Hilbert space space $\mathcal{V}$, a convex cone $\mathcal{K} \subset \mathcal{V}$ and an element $u \in \mathcal{V}$ (more precisely, see Section 2.1). For example, the GPTs $(\mathbb{R}^d, [0,\infty)^d, \mathbf{1}_d)$ and $(\mathsf{Herm}(d), \mathsf{PSD}(d), I_d)$ are *classical probability theory* and *quantum theory*, respectively, where $\mathbf{1}_d$ denotes the vector $[1, \dots, 1]^\top \in \mathbb{R}^d$; $\mathsf{Herm}(d)$ denotes the set of all Hermitian matrices on $\mathbb{C}^d$; $\mathsf{PSD}(d)$ denotes the set of all positive semi-definite matrices on $\mathbb{C}^d$; I_d denotes the identity matrix on $\mathbb{C}^d$. The Hilbert spaces $\mathbb{R}^d$ and $\mathsf{Herm}(d)$ are equipped with the inner products $\sum_{i=1}^d x_i y_i$ and $\operatorname{Tr} XY$, respectively, where $\operatorname{Tr} X$ denotes the (non-normalized) trace of a square matrix X. See also Table 1.1 which summarizes the definitions of classical probability theory and quantum theory as GPTs. Each GPT $(\mathcal{V}, \mathcal{K}, u)$ has the *state class* $\mathcal{S}(\mathcal{K}, u)$ and *measurement class* $\mathcal{M}(\mathcal{K}^*, u)$ defined as

$$\begin{aligned} \mathcal{S}(\mathcal{K}, u) &= \{x \in \mathcal{K} : \langle x, u\rangle = 1\}, \\ \mathcal{M}(\mathcal{K}^*, u) &= \left\{ (y_i)_{i=1}^m \text{ } m\text{-tuple of elements in } \mathcal{K}^* : m \in \mathbb{N},\ \sum_{i=1}^m y_i = u \right\}, \end{aligned} \tag{1.1}$$

where $\mathcal{K}^*$ denotes the *dual cone* of $\mathcal{K}$:

$$\mathcal{K}^* = \{y \in \mathcal{V} : \forall x \in \mathcal{K},\ \langle y, x\rangle \geq 0\}.$$

An element in the state class (resp. measurement class) is called a *state* (resp. *measurement*). For example, a state in classical probability theory (resp. quantum theory) is a probability vector (resp. density matrix). Although a measurement in classical probability theory has no particular name, a measurement in quantum theory is a positive-operator-valued measure (POVM).

Table 1.1: Classical probability theory and quantum theory as GPTs.

GPT	Hilbert space $\mathcal{V}$	Inner product $\langle \cdot, \cdot \rangle$	Convex cone $\mathcal{K}$
Classical	$\mathbb{R}^d$	$\sum_{i=1}^d x(i)y(i)$	$[0,\infty)^d$
Quantum	$\mathsf{Herm}(d)$	$\operatorname{Tr} XY$	$\mathsf{PSD}(d)$

GPT	Element u	State x	Measurement $(y_i)_{i=1}^m$
Classical	$\mathbf{1}_d$	Probability vector p	No name
Quantum	I_d	Density matrix ρ	POVM $(M_i)_{i=1}^m$

Given a state $x \in \mathcal{S}(\mathcal{K}, u)$ and a measurement $(y_i)_{i=1}^m \in \mathcal{M}(\mathcal{K}^*, u)$, the probability of obtaining each outcome $i = 1, \dots, m$ is $\langle x, y_i \rangle$. Note that $(\langle x, y_i \rangle)_{i=1}^m$ is a probability vector. For instance, a dice roll is described by classical probability theory, and its state is $x = (1/6)\mathbf{1}_6$. If we want to know whether the number on a cast dice is even or odd, then we should use the measurement consisting of $y_{\text{even}} = e_2 + e_4 + e_6$ and $y_{\text{odd}} = e_1 + e_3 + e_5$, where $(e_i)_{i=1}^6$ denotes the standard basis of $\mathbb{R}^6$. The probability for the number to be even (resp. odd) is $\langle x, y_{\text{even}} \rangle$ (resp. $\langle x, y_{\text{odd}} \rangle$).

As stated above, classical probability theory and quantum theory are typical GPTs, but there are many other GPTs. A simple example is the PR box [35] (named after Popescu and Rohrlich [47]). The convex cone $\mathcal{K}$ of the PR box $(\mathbb{R}^3, \mathcal{K}, e_3)$ is a square pyramid, and is different from $[0,\infty)^d$ and $\mathsf{PSD}(d)$ which appear in classical probability theory and quantum theory, respectively.[1]

Whole systems and subsystems.—Consider classical probability theory. In classical probability theory, one often considers the joint distribution $\mathbb{P}_{X_1 \cdots X_n}$ of random variables $X_1, \dots, X_n$ and its marginal distributions $\mathbb{P}_{X_1}, \dots, \mathbb{P}_{X_n}$. The marginal distributions come from the joint distribution, but in general, one cannot recover the joint distribution from the marginal distributions.

The study of GPTs also has an analog of the above situation. We say that a GPT $(\mathcal{V}, \mathcal{K}, u)$ is *a whole system of subsystems* $(\mathcal{V}^{[i]}, \mathcal{K}^{[i]}, u^{[i]})$, $i = 1, \dots, n$, if the n GPTs $(\mathcal{V}^{[i]}, \mathcal{K}^{[i]}, u^{[i]})$ satisfy (i) $\mathcal{V} = \mathcal{V}^{[1]} \otimes \cdots \otimes \mathcal{V}^{[n]}$, (ii) $\mathcal{K}_{\min} \subset \mathcal{K} \subset \mathcal{K}_{\max}$, and (iii) $u = u^{[1]} \otimes \cdots \otimes u^{[n]}$, where $\mathcal{K}_{\min}$ and $\mathcal{K}_{\max}$ are defined as

$$\begin{aligned} \mathcal{K}_{\min} &= \operatorname{conv}\{x^{[1]} \otimes \cdots \otimes x^{[n]} : x^{[1]} \in \mathcal{K}^{[1]}, \dots, x^{[n]} \in \mathcal{K}^{[n]}\}, \\ \mathcal{K}_{\max} &= \{x \in \mathcal{V} : \forall y^{[1]} \in (\mathcal{K}^{[1]})^*, \dots, \forall y^{[n]} \in (\mathcal{K}^{[n]})^*,\ \langle x, y^{[1]} \otimes \cdots \otimes y^{[n]} \rangle \geq 0\}. \end{aligned} \tag{1.2}$$

That is, an element in $\mathcal{K}_{\min}$ is a convex combination of tensor products of $x^{[1]} \in \mathcal{K}^{[1]}, \dots, x^{[n]} \in \mathcal{K}^{[n]}$, and an element in $\mathcal{K}_{\max}^*$ is a convex combination of tensor prod-

[1] Actually, the convex cones $[0,\infty)^d$ and $\mathsf{PSD}(d)$ are special cones called *symmetric cones*. Hence, GPTs are also related to symmetric cones and Euclidean Jordan algebras [6, 37, 39, 44, 50].

ucts of $y^{[1]} \in (\mathcal{K}^{[1]})^*, \ldots, y^{[n]} \in (\mathcal{K}^{[n]})^*$.[2] It is the most important here that the whole system (namely, its convex cone $\mathcal{K}$) is not uniquely determined even if its subsystems are given, since $\mathcal{K}_{\min}$ and $\mathcal{K}_{\max}$ are not equal to each other in general. However, it follows that $\mathcal{K}_{\min} = \mathcal{K}_{\max}$ if all subsystems are classical (i.e., described by classical probability theory). In this case, the whole system (namely, convex cone $\mathcal{K}$) is uniquely determined and classical.

However, the quantum case is different from the classical case. We say that a GPT $(\mathcal{V}, \mathcal{K}, u)$ is a *locally quantum system* if $(\mathcal{V}, \mathcal{K}, u)$ is a whole system of quantum subsystems (i.e., subsystems are described by quantum theory). When $(\mathcal{V}, \mathcal{K}, u)$ is a locally quantum system, we simply write $\mathcal{S}(\mathcal{K}, u)$ and $\mathcal{M}(\mathcal{K}^*, u)$ as $\mathcal{S}(\mathcal{K})$ and $\mathcal{M}(\mathcal{K}^*)$, respectively, since u is the identity matrix. A quantum system is locally quantum, but there are many other locally quantum systems. We are interested in common or different properties for locally quantum systems, which are studied, e.g., in [42]. However, many of such properties are not made clear and not studied well.

Structure of this section.—In this thesis, we study three topics associated with quantum systems and locally quantum systems: (i) capacity, (ii) differential privacy, and (iii) perfect discrimination of two states. The first one is a property that almost never depends on the locally quantum system, but the third one is a property that strongly depends on the locally quantum system. Although the first and third ones are discussed for locally quantum systems, the second one is only discussed in quantum theory. This is because the quantum case is still not sufficiently compared with the classical case in the viewpoint of (ii). Note that all the vector spaces we are dealing with in this thesis are finite-dimensional. In Sections 1.1, 1.2 and 1.3, we give a description of each of these three contributions.

1.1 Statement determining the capacities of GPTs, and weaker statement

Any problem for locally quantum systems can be regarded as a problem in matrix theory, since a locally quantum system is described by Hermitian matrices on $\mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$. In particular, the so-called separability problem is one of the most important problems, and attracts attention in quantum theory [4, 25, 28, 31, 32]. The separability problem is the problem to investigate whether a given positive semi-definite matrix is separable or not (we state the definition of separability in the

[2] This is consistent with the definition of $\mathcal{K}_{\max}$, since $\mathcal{K}^{**} = \mathcal{K}$ for every non-empty closed convex cone [8, p. 53], [20, p. 63].

next paragraph). There are several necessary or sufficient conditions for a positive semi-definite matrix to be separable [25, 31, 32]. While motivated by a problem from locally quantum systems, in this thesis, we discuss a sufficient condition for separability (statement S below) as a linear algebraic one.

Let $\mathcal{H}(d_1, \ldots, d_n)$ be an n-partite complex Hilbert space $\mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, and $\tilde{d}$ be the dimension $d_1 d_2 \cdots d_n$ of $\mathcal{H}(d_1, \ldots, d_n)$. For each GPT, the maximum number of simultaneously and perfectly distinguishable states is called the *capacity* (for the definition of simultaneously and perfectly distinguishable states, see Section 1.3). The capacities of GPTs have been studied, e.g., in [41–43]. To determine the capacities of special GPTs, the following statement plays an important role (see Section 2.2):

(S) for every unit vector $u \in \mathcal{H}(d_1, \ldots, d_n)$, the two matrices $I_{\tilde{d}} \pm |u\rangle\langle u|$ lie in the set $\mathsf{Sep}(d_1, \ldots, d_n) \coloneqq \mathrm{conv}\{X^{[1]} \otimes \cdots \otimes X^{[n]} : X^{[1]}, \ldots, X^{[n]} \text{ positive semi-definite}\}$,

where $\mathrm{conv}(\mathcal{S})$ denotes the convex hull of a subset $\mathcal{S}$. Throughout this thesis, we use the bra-ket notation (see Section 2.2), and use the superscript $[j]$ (resp. $[k : l]$) to express the jth site (resp. the sites from kth to lth). A matrix in $\mathsf{Sep}(d_1, \ldots, d_n)$ is called *separable*. Every separable matrix is positive semi-definite, but the converse does not necessarily hold. If $n = 2$, then statement S is true for all integers $d_1, d_2 \geq 2$ [25]. However, statement S is still open for $n \geq 3$ to the best of our knowledge.

Main result.—Our main interest is whether statement S holds for all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$. In this thesis, we show the following statement weaker than statement S: for all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$,

(WS) every $(\tilde{d} - 1)$-dimensional subspace $\mathcal{L}$ of $\mathcal{H}(d_1, \ldots, d_n)$ has a product basis,

where a vector $u \in \mathcal{H}(d_1, \ldots, d_n)$ is called a *product vector* if $u = u^{[1]} \otimes \cdots \otimes u^{[n]}$ for some $u^{[1]} \in \mathbb{C}^{d_1}, \ldots, u^{[n]} \in \mathbb{C}^{d_n}$; a basis composed of product vectors is called a *product basis*. In Section 3.1, we give a $(\tilde{d} - 2)$-dimensional subspace with no product basis. These results yield the following theorem.

Theorem 1.1. *For all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$,*

$$\max\left\{\dim \mathcal{L} : \begin{array}{l} \mathcal{L} \text{ is a subspace of } \mathcal{H}(d_1, \ldots, d_n) \text{ and} \\ \text{has no product basis} \end{array}\right\} = \tilde{d} - 2.$$

Since Theorem 1.1 can be regarded simply as a mathematical one, we generalize the scalar field $\mathbb{C}$ to an arbitrary field. Theorem 1.1 is still true even if the scalar field $\mathbb{C}$ is replaced with an arbitrary infinite field (Remark 3.5). We address the case of finite fields in Section 3.2. For every finite field $\mathcal{F}$, we show that Theorem 1.1 is

also true if either (i) $n = 2$ or (ii) $n \geq 3$ and $\#\mathcal{F} > \max\{d_i : i \neq n_1, n_2\}$ for some n_1 and n_2 (Theorem 3.9), where $\#\mathcal{F}$ denotes the order of $\mathcal{F}$.

Related work.—Existing studies often consider an *orthogonal product basis* [2,7, 10,13,21,32], which is defined as an orthonormal basis composed of product vectors. An orthogonal product basis of a subspace $\mathcal{L}$ is called *unextendible* if the orthogonal complement of $\mathcal{L}$ contains no non-zero product vector. Unextendible orthogonal product bases (UPBs; "orthogonal" is usually omitted) are used to construct bound entangled states [7, 13, 32]. In particular, quantum information theory motivates us to find UPBs of the minimum possible number. Alon and Lovász [2] proved that the minimum dimension of subspaces of $\mathcal{H}(d_1, \ldots, d_n)$ with UPBs is equal to $d_1 + \cdots + d_n - n + 1$ unless either (i) $n = 2$ and $2 \in \{d_1, d_2\}$ or (ii) $d_1 + \cdots + d_n - n + 1$ is odd and at least one d_i is even. Moreover, the minimum dimension is strictly greater than $d_1 + \cdots + d_n - n + 1$ in cases (i) and (ii). After the appearance of their work, cases (i) and (ii) have been studied in more detail [10, 21].

There are two statements similar to Theorem 1.1. A subspace of $\mathcal{H}(d_1, \ldots, d_n)$ containing no non-zero product vector is called *completely entangled*. Wallach [51] and Parthasarathy [45] proved that for all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$,

$$\begin{aligned} &\max\{\dim \mathcal{L} : \mathcal{L} \text{ is a completely entangled subspace of } \mathcal{H}(d_1, \ldots, d_n)\} \\ &= \tilde{d} - (d_1 + \cdots + d_n) + n - 1. \end{aligned} \tag{1.3}$$

Cubitt et al. [12] proved that for all integers $d_1, d_2 \geq 2$ and $r \in [0, \min\{d_1, d_2\} - 1]$,

$$\begin{aligned} &\max\left\{\dim \mathcal{L} : \begin{array}{l} \mathcal{L} \text{ is a subspace of } \mathcal{H}(d_1, d_2) \text{ satisfying that} \\ \text{s-rank}\, u \geq r + 1 \text{ for all non-zero } u \in \mathcal{L} \end{array}\right\} \\ &\leq (d_1 - r)(d_2 - r), \end{aligned} \tag{1.4}$$

where s-rank u denotes the Schmidt rank of $u \in \mathcal{H}(d_1, d_2)$, i.e., a unique number k such that u is expressed as $u = \sum_{i=1}^{k} \alpha_i u_i^{[1]} \otimes u_i^{[2]}$ with positive numbers $\alpha_1, \ldots, \alpha_k$ and two orthonormal systems $(u_i^{[1]})_{i=1}^k$ and $(u_i^{[2]})_{i=1}^k$. If $r = 0, 1$, then (1.4) has equality due to (1.3). Recently, Bag et al. [5] constructed subspaces that achieve equality in (1.4) for all $d_1, d_2 \geq 4$ and $r = 1, 2, 3$.

Actually, if $n = 2$, then for all integers $d_1, d_2 \geq 2$, the following statement holds [25]:

(SS) the matrix $I + X$ lies in $\mathsf{Sep}(d_1, \ldots, d_n)$ for every Hermitian matrix X with $\|X\|_2 \coloneqq (\operatorname{Tr} X^* X)^{1/2} \leq 1$.

Statement SS is stronger than statement S and does not hold in general [4, 28].

Finally, we briefly describe entangled vectors which are related to product vectors. If $u \in \mathcal{H}(d_1, \dots, d_n)$ is not any product vectors, we say that u is *entangled*. It is widely known [32] that for every entangled vector $u \in \mathcal{H}(d_1, \dots, d_n)$, the matrix $|u\rangle\langle u|$ does not lie in $\mathsf{Sep}(d_1, \dots, d_n)$ (see also Proposition 3.6). Normalized entangled vectors are significant resources in quantum information processing.

1.2 Differential privacy

In data analysis, data analysts need to know only some statistical information about private data while protecting the private data. They hope to maximally utilize private data under some privacy protection. In general, protection and utilization of private data have a trade-off relation, and researchers optimize the trade-off relation [22–24, 30, 38, 55].

As a way protecting private data, Warner [52] proposed *randomized response* in 1965, in which private data X are converted to other data Y subject to a conditional probability distribution $\mathbb{P}_{Y|X}$, and the data Y is released instead of X. Since a data analyst collects only randomized data Y, private data X are protected.

However, private data are not always protected in the above way. For instance, if Y is always equal to X, then it is clear that private data are not protected. To further understand such issues, consider another case: suppose that X is binary, Y is ternary,

$$\mathbb{P}_{Y|X}(\cdot|0) = \overset{Y=0}{[}1/3, \overset{Y=1}{1/3}, \overset{Y=2}{1/3}] \quad \text{and} \quad \mathbb{P}_{Y|X}(\cdot|1) = [\overset{Y=0}{\ 0\ }, \overset{Y=1}{1/2}, \overset{Y=2}{1/2}].$$

Then the data analyst finds that $X = 0$ if $Y = 0$, since the conditional probability distribution satisfies that $\mathbb{P}_{Y|X}(0|0) > 0$ and $\mathbb{P}_{Y|X}(0|1) = 0$.

Differential privacy.—To enforce protection of data, we impose the following condition on the conditional probability distribution $\mathbb{P}_{Y|X}$:

$$\forall x, x',\ \mathbb{P}_{Y|X}(\cdot|x') \le e^{\varepsilon}\mathbb{P}_{Y|X}(\cdot|x), \tag{1.5}$$

where $\varepsilon > 0$ is a constant. This condition is called *ε-differential privacy (ε-DP)* [17–19]. Differential privacy (DP) was introduced by Dwork et al. [19] and Dwork [18] in the *global privacy* context (the case when a company or government releases users' data partially for machine learning). After that, DP was also introduced by Duchi et al. [17] in the *local privacy* context (the case when data providers do not trust a data analyst). Definition (1.5) is that in the local privacy context.

DP has been studied intensively by using classical probability theory. However, there are only a few studies of quantum versions of DP [1, 15, 16, 56] to the best of our knowledge. In this thesis, we define a quantum version of DP and investigate its mathematical aspects when n-ary data X are converted to quantum states ρ depending on X (i.e., classical-quantum setting) in the local privacy context.

To define a quantum version of DP, we consider an n-tuple of quantum states $(\rho_x)_{x=1}^n$, where x and ρ_x correspond to an input classical state and its output quantum state, respectively. Now, a data analyst needs to measure a quantum state by a measurement $(M_y)_{y=1}^m$ in order to obtain some information about the quantum state. Hence, following the classical definition of DP, we define the *classical-quantum ε-differential privacy (CQ ε-DP)* as

$$\forall (M_y)_{y=1}^m \text{ POVM, the c.p.d. } \mathbb{P}(y|x) = \operatorname{Tr} \rho_x M_y \text{ satisfies } \varepsilon\text{-DP},$$

where "c.p.d." is an abbreviation of "conditional probability distribution". This condition is equivalent to the following one:

$$\forall x, x', \ \rho_{x'} \leq e^{\varepsilon} \rho_x,$$

where for Hermitian matrices H and H' the inequality $H \leq H'$ means for $H' - H$ to be positive semi-definite. The definition of CQ ε-DP is a simple extension of the classical one, because (1.5) can be written as

$$\forall x, x', \ p_{x'} \leq e^{\varepsilon} p_x$$

if replacing the probability distributions $\mathbb{P}_{Y|X}(\cdot|x)$ with probability vectors p_x, where for probability vectors p and p' the inequality $p \leq p'$ means for $p' - p$ to be non-negative. From now on, we use an n-tuple $(p_i)_{i=1}^n$ of probability vectors instead of $(\mathbb{P}_{Y|X}(\cdot|x))_{x=1}^n$.

We summarize the above definitions.

Definition 1.2 (Classical ε-DP [17] and classical-quantum ε-DP)**.** *Let $\varepsilon > 0$ be a real number and $n \geq 2$ be an integer. An n-tuple $(p_i)_{i=1}^n$ of probability vectors is called ε-differentially private (ε-DP) if $p_i \leq e^{\varepsilon} p_j$ for all $i, j = 1, \ldots, n$. An n-tuple $(\rho_i)_{i=1}^n$ of density matrices is called classical-quantum ε-differentially private (CQ ε-DP) if $\rho_i \leq e^{\varepsilon} \rho_j$ for all $i, j = 1, \ldots, n$. Also, define the sets $\mathrm{C}_n^{(d)}(\varepsilon)$, $\mathrm{CQ}_n^{(d)}(\varepsilon)$, $\mathrm{C}_n(\varepsilon)$ and $\mathrm{CQ}_n(\varepsilon)$ as*

$$\mathrm{C}_n^{(d)}(\varepsilon) = \{\varepsilon\text{-DP } (p_i)_{i=1}^n : \text{all } p_i \text{ are probability vectors in } \mathbb{R}^d\} \quad (d \geq 2),$$
$$\mathrm{CQ}_n^{(d)}(\varepsilon) = \{\text{CQ } \varepsilon\text{-DP } (\rho_i)_{i=1}^n : \text{all } \rho_i \text{ are density matrices on } \mathbb{C}^d\} \quad (d \geq 2),$$
$$\mathrm{C}_n(\varepsilon) = \bigcup_{d \geq 2} \mathrm{C}_n^{(d)}(\varepsilon), \quad \mathrm{CQ}_n(\varepsilon) = \bigcup_{d \geq 2} \mathrm{CQ}_n^{(d)}(\varepsilon).$$

If $(\rho_i)_{i=1}^n$ is CQ ε-DP, then all ρ_i have the same support, i.e., all the ranges of ρ_i are equal to one another. Hence, we often implicitly assume that all ρ_i have full rank if $(\rho_i)_{i=1}^n$ is CQ ε-DP.

Embedding classical states into quantum ones.—Next, let us consider a subset of $\mathrm{CQ}_n(\varepsilon)$ that corresponds to $\mathrm{C}_n(\varepsilon)$. For a probability vector $p = (p(i))_{i=1}^d \in \mathbb{R}^d$, define $\mathrm{diag}(p)$ as the diagonal matrix with diagonal entries $p(1), \dots, p(d)$, which is a density matrix on $\mathbb{C}^d$. Since a quantum (resp. classical) state is a density matrix (resp. probability vector), the mapping $\mathrm{diag}(\cdot)$ is an embedding from the set of classical states into the set of quantum ones. Using the mapping $\mathrm{diag}(\cdot)$, we obtain the set

$$\mathrm{diag}(\mathrm{C}_n(\varepsilon)) \coloneqq \{(\mathrm{diag}(p_i))_{i=1}^n : (p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)\}$$

that corresponds to $\mathrm{C}_n(\varepsilon)$.

Essentially classical elements.—The set $\mathrm{diag}(\mathrm{C}_n(\varepsilon))$ is much smaller than $\mathrm{CQ}_n(\varepsilon)$, but actually, there is a set larger than $\mathrm{diag}(\mathrm{C}_n(\varepsilon))$ that is "essentially classical". To describe such a set, we consider two optimization problems: one is the classical case

$$S_n^{\mathrm{C}}(\varepsilon;\Phi) = \underbrace{\sup_{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)}}_{\text{Privacy protection}} \underbrace{\Phi(\mathrm{diag}(p_1), \dots, \mathrm{diag}(p_n))}_{\text{Utility}}, \tag{1.6}$$

which is often considered in information-theoretic studies of DP [22–24, 30, 38]; the other is the quantum case

$$S_n^{\mathrm{CQ}}(\varepsilon;\Phi) = \underbrace{\sup_{(\rho_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)}}_{\text{Privacy protection}} \underbrace{\Phi(\rho_1, \dots, \rho_n)}_{\text{Utility}}.$$

The above Φ is a real-valued function of n density matrices that represents the utility of private data, and the conditions $(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)$ and $(\rho_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)$ represent the privacy protection. Since the data analyst's purpose is to maximally utilize private data under the privacy protection, we arrive at the above optimization problems.

Now, we want to define a subset of $\mathrm{CQ}_n(\varepsilon)$ that is "essentially classical". For this purpose, assume that the objective function Φ must satisfy monotonicity for *completely positive and trace-preserving linear maps (CPTP maps)*.

Definition 1.3 (Monotonicity for CPTP maps)**.** *A real-valued function Φ of n density matrices is called monotone for CPTP maps if*

$$\Phi(\Lambda(\rho_1), \dots, \Lambda(\rho_n)) \le \Phi(\rho_1, \dots, \rho_n)$$

for all density matrices $\rho_1, \dots, \rho_n$ and CPTP maps Λ. This inequality is called the information processing inequality (or data processing inequality).

Since a CPTP map is regarded as a quantum operation in quantum information theory, information-theoretic quantities usually satisfy monotonicity for CPTP maps. For example, quantum relative entropy, symmetric logarithmic derivative (SLD) Fisher information, Kubo–Mori–Bogoljubov (KMB) Fisher information, right logarithmic derivative (RLD) Fisher information, and trace distance satisfy monotonicity for CPTP maps [26, Theorems 5.7 and 6.2], [27, Theorem 6.7 and Lemma 6.9].

By monotonicity for CPTP maps, it follows that

$$\sup_{\substack{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon) \\ \Lambda \text{ CPTP map}}} \Phi\big(\Lambda(\mathrm{diag}(p_1)), \dots, \Lambda(\mathrm{diag}(p_n))\big) \le S_n^{\mathrm{C}}(\varepsilon; \Phi).$$

Moreover, the opposite inequality also holds, since the identity mapping on $\mathsf{Herm}(d)$ is a CPTP map. This fact leads us to the following definition.

Definition 1.4 (Essentially classical element)**.** *Let $\varepsilon > 0$ be a real number and $n \ge 2$ be an integer. We say that $(\rho_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)$ is essentially classical if there exist an ε-DP n-tuple $(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)$ and a CPTP map Λ such that $\Lambda(\mathrm{diag}(p_i)) = \rho_i$ for all $i = 1, \dots, n$. We denote by $\mathrm{EC}_n(\varepsilon)$ the set of all essentially classical elements in $\mathrm{CQ}_n(\varepsilon)$.*

Although an element in $\mathrm{EC}_n(\varepsilon)$ consists of quantum states, the equality

$$S_n^{\mathrm{EC}}(\varepsilon; \Phi) = S_n^{\mathrm{C}}(\varepsilon; \Phi)$$

holds, where $S_n^{\mathrm{EC}}(\varepsilon; \Phi)$ is defined in the same way as $S_n^{\mathrm{CQ}}(\varepsilon; \Phi)$. Hence, the comparison of $S_n^{\mathrm{C}}(\varepsilon; \Phi)$ and $S_n^{\mathrm{CQ}}(\varepsilon; \Phi)$ is the same as that of $S_n^{\mathrm{EC}}(\varepsilon; \Phi)$ and $S_n^{\mathrm{CQ}}(\varepsilon; \Phi)$.

Comparison of $\mathrm{EC}_n(\varepsilon)$ and $\mathrm{CQ}_n(\varepsilon)$.—Although the set $\mathrm{EC}_n(\varepsilon)$ is a subset of $\mathrm{CQ}_n(\varepsilon)$, we are interested in whether they are equal to each other or not. If $\mathrm{EC}_n(\varepsilon)$ is equal to $\mathrm{CQ}_n(\varepsilon)$, then $S_n^{\mathrm{C}}(\varepsilon; \Phi) = S_n^{\mathrm{EC}}(\varepsilon; \Phi) = S_n^{\mathrm{CQ}}(\varepsilon; \Phi)$, i.e., CQ ε-DP mechanisms have no quantum advantage in optimization. In this perspective, it is important to compare $\mathrm{EC}_n(\varepsilon)$ with $\mathrm{CQ}_n(\varepsilon)$.

Main results.—In this thesis, we show the following theorems.

Theorem 1.5. *For all $\varepsilon > 0$, $\mathrm{EC}_2(\varepsilon) = \mathrm{CQ}_2(\varepsilon)$.*

Theorem 1.6. *For all $\varepsilon > 0$ and $n \ge 3$, $\mathrm{EC}_n(\varepsilon) \ne \mathrm{CQ}_n(\varepsilon)$.*

Table 1.2: Quantum versions of DP.

	Input	Output	Context
This thesis	Classical	Quantum	Local privacy
Ref. [16]	Quantum	Quantum	Local privacy
Refs. [1, 15, 56]	Quantum	Quantum	Global privacy

By Theorem 1.5, it follows that $S_2^{\mathrm{C}}(\varepsilon;\Phi) = S_2^{\mathrm{EC}}(\varepsilon;\Phi) = S_2^{\mathrm{CQ}}(\varepsilon;\Phi)$. We will actually prove Theorem 4.2 that is stronger than Theorem 1.5, and prove Theorem 1.6 by giving a concrete objective function Φ such that $S_n^{\mathrm{C}}(\varepsilon;\Phi) = S_n^{\mathrm{EC}}(\varepsilon;\Phi) < S_n^{\mathrm{CQ}}(\varepsilon;\Phi)$ for every $n \geq 3$ (Theorem 4.5). Theorem 4.5 implies a sufficient condition for a CQ ε-DP n-tuple not to lie in $\mathrm{EC}_n(\varepsilon)$ (Corollary 4.6). Using Corollary 4.6, we construct CQ ε-DP n-tuples that do not lie in $\mathrm{EC}_n(\varepsilon)$ (Section 4.5).

We mention a relation among this thesis and existing studies briefly. As seen from Table 1.2, Refs. [1, 15, 16, 56] consider the case when input and output states are quantum. The definition of CQ ε-DP can be regarded as a special case of quantum DP [16], but [16] does not include our results.

Supplement on the set $\mathrm{EC}_n(\varepsilon)$**.**—Actually, the set $\mathrm{EC}_n(\varepsilon)$ can be written without CPTP maps.

Proposition 1.7. *For all $\varepsilon > 0$ and $n \geq 2$,*

$$\mathrm{EC}_n(\varepsilon) = \left\{ \left(\sum_k p_i(k)\sigma_k \right)_{i=1}^n : (p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon), \ \textit{density matrices } \sigma_k \right\}, \tag{1.7}$$

where the above sum is taken all over $k = 1, \ldots, d$ if d is the dimension of the vector space that $p_1, \ldots, p_n$ inhabit.

Proposition 1.7 can easily be checked; see Section 4.1. Although we have defined the set $\mathrm{EC}_n(\varepsilon)$ with CPTP maps, the same set is obtained even if replacing CPTP maps with positive and trace-preserving linear maps (PTP maps). That is, complete positivity is unnecessary, and positivity suffices in Definition 1.4. However, we have used CPTP maps in Definition 1.4 because CPTP maps are more natural in quantum information theory than PTP maps, and monotonicity for CPTP maps is used in Section 4.3.

1.3 Perfect discrimination of two states

Let $(\mathcal{V}, \mathcal{K}, u)$ be a GPT. We say that m states $x_1, \ldots, x_m \in \mathcal{S}(\mathcal{K}, u)$ are *simultaneously and perfectly distinguishable* if there exists a measurement $(y_j)_{j=1}^m \in \mathcal{M}(\mathcal{K}^*, u)$ such

that $\langle x_i, y_j \rangle = \delta_{i,j}$ for all $i, j = 1, \ldots, m$, where $\delta_{i,j}$ denotes the Kronecker delta. In the case $m = 2$, two states x_1 and x_2 are called *perfectly distinguishable* if they are simultaneously and perfectly distinguishable. It is a fundamental problem whether two given states are perfectly distinguishable or not.

In quantum theory, the following equivalence is widely known (see a textbook in quantum information theory, e.g., [26, p. 138], [27, Proposition 5.13]):

(E) two states ρ_1 and ρ_2 are perfectly distinguishable if and only if $\operatorname{Tr} \rho_1 \rho_2 = 0$.

However, equivalence E does not hold for a general GPT even if the GPT is locally quantum [3]. Some existing studies other than [3] show a difference between quantum theory and an alternative model, but they consider only GPTs that are too far from quantum theory. For example, quantum theory has an upper bound called Tsirelson's bound in the CHSH inequality (named after Clauser, Horne, Shimony, and Holt [11]). The GPT called PR box violates it [46,47], but the PR box is never close to quantum theory, since the set of states in the PR box is a square. Such GPTs are unlikely to exist in reality. Hence, it is more insightful to consider GPTs that are sufficiently close to quantum theory in order to further understand quantum theory.

Main results.—In this thesis, we investigate perfect discrimination of two states in a bipartite locally quantum system $(\mathsf{Herm}(d_1 d_2), \mathcal{K}, I_{d_1 d_2})$, i.e., a whole system of two quantum subsystems $(\mathsf{Herm}(d_1), \mathsf{PSD}(d_1), I_{d_1})$ and $(\mathsf{Herm}(d_2), \mathsf{PSD}(d_2), I_{d_2})$. Since our purpose is to make $\mathcal{K}$ sufficiently close to $\mathsf{PSD}(d_1 d_2)$, we construct two convex cones $\mathcal{K}_s^{\mathrm{neg}}$ and $\mathcal{K}_s^{\mathrm{sc}}$ for $s \geq 0$ in a certain natural manner (for details, see Section 5.1), and consider the locally quantum systems

$$(\mathsf{Herm}(d_1 d_2), (\mathcal{K}_s^{\mathrm{neg}})^*, I_{d_1 d_2}) \quad \text{and} \quad (\mathsf{Herm}(d_1 d_2), (\mathcal{K}_s^{\mathrm{sc}})^*, I_{d_1 d_2}). \tag{1.8}$$

The resulting convex cones $\mathcal{K}_s^{\mathrm{neg}}$, $\mathcal{K}_s^{\mathrm{sc}}$, $(\mathcal{K}_s^{\mathrm{neg}})^*$ and $(\mathcal{K}_s^{\mathrm{sc}})^*$ are sufficiently close to $\mathsf{PSD}(d_1 d_2)$ if s is small enough. In this sense, the locally quantum systems (1.8) are sufficiently close to quantum theory if s is small enough. Nevertheless, the locally quantum systems (1.8) violate equivalence E unless $s = 0$. More precisely, we show the following theorems in Section 5.2.

Theorem 1.8 (Perfect discrimination with $\mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$)**.** *Let s be a real number in the interval $[0, 1/4]$, and $\rho_1^{[1]}, \rho_1^{[2]}, \rho_2^{[1]}, \rho_2^{[2]}$ be rank-one density matrices. If the point $(\operatorname{Tr} \rho_1^{[1]} \rho_2^{[1]}, \operatorname{Tr} \rho_1^{[2]} \rho_2^{[2]})$ belongs to the set*

$$\{(x, y) \in [0, 1]^2 : xy \leq 16 s^2 (1 - x)(1 - y)\}, \tag{1.9}$$

then the two states $\rho_1 = \rho_1^{[1]} \otimes \rho_1^{[2]}$ and $\rho_2 = \rho_2^{[1]} \otimes \rho_2^{[2]}$ are perfectly distinguishable by some measurement in $\mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$.

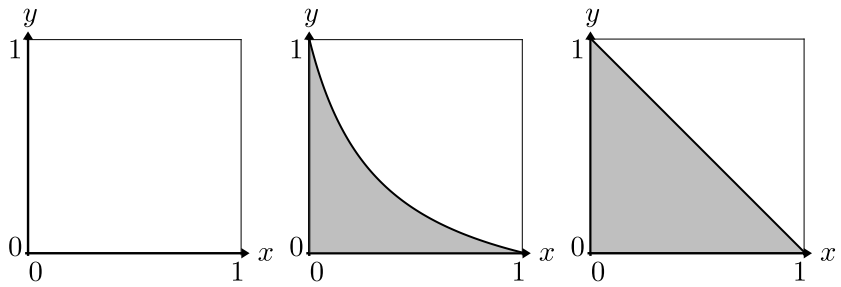

Figure 1.1: The above figures illustrate the set (1.9) for $s = 0, 1/8, 1/4$, from left to right. They also correspond to the set (1.10) for $(s,t) = (0,0), (2/5,1/4), (1/2,1)$, from left to right.[1]

Theorem 1.9 (Perfect discrimination with $\mathcal{M}(\mathcal{K}_s^{\rm sc})$)**.** *Let t be a real number in the interval $[0,1]$, and $\rho_1^{[1]}, \rho_1^{[2]}, \rho_2^{[1]}, \rho_2^{[2]}$ be rank-one density matrices. If the point $(\mathrm{Tr}\,\rho_1^{[1]}\rho_2^{[1]}, \mathrm{Tr}\,\rho_1^{[2]}\rho_2^{[2]})$ belongs to the set*

$$\{(x,y) \in [0,1]^2 : xy \leq t(1-x)(1-y)\}, \tag{1.10}$$

then the two states $\rho_1 = \rho_1^{[1]} \otimes \rho_1^{[2]}$ and $\rho_2 = \rho_2^{[1]} \otimes \rho_2^{[2]}$ are perfectly distinguishable by some measurement in $\mathcal{M}(\mathcal{K}_s^{\rm sc})$ with $s = \sqrt{t}/(1+t)$.

The sets (1.9) and (1.10) are illustrated as Figure 1.1. Once the parameter s decreases, the sets (1.9) and (1.10) become smaller. Since the orthogonality $\mathrm{Tr}\,\rho_1\rho_2 = 0$ can be rewritten as $(\mathrm{Tr}\,\rho_1^{[1]}\rho_2^{[1]})(\mathrm{Tr}\,\rho_1^{[2]}\rho_2^{[2]}) = 0$, we find that the locally quantum systems (1.8) violate equivalence E unless $s = 0$. Also, a rank-one density matrix is called *pure*, and often plays an important role in quantum information processing. Hence, Theorems 1.8 and 1.9 are meaningful results.

[1] [53]

Chapter 2

GPTs and their capacities

In this chapter, we describe the framework of GPTs, define the capacities of GPTs, and prove a few statements on capacities briefly. The contents of this chapter except for Proposition 2.3 rely on [54] (framework of GPTs) and [42] (capacities) essentially.

2.1 Framework of GPTs

A GPT is defined as the triplet of (i) a real Hilbert space $\mathcal{V}$ equipped with an inner product $\langle \cdot, \cdot \rangle$, (ii) a proper cone $\mathcal{K}$ of $\mathcal{V}$, and (iii) an element u in the interior of the dual cone $\mathcal{K}^*$, where a subset $\mathcal{K}$ of $\mathcal{V}$ is called a *convex cone* if $\alpha u + \beta v \in \mathcal{K}$ for all $u, v \in \mathcal{K}$ and $\alpha, \beta \geq 0$; a convex cone $\mathcal{K}$ is called *proper* if $\mathcal{K}$ is closed, has an interior point, and satisfies $\mathcal{K} \cap (-\mathcal{K}) = \{0\}$. Throughout this thesis, we assume that $\mathcal{V}$ is finite-dimensional. It is widely known that (see a textbook in convex analysis, e.g., [8, p. 53])

- if $\mathcal{K}$ is a non-empty closed convex cone, then $\mathcal{K}^{**} = \mathcal{K}$;
- if $\mathcal{K}$ is a proper cone, then so is $\mathcal{K}^*$.

The element u is called a *unit effect* and fixed for each GPT. Also, for a GPT $(\mathcal{V}, \mathcal{K}, u)$, the state class $\mathcal{S}(\mathcal{K}, u)$ and measurement class $\mathcal{M}(\mathcal{K}^*, u)$ are defined as (1.1). As a convex cone to define a measurement class, one can use another proper cone $\mathcal{K}' \subset \mathcal{K}^*$ instead of $\mathcal{K}^*$, but the condition $\mathcal{K}' = \mathcal{K}^*$ is imposed in usual, which is assumed in this thesis.

Given a state $x \in \mathcal{S}(\mathcal{K}, u)$ and a measurement $(y_i)_{i=1}^m \in \mathcal{M}(\mathcal{K}^*, u)$, the probability of obtaining each outcome $i = 1, \ldots, m$ is $\langle x, y_i \rangle$. Note that $(\langle x, y_i \rangle)_{i=1}^m$ is a probability vector due to definition (1.1).

For n GPTs $(\mathcal{V}^{[i]}, \mathcal{K}^{[i]}, u^{[i]})$ (which are called subsystems), a whole system $(\mathcal{V}, \mathcal{K}, u)$ of these subsystems is defined as stated in Chapter 1. It is important that $\mathcal{K}$ is not uniquely determined even if its subsystems are given, since $\mathcal{K}_{\min}$ and $\mathcal{K}_{\max}$ defined in (1.2) are not equal to each other in general.

We recall the three types of GPTs below which have been defined in Chapter 1. For classical and quantum systems, see also Table 1.1.

Classical system.—The triplet $(\mathbb{R}^d, [0,\infty)^d, \mathbf{1}_d)$ is a GPT called *d-level classical system*. The proper cone $[0,\infty)^d$ is *self-dual*, i.e., $([0,\infty)^d)^* = [0,\infty)^d$. If $\mathcal{K}^{[i]} = [0,\infty)^{d_i}$ for all $i = 1, \ldots, n$, then it can easily be checked that $\mathcal{K}_{\min} = \mathcal{K}_{\max}$. Therefore, a whole system of classical subsystems is classical.

Quantum system.—The triplet $(\mathsf{Herm}(d), \mathsf{PSD}(d), I_d)$ is a GPT called *d-level quantum system*. Note that $\mathsf{PSD}(d)$ is self-dual, i.e., $\mathsf{PSD}(d)^* = \mathsf{PSD}(d)$. The state class $\mathcal{S}(\mathsf{PSD}(d), I_d)$ is the set of all density matrices, and the measurement class $\mathcal{M}(\mathsf{PSD}(d), I_d)$ is the set of all POVMs.

Locally quantum system.—For integers $d_1, \ldots, d_n \geq 2$, denote by $\tilde{d}$ the product $d_1 d_2 \cdots d_n$. For d_i-level quantum systems, $i = 1, \ldots, n$, a whole system $(\mathcal{V}, \mathcal{K}, u)$ of these subsystems is called a *$(d_1, \ldots, d_n)$-level locally quantum system*. Let $(\mathcal{V}, \mathcal{K}, u)$ be a $(d_1, \ldots, d_n)$-level locally quantum system. Then

$$\mathcal{V} = \mathsf{Herm}(d_1) \otimes \cdots \otimes \mathsf{Herm}(d_n) \quad \text{and} \quad u = I_{d_1} \otimes \cdots \otimes I_{d_n} = I_{\tilde{d}}.$$

The tensor product $\mathcal{V}$ can be regarded as a subspace of $\mathsf{Herm}(\tilde{d})$ by using the Kronecker product below. The tensor product of two matrices $A^{[1]} = (a^{[1]}_{i,j})_{1 \leq i,j \leq d_1}$ and $A^{[2]} = (a^{[2]}_{i,j})_{1 \leq i,j \leq d_2}$ can be expressed as a block matrix:

$$A^{[1]} \otimes A^{[2]} = \begin{bmatrix} a^{[1]}_{1,1} A^{[2]} & \cdots & a^{[1]}_{1,d_1} A^{[2]} \\ \vdots & \ddots & \vdots \\ a^{[1]}_{d_1,1} A^{[2]} & \cdots & a^{[1]}_{d_1,d_1} A^{[2]} \end{bmatrix}$$

This is called the *Kronecker product*. For $n \geq 3$, the tensor product of n matrices can also be expressed in the same way (but we do not use it in this thesis). Under this identification, $\mathcal{V}$ is equal to $\mathsf{Herm}(\tilde{d})$, since (i) $\mathcal{V}$ is a subspace of $\mathsf{Herm}(\tilde{d})$, and (ii) the dimensions of $\mathcal{V}$ and $\mathsf{Herm}(\tilde{d})$ are equal to each other.

Let us return to the $(d_1, \ldots, d_n)$-level locally quantum system $(\mathcal{V}, \mathcal{K}, u)$. Using the set $\mathsf{Sep}(d_1, \ldots, d_n)$ defined in Section 1.1, we have

$$\mathcal{K}_{\min} = \mathsf{Sep}(d_1, \ldots, d_n) \quad \text{and} \quad \mathcal{K}_{\max} = \mathsf{Sep}(d_1, \ldots, d_n)^*.$$

Thus, $\mathcal{K}$ satisfies the inclusion relation $\mathsf{Sep}(d_1,\ldots,d_n) \subset \mathcal{K} \subset \mathsf{Sep}(d_1,\ldots,d_n)^*$. Moreover, for all integers $n \geq 2$ and $d_1,\ldots,d_n \geq 2$, the two proper cones $\mathsf{Sep}(d_1,\ldots,d_n)$ and $\mathsf{Sep}(d_1,\ldots,d_n)^*$ are not equal to each other. Also, the $\tilde{d}$-level quantum system is a $(d_1,\ldots,d_n)$-level locally quantum system, since the inclusion relation $\mathsf{Sep}(d_1,\ldots,d_n) \subset \mathsf{PSD}(\tilde{d}) \subset \mathsf{Sep}(d_1,\ldots,d_n)^*$ holds.

2.2 Capacities of locally quantum systems

For a GPT $(\mathcal{V},\mathcal{K},u)$, simultaneously and perfectly distinguishable states are defined in Sections 1.3. We define the capacity of a GPT.

Definition 2.1 (Capacity)**.** *For a GPT $(\mathcal{V},\mathcal{K},u)$, the maximum number of simultaneously and perfectly distinguishable states is called the capacity. We denote by* $\mathrm{capa}(\mathcal{V},\mathcal{K},u)$ *the capacity of a GPT $(\mathcal{V},\mathcal{K},u)$.*

For example, it is known that the capacity of d-level quantum system is equal to d. As proved below, the capacity of each (d_1,d_2)-level locally quantum system is equal to d_1d_2. This fact is found in [42] (without proof).

Proposition 2.2. *Let $d_1,d_2 \geq 2$ be integers. For every (d_1,d_2)-level locally quantum system, the capacity is equal to d_1d_2.*

Proposition 2.2 asserts that the capacity of a locally quantum system only depends on its dimension. However, another property discussed in Chapter 5 changes depending on the convex cone of the locally quantum system.

Before proving Proposition 2.2, we describe notational conventions. A vector $u \in \mathbb{C}^d$ is expressed as a column vector. Also, we use the bra-ket notation: for $u \in \mathbb{C}^d$, $|u\rangle$ and $\langle u|$ denote the column vector u and its conjugate transpose, respectively. Hence, $\langle\cdot|\cdot\rangle$ gives the standard Hermitian inner product on $\mathbb{C}^d$, and $|u\rangle\langle u|$ is a rank-one orthogonal projection for every unit vector $u \in \mathbb{C}^d$. When $(\mathcal{V},\mathcal{K},u)$ is a locally quantum system, we simply write $\mathcal{S}(\mathcal{K},u)$ and $\mathcal{M}(\mathcal{K}^*,u)$ as $\mathcal{S}(\mathcal{K})$ and $\mathcal{M}(\mathcal{K}^*)$, respectively.

Proof of Proposition 2.2. We use the fact that statement SS holds in the case $n=2$ [25]. First, let us show that every $Y \in \mathsf{Sep}(d_1,d_2)^*$ satisfies $\|Y\|_2 \leq \operatorname{Tr} Y$. Since the case $Y=0$ is trivial, assume that $Y \in \mathsf{Sep}(d_1,d_2)^*$ is non-zero. Set $X = -Y/\|Y\|_2$. Then $I_{d_1d_2}+X$ lies in $\mathsf{Sep}(d_1,d_2)$. Thus, $\operatorname{Tr} Y - \|Y\|_2 = \operatorname{Tr}(I_{d_1d_2}+X)Y \geq 0$.

Let $(\mathsf{Herm}(d_1d_2),\mathcal{K},I_{d_1d_2})$ be a (d_1,d_2)-level locally quantum system. Next, we show that the capacity is equal to d_1d_2. Suppose that m states $\rho_1,\ldots,\rho_m \in \mathcal{S}(\mathcal{K})$

are simultaneously and perfectly distinguishable by a measurement $(M_j)_{j=1}^m$. Then

$$\begin{aligned} m &\overset{(a)}{=} \sum_{i=1}^m \operatorname{Tr} \rho_i M_i \leq \sum_{i=1}^m \|\rho_i\|_2 \, \|M_i\|_2 \overset{(b)}{\leq} \sum_{i=1}^m (\operatorname{Tr} \rho_i)(\operatorname{Tr} M_i) \\ &\overset{(c)}{=} \sum_{i=1}^m \operatorname{Tr} M_i \overset{(d)}{=} \operatorname{Tr} I_{d_1 d_2} = d_1 d_2, \end{aligned} \tag{2.1}$$

where (a), (b), (c) and (d) follow from the facts $\operatorname{Tr} \rho_i M_i = 1$, $\rho_i, M_i \in \mathsf{Sep}(d_1, d_2)^*$, $\operatorname{Tr} \rho_i = \operatorname{Tr} \rho_i I_{d_1 d_2} = 1$ and $\sum_{i=1}^m M_i = I_{d_1 d_2}$, respectively. Therefore, the capacity is less than or equal to $d_1 d_2$. Since the $d_1 d_2$ states

$$|e_i^{[1]}\rangle\langle e_i^{[1]}| \otimes |e_j^{[2]}\rangle\langle e_j^{[2]}| \in \mathcal{S}(\mathcal{K}) \quad (1 \leq i \leq d_1, \ 1 \leq j \leq d_2)$$

are simultaneously and perfectly distinguishable by the measurement $(|e_i^{[1]}\rangle\langle e_i^{[1]}| \otimes |e_j^{[2]}\rangle\langle e_j^{[2]}|)_{i,j} \in \mathcal{M}(\mathcal{K}^*)$, we find that the capacity is equal to $d_1 d_2$. □

We have used statement SS with $n = 2$ in the above proof, but statement SS is false in general [4, 28]. Instead of statement SS, let us focus on statement S. As already stated in Section 1.1, statement S is still open for $n \geq 3$ to the best of our knowledge. Finally, assuming statement S, we show the following proposition.

Proposition 2.3. *Assume that statement S is true for all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$. Let $(\mathsf{Herm}(\tilde{d}), \mathcal{K}, I_{\tilde{d}})$ be a $(d_1, \ldots, d_n)$-level locally quantum system satisfying either $\mathcal{K} \subset \mathsf{PSD}(\tilde{d})$ or $\mathcal{K} \supset \mathsf{PSD}(\tilde{d})$. Then* $\operatorname{capa}(\mathsf{Herm}(\tilde{d}), \mathcal{K}, I_{\tilde{d}})$ *is equal to $\tilde{d}$.*

Proof. First, let us show that every $Y \in \mathsf{Sep}(d_1, \ldots, d_n)^*$ satisfies $\|Y\| \leq \operatorname{Tr} Y$, where $\|\cdot\|$ denotes the operator norm. Due to statement S, it follows that $\operatorname{Tr} Y \pm \langle u|Y|u\rangle = \operatorname{Tr}(I_{\tilde{d}} \pm |u\rangle\langle u|)Y \geq 0$ for every unit vector $u \in \mathcal{H}(d_1, \ldots, d_n)$. Thus, $\|Y\| \leq \operatorname{Tr} Y$.

The remainder is almost the same as the proof of Proposition 2.2. The difference between the proof of Proposition 2.2 and this proof is only (2.1). We must change (2.1) as follows:

$$\begin{aligned} m = \sum_{i=1}^m \operatorname{Tr} \rho_i M_i &\leq \begin{cases} \sum_{i=1}^m \|\rho_i\|_1 \, \|M_i\| & \mathcal{K} \subset \mathsf{PSD}(\tilde{d}), \\ \sum_{i=1}^m \|\rho_i\| \, \|M_i\|_1 & \mathcal{K} \supset \mathsf{PSD}(\tilde{d}) \end{cases} \\ &\leq \sum_{i=1}^m (\operatorname{Tr} \rho_i)(\operatorname{Tr} M_i) = \sum_{i=1}^m \operatorname{Tr} M_i = \operatorname{Tr} I_{\tilde{d}} = \tilde{d}, \end{aligned}$$

where $\|\cdot\|_1$ denotes the trace norm. □

Chapter 3

Weaker statement: Maximum dimension of subspaces with no product basis

In this chapter, we prove Theorem 1.1. Although the scalar field in Theorem 1.1 is the field of complex numbers, the same theorem holds in replacing it with an arbitrary infinite field. We also address the case of finite fields.

3.1 More general proposition and proof

Let $(e_i^{[j]})_{i=1}^{d_j}$ be the standard basis of $\mathbb{C}^{d_j}$ for $j = 1, \ldots, n$. Denote by $\mathrm{span}(\mathcal{S})$ the linear span of a subset $\mathcal{S}$, and by $\mathcal{L}^\perp$ the orthogonal complement of a subspace $\mathcal{L}$. Although product vectors have been already defined in the case $n \geq 2$, all vectors are regarded as product vectors in the case $n = 1$.

Now, we prove the following proposition which is more general than statement WS.

Proposition 3.1. *Let $n \geq 1$ and $d_1, \ldots, d_n \geq 2$ be integers, and r be an integer in the interval $[0, \min\{d_1, \ldots, d_n\}]$. If the dimension of a subspace $\mathcal{L}$ of $\mathcal{H}(d_1, \ldots, d_n)$ is greater than or equal to $\tilde{d} - r$, then $\mathcal{L}$ has a $(\tilde{d} - r^n)$-tuple $(u_i)_{i=1}^{\tilde{d}-r^n}$ of linearly independent product vectors.*

To prove Proposition 3.1, we need two lemmas. The first one is basic in algebra, and the second one is proved by using the first one.

Lemma 3.2. *Let $\mathcal{F}$ be an infinite field, $n \geq 1$ be an integer, and $f(x_1, \ldots, x_n)$ be a polynomial over $\mathcal{F}$. Then the following conditions are equivalent:*

1. *$f(\alpha_1, \ldots, \alpha_n) = 0$ for all $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$;*
2. *$f(x_1, \ldots, x_n) = 0$ as a polynomial.*

Proof. See [34, Theorem 2.19]. □

Lemma 3.3. *Let $m, n \geq 1$, $d_1, \ldots, d_n \geq 2$ and $r \in [1, \tilde{d}]$ be integers, and let $(u_{k,l})_{l=1}^{\tilde{d}-r}$, $k = 1, \ldots, m$, be $(\tilde{d}-r)$-tuples of linearly independent vectors in $\mathcal{H}(d_1, \ldots, d_n)$. Then there exist product vectors $v_1, \ldots, v_r \in \mathcal{H}(d_1, \ldots, d_n)$ such that*

$$\det[u_{k,1}, \ldots, u_{k,\tilde{d}-r}, v_1, \ldots, v_r] \neq 0$$

for all $k = 1, \ldots, m$.

Proof. Let $(e_i)_{i=1}^{\tilde{d}}$ be the standard basis of $\mathcal{H}(d_1, \ldots, d_n)$, and let $n' = r(d_1 + \cdots + d_n)$. Define the m polynomials $f_k(x_1, \ldots, x_{n'})$ over $\mathbb{C}$ as

$$f_k(x_1, \ldots, x_{n'}) = \det[u_{k,1}, \ldots, u_{k,\tilde{d}-r}, v_1, \ldots, v_r] \quad (k = 1, \ldots, m),$$
$$v_i = v_i^{[1]} \otimes \cdots \otimes v_i^{[n]} \quad (i = 1, \ldots, r),$$

where the variables $x_1, \ldots, x_{n'}$ correspond to the n' entries of $v_i^{[j]}$, $1 \leq i \leq r$, $1 \leq j \leq n$. Since $(u_{k,l})_{l=1}^{\tilde{d}-r}$, $k = 1, \ldots, m$, are tuples of linearly independent vectors, we have $f_k(\alpha_1, \ldots, \alpha_{n'}) \neq 0$ for some $\alpha_1, \ldots, \alpha_{n'} \in \mathbb{C}$ corresponding to $v_1, \ldots, v_r \in \{e_1, \ldots, e_{\tilde{d}}\}$ (note that $e_1, \ldots, e_{\tilde{d}}$ are product vectors). Therefore, for every $k = 1, \ldots, m$, the polynomial $f_k(x_1, \ldots, x_{n'})$ is not zero as a polynomial. Since the polynomial ring $\mathbb{C}[x_1, \ldots, x_{n'}]$ is an integral domain, the product $f(x_1, \ldots, x_{n'}) \coloneqq \prod_{k=1}^{m} f_k(x_1, \ldots, x_{n'})$ is not also zero as a polynomial. Thus, Lemma 3.2 implies that $f(\beta_1, \ldots, \beta_{n'}) \neq 0$ for some $\beta_1, \ldots, \beta_{n'} \in \mathbb{C}$. Taking the vectors $v_i^{[j]}$ corresponding to $\beta_1, \ldots, \beta_{n'} \in \mathbb{C}$, we obtain desired product vectors $v_1, \ldots, v_r$. □

Proof of Proposition 3.1. Since the case $r = 0$ is clear, we assume the condition $r \geq 1$ in this proof. We show the proposition by induction on $n \geq 1$. First, the case $n = 1$ is trivial. Let $n \geq 2$ and assume that the proposition is true for $n-1$. Then we show that the proposition is also true for n. Let the dimension of a subspace $\mathcal{L}$ be greater than or equal to $\tilde{d} - r$. For some $w_1, \ldots, w_r \in \mathcal{L}^{\perp}$, the subspace $\mathcal{L}$ can be expressed as

$$\mathcal{L} = \{u \in \mathcal{H}(d_1, \ldots, d_n) : \forall i = 1, \ldots, r,\ \langle w_i | u \rangle = 0\}.$$

Now, take a basis $(u_k^{[1]})_{k=1}^{d_1}$ of $\mathbb{C}^{d_1}$ and set $\tilde{d}' = \tilde{d}/d_1$. Since the dimension of the subspace

$$\mathcal{L}_k^{[2:n]} := \{u^{[2:n]} \in \mathcal{H}(d_2, \dots, d_n) : \forall i = 1, \dots, r,\ \langle w_i | u_k^{[1]} \otimes u^{[2:n]} \rangle = 0\}$$

is greater than or equal to $\tilde{d}' - r$ for every $k = 1, \dots, d_1$, the induction hypothesis implies that $\mathcal{L}_k^{[2:n]}$ has a $(\tilde{d}' - r^{n-1})$-tuple $(u_{k,l}^{[2:n]})_{l=1}^{\tilde{d}' - r^{n-1}}$ of linearly independent product vectors. Also, due to Lemma 3.3, we can take an r^{n-1}-tuple $(v_s^{[2:n]})_{s=1}^{r^{n-1}}$ of product vectors with the following condition:

$$\forall k = 1, \dots, d_1,\ \det[u_{k,1}^{[2:n]}, \dots, u_{k,\tilde{d}' - r^{n-1}}^{[2:n]}, v_1^{[2:n]}, \dots, v_{r^{n-1}}^{[2:n]}] \neq 0. \tag{3.1}$$

Moreover, for every $s = 1, \dots, r^{n-1}$, take a $(d_1 - r)$-tuple $(v_{s,t}^{[1]})_{t=1}^{d_1 - r}$ of linearly independent vectors in the subspace

$$\mathcal{L}_s^{[1]} := \{u^{[1]} \in \mathbb{C}^{d_1} : \forall i = 1, \dots, r,\ \langle w_i | u^{[1]} \otimes v_s^{[2:n]} \rangle = 0\}.$$

Note that the $r^{n-1}(d_1 - r)$ vectors $v_{s,t}^{[1]} \otimes v_s^{[2:n]}$ are linearly independent.

Let us show that the $\tilde{d} - r^n$ product vectors of $\mathcal{L}$

$$u_k^{[1]} \otimes u_{k,l}^{[2:n]}, \quad v_{s,t}^{[1]} \otimes v_s^{[2:n]} \quad \left(\begin{array}{cc} 1 \le k \le d_1, & 1 \le l \le \tilde{d}' - r^{n-1}, \\ 1 \le s \le r^{n-1}, & 1 \le t \le d_1 - r \end{array} \right) \tag{3.2}$$

are linearly independent. Suppose that $\tilde{d} - r^n$ scalars $\alpha_{k,l}$ and $\beta_{s,t}$ satisfy

$$\sum_{k,l} \alpha_{k,l} u_k^{[1]} \otimes u_{k,l}^{[2:n]} + \sum_{s,t} \beta_{s,t} v_{s,t}^{[1]} \otimes v_s^{[2:n]} = 0. \tag{3.3}$$

Since $(u_k^{[1]})_{k=1}^{d_1}$ is a basis of $\mathbb{C}^{d_1}$, for all s and t, there exist scalars $\gamma_{s,t,k}$ such that $v_{s,t}^{[1]} = \sum_k \gamma_{s,t,k} u_k^{[1]}$. Thus, (3.3) can be rewritten as follows:

$$\begin{aligned} 0 &= \sum_{k,l} \alpha_{k,l} u_k^{[1]} \otimes u_{k,l}^{[2:n]} + \sum_{s,t,k} \beta_{s,t} \gamma_{s,t,k} u_k^{[1]} \otimes v_s^{[2:n]} \\ &= \sum_k u_k^{[1]} \otimes \Big(\sum_l \alpha_{k,l} u_{k,l}^{[2:n]} + \sum_{s,t} \beta_{s,t} \gamma_{s,t,k} v_s^{[2:n]} \Big). \end{aligned}$$

Since $(u_k^{[1]})_{k=1}^{d_1}$ is a basis of $\mathbb{C}^{d_1}$, we have

$$\sum_l \alpha_{k,l} u_{k,l}^{[2:n]} + \sum_{s,t} \beta_{s,t} \gamma_{s,t,k} v_s^{[2:n]} = 0$$

for every $k = 1, \dots, d_1$. This and (3.1) imply that $\alpha_{k,l} = 0$ for all k and l. Thus, (3.3) turns to $\sum_{s,t} \beta_{s,t} v_{s,t}^{[1]} \otimes v_s^{[2:n]} = 0$. Since the $r^{n-1}(d_1 - r)$ vectors $v_{s,t}^{[1]} \otimes v_s^{[2:n]}$ are linearly independent, it follows that $\beta_{s,t} = 0$ for all s and t. Therefore, the vectors (3.2) are linearly independent, and the proposition is also true for n. □

Next, we construct a $(\tilde{d}-2)$-dimensional subspace with no product basis by using the case $n = 2$.

Proposition 3.4. *For all integers $n \geq 2$ and $d_1, \dots, d_n \geq 2$, there exists a $(\tilde{d}-2)$-dimensional subspace of $\mathcal{H}(d_1, \dots, d_n)$ with no product basis.*

Proof. First, assuming $n = 2$, we show that the $(\tilde{d}-2)$-dimensional subspace

$$\mathcal{L}^{[1:2]} \coloneqq \operatorname{span}\big(\{e_1^{[1]} \otimes e_1^{[2]} + e_2^{[1]} \otimes e_2^{[2]}\} \cup \{e_i^{[1]} \otimes e_j^{[2]} : (i,j) \neq (1,1), (2,1), (2,2)\}\big) \quad (3.4)$$

has no product basis. Take an arbitrary product vector $u = u^{[1]} \otimes u^{[2]} \in \mathcal{L}^{[1:2]}$ with the expressions $u^{[k]} = \sum_{i=1}^{d_k} \alpha_i^{[k]} e_i^{[k]}$, $\alpha_i^{[k]} \in \mathbb{C}$, $k = 1, 2$. Then u is expressed in two ways:

$$\begin{aligned} u &= \sum_{i,j} \alpha_i^{[1]} \alpha_j^{[2]} e_i^{[1]} \otimes e_j^{[2]} \\ &= \beta(e_1^{[1]} \otimes e_1^{[2]} + e_2^{[1]} \otimes e_2^{[2]}) + \sum_{(i,j) \neq (1,1),(2,1),(2,2)} \alpha_i^{[1]} \alpha_j^{[2]} e_i^{[1]} \otimes e_j^{[2]} \quad (\exists \beta \in \mathbb{C}), \end{aligned}$$

where the second equality follows from the basis (3.4) of $\mathcal{L}^{[1:2]}$. For readability, write the matrix representation of the above expression:

$$\begin{bmatrix} \alpha_1^{[1]}\alpha_1^{[2]} & \alpha_1^{[1]}\alpha_2^{[2]} & \cdots & \alpha_1^{[1]}\alpha_{d_2}^{[2]} \\ \alpha_2^{[1]}\alpha_1^{[2]} & \alpha_2^{[1]}\alpha_2^{[2]} & \cdots & \alpha_2^{[1]}\alpha_{d_2}^{[2]} \\ \vdots & \vdots & & \vdots \\ \alpha_{d_1}^{[1]}\alpha_1^{[2]} & \alpha_{d_1}^{[1]}\alpha_2^{[2]} & \cdots & \alpha_{d_1}^{[1]}\alpha_{d_2}^{[2]} \end{bmatrix} = \begin{bmatrix} \beta & \alpha_1^{[1]}\alpha_2^{[2]} & \cdots & \alpha_1^{[1]}\alpha_{d_2}^{[2]} \\ 0 & \beta & \cdots & \alpha_2^{[1]}\alpha_{d_2}^{[2]} \\ \vdots & \vdots & & \vdots \\ \alpha_{d_1}^{[1]}\alpha_1^{[2]} & \alpha_{d_1}^{[1]}\alpha_2^{[2]} & \cdots & \alpha_{d_1}^{[1]}\alpha_{d_2}^{[2]} \end{bmatrix}.$$

This yields that $\alpha_2^{[1]}\alpha_1^{[2]} = 0$ and $\alpha_1^{[1]}\alpha_1^{[2]} = \alpha_2^{[1]}\alpha_2^{[2]}$. Since $(\alpha_1^{[1]}\alpha_1^{[2]})^2 = (\alpha_1^{[1]}\alpha_1^{[2]})(\alpha_2^{[1]}\alpha_2^{[2]}) = 0$, it turns out that $\langle e_1^{[1]} \otimes e_1^{[2]} | u \rangle = \alpha_1^{[1]}\alpha_1^{[2]} = 0$. That is, u is orthogonal to $e_1^{[1]} \otimes e_1^{[2]}$. However, the vector $e_1^{[1]} \otimes e_1^{[2]} + e_2^{[1]} \otimes e_2^{[2]} \in \mathcal{L}^{[1:2]}$ is not orthogonal to $e_1^{[1]} \otimes e_1^{[2]}$, which implies that $\mathcal{L}^{[1:2]}$ has no product basis.

Next, consider the case $n \geq 3$. We show that the $(\tilde{d}-2)$-dimensional subspace

$$\mathcal{L} = \mathcal{L}^{[1:2]} \otimes \operatorname{span}(u_0^{[3:n]}) + \mathcal{H}(d_1, d_2) \otimes \operatorname{span}(u_0^{[3:n]})^{\perp}$$

has no product basis, where $u_0^{[3:n]} := e_1^{[3]} \otimes \cdots \otimes e_1^{[n]}$. Take an arbitrary product vector $u \in \mathcal{L}$. Then u is expressed as $u = u^{[1:2]} \otimes u_0^{[3:n]} + v^{[1:2]} \otimes v^{[3:n]}$ with suitable vectors $u^{[1:2]} \in \mathcal{L}^{[1:2]}$, $v^{[1:2]} \in \mathcal{H}(d_1, d_2)$ and $v^{[3:n]} \in \mathrm{span}(u_0^{[3:n]})^\perp$. Since u is a product vector, so is $(I^{[1:2]} \otimes \langle u_0^{[3:n]}|)u = u^{[1:2]}$, where $I^{[1:2]}$ denotes the identity matrix on $\mathcal{H}(d_1, d_2)$. As already proved, the product vector $u^{[1:2]} \in \mathcal{L}^{[1:2]}$ is orthogonal to $e_1^{[1]} \otimes e_1^{[2]}$. Thus, u is orthogonal to $e_1^{[1]} \otimes e_1^{[2]} \otimes u_0^{[3:n]}$. However, the vector $(e_1^{[1]} \otimes e_1^{[2]} + e_2^{[1]} \otimes e_2^{[2]}) \otimes u_0^{[3:n]} \in \mathcal{L}$ is not orthogonal to $e_1^{[1]} \otimes e_1^{[2]} \otimes u_0^{[3:n]}$, which implies that $\mathcal{L}$ has no product basis. □

Proof of Theorem 1.1. Proposition 3.1 with $r = 0, 1$ and Proposition 3.4 yield the theorem immediately. □

Remark 3.5. Let us consider the case when the scalar field $\mathbb{C}$ and the Hermitian inner product $\langle v|u\rangle = \sum_i \overline{v(i)}u(i)$ are replaced with an arbitrary field $\mathcal{F}$ and the non-degenerate bilinear form $\langle v, u\rangle = \sum_i v(i)u(i)$, respectively. In this case, the proof of Proposition 3.4 works well. Moreover, if $\mathcal{F}$ is infinite, then the proof of Proposition 3.1 also works well because (i) $\dim \mathcal{L} + \dim \mathcal{L}^\perp = d$ and $(\mathcal{L}^\perp)^\perp = \mathcal{L}$ for every subspace $\mathcal{L}$ of $\mathcal{F}^d$ and (ii) Lemma 3.2 holds. The fact (i) is also true for every finite field $\mathcal{F}$, but (ii) is false for every finite field even if the polynomial $f(x_1, \ldots, x_n)$ is homogeneous. Nevertheless, a modified version of Lemma 3.2 holds for every finite field (see Lemma 3.10).

Finally, we verify that statement S implies statement WS, which follows from the following proposition immediately.

Proposition 3.6. *For a subspace $\mathcal{L}$ of $\mathcal{H}(d_1, \ldots, d_n)$, consider the following conditions:*

1. *the orthogonal projection $P_\mathcal{L}$ onto $\mathcal{L}$ lies in $\mathsf{Sep}(d_1, \ldots, d_n)$;*

2. *$\mathcal{L}$ has a product basis.*

The one direction "1 $\Rightarrow$ 2" holds for all integers $n \geq 2$ and $d_1, \ldots, d_n \geq 2$ and subspaces $\mathcal{L}$, but the converse does not necessarily hold.

Proof. 1 $\Rightarrow$ 2. See [32, Theorem 2] (which is only the case $n = 2$, but the case $n \geq 3$ is also proved in the same way).

2 $\not\Rightarrow$ 1. Let $n \geq 2$ and $d_1, \ldots, d_n \geq 2$ be integers. Choose $\mathcal{L}$ as the subspace spanned by the two vectors $e_1^{[1]} \otimes e_1^{[2]} \otimes u^{[3:n]}$ and $(e_1^{[1]} + e_2^{[1]}) \otimes (e_1^{[2]} + e_2^{[2]}) \otimes u^{[3:n]}$, where $u^{[3:n]}$ be an arbitrary unit product vector in $\mathcal{H}(d_3, \cdots, d_n)$. Then $\mathcal{L}$ has the

product basis composed of $e_1^{[1]} \otimes e_1^{[2]} \otimes u^{[3:n]}$ and $(e_1^{[1]} + e_2^{[1]}) \otimes (e_1^{[2]} + e_2^{[2]}) \otimes u^{[3:n]}$. Also, the orthogonal projection $P_{\mathcal{L}}$ is equal to

$$P_{\mathcal{L}} = (|e_1^{[1]}\rangle\langle e_1^{[1]}| \otimes |e_1^{[2]}\rangle\langle e_1^{[2]}| + |u^{[1:2]}\rangle\langle u^{[1:2]}|) \otimes |u^{[3:n]}\rangle\langle u^{[3:n]}|\,,$$

where $u^{[1:2]}$ is the unit vector $(e_1^{[1]} \otimes e_2^{[2]} + e_2^{[1]} \otimes e_1^{[2]} + e_2^{[1]} \otimes e_2^{[2]})/\sqrt{3}$. Since the matrix $|e_1^{[1]}\rangle\langle e_1^{[1]}| \otimes |e_1^{[2]}\rangle\langle e_1^{[2]}| + |u^{[1:2]}\rangle\langle u^{[1:2]}|$ is not separable (we can use the positive partial transpose criterion), the orthogonal projection $P_{\mathcal{L}}$ is not also separable. □

3.2 Case of finite fields

As already stated in Remark 3.5, Theorem 1.1 holds for every infinite field. In this section, we consider the case of finite fields. Let $\mathcal{F}$ be a finite field of order q, $\langle \cdot, \cdot \rangle$ be the non-degenerate bilinear form $\langle v, u \rangle = \sum_i v(i)u(i)$, $\tilde{d}$ be the dimension $d_1 d_2 \cdots d_n$ of $\mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$, and $(e_i^{[j]})_{i=1}^{d_j}$ be the standard basis of $\mathcal{F}^{d_j}$ for $j = 1, \ldots, n$. We denote by $\mathcal{L}^{\perp}$ the orthogonal compliment of a subspace $\mathcal{L}$ with respect to the non-degenerate bilinear form $\langle \cdot, \cdot \rangle$.

Proposition 3.7. *Let $d_1, d_2 \geq 2$ be integers. Then every $(d_1 d_2 - 1)$-dimensional subspace of $\mathcal{F}^{d_1} \otimes \mathcal{F}^{d_2}$ has a product basis.*

Proof. Let $\mathcal{L}$ be a $(d_1 d_2 - 1)$-dimensional subspace of $\mathcal{F}^{d_1} \otimes \mathcal{F}^{d_2}$. Taking a non-zero $w \in \mathcal{L}^{\perp}$, we have $\mathcal{L} = \{u \in \mathcal{F}^{d_1} \otimes \mathcal{F}^{d_2} : \langle w, u \rangle = 0\}$.

Step 1. Let us consider the case $w = w_r := \sum_{i=1}^{r} e_i^{[1]} \otimes e_i^{[2]}$ with $1 \leq r \leq \min\{d_1, d_2\}$. Set $u_0^{[2]} = \sum_{i=1}^{r} e_i^{[2]}$. In this case, the $d_1 d_2 - 1$ product vectors of $\mathcal{L}$

$$e_i^{[1]} \otimes e_j^{[2]}, \quad (e_k^{[1]} - e_{k+1}^{[1]}) \otimes u_0^{[2]} \quad \big((i,j) \neq (1,1), (2,2), \ldots, (r,r),\ 1 \leq k \leq r-1\big) \tag{3.5}$$

are linearly independent, which is proved as follows. First, it is easily checked that all the vectors (3.5) are orthogonal to w_r, where we note that if $r = 1$, then the vectors (3.5) are only $e_i^{[1]} \otimes e_j^{[2]}$, $(i,j) \neq (1,1)$. Next, suppose that $d_1 d_2 - 1$ scalars $\alpha_{i,j}$ and β_k satisfy

$$\sum_{(i,j) \neq (1,1), (2,2), \ldots, (r,r)} \alpha_{i,j} e_i^{[1]} \otimes e_j^{[2]} + \sum_{k=1}^{r-1} \beta_k (e_k^{[1]} - e_{k+1}^{[1]}) \otimes u_0^{[2]} = 0. \tag{3.6}$$

Taking the inner product of (3.6) and $e_l^{[1]} \otimes e_l^{[2]}$ for $l = 1, \ldots, r$, we obtain that $\beta_1 = 0$ and $\beta_l - \beta_{l-1} = 0$ for all $l = 2, \ldots, r$. Thus, all β_k are zero. Since the vectors

$e_i^{[1]} \otimes e_j^{[2]}$, $(i,j) \neq (1,1),(2,2),\dots,(r,r)$, are linearly independent, all $\alpha_{i,j}$ are also zero. Therefore, the vectors (3.5) are linearly independent, and $\mathcal{L}$ has a product basis.

Step 2. Let us reduce the case of general w to Step 1. For a matrix $A = (\alpha_{i,j}) \in \mathcal{F}^{d_1 \times d_2}$, define the vector $\mathrm{vec}(A) \in \mathcal{F}^{d_1} \otimes \mathcal{F}^{d_2}$ as $\mathrm{vec}(A) = \sum_{i,j} \alpha_{i,j} e_i^{[1]} \otimes e_j^{[2]}$. Then $\mathrm{vec}(PAQ^\top) = (P \otimes Q)\,\mathrm{vec}(A)$ for all matrices $A \in \mathcal{F}^{d_1 \times d_2}$, $P \in \mathcal{F}^{d_1 \times d_1}$ and $Q \in \mathcal{F}^{d_2 \times d_2}$, where $Q^\top$ denotes the transpose of Q. Now, express w as $w = \mathrm{vec}(A)$ with $A \in \mathcal{F}^{d_1 \times d_2}$. For $r = 0, 1, \dots, \min\{d_1, d_2\}$, define the matrix $B_r = (\beta_{i,j}) \in \mathcal{F}^{d_1 \times d_2}$ as $\beta_{i,j} = 1$ if $(i,j) = (1,1),(2,2),\dots,(r,r)$ and $\beta_{i,j} = 0$ otherwise. Since A can be factorized as $A = P^\top B_r Q$ with an integer $r \in [1, \min\{d_1, d_2\}]$ and invertible matrices $P \in \mathcal{F}^{d_1 \times d_1}$ and $Q \in \mathcal{F}^{d_2 \times d_2}$, it follows that

$$w = \mathrm{vec}(A) = (P^\top \otimes Q^\top)\,\mathrm{vec}(B_r) = (P^\top \otimes Q^\top) w_r.$$

Letting $(u_i)_{i=1}^{d_1 d_2 - 1}$ be the product basis (3.5), we find that $((P^{-1} \otimes Q^{-1}) u_i)_{i=1}^{d_1 d_2 - 1}$ is a product basis of $\mathcal{L}$. □

Proposition 3.8. *Let $n \geq 3$ and $d_1, \dots, d_n \geq 2$ be integers. If $q > \max\{d_i : i \neq n_1, n_2\}$ for some n_1 and n_2, then every $(\tilde{d}-1)$-dimensional subspace of $\mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$ has a product basis.*

Since Proposition 3.4 holds for every finite field (see Remark 3.5), we obtain the following theorem.

Theorem 3.9. *Let $n \geq 2$ and $d_1, \dots, d_n \geq 2$ be integers. If either (i) $n = 2$ or (ii) $n \geq 3$ and $q > \max\{d_i : i \neq n_1, n_2\}$ for some n_1 and n_2, then*

$$\max\Bigl\{\dim \mathcal{L} : \begin{array}{l} \mathcal{L} \text{ is a subspace of } \mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n} \text{ and} \\ \text{has no product basis} \end{array}\Bigr\} = \tilde{d} - 2.$$

To prove Proposition 3.8, we use the following lemmas instead of Lemmas 3.2 and 3.3.

Lemma 3.10. *Let $n \geq 1$ be an integer, $f(x_1, \dots, x_n)$ be a polynomial over $\mathcal{F}$, and d_i be the degree of $f(x_1, \dots, x_n)$ in x_i. If $q > \max\{d_1, \dots, d_n\}$, then the following conditions are equivalent:*

1. *$f(\alpha_1, \dots, \alpha_n) = 0$ for all $\alpha_1, \dots, \alpha_n \in \mathcal{F}$;*
2. *$f(x_1, \dots, x_n) = 0$ as a polynomial.*

Proof. See [34, Theorem 2.19] (where only Lemma 3.2 is proved but the proof works well for Lemma 3.10). □

Lemma 3.11. *Let $m \in [1, q-1]$, $n \geq 1$ and $d_1, \dots, d_n \geq 2$ be integers, and let $(u_{k,l})_{l=1}^{\tilde{d}-1}$, $k = 1, \dots, m$, be $(\tilde{d}-1)$-tuples of linearly independent vectors in $\mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$. Then there exists a product vector $v \in \mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$ such that*

$$\det[u_{k,1}, \dots, u_{k,\tilde{d}-1}, v] \neq 0$$

for all $k = 1, \dots, m$.

Proof. This proof is almost the same as the proof of Lemma 3.3. Let $n' = d_1 + \cdots + d_n$. Define the m polynomials $f_k(x_1, \dots, x_{n'})$ over $\mathcal{F}$ as

$$f_k(x_1, \dots, x_{n'}) = \det[u_{k,1}, \dots, u_{k,\tilde{d}-1}, v] \quad (k = 1, \dots, m),$$
$$v = v^{[1]} \otimes \cdots \otimes v^{[n]},$$

where the variables $x_1, \dots, x_{n'}$ correspond to the n' entries of $v^{[j]}$, $1 \leq j \leq n$. Then, for every $k = 1, \dots, m$, the polynomial $f_k(x_1, \dots, x_{n'})$ is not zero as a polynomial. Since the polynomial ring $\mathcal{F}[x_1, \dots, x_{n'}]$ is an integral domain, the product $f(x_1, \dots, x_{n'}) \coloneqq \prod_{k=1}^{m} f_k(x_1, \dots, x_{n'})$ is not also zero as a polynomial. Also, for every $i = 1, \dots, n'$, the degree of the polynomial $f(x_1, \dots, x_{n'})$ in x_i is less than or equal to $m \leq q-1$. Thus, Lemma 3.10 implies that $f(\beta_1, \dots, \beta_{n'}) \neq 0$ for some $\beta_1, \dots, \beta_{n'} \in \mathcal{F}$. Taking the vectors $v^{[j]}$ corresponding to $\beta_1, \dots, \beta_{n'} \in \mathcal{F}$, we obtain a desired product vector v. □

Proof of Proposition 3.8. Without loss of generality, we may assume that $2 \leq d_1 \leq \cdots \leq d_n$ and $q > d_{n-2}$ ($\{n_1, n_2\} = \{n-1, n\}$ in this case). The proposition is proved in the same way as the proof of Proposition 3.1 by using Lemmas 3.10 and 3.11 instead of Lemmas 3.2 and 3.3. □

Chapter 4

Classical-quantum differential privacy

In this chapter, we introduce linear mappings used in quantum information theory, prove Theorems 1.5 and 1.6, and give concrete CQ ε-DP n-tuples that do not lie in $\mathrm{EC}_n(\varepsilon)$.

4.1 Linear mappings in quantum information theory

In this section, we discuss linear mappings from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ which are used in quantum information theory. First, let us begin with several basic terms (see also a textbook in quantum information theory, e.g., [26,27]). For two linear mapping Λ_i, $i = 1, 2$, from $\mathsf{Herm}(d_i)$ into $\mathsf{Herm}(d_i')$, the tensor product $\Lambda_1 \otimes \Lambda_2$ is a linear mapping from $\mathsf{Herm}(d_1) \otimes \mathsf{Herm}(d_2)$ into $\mathsf{Herm}(d_1') \otimes \mathsf{Herm}(d_2')$. Since $\mathsf{Herm}(d_1) \otimes \mathsf{Herm}(d_2)$ can be regarded as $\mathsf{Herm}(d_1 d_2)$ (see Section 2.1), the tensor product $\Lambda_1 \otimes \Lambda_2$ is also a linear mapping from $\mathsf{Herm}(d_1 d_2)$ into $\mathsf{Herm}(d_1' d_2')$. Let id_d be the identity mapping on $\mathsf{Herm}(d)$.

- A linear mapping Λ from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ is called *positive* if $\Lambda(\mathsf{PSD}(d)) \subset \mathsf{PSD}(d')$.
- A linear mapping Λ from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ is called *completely positive* if $\Lambda \otimes \mathrm{id}_k$ is positive for every integer $k \geq 2$.
- A linear mapping Λ from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ is called *trace-preserving* if $\mathrm{Tr}\,\Lambda(X) = \mathrm{Tr}\,X$ for every $X \in \mathsf{Herm}(d)$.

- A linear mapping Λ from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ is called *CPTP* if Λ is completely positive and trace-preserving.

In quantum information theory, a quantum channel is a CPTP map.

Example 4.1 (Entanglement breaking channel)**.** The linear mapping Λ below is a CPTP map called *entanglement breaking channel*. Let $\sigma_1, \dots, \sigma_m$ be density matrices on $\mathbb{C}^{d'}$ and $(M_k)_{k=1}^m$ be a POVM, i.e., $M_1, \dots, M_m \geq 0$ and $\sum_{k=1}^m M_k = I_d$. For example, $(|e_k\rangle\langle e_k|)_{k=1}^d$ is a POVM, where $(e_k)_{k=1}^d$ denotes the standard basis of $\mathbb{C}^d$. Define the linear mapping Λ from $\mathsf{Herm}(d)$ into $\mathsf{Herm}(d')$ as $\Lambda(X) = \sum_{k=1}^m (\operatorname{Tr} M_k X)\sigma_k$. It can easily be checked that Λ is a CPTP map. This fact is used implicitly in this section.

Using an entanglement breaking channel, we prove Proposition 1.7.

Proof of Proposition 1.7. First, assume that $(\rho_i)_{i=1}^n$ lies in $\mathrm{EC}_n(\varepsilon)$, i.e., there exists an ε-DP n-tuple $(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)$ and a CPTP map Λ such that $\rho_i = \Lambda(\mathrm{diag}(p_i))$ for all $i = 1, \dots, n$. Denote by $(e_k)_{k=1}^d$ the standard basis of $\mathbb{C}^d$, where d is the dimension of the vector space that $p_1, \dots, p_n$ inhabit. Then $\rho_i = \sum_{k=1}^d p_i(k)\Lambda(|e_k\rangle\langle e_k|)$ for all $i = 1, \dots, n$. Since all $\Lambda(|e_k\rangle\langle e_k|)$ are density matrices, the n-tuple $(\rho_i)_{i=1}^n$ lies in the right-hand side of (1.7).

Conversely, assume that $(\rho_i)_{i=1}^n$ lies in the right-hand side of (1.7): there exist $(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)$ and density matrices σ_k such that $\rho_i = \sum_{k=1}^d p_i(k)\sigma_k$ for all $i = 1, \dots, n$, where d is the dimension of the vector space that $p_1, \dots, p_n$ inhabit. Define the CPTP map Λ as $\Lambda(X) = \sum_{k=1}^d \langle e_k|X|e_k\rangle\, \sigma_k$. Then $\Lambda(\mathrm{diag}(p_i)) = \rho_i$ for all $i = 1, \dots, n$. Therefore, $(\rho_i)_{i=1}^n$ lies in $\mathrm{EC}_n(\varepsilon)$. □

4.2 Case $n = 2$

In this section, we show the following theorem that is stronger than Theorem 1.5.

Theorem 4.2. *Let $\bar{p}_1$ and $\bar{p}_2$ be the probability vectors defined as*

$$\bar{p}_1 = \Big[\frac{e^\varepsilon}{e^\varepsilon+1}, \frac{1}{e^\varepsilon+1}\Big], \quad \bar{p}_2 = \Big[\frac{1}{e^\varepsilon+1}, \frac{e^\varepsilon}{e^\varepsilon+1}\Big].$$

Then, for every $(\rho_i)_{i=1}^2 \in \mathrm{CQ}_2(\varepsilon)$, there exists a CPTP map Λ such that $\Lambda(\mathrm{diag}(\bar{p}_i)) = \rho_i$ for $i = 1, 2$.

That is, the pair $(\bar{p}_1, \bar{p}_2)$ generates all CQ ε-DP 2-tuples by CPTP maps. The pair $(\bar{p}_1, \bar{p}_2)$ also plays an important role in the classical setting [30,38]. Since $\mathrm{EC}_2(\varepsilon)$ is a subset of $\mathrm{CQ}_2(\varepsilon)$, Theorem 1.5 follows from Theorem 4.2 and Proposition 1.7 immediately.

In general, many researchers in quantum information theory are interested in whether, given $2n$ density matrices $\rho_1, \ldots, \rho_n, \sigma_1, \ldots, \sigma_n$, there exists a CPTP map Λ such that $\Lambda(\rho_i) = \sigma_i$ for all $i = 1, \ldots, n$. In this context, the CPTP map Λ is called a *physical transformation* [9,33]. If the above Λ exists, we write $(\rho_1, \ldots, \rho_n) \to (\sigma_1, \ldots, \sigma_n)$. Then the assertion of Theorem 4.2 can be rewritten as

$$\forall (\rho_i)_{i=1}^2 \in \mathrm{CQ}_2(\varepsilon),\ (\mathrm{diag}(\bar{p}_i))_{i=1}^2 \to (\rho_i)_{i=1}^2.$$

If inputs ρ_1 and ρ_2 are of rank one, it is easy to investigate whether $(\rho_1, \rho_2) \to (\sigma_1, \sigma_2)$, because $(\rho_1, \rho_2) \to (\sigma_1, \sigma_2)$ if and only if $F(\rho_1, \rho_2) \leq F(\sigma_1, \sigma_2)$ [9, 33, 49], where F denotes the *fidelity* defined as $F(\rho, \sigma) = \mathrm{Tr}\left|\rho^{1/2}\sigma^{1/2}\right|$ for density matrices ρ and σ. However, if inputs ρ_1 and ρ_2 are not necessarily of rank one, it is difficult to investigate whether $(\rho_1, \rho_2) \to (\sigma_1, \sigma_2)$ in general. Since both the inputs in Theorem 4.2 are of rank two, Theorem 4.2 is never trivial.

Now, we show the following preliminary lemma before proving Theorem 4.2.

Lemma 4.3. *If density matrices ρ_1 and ρ_2 are orthogonal to each other, i.e., $\mathrm{Tr}\,\rho_1\rho_2 = 0$, then for all density matrices σ_1 and σ_2 there exists a CPTP map Λ such that $\Lambda(\rho_1) = \sigma_1$ and $\Lambda(\rho_2) = \sigma_2$.*

Proof. Take the orthogonal projection P_1 onto the support of ρ_1. Put $P_2 = I_d - P_1$. Defining $\Lambda(X) = (\mathrm{Tr}\,XP_1)\sigma_1 + (\mathrm{Tr}\,XP_2)\sigma_2$ for $X \in \mathsf{Herm}(d)$, we find that Λ is a CPTP map satisfying that $\Lambda(\rho_1) = \sigma_1$ and $\Lambda(\rho_2) = \sigma_2$. □

Proof of Theorem 4.2. Let $(\rho_i)_{i=1}^2$ be a CQ ε-DP 2-tuple. Since $e^\varepsilon\rho_1 - \rho_2$ and $e^\varepsilon\rho_2 - \rho_1$ are positive semi-definite, they are expressed as

$$e^\varepsilon\rho_1 - \rho_2 = (e^\varepsilon - 1)\sigma_1, \quad e^\varepsilon\rho_2 - \rho_1 = (e^\varepsilon - 1)\sigma_2,$$

where σ_1 and σ_2 are density matrices. Lemma 4.3 implies that there exists a CPTP map Λ such that $\Lambda(|e_1\rangle\langle e_1|) = \sigma_1$ and $\Lambda(|e_2\rangle\langle e_2|) = \sigma_2$. Thus,

$$\begin{aligned}
e^\varepsilon\,\mathrm{diag}(\bar{p}_1) - \mathrm{diag}(\bar{p}_2) &= (e^\varepsilon - 1)\,|e_1\rangle\langle e_1|\,, \\
e^\varepsilon\,\mathrm{diag}(\bar{p}_2) - \mathrm{diag}(\bar{p}_1) &= (e^\varepsilon - 1)\,|e_2\rangle\langle e_2|\,, \\
e^\varepsilon\Lambda(\mathrm{diag}(\bar{p}_1)) - \Lambda(\mathrm{diag}(\bar{p}_1)) &= (e^\varepsilon - 1)\Lambda(|e_1\rangle\langle e_1|) = (e^\varepsilon - 1)\sigma_1 = e^\varepsilon\rho_1 - \rho_2, \quad (4.1) \\
e^\varepsilon\Lambda(\mathrm{diag}(\bar{p}_2)) - \Lambda(\mathrm{diag}(\bar{p}_1)) &= (e^\varepsilon - 1)\Lambda(|e_2\rangle\langle e_2|) = (e^\varepsilon - 1)\sigma_2 = e^\varepsilon\rho_2 - \rho_1. \quad (4.2)
\end{aligned}$$

Solving the simultaneous equations (4.1) and (4.2), we obtain $\Lambda(\mathrm{diag}(\bar{p}_i)) = \rho_i$ for all $i = 0, 1$. □

4.3 Case $n \geq 3$: Main idea and result

We describe the main idea and result in the case $n \geq 3$. A key point to distinguish elements in $\mathrm{EC}_n(\varepsilon)$ and $\mathrm{CQ}_n(\varepsilon)$ is monotonicity for CPTP maps (see Definition 1.3). Let Φ be a real-valued function of n density matrices satisfying monotonicity for CPTP maps. As stated in Section 1.2, the equality $S_n^{\mathrm{EC}}(\varepsilon;\Phi) = S_n^{\mathrm{C}}(\varepsilon;\Phi)$ holds. This fact gives us an idea to distinguish elements in $\mathrm{EC}_n(\varepsilon)$ and $\mathrm{CQ}_n(\varepsilon)$: if $\Phi(\rho_1,\dots,\rho_n)$ with $(\rho_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)$ is greater than $S_n^{\mathrm{C}}(\varepsilon;\Phi)$, then $(\rho_i)_{i=1}^n$ does not lie in $\mathrm{EC}_n(\varepsilon)$. To use this criterion, we must solve optimization problem (1.6). Fortunately, for special Φ, optimization problem (1.6) can be reduced to a linear program [38, Theorem 4], which is stated in Section 4.4.

Before stating our main result, we define the RLD Fisher information of a one-parameter family, which satisfies monotonicity for CPTP maps.

Definition 4.4 (RLD Fisher information [26, p. 260])**.** *For density matrices ρ and σ with full rank, we denote the RLD Fisher information of the one-parameter family $((1-\theta)\rho+\theta\sigma)_{\theta\in[0,1]}$ at the point θ as*

$$J_\theta(\rho,\sigma) = \mathrm{Tr}(\sigma-\rho)^2((1-\theta)\rho+\theta\sigma)^{-1}.$$

For probability vectors p and q, we set $J_\theta(p,q) = J_\theta(\mathrm{diag}(p),\mathrm{diag}(q))$.

If $(\rho_i)_{i=1}^n$ is CQ ε-DP, we may assume that all ρ_i have full rank (see Section 1.2), and hence, we can consider the value $J_\theta(\rho_i,\rho_j)$ for all $i,j=1,\dots,n$. Also, for probability vectors p and q, the value $J_\theta(p,q)$ is the Fisher information in the classical sense. From now on, we denote by $\mathrm{avg}_{i\neq j}\,\alpha_{i,j}$ the arithmetic mean of real numbers $\alpha_{i,j}$, $i\neq j$. Now, our main result is as follows.

Theorem 4.5. *For real numbers $\theta\in[0,1]$ and $\varepsilon>0$ and an integer $n\geq 2$, we define the suprema $M_n^{\mathrm{C}}(\varepsilon;J_\theta)$, $M_n^{\mathrm{EC}}(\varepsilon;J_\theta)$ and $M_n^{\mathrm{CQ}}(\varepsilon;J_\theta)$ as*

$$\begin{aligned} M_n^{\mathrm{C}}(\varepsilon;J_\theta) &= \sup_{(p_i)_{i=1}^n\in \mathrm{C}_n(\varepsilon)} \min_{i\neq j} J_\theta(p_i,p_j),\\ M_n^{\mathrm{X}}(\varepsilon;J_\theta) &= \sup_{(\rho_i)_{i=1}^n\in \mathrm{X}_n(\varepsilon)} \min_{i\neq j} J_\theta(\rho_i,\rho_j) \quad (\mathrm{X}=\mathrm{EC},\mathrm{CQ}). \end{aligned}$$

Then, for all $\theta\in[0,1]$, $\varepsilon>0$ and $n\geq 2$, we have $M_n^{\mathrm{CQ}}(\varepsilon;J_\theta) = M_2^{\mathrm{C}}(\varepsilon;J_\theta)$ and

$$\begin{aligned} M_n^{\mathrm{EC}}(\varepsilon;J_\theta) = M_n^{\mathrm{C}}(\varepsilon;J_\theta) &= \sup_{(p_i)_{i=1}^n\in \mathrm{C}_n(\varepsilon)} \mathrm{avg}_{i\neq j} J_\theta(p_i,p_j)\\ &= \frac{f_\theta(e^\varepsilon,1)+f_\theta(1,e^\varepsilon)}{n-1} \max_{1\leq k\leq n/2} \frac{k(n-k)}{ke^\varepsilon+n-k}, \end{aligned}$$

where $f_\theta(\alpha,\beta) \coloneqq (\alpha-\beta)^2/((1-\theta)\alpha+\theta\beta)$ *for* $\alpha,\beta>0$. *Moreover,* $M_n^{\mathrm{EC}}(\varepsilon;J_\theta) < M_n^{\mathrm{CQ}}(\varepsilon;J_\theta)$ *for all* $\theta\in[0,1]$, $\varepsilon>0$ *and* $n\geq 3$.

Theorem 4.5 implies Theorem 1.6 and the following corollary immediately.

Corollary 4.6. *Let* $\varepsilon>0$ *be a real number and* $n\geq 3$ *be an integer. If* $(\rho_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)$ *satisfies that* $M_n^{\mathrm{C}}(\varepsilon;J_\theta) < \mathrm{avg}_{i\neq j} J_\theta(\rho_i,\rho_j)$ *for some* $\theta\in[0,1]$, *then* $(\rho_i)_{i=1}^n$ *does not lie in* $\mathrm{EC}_n(\varepsilon)$.

4.4 Case $n\geq 3$: Proof

First, we begin with the classical optimization, for which we need the following definition and lemma [38, Theorem 4].

Definition 4.7 (Sublinear function)**.** *We say that a function* $\phi\colon (0,\infty)^n\to\mathbb{R}$ *is sublinear if* $\phi(x+y)\leq\phi(x)+\phi(y)$ *and* $\phi(\alpha x)=\alpha\phi(x)$ *for all* $x,y\in(0,\infty)^n$ *and* $\alpha>0$.

Lemma 4.8. *Let* Φ_{C} *be a real-valued function of* n *probability vectors with the following condition: there exists a sublinear function* $\phi\colon(0,\infty)^n\to\mathbb{R}$ *such that*

$$\Phi_{\mathrm{C}}(p_1,\dots,p_n)=\sum_{p_1(k),\dots,p_n(k)>0}\phi(p_1(k),\dots,p_n(k)), \tag{4.3}$$

where the above sum is taken all over k *with* $p_1(k),\dots,p_n(k)>0$. *Then, for all* $\varepsilon>0$ *and* $n\geq 2$,

$$\begin{aligned}&\sup_{(p_i)_{i=1}^n\in\mathrm{C}_n(\varepsilon)}\Phi_{\mathrm{C}}(p_1,\dots,p_n)\\ &=\max\Bigg\{\sum_{v\in\mathcal{S}_n(\varepsilon)}\phi(v(1),\dots,v(n))\alpha_v:\ \begin{array}{l}\sum_{v\in\mathcal{S}_n(\varepsilon)}\alpha_v v=\mathbf{1}_n,\\ \forall v\in\mathcal{S}_n(\varepsilon),\ \alpha_v\geq 0\end{array}\Bigg\},\end{aligned}$$

where $\mathcal{S}_n(\varepsilon)\coloneqq\{1,e^\varepsilon\}^n$ *and* $\mathbf{1}_n\coloneqq[1,\dots,1]^\top\in\mathbb{R}^n$.

Many information-theoretic quantities can be expressed as (4.3). Such examples are relative entropy, Fisher information, total variation distance. Especially, $J_\theta(p,q)$ is expressed as

$$J_\theta(p,q)=\sum_{p(k),q(k)>0}f_\theta(p(k),q(k)),$$

where the above sum is taken all over k with $p(k),q(k)>0$, and the function f_θ defined in Theorem 4.5 is sublinear. We now prove the following lemma by using Lemma 4.8.

Lemma 4.9. *Let $\psi\colon (0,\infty)^2 \to \mathbb{R}$ be a sublinear function with $\psi(1,1) = 0$, and Ψ be the function $\Psi(p,q) = \sum_{p(k),q(k)>0} \psi(p(k),q(k))$ of two probability vectors. Then, for all $\varepsilon > 0$ and $n \geq 2$,*

$$\begin{aligned} M_n^{\mathrm{C}}(\varepsilon;\Psi) &\coloneqq \sup_{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)} \min_{i\neq j} \Psi(p_i,p_j) = \sup_{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)} \operatorname*{avg}_{i\neq j} \Psi(p_i,p_j) \\ &= \frac{\psi(e^\varepsilon,1)+\psi(1,e^\varepsilon)}{n-1} \max_{1\leq k\leq n/2} \frac{k(n-k)}{ke^\varepsilon + n - k}. \end{aligned}$$

Proof. Let $\varepsilon > 0$ be a real number and $n \geq 2$ be an integer. The following inequality holds:

$$M_n^{\mathrm{C}}(\varepsilon;\Psi) \leq \sup_{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)} \operatorname*{avg}_{i\neq j} \Psi(p_i,p_j). \tag{4.4}$$

Recall the definition $\mathcal{S}_n(\varepsilon) = \{1, e^\varepsilon\}^n$. Set $\Phi_{\mathrm{C}}(p_1,\dots,p_n) = \sum_{i\neq j} \Psi(p_i,p_j)$ and $\phi(x) = \sum_{i\neq j} \psi(x(i),x(j))$ for $x \in (0,\infty)^n$. Lemma 4.8 yields that

$$\begin{aligned} &\sup_{(p_i)_{i=1}^n \in \mathrm{C}_n(\varepsilon)} \sum_{i\neq j} \Psi(p_i,p_j) \\ &= \max\left\{ \sum_{v\in\mathcal{S}_n(\varepsilon)} \sum_{i\neq j} \psi(v(i),v(j))\alpha_v : \begin{array}{l} \sum_{v\in\mathcal{S}_n(\varepsilon)} \alpha_v v = \mathbf{1}_n, \\ \forall v \in \mathcal{S}_n(\varepsilon),\ \alpha_v \geq 0 \end{array} \right\}. \end{aligned} \tag{4.5}$$

Consider the partition of $\mathcal{S}_n(\varepsilon)$ into the $n+1$ subsets

$$\mathcal{S}_{n,k}(\varepsilon) \coloneqq \{v \in \mathcal{S}_n(\varepsilon) : \text{the number of } i \text{ with } v(i) = e^\varepsilon \text{ is } k\} \quad (k = 0,1,\dots,n).$$

If $v \in \mathcal{S}_{n,k}(\varepsilon)$, then $\sum_{i\neq j} \psi(v(i),v(j)) = \big(\psi(e^\varepsilon,1)+\psi(1,e^\varepsilon)\big)k(n-k)$ due to the assumption $\psi(1,1) = 0$. Thus, for every $k = 0,1,\dots,n$, we have

$$\begin{aligned} \sum_{v\in\mathcal{S}_n(\varepsilon)} \sum_{i\neq j} \psi(v(i),v(j))\alpha_v &= \sum_{k=0}^n \sum_{v\in\mathcal{S}_{n,k}(\varepsilon)} \sum_{i\neq j} \psi(v(i),v(j))\alpha_v \\ &= \sum_{k=0}^n \big(\psi(e^\varepsilon,1)+\psi(1,e^\varepsilon)\big)k(n-k)\beta_k, \end{aligned}$$

where $\beta_k = \sum_{v\in\mathcal{S}_{n,k}(\varepsilon)} \alpha_v$. Since the equality $\sum_{v\in\mathcal{S}_n(\varepsilon)} \alpha_v v = \mathbf{1}_n$ yields

$$\sum_{k=0}^n (ke^\varepsilon + n - k)\beta_k = \sum_{v\in\mathcal{S}_n(\varepsilon)} \alpha_v \langle \mathbf{1}_n | v \rangle = \langle \mathbf{1}_n | \mathbf{1}_n \rangle = n,$$

the right-hand side in (4.5) is bounded above by

$$\begin{aligned}
&\max\left\{\sum_{k=0}^{n}\bigl(\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})\bigr)k(n-k)\beta_k : \begin{array}{c}\sum_{k=0}^{n}(ke^{\varepsilon}+n-k)\beta_k=n,\\ \beta_0,\dots,\beta_n\ge 0\end{array}\right\}\\
&=\bigl(\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})\bigr)n\max_{0\le k\le n}\frac{k(n-k)}{ke^{\varepsilon}+n-k}\\
&=\bigl(\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})\bigr)n\max_{1\le k\le n/2}\frac{k(n-k)}{ke^{\varepsilon}+n-k}. \qquad (4.6)
\end{aligned}$$

From (4.4), (4.5) and (4.6), it follows that

$$M_n^{\mathrm{C}}(\varepsilon;\Psi)\le\sup_{(p_i)_{i=1}^n\in\mathrm{C}_n(\varepsilon)}\operatorname*{avg}_{i\ne j}\Psi(p_i,p_j)\le\frac{\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})}{n-1}\max_{1\le k\le n/2}\frac{k(n-k)}{ke^{\varepsilon}+n-k}. \qquad (4.7)$$

Fix an arbitrary integer $1\le k\le n/2$. Let d be the number of elements in $\mathcal{S}_{n,k}(\varepsilon)$, i.e., $d=\binom{n}{k}$. Then the vector space $\mathbb{R}^{\mathcal{S}_{n,k}(\varepsilon)}$ is isomorphic to $\mathbb{R}^d$. Define the probability vectors $p_1,\dots,p_n\in\mathbb{R}^{\mathcal{S}_{n,k}(\varepsilon)}$ as

$$p_i(v)=\frac{v(i)}{\binom{n-1}{k-1}e^{\varepsilon}+\binom{n-1}{k}}\quad(v\in\mathcal{S}_{n,k}(\varepsilon);\ i=1,\dots,n).$$

Then $(p_i)_{i=1}^n$ is ε-DP, and moreover,

$$\begin{aligned}
&\min_{i\ne j}\Psi(p_i,p_j)=\min_{i\ne j}\frac{1}{\binom{n-1}{k-1}e^{\varepsilon}+\binom{n-1}{k}}\sum_{v\in\mathcal{S}_{n,k}(\varepsilon)}\psi(v(i),v(j))\\
&=\frac{1}{\binom{n-1}{k-1}e^{\varepsilon}+\binom{n-1}{k}}\cdot\bigl(\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})\bigr)\binom{n-2}{k-1}\\
&=\frac{\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})}{((n-1)/(n-k))e^{\varepsilon}+(n-1)/k}=\frac{\psi(e^{\varepsilon},1)+\psi(1,e^{\varepsilon})}{n-1}\cdot\frac{k(n-k)}{ke^{\varepsilon}+n-k}.
\end{aligned}$$

Since $1\le k\le n/2$ is arbitrary, the inequalities in (4.7) turn to equality. □

Next, we consider the quantum optimization, for which we need the following lemmas.

Lemma 4.10. *Let $n\ge 2$ be an integer and $c\in[0,1]$ be a real number. There exists an n-tuple $(u_i)_{i=1}^n$ of unit vectors in $\mathbb{R}^n$ such that $\langle u_i|u_j\rangle=c$ for all $i\ne j$.*

Proof. Since the matrix $A=(1-c)I_n+c\,|\mathbf{1}_n\rangle\langle\mathbf{1}_n|$ is positive semi-definite, there exists a real square matrix B of order n such that $A=B^{\top}B$. The column vectors $u_1,\dots,u_n\in\mathbb{R}^n$ of B satisfy that $\langle u_i|u_j\rangle=1$ if $i=j$ and $\langle u_i|u_j\rangle=c$ if $i\ne j$. □

Lemma 4.11. *Let $c \in [0,1)$ and $\varepsilon, t > 0$ be real numbers, $(u_i)_{i=1}^n$ be the n-tuple in Lemma 4.10, and $\rho_1, \dots, \rho_n$ be the density matrices defined as*

$$\rho_i = \frac{1}{n+t}(I_n + t\,|u_i\rangle\langle u_i|) \quad (i = 1, \dots, n),$$

where I_n denotes the identity matrix of order n. If $D = (e^\varepsilon - 1)^2 + 4(1-c^2)e^\varepsilon$ and

$$0 < t \le t_{\max} \coloneqq \frac{2(e^\varepsilon - 1)}{\sqrt{D} + 1 - e^\varepsilon},$$

then $(\rho_i)_{i=1}^n$ is CQ ε-DP.

Proof. Let $i \neq j$. We show that

$$|u_i\rangle\langle u_i| - e^\varepsilon\,|u_j\rangle\langle u_j| \le \frac{1 - e^\varepsilon + \sqrt{D}}{2} I_n. \tag{4.8}$$

Take an orthonormal system $(e_i)_{i=1}^2$ of $\mathbb{C}^n$ such that $u_i = e_1$, $u_j = \alpha e_1 + \beta e_2$, $\alpha = c$ and $\beta = \sqrt{1-\alpha^2}$. Then the matrix $|u_i\rangle\langle u_i| - e^\varepsilon\,|u_j\rangle\langle u_j|$ can be expressed as a square matrix of order 2:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - e^\varepsilon \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix} = \begin{bmatrix} 1 - e^\varepsilon\alpha^2 & -e^\varepsilon\alpha\beta \\ -e^\varepsilon\alpha\beta & -e^\varepsilon\beta^2 \end{bmatrix} =: A. \tag{4.9}$$

Since $\operatorname{Tr} A = 1 - e^\varepsilon$, $\det A = -e^\varepsilon\beta^2$ and $D = (\operatorname{Tr} A)^2 - 4\det A$, the greatest eigenvalue of A is equal to $(1 - e^\varepsilon + \sqrt{D})/2$. Therefore, inequality (4.8) holds. Consequently, we obtain

$$t(|u_i\rangle\langle u_i| - e^\varepsilon\,|u_j\rangle\langle u_j|) \le t_{\max}\frac{1 - e^\varepsilon + \sqrt{D}}{2} I_n = (e^\varepsilon - 1) I_n$$

for all $0 < t \le t_{\max}$. This implies $\rho_i \le e^\varepsilon \rho_j$. □

Recalling the definition of $M_n^{\mathrm{X}}(\varepsilon; J_\theta)$, we have the monotonicity

$$M_2^{\mathrm{X}}(\varepsilon; J_\theta) \ge M_3^{\mathrm{X}}(\varepsilon; J_\theta) \ge \cdots$$

for $\mathrm{X} = \mathrm{C}, \mathrm{EC}, \mathrm{CQ}$. This monotonicity is used below.

Lemma 4.12. *For all $\theta \in [0,1]$, $\varepsilon > 0$ and $n \ge 2$, $M_n^{\mathrm{CQ}}(\varepsilon; J_\theta) = M_2^{\mathrm{C}}(\varepsilon; J_\theta)$.*

Proof. Let $\theta \in [0,1]$, $c \in [0,1)$ and $\varepsilon, t > 0$ be real numbers, and $n \geq 2$ be an integer. Take a CQ ε-DP tuple $(\rho_i)_{i=1}^n$ in Lemma 4.11, i.e.,

$$\rho_i = \frac{1}{n+t}(I_n + t\,|u_i\rangle\langle u_i|), \quad u_i \in \mathbb{R}^n \quad (i = 1, \dots, n),$$

and $\langle u_i | u_j \rangle = c$ for all $i \neq j$. Fix $i \neq j$ arbitrarily. The matrix $|u_i\rangle\langle u_i| - |u_j\rangle\langle u_j|$ can be expressed as a square matrix of order 2 in the same way as (4.9):

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix} = \begin{bmatrix} \beta^2 & -\alpha\beta \\ -\alpha\beta & -\beta^2 \end{bmatrix} = -\beta \begin{bmatrix} -\beta & \alpha \\ \alpha & \beta \end{bmatrix},$$

where $\alpha = c$ and $\beta = \sqrt{1-\alpha^2}$. Moreover, $(|u_i\rangle\langle u_i| - |u_j\rangle\langle u_j|)^2$ is expressed as

$$\beta^2 \begin{bmatrix} -\beta & \alpha \\ \alpha & \beta \end{bmatrix}^2 = \beta^2 I_2.$$

Denote by λ_1 and λ_2 two eigenvalues of the matrix

$$A \coloneqq I_2 + t\Big((1-\theta)\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \theta \begin{bmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{bmatrix}\Big) = \begin{bmatrix} 1 + t(1-\theta\beta^2) & t\theta\alpha\beta \\ t\theta\alpha\beta & 1 + t\theta\beta^2 \end{bmatrix}.$$

It follows that

$$\begin{aligned} J_\theta(\rho_i, \rho_j) &= \frac{t^2}{n+t} \operatorname{Tr}(|u_i\rangle\langle u_i| - |u_j\rangle\langle u_j|)^2 \Big(I_n + t\big((1-\theta)\,|u_i\rangle\langle u_i| + \theta\,|u_j\rangle\langle u_j|\big)\Big)^{-1} \\ &= \frac{t^2}{n+t}\beta^2 \operatorname{Tr} A^{-1} = \frac{t^2}{n+t}\beta^2(1/\lambda_1 + 1/\lambda_2) = \frac{t^2}{n+t}\beta^2\frac{\lambda_1+\lambda_2}{\lambda_1\lambda_2} = \frac{t^2}{n+t}\beta^2\frac{\operatorname{Tr} A}{\det A}. \end{aligned}$$

Since $\operatorname{Tr} A = 2 + t$ and

$$\begin{aligned} \det A &= \big(1 + t(1-\theta\beta^2)\big)(1 + t\theta\beta^2) - (t\theta\alpha\beta)^2 \\ &= 1 + t + t^2(1-\theta\beta^2)\theta\beta^2 - (t\theta\beta)^2\alpha^2 \\ &= 1 + t + t^2\theta\beta^2 - (t\theta\beta)^2 = 1 + t + t^2\theta(1-\theta)\beta^2 \\ &= 1 + t + t^2\theta(1-\theta)(1-c^2), \end{aligned}$$

we have

$$J_\theta(\rho_i, \rho_j) = \frac{t^2}{n+t}\beta^2\frac{\operatorname{Tr} A}{\det A} = \frac{t^2}{n+t} \cdot (1-c^2) \cdot \frac{2+t}{1 + t + t^2\theta(1-\theta)(1-c^2)}. \tag{4.10}$$

Finally, putting $t = t_{\max}$, we take the limit $c \to 1-0$. Set $s = e^{\varepsilon} - 1 > 0$. Then $D = s^2 + 4(1-c^2)e^{\varepsilon}$ and

$$t_{\max} = \frac{2s}{\sqrt{D} - s} = \frac{2s(\sqrt{D} + s)}{D - s^2} = \frac{s(\sqrt{D} + s)}{2(1-c^2)e^{\varepsilon}}.$$

Thus, the positive number $t = t_{\max}$ diverges to $+\infty$ as $c \to 1-0$, and moreover,

$$\lim_{c \to 1-0} \frac{t}{n+t} = 1, \quad \lim_{c \to 1-0} (1-c^2)t = \frac{s^2}{e^{\varepsilon}},$$
$$\lim_{c \to 1-0} \frac{2+t}{1+t+t^2\theta(1-\theta)(1-c^2)} = \lim_{c \to 1-0} \frac{t}{t+t^2\theta(1-\theta)(1-c^2)}$$
$$= \lim_{c \to 1-0} \frac{1}{1+t\theta(1-\theta)(1-c^2)} = \frac{1}{1+\theta(1-\theta)s^2/e^{\varepsilon}} = \frac{e^{\varepsilon}}{e^{\varepsilon}+\theta(1-\theta)s^2}.$$

Since Theorem 1.5 and Lemma 4.9 yield that

$$M_2^{\mathrm{CQ}}(\varepsilon; J_\theta) = M_2^{\mathrm{C}}(\varepsilon; J_\theta) = \frac{f_\theta(e^{\varepsilon}, 1) + f_\theta(1, e^{\varepsilon})}{e^{\varepsilon}+1}$$
$$= \frac{1}{e^{\varepsilon}+1} \cdot \frac{(e^{\varepsilon}-1)^2(e^{\varepsilon}+1)}{((1-\theta)e^{\varepsilon}+\theta)(\theta e^{\varepsilon}+1-\theta)} = \frac{s^2}{((1-\theta)s+1)(\theta s+1)},$$

it turns out that

$$M_2^{\mathrm{C}}(\varepsilon; J_\theta) = M_2^{\mathrm{CQ}}(\varepsilon; J_\theta) \geq M_n^{\mathrm{CQ}}(\varepsilon; J_\theta) \geq \lim_{c \to 1-0} J(\rho_1, \rho_2)$$
$$= \lim_{c \to 1-0} \frac{t^2}{n+t} \cdot (1-c^2) \cdot \frac{2+t}{1+t+t^2\theta(1-\theta)(1-c^2)}$$
$$= \frac{s^2}{e^{\varepsilon}} \cdot \frac{e^{\varepsilon}}{e^{\varepsilon}+\theta(1-\theta)s^2} = \frac{s^2}{e^{\varepsilon}+\theta(1-\theta)s^2} = \frac{s^2}{((1-\theta)s+1)(\theta s+1)}$$
$$= M_2^{\mathrm{C}}(\varepsilon; J_\theta).$$

□

Proof of Theorem 4.5. The former assertion follows from Lemmas 4.9 and 4.12 immediately. Let us show the latter assertion. Let $\theta \in [0,1]$ and $\varepsilon > 0$ be real numbers, and $n \geq 3$ be an integer. Since Lemmas 4.9 and 4.12 imply that

$$M_n^{\mathrm{C}}(\varepsilon; J_\theta) \leq M_3^{\mathrm{C}}(\varepsilon; J_\theta) = \frac{f_\theta(e^{\varepsilon}, 1) + f_\theta(1, e^{\varepsilon})}{2} \cdot \frac{2}{e^{\varepsilon}+2}$$
$$= \frac{e^{\varepsilon}+1}{e^{\varepsilon}+2} M_2^{\mathrm{C}}(\varepsilon; J_\theta) < M_2^{\mathrm{C}}(\varepsilon; J_\theta) = M_n^{\mathrm{CQ}}(\varepsilon; J_\theta),$$

we obtain the latter assertion. □

4.5 Concrete CQ ε-DP n-tuples that do not lie in $\mathrm{EC}_n(\varepsilon)$

We construct CQ ε-DP n-tuples that do not lie in $\mathrm{EC}_n(\varepsilon)$. In this section, we use the following lemmas instead of Lemmas 4.10 and 4.11.

Lemma 4.13. *Let $d \geq 2$ be an integer and $c \in [1/d, 1]$ be a real number. There exists a $(d+1)$-tuple $(u_i)_{i=1}^{d+1}$ of unit vectors in $\mathbb{C}^d$ such that $|\langle u_i|u_j\rangle| = c$ for all $i \neq j$.*

Proof. For $z \in \mathbb{C}$, define the Hermitian matrix $A(z) = (\alpha_{i,j})$ of order $d+1$ as $\alpha_{i,j} = 1$ if $i = j$ and $\alpha_{i,j} = z$ if $i < j$. Denote by $\operatorname{eig} A(z)$ the set of all eigenvalues of $A(z)$. Then $\operatorname{eig} A(c) = \{1+dc, 1-c\}$, $\operatorname{eig} A(-c) = \{1-dc, 1+c\}$, $\min\operatorname{eig} A(c) = 1-c \geq 0$ and $\min\operatorname{eig} A(-c) = 1-dc \leq 0$. Since the minimum eigenvalue of $A(z)$ can be expressed as

$$\min\operatorname{eig} A(z) = \min_{\|u\|=1} \langle u|A(z)|u\rangle\,,$$

it follows that

$$|\min\operatorname{eig} A(z) - \min\operatorname{eig} A(z')| \leq \|A(z) - A(z')\|.$$

for all $z, z' \in \mathbb{C}$, which shows that $\min\operatorname{eig} A(z)$ is continuous in z. Thus, the intermediate value theorem implies that $\min\operatorname{eig} A(z_0) = 0$ for some $z_0 \in \mathbb{C}$ of magnitude c. Therefore, there exists a $d \times (d+1)$ complex matrix B such that $A(z_0) = B^*B$. The column vectors $u_1, \ldots, u_{d+1} \in \mathbb{C}^d$ of B satisfy that $\langle u_i|u_j\rangle = 1$ if $i = j$ and $\langle u_i|u_j\rangle = z_0$ if $i < j$. □

Lemma 4.14. *Let $c \in [1/d, 1)$ and $\varepsilon, t > 0$ be real numbers, $(u_i)_{i=1}^{d+1}$ be the $(d+1)$-tuple in Lemma 4.13, and $\rho_1, \ldots, \rho_{d+1}$ be the density matrices defined as*

$$\rho_i = \frac{1}{d+t}(I_d + t\,|u_i\rangle\langle u_i|) \quad (i = 1, \ldots, d+1).$$

If $D = (e^\varepsilon - 1)^2 + 4(1-c^2)e^\varepsilon$ and

$$0 < t \leq t_{\max} := \frac{2(e^\varepsilon - 1)}{\sqrt{D} + 1 - e^\varepsilon},$$

then $(\rho_i)_{i=1}^{d+1}$ is CQ ε-DP.

Proof. See the proof of Lemma 4.11. □

Theorem 4.15. *Let $(\rho_i)_{i=1}^3$ be a CQ ε-DP 3-tuple in Lemma 4.14 with $d = 2$ and $t = t_{\max}$. Then $(\rho_i)_{i=1}^3$ does not lie in $\mathrm{EC}_3(\varepsilon)$.*

Proof. Set $s = e^\varepsilon - 1 > 0$. Then $D = s^2 + 4(1-c^2)(s+1)$ and $t = t_{\max} = 2s/(\sqrt{D} - s)$. Let $i \neq j$. We show that $M_3(\varepsilon; J_{1/2}) < J_{1/2}(\rho_i, \rho_j)$. First, Lemma 4.9 and the equality

$$f_{1/2}(e^\varepsilon, 1) + f_{1/2}(1, e^\varepsilon) = \frac{4(e^\varepsilon - 1)^2}{e^\varepsilon + 1}$$

imply that

$$M_3(\varepsilon; J_{1/2}) = \frac{4(e^\varepsilon - 1)^2}{2(e^\varepsilon + 1)} \cdot \frac{2}{e^\varepsilon + 2} = \frac{4s^2}{(s+2)(s+3)}.$$

Also, it follows form the same calculation as (4.10) that

$$J_{1/2}(\rho_i, \rho_j) = \frac{t^2}{2+t} \cdot (1 - c^2) \cdot \frac{2+t}{1 + t + (t/2)^2(1-c^2)} = \frac{(1-c^2)t^2}{1 + t + (t/2)^2(1-c^2)},$$

where we must replace n in (4.10) with the dimension $d = 2$. Thus,

$$\begin{aligned}
&M_3(\varepsilon; J_{1/2}) < J_{1/2}(\rho_i, \rho_j) \iff \frac{4s^2}{(s+2)(s+3)} < \frac{(1-c^2)t^2}{1 + t + (t/2)^2(1-c^2)} \\
&\iff \frac{(s+2)(s+3)}{s^2} > \frac{4}{1-c^2} \cdot \frac{1 + t + (t/2)^2(1-c^2)}{t^2} \\
&\iff 1 + \frac{5s+6}{s^2} > \frac{4}{1-c^2}\Big(\frac{1+t}{t^2} + \frac{1-c^2}{4}\Big) \iff \frac{5s+6}{s^2} > \frac{4}{1-c^2} \cdot \frac{1+t}{t^2}.
\end{aligned}$$

Recalling that $D = s^2 + 4(1-c^2)(s+1)$ and $t = t_{\max} = 2s/(\sqrt{D} - s)$, we have

$$\begin{aligned}
\frac{t^2}{1+t} &= t - 1 + \frac{1}{1+t} = \frac{2s}{\sqrt{D} - s} - 1 + \frac{\sqrt{D} - s}{\sqrt{D} + s} = \frac{2s}{\sqrt{D} - s} + \frac{-2s}{\sqrt{D} + s} \\
&= \frac{4s^2}{D - s^2} = \frac{s^2}{(1-c^2)(s+1)}.
\end{aligned}$$

Therefore,

$$M_3(\varepsilon; J_{1/2}) < J_{1/2}(\rho_i, \rho_j) \iff \frac{5s+6}{s^2} > \frac{4(s+1)}{s^2}.$$

Since the right inequality always holds, so does the left inequality. From Corollary 4.6, it follows that $(\rho_i)_{i=1}^3$ does not lie in $\mathrm{EC}_3(\varepsilon)$. □

Corollary 4.16. *Let $n \geq 3$ be an integer, and $(\rho_i)_{i=1}^3$ be a CQ ε-DP 3-tuple in Lemma 4.14 with $d = 2$ and $t = t_{\max}$. Then every $(\sigma_i)_{i=1}^n \in \mathrm{CQ}_n(\varepsilon)$ with $\sigma_i = \rho_i$, $i = 1, 2, 3$, does not lie in $\mathrm{EC}_n(\varepsilon)$.*

Proof. This corollary follows from Theorem 4.15 and Definition 1.4. □

Chapter 5

Perfect discrimination of two states in approximate quantum theory

In this chapter, we construct two kinds of one-parameter family of proper cones. They define locally quantum systems that are sufficiently close to quantum theory. We show sufficient conditions for two special states to be perfectly distinguishable in the locally quantum systems.

5.1 One-parameter families of proper cones

We begin with a few basic terms. Let $d_1, d_2 \geq 2$ be integers. For $v \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, there exist unique coefficients $\lambda_1 \geq \cdots \geq \lambda_d \geq 0$, $d = \min\{d_1, d_2\}$, such that v is expressed as $v = \sum_{i=1}^{d} \lambda_i v_i^{[1]} \otimes v_i^{[2]}$ with two orthonormal systems $(v_i^{[1]})_{i=1}^{d}$ and $(v_i^{[2]})_{i=1}^{d}$. The coefficients $\lambda_1 \geq \cdots \geq \lambda_d$ are called the *Schmidt coefficients* of v. If $v \neq 0$, they are closely related to the entanglement of the quantum state $\|v\|^{-2} |v\rangle\langle v|$ (see a textbook in quantum information theory, e.g., [26, 27]). Also, let id_d be the identity mapping on $\mathsf{Herm}(d)$, and τ_d be the transposition on $\mathsf{Herm}(d)$. We denote by Γ the partial transpose on the second system, i.e., $\Gamma = \mathrm{id}_{d_1} \otimes \tau_{d_2}$. If a density matrix ρ lies in $\mathsf{Sep}(d_1, d_2)$, then ρ has positive partial transpose, i.e., $\Gamma(\rho) \geq 0$. This fact is called the *positive partial transpose criterion*. The converse is true for $(d_1, d_2) = (2, 2), (2, 3)$ [31], but is false for $(d_1, d_2) = (3, 3), (2, 4)$ [32].

Now, we consider (d_1, d_2)-level locally quantum systems. Let us construct two kinds of one-parameter family of proper cones.

Definition 5.1 (One-parameter family of proper cones, I)**.** *For $s \geq 0$, we define the proper cone $\mathcal{K}_s^{\mathrm{neg}}$ as*

$$\mathcal{K}_s^{\mathrm{neg}} = \{X \in \mathsf{Sep}(d_1, d_2)^* : \mathrm{neg}(X) \leq s \operatorname{Tr} X\},$$

where for $X \in \mathsf{Herm}(d_1 d_2)$ the value $\mathrm{neg}(X)$ is defined as

$$\mathrm{neg}(X) = \max_{\lambda \text{ eigenvalue of } X} \{-\lambda, 0\}.$$

Note that the inequality

$$\mathrm{neg}(X + Y) \leq \mathrm{neg}(X) + \mathrm{neg}(Y)$$

holds for all $X, Y \in \mathsf{Herm}(d_1 d_2)$.

Definition 5.2 (One-parameter family of proper cones, II)**.** *For a vector $v \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, let $\mathrm{sc}(v)$ be the value*

$$\mathrm{sc}(v) = \begin{cases} \lambda_1 \lambda_2 & v \neq 0, \\ 0 & v = 0, \end{cases}$$

where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$, $d = \min\{d_1, d_2\}$, denote the Schmidt coefficients of $v/\|v\|$. Then, for $s \geq 0$, we define the proper cones $\mathcal{K}_s^{(0)}$ and $\mathcal{K}_s^{\mathrm{sc}}$ as

$$\begin{aligned} \mathcal{K}_s^{(0)} &= \operatorname{conv}\{|v\rangle\langle v| : v \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2},\ \mathrm{sc}(v) \leq s\}, \\ \mathcal{K}_s^{\mathrm{sc}} &= \mathsf{PSD}(d_1 d_2) + \Gamma(\mathcal{K}_s^{(0)}), \end{aligned}$$

where $\mathcal{K}_1 + \mathcal{K}_2$ denotes the Minkowski sum of convex cones $\mathcal{K}_1$ and $\mathcal{K}_2$.

The value $\mathrm{sc}(v)$ is closely related to negative eigenvalues of $\Gamma(|v\rangle\langle v|)$: the equality

$$\|v\|^2 \mathrm{sc}(v) = \mathrm{neg}(\Gamma(|v\rangle\langle v|)) \tag{5.1}$$

holds for every $v \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$. This is because if $v \neq 0$, then the set of all eigenvalues of $\Gamma(|v\rangle\langle v|)/\|v\|^2$ is

$$\{\pm\lambda_i\lambda_j,\ \lambda_k^2 : 1 \leq i < j \leq d,\ 1 \leq k \leq d\},$$

where $\lambda_1 \geq \cdots \geq \lambda_d$ denote the Schmidt coefficients of $v/\|v\|$. An element in $\mathcal{K}_s^{\mathrm{sc}}$ may have negative eigenvalues, but they are restricted by the definition of $\mathcal{K}_s^{\mathrm{sc}}$.

Once the parameter s increases, the proper cones $\mathcal{K}_s^{\mathrm{neg}}$, $\mathcal{K}_s^{(0)}$, and $\mathcal{K}_s^{\mathrm{sc}}$ become larger. Thus, the following inclusion relations hold:

$$\begin{aligned}\mathsf{PSD}(d_1d_2) = \mathcal{K}_0^{\mathrm{neg}} \subset \mathcal{K}_s^{\mathrm{neg}} \subset \mathsf{Sep}(d_1,d_2)^*,\\ \mathsf{Sep}(d_1,d_2) = \mathcal{K}_0^{(0)} \subset \mathcal{K}_s^{(0)} \subset \mathsf{PSD}(d_1d_2),\\ \mathsf{PSD}(d_1d_2) = \mathcal{K}_0^{\mathrm{sc}} \subset \mathcal{K}_s^{\mathrm{sc}} \subset \mathsf{Sep}(d_1,d_2)^*.\end{aligned}$$

Since $\mathcal{K}_s^{(0)}$ satisfies *local unitary invariance*, i.e., $(U^{[1]} \otimes U^{[2]})\mathcal{K}_s^{(0)}(U^{[1]} \otimes U^{[2]})^* = \mathcal{K}_s^{(0)}$ for all unitary matrices $U^{[1]}$ and $U^{[2]}$, no proper cones $\mathcal{K}_s^{\mathrm{sc}}$ depend on the orthonormal basis of $\mathbb{C}^{d_2}$ that defines the partial transpose Γ.

5.2 Proofs

Actually, it suffices to prove Theorems 1.8 and 1.9 only for $(d_1, d_2) = (2, 2)$ due to the following reason. Let $\rho_1^{[1]}, \rho_1^{[2]}, \rho_2^{[1]}, \rho_2^{[2]}$ be the density matrices in Theorems 1.8 and 1.9. Then there exist orthonormal bases $\mathcal{B}^{[i]}$ of $\mathbb{C}^{d_i}$, $i = 1, 2$, such that the matrix representations of $\rho_1^{[1]}, \rho_1^{[2]}, \rho_2^{[1]}, \rho_2^{[2]}$ with respect to $\mathcal{B}^{[1]}$ and $\mathcal{B}^{[2]}$ are given below:

$$\rho_1^{[1]} = \begin{bmatrix} 1 & 0 & & & \\ 0 & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix}, \qquad \rho_1^{[2]} = \begin{bmatrix} 1 & 0 & & & \\ 0 & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix},$$

$$\rho_2^{[1]} = \begin{bmatrix} 1-\alpha_1 & \beta_1 & & & \\ \beta_1 & \alpha_1 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix}, \qquad \rho_2^{[2]} = \begin{bmatrix} 1-\alpha_2 & \beta_2 & & & \\ \beta_2 & \alpha_2 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix},$$

where $\alpha_1, \alpha_2 \in [0, 1]$ and $\beta_i = \sqrt{\alpha_i(1-\alpha_i)}$. That is, each representation matrix above is equal to the direct sum of a 2×2 matrix and the zero matrix. Since the proper cones $\mathcal{K}_s^{\mathrm{sc}}$ are independent of an orthonormal basis of $\mathbb{C}^{d_2}$ that defines the partial transpose Γ, the general case is reduced to the case $(d_1, d_2) = (2, 2)$. Therefore, it suffices to prove the following lemmas.

Lemma 5.3 (Perfect discrimination with $\mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$)**.** *Let ρ_1 and ρ_2 be the rank-one density matrices in $\mathsf{Sep}(2,2)$ given as*

$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \rho_2 = \begin{bmatrix} 1-\alpha_1 & \beta_1 \\ \beta_1 & \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} 1-\alpha_2 & \beta_2 \\ \beta_2 & \alpha_2 \end{bmatrix}, \tag{5.2}$$

where $\alpha_1, \alpha_2 \in [0,1]$ and $\beta_i = \sqrt{\alpha_i(1-\alpha_i)}$. If $s \in [0, 1/4]$ and

$$(1-\alpha_1)(1-\alpha_2) \leq 16 s^2 \alpha_1 \alpha_2, \tag{5.3}$$

then the two states ρ_1 and ρ_2 are perfectly distinguishable by some measurement $\{T_i + \Gamma(T_i)\}_{i=1,2} \in \mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$. The measurement $\{T_i + \Gamma(T_i)\}_{i=1,2} \in \mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$ is given below except for the trivial cases $\alpha_1 = 1$ and $\alpha_2 = 1$: If $\gamma := \alpha_1 + \alpha_2 > 1$, then

$$2\gamma T_1 = \gamma \left|v_1\right\rangle\!\left\langle v_1\right| + (\gamma - 1)\left|v_2\right\rangle\!\left\langle v_2\right| + (\gamma - 1)\left|v_3\right\rangle\!\left\langle v_3\right|, \tag{5.4}$$

$$v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{\beta_1 \beta_2}{\alpha_1 \alpha_2} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{5.5}$$

$$v_2 = \begin{bmatrix} 1 \\ -\beta_1/\alpha_1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ -\beta_2/\alpha_2 \end{bmatrix}, \tag{5.6}$$

$$T_2 = (U^{[1]} \otimes U^{[2]}) T_1 (U^{[1]} \otimes U^{[2]})^*, \tag{5.7}$$

$$U^{[1]} = \frac{1}{\sqrt{\alpha_1}} \begin{bmatrix} \beta_1 & \alpha_1 \\ \alpha_1 & -\beta_1 \end{bmatrix}, \quad U^{[2]} = \frac{1}{\sqrt{\alpha_2}} \begin{bmatrix} \beta_2 & \alpha_2 \\ \alpha_2 & -\beta_2 \end{bmatrix}; \tag{5.8}$$

if $\gamma = 1$, then

$$T_1 = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}, \quad T_2 = \frac{1}{2} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Lemma 5.4 (Perfect discrimination with $\mathcal{M}(\mathcal{K}_s^{\mathrm{sc}})$)**.** *Let ρ_1 and ρ_2 be the rank-one density matrices in $\mathsf{Sep}(2,2)$ given as (5.2). If $s = \sqrt{t}/(1+t)$, $t \in [0,1]$, and*

$$(1-\alpha_1)(1-\alpha_2) \leq t \alpha_1 \alpha_2, \tag{5.9}$$

then the two states ρ_1 and ρ_2 are perfectly distinguishable by the measurement $\{T_i + \Gamma(T_i)\}_{i=1,2} \in \mathcal{M}(\mathcal{K}_s^{\mathrm{neg}})$ given in Lemma 5.3.

We prove Lemmas 5.4 and 5.3 in this order.

Proof of Lemma 5.4. Assume that $s = \sqrt{t}/(1+t)$, $t \in [0,1]$, and (5.9). All we need is to show that

(i) $T_1 + T_2 + \Gamma(T_1 + T_2) = I_4$,

(ii) $T_i \in \mathcal{K}_s^{(0)}$ for $i = 1, 2$,

(iii) $\operatorname{Tr} \rho_1 T_2 = \operatorname{Tr} \rho_2 T_1 = 0$.

Indeed, if (i) and (ii) hold, then $\{T_i + \Gamma(T_i)\}_{i=1,2} \in \mathcal{M}(\mathcal{K}_s^{\mathrm{sc}})$. Also, if (i) and (iii) hold, then the equations $\Gamma(\rho_i) = \rho_i$, $i = 1, 2$, imply that $\operatorname{Tr} \rho_i(T_j + \Gamma(T_j)) = 2 \operatorname{Tr} \rho_i T_j = \delta_{ij}$ for all $i, j \in \{1, 2\}$. Therefore, if (i)–(iii) hold, then Lemma 5.4 follows. Also, note that $(1-\alpha_2)(1-\alpha_1) \le t\alpha_1\alpha_2 \le \alpha_1\alpha_2$ due to $t \in [0,1]$ and (5.9). Thus, $\gamma = \alpha_1 + \alpha_2 \ge 1$. If $\alpha_1\alpha_2 = 0$, then $\alpha_1 = 1$ or $\alpha_2 = 1$, which is a trivial case. Therefore, without loss of generality, we may assume $\alpha_1\alpha_2 > 0$.

Proof of (i). First, assume $\gamma = 1$. Then

$$T_1 + T_2 + \Gamma(T_1 + T_2) = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = I_4.$$

Next, assume $\gamma > 1$. Put $w_i = (U^{[1]} \otimes U^{[2]})v_i$ for $i = 1, 2, 3$. Then w_i, $i = 1, 2, 3$, can be calculated as follows:

$$\begin{aligned} w_1 &= \frac{1}{\sqrt{\alpha_1\alpha_2}}\left(\begin{bmatrix}\beta_1 \\ \alpha_1\end{bmatrix} \otimes \begin{bmatrix}\beta_2 \\ \alpha_2\end{bmatrix} - \frac{\beta_1\beta_2}{\alpha_1\alpha_2}\begin{bmatrix}\alpha_1 \\ -\beta_1\end{bmatrix} \otimes \begin{bmatrix}\alpha_2 \\ -\beta_2\end{bmatrix}\right) \\ &= \frac{1}{\sqrt{\alpha_1\alpha_2}}\left(\begin{bmatrix}\beta_1\beta_2 \\ \beta_1\alpha_2 \\ \alpha_1\beta_2 \\ \alpha_1\alpha_2\end{bmatrix} - \frac{\beta_1\beta_2}{\alpha_1\alpha_2}\begin{bmatrix}\alpha_1\alpha_2 \\ -\alpha_1\beta_2 \\ -\beta_1\alpha_2 \\ \beta_1\beta_2\end{bmatrix}\right) = \frac{1}{\sqrt{\alpha_1\alpha_2}}\begin{bmatrix}0 \\ \beta_1 \\ \beta_2 \\ \gamma - 1\end{bmatrix}, \end{aligned}$$

$$w_2 = \frac{1}{\sqrt{\alpha_1\alpha_2}}\begin{bmatrix}0 \\ 1\end{bmatrix} \otimes \begin{bmatrix}\alpha_2 \\ -\beta_2\end{bmatrix} = \sqrt{\frac{\alpha_2}{\alpha_1}}v_3, \quad w_3 = \frac{1}{\sqrt{\alpha_1\alpha_2}}\begin{bmatrix}\alpha_1 \\ -\beta_1\end{bmatrix} \otimes \begin{bmatrix}0 \\ 1\end{bmatrix} = \sqrt{\frac{\alpha_1}{\alpha_2}}v_2.$$

Thus, putting $\xi = \beta_1\beta_2/\alpha_1\alpha_2$, we have

$$\begin{aligned} &T_1 + T_2 = \frac{1}{2}(|v_1\rangle\langle v_1| + |w_1\rangle\langle w_1|) + \frac{\gamma-1}{2\gamma}(|v_2\rangle\langle v_2| + |v_3\rangle\langle v_3| + |w_2\rangle\langle w_2| + |w_3\rangle\langle w_3|) \\ &= \frac{1}{2}(|v_1\rangle\langle v_1| + |w_1\rangle\langle w_1|) + \frac{\gamma-1}{2\gamma}\Big(|v_2\rangle\langle v_2| + |v_3\rangle\langle v_3| + \frac{\alpha_2}{\alpha_1}|v_3\rangle\langle v_3| + \frac{\alpha_1}{\alpha_2}|v_2\rangle\langle v_2|\Big) \\ &= \frac{1}{2}(|v_1\rangle\langle v_1| + |w_1\rangle\langle w_1|) + \frac{\gamma-1}{2}\Big(\frac{1}{\alpha_2}|v_2\rangle\langle v_2| + \frac{1}{\alpha_1}|v_3\rangle\langle v_3|\Big) \end{aligned}$$

and

$$
\begin{aligned}
T_1+T_2 &= \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -\xi \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\xi & 0 & 0 & \xi^2 \end{bmatrix} + \frac{1}{2\alpha_1\alpha_2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \beta_1^2 & \beta_1\beta_2 & (\gamma-1)\beta_1 \\ 0 & \beta_1\beta_2 & \beta_2^2 & (\gamma-1)\beta_2 \\ 0 & (\gamma-1)\beta_1 & (\gamma-1)\beta_2 & (\gamma-1)^2 \end{bmatrix} \\
&\quad + \frac{\gamma-1}{2\alpha_1\alpha_2}\left(\begin{bmatrix} \alpha_1 & -\beta_1 \\ -\beta_1 & 1-\alpha_1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 & -\beta_2 \\ -\beta_2 & 1-\alpha_2 \end{bmatrix}\right) \\
&= \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -\xi \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -\xi & 0 & 0 & \xi^2 \end{bmatrix} + \frac{1}{2\alpha_1\alpha_2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \beta_1^2 & \beta_1\beta_2 & (\gamma-1)\beta_1 \\ 0 & \beta_1\beta_2 & \beta_2^2 & (\gamma-1)\beta_2 \\ 0 & (\gamma-1)\beta_1 & (\gamma-1)\beta_2 & (\gamma-1)^2 \end{bmatrix} \\
&\quad + \frac{\gamma-1}{2\alpha_1\alpha_2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \alpha_1 & 0 & -\beta_1 \\ 0 & 0 & 0 & 0 \\ 0 & -\beta_1 & 0 & 1-\alpha_1 \end{bmatrix} + \frac{\gamma-1}{2\alpha_1\alpha_2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha_2 & -\beta_2 \\ 0 & 0 & -\beta_2 & 1-\alpha_2 \end{bmatrix}.
\end{aligned}
$$

When t_{ij} denotes the (i,j)-th entry of T_1+T_2, it follows that $t_{11}=1/2$, $t_{12}=t_{21}=t_{13}=t_{31}=0$, $t_{14}=t_{41}=-\xi/2$, $t_{23}=t_{32}=\xi/2$,

$$
t_{24}=t_{42}=\frac{(\gamma-1)\beta_1}{2\alpha_1\alpha_2}-\frac{(\gamma-1)\beta_1}{2\alpha_1\alpha_2}=0, \quad t_{34}=t_{43}=\frac{(\gamma-1)\beta_2}{2\alpha_1\alpha_2}-\frac{(\gamma-1)\beta_2}{2\alpha_1\alpha_2}=0,
$$

$$
\begin{aligned}
t_{22} &= \frac{\beta_1^2}{2\alpha_1\alpha_2}+\frac{(\gamma-1)\alpha_1}{2\alpha_1\alpha_2}=\frac{1-\alpha_1}{2\alpha_2}+\frac{\gamma-1}{2\alpha_2}=1/2, \\
t_{33} &= \frac{\beta_2^2}{2\alpha_1\alpha_2}+\frac{(\gamma-1)\alpha_2}{2\alpha_1\alpha_2}=\frac{1-\alpha_2}{2\alpha_1}+\frac{\gamma-1}{2\alpha_1}=1/2, \\
t_{44} &= \frac{\xi^2}{2}+\frac{(\gamma-1)^2}{2\alpha_1\alpha_2}+\frac{(\gamma-1)(1-\alpha_1)}{2\alpha_1\alpha_2}+\frac{(\gamma-1)(1-\alpha_2)}{2\alpha_1\alpha_2} \\
&= \frac{(1-\alpha_1)(1-\alpha_2)}{2\alpha_1\alpha_2}+\frac{(\gamma-1)^2}{2\alpha_1\alpha_2}+\frac{(\gamma-1)(2-\gamma)}{2\alpha_1\alpha_2} \\
&= \frac{1-\gamma+\alpha_1\alpha_2}{2\alpha_1\alpha_2}+\frac{\gamma-1}{2\alpha_1\alpha_2}=1/2.
\end{aligned}
$$

Therefore,

$$
T_1+T_2+\Gamma(T_1+T_2)=\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -\xi \\ 0 & 1 & \xi & 0 \\ 0 & \xi & 1 & 0 \\ -\xi & 0 & 0 & 1 \end{bmatrix}+\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & \xi \\ 0 & 1 & -\xi & 0 \\ 0 & -\xi & 1 & 0 \\ \xi & 0 & 0 & 1 \end{bmatrix}=I_4.
$$

Proof of (ii). First, assume $\gamma = 1$. Then

$$\alpha_1\alpha_2 \overset{\gamma=1}{=} (1-\alpha_2)(1-\alpha_1) \overset{(5.9)}{\leq} t\alpha_1\alpha_2 \overset{t\in[0,1]}{\leq} \alpha_1\alpha_2,$$

which shows that $t = 1$ and $s = 1/2$. Since it is easily checked that $T_i \in \mathcal{K}^{(0)}_{1/2}$ for $i = 1, 2$, we obtain (ii). Next, assume $\gamma > 1$. Since the function $\sqrt{t'}/(1+t')$, $t' \in [0, 1]$, is increasing, from (5.5) and (5.6), it follows that $\mathrm{sc}(v_2) = \mathrm{sc}(v_3) = 0$ and

$$\mathrm{sc}(v_1) = \frac{\beta_1\beta_2/\alpha_1\alpha_2}{1+(\beta_1\beta_2/\alpha_1\alpha_2)^2} \overset{(5.9)}{\leq} \frac{\sqrt{t}}{1+t} = s.$$

Thus, $T_1 \in \mathcal{K}^{(0)}_s$. Thanks to (5.7), we also have $T_2 \in \mathcal{K}^{(0)}_s$. Therefore, (ii) holds.

Proof of (iii). First, assume $\gamma = 1$. Then it is easily checked that $\operatorname{Tr}\rho_1 T_2 = 0$ and

$$\operatorname{Tr}\rho_2 T_1 = (1-\alpha_1)(1-\alpha_2) + \alpha_1\alpha_2 - 2\beta_1\beta_2 \overset{\gamma=1}{=} \alpha_1\alpha_2 + \alpha_1\alpha_2 - 2\alpha_1\alpha_2 = 0,$$

which are just (iii). Next, assume $\gamma > 1$. Using (5.4), $\rho_2 |v_2\rangle = \rho_2 |v_3\rangle = 0$, and

$$\begin{aligned}\langle v_1|\rho_2|v_1\rangle &= (1-\alpha_1)(1-\alpha_2) + \Big(\frac{\beta_1\beta_2}{\alpha_1\alpha_2}\Big)^2\alpha_1\alpha_2 - \frac{\beta_1\beta_2}{\alpha_1\alpha_2}\cdot 2\beta_1\beta_2 \\ &= (1-\alpha_1)(1-\alpha_2) - \frac{(\beta_1\beta_2)^2}{\alpha_1\alpha_2} = 0,\end{aligned}$$

we have

$$\operatorname{Tr}\rho_2 T_1 = \frac{1}{2}\langle v_1|\rho_2|v_1\rangle + \frac{\gamma-1}{2\gamma}\langle v_2|\rho_2|v_2\rangle + \frac{\gamma-1}{2\gamma}\langle v_3|\rho_2|v_3\rangle = 0.$$

Moreover, since $\rho_2 = (U^{[1]}\otimes U^{[2]})^*\rho_1(U^{[1]}\otimes U^{[2]})$ holds, we obtain

$$\begin{aligned}\operatorname{Tr}\rho_1 T_2 &\overset{(5.7)}{=} \operatorname{Tr}\rho_1(U^{[1]}\otimes U^{[2]})T_1(U^{[1]}\otimes U^{[2]})^* \\ &= \operatorname{Tr}(U^{[1]}\otimes U^{[2]})^*\rho_1(U^{[1]}\otimes U^{[2]})T_1 = \operatorname{Tr}\rho_2 T_1 = 0.\end{aligned}$$

Therefore, (iii) holds. □

Proof of Lemma 5.3. Assume that $s \in [0, 1/4]$ and (5.3). All we need is to show that

(i) $T_1 + T_2 + \Gamma(T_1 + T_2) = I_4$,

(ii) $\mathrm{neg}(T_i + \Gamma(T_i)) \leq s \operatorname{Tr}(T_i + \Gamma(T_i))$ for $i = 1, 2$,

(iii) $\operatorname{Tr}\rho_1 T_2 = \operatorname{Tr}\rho_2 T_1 = 0$,

by the same reason as the proof of Lemma 5.4. Since (i) and (iii) have been already proved, we show only (ii). Also, the inequality $\gamma = \alpha_1 + \alpha_2 \geq 1$ holds, and we may assume $\alpha_1\alpha_2 > 0$, by the same reason as the proof of Lemma 5.4. Moreover, (5.7) and (i) yield that $\operatorname{Tr} T_1 = \operatorname{Tr} T_2$ and $\operatorname{Tr} T_1 + \operatorname{Tr} T_2 = 2$, which implies $\operatorname{Tr} T_1 = \operatorname{Tr} T_2 = 1$.

Proof of (ii). First, assume $\gamma = 1$. Then

$$\alpha_1\alpha_2 \overset{\gamma=1}{=} (1-\alpha_2)(1-\alpha_1) \overset{(5.3)}{\leq} 16s^2\alpha_1\alpha_2 \overset{s\in[0,1/4]}{\leq} \alpha_1\alpha_2,$$

which implies $s = 1/4$. Since it is easily checked that $\operatorname{neg}(T_i + \Gamma(T_i)) = 1/2$ for $i = 1, 2$, we obtain (ii). Next, assume $\gamma > 1$. Then

$$\begin{aligned}\operatorname{neg}(T_1 + \Gamma(T_1)) \leq \operatorname{neg}(\Gamma(T_1)) &\overset{(5.4)}{\leq} \operatorname{neg}\Big(\Gamma\Big(\frac{1}{2}\,|v_1\rangle\langle v_1|\Big)\Big) \\ &\overset{(5.1)}{=} \frac{1}{2}\|v_1\|^2 \operatorname{sc}(v_1) \overset{(5.5)}{=} \frac{\beta_1\beta_2}{2\alpha_1\alpha_2} \overset{(5.3)}{\leq} 2s = s\operatorname{Tr}(T_1 + \Gamma(T_1)).\end{aligned}$$

By (5.7), we have

$$\operatorname{neg}(T_2 + \Gamma(T_2)) \leq \operatorname{neg}(\Gamma(T_2)) = \operatorname{neg}(\Gamma(T_1)) \leq 2s = s\operatorname{Tr}(T_2 + \Gamma(T_2)).$$

Therefore, (ii) holds. □

Chapter 6

Conclusion

We have studied three topics associated with quantum systems and locally quantum systems: (i) capacity, (ii) differential privacy, and (iii) perfect discrimination of two states.

6.1 Statement determining the capacities of GPTs, and weaker statement

As stated in Section 1.1, statement S is useful to determine the capacities of special locally quantum systems. We have shown statement WS that is weaker than statement S, but we still do not know whether statement S holds. If statement S is true, it is a separability criterion in the n-partite case. Other separability criteria are known, e.g., the positive partial transpose criterion (see Section 5.1) and k-extendability [14]. However, both of them are criteria in the bipartite case. In general, it is difficult to prove a separability criterion in the n-partite case.

In Chapter 3, we have shown that the maximum dimension of subspaces of $\mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$ with no product basis is equal to $\tilde{d} - 2$ if either (i) $n = 2$ or (ii) $n \geq 3$ and $\#\mathcal{F} > \max\{d_i : i \neq n_1, n_2\}$ for some n_1 and n_2. When $n \geq 3$, assumption (ii) is maybe unnecessary, but we do not know its proof. Also, we have shown that a subspace $\mathcal{L}$ of $\mathcal{F}^{d_1} \otimes \cdots \otimes \mathcal{F}^{d_n}$ contains a $(\tilde{d} - r^n)$-dimensional subspace with no product basis if the dimension of $\mathcal{L}$ is equal to $\tilde{d} - r$ and if $\mathcal{F}$ is infinite. This is best possible for $r = 0, 1$, but we do not know the case $r \geq 2$, which is an interesting problem.

6.2 Differential privacy

In Chapter 4, we have investigated the difference between the sets $\mathrm{EC}_n(\varepsilon)$ and $\mathrm{CQ}_n(\varepsilon)$. Elements in $\mathrm{CQ}_n(\varepsilon)$ correspond to CQ ε-DP mechanisms in the local privacy context, and elements in $\mathrm{EC}_n(\varepsilon)$ correspond to essentially classical ones. Although we have not fixed the dimension d of the finite-dimensional vector spaces $\mathbb{C}^d$ and $\mathbb{R}^d$, it is also important to study the case when d is fixed. For instance, it is an interesting problem to find extreme points of $\mathrm{CQ}_n^{(d)}(\varepsilon)$. For the classical case, Holohan et al. [29] studied extreme points of $\mathrm{C}_n^{(d)}(\varepsilon)$. Also, CQ-DP mechanisms are expected to be superior to classical ones in information processing. Hence, we hope that such information processing will be found in the near future.

We have used Lemma 4.13 to construct CQ ε-DP n-tuples that do not lie in $\mathrm{EC}_n(\varepsilon)$. Instead of Lemma 4.13, one might use *symmetric, informationally complete, positive-operator-valued measures (SIC-POVMs)*. In this case, one can probably prove that the CQ-ε-DP d^2-tuple $(\rho_i)_{i=1}^{d^2}$ of density matrices on $\mathbb{C}^d$ constructed by a SIC-POVM does not lie in $\mathrm{EC}_{d^2}(\varepsilon)$. However, we can prove this statement only for large $\varepsilon > 0$ if using Corollary 4.6. Hence, one needs an alternative criterion instead of Corollary 4.6 to prove the above statement.

6.3 Perfect discrimination of two states

In Chapter 5, we have constructed two kinds of one-parameter family of proper cones in a certain natural manner. However, there are other natural manners to construct one-parameter families. Given a concrete one-parameter family, one will show a similar result to Theorems 1.8 and 1.9. However, it is difficult to show such a result in the general case. Hence, we need another idea for further research. For instance, it is an interesting problem whether equivalence E can characterize quantum theory in some sense. Since this problem can be regarded as that to characterize a symmetric cone, it might also be mathematically interesting.

Since we have had no chance to introduce symmetric cones and Jordan algebras, we mention them briefly here. A convex cone $\mathcal{K}$ of a real Hilbert space $\mathcal{V}$ is called *symmetric* if $\mathcal{K}$ is

- self-dual, i.e., $\mathcal{K}^* = \mathcal{K}$ and
- homogeneous, i.e., $\forall x, x'$ in the interior of $\mathcal{K}$, $\exists g \in G(\mathcal{K})$, $gx = x'$,

where the group $G(\mathcal{K})$ is defined as

$$G(\mathcal{K}) = \{g \in \mathrm{GL}(\mathcal{V}) : g\mathcal{K} = \mathcal{K}\}.$$

Table 6.1: Euclidean Jordan algebras.

Symmetric cone	Euclidean Jordan algebra	Multiplication	Inner product
Orthant $[0,\infty)^d$	$\mathbb{R}^d$	$x \circ y = \begin{bmatrix} x(1)y(1) \\ \vdots \\ x(d)y(d) \end{bmatrix}$	$\sum_{i=1}^{d} x(i)y(i)$
$\mathsf{PSD}(d)$	$\mathsf{Herm}(d)$	$X \circ Y = (XY + YX)/2$	$\operatorname{Tr} XY$
Lorentz cone $\left\{ \begin{bmatrix} \xi \\ x \end{bmatrix} : \|x\| \le \xi \right\}$	$\mathbb{R}^{1+d}$	$\begin{bmatrix} \xi \\ x \end{bmatrix} \circ \begin{bmatrix} \eta \\ y \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} \xi\eta + x^\top y \\ \xi y + \eta x \end{bmatrix}$	$\xi\eta + x^\top y$

Mathematically, a symmetric cone $\mathcal{K}$ is characterized by a Euclidean Jordan algebra $\mathcal{V}$ [39, 50]:

$$\mathcal{K} \text{ symmetric cone} \iff \exists \mathcal{V} \text{ Euclidean Jordan algebra, } \mathcal{K} = \{x^2 : x \in \mathcal{V}\}.$$

A real Hilbert space $\mathcal{V}$ with multiplication is called a *Euclidean Jordan algebra* if $\mathcal{V}$ satisfies the following conditions.

- $\mathcal{V}$ has an identity element.
- Distributive property: $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$ for all $x, y, z \in \mathcal{V}$.
- Compatible property with scalars: $(\alpha x)(\beta y) = \alpha\beta(xy)$ for all $x, y \in \mathcal{V}$ and $\alpha, \beta \in \mathbb{R}$.
- Commutative property: $xy = yx$ for all $x, y \in \mathcal{V}$.
- Jordan identity: $x(y(xx)) = (xy)(xx)$ for all $x, y \in \mathcal{V}$.
- Euclidean property: $\langle x, yz \rangle = \langle xy, z \rangle$ for all $x, y, z \in \mathcal{V}$.

Table 6.1 has three types of Euclidean Jordan algebras. Every Euclidean Jordan algebra can be decomposed to simple ones, and the classification of simple Euclidean

Jordan algebras is known [37]. In this way, convex cones are often studied in mathematics with an algebraic view. However, it is maybe more useful to study a topic like perfect discrimination in order to further understand GPTs. We hope that such studies will increase much more.

Bibliography

[1] S. Aaronson and G. N. Rothblum. Gentle measurement of quantum states and differential privacy. In *STOC'19—Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 322–333. ACM, New York, 2019.

[2] N. Alon and L. Lovász. Unextendible product bases. *J. Combin. Theory Ser. A*, 95(1):169–179, 2001.

[3] H. Arai, Y. Yoshida, and M. Hayashi. Perfect discrimination of non-orthogonal separable pure states on bipartite system in general probabilistic theory. *J. Phys. A*, 52(46):465304, 14, 2019.

[4] G. Aubrun and S. J. Szarek. Tensor products of convex sets and the volume of separable states on n qudits. *Phys. Rev. A*, 73(2):022109, 10, 2006.

[5] P. Bag, S. Dey, M. Nagisa, and H. Osaka. The order-n minors of certain $(n + k) \times n$ matrices. *Linear Algebra Appl.*, 603:368–389, 2020.

[6] H. Barnum and J. Hilgert. Strongly symmetric spectral convex bodies are jordan algebra state spaces. preprint, available at `https://arxiv.org/abs/1904.03753`, 2019.

[7] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, 82(26, part 1):5385–5388, 1999.

[8] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge University Press, Cambridge, 2004.

[9] A. Chefles, R. Jozsa, and A. Winter. On the existence of physical transformations between sets of quantum states. *Int. J. Quantum Inf.*, 2(01):11–21, 2004.

[10] J. Chen and N. Johnston. The minimum size of unextendible product bases in the bipartite case (and some multipartite cases). *Comm. Math. Phys.*, 333(1):351–365, 2015.

[11] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[12] T. Cubitt, A. Montanaro, and A. Winter. On the dimension of subspaces with bounded Schmidt rank. *J. Math. Phys.*, 49(2):022107, 6, 2008.

[13] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases, uncompletable product bases and bound entanglement. *Comm. Math. Phys.*, 238(3):379–410, 2003.

[14] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A*, 69(2):022308, 20, 2004.

[15] Y. Du, M.-H. Hsieh, T. Liu, D. Tao, and N. Liu. Quantum noise protects quantum classifiers against adversaries. *Phys. Rev. Research*, 3(2):023153, 18, 2021.

[16] Y. Du, M.-H. Hsieh, T. Liu, S. You, and D. Tao. Quantum differentially private sparse regression learning. preprint, available at `https://arxiv.org/abs/2007.11921`, 2020.

[17] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science—FOCS 2013*, pages 429–438. IEEE Computer Soc., Los Alamitos, CA, 2013.

[18] C. Dwork. Differential privacy. In *Automata, languages and programming, Part II*, volume 4052 of *Lecture Notes in Comput. Sci.*, pages 1–12. Springer, Berlin, 2006.

[19] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography*, volume 3876 of *Lecture Notes in Comput. Sci.*, pages 265–284. Springer, Berlin, 2006.

[20] I. Ekeland and R. Témam. *Convex analysis and variational problems*, volume 28 of *Classics in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, english edition, 1999. Translated from the French.

[21] K. Feng. Unextendible product bases and 1-factorization of complete graphs. *Discrete Appl. Math.*, 154(6):942–949, 2006.

[22] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath. The staircase mechanism in differential privacy. *IEEE J. Sel. Topics Signal Process.*, 9(7):1176–1184, 2015.

[23] Q. Geng and P. Viswanath. The optimal noise-adding mechanism in differential privacy. *IEEE Trans. Inform. Theory*, 62(2):925–951, 2016.

[24] Q. Geng and P. Viswanath. Optimal noise adding mechanisms for approximate differential privacy. *IEEE Trans. Inform. Theory*, 62(2):952–969, 2016.

[25] L. Gurvits and H. Barnum. Largest separable balls around the maximally mixed bipartite quantum state. *Phys. Rev. A*, 66(6):062311, 7, 2002.

[26] M. Hayashi. *Quantum Information Theory: Mathematical Foundation, Second Edition*. Springer, Berlin, Heidelberg, 2017.

[27] M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa. *Introduction to Quantum Information Science*. Springer, Berlin, Heidelberg, 2015.

[28] R. Hildebrand. Entangled states close to the maximally mixed state. *Phys. Rev. A*, 75(6):062330, 10, 2007.

[29] N. Holohan, D. J. Leith, and O. Mason. Extreme points of the local differential privacy polytope. *Linear Algebra Appl.*, 534:78–96, 2017.

[30] N. Holohan, D. J. Leith, and O. Mason. Optimal differentially private mechanisms for randomised response. *IEEE Trans. Inf. Forensics Secur.*, 12(11):2726–2735, 2017.

[31] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1-2):1–8, 1996.

[32] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232(5):333–339, 1997.

[33] Z. Huang, C.-K. Li, E. Poon, and N.-S. Sze. Physical transformations between quantum states. *J. Math. Phys.*, 53(10):102209, 12, 2012.

[34] N. Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[35] P. Janotta. Generalizations of boxworld. In *Proc. 8th International Workshop on Quantum Physics and Logic*, volume 95, pages 183–192, 2012.

[36] P. Janotta and H. Hinrichsen. Generalized probability theories: what determines the structure of quantum theory? *J. Phys. A*, 47(32):323001, 32, 2014.

[37] P. Jordan, J. von Neumann, and E. Wigner. On an algebraic generalization of the quantum mechanical formalism. *Ann. of Math. (2)*, 35(1):29–64, 1934.

[38] P. Kairouz, S. Oh, and P. Viswanath. Extremal mechanisms for local differential privacy. *J. Mach. Learn. Res.*, 17:Paper No. 17, 51, 2016.

[39] M. Koecher. Positivitätsbereiche im R^n. *Amer. J. Math.*, 79:575–596, 1957.

[40] L. Lami, C. Palazuelos, and A. Winter. Ultimate data hiding in quantum mechanics and beyond. *Comm. Math. Phys.*, 361(2):661–708, 2018.

[41] L. Masanes and M. P. Müller. A derivation of quantum theory from physical requirements. *New J. Phys.*, 13(6):063001, 29, 2011.

[42] K. Matsumoto and G. Kimura. On additivity of strong converse bound of noiseless channels in locally quantum systems —in relation to the radius of the separable ball—. In *Proc. of The 37th Quantum Information Technology Symposium (QIT37)*, pages 13–16, 2017. `https://www.ieice.org/ken/paper/20171116Z1AP/eng/`.

[43] M. P. Müller, O. C. O. Dahlsten, and V. Vedral. Unifying typical entanglement and coin tossing: on randomization in probabilistic theories. *Comm. Math. Phys.*, 316(2):441–487, 2012.

[44] M. P Müller and C. Ududec. Structure of reversible computation determines the self-duality of quantum theory. *Phys. Rev. Lett.*, 108:130401, 5, 2012.

[45] K. R. Parthasarathy. On the maximal dimension of a completely entangled subspace for finite level quantum systems. *Proc. Indian Acad. Sci. Math. Sci.*, 114(4):365–374, 2004.

[46] M. Plávala and M. Ziman. Popescu-Rohrlich box implementation in general probabilistic theory of processes. *Phys. Lett. A*, 384(16):126323, 6, 2020.

[47] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–385, 1994.

[48] A. J. Short and S. Wehner. Entropy in general physical theories. *New J. Phys.*, 12(March):033023, 34, 2010.

[49] A. Uhlmann. The transition probability for states of *-algebras. *Ann. Physik (7)*, 42(4-6):524–532, 1985.

[50] È. B. Vinberg. Homogeneous cones. *Soviet Math. Dokl.*, 1:787–790, 1960.

[51] N. R. Wallach. An unentangled Gleason's theorem. In *Quantum computation and information (Washington, DC, 2000)*, volume 305 of *Contemp. Math.*, pages 291–298. Amer. Math. Soc., Providence, RI, 2002.

[52] S. L. Warner. Randomized response: a survey technique for eliminating evasive answer bias. *J. Amer. Statist. Assoc.*, 60(309):63–69, 1965.

[53] Y. Yoshida, H. Arai, and M. Hayashi. Perfect discrimination in approximate quantum theory of general probabilistic theories. *Phys. Rev. Lett.*, 125(15):150402, 5, 2020.

[54] Y. Yoshida and M. Hayashi. Asymptotic properties for Markovian dynamics in quantum theory and general probabilistic theories. *J. Phys. A*, 53(21):215303, 43, 2020.

[55] Y. Yoshida, M.-H. Yung, and M. Hayashi. Optimal mechanism for randomized responses under universally composable security measure. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 547–551. IEEE, Paris, France, 2019.

[56] L. Zhou and M. Ying. Differential privacy in quantum computation. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, pages 249–262. IEEE Computer Soc., Santa Barbara, CA, 2017.