Optimal discrimination between quantum operations

2008 J. Phys. A: Math. Theor. 41 335302

(http://iopscience.iop.org/1751-8121/41/33/335302)

IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **41** (2008) 335302 (10pp) doi:10.1088/1751-8113/41/33/335302

Optimal discrimination between quantum operations

Lvzhou Li and Daowen Qiu

Department of Computer Science, Zhongshan University, Guangzhou 510275, People's Republic of China

E-mail: issqdw@mail.sysu.edu.cn

Received 28 January 2008, in final form 16 June 2008
Published 11 July 2008
Online at stacks.iop.org/JPhysA/41/335302

Abstract

In this paper, we consider the problem of discriminating two given quantum operations. Based on the Bloch representation of a single qubit, we give an implicit expression that can be used to evaluate the exact minimum error probability of discriminating any two single-qubit quantum operations by unentangled input states. In particular, for the Pauli channels discussed in Sacchi (2005 *Phys. Rev.* A **71** 062340), we use a more intuitive and visual method to deal with their discrimination problem. Also, we consider the condition for perfect discrimination of two quantum operations.

PACS numbers: 03.67.−a, 03.65.Ta

1. Introduction

Discriminating quantum states is a fundamental task in quantum information. It is well known that nonorthogonal quantum states cannot be perfectly discriminated. However, it is possible to discriminate them in some relaxed ways. Specifically, there are two typical discrimination schemes for nonorthogonal states: one is the minimum error discrimination [1] (also see [2] and references therein), where each measurement outcome selects one of the possible states and the error probability is minimized, and the other is the optimal unambiguous discrimination [3–5], where unambiguity is paid by the possibility of getting inconclusive results from the measurement. Besides, discrimination of quantum states has also been considered in the minimax approach [6], where there are no *a priori* probabilities, and one maximizes the smallest of the probabilities of correct detection. For a recent review on discrimination of quantum states, we would like to refer the reader to [7].

The problem of discrimination can also be applied to quantum operations. In [8–10], the authors considered discrimination between unitary transformations (special quantum operations), and they found that entanglement-assisted input cannot enhance the distinguishability of a pair of unitary transformations. For the problem of discriminating general quantum operations, however, there is not very much work, and the first work on this problem may be owed to Sacchi [11, 12], where the problem of discriminating two given general quantum operations was first formulated, and for Pauli channels, this problem was addressed in detail. Specially, Sacchi [11, 12] showed that unlike unitary transformations [8–10], entangled input states generally enhance the distinguishability of two general quantum operations. Also, Pauli channels, as a nontrivial kind of quantum operations, were considered by D'Ariano *et al* [13] in the approach of minimax discrimination. Recently, in [2] a general bound on the minimum error probability for discriminating arbitrary n quantum operations was obtained. In addition, the unambiguous scheme was also discussed for general quantum operations by Wang and Ying [14], where a necessary and sufficient condition was given for a given set of quantum operations to be unambiguously distinguishable. By the way, recently there is another interesting problem addressed by Chefles *et al* [15], which considered unambiguous discrimination among oracle operators. Notably, it is worth mentioning that some experimental schemes were recently proposed for discrimination of quantum operations in [16].

Despite some work as mentioned above, having been done on the discrimination of quantum operations, there are still some fundamental problems left open and further study is needed. For instance, so far we have not got a computable expression for the minimum error probability of discriminating two quantum operations, and not even for the simplest case—discriminating two single-qubit quantum operations. This problem is of course highly nontrivial in the study of discriminating quantum operations. Notably, a similar problem for the discrimination of quantum states has been successfully solved by Helstrom [1], where a general expression for the minimum error probability of discriminating two quantum states ρ_1 and ρ_2 (with *a priori* probabilities p_1 and p_2, respectively) is given as

$$P_E = \tfrac{1}{2}(1 - \|p_1\rho_1 - p_2\rho_2\|_1), \tag{1}$$

where $\|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A}$ denotes the trace norm of A. (If A is Hermitian, $\|A\|_1$ also equals the sum of the absolute value of the eigenvalues of A.) Recently, Qiu [2] derived a general bound on the minimum error probability for discriminating arbitrary n mixed states.

With these considerations in mind, in this paper we further consider the problem of discriminating quantum operations in the minimum error scheme. Generally, we should transform this problem to that of discriminating quantum states. Thus, a natural approach to discriminate two quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$ is to choose a suitable state ρ in the input Hilbert space $\mathcal{H}$, such that the error probability in the discrimination of the output states $\mathcal{E}_1(\rho)$ and $\mathcal{E}_2(\rho)$ is minimum. We call such a discrimination strategy a *non-entanglement strategy*. Besides, we have another more general strategy, called *entanglement strategy*, where we can introduce entanglement-assisted input states to increase the distinguishability of the output states. In this case, the output states to be discriminated will be of the form $(\mathcal{E}_1 \otimes \mathcal{I})\rho$ and $(\mathcal{E}_2 \otimes \mathcal{I})\rho$, where the input ρ is generally a bipartite state of $\mathcal{H}\otimes\mathcal{K}$, and the quantum operations act just on the first party whereas the identity map $\mathcal{I} = \mathcal{I}_{\mathcal{K}}$ acts on the second.

We denote with P_E the minimum error probability when the non-entanglement strategy is adopted. Then we have

$$P_E(\mathcal{E}_1, \mathcal{E}_2) = \tfrac{1}{2}\Big(1 - \max_{\rho\in\mathcal{H}} \|p_1\mathcal{E}_1(\rho) - p_2\mathcal{E}_2(\rho)\|_1\Big), \tag{2}$$

where p_1 and p_2 are the *a priori* probabilities for the quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$, respectively. On the other hand, by allowing the use of entanglement-assisted input, we have

$$P'_E(\mathcal{E}_1, \mathcal{E}_2) = \tfrac{1}{2}\Big(1 - \max_{\rho\in\mathcal{H}\otimes\mathcal{K}} \|p_1(\mathcal{E}_1 \otimes I)\rho - p_2(\mathcal{E}_2 \otimes I)\rho\|_1\Big). \tag{3}$$

Regarding (2) and (3), we mention the following two points. (i) In (3), we can simply let $\mathcal{H} = \mathcal{K}$, because it is known that [19] the maximum of the trace norm in (3) over all finite

Hilbert space $\mathcal{K}$ can be achieved when $\dim(\mathcal{H}) = \dim(\mathcal{K})$. (ii) By the linearity of quantum operations, the triangle inequality of the trace norm [20] and the spectral decomposition of quantum states, it is not difficult to see that the maximum in (2) and (3) can be achieved by pure states. For instance, by letting $\rho = \sum_i \lambda_i |i\rangle\langle i|$, we have

$$\begin{aligned} \|p_1\mathcal{E}_1(\rho) - p_2\mathcal{E}_2(\rho)\|_1 &= \left\| \sum_i \lambda_i (p_1\mathcal{E}_1(|i\rangle\langle i|) - p_2\mathcal{E}_2(|i\rangle\langle i|)) \right\|_1 \\ &\leqslant \sum_i \lambda_i \|p_1\mathcal{E}_1(|i\rangle\langle i|) - p_2\mathcal{E}_2(|i\rangle\langle i|)\|_1 \\ &\leqslant \max_{|i\rangle} \|p_1\mathcal{E}_1(|i\rangle\langle i|) - p_2\mathcal{E}_2(|i\rangle\langle i|)\|_1. \end{aligned} \tag{4}$$

Thus, in the following we only need to consider pure states as input states.

The remainder of this paper is organized as follows. In section 2, firstly we give an implicit expression (given by (10)) that can be used to evaluate the exact minimum error probability of discriminating any two single-qubit quantum operations by the non-entanglement strategy, and then by applying this result to the Pauli channels, we obtain a more intuitive and visual solution to their discrimination problem than that given in [11, 12]. In section 3, we give a necessary and sufficient condition for two given quantum operations to be perfectly distinguishable, and as an application, we further get that two generalized Pauli channels are perfectly distinguishable if and only if their characteristic vectors are orthogonal. Finally, some conclusions are made in section 4.

2. Discrimination of single-qubit quantum operations

As mentioned before, a computable expression for the minimum error probability of distinguishing two quantum operations, even restricted to the single-qubit quantum operations, has not been obtained. Thus in this section, we try to consider this by starting with the discrimination of single-qubit operations by the non-entanglement strategy. We think that this consideration will not lose significance, based on the following two points: (i) single-qubit quantum operations as the most basic but not trivial quantum operations are of great importance in quantum computation and quantum information; (ii) in a certain sense, the non-entanglement strategy may be the optimal one in practice, since this strategy does not need entangled input which as a valuable physical resource is generally difficult to prepare. Indeed, by making use of the Bloch representation [21] of single-qubit systems, we can evaluate the minimum error probability P_E (given by (2)) for any two single-qubit quantum operations as follows.

It is well known that the density operator ρ of a single-qubit system can always be written in the form

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}, \tag{5}$$

where $\vec{r} = (r_x, r_y, r_z)$ is a three-dimensional real vector with norm $\|\vec{r}\| \leqslant 1$ ($\|\cdot\|$ denotes the *Euclidean norm* on $\mathbf{C}^n$) and $\vec{r}\cdot\vec{\sigma} = r_x\sigma_x + r_y\sigma_y + r_z\sigma_z$ with $\{\sigma_x, \sigma_y, \sigma_z\}$ denoting the Pauli operators [21]. In this way, $\vec{r}$ is called the *Bloch vector* of ρ, and they have a one-to-one relation. Also, we have that ρ is a pure state if and only if $\|\vec{r}\| = 1$.

Based on the Bloch representation, we can visualize the effect of any trace-preserving single-qubit quantum operation $\mathcal{E}$ as the transformation of Bloch vectors

$$\vec{r} \to \vec{r} = M\vec{r} + \vec{c}, \tag{6}$$

where M is a 3×3 real matrix and $\vec{c}$ is a three-dimensional real vector, all of which can be computed from the operator-sum representation of $\mathcal{E}$. Therefore, the quantum operation $\mathcal{E}$ on a single qubit is characterized by the 2-tuple $(M, \vec{c})$. For the details, we refer to [21].

Next, we try to evaluate the minimum error probability of discriminating two single-qubit quantum operations. Before that, we give some useful results below.

First, we have

$$\tfrac{1}{2}(|a+b| + |a-b|) = \max\{|a|, |b|\}, \tag{7}$$

where a and b are any real numbers. This equation can be easily verified by discussing the two cases: $|a| \geqslant |b|$ and $|a| < |b|$.

Secondly, we have a useful lemma in the following.

Lemma 1. *Let ρ_1 and ρ_2 be the states of a single-qubit system with a priori probabilities p_1 and p_2, respectively. Let $\vec{r}_1$ and $\vec{r}_2$ be the Bloch vectors of ρ_1 and ρ_2, respectively. Then we have*

$$\|p_1\rho_1 - p_2\rho_2\|_1 = \max\{|p_1 - p_2|, \|p_1\vec{r}_1 - p_2\vec{r}_2\|\}. \tag{8}$$

Proof. First, we note that $\vec{r} \cdot \vec{\sigma}$ has eigenvalues $\pm\|\vec{r}\|$. Then, by the Bloch representation, we have

$$\begin{aligned}\|p_1\rho_1 - p_2\rho_2\|_1 &= \tfrac{1}{2}\|p_1(I + \vec{r}_1 \cdot \vec{\sigma}) - p_2(I + \vec{r}_2 \cdot \vec{\sigma})\|_1 \\ &= \tfrac{1}{2}\|(p_1 - p_2)I + (p_1\vec{r}_1 - p_2\vec{r}_2).\vec{\sigma}\|_1 \\ &= \tfrac{1}{2}(|a-b| + |a+b|),\end{aligned} \tag{9}$$

where we let $a = p_1 - p_2$ and $b = \|p_1\vec{r}_1 - p_2\vec{r}_2\|$. Therefore, by (7), we have completed the proof. □

Now, suppose that $\mathcal{E}_1$ and $\mathcal{E}_2$ are two single-qubit quantum operations, and by the Bloch representation, $\mathcal{E}_1$ and $\mathcal{E}_2$ correspond to $(M_1, \vec{c}_1)$ and $(M_2, \vec{c}_2)$, respectively. Then, the minimum error probability of discriminating $\mathcal{E}_1$ and $\mathcal{E}_2$ with the non-entanglement strategy can be evaluated as follows

$$\begin{aligned}P_E(\mathcal{E}_1, \mathcal{E}_2) &= \tfrac{1}{2}\Big(1 - \max_{|\psi\rangle\in\mathcal{H}} \|p_1\mathcal{E}_1(|\psi\rangle\langle\psi|) - p_2\mathcal{E}_2(|\psi\rangle\langle\psi|)\|_1\Big) \\ &= \tfrac{1}{2}\Big[1 - \max_{\|\vec{r}\|=1} \max\{|p_1 - p_2|, \|p_1(M_1\vec{r} + \vec{c}_1) - p_2(M_2\vec{r} + \vec{c}_2)\|\}\Big] \\ &= \tfrac{1}{2}\Big[1 - \max\{|p_1 - p_2|, \max_{\|\vec{r}\|=1} \|(p_1M_1 - p_2M_2)\vec{r} + (p_1\vec{c}_1 - p_2\vec{c}_2)\|\}\Big] \\ &= \tfrac{1}{2}\Big[1 - \max\{|p_1 - p_2|, \max_{\|\vec{r}\|=1} \|M\vec{r} + \vec{c}\|\}\Big],\end{aligned} \tag{10}$$

where we denote $(p_1M_1 - p_2M_2)$ and $(p_1\vec{c}_1 - p_2\vec{c}_2)$ by M and $\vec{c}$, respectively. Note that the value $\max_{\|\vec{r}\|=1} \|M\vec{r} + \vec{c}\|$ can be computed exactly for any fixed M and $\vec{c}$. Therefore, the minimum error probability $P_E(\mathcal{E}_1, \mathcal{E}_2)$ given above can be evaluated for any two given single-qubit quantum operations.

Below, we show explicitly how to compute the value $\max_{\|\vec{r}\|=1} \|M\vec{r} + \vec{c}\|$ by computing its square. Without loss of generality, suppose that

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \qquad \vec{c} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}, \qquad \vec{r} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}. \tag{11}$$

Then $\|M\vec{r}+\vec{c}\|^2 = f(x,y,z)$, where the function f is defined as

$$\begin{aligned} f(x,y,z) = {} & (a_{11}x + a_{12}y + a_{13}z + c_1)^2 + (a_{21}x + a_{22}y + a_{23}z + c_2)^2 \\ & + (a_{31}x + a_{32}y + a_{33}z + c_3)^2. \end{aligned} \tag{12}$$

The problem now reduces to finding out the maximal value of $f(x,y,z)$ under the constraint $x^2+y^2+z^2 = 1$. Clearly, this problem belongs to the class of *constrained extremum problems* [22], and we can solve it by the way of *Lagrange multipliers*. More specifically, we first define a Lagrange function as

$$L(x,y,z) = f(x,y,z) + \lambda(x^2+y^2+z^2-1), \tag{13}$$

where λ is a Lagrange multiplier and $f(x,y,z)$ is given by (12); then we have the following set of equations

$$\begin{cases} \dfrac{\partial L(x,y,z)}{\partial x} = 0, \\ \dfrac{\partial L(x,y,z)}{\partial y} = 0, \\ \dfrac{\partial L(x,y,z)}{\partial z} = 0, \\ x^2+y^2+z^2 = 1. \end{cases} \tag{14}$$

Now, there are four unknowns to be solved and four equations known to us. Thus, in principle, we can determine the values for the four unknowns x, y, z, λ, and then substituting these values into (12), we obtain the result. Therefore, $P_E(\mathcal{E}_1, \mathcal{E}_2)$ can be evaluated for any two given single-qubit quantum operations.

In the above process, we cannot provide a more concrete expression for $P_E(\mathcal{E}_1, \mathcal{E}_2)$ than equation (10), since in general we cannot present the solution of (14) in an explicit and succinct form. However, that does not matter and what is now important is that by (10) we can evaluate $P_E(\mathcal{E}_1, \mathcal{E}_2)$ for any two given single-qubit quantum operations. Of course, more concrete and succinct expressions can be given for some special cases as we will see soon.

There are some nontrivial special cases in (10) worthy of further explanation.

(i) For a general Bloch representation $(M, \vec{c})$ of single-qubit quantum operation $\mathcal{E}$, there is a nontrivial case where $\vec{c} = 0$ and then $\mathcal{E}$ is called *unital* (equivalently, $\mathcal{E}$ is called unital, if $\mathcal{E}(I) = I$). Indeed, unital operations attract considerable attention in the literature, for example in [17, 18]. Now for two unital operations $\mathcal{E}_1$ and $\mathcal{E}_2$ (with $\vec{c}_1 = \vec{c}_2 = 0$) to be distinguished, the minimum error probability can be evaluated as follows:

$$\begin{aligned} P_E(\mathcal{E}_1, \mathcal{E}_2) &= \tfrac{1}{2}[1 - \max\{|p_1 - p_2|, \max_{\|\vec{r}\|=1} \|(p_1M_1 - p_2M_2)\vec{r}\|\}] \\ &= \tfrac{1}{2}[1 - \max\{|p_1 - p_2|, \|p_1M_1 - p_2M_2\|_2\}], \end{aligned} \tag{15}$$

where $\|A\|_2$ denotes the *spectral norm* [20] of matrix A defined as

$$\begin{aligned} \|A\|_2 &= \max\{\sqrt{\lambda} : \lambda \text{ is an eigenvalue of } A^\dagger A\} \\ &= \max_{\|x\|=1} \|Ax\|. \end{aligned} \tag{16}$$

(ii) When $|p_1 - p_2| \geqslant \max_{\|\vec{r}\|=1} \|M\vec{r} + \vec{c}\|$, we have

$$P_E(\mathcal{E}_1, \mathcal{E}_2) = \min\{p_1, p_2\}, \tag{17}$$

which implies that in this case no input state and no measurements are needed, and the minimum error can always be achieved by just guessing the most likely operation. We note that similar insight was also gained for discrimination of quantum states by Rudin

[23], who found that for some set of states, measurement does not aid minimum error discrimination, and the minimum error probability can always be achieved by guessing the most likely state.

In [21], some important single-qubit quantum operations were introduced, and they are bit flip, phase flip, bit–phase flip, depolarizing, phase damping and amplitude damping channels. One can refer to [21] for their operator-sum representations, and below we visualize them as the Bloch vector transformations in turn:

$$\begin{aligned}
BF &: (r_x, r_y, r_z) \to (r_x, (2p-1)r_y, (2p-1)r_z),\\
PF &: (r_x, r_y, r_z) \to ((2p-1)r_x, (2p-1)r_y, r_z),\\
BPF &: (r_x, r_y, r_z) \to ((2p-1)r_x, r_y, (2p-1)r_z),\\
DE &: (r_x, r_y, r_z) \to ((1-p)r_x, (1-p)r_y, (1-p)r_z),\\
PD &: (r_x, r_y, r_z) \to (r_x\sqrt{1-\lambda}, r_y\sqrt{1-\lambda}, r_z),\\
AD &: (r_x, r_y, r_z) \to (r_x\sqrt{1-\lambda}, r_y\sqrt{1-\lambda}, r_z(1-\lambda)+\lambda).
\end{aligned} \tag{18}$$

Therefore, by using (10) (or (15)) and the above transformations, it is easy to get the minimum error probability of discriminating the above quantum operations.

In fact, bit flip, phase flip, bit–phase flip and depolarizing channels are generalized by the more general quantum operations—Pauli channels defined as

$$\mathcal{E}(\rho) = \sum_{i=0}^{3} q_i \sigma_i \rho \sigma_i, \tag{19}$$

where $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\} = \{I, \sigma_x, \sigma_y, \sigma_z\}$, $\sum_i q_i = 1$ and $q_i \geqslant 0$ for any i. Discrimination of Pauli channels was discussed in detail for both entanglement strategy and non-entanglement strategy by Sacchi [11, 12], and the minimum error probability $P_E(\mathcal{E}_1, \mathcal{E}_2)$ for them was derived by an elaborate calculation. However, below we will give a more intuitive and visual derivation of $P_E(\mathcal{E}_1, \mathcal{E}_2)$, based on the Bloch representation. At starting, we give a lemma as follows.

Lemma 2. *Let $\mathcal{E}(\rho) = \sum_{i=0}^{3} q_i \sigma_i \rho \sigma_i$ be a Pauli channel. Then $\mathcal{E}$ corresponds to this Bloch vector transformation*

$$\vec{r} \to \vec{r}\,' = M\vec{r}, \tag{20}$$

where $M = \mathrm{diag}\{\Delta_1, \Delta_2, \Delta_3\}$ and $\Delta_i = 2(q_0 + q_i) - 1$.

Proof. First, note that for the Pauli operators, we have

$$\sigma_i \sigma_j \sigma_i = \begin{cases} -\sigma_j & j \neq i \\ \sigma_j & j = i, \end{cases}$$

for $i, j = 1, 2, 3$. Then we get that

$$\begin{aligned}
\mathcal{E}(\rho) &= \sum_{i=0}^{3} q_i \sigma_i \frac{I + \vec{r}\cdot\vec{\sigma}}{2} \sigma_i\\
&= \frac{1}{2}[I + (q_0 + q_1 - q_2 - q_3) r_1 \sigma_1 + (q_0 - q_1 + q_2 - q_3) r_2 \sigma_2 + (q_0 - q_1 - q_2 + q_3) r_3 \sigma_3]\\
&= \frac{1}{2}[I + (M\vec{r})\cdot\vec{\sigma}],
\end{aligned} \tag{21}$$

where M is defined as above. This completes the proof. □

Now, for the two Pauli channels

$$\mathcal{E}_1(\rho) = \sum_{i=0}^{3} q_i^{(1)} \sigma_i \rho \sigma_i \qquad \text{and} \qquad \mathcal{E}_2(\rho) = \sum_{i=0}^{3} q_i^{(2)} \sigma_i \rho \sigma_i, \tag{22}$$

by lemma 2, we know that $\mathcal{E}_1$ and $\mathcal{E}_2$ have 2-tuple representations $(M_1, \vec{0})$ and $(M_2, \vec{0})$, respectively. Then by (15), we have

$$\begin{aligned} P_E(\mathcal{E}_1, \mathcal{E}_2) &= \tfrac{1}{2}[1 - \max\{|p_1 - p_2|, \|p_1 M_1 - p_2 M_2\|_2\}] \\ &= \tfrac{1}{2}[1 - \max\{|p_1 - p_2|, C\}], \end{aligned} \tag{23}$$

where

$$C = \max\{|r_0 + r_1 - r_2 - r_3|, |r_0 + r_2 - r_1 - r_3|, |r_0 + r_3 - r_1 - r_2|\}, \tag{24}$$

and $r_i = p_1 q_i^{(1)} - p_2 q_i^{(2)}$ for $i = 0, 1, 2, 3$.

In (23), if $C \leqslant |p_1 - p_2|$, then $P_E = \min\{p_1, p_2\}$, and thus no exploring input state is needed as pointed out before. Else, the optimal exploring input state has the Bloch vector that is the eigenvector corresponding to the eigenvalue of $p_1 M_1 - p_2 M_2$ having the largest absolute value.

We mention that discrimination of Pauli channels was also discussed in [11, 12], where the minimum error probability in the non-entanglement strategy was given as

$$P_E = \tfrac{1}{2}(1 - M), \tag{25}$$

where

$$M = \max\{|r_0 + r_3| + |r_1 + r_2|, |r_0 + r_1| + |r_2 + r_3|, |r_0 + r_2| + |r_1 + r_3|\}. \tag{26}$$

In fact, one can verify that (23) and (25) are equivalent by using (7) and by noting that $p_1 - p_2 = r_0 + r_1 + r_2 + r_3$. However, as we can see, our method is based on the Bloch representation of single-qubit systems, and thus, it is more intuitive and visual than the way used in [11, 12], where an elaborate calculation was required.

3. Perfect discrimination of quantum operations

In this section, we consider the condition for perfect discrimination of two quantum operations, and we give a result as follows.

Theorem 1. *Given two quantum operations*

$$\mathcal{E}_1(\rho) = \sum_{i=1}^{n_1} E_i^{(1)} \rho E_i^{(1)\dagger} \qquad \textit{and} \qquad \mathcal{E}_2(\rho) = \sum_{j=1}^{n_2} E_j^{(2)} \rho E_j^{(2)\dagger}, \tag{27}$$

we have

(i) $\mathcal{E}_1$ *and* $\mathcal{E}_2$ *are perfectly distinguishable with the non-entanglement strategy iff there exists a state* $|\psi\rangle \in \mathcal{H}$ *such that* $\langle\psi|E_i^{(1)\dagger} E_j^{(2)}|\psi\rangle = 0$ *for all* i, j.

(ii) $\mathcal{E}_1$ *and* $\mathcal{E}_2$ *are perfectly distinguishable with the entanglement strategy iff there exists a state* $\rho \in \mathcal{H}$ *such that* $\mathrm{Tr}\big(\rho E_i^{(1)\dagger} E_j^{(2)}\big) = 0$ *for all* i, j.

Proof. We first verify part (i). From the discussion in section 1, we know that $\mathcal{E}_1$ and $\mathcal{E}_2$ are perfectly distinguishable if and only if there exists a pure state $|\psi\rangle \in \mathcal{H}$, such that the output density operators are mutually orthogonal, i.e., they have mutual orthogonal support. The support of the density operator ρ, denoted by supp(ρ), is defined as the space spanned by the eigenvectors corresponding to the no-zero eigenvalues of ρ. We denote

$$\begin{aligned} \rho_1 &\equiv \mathcal{E}_1(|\psi\rangle\langle\psi|) = \sum_{i=1}^{n_1} E_i^{(1)}|\psi\rangle\langle\psi|E_i^{(1)\dagger}, \\ \rho_2 &\equiv \mathcal{E}_2(|\psi\rangle\langle\psi|) = \sum_{j=1}^{n_2} E_j^{(2)}|\psi\rangle\langle\psi|E_j^{(2)\dagger}. \end{aligned} \tag{28}$$

Then it follows that

$$\begin{aligned} \mathrm{supp}(\rho_1) &= \mathrm{span}\big\{E_i^{(1)}|\psi\rangle : i = 1, \ldots, n_1\big\}, \\ \mathrm{supp}(\rho_2) &= \mathrm{span}\big\{E_j^{(2)}|\psi\rangle : j = 1, \ldots, n_2\big\}. \end{aligned} \tag{29}$$

Hence it is readily seen that $\mathrm{supp}(\rho_1) \perp \mathrm{supp}(\rho_2)$ if and only if $E_i^{(1)}|\psi\rangle \perp E_j^{(2)}|\psi\rangle$, i.e., $\langle\psi|E_i^{(1)\dagger}E_j^{(2)}|\psi\rangle = 0$ for all i, j.

When the entanglement strategy is considered, we can similarly get the condition that there exists a state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ such that $\langle\psi|E_i^{(1)\dagger}E_j^{(2)} \otimes I|\psi\rangle = 0$ for all i and j, which is equivalent to that given in part (ii), by noting that $|\psi\rangle$ has the Schmidt decomposition $|\psi\rangle = \sum_k \sqrt{\lambda_k}|k\rangle|k\rangle$ and

$$\begin{aligned} \langle\psi|E_i^{(1)\dagger}E_j^{(2)} \otimes I|\psi\rangle &= \sum_k \lambda_k\langle k|E_i^{(1)\dagger}E_j^{(2)}|k\rangle \\ &= \mathrm{Tr}\big(\rho E_i^{(1)\dagger}E_j^{(2)}\big), \end{aligned} \tag{30}$$

where $\rho = \sum_k \lambda_k|k\rangle\langle k|$. This completes the proof. □

In theorem 1, it is easy to see that if two quantum operations are perfectly distinguishable by the non-entanglement strategy, then they must be perfectly distinguishable by the entanglement strategy, and the contrary implication, however, is not true.

Notably, when two unitary operations U_1 and U_2 are considered, the condition for perfect discrimination between them reduces to $\langle\psi|U_1^\dagger U_2|\psi\rangle = 0$ for some input state $|\psi\rangle \in \mathcal{H}$, i.e., the polygon of the eigenvalues of $U_1^\dagger U_2$ encircles the origin, which was discussed in [9, 10].

The condition given in theorem 1, in mathematics, is equivalent to decide if a set of matrices have a *common isotropic vector*[1], which is generally a difficult problem, and one may use the theory of *numerical range* [24] to study that. Thus, it is generally difficult to decide if two quantum operations are perfectly distinguishable. However, it will become easy in some special cases as we will show below.

In the following, we consider the condition for two Pauli channels to be perfectly distinguishable. For that, we discuss a more general case—discriminating the following quantum operations [11, 12]:

$$\mathcal{E}_i(\rho) = \sum_{n=0}^{d^2-1} q_n^{(i)} U_n\rho U_n^\dagger, \qquad \sum_n q_n^{(i)} = 1 \qquad \text{and} \qquad q_n^{(i)} \geqslant 0, \tag{31}$$

with $\mathrm{Tr}\big(U_m^\dagger U_n\big) = \mathrm{d}\delta_{mn}$. From the above form, we know that $\mathcal{E}_i$ has an operator-sum element set $\Big\{\sqrt{q_n^{(i)}}U_n\Big\}$. Also, we can see that when the orthogonal set $\{U_n\}$ is fixed, $\mathcal{E}_i$ is uniquely determined by the unit d^2-dimensional vector $\mathbf{q^{(i)}} = \Big(\sqrt{q_0^{(i)}}, \ldots, \sqrt{q_{d^2-1}^{(i)}}\Big)$, which is called

[1] A set of matrices $\{A_i\}$ are said to have a common isotropic vector if there exists a nozero vector $x \in \mathbf{C}^n$ such that $x^\dagger A_i x = 0$ for all i [24].

the *characteristic vector* of $\mathcal{E}_i$. As we can see, when $d = 2$, these operations reduce to the Pauli channels. Thus, we call these quantum operations defined above *general Pauli channels* (GPCs). Now by theorem 1, we have the following result for these general Pauli channels.

Corollary 1. *Two GPCs $\mathcal{E}_1$ and $\mathcal{E}_2$ are perfectly distinguishable with the entanglement strategy iff their characteristic vectors are orthogonal.*

Proof. Suppose that $\mathcal{E}_1$ and $\mathcal{E}_2$ have characteristic vectors $\mathbf{q}^{(1)} = \left[\sqrt{q_i^{(1)}}\right]$ and $\mathbf{q}^{(2)} = \left[\sqrt{q_i^{(2)}}\right]$, respectively. Then from theorem 1, we know that $\mathcal{E}_1$ and $\mathcal{E}_2$ are perfectly distinguishable with the entanglement strategy iff the following

$$\sqrt{q_i^{(1)} q_j^{(2)}}\langle\psi|U_i^{\dagger}U_j \otimes I|\psi\rangle = 0 \tag{32}$$

holds for $i, j = 0, \ldots, d^2 - 1$ and some $|\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$. Let $i = j$ in (32). Then we have

$$\sqrt{q_i^{(1)} q_i^{(2)}} = 0, \qquad \text{for} \quad i = 0, \ldots, d^2 - 1, \tag{33}$$

which is equivalent to $\mathbf{q}^{(1)} \perp \mathbf{q}^{(2)}$. Now we have verified the necessity.

Next, suppose that $\mathbf{q}^{(1)} \perp \mathbf{q}^{(2)}$ holds, i.e., (33) holds. Then for any i, j, by inputting the maximal entangled state $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle|k\rangle$, we immediately have

$$\begin{aligned}
\sqrt{q_i^{(1)} q_j^{(2)}}\langle\psi|U_i^{\dagger}U_j \otimes I|\psi\rangle &= \frac{1}{d}\sqrt{q_i^{(1)} q_j^{(2)}}\sum_k \langle k|U_i^{\dagger}U_j|k\rangle \\
&= \frac{1}{d}\sqrt{q_i^{(1)} q_j^{(2)}}\,\mathrm{Tr}\big(U_i^{\dagger}U_j\big) \\
&= \sqrt{q_i^{(1)} q_j^{(2)}}\delta_{ij} \\
&= 0.
\end{aligned} \tag{34}$$

Thus, from theorem 1, $\mathcal{E}_1$ and $\mathcal{E}_2$ are perfectly distinguishable by the maximal entangled state $|\psi\rangle$. This completes the proof. □

Notably, the condition given in the above theorem is also a necessary condition for $\mathcal{E}_1$ and $\mathcal{E}_2$ to be perfectly distinguishable with the non-entanglement strategy. However, it is not sufficient. An example of this case is the two channels of this form [12]:

$$\mathcal{E}_1(\rho) = \sum_{\alpha\neq\beta} q_\alpha\sigma_\alpha\rho\sigma_\alpha, \qquad \mathcal{E}_2(\rho) = \sigma_\beta\rho\sigma_\beta, \tag{35}$$

with $q_\alpha \neq 0$.

4. Conclusions

In this work, we addressed the problem of discriminating two given quantum operations. For the single-qubit quantum operations, we obtained an implicit expression that can be used to evaluate the minimum error probability of discriminating any two single-qubit quantum operations when the non-entanglement strategy is adopted. For the Pauli channels discussed in [11, 12], we gave a more intuitive and visual solution to their discrimination problem. Also, we gave a necessary and sufficient condition for two quantum operations to be perfectly distinguishable, and as an application, we found that two generalized Pauli channels are perfectly distinguishable if and only if their characteristic vectors are orthogonal.

Acknowledgments

We are very grateful to the referees for their invaluable comments and suggestions that helped us improve the presentation of this paper. This work is supported by the National Natural Science Foundation (nos. 90303024, 60573006), the Research Foundation for the Doctorial Program of Higher School of Ministry of Education (no. 20050558015) and Program for New Century Excellent Talents in University (NCET) of China.

References

[1] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)
[2] Qiu D W 2008 *Phys. Rev.* A **77** 012328
[3] Ivanovic I D 1987 *Phys. Lett.* A **123** 257
Dieks D 1988 *Phys. Lett.* A **126** 303
Peres A 1988 *Phys. Lett.* A **128** 19
Jaeger G and Shimony A 1995 *Phys. Lett.* A **197** 83
Chefles A 1998 *Phys. Lett.* A **239** 339
[4] Zhang C W, Li C F and Guo G C 1999 *Phys. Lett.* A **261** 25
[5] Qiu D W 2003 *Phy. Lett.* A **303** 140
Qiu D W 2003 *Phy. Lett.* A **309** 189
[6] D'Ariano G M, Sacchi M F and Kahn J 2005 *Phys. Rev.* A **72** 032310
[7] Bergou J A, Herzog U and Hillery M 2004 *Quantum State Estimation* (Berlin: Springer) p 417
Chefles A 2004 *Quantum State Estimation* (Berlin: Springer) p 467
[8] Childs A M, Preskill J and Renes J 2000 *J. Mod. Opt.* **47** 155
[9] Acín A 2001 *Phys. Rev. Lett.* **87** 177901
[10] D'Ariano G M, Presti P Lo and Paris M G A 2001 *Phys. Rev. Lett.* **87** 270404
[11] Sacchi M F 2005 *J. Opt. B: Quantum Semiclass. Opt.* B **7** S333
[12] Sacchi M F 2005 *Phys. Rev.* A **71** 062340
[13] D'Ariano G M, Sacchi M F and Kahn J 2005 *Phys. Rev.* A **72** 052302
[14] Wang G and Ying M 2006 *Phys. Rev.* A **73** 042301
[15] Chefles A, Kitagawa A, Takeoka M, Sasaki M and Twamley J 2007 *J. Phys. A: Math. Theor.* **40** 10183 (*Preprint* quant-ph/0702245v3)
[16] Laing A, Rudolph T and O'Brien J L 2008 *Preprint* arXiv:0801.3831
Zhang P, Peng L, Wang Z W, Ren X F, Liu B H, Huang Y F and Guo G C 2008 *Preprint* arXiv:0801.3493
[17] Bourdon P S and Williams H T 2004 *Phys. Rev.* A **69** 022314
[18] King C and Ruskai M B 2001 *IEEE Trans. Inf. Theory* **47** 192
[19] Paulsen V I 1986 *Completely Bounded Maps and Dilations* (New York: Longman Scientific and Technical)
[20] Horn R A and Johnson C R 1986 *Matrix Analysis* (Cambridge: Cambridge University Press)
[21] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[22] Rudin W 1976 *Principles of Mathematical Analysis* (New York: McGraw-Hill)
[23] Hunter K 2003 *Phys. Rev.* A **68** 012306
[24] Horn R A and Johnson C R 1991 *Topics in Matrix Analysis* (Cambridge: Cambridge University Press)