Unambiguous comparison of unitary channels

Michal Sedlák[1,3], Mário Ziman[1,2]
[1] *Research Center for Quantum Information, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia*
[2] *Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic*
[3] Quniverse, *Líščie údolie 116, 841 04 Bratislava, Slovakia*

We address the problem of unambiguous comparison of a pair of unknown qudit unitary channels. Using the framework of process positive operator valued measures (PPOVM) we characterize all solutions and identify the optimal ones. We prove that the entanglement is the key ingredient in designing the optimal experiment for comparison of unitary channels. Without entanglement the optimality can not be achieved. The proposed scheme is also experimentally feasible.

PACS numbers: 03.67.Lx,03.65.Ta

I. INTRODUCTION

The unavoidable uncertainty of quantum predictions represents one of the key features of quantum theory [1, 2]. It might seem surprising at first sight, but even in probabilistic theories there are problems in which error-free nontrivial conclusions can be based on single experimental events (clicks). Consider, for example, the Stern-Gerlach experiment in which the spin of a particle is measured along the z axis. Finding the outcome *spin up* implies that the particle was not for sure in the *spin down* state. In general, this information does not seem to be very useful. However, if we have additional information that the spin was either ϱ, or *spin down*, then the outcome *spin up* identifies the spin state ϱ.

A class of problems extending this example is known as unambiguous identification problems. Over last decades authors have investigated unambiguous discrimination of states [3, 4, 5, 6, 7, 8, 9], channels [10, 11] and observables [12]. All these works are showing that single clicks can give us nontrivial information about all types of quantum devices. In their seminal work Barnett et al. [13] introduced the concept of unambiguous state comparison. In this problem an experimentalist is given two preparators, each producing a single quantum system in a particular pure state. The aim is to compare produced states. It turns out that in all possible experiments only the difference of the compared states can be unambiguously concluded. We can never confirm experimentally (without making some error) that two unknown pure states are the same. Different versions of unambiguous state comparison have been investigated in [14, 15, 16].

The goal of this paper is to investigate a comparison of quantum devices implementing unknown unitary channels. Such universal comparator of unitary channels can be of use, for instance, in the calibration and testing of the quality of elementary quantum gates.

Quantum channels are tested in two steps. First we prepare a so-called test state and apply the channel. After that the output state is measured. Therefore, it is natural to employ a state comparator to compare the channels. As we shall see these two problems are indeed closely related, but there are also important differences concerning the optimal strategies. We shall elaborate on this point later.

The paper is organized as follows: in Section II the problem is reformulated in the framework of process positive operator valued measures (PPOVM) and existence of a solution is shown. The optimal solution is described in Section III together with its uniqueness. The last section is left for summary and conclusions.

II. FORMULATION OF THE PROBLEM

Consider we are given two black boxes implementing unknown unitary channels $\mathcal{E}_U$ and $\mathcal{E}_V$ on qudit, i.e. d-dimensional quantum system. Our task is to unambiguously decide whether the black boxes perform the same unitary channels, or not. More formally, whether a process implemented on $D = d \times d$ dimensional quantum system by the pair of devices is described by a channel $\mathcal{E}_U \otimes \mathcal{E}_V$ with $U \neq V$, or by a channel $\mathcal{E}_U \otimes \mathcal{E}_U$. As in any comparison problem we implicitly assume that the probability that the channels are the same is nonzero. Otherwise the problem would be senseless.

The most general experimental procedure for the comparison is depicted in Figure 1. Using each of the quantum boxes at most once the experiment will end by measurement, whose outcome uniquely determines our conclusion. In particular, the experiment consists of three steps. At first, we prepare a so-called test state $\xi \in \mathcal{S}(\mathcal{H}_{\rm anc} \otimes \mathcal{H}_d \otimes \mathcal{H}_d)$, where $\mathcal{H}_{\rm anc}$ is the Hilbert space of some ancilliary system. After that black boxes are applied and a measurement F on the whole system including the ancilla is performed. Measurement outcomes are associated with effects $F_{\rm same}, F_{\rm diff}, F_?$ forming a three-valued POVM, i.e.

$$O \leq F_{\rm same}, F_{\rm diff}, F_? \leq I\,; \qquad F_? + F_{\rm same} + F_{\rm diff} = I\,.$$

As in any unambiguous identification problem the inconclusive outcome $F_?$ is needed in order to make the conclusive outcomes $F_{\rm same}, F_{\rm diff}$ unambiguous. In fact, we shall see explicitly that $F_? \neq O$. An outcome $x \in \{\text{same, diff, ?}\}$ is observed with the probability

$$p_x(U \otimes V) = {\rm tr}[F_x(\mathcal{I}_{\rm anc} \otimes \mathcal{E}_U \otimes \mathcal{E}_V)[\xi]]\,, \qquad (2.1)$$

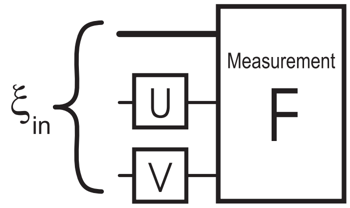

FIG. 1: The most general experiment for comparison of two unitary channels $\mathcal{E}_U, \mathcal{E}_V$.

where $\mathcal{E}_U[\cdot] = U \cdot U^\dagger, \mathcal{E}_V[\cdot] = V \cdot V^\dagger$ are unitary channels implemented by the black boxes.

Our goal is to characterize all possible experiments (determined by pairs ξ, F) performing the unambiguous comparison of unitary channels and identify the optimal strategy. The figure of merit for the optimization will be specified in details later. The analysis can be significantly simplified by adopting a framework introduced in Refs. [17, 18]. According to work [17] each experiment measuring some parameters of a channel can be decribed by the so-called process POVM (PPOVM). The key idea behind the PPOVM framework is that each experiment can be understood as a fictitious experiment using the maximally entangled state as the test state. In particular, in this framework channels acting on D dimensional quantum systems are represented via Choi-Jamiolkowski isomorphism [19, 20] by operators

$$\omega_{\mathcal{E}} = (\mathcal{I} \otimes \mathcal{E})[\Psi_D^+] \tag{2.2}$$

defined on D^2-dimensional Hilbert space, where $\Psi_D^+ = |\Psi_D^+\rangle\langle\Psi_D^+|$ and $|\Psi_D^+\rangle = \sum_{j=1}^D |j\rangle \otimes |j\rangle$. Let us note that in this parametrization $\mathrm{tr}[\omega_{\mathcal{E}}] = D$. For a given pair of test state ξ and observed effect F_x there exists an operator $O \leq M_x \leq I_D \otimes I_D$ on D^2-dimensional Hilbert space such that $p_x = \mathrm{tr}[\omega_{\mathcal{E}} M_x] = \mathrm{tr}[(\mathcal{I} \otimes \mathcal{E})[\xi] F_x]$ for all channels $\mathcal{E}$. Moreover, the normalization condition $\sum_x M_x = \varrho^T \otimes I_D$ holds, where ϱ is a state of D-dimensional system and ϱ^T denotes the matrix transposition with respect to basis used in the definition of the maximally entangled state Ψ_D^+. Let us note that for a given PPOVM, i.e. a set of positive operators $M_1, \dots, M_n$ such that $\sum_x M_x = \varrho^T \otimes I_D$ there exists many different experiments with different choices of test states and POVMs [17]. In particular, consider a PPOVM such that $M_j = \varrho^T \otimes F_j$ for all j. Since the identity

$$\mathrm{tr}[\mathcal{E}[\varrho] F_j] = \mathrm{tr}[(\mathcal{I} \otimes \mathcal{E})[\Psi_D^+](\varrho^T \otimes F_j)] = \mathrm{tr}[\omega_{\mathcal{E}} M_j]$$

holds for all qudit channels $\mathcal{E}$ and all qudit operators ϱ, F, it follows that this type of PPOVM can be realized by using a single ancilla-free test state ϱ and performing the measurement described by POVM consisting of positive operators F_j.

A. Requirements on unambiguous comparators

Translating the comparison problem into PPOVM framework we set $D = d^2$ and associate the two black boxes acting on d-dimensional systems with operators

$$\omega_{U\otimes U} = (I_D \otimes U \otimes U)\Psi_D^+(I_D \otimes U^\dagger \otimes U^\dagger), \tag{2.3}$$
$$\omega_{U\otimes V} = (I_D \otimes U \otimes V)\Psi_D^+(I_D \otimes U^\dagger \otimes V^\dagger), \tag{2.4}$$

where $\Psi_D^+ = |\Psi_D^+\rangle\langle\Psi_D^+|$ and $|\Psi_D^+\rangle_{1234} = |\Psi_d^+\rangle_{13} \otimes |\Psi_d^+\rangle_{24} \in \mathcal{H}_d^{\otimes 4}$. Operators $M_{\mathrm{same}}, M_{\mathrm{diff}}, M_?$ defining the PPOVM have to satisfy following no-error conditions ensuring the unambiguity of the corresponding conclusions:

$$p_{\mathrm{diff}}(U \otimes U) = \mathrm{tr}[\omega_{U\otimes U} M_{\mathrm{diff}}] = 0$$
$$p_{\mathrm{same}}(U \otimes V) = \mathrm{tr}[\omega_{U\otimes V} M_{\mathrm{same}}] = 0$$

for all $U, V \in U(d)$, where $U(d)$ denotes the group of unitary operators on d-dimensional Hilbert space.

Defining average channels as

$$\mathcal{A}[X] = \int_{U(d)} dU U X U^\dagger, \tag{2.5}$$
$$\mathcal{T}[Y] = \int_{U(d)} dU (U \otimes U) Y (U^\dagger \otimes U^\dagger), \tag{2.6}$$

the above conditions can be equivalently rewritten as

$$0 = \mathrm{tr}[(\mathcal{I}_{12} \otimes \mathcal{T}_{34})[\Psi_D^+] M_{\mathrm{diff}}], \tag{2.7}$$
$$0 = \mathrm{tr}[(\mathcal{I}_{12} \otimes \mathcal{A}_3 \otimes \mathcal{A}_4)[\Psi_D^+] M_{\mathrm{same}}], \tag{2.8}$$

because all the relevant operators are positive. The actions of the twirling channel $\mathcal{T}$ and the average channel $\mathcal{A}$ are derived in Appendices. In particular,

$$\mathcal{A}[X] = \mathrm{tr}[X] \frac{1}{d} I_d, \tag{2.9}$$
$$\mathcal{T}[Y] = \frac{\mathrm{tr}[Y P_+]}{d_+} P_+ + \frac{\mathrm{tr}[Y P_-]}{d_-} P_-, \tag{2.10}$$

where $P_\pm$ are projectors onto symmetric and antisymmetric subspaces of $\mathcal{H}_d \otimes \mathcal{H}_d$, respectively, and $d_\pm = \mathrm{tr}[P_\pm] = d(d \pm 1)/2$ are the corresponding dimensions of these subspaces. Let us note that $P_\pm = \frac{1}{2}(I \pm S)$, where S is the swap operator acting as $S|\psi\rangle \otimes |\varphi\rangle = |\varphi\rangle \otimes |\psi\rangle$ for all $\psi, \varphi \in \mathcal{H}_d$. Using these expressions we obtain

$$(\mathcal{I}_{12} \otimes \mathcal{A}_3 \otimes \mathcal{A}_4)[\Psi_D^+] = \frac{1}{d^2} I_d^{\otimes 4} \tag{2.11}$$

and since

$$\mathcal{T}[|jm\rangle\langle kn|] = \sum_{s=\pm} \frac{1}{d_s} \langle kn|P_s|jm\rangle P_s$$
$$= \sum_{s=\pm} \frac{1}{2d_s} (\delta_{jk}\delta_{mn} + s\delta_{jn}\delta_{mk}) P_s$$

we have

$$
\begin{aligned}
\omega_{\mathcal{T}} &= (\mathcal{I}_{12}\otimes\mathcal{T}_{34})[(\Psi_d^+)_{13}\otimes(\Psi_d^+)_{24}] \\
&= \sum_{j,k,m,n} |jm\rangle_{12}\langle kn|\otimes\mathcal{T}_{34}[|jm\rangle_{34}\langle kn|] \\
&= \frac{1}{2d_+}\sum_{j,m}\Big[|jm\rangle\langle jm| + |jm\rangle\langle mj|\Big]\otimes P_+ \\
&\quad +\frac{1}{2d_-}\sum_{j,m}[|jm\rangle\langle jm| - |jm\rangle\langle mj|]\otimes P_- \\
&= \frac{1}{4d_+}\sum_{j,m}[(|jm\rangle+|mj\rangle)(\langle jm|+\langle mj|)]\otimes P_+ \\
&\quad +\frac{1}{4d_-}\sum_{j,m}[(|jm\rangle-|mj\rangle)(\langle jm|-\langle mj|)]\otimes P_- \\
&= \frac{1}{d_+}P_+\otimes P_+ + \frac{1}{d_-}P_-\otimes P_- .
\end{aligned}
$$

Putting all formulas together the conditions in Eqs.(2.7),(2.8) take the form

$$
\begin{aligned}
0 &= \mathrm{tr}[\omega_\tau M_{\mathrm{diff}}]\,, && (2.12)\\
0 &= \frac{1}{d^2}\mathrm{tr}[I_d^{\otimes 4}M_{\mathrm{same}}] = \mathrm{tr}[M_{\mathrm{same}}]\,. && (2.13)
\end{aligned}
$$

Since $M_{\mathrm{same}}, M_{\mathrm{diff}}$ are positive operators it follows that $M_{\mathrm{same}} = O$ and M_{diff} has support in the orthocomplement of ω_τ. Consequently, we can unambiguously conclude only that the unitary channels are different. We can formulate the following proposition.

Proposition 1. *If a PPOVM $M_{\mathrm{same}}, M_{\mathrm{diff}}, M_?$ describes an unambiguous comparison of arbitrary unitary channels, then necessarily*

$$
\mathrm{supp}M_{\mathrm{diff}}\perp\mathrm{supp}\omega_{\mathcal{T}}\,;\qquad M_{\mathrm{same}} = O\,;\\
M_? = \varrho^T\otimes I_D - M_{\mathrm{diff}}\,, \qquad (2.14)
$$

for some state $\varrho\in\mathcal{S}(\mathcal{H}_d\otimes\mathcal{H}_d)$.

III. OPTIMAL UNAMBIGUOUS COMPARATOR

Following the previous section as a figure of merit for unambiguous comparators of unitary channels we shall use the average conditioned probability of revealing their difference

$$
\begin{aligned}
\overline{p}_{\mathrm{diff}} &= \int_{U(d)\times U(d)} dU dV\, p_{\mathrm{diff}}(U\otimes V) \\
&= \mathrm{tr}[(\mathcal{I}_{12}\otimes\mathcal{A}_3\otimes\mathcal{A}_4)[\Psi_D^+]M_{\mathrm{diff}}] \\
&= \frac{1}{d^2}\mathrm{tr}[M_{\mathrm{diff}}]\,. \qquad (3.1)
\end{aligned}
$$

The overall average success probability equals $(1-\eta_{\mathrm{same}})\overline{p}_{\mathrm{diff}}$, where $\eta_{\mathrm{same}}\neq 0$ is the prior probability for channels being the same. This prior is independent of the particular PPOVM $\{M_{\mathrm{diff}}, M_?\}$ and therefore we shall use only the conditional average probability to evaluate the quality of the unambiguous comparison strategy. Our task is to maximize the conditional success probability $\overline{p}_{\mathrm{success}}\equiv\overline{p}_{\mathrm{diff}}$ by finding a positive operator M_{diff} defined on $\mathcal{H}_D\otimes\mathcal{H}_D$ together with a state $\varrho\in\mathcal{S}(\mathcal{H}_D)$ such that also the operator $M_? = \varrho^T\otimes I_D - M_{\mathrm{diff}}$ is positive. Before specifying the optimal solution let us prove the following upper bound on the success probability.

Theorem 1. *If a process POVM consisting of positive operators $M_{\mathrm{diff}}, M_?$ with normalization $M_{\mathrm{diff}}+M_? = \varrho^T\otimes I_D$ unambiguously compares an arbitrary pair of unitary channels, then*

$$
\overline{p}_{\mathrm{success}}\leq\frac{d+1}{2d}\,. \qquad (3.2)
$$

Proof. The validity of the no-error condition $\mathrm{tr}[\omega_{\mathcal{T}}M_{\mathrm{diff}}] = 0$ implies that supports of M_{diff} and $\omega_{\mathcal{T}}$ are orthogonal. Let us denote by $|s_1\rangle,\ldots,|s_{d_+}\rangle$, $|a_1\rangle,\ldots,|a_{d_-}\rangle$ the vectors forming orthonormal bases of symmetric and antisymmetric subspaces of $\mathcal{H}_d\otimes\mathcal{H}_d$, respectively. Then $\mathrm{supp}\,\omega_{\mathcal{T}} = \mathrm{span}\{|s_j\otimes s_k\rangle, |a_m\otimes a_n\rangle\}$, where $j,k = 1,\ldots,d_+$ and $m,n = 1,\ldots,d_-$, and because of the mentioned orthogonality

$$
\mathrm{supp}M_{\mathrm{diff}}\subset\mathrm{span}\{|s_j\otimes a_n\rangle, |a_n\otimes s_j\rangle\}\,. \qquad (3.3)
$$

It follows that in a spectral form

$$
M_{\mathrm{diff}} = \sum_\alpha\lambda_\alpha|\phi_\alpha\rangle\langle\phi_\alpha|\,, \qquad (3.4)
$$

where $0\leq\lambda_\alpha\leq 1$ and

$$
|\phi_\alpha\rangle = \sum_{nj} c^\alpha_{nj}|a_n\otimes s_j\rangle + d^\alpha_{jn}|s_j\otimes a_n\rangle\,. \qquad (3.5)
$$

Consequently,

$$
M_{\mathrm{diff}} = \sum_n |a_n\rangle\langle a_n|\otimes A_n + \sum_n B_n\otimes|a_n\rangle\langle a_n| + R\,,
$$

with

$$
\begin{aligned}
A_n &= \sum_\alpha\lambda_\alpha\sum_{jl} c^\alpha_{nj}\overline{c^\alpha_{nl}}|s_j\rangle\langle s_l|\,; \\
B_n &= \sum_\alpha\lambda_\alpha\sum_{jl} d^\alpha_{nj}\overline{d^\alpha_{nl}}|s_j\rangle\langle s_l|\,; \\
R &= \sum_\alpha\lambda_\alpha\Bigg[\sum_{m\neq n,j,l} c^\alpha_{mj}\,\overline{c^\alpha_{nl}}|a_m\otimes s_j\rangle\langle a_n\otimes s_l| + \\
&\quad + \sum_{m\neq n,j,l} d^\alpha_{jm}\,\overline{d^\alpha_{ln}}|s_j\otimes a_m\rangle\langle s_l\otimes a_n| + \\
&\quad + \sum_{m,n,j,l} c^\alpha_{mj}\,\overline{d^\alpha_{ln}}|a_m\otimes s_j\rangle\langle s_l\otimes a_n| + \\
&\quad + \sum_{m,n,j,l} d^\alpha_{jm}\,\overline{c^\alpha_{nl}}|s_j\otimes a_m\rangle\langle a_n\otimes s_l|\Bigg]\,.
\end{aligned}
$$

Since $\mathrm{tr}[R]=0$ we get for the average success probability

$$\overline{p}_{\text{success}}=\frac{1}{d^2}\sum_{n=1}^{d_-}(\mathrm{tr}[A_n]+\mathrm{tr}[B_n])\,. \tag{3.6}$$

The operators A_n, B_n have the form of positive sum of one-dimensional projectors, hence they are positive.

Let us evaluate the mean value of operator $M_? = \varrho^T\otimes I - M_{\text{diff}}$ in a pure state associated with the vector $|s_j\otimes a_n\rangle$. Due to the required positivity of $M_?$ we get the inequality

$$0\leq \langle s_j\otimes a_n|M_?|s_j\otimes a_n\rangle = \langle s_j|\varrho^T - B_n|s_j\rangle\,. \tag{3.7}$$

Similarly, also the inequality

$$\begin{aligned}0 &\leq \langle a_n\otimes s_j|M_?|a_n\otimes s_j\rangle\\ &\leq \langle a_n|\varrho^T|a_n\rangle - \langle s_j|A_n|s_j\rangle\end{aligned} \tag{3.8}$$

holds. These two inequalities can be used to bound the trace of the density operator ϱ^T as follows

$$\begin{aligned}\mathrm{tr}[\varrho^T] &= \sum_n\langle a_n|\varrho^T|a_n\rangle + \sum_j\langle s_j|\varrho^T|s_j\rangle\\ &\geq \sum_n\langle s_k|A_n|s_k\rangle + \sum_j\langle s_j|B_m|s_j\rangle\\ &\geq \langle s_k|\sum_n A_n|s_k\rangle + \mathrm{tr}[B_m]\,,\end{aligned} \tag{3.9}$$

where we used the fact that by definition operators B_m have support only on the symmetric subspace. The inequality holds for all choices of k and m. Moreover, since $\mathrm{tr}[\varrho^T]=1$ and B_m is positive, i.e. $\mathrm{tr}[B_m]\geq 0$, we obtain that also

$$\langle s_k|\sum_n A_n|s_k\rangle\leq 1\,. \tag{3.10}$$

for all k. Using these inequalities the success probability can be upper bounded as follows

$$\begin{aligned}\overline{p}_{\text{success}} &= \frac{1}{d^2}\left(\sum_{j=1}^{d_+}\langle s_j|\sum_{n=1}^{d_-}A_n|s_j\rangle + \sum_{m=1}^{d_-}\mathrm{tr}[B_m]\right)\\ &= \frac{1}{d^2}\left[\sum_{m=1}^{d_-}\left(\langle s_m|\sum_{n=1}^{d_-}A_n|s_m\rangle + \mathrm{tr}[B_m]\right) + \right.\\ &\qquad\left. + \sum_{j=d_-+1}^{d_+}\langle s_j|\sum_{n=1}^{d_-}A_n|s_j\rangle\right]\\ &\leq \frac{1}{d^2}(d_-+d) = \frac{d_+}{d^2} = \frac{d+1}{2d}\,,\end{aligned} \tag{3.11}$$

which proves the theorem. □

A. Antisymmetric test states

In what follows we shall design a process POVM saturating the upper bound on the success probability. In particular, for operators

$$M_{\text{diff}}=\xi^T\otimes P_+\,,\qquad M_? = \xi^T\otimes P_-\,. \tag{3.12}$$

the success probability equals

$$\overline{p}_{\text{success}}=\frac{1}{d^2}\mathrm{tr}[M_{\text{diff}}]=\frac{1}{d^2}\mathrm{tr}[\xi^T\otimes P_+]=\frac{d_+}{d^2}\,, \tag{3.13}$$

hence the upper bound is saturated. Let us note that the state ξ is not arbitrary, because the support of M_{diff} must be orthogonal to support of $\omega_{\mathcal{T}}$ (see Eq.(3.3)). It implies that the state ξ has support only on antisymmetric subspace. We shall call such states antisymmetric. Similarly, if the support of a state is only in symmetric subspace we denote it as symmetric state.

The form of PPOVM in Eq. (3.12) suggests that one possible experimental realization consists of the folowing steps: i) prepare a two-qudit antisymmetric state ξ; ii) insert each qudit into different black box; iii) measure a two-valued observable described by POVM $F_{\text{diff}}=P_+$ and $F_? = P_-$, which identifies the exchange symmetry of the joint state of the two-qudit system.

The test state ξ is antisymmetric. If $U=V$ the action of the apparatuses preserves the symmetry, i.e. the output state remains antisymmetric and in such case $F_?$ must be observed. For $U\neq V$ the measurement outcome cannot be predicted with certainty, so both outcomes $F_{\text{diff}}, F_?$ have nonvanishing probability of occurence. However, if an outcome F_{diff} is observed, we can unambiguously conclude that U and V are different.

B. Symmetric test states

Alternatively, we can consider a process POVM

$$M_{\text{diff}}=\xi^T\otimes P_-\,,\qquad M_? = \xi^T\otimes P_+ \tag{3.14}$$

satisfying all the constraints providing ξ has support in the symmetric subspace. For this choice the success probability reads

$$\overline{p}_{\text{success}}=\mathrm{tr}[\xi^T\otimes P_-]=\frac{d_-}{d^2}=\frac{d-1}{2d}\,, \tag{3.15}$$

which is not optimal. Such PPOVM describes an experiment in which a "symmetric" test state is used. The same measurement is carried out as in the antisymmetric case, but the role of conclusive and inconclusive results is exchanged, i.e. $F_{\text{diff}}=P_-$ and $F_? = P_+$.

As we have mentioned at the beginning of this paper one possibility how to tackle the problem of unambiguous comparison of unitary channels is to adopt the universal comparison machines for states. Consider a pair of unitary channels applied on independent systems initially prepared in the same state. If $U=V$, then the resulting states are still described by the same state. However, if $U\neq V$, then the output states can be different. That is the state comparator can be used to find out whether the output states are different, which means that the unitary channels are different as well. In the language of channel comparison the described strategy can be interpreted as a strategy with a symmetric factorized test state $\xi=|\varphi\otimes\varphi\rangle\langle\varphi\otimes\varphi|$. Since the optimal state comparison is based on projective measurement described by projectors $P_\pm$, the value of the success probability is given in Eq.(3.15).

C. Uniqueness of optimal solution

In previous paragraphs we have shown that optimal strategy for comparison of unitary channels saturates the upper bound on probability of success imposed by Theorem 1. It means that PPOVM elements of each optimal strategy have to saturate all inequalities used in proof of this theorem. Analyzing this fact we can characterize all optimal strategies.

Theorem 2. *If a process POVM $\{M_{\rm diff},M_?\}$ with normalization $\varrho^T\otimes I_D$ unambiguously compares arbitrary pair of unitary channels with $\overline{p}_{\rm success}=\frac{d+1}{2d}$, then*

$$M_{\rm diff}=\varrho^T\otimes P_+\,,\qquad M_?=\varrho^T\otimes P_-\,,\tag{3.16}$$

where ϱ is a state with a support belonging only to the antisymmetric subspace of $\mathcal{H}_d\otimes\mathcal{H}_d$.

Proof. Saturation of inequality (3.10) for $k=d_+$ together with inequality (3.9) implies that $\mathrm{tr}[B_n]=0$ for all n. Consequently, positivity of operators B_n implies $B_n=0$ for all n i.e. coefficients d^α_{jn} vanish. This in turn requires

$$\langle s_k|\sum_n A_n|s_k\rangle=1\tag{3.17}$$

for all k. Using Eq. (3.8) and Eq. (3.17) we get

$$1=\sum_n\langle s_k|A_n|s_k\rangle\leq\sum_n\langle a_n|\varrho^T|a_n\rangle\leq\mathrm{tr}[\varrho^T]=1\,,$$

thus, $\sum_n\langle a_n|\varrho^T|a_n\rangle=1$. Due to positivity of ϱ^T we obtain $\langle s_j|\varrho^T|s_j\rangle=0$ for all j. This tells us that ϱ^T has support only on antisymmetric states. Since the used transposition is defined with respect to a product basis, the antisymmetric states preserve their antisymmetry, i.e. the state ϱ is antisymmetric as it is stated in the theorem.

Using the spectral form (3.4) and Eq. (3.5) we can rewrite $M_{\rm diff}$ as:

$$M_{\rm diff}=\sum_j C_j\otimes|s_j\rangle\langle s_j|+H\,,\tag{3.18}$$

with

$$\begin{aligned}C_j&=\sum_\alpha\lambda_\alpha\sum_{nm}c^\alpha_{nj}\overline{c^\alpha_{mj}}|a_n\rangle\langle a_m|\,;\\ H&=\sum_\alpha\lambda_\alpha\sum_{j\neq l,m,n}c^\alpha_{mj}\,\overline{c^\alpha_{nl}}|a_m\otimes s_j\rangle\langle a_n\otimes s_l|\end{aligned}$$

We rewrite also the probability of success [Eq. (3.1)] in terms of C_j and because the operator H is traceless we get

$$\overline{p}_{\rm success}=\frac{1}{d^2}\sum_j\mathrm{tr}[C_j].\tag{3.19}$$

Positivity of $M_?=\varrho^T\otimes\mathbb{1}-\sum_j C_j\otimes|s_j\rangle\langle s_j|-H$ implies

$$0\leq\langle a\otimes s_j|M_?|a\otimes s_j\rangle=\langle a|\varrho^T-C_j|a\rangle\,,\tag{3.20}$$

where $|a\rangle$ is arbitrary vector from $\mathcal{H}_D$. Hence, we have that operator ϱ^T-C_j is positive for all j and consequently that $1=\mathrm{tr}[\varrho^T]\geq\mathrm{tr}[C_j]$. Saturation of inequality (3.2) requires $\mathrm{tr}[C_j]=1$ for all j, which in turn implies $\mathrm{tr}[\varrho^T-C_j]=0$. This together with the positivity of operator ϱ^T-C_j enables us to conclude that $C_j=\varrho^T$ for all j. The operators $M_{\rm diff}$,$M_?$ therefore read

$$\begin{aligned}M_{\rm diff}&=\varrho^T\otimes P_++H\,,\\ M_?&=\varrho^T\otimes P_--H\,.\end{aligned}$$

The support of the selfadjoint operator H is orthogonal to the support of the operator $\varrho^T\otimes P_-$. Since H is traceless it has both positive and negative eigenvalues unless $H=O$. However, positive eigenvalues of H would spoil positivity of $M_?$, so the operator H must vanish, which concludes the proof. □

IV. CONCLUSIONS

The goal of this paper was to find an optimal strategy for comparison of two unknown unitary channels. Exploiting the framework of process POVM we have shown that the optimal strategy achieves the average conditional success probability $\overline{p}_{\rm success}=(d+1)/(2d)$. An interesting observation is that the optimal strategy for comparison of unitary channels is very closely related to the comparison of pure states. In fact, the optimal state comparison is based on the implementation of the two-valued projective measurement measuring the exchange symmetry of the bipartite states. Outcomes are associated with projectors $P_\pm$ onto symmetric and antisymmetric subspaces of the joint Hilbert space. The optimal procedure for the comparison of unitary channels is exploiting the same measurement, but the outcomes are interpreted in the opposite way. Whereas for comparison of pure states the projector P_+ corresponds to the inconclusive result, for unitaries this projector is associated with the unambiguous conclusion that the channels are different. Similarly, the projector P_- indicates the difference of compared pure states, but corresponds to no conclusion for unitaries. In both cases, the unambiguous conclusion that the states, or unitaries are the same, cannot be made.

Devices implementing quantum channels are tested indirectly via their action on quantum states. In the experiment the unknown apparatuses are probed by some test states. We have shown that the optimal solution is achieved if and only if the test state is antisymmetric, i.e. its support is only in antisymmetric subspace. Let us note that if a state is separable, then necessarily its support contains product vectors. However, by definition there is no antisymmetric product vector, hence the support of each antisymmetric state does not contain any product vectors. Consequently, each antisymmetric state is necessarily entangled. In conclusion, the entanglement is the key ingredient for comparison of unitary channels. It enhances the success probability to reach the optimal value.

Let us note that the proposed optimal strategy is feasible in current quantum information experiments with photons and ions. In particular, in the qubit version the experiment consists of preparation of a singlet, application of the unknown single-qubit unitary channels on individual qubits and a projective measurement consisting of the projection onto a singlet, or arbitrary other maximally entangled state. As the measurement we can use, for instance, the Bell measurement, but it is not necessary. Moreover, for the comparison of few qubit unitary channels mixed test states are allowed.

ACKNOWLEDGMENTS

This work was supported by the European Union project QAP 2004-IST-FETPI-15848 and by APVV via projects RPEU-0014-06 and APVV-0673-07 QIAM.

APPENDIX A: AVERAGE UNITARY CHANNEL

In this section we shall prove that the action of the average unitary channel can be expressed as

$$\mathcal{A}[X] = \int_{U(d)} dU\, UXU^\dagger = \frac{\mathrm{tr}[X]}{d} I\,, \tag{A1}$$

where dU is the unique *Haar invariant measure* defined on the group of unitary operators $U(d)$. By definition the image $\mathcal{A}[X]$ of any operator X must commute with all unitary operators, i.e. $[\mathcal{A}[X], U] = 0$ for all $U \in U(d)$. The Schurr lemma implies that $\mathcal{A}[X] = c(X)I$. The transformation $\mathcal{A}$ is by definition trace-preserving. That is, $\mathrm{tr}[X] = c(X)\mathrm{tr}[I] = c(X)d$. It follows that $c(X) = \mathrm{tr}[X]/d$, hence the Eq.(A1) holds.

APPENDIX B: TWIRLING CHANNEL

We shall prove that the action of the twirling channel

$$\mathcal{T}[X] = \int_{U(d)} dU\, U\otimes UXU^\dagger \otimes U^\dagger\,, \tag{B1}$$

on selfadjoint operators X takes the form

$$\mathcal{T}[X] = \frac{\mathrm{tr}[XP_+]}{d_+} P_+ + \frac{\mathrm{tr}[XP_-]}{d_-} P_-\,. \tag{B2}$$

The properties of Haar invariant measure dU implies that the operator $\mathcal{T}[X]$ commutes with all unitary operators of the type $U \otimes U$. If X is selfadjoint, then $\mathcal{T}[X]$ is also selfadjoint and $\mathcal{T}[X] = \sum_j x_j P_j$, where x_j are real eigenvalues and P_j are the corresponding eigenprojectors. The commutation of $\mathcal{T}[X]$ with unitaries $U \otimes U$ implies that $[P_j, U \otimes U] = 0$ for all U. The subspaces $\mathcal{H}_j = P_j(\mathcal{H}_d \otimes \mathcal{H}_d) = \{\psi \in \mathcal{H}_d \otimes \mathcal{H}_d$ such that $P_j\psi = \psi\}$ are invariant under the action of operators $U \otimes U$.

It turns out there are only two invariant subspaces of $\mathcal{H}_d \otimes \mathcal{H}_d$ - *symmetric* and *antisymmetric* subspace. A vector $\psi \in \mathcal{H}_d \otimes \mathcal{H}_d$ is called symmetric (antisymmetric) if $S\psi = \pm\psi$, respectively, where S is the *swap* operator. Let us denote by $P_\pm$ the projectors onto the symmetric and antisymmetric subspaces, respectively. Consider an orthonormal basis of $\mathcal{H}_d$ composed of vectors $\varphi_1, \ldots, \varphi_d$. Defining the vectors $\psi_{j\pm k} = \frac{1}{\sqrt{2}}(\varphi_j \otimes \varphi_k \pm \varphi_k \otimes \varphi_j)$ for $j \neq k$, $\psi_{j+j} = \varphi_j \otimes \varphi_j$ and $\psi_{j-j} = 0$ we can write

$$P_\pm = \sum_{jk} |\psi_{j\pm k}\rangle\langle\psi_{j\pm k}|\,. \tag{B3}$$

Let us note that vectors $\psi_{j\pm k}$ $(j, k = 1, \ldots, d)$ are forming an orthonormal basis of $\mathcal{H}_d \otimes \mathcal{H}_d$ and $S\psi_{j\pm k} = \pm\psi_{j\pm k}$. It follows that the dimensions of symmetric and antisymmetric subspaces are $d_\pm = d(d \pm 1)/2$, respectively. As a result we obtain that

$$\mathcal{T}[X] = a_+(X)P_+ + a_-(X)P_- \tag{B4}$$

is the spectral form of $\mathcal{T}[X]$. In order to verify that Eq.(B1) and Eq.(B2) define the same mapping, it is sufficient to verify their actions on elements of arbitrary operator basis. We shall use an orthonormal operator basis consisting of operators $E_{j\pm k,m\pm n} = |\psi_{j\pm k}\rangle\langle\psi_{m\pm n}|$.

According to Eq.(B4) $\mathrm{tr}[Y^\dagger \mathcal{T}[X]] = 0$ for arbitrary operator Y orthogonal to $P_\pm$, i.e. $\mathrm{tr}[Y^\dagger P_\pm] = 0$. This identity holds for both expressions of $\mathcal{T}$. Consequently, it is sufficient to verify that the values of $\Delta = \mathrm{tr}[P_\pm \mathcal{T}[E_{j\pm k,m\pm n}]]$ coincide for both expressions of the twirling channel given in Eq.(B1) and in Eq.(B2). Direct calculation gives

$$\begin{aligned}\Delta &= \mathrm{tr}[P_\pm \int_{U(d)} dU\, U\otimes U E_{j\pm k,m\pm n} U^\dagger \otimes U^\dagger] \\ &= \mathrm{tr}[E_{j\pm k,m\pm n} \int_{U(d)} dU\, U\otimes U P_\pm U^\dagger \otimes U^\dagger] \\ &= \mathrm{tr}[E_{j\pm k,m\pm n} P_\pm]\end{aligned}$$

and, simultaneuously,

$$\Delta = \frac{\mathrm{tr}[E_{j\pm k,m\pm n}P_+]}{d_+}\mathrm{tr}[P_\pm P_+] + \frac{\mathrm{tr}[E_{j\pm k,m\pm n}P_-]}{d_-}\mathrm{tr}[P_\pm P_-] = \mathrm{tr}[E_{j\pm k,m\pm n}P_\pm] \,.$$

That is, the Eqs.(B2) and (B1) determine the same channel.

[1] C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[2] A.Peres, *Quantum Theory: Concepts and Methods* (Kluwer 1996)
[3] I.D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[4] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[5] A. Peres, Phys. Lett. A **128**, 19 (1988).
[6] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[7] M. Kleinmann, H. Kampermann and D. Bruss, arXiv:0807.3923 (2008)
[8] A. Hayashi, M. Horibe, and T. Hashimoto, Phys. Rev. A **73**, 012328 (2006).
[9] C.Zhang, M.Ying, and B. Qiao Phys. Rev. A **74**, 042308 (2006) [quant-ph/0606189].
[10] G.Wang, M.Ying, Phys. Rev. A **73**, 042301 (2006) [quant-ph/0512142].
[11] A.Chefles, A.Kitagawa, M.Takeoka, M.Sasaki, J.Twamley, J. Phys. A 40 10183-10213 (2007) [quant-ph/0702245].
[12] M.Ziman and T.Heinosaari, Phys. Rev. A **77**, 042321 (2008) [arXiv:0712.3675]
[13] S.M.Barnett, A.Chefles, and I.Jex, Phys. Lett. A **307**, 189 (2003).
[14] A.Chefles, E.Andersson, and I.Jex, J. Phys. A: Math. Gen. 37, 7315 (2004).
[15] M.Kleinmann, H.Kampermann, and D.Bruss, Phys. Rev. A **72**, 032308 (2005).
[16] M.Sedlák, M.Ziman, V.Bužek and M.Hillery, Phys.Rev.A **77**,042304 (2008) [arXiv:0712.1616]
[17] M.Ziman, Phys. Rev. A **77**, 062112 (2008) [arXiv:0802.3862]
[18] G.Chiribella, G.M.D'Ariano, and P.Perinotti, EPL **83** 30004 (2008) [arXiv:0804.0180]
[19] M. Choi, Linear Algebra and its Applications, 10 (3): 285-290, (1975).
[20] A. Jamiolkowski, Rep. Math. Phys. 3, 275 (1972).