Comments on and Corrections to “When Is the Chernoff Exponent for Quantum Operations Finite?”

Nengkun Yu and Li Zhou

I. Introduction

In THE above article [1], we add some missing citations in the Notations and Preliminaries section. The new Notations and Preliminaries section is as follows.

II. Notations and Preliminaries

We use the symbols $\mathcal{H}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$ to denote finite-dimensional Hilbert spaces over complex numbers and $\mathrm{L}(\mathcal{H})$ to denote the set of linear operators mapping from $\mathcal{H}$ into itself. For Hermitian matrices A, B, we use $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B) = \mathrm{Tr}(AB)$ to denote their inner product. Let $\mathrm{Pos}(\mathcal{H}) \subset \mathrm{L}(\mathcal{H})$ be the set of positive (semidefinite) matrices, and $\mathcal{D}(\mathcal{H}) \subset \mathrm{Pos}(\mathcal{H})$ is the set of positive matrices with trace one. A pure quantum state of $\mathcal{H}$ is just a normalized vector $|\psi\rangle \in \mathcal{H}$, while a general quantum state is characterized by a density operator $\rho \in \mathcal{D}(\mathcal{H})$. For simplicity, we use ψ to represent the density operator of a pure state $|\psi\rangle$ which is just the projector $\psi = |\psi\rangle\langle\psi|$. A density operator ρ can always be decomposed into a convex combination of pure states:

$$\rho = \sum_{k=1}^{n} p_k |\psi_k\rangle\langle\psi_k|,$$

where the coefficients p_k are strictly positive numbers and add up to one. The support of ρ is defined as $\mathrm{supp}(\rho) = \mathrm{span}\{|\psi_k\rangle : 1 \leq k \leq n\}$. We say two pure states $|\psi\rangle$ and $|\phi\rangle$ are orthogonal if and only if their inner product $\langle\psi, \phi\rangle$ is equal to zero, and the orthogonality of two density operators ρ and σ is defined by the orthogonality of their supports, namely, ρ and σ are orthogonal if and only if $\mathrm{supp}(\rho) \perp \mathrm{supp}(\sigma)$. Two density operators ρ and σ are said to be disjoint if $\mathrm{supp}(\rho) \cap \mathrm{supp}(\sigma) = \{0\}$ and joint if the intersection of their support contains some non-zero vectors.

There are two commonly used measures to characterize the difference between the quantum states: trace distance and fidelity. The trace distance D between two density operators ρ and σ is defined as

$$D(\rho, \sigma) \equiv \frac{1}{2}\mathrm{Tr}|\rho - \sigma|$$

where we define $|A| \equiv \sqrt{A^\dagger A}$ to be the positive square root of $A^\dagger A$.

The fidelity of states ρ and σ is defined to be

$$F(\rho, \sigma) \equiv \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}.$$

For pure states $|\psi\rangle$ and $|\phi\rangle$, $F(\psi, \phi) = |\langle\psi|\phi\rangle|$.

The strong concavity property for the fidelity is quite useful, which can be formalized as

Fact 1 [4]: For quantum states ρ_i, σ_i and probability distributions $(p_0, p_1, \cdots, p_n)$ and $(q_0, q_1, \cdots, q_n)$

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_{i=0}^{n} \sqrt{p_i q_i} F(\rho_i, \sigma_i).$$

If $\rho_i = \psi_i$ and $\sigma_i = \phi_i$ are all pure states, we obtain

$$F\left(\sum_i p_i\psi_i, \sum_i q_i\phi_i\right) \geq \sum_{i=0}^{n} \sqrt{p_i q_i} F(\psi_i, \phi_i)$$
$$= \sum_{i=0}^{n} |\langle\sqrt{p_i}\psi_i|\sqrt{q_i}\phi_i\rangle|.$$

Definition 1: We say that a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is a purification of some state ρ if $\mathrm{tr}_A(\psi) = \rho$.

Fact 2 (Uhlmann’s Theorem, [5]): Given quantum states ρ, σ, and a purification $|\psi\rangle$ of ρ, it holds that $F(\rho, \sigma) = \max_{|\phi\rangle} |\langle\phi|\psi\rangle|$, where the maximum is ranging over all purifications of σ.

The following fact connects the trace distance and the fidelity between two states.

Fact 3 (Fuchs-van de Graaf Inequalities [3]): For quantum states ρ and σ, it holds that

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}.$$

For pure states $|\phi\rangle$ and $|\psi\rangle$, we have

$$D(\phi, \psi) = \sqrt{1 - F(\phi, \psi)^2} = \sqrt{1 - |\langle\phi|\psi\rangle|^2}.$$

The trace distance is a static measure quantifying how close two quantum states are and is closely related to the discrimination of quantum states. Let us consider the two hypotheses, H_0 and H_1. Hypothesis H_0 assumes that a given unknown quantum state is equal to ρ_0, and Hypothesis H_1 assumes that a given unknown quantum state is equal to ρ_1. We assume that the prior probability distribution of ρ_0 and ρ_1 are Π_0 and Π_1, respectively, which add up to one.

A physical strategy to discriminate between these two hypotheses is to perform a positive-operator valued measure (POVM) on the quantum state with two outcomes, 0 and 1. Such a POVM has two elements $\{E_0, E_1\}$ satisfying $E_0, E_1 \in \mathrm{Pos}(\mathcal{H})$ and $E_0 + E_1 = I$, where I is the identity matrix of $\mathcal{H}$. The aim of quantum state discrimination is to find the elements E_0 and E_1 that minimize the total error P_{err}, which is

$$P_{err} = \Pi_0 \mathrm{Tr}[E_1\rho_0] + \Pi_1 \mathrm{Tr}[E_0\rho_1].$$

This optimal error has been identified by Helstrom as expressed in the following equation

$$P_{err,min} = \frac{1}{2}\left(1 - \mathrm{Tr}|\Pi_1\rho_1 - \Pi_0\rho_0|\right).$$

A quantum operation $\mathcal{E}$ from $\mathrm{L}(\mathcal{H})$ to $\mathrm{L}(\mathcal{Z})$ is a completely positive and trace-preserving map used to describe the evolution of

Manuscript received February 1, 2022; accepted February 1, 2022. Date of current version May 20, 2022. *(Corresponding author: Nengkun Yu.)*

Nengkun Yu is with the Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: nengkunyu@gmail.com).

Li Zhou is with the Max Planck Institute for Security and Privacy, 44799 Bochum, Germany.

Digital Object Identifier 10.1109/TIT.2022.3148774

an open quantum system. A quantum operation $\mathcal{E}$ can always be represented using the Kraus representation as

$$\mathcal{E}(\rho) = \sum_{i=1}^{k} E_i \rho E_i^\dagger,$$

where $\{E_i\}_{i=1,\cdots,k}$ are the Kraus operators of $\mathcal{E}$ satisfying $\sum_{i=1}^{k} E_i^\dagger E_i = I$, the identity of $\mathcal{H}$.

The following fact states that the fidelity between two states is non-decreasing under quantum operations.

Fact 4 [4]: For states ρ, σ, and quantum operation $\mathcal{E}(\cdot)$, it holds that

$$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma).$$

Quantum operations $\mathcal{E}$ and $\mathcal{F}$ are said to be perfectly distinguishable with finite uses if there exists a strategy illustrated as Figure 1 such that σ_n and ρ_n are orthogonal.

Two conditions introduced by [2] characterize the perfect distinguishability between quantum operations.

Definition 2 [2]: Two quantum operations, $\mathcal{E}$ and $\mathcal{F}$, acting on the same principal system, denoted by Q, are said to be disjoint if there is an auxiliary system R, and a pure state $\left|\psi^{RQ}\right\rangle$, such that $(\mathcal{I}^R \otimes \mathcal{E}^Q)(\psi^{RQ})$ and $(\mathcal{I}^R \otimes \mathcal{F}^Q)(\psi^{RQ})$ are disjoint, where $\mathcal{I}^R$ is the identity operation on R, and the superscripts only identify which systems the operations acted on. Otherwise, they are called joint.

Intuitively, this disjointness guarantees that the outputs do not have a common part with the carefully chosen input. This disjointness is necessary to achieve perfect distinguishability. Otherwise, according to an inductive argument, there is always a non-zero common part between the outputs for an arbitrary strategy with finite uses.

Another relationship is to ensure that non-orthogonal states, ρ and σ, exist such that $(\mathcal{I}^R \otimes \mathcal{E}^Q)(\rho^{RQ})$ and $(\mathcal{I}^R \otimes \mathcal{F}^Q)(\sigma^{RQ})$ become orthogonal, then one can distinguish $(\mathcal{I}^R \otimes \mathcal{E}^Q)(\rho^{RQ})$ and $(\mathcal{I}^R \otimes \mathcal{F}^Q)(\sigma^{RQ})$ without error. This is the final step of any strategy to achieve perfect distinguishability between $\mathcal{E}$ and $\mathcal{F}$.

Interestingly, these two conditions are not only necessary but also sufficient for the perfect distinguishability between quantum operations [2].

Proposition 1 [2]: Two quantum operations $\mathcal{E}$ and $\mathcal{F}$ are perfectly distinguishable if and only if: 1). They are disjoint; 2). They can map some non-orthogonal states into orthogonal states.

We remark here that ancillary systems are also allowed to achieve perfect discrimination.

In the following, we give an analytical characterization of the negation of the second condition, i.e., that $\mathcal{E}$ and $\mathcal{F}$ cannot map some non-orthogonal states into orthogonal states even with the help of ancillary system.

Remark 1[2]: For $\mathcal{E}(\cdot) = \sum_i E_i \cdot E_i^\dagger$ and $\mathcal{F}(\cdot) = \sum_j F_j \cdot F_j^\dagger$, Condition 2) of Proposition 1 is equivalent to $I \notin \operatorname{span}\{({E_i}^\dagger F_j); 1 \leq i, j \leq m\}$.

We want to emphasize this proof of the characterization is precisely the same as given in [2]. We provide the following argument for the readers' convenience.

Without loss of generality, we assume that $\mathcal{E}$ and $\mathcal{F}$ have the same number of Kraus operators by adding zero Kraus operators, if necessary. That is, $\mathcal{E}(\cdot) = \sum_{i=1}^{m} E_i \cdot E_i^\dagger$ and $\mathcal{F}(\cdot) = \sum_{j=1}^{m} F_j \cdot F_j^\dagger$, cannot make non-orthogonal states orthogonal. That is, if ρ^{RQ} and σ^{RQ} are not orthogonal, then $(\mathcal{I}^R \otimes \mathcal{E}^Q)(\rho^{RQ})$ and $(\mathcal{I}^R \otimes \mathcal{F}^Q)(\sigma^{RQ})$ are not orthogonal. Equivalently, if pure states $\rho^{RQ} = |\psi^{RQ}\rangle\langle\psi^{RQ}|$ and $\sigma^{RQ} = |\phi^{RQ}\rangle\langle\phi^{RQ}|$ are not orthogonal, then $(\mathcal{I}^R \otimes \mathcal{E}^Q)(\rho^{RQ})$ and $(\mathcal{I}^R \otimes \mathcal{F}^Q)(\sigma^{RQ})$ are not orthogonal. In other words,

$$\operatorname{Tr}[(\mathcal{I}^R \otimes \mathcal{E}^Q)(\psi^{RQ})(\mathcal{I}^R \otimes \mathcal{F}^Q)(\phi^{RQ})] = 0$$

implies

$$\langle\psi^{RQ}|\phi^{RQ}\rangle = 0.$$

That is, if $\forall 1 \leq i, j \leq m$,

$$(I^R \otimes E_i^Q)|\psi^{RQ}\rangle\langle\psi^{RQ}|(I^R \otimes E_i^Q)^\dagger$$

is orthgonal to

$$(I^R \otimes F_j^Q)|\phi^{RQ}\rangle\langle\phi^{RQ}|(I^R \otimes F_j^Q)^\dagger],$$

then

$$\langle\psi^{RQ}|\phi^{RQ}\rangle = 0.$$

The above condition is equivalent to for $\left|\psi^{RQ}\right\rangle$ and $\left|\phi^{RQ}\right\rangle$, if

$$\langle\psi^{RQ}|(I^R \otimes E_i^Q)^\dagger(I^R \otimes F_j^Q)\left|\phi^{RQ}\right\rangle = 0$$

for all $1 \leq i, j \leq m$, then

$$\langle\psi^{RQ}|\phi^{RQ}\rangle = 0.$$

That is, if $\forall 1 \leq i, j \leq m$

$$\langle\psi^{RQ}|(I^R \otimes {E_i}^\dagger F_j)\left|\phi^{RQ}\right\rangle = 0,$$

then

$$\langle\psi^{RQ}|\phi^{RQ}\rangle = 0.$$

For any $M \in \mathrm{L}(\mathcal{H}_Q)$, one can find $\left|\phi^{RQ}\right\rangle$ and $\left|\psi^{RQ}\right\rangle$ such that $M = \operatorname{Tr}_R|\phi^{RQ}\rangle\langle\psi^{RQ}|$. We know that $\forall 1 \leq i, j \leq m$

$$\operatorname{Tr}(M{E_i}^\dagger F_j) = \langle\psi^{RQ}|(I^R \otimes {E_i}^\dagger F_j)\left|\phi^{RQ}\right\rangle = 0,$$

implies

$$\operatorname{Tr} M = 0.$$

That is satisfied if and only if $I^{RQ} \in \operatorname{span}\{(I^R \otimes {E_i}^\dagger F_j); 1 \leq i, j \leq m\}$, which in turn is equivalent to $I \in \operatorname{span}\{E_i^\dagger F_j; 1 \leq i, j \leq m\}$.

Therefore, $\mathcal{E}$ and $\mathcal{F}$ can map some non-orthogonal states into orthogonal states, Condition 2) of Proposition 1, is equivalent to $I \notin \operatorname{span}\{({E_i}^\dagger F_j); 1 \leq i, j \leq m\}$.

References

[1] N. Yu and L. Zhou, "When is the Chernoff exponent for quantum operations finite?" *IEEE Trans. Inf. Theory*, vol. 67, no. 7, pp. 4517–4523, Jul. 2021.

[2] R. Duan, Y. Feng, and M. Ying, "Perfect distinguishability of quantum operations," *Phys. Rev. Lett.*, vol. 103, no. 21, Nov. 2009, Art. no. 210501.

[3] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1216–1227, May 1999.

[4] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[5] A. Uhlmann, "The 'transition probability' in the state space of a †-algebra," *Rep. Math. Phys.*, vol. 9, no. 2, p. 273, 1976.