DISCRIMINATION AND CERTIFICATION OF UNKNOWN QUANTUM MEASUREMENTS

ALEKSANDRA KRAWIEC[1,*], ŁUKASZ PAWELA[1], AND ZBIGNIEW PUCHAŁA[1]

Abstract. We study the discrimination of von Neumann measurement in the scenario when we are given a reference measurement and some other measurement. The aim of the discrimination is to determine whether the other measurement is the same as the first one. We consider the cases when the reference measurement is given without the classical description and when its classical description is known. Both cases are studied in the symmetric and asymmetric discrimination setups. Moreover, we provide optimal certification schemes enabling us to certify a known quantum measurement against the unknown one.

1. Introduction

The need for appropriate certification tools is one of the barriers to the development of large-scale quantum technologies. [1] In this work, we propose tests that verify if a given device corresponds to its classical description or the reference device.

But why should we care about the discrimination of devices which description we do not know? A lot is known about discrimination of quantum states, channels and measurements, which description we do know. In the standard discrimination problem, there are two quantum objects, and one of them is secretly chosen. The goal of discrimination is to decide which of the objects was chosen. These objects can be quantum states but also quantum channels and measurements. However, what if we were given a reference quantum measurement or channel instead of its classical description? Then we may want to discriminate them regardless of their classical descriptions. Therefore, we arrive at the new problem of discrimination of unknown objects.

Discrimination of known quantum channels was mainly studied for certain classes of channels like unitary channels [2–4]. Advantage of using entangled states for minimum-error discrimination of quantum channels was studied in [5, 6]. General conditions when quantum channels can be discriminated in the minimum error, unambiguous and asymmetric scenarios were derived in [7], [8] and [9] respectively. Another formalism used for for studying discrimination of quantum channels is based on process POVM (PPOVM) [10]. It was applied to discrimination of unitary channels in [11, 12].

Discrimination of unknown unitary channels was first studied in the work [13] in both minimum-error and unambiguous setups. The authors calculated that the probability of successful minimum-error discrimination between two random qubit unitary channels

[1] Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, ul. Bałtycka 5, 44-100 Gliwice, Poland

E-mail address: akrawiec@iitis.pl.

Date: January 13, 2023.

equals 7/8 and they made use of the input state $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The authors of [14] proved that the probability 7/8 is optimal in the sense that it cannot be improved by the use of any (even adaptive) discrimination strategy for the qubit case. Recent results concerning discrimination of unknown unitary channels can be found in [15].

Minimum error discrimination of quantum measurements was studied in single-shot [16] and multiple-shot [17] regimes. Asymmetric discrimination of von Neumann measurements was studied in [18] The advantage of using entangled stated for single-shot discrimination between qubit measurements was experimentally shown in [19]. Application of process POVMs for discrimination of quantum measurements can be found in [20, 21]

In this work we study discrimination of unknown von Neumann measurements in symmetric and asymmetric scenarios. We begin with preliminaries in Section 2 and detailed setups for symmetric and asymmetric discrimination of quantum measurements will be presented therein. Next, we will study the problem when one of the measurements is given without classical description and we want to verify if the other measurement is a copy of the same measurements or it is some other one. This problem will be studied in Section 3. Later, we will assume that one copy of a measurement is given with its classical description and we want to know whether the other measurement is a copy of the same measurement. This problem will be studied in Section 4. We will conclude in Section 5.

2. Preliminaries

Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be Hilbert spaces where $\dim(\mathcal{X}) = \dim(\mathcal{Y}) = d$, $\dim(\mathcal{Z}) = d^2$. Let $\mathcal{L}(\mathcal{X})$ be a set of linear operators acting from $\mathcal{X}$ to $\mathcal{X}$. Let $\mathcal{U}(\mathcal{X})$ denote the set of unitary operators. Let $\mathcal{D}(\mathcal{X})$ denote the set of quantum states, $\mathcal{C}(\mathcal{X})$ denote the set of quantum channels and $\mathcal{T}(\mathcal{X})$ denote the set of quantum operations. For $U \in \mathcal{U}(\mathcal{X})$, a unitary channel will be denoted $\Phi_U(\cdot) \coloneqq U \cdot U^\dagger$. We will also utilize two special quantum channels. The first one is the depolarizing channel, which transforms every quantum state into the maximally mixed state. Formally, it is defined for $X \in \mathcal{L}(\mathcal{X})$ as

$$\Phi_*(X) \coloneqq \mathrm{Tr}(X)\frac{\mathbb{1}}{\dim(\mathcal{X})}.$$

The second one is the dephasing channel defined as

$$\Delta(X) \coloneqq \sum_i |i\rangle\langle i|X|i\rangle\langle i|.$$

A quantum measurement is defined as a collection of positive semidefinite operator $\mathcal{P} = \{E_1, \ldots, E_m\}$ which satisfy $\sum_{i=1}^m = \mathbb{1}$, where $\mathbb{1}$ is the identity operator. Operators E_i are called effects. When a quantum state ρ is measured by the measurement $\mathcal{P}$, then we obtain a label i with probability $p(i) = \mathrm{tr}(E_i\rho)$ and the state ρ ceases to exist. We will be particularly interested in von Neumann measurements, which effects are of the form $\mathcal{P}_U = \{|u_1\rangle\langle u_1|, \ldots, |u_d\rangle\langle u_d|\}$, where $|u_i\rangle = U|i\rangle$ is the i-th column of the unitary matrix U. Every quantum measurement can be associated with a quantum channel

$$\mathcal{P}(\rho) = \sum_i |i\rangle\langle i| \,\mathrm{tr}(E_i\rho), \tag{1}$$

which outputs a diagonal matrix where i-th entry on the diagonal corresponds to the probability of obtaining i-th label.

The Choi-Jamiołkowski representation of quantum operation $\Psi \in \mathcal{T}(\mathcal{X})$ is defined as $J(\Psi) \coloneqq (\Psi \otimes \mathbb{1}_{\mathcal{X}})(|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|)$, where $\mathbb{1}_{\mathcal{X}}$ is the identity channel on the space $\mathcal{L}(\mathcal{X})$ and $|X\rangle\rangle$ denotes the (lexicographical) vectorization of the operator X.

The diamond norm of a quantum operation $\Psi \in \mathcal{T}(\mathcal{X})$ is defined as

$$\|\Psi\|_\diamond \coloneqq \max_{X:\|X\|_1=1} \|(\Psi \otimes \mathbb{1}_{\mathcal{X}})(X)\|_1, \tag{2}$$

where $\mathbb{1}_{\mathcal{X}}$ is, as previously, the identity channel on the space $\mathcal{L}(\mathcal{X})$. We will often use the bounds on the diamond norm [22, 23]

$$\frac{1}{d}\|J(\Psi)\|_1 \le \|\Psi\|_\diamond \le \| \operatorname{Tr}_1 |J(\Psi)|\|. \tag{3}$$

In this work we will focus on two approaches to discrimination of quantum measurements, which are symmetric and asymmetric discrimination.

2.1. **Symmetric discrimination.** The goal of symmetric discrimination is to maximize the probability of correct discrimination. It is also known as minimum-error discrimination. The schematic representation of symmetric discrimination of quantum measurements is depicted in Figure 1.

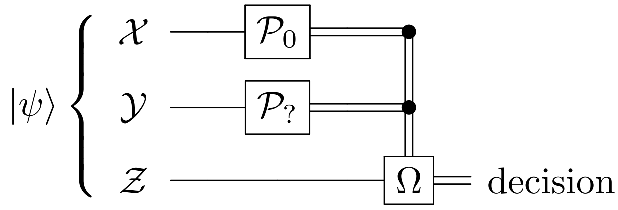

FIGURE 1. Entanglement-assisted discrimination of von Neumann measurements

There are two black boxes. In the first black box there is a measurement $\mathcal{P}_0$. In the second box there is a measurement $\mathcal{P}_?$, which can either the same measurement $\mathcal{P}_0$, or some other measurement, $\mathcal{P}_1$. In other words $\mathcal{P}_? \in \{\mathcal{P}_0, \mathcal{P}_1\}$. As the input state to the discrimination procedure we take a state $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$ and we will write $\psi \coloneqq |\psi\rangle\langle\psi|$ for the sake of simplicity. The measurement in the first black box acts on the register $\mathcal{X}$ and the second black box acts on the register $\mathcal{Y}$. Basing on the outcomes of both measurements in the black boxes, we prepare a final measurement on the register $\mathcal{Z}$. Having the output of the final register, we make a decision whether $\mathcal{P}_? = \mathcal{P}_0$ or $\mathcal{P}_? = \mathcal{P}_1$.

To calculate the probability of the successful discrimination between quantum measurements, we will make use of the Holevo-Helstrom theorem. It states that the optimal probability of successful discrimination between any quantum channels Ψ_0 and $\Psi_1 \in \mathcal{C}(\mathcal{X})$ is upper-bounded by

$$p_{succ} \le \frac{1}{2} + \frac{1}{4}\|\Psi_0 - \Psi_1\|_\diamond \tag{4}$$

and this bound can be saturated. This optimal probability of successful discrimination will be denoted $p_{succ}^H \coloneqq \frac{1}{2} + \frac{1}{4}\|\Psi_0 - \Psi_1\|_\diamond$.

2.2. **Asymmetric discrimination.** Asymmetric discrimination is based on hypothesis testing. The null hypothesis H_0 corresponds to the situation when $\mathcal{P}_? = \mathcal{P}_0$. The converse situation, $\mathcal{P}_? = \mathcal{P}_1$ corresponds to alternative hypothesis H_1. The scheme of asymmetric discrimination is as follows. We begin with preparing an input state $|\psi\rangle \in \mathcal{L}(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z})$ and apply $\mathcal{P}_0$ and $\mathcal{P}_?$ on registers $\mathcal{X}$ and $\mathcal{Y}$ respectively. Therefore, in the case when $\mathcal{P}_? = \mathcal{P}_0$, we obtain as the output $(\mathcal{P}_0 \otimes \mathcal{P}_0 \otimes \mathbb{1})(\psi)$ and if $\mathcal{P}_? = \mathcal{P}_1$, then the output state yields $(\mathcal{P}_0 \otimes \mathcal{P}_1 \otimes \mathbb{1})(\psi)$. Having the output states, we prepare a binary measurement $\{\Omega, \mathbb{1} - \Omega\}$, where the effect Ω accepts the null hypothesis and the effect $\mathbb{1} - \Omega$ accepts the alternative hypothesis.

The type I error (false positive) happens when we reject the correct null hypothesis. When the input state ψ and measurement Ω are fixed, then the probability of making the type I error is given by the expression

$$p_{\mathrm{I}}^{(\psi,\Omega)} := \mathrm{Tr}\left((\mathbb{1} - \Omega)\left(\mathcal{P}_0 \otimes \mathcal{P}_0 \otimes \mathbb{1}\right)(\psi)\right) = 1 - \mathrm{Tr}\left(\Omega\left(\mathcal{P}_0 \otimes \mathcal{P}_0 \otimes \mathbb{1}\right)(\psi)\right). \tag{5}$$

The optimized probability of the type I error yields

$$p_{\mathrm{I}} := \min_{\psi,\Omega} p_{\mathrm{I}}^{(\psi,\Omega)} \tag{6}$$

The probability of making the type II error (also known as false negative) for fixed input state and measurement equals

$$p_{\mathrm{II}}^{(\psi,\Omega)} = \mathrm{Tr}\left(\Omega\left(\mathcal{P}_0 \otimes \mathcal{P}_1 \otimes \mathbb{1}\right)(\psi)\right) \tag{7}$$

and corresponds to the situation when we accept the null hypothesis when the alternative one was correct. The optimized probability of making the type II error yields

$$p_{\mathrm{II}} := \min_{\psi,\Omega} p_{\mathrm{II}}^{(\psi,\Omega)}. \tag{8}$$

For both symmetric and asymmetric schemes we will study two cases. First we will assume that both measurements are unknown. Later, we will assume that we know the description of the reference measurement and the other measurement is unknown. We will be also interested whether the additional register is necessary for optimal discrimination. The summary of results is presented in the following table.

	p^H_{succ}	p^H_{err}	p_{I}	p_{II}	additional register
both unknown	$\frac{1}{2} + \frac{1}{2d}$	$\frac{1}{2} - \frac{1}{2d}$	0	$1 - \frac{1}{d}$	no
one fixed	$1 - \frac{1}{2d}$	$\frac{1}{2d}$	0	$\frac{1}{d}$	yes

Table 1. Summary of for symmetric and asymmetric discrimination of unknown von Neumann measurements

3. Discrimination of both unknown von Neumann measurements

In this section we will study a situation when we are given a von Neumann measurement $\mathcal{P}_0$ but no classical description of it. This measurement will be our reference. We also have another von Neumann measurement $\mathcal{P}_1$, which can be the same as the reference one, but it does not have to. In this section we will study the problem how to verify whether the second measurement is the same as the first one or not. Similar problem of discrimination of both unknown unitary channels was recently studied in [15].

3.1. **Symmetric discrimination.** We will be calculating the success probability for the discrimination of von Neumann measurements in the scenario depicted in Fig. 1. Therefore we will be actually discriminating between $\mathcal{P}_0 \otimes \mathcal{P}_0$ and $\mathcal{P}_0 \otimes \mathcal{P}_1$ in the entanglement-assisted scenario. Thus, in order to use Holevo-Helstrom theorem we will need to calculate the value of the diamond norm. As we do not have classical description of either $\mathcal{P}_0$ or $\mathcal{P}_1$, we will assume that both measurement are Haar-random, that is we will be discriminating between $\int \mathcal{P}_U \otimes \mathcal{P}_U dU$ and $\int \mathcal{P}_U \otimes \mathcal{P}_V dUdV$. The probability of successful discrimination is formulated as the following theorem.

Theorem 1. Let $\mathcal{P}_0$ be a reference von Neumann measurement of dimension d given without classical description. Let $\mathcal{P}_1$ be another von Neumann measurement of the same dimension, also given without classical description. The optimal probability of correct verification if $\mathcal{P}_1$ is the same as the reference channel in the scheme described in Subsection 2.1 equals

$$p^H_{succ} = \frac{1}{2} + \frac{1}{2d}. \tag{9}$$

Remark 1. The above theorem is a direct application of Holevo-Helstrom Theorem (see Eq. (4)) for discrimination between channels $\int \mathcal{P}_U \otimes \mathcal{P}_U dU$ and $\int \mathcal{P}_U \otimes \mathcal{P}_V dUdV$, that is

$$p^H_{succ} = \frac{1}{2} + \frac{1}{4}\left\| \int \mathcal{P}_U \otimes \mathcal{P}_U dU - \int \mathcal{P}_U \otimes \mathcal{P}_V dUdV \right\|_\diamond = \frac{1}{2} + \frac{1}{2d}. \tag{10}$$

Proof. Let $U \in \mathcal{U}(\mathcal{X})$, $V \in \mathcal{U}(\mathcal{Y})$ be unitary operators and $\dim(\mathcal{X}) = \dim(\mathcal{Y}) = d$. The probability of successful discrimination is given by the Holevo-Helstrom theorem. To calculate this probability (Eq. (4)), we need to calculate the diamond norm distance between the averaged channels

$$\left\| \int \mathcal{P}_U \otimes \mathcal{P}_U dU - \int \mathcal{P}_U \otimes \mathcal{P}_V dUdV \right\|_\diamond . \tag{11}$$

As the von Neumann measurement $\mathcal{P}_U$ can be seen as $\Delta\Phi_{U^\dagger}$, where Δ is a dephasing channel defined in Eq. (2), we will actually be discriminating between

$$\int (\Delta \otimes \Delta)(\Phi_{U^\dagger} \otimes \Phi_{U^\dagger}) dU \quad \text{and} \quad \int (\Delta \otimes \Delta)(\Phi_{U^\dagger} \otimes \Phi_{V^\dagger}) dUdV. \tag{12}$$

Using [24, 25] we calculate the Choi-Jamiołkowski representations of averaged unitary channels

$$\begin{aligned} J\left(\int \Phi_U \otimes \Phi_U dU\right) &= \frac{1}{d^2-1}\left(\mathbb{1} \otimes \mathbb{1} + S \otimes S\right) - \frac{1}{d(d^2-1)}\left(S \otimes \mathbb{1} + \mathbb{1} \otimes S\right), \\ J\left(\int \Phi_U \otimes \Phi_V dUdV\right) &= \frac{1}{d^2}\mathbb{1} \otimes \mathbb{1}, \end{aligned} \tag{13}$$

where, unless said otherwise, S is the Swap matrix of dimension d^2 and identity matrices $\mathbb{1}$-s are also of dimension d^2.

Using the above, we can calculate the Choi-Jamiołkowski representations of the averaged measurements, that is

$$J\left(\int \mathcal{P}_U \otimes \mathcal{P}_U dU\right) = \frac{1}{d^2-1}\left(\mathbb{1} \otimes \left(\mathbb{1} - \frac{1}{d}S\right) + T \otimes \left(S - \frac{1}{d}\mathbb{1}\right)\right) \tag{14}$$

where $T \coloneqq \Delta(S)$, and

$$J\left(\int \mathcal{P}_U \otimes \mathcal{P}_V dUdV\right) = \frac{1}{d^2}\mathbb{1} \otimes \mathbb{1}. \tag{15}$$

For later convenience, we introduce J as a difference of Choi matrices of both randomized measurements, that is

$$\begin{aligned} J &\coloneqq J\left(\int \mathcal{P}_U \otimes \mathcal{P}_U dU\right) - J\left(\int \mathcal{P}_U \otimes \mathcal{P}_V dUdV\right) \\ &= \frac{1}{d^2-1}\left(\mathbb{1} \otimes \left(\frac{1}{d^2}\mathbb{1} - \frac{1}{d}S\right) + T \otimes \left(S - \frac{1}{d}\mathbb{1}\right)\right). \end{aligned} \tag{16}$$

The remaining part of the proof goes as follows. We will first calculate the upper bound on the diamond norm $\| \int \mathcal{P}_U \otimes \mathcal{P}_U dU - \int \mathcal{P}_U \otimes \mathcal{P}_V dUdV \|_\diamond \leq \|\mathrm{Tr}_{\mathcal{X},\mathcal{Y}} |J|\|$ from Eq. (3). Later, we will show that this inequality is saturated by Proposition 3 in [22].

Now we will focus on the upper bound. To calculate the upper bound we first need to find $|J| = \sqrt{J^\dagger J}$. From Lemma 1 in Appendix A, taking $W \coloneqq (2T - \mathbb{1}) \otimes S$ it holds that $(WJ)^2 = J^2$, and this gives a polar decomposition of J.

To calculate the upper bound for the diamond norm from Eq. (3) we need to calculate $\|\mathrm{Tr}_{\mathcal{X},\mathcal{Y}} |J|\| = \|\mathrm{Tr}_{\mathcal{X},\mathcal{Y}} WJ\|$. Hence we calculate

$$\begin{aligned} \mathrm{Tr}_{\mathcal{X},\mathcal{Y}}(WJ) &= \frac{1}{d^2-1}\mathrm{Tr}_{\mathcal{X},\mathcal{Y}}\left(\frac{1}{d}\mathbb{1}\otimes\mathbb{1} - \frac{1}{d^2}\mathbb{1}\otimes S + \frac{d-2}{d}T\otimes\mathbb{1} - \frac{d-2}{d^2}T\otimes S\right) \\ &= \frac{1}{d^2-1}\left(\frac{d^2}{d}\mathbb{1} - \frac{d^2}{d^2}S + \frac{d(d-2)}{d}\mathbb{1} - \frac{d(d-2)}{d^2}S\right) \\ &= \frac{1}{d^2-1}\left((2d-2)\mathbb{1} - \frac{2d-2}{d}S\right) = \frac{2}{d+1}\left(\mathbb{1} - \frac{1}{d}S\right) \end{aligned} \tag{17}$$

and eventually we have

$$\|\mathrm{Tr}_{\mathcal{X},\mathcal{Y}} |J|\| = \left\|\frac{2}{d+1}\left(\mathbb{1} - \frac{1}{d}S\right)\right\| = \frac{2}{d+1}\left\|\mathbb{1} - \frac{1}{d}S\right\| = \frac{2}{d}. \tag{18}$$

Now we proceed to proving that the upper bound is saturated. By Proposition 3 in [22] we need to check whether there exist a vector $|a\rangle$ and a unitary matrix W such that

(i) $\langle a| \mathrm{Tr}_{\mathcal{X},\mathcal{Y}} \sqrt{J^\dagger J}|a\rangle = \left\|\mathrm{Tr}_{\mathcal{X},\mathcal{Y}} \sqrt{J^\dagger J}\right\|$
(ii) $(\mathbb{1} \otimes |a\rangle\langle a|)\, W = W\, (\mathbb{1} \otimes |a\rangle\langle a|)$
(iii) W is the angular part of some polar decomposition of J (*i.e.* $J = WP$ for some positive semidefinite P)

As the matrix W we take $W \coloneqq (2T - \mathbb{1}) \otimes S$ and as the vector $|a\rangle$ we take some vector $\frac{1}{\sqrt{2}}(|ij\rangle - |ji\rangle) \in \mathcal{Z}$, where $i > j$ and $\dim(\mathcal{Z}) = d^2$. The condition (ii) translates to

$(\mathbb{1} \otimes |a\rangle\langle a|) S \otimes S = S \otimes S (\mathbb{1} \otimes |a\rangle\langle a|)$ hence it suffices to note that $|a\rangle\langle a|S = S|a\rangle\langle a|$. The condition (iii) follows directly.

Therefore

$$\left\| \int \mathcal{P}_U \otimes \mathcal{P}_U dU - \int \mathcal{P}_U \otimes \mathcal{P}_V dU dV \right\|_\diamond = \frac{2}{d} \tag{19}$$

and eventually

$$p^H_{succ} = \frac{1}{2} + \frac{1}{2d}. \tag{20}$$

□

3.2. **Asymmetric discrimination.** In the asymmetric discrimination we will consider two types of errors separately. We would like to verify whether measurements in both black boxes are the same (which corresponds to H_0 hypothesis) or they are different (which corresponds to H_1 hypothesis). Formally, when the measurement in the first black box, $\mathcal{P}_0$, is unknown, we say that $\mathcal{P}_0 = \int \mathcal{P}_U dU$. The measurement in the second black box can be either the same as in the first black box ($\mathcal{P}_? = \mathcal{P}_0$) or it can be some other measurement, that is $\mathcal{P}_? = \int \mathcal{P}_V dV$. When performing asymmetric discrimination, we prepare an input state $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}$. If in both black boxes there were the same measurements, then the output state yields $\rho_0^{(\psi)} = \int (\mathcal{P}_U \otimes \mathcal{P}_U \otimes \mathbb{1}_\mathcal{Z}) (\psi) dU$. If the measurements in the black boxes were different, when the output state is $\rho_1^{(\psi)} = \int (\mathcal{P}_U \otimes \mathcal{P}_V \otimes \mathbb{1}_\mathcal{Z}) (\psi) dU dV$. Next, we measure the output state by a binary measurement $\{\Omega, \mathbb{1} - \Omega\}$. We will focus on the case when he type I error cannot occur. The optimal probability of the type II error is formulated as the following theorem.

Theorem 2. Let $\mathcal{P}_0$ be a reference von Neumann measurement of dimension d given without classical description. Let $\mathcal{P}_1$ be another von Neumann measurement of the same dimension, also given without classical description. Consider the hypotheses testing problem described in Subsection 2.2. Let H_0 hypothesis state that $\mathcal{P}_? = \mathcal{P}_0$ and let the alternative H_1 hypothesis state that $\mathcal{P}_? = \mathcal{P}_1$. If no false positive error can occur, then the optimal probability of false negative error yields

$$p_{\mathrm{II}} = 1 - \frac{1}{d}. \tag{21}$$

Moreover, no additional register is needed to obtain this value.

Proof. As the input state to the discrimination procedure we take some state $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$. Note that we assumed that this state is only on two registers. In this proof we will calculate the probability of the type II error assuming that the register $\mathcal{Z}$ is trivial. Later, we will prove that this gives the optimal probability and the additional register is not needed.

If both measurements are the same, then the output state will be

$$\rho_0^{(\psi)} = \int (\mathcal{P}_U \otimes \mathcal{P}_U) (\psi) dU. \tag{22}$$

If the measurement in the black boxes are different, then the output state will be

$$\rho_1^{(\psi)} = \int (\mathcal{P}_U \otimes \mathcal{P}_V) (\psi) dU dV. \tag{23}$$

We begin with calculating $\int \left(\mathcal{P}_U \otimes \mathcal{P}_U\right)(\psi) dU$ by the use of formula for recovering the action of a quantum channel given its Choi matrix. Using the formula for the Choi matrix from Eq. (14) and using the notation $T \coloneqq \Delta(S)$ we calculate

$$\begin{aligned}\rho_0^{(\psi)} &= \operatorname{Tr}_{\mathcal{Z}}\left(J\left(\int \mathcal{P}_U \otimes \mathcal{P}_U dU\right)\left(\mathbb{1} \otimes \psi^\top\right)\right) \\ &= \frac{1}{d(d^2-1)}\left(\left(d - \operatorname{tr}\left(S\psi^\top\right)\right)\mathbb{1} + \left(d \operatorname{tr}\left(S\psi^\top\right) - 1\right)T\right).\end{aligned} \tag{24}$$

Let us take the input state to be antisymmetric, that is it satisfies $\operatorname{tr}\left(S\psi^\top\right) = -1$. We calculate

$$\rho_0^{(\psi)} = \frac{1}{d(d^2-1)}\left((d+1)\mathbb{1} - (d+1)T\right) = \frac{1}{d(d-1)}\left(\mathbb{1} - T\right). \tag{25}$$

By similar calculation, using the antisymmetric input state we have

$$\begin{aligned}\rho_1^{(\psi)} &= \operatorname{Tr}_{\mathcal{Z}}\left(J\left(\int \mathcal{P}_U \otimes \mathcal{P}_V dU\right)\left(\mathbb{1} \otimes \psi^\top\right)\right) = \operatorname{Tr}_{\mathcal{Z}}\left(\left(\frac{1}{d^2}\mathbb{1} \otimes \mathbb{1}\right)\left(\mathbb{1} \otimes \psi^\top\right)\right) \\ &= \frac{1}{d^2}\operatorname{Tr}_{\mathcal{Z}}\left(\mathbb{1} \otimes \psi^\top\right) = \frac{1}{d^2}\mathbb{1}.\end{aligned} \tag{26}$$

As the measurement effect we take $\Omega \coloneqq \mathbb{1} - T$. Hence

$$p_{\mathrm{I}}^{(\psi,\Omega)} = 1 - \operatorname{tr}\left(\Omega \rho_0^{(\psi)}\right) = 1 - \frac{1}{d(d-1)}\operatorname{tr}\left(\left(\mathbb{1} - T\right)\left(\mathbb{1} - T\right)\right) = 0, \tag{27}$$

and

$$p_{\mathrm{II}}^{(\psi,\Omega)} = \operatorname{tr}\left(\Omega \rho_1^{(\psi)}\right) = \frac{1}{d^2}\operatorname{tr}\left(\mathbb{1} - T\right) = \frac{d(d-1)}{d^2} = 1 - \frac{1}{d}. \tag{28}$$

From Appendix B we know that the probability of erroneous discrimination is the symmetric scheme (which equals $1 - p_{succ}^H$) is never bigger than the arithmetic mean of probabilities of the type I and type II errors. As

$$\frac{1}{2}\left(p_{\mathrm{I}}^{(\psi,\Omega)} + p_{\mathrm{II}}^{(\psi,\Omega)}\right) = \frac{1}{2} - \frac{1}{2d}, \tag{29}$$

then we conclude that our value of $p_{\mathrm{II}}^{(\psi,\Omega)} = 1 - \frac{1}{d}$ is optimal and hence $p_{\mathrm{II}} = p_{\mathrm{II}}^{(\psi,\Omega)}$.

Finally, note the optimal value p_{II} can be achieved for the input state $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$, that is when the register $\mathcal{Z}$ is trivial. Hence, the additional register is not needed for asymmetric discrimination in this case. □

4. Discrimination between a fixed and unknown von Neumann measurements

In this section we assume that instead of the unknown reference measurement from the previous section, we are given $\mathcal{P}_0$ as a fixed von Neumann measurement $\mathcal{P}_U$. We will begin with studying symmetric discrimination and later proceed to studying the asymmetric discrimination scheme.

4.1. **Symmetric discrimination.** Now we focus on the situation when we want to distinguish between a fixed von Neumann measurement $\mathcal{P}_U$ and a Haar-random measurement $\int \mathcal{P}_V dV$. The probability of successful discrimination is formulated as a theorem.

Theorem 3. Let $\mathcal{P}_0 = \mathcal{P}_U$ be a reference von Neumann measurement of dimension d. Let $\mathcal{P}_1$ be another von Neumann measurement of the same dimension, but given without classical description. The optimal probability of correct verification whether $\mathcal{P}_1 = \mathcal{P}_0$ or $\mathcal{P}_1 \neq \mathcal{P}_0$ in the scheme described in Subsection 2.1 equals

$$p_{succ}^{H} = 1 - \frac{1}{2d}. \tag{30}$$

Proof. Without loss of generality we can take $U = \mathbb{1}$. To calculate the bound from Holevo-Helstrom theorem (4), we want to calculate the diamond norm distance between quantum measurements

$$\left\| \mathcal{P}_{\mathbf{1}} \otimes \mathcal{P}_{\mathbf{1}} - \mathcal{P}_{\mathbf{1}} \otimes \int \mathcal{P}_V dV \right\|_{\diamond}. \tag{31}$$

Using properties of the diamond norm [23] we calculate

$$\begin{aligned} \left\| \mathcal{P}_{\mathbf{1}} \otimes \mathcal{P}_{\mathbf{1}} - \mathcal{P}_{\mathbf{1}} \otimes \int \mathcal{P}_V dV \right\|_{\diamond} &= \left\| \mathcal{P}_{\mathbf{1}} \otimes \left(\mathcal{P}_{\mathbf{1}} - \int \mathcal{P}_V dV \right) \right\|_{\diamond} \\ &= \|\mathcal{P}_{\mathbf{1}}\|_{\diamond} \left\| \mathcal{P}_{\mathbf{1}} - \int \mathcal{P}_V dV \right\|_{\diamond} \\ &= \left\| \mathcal{P}_{\mathbf{1}} - \int \mathcal{P}_V dV \right\|_{\diamond}. \end{aligned} \tag{32}$$

To do this, we use the fact that $\mathcal{P}_V = \Delta \Phi_{V^\dagger}$. Moreover, we know that $J(\Phi_{\mathbf{1}}) = |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|$ and $J(\Phi_\star) = \mathbb{1}/d$, where $\Phi_\star$ is the depolarizing channel defined in Eq. (2). Therefore, calculating directly both lower and upper bounds for the diamond norm from Eq. (3), we obtain

$$\left\| \mathcal{P}_{\mathbf{1}} - \int \mathcal{P}_V dV \right\|_{\diamond} = 2 - \frac{2}{d}. \tag{33}$$

Finally

$$p_{succ}^{H} = \frac{1}{2} + \frac{1}{4}\left(2 - \frac{2}{d}\right) = 1 - \frac{1}{2d}. \tag{34}$$

□

4.2. **Asymmetric discrimination.** In this subsection we will focus on asymmetric discrimination between a fixed von Neumann measurement $\mathcal{P}_U$ and a Haar-random measurement $\mathcal{P}_V$. We will be interested in the scenario when the false positive error cannot occur. The optimized probability of the false negative error is formulated as a theorem.

Theorem 4. Let $\mathcal{P}_0 = \mathcal{P}_U$ be a fixed von Neumann measurement and $\mathcal{P}_1$ be some other von Neumann measurement given without classical description. Let the H_0 hypothesis correspond to the case when $\mathcal{P}_? = \mathcal{P}_0$ and H_1 hypothesis correspond to the case when

$\mathcal{P}_? = \mathcal{P}_1$. Consider the discrimination scheme described in Subsection 2.2. If no false positive error can occur, then the optimal probability of false negative error yields

$$p_{\mathrm{II}} = \frac{1}{d}. \tag{35}$$

Proof. This proof goes similar as the proof of Theorem 1. We will choose a fixed input state on only two registers. We will also fix the final measurement and calculate the probabilities of making the false positive and false negative errors. Later, from inequality between errors in symmetric and asymmetric schemes in Appendix B we will see that the calculated p_{II} is the optimal one.

As the input state we take $\psi \coloneqq \frac{1}{d}|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|$. We calculate the output states

$$\rho_0^{(\psi)} \coloneqq (\mathcal{P}_U \otimes \mathbb{1})(\psi) = \frac{1}{d}(\mathcal{P}_U \otimes \mathbb{1})(|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|) = \frac{1}{d}\sum_i |i\rangle\langle i| \otimes |u_i\rangle\langle u_i|^\top \tag{36}$$

and

$$\begin{aligned} \rho_1^{(\psi)} &\coloneqq \int (\mathcal{P}_V \otimes \mathbb{1})(\psi) dV = \frac{1}{d}\int (\mathcal{P}_V \otimes \mathbb{1})(|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|) dV \\ &= \frac{1}{d}\int \sum_i |i\rangle\langle i| \otimes |v_i\rangle\langle v_i|^\top dV = \frac{1}{d}\sum_i |i\rangle\langle i| \otimes \int |v_i\rangle\langle v_i|^\top dV = \frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}. \end{aligned} \tag{37}$$

Recall that the measurement effect Ω correspond to H_0 hypothesis and $\mathbb{1} - \Omega$ correspond to H_1 hypothesis. Hence we have probabilities of false positive and false negative errors (for given input state) equal

$$p_{\mathrm{I}}^{(\psi,\Omega)} = 1 - \operatorname{tr}\left(\Omega\rho_0^{(\psi)}\right), \quad p_{\mathrm{II}}^{(\psi,\Omega)} = \operatorname{tr}\left(\Omega\rho_1^{(\psi)}\right). \tag{38}$$

Without loss of generality we can consider Ω in the block-diagonal form, ie.

$$\Omega \coloneqq \sum_i |i\rangle\langle i| \otimes \Omega_i^\top. \tag{39}$$

As the unitary matrix U is known, we can use it to construct the final measurement. Let

$$\Omega_i \coloneqq |u_i\rangle\langle u_i| \tag{40}$$

for every $i = 1, \ldots, d$.

Then

$$\begin{aligned} \operatorname{tr}\left(\Omega\rho_0^{(\psi)}\right) &= \operatorname{tr}\left(\left(\sum_i |i\rangle\langle i| \otimes |u_i\rangle\langle u_i|^\top\right)\left(\frac{1}{d}\sum_j |j\rangle\langle j| \otimes |u_j\rangle\langle u_j|^\top\right)\right) \\ &= \frac{1}{d}\sum_i \operatorname{tr}\left(|u_i\rangle\langle u_i|u_i\rangle\langle u_i|\right) = \frac{1}{d}\sum_i |\langle u_i|u_i\rangle|^2 = 1 \end{aligned} \tag{41}$$

and hence

$$p_{\mathrm{I}}^{(\psi,\Omega)} = 1 - \operatorname{tr}\left(\Omega\rho_0^{(\psi)}\right) = 0. \tag{42}$$

Eventually

$$\begin{aligned} p_{\mathrm{II}}^{(\psi,\Omega)} &= \operatorname{tr}\left(\Omega\rho_1^{(\psi)}\right) = \operatorname{tr}\left(\left(\sum_i |i\rangle\langle i| \otimes |u_i\rangle\langle u_i|^\top\right)\left(\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}\right)\right) \\ &= \frac{1}{d^2}\sum_i \operatorname{tr}\left(|u_i\rangle\langle u_i|\right) = \frac{1}{d}. \end{aligned} \tag{43}$$

It remains to explain why $p_{\mathrm{II}}^{(\psi,\Omega)} = p_{\mathrm{II}}$. Note that the arithmetic mean of probabilities of both types of errors equals $\frac{1}{2d}$ which is equal to the probability of erroneous discrimination in the symmetric scheme (see Theorem 3). From the inequality between errors in the symmetric and asymmetric schemes in Appendix B we conclude that $p_{\mathrm{II}} = \frac{1}{d}$. □

5. Conclusion

We were studying the problem whether the given von Neumann measurement is the same as the reference one. We were considering the situation when the reference measurement is given without classical description and when its classical description is known. Both situations were studied in the symmetric and asymmetric scenarios. We proved that in both cases one can achieve the probability of false positive error equal zero and we calculated optimal probabilities of false negative errors. We also calculated the probabilities of successful discrimination in the symmetric discrimination scheme.

Acknowledgements

This work was supported by the project ,,Near-term quantum computers Challenges, optimal implementations and applications” under Grant Number POIR.04.04.00-00-17C1/18-00, which is carried out within the Team-Net programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund.

References

[1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, “Quantum certification and benchmarking,” *Nature Reviews Physics*, pp. 1–9, 2020.

[2] A. Acin, “Statistical distinguishability between unitary operations,” *Physical Review Letters*, vol. 87, no. 17, p. 177901, 2001.

[3] J. Bae, “Discrimination of two-qubit unitaries via local operations and classical communication,” *Scientific Reports*, vol. 5, no. 1, pp. 1–8, 2015.

[4] A. Kawachi, K. Kawano, F. Le Gall, and S. Tamaki, “Quantum query complexity of unitary operator discrimination,” *IEICE TRANSACTIONS on Information and Systems*, vol. 102, no. 3, pp. 483–491, 2019.

[5] M. F. Sacchi, “Optimal discrimination of quantum operations,” *Physical Review A*, vol. 71, no. 6, p. 062340, 2005.

[6] M. Piani and J. Watrous, “All entangled states are useful for channel discrimination,” *Physical Review Letters*, vol. 102, no. 25, p. 250501, 2009.

[7] R. Duan, Y. Feng, and M. Ying, “Perfect distinguishability of quantum operations,” *Physical Review Letters*, vol. 103, no. 21, p. 210501, 2009.

[8] G. Wang and M. Ying, “Unambiguous discrimination among quantum operations,” *Physical Review A*, vol. 73, no. 4, p. 042301, 2006.

[9] A. Krawiec, Ł. Pawela, and Z. Puchała, "Excluding false negative error in certification of quantum channels," *Scientific Reports*, vol. 11, no. 1, pp. 1–11, 2021.
[10] M. Ziman, "Process positive-operator-valued measure: A mathematical framework for the description of process tomography experiments," *Physical Review A*, vol. 77, no. 6, p. 062112, 2008.
[11] M. Sedlák and M. Ziman, "Unambiguous comparison of unitary channels," *Physical Review A*, vol. 79, no. 1, p. 012303, 2009.
[12] M. Ziman and M. Sedlák, "Single-shot discrimination of quantum unitary processes," *Journal of Modern Optics*, vol. 57, no. 3, pp. 253–259, 2010.
[13] M. Hillery, E. Andersson, S. M. Barnett, and D. Oi, "Decision problems with quantum black boxes," *Journal of Modern Optics*, vol. 57, no. 3, pp. 244–252, 2010.
[14] A. Soeda, A. Shimbo, and M. Murao, "Optimal quantum discrimination of single-qubit unitary gates between two candidates," *Physical Review A*, vol. 104, no. 2, p. 022422, 2021.
[15] Y. Hashimoto, A. Soeda, and M. Murao, "Comparison of unknown unitary channels with multiple uses," *arXiv preprint arXiv:2208.12519*, 2022.
[16] Z. Puchała, Ł. Pawela, A. Krawiec, and R. Kukulski, "Strategies for optimal single-shot discrimination of quantum measurements," *Physical Review A*, vol. 98, no. 4, p. 042103, 2018.
[17] Z. Puchała, Ł. Pawela, A. Krawiec, R. Kukulski, and M. Oszmaniec, "Multiple-shot and unambiguous discrimination of von Neumann measurements," *Quantum*, vol. 5, p. 425, 2021.
[18] P. Lewandowska, A. Krawiec, R. Kukulski, Ł. Pawela, and Z. Puchała, "On the optimal certification of von Neumann measurements," *Scientific Reports*, vol. 11, no. 1, pp. 1–16, 2021.
[19] M. Miková, M. Sedlák, I. Straka, M. Mičuda, M. Ziman, M. Ježek, M. Dušek, and J. Fiurášek, "Optimal entanglement-assisted discrimination of quantum measurements," *Physical Review A*, vol. 90, no. 2, p. 022317, 2014.
[20] M. Ziman, T. Heinosaari, and M. Sedlák, "Unambiguous comparison of quantum measurements," *Physical Review A*, vol. 80, no. 5, p. 052102, 2009.
[21] M. Sedlák and M. Ziman, "Optimal single-shot strategies for discrimination of quantum measurements," *Physical Review A*, vol. 90, no. 5, p. 052312, 2014.
[22] I. Nechita, Z. Puchała, Ł. Pawela, and K. Życzkowski, "Almost all quantum channels are equidistant," *Journal of Mathematical Physics*, vol. 59, no. 5, p. 052201, 2018.
[23] J. Watrous, *The Theory of Quantum Information.* Cambridge University Press, 2018.
[24] Z. Puchała and J. Miszczak, "Symbolic integration with respect to the Haar measure on the unitary groups," *Bulletin of the Polish Academy of Sciences. Technical Sciences*, vol. 65, no. 1, 2017.
[25] B. Collins and P. Śniady, "Integration with respect to the Haar measure on unitary, orthogonal and symplectic group," *Communications in Mathematical Physics*, vol. 264, no. 3, pp. 773–795, 2006.

Appendix A. Lemma 1

Lemma 1. Let J be as defined in Eq. (16), $T \coloneqq \Delta(S)$ and $W \coloneqq (2T - \mathbb{1}) \otimes S$, where S is the swap matrix of dimension d^2. Then $J^2 = (WJ)^2$.

Proof. As

$$J^2 = \left(\frac{1}{d^2-1}\right)^2 \left(\frac{1}{d^2}\mathbb{1} \otimes \mathbb{1} - \frac{1}{d}\mathbb{1} \otimes S + T \otimes S - \frac{1}{d} T \otimes \mathbb{1}\right)^2, \tag{44}$$

we calculate

$$
\begin{aligned}
&\left(\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d}\mathbb{1}\otimes S+T\otimes S-\frac{1}{d}T\otimes\mathbb{1}\right)^2\\
&=\frac{1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d^3}\mathbb{1}\otimes S+\frac{1}{d^2}T\otimes S-\frac{1}{d^3}T\otimes\mathbb{1}\\
&-\frac{1}{d^3}\mathbb{1}\otimes S+\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d}T\otimes\mathbb{1}+\frac{1}{d^2}T\otimes S\\
&+\frac{1}{d^2}T\otimes S-\frac{1}{d}T\otimes\mathbb{1}+T\otimes\mathbb{1}-\frac{1}{d}T\otimes S\\
&-\frac{1}{d^3}T\otimes\mathbb{1}+\frac{1}{d^2}T\otimes S-\frac{1}{d}T\otimes S+\frac{1}{d^2}T\otimes\mathbb{1}\\
&=\frac{d^2+1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{2}{d^3}\mathbb{1}\otimes S+\left(1+\frac{1}{d^2}-\frac{2}{d}-\frac{2}{d^2}\right)T\otimes\mathbb{1}+\left(\frac{4}{d^2}-\frac{2}{d}\right)T\otimes S\\
&=\frac{d^2+1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{2}{d^3}\mathbb{1}\otimes S+\frac{(d^2+1)(d-2)}{d^3}T\otimes\mathbb{1}+\frac{4-2d}{d^2}T\otimes S,
\end{aligned}
\tag{45}
$$

and eventually

$$
J^2=\left(\frac{1}{d^2-1}\right)^2\left(\frac{d^2+1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{2}{d^3}\mathbb{1}\otimes S+\frac{(d^2+1)(d-2)}{d^3}T\otimes\mathbb{1}+\frac{4-2d}{d^2}T\otimes S\right).
\tag{46}
$$

On the other hand

$$
WJ=(2T\otimes S-\mathbb{1}\otimes S)\,\frac{1}{d^2-1}\left(\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d}\mathbb{1}\otimes S+T\otimes S-\frac{1}{d}T\otimes\mathbb{1}\right).
\tag{47}
$$

Hence we calculate

$$
\begin{aligned}
&(2T\otimes S-\mathbb{1}\otimes S)\left(\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d}\mathbb{1}\otimes S+T\otimes S-\frac{1}{d}T\otimes\mathbb{1}\right)\\
&=\frac{2}{d^2}T\otimes S-\frac{2}{d}T\otimes\mathbb{1}+2T\otimes\mathbb{1}-\frac{2}{d}T\otimes S\\
&-\frac{1}{d^2}\mathbb{1}\otimes S+\frac{1}{d}\mathbb{1}\otimes\mathbb{1}-T\otimes\mathbb{1}+\frac{1}{d}T\otimes S\\
&=\frac{1}{d}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d^2}\mathbb{1}\otimes S+\frac{d-2}{d}T\otimes\mathbb{1}-\frac{d-2}{d^2}T\otimes S.
\end{aligned}
\tag{48}
$$

and thus

$$
\begin{aligned}
&\left(\frac{1}{d}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d^2}\mathbb{1}\otimes S+\frac{d-2}{d}T\otimes\mathbb{1}-\frac{d-2}{d^2}T\otimes S\right)^2\\
&=\frac{1}{d^2}\mathbb{1}\otimes\mathbb{1}-\frac{1}{d^3}\mathbb{1}\otimes S+\frac{d-2}{d^2}T\otimes\mathbb{1}-\frac{d-2}{d^3}T\otimes S\\
&-\frac{1}{d^3}\mathbb{1}\otimes S+\frac{1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{d-2}{d^3}T\otimes S+\frac{d-2}{d^4}T\otimes\mathbb{1}\\
&+\frac{d-2}{d^2}T\otimes\mathbb{1}-\frac{d-2}{d^3}T\otimes S+\frac{(d-2)^2}{d^2}T\otimes\mathbb{1}-\frac{(d-2)^2}{d^3}T\otimes S\\
&-\frac{d-2}{d^3}T\otimes S+\frac{d-2}{d^4}T\otimes\mathbb{1}-\frac{(d-2)^2}{d^3}T\otimes S+\frac{(d-2)^2}{d^4}T\otimes\mathbb{1}\\
&=\frac{d^2+1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{2}{d^3}\mathbb{1}\otimes S+\frac{(d^2+1)(d-2)}{d^3}T\otimes\mathbb{1}+\frac{4-2d}{d^2}T\otimes S.
\end{aligned}
\tag{49}
$$

Eventually

$$
(WJ)^2=\left(\frac{1}{d^2-1}\right)^2\left(\frac{d^2+1}{d^4}\mathbb{1}\otimes\mathbb{1}-\frac{2}{d^3}\mathbb{1}\otimes S+\frac{(d^2+1)(d-2)}{d^3}T\otimes\mathbb{1}+\frac{4-2d}{d^2}T\otimes S\right)
\tag{50}
$$

and hence $(WJ)^2=J^2$. □

Appendix B. Inequality between errors

We will show that

$$
p_e^H\le\frac{1}{2}(p_1+p_2),
\tag{51}
$$

where $p_e^H=1-p_{succ}^H$ is the probability of error from the Holevo-Helstrom Theorem.

Let us recall that from Holevo-Helstrom Theorem we have

$$
\frac{1}{2}\operatorname{Tr}(\Omega_0\rho_0)+\frac{1}{2}\operatorname{Tr}(\Omega_1\rho_1)\le 1-p_e^H,
\tag{52}
$$

hence

$$
p_e^H\le 1-\frac{1}{2}\left(\operatorname{Tr}(\Omega_0\rho_0)+\operatorname{Tr}(\Omega_1\rho_1)\right).
\tag{53}
$$

On the other hand we know that

$$
\begin{aligned}
\operatorname{Tr}(\Omega_0\rho_0)+\operatorname{Tr}(\Omega_1\rho_0)=1\\
\operatorname{Tr}(\Omega_0\rho_1)+\operatorname{Tr}(\Omega_1\rho_1)=1
\end{aligned}
\tag{54}
$$

and hence

$$
\operatorname{Tr}(\Omega_0\rho_0)+\operatorname{Tr}(\Omega_1\rho_1)=2-(p_1+p_2).
\tag{55}
$$

Therefore

$$
\begin{aligned}
p_e^H&\le 1-\frac{1}{2}\left(\operatorname{Tr}(\Omega_0\rho_0)+\operatorname{Tr}(\Omega_1\rho_1)\right)=1-\frac{1}{2}\left(2-(p_1+p_2)\right)\\
&=\frac{1}{2}(p_1+p_2).
\end{aligned}
\tag{56}
$$