scientific reports

Check for updates

OPEN

Local certification of unitary operations

Ryszard Kukulski[1], Mateusz Stępniak[2], Kamil Hendzel[2], Łukasz Pawela[3]✉, Bartłomiej Gardas[3] & Zbigniew Puchała[3]

In this work, we analyze the local certification of unitary quantum channels, which is a natural extension of quantum hypothesis testing. A particular case of a quantum channel operating on two systems corresponding to product states at the input, is considered. The goal is to minimize the probability of the type II error, given a specified maximum probability of the type I error, considering assistance through entanglement with auxiliary systems. Our result indicates connection of the local certification problem with a product numerical range of unitary matrices. We show that the optimal local strategy does not need usage of auxiliary systems and requires only single round of one-way classical communication. Moreover, we compare local and global certification strategies and show that typically local strategies are optimal, yet in some extremal cases, where global strategies make no errors, local ones may fail miserably. Finally, some application for local certification of von Neumann measurements are discussed as well.

In quantum information theory, a well-known problem is the discrimination of states and quantum channels, as solved by Helstrom[1]. This problem involves distinguishing which state or channel from a given pair we are dealing with, based on a prepared measurement. It plays a pivotal role in the comprehension and manipulation of quantum systems. The ensuing step is certification, a process aimed at confirming whether a given hypothesis regarding the state, channel, or measurement holds true; this is achieved by contrasting it with an alternative hypothesis. Certification safeguards the integrity and reliability of quantum operations, rendering it indispensable for quantum computing and communications. The mathematical explanation of the *modus operandi* of quantum computers involves the use of quantum operations and channels. This paper focuses on the local certification of unitary operations, a technique which is crucial for enhancing quantum computing applications, and developing quantum algorithms and error correction strategies. This certification is useful for benchmarking quantum devices, thus steering the progression of quantum algorithm design.

Great deal of work has been done in the domain of local certification and distinguishability of quantum states. The research were focused on presenting conditions for a finite set of orthogonal quantum states to be distinguishable by local operations[2–6]. It has been noticed, that local certification strategies not always are as powerful as global strategies involving usage of a quantum entanglement. Many examples of sets of orthogonal quantum states that cannot be perfectly certified were discovered in the literature[7,8]; also in the domain of mixed quantum states[9].

The following up research about local discrimination of unitary channels has been built upon the results concerning quantum states. It was observed that there exist discrimination problems for which local procedures may be optimal as well as there exist problems for which they perform poorly[10]. Some conditions concerning optimal local discrimination strategies were already proposed too[11]. Eventually, couple of works focused on many copies scenario, were it was shown that any two different unitary operations acting on an arbitrary multipartite quantum system can be perfectly distinguishable by local operations and classical communication when a finite number of runs[12–14]. However, in the literature, the problem of certification of unitary channels has not been yet considered. Taking up this challenge, in this work we explore a scenario where two parties, having access to a shared quantum unitary channel, engage in its certification. We compare local certification strategies with global ones and find the optimal and resource efficient local certification strategies.

Certification is closely related to statistical hypothesis testing, which is a fundamental concept in statistical decision theory[15]. We consider a system with two hypotheses: the null hypothesis (H_0) and the alternative hypothesis (H_1). The null hypothesis intuitively corresponds to a promise about the system given by its creator. By performing a test, we decide which hypothesis to accept as true. A type I error occurs if we reject the null hypothesis when it is true. The probability of this error occurring is called the level of significance. On the other hand, a type II error occurs when we accept the null hypothesis, even though it is false. We want to minimize

[1]Faculty of Physics, Astronomy and Applied Computer Science, Jagiellonian University, ul. Łojasiewicza 11, 30-348 Kraków, Poland. [2]Quantumz.io Sp. z o.o., Puławska 12/3, 02-566 Warsaw, Poland. [3]Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland. ✉email: lpawela@iitis.pl

the type II error given an assumed level of significance. This approach is commonly referred to as certification. It turns out that the concept of the numerical range of a matrix is an useful tool in such issues. The numerical range provides insights into the spectral and structural properties of matrices, making it important in quantum mechanics[16].

Preliminaries

In this section, we elucidate the foundational principles underlying the certification processes under consideration.

Notation

In this work, we will encounter the notation of quantum states, quantum measurements and quantum channels. In order to set notation, we mention them here briefly (see[17] for more detailed explanation).

We say that operator ρ represents a quantum state defined on a system of dimension d if this operator is positive semidefinite ($\rho \geq 0$) with unit trace ($\mathrm{tr}\rho = 1$). An linear map Ψ will be called quantum channel if it is completely positive and trace preserving map (CPTP). We will consider a special family of quantum channels known as unitary channels. For an unitary matrix U we define unitary quantum channel Ψ_U by

$$\Psi_U(\rho) = U\rho U^\dagger, \tag{1}$$

where ρ is an input quantum state ρ.

In a finite-dimensional case, quantum measurement, also called as positive operator-valued measure (POVM), is be represented by a set of positive semidefinite operators $\Omega = \{\Omega_i\}_i$ (also known as effects), such that $\sum_i \Omega_i = \mathbb{1}$. According to the Born rule, for a given state ρ the probability of obtaining the measurement outcome i is given by $p_i = \mathrm{Tr}\rho\Omega_i$. The special subclass of quantum measurements consists of Von Neumann measurements. They fulfill the additional requirement that all effects Ω_i are rank-one projectors. Hence, for a von Neumann measurement acting on a state of dimension d there are exactly d effects Ω_i which are pairwise orthogonal. This simple observation allows us to parameterize a d-dimensional von Neumann measurement using a unitary matrix U, $P_U = \{U|i\rangle\langle i|U^\dagger\}_{i=1}^d$. As a shorthand notation, we will write $|u_i\rangle := U|i\rangle$. We can associate a measure-and-prepare channel with a von Neumann measurement

$$P_U(\rho) = \sum_{i=1}^{d} \langle u_i|\rho|u_i\rangle |i\rangle\langle i|. \tag{2}$$

Finally, in this work we will consider the family of bipartite quantum channels and measurements that can be realized by using only local operations and classical communication (LOCC) between two involved parties, say Alice and Bob. Let us assume that Alice has access to a system $\mathcal{A}$ and Bob to a system $\mathcal{B}$. Then, we say that bipartite quantum channel Ψ (or measurement Ω) is LOCC with respect to the partition $\mathcal{A} : \mathcal{B}$, if it can be realized by using local quantum operations on $\mathcal{A}$ and $\mathcal{B}$ separately, and by sharing classical information between $\mathcal{A}$ and $\mathcal{B}$. Such operations will be used notoriously in this work to prepare input quantum states and POVMs without creating quantum entanglement between involved parties.

Numerical ranges of a matrix

In the context of certifying unitary channels, the numerical range and the product numerical range play a pivotal role. The *numerical range* of a square matrix X of size d, is defined as a subset of the complex plane:

$$W(X) = \{\langle\psi|X|\psi\rangle : \langle\psi|\psi\rangle = 1, |\psi\rangle \in \mathbb{C}^d\}. \tag{3}$$

The set $W(X)$ is compact and convex; an in depth discussion of its properties and application can be found in[18,19].

The *product numerical range* of a square matrix X of size $d_1 \cdot d_2$ with the partition $d_1 : d_2$ is defined as:

$$\begin{aligned} W^{\otimes}_{d_1:d_2}(X) = \{&(\langle\psi_1| \otimes \langle\psi_2|)X(|\psi_1\rangle \otimes |\psi_2\rangle) : \\ &\langle\psi_1|\psi_1\rangle = 1, \langle\psi_2|\psi_2\rangle = 1, \\ &|\psi_1\rangle \in \mathbb{C}^{d_1}, |\psi_2\rangle \in \mathbb{C}^{d_2}\}. \end{aligned} \tag{4}$$

The core properties of this object are described in[20].

Operational scenario

In the certification of a unitary channel, two parties, Alice and Bob, have an access to a quantum unitary channel. They have knowledge that the given channel is one of two possible unitary channels: Ψ_U, which will be identified with H_0 hypothesis or Ψ_V, which will be identified with H_1 hypothesis. Alice and Bob do not know which one is provided to them. Their goal is to find the best strategy to certificate that the given unknown channel is Ψ_U and detect whenever the unknown operation is Ψ_V. More precisely, given the level of significance $\delta \geq 0$ as a

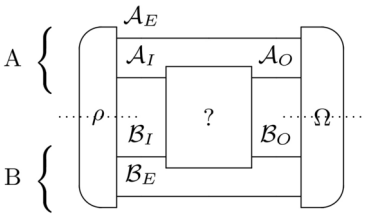

Fig. 1. Schematic representation of the operational scenario for unitary channel certification. Alice (**A**) and Bob (**B**) can prepare the initial state ρ and the final measurement Ω by using LOCC operations to certificate if $? = \Psi_U$ or $? = \Psi_V$.

parameter, they want to minimize the probability of making type II error provided the probability of making type I error is not greater than δ.

The unknown operation has two inputs on the spaces $\mathcal{A}_I$ and $\mathcal{B}_I$, and two outputs on the spaces $\mathcal{A}_O$ and $\mathcal{B}_O$ (see Fig. 1). Alice has an access to spaces $\mathcal{A}_I$ and $\mathcal{A}_O$ and auxiliary space $\mathcal{A}_E$, while Bob to $\mathcal{B}_I$ and $\mathcal{B}_O$ and auxiliary system $\mathcal{B}_E$, respectively. To produce an input state ρ Alice and Bob are limited to use LOCC operations with respect to the partition $\mathcal{A}_I \otimes \mathcal{A}_E : \mathcal{B}_I \otimes \mathcal{B}_E$. We will write in short that $\rho \in \texttt{LOCC}$. Similarly, to produce a POVM $\Omega = \{\Omega_0, \Omega_1\}$ Alice and Bob are limited to use LOCC operations with respect to the partition $\mathcal{A}_O \otimes \mathcal{A}_E : \mathcal{B}_O \otimes \mathcal{B}_E$. We will use the notation $\Omega \in \texttt{LOCC}$. Based on the results (classical labels) of their measurements, they decide, which unitary channel they are dealing with: label 0 associated with the effect Ω_0 indicates H_0, while label 1 associated with the effect Ω_1 indicates H_1.

Main results

Unitary channel certification

In this section we will state the solution to the problem introduced in the Section 2.3. Let $\mathcal{A}_I = \mathcal{A}_O = \mathbb{C}^{d_1}$, $\mathcal{B}_I = \mathcal{B}_O = \mathbb{C}^{d_2}$. We are given two unitary matrices U and V of size $d_1 \cdot d_2$ and consider two hypotheses:

- H_0: The operation is Ψ_U.
- H_1: The operation is Ψ_V.As mentioned previously (see also Fig. 1), Alice and Bob can prepare the input state ρ and the measurement $\Omega = \{\Omega_0, \Omega_1\}$ by using LOCC operations with respect to the partitions $\mathcal{A}_I \otimes \mathcal{A}_E : \mathcal{B}_I \otimes \mathcal{B}_E$ and $\mathcal{A}_O \otimes \mathcal{A}_E : \mathcal{B}_O \otimes \mathcal{B}_E$, respectively. The dimension of spaces $\mathcal{A}_E$ and $\mathcal{B}_E$ are arbitrary. Alice and Bob accept accept the null hypothesis if the measurement result is Ω_0, otherwise, they reject it. Thus, we arrive at the following formulas for the probabilities of type I and type II errors:

$$\begin{aligned} p_{\mathrm{I}}(\Omega, \rho) &= \mathrm{tr}\left(\Omega_1(\Psi_U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E})(\rho)\right), \\ p_{\mathrm{II}}(\Omega, \rho) &= \mathrm{tr}\left(\Omega_0(\Psi_V \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E})(\rho)\right). \end{aligned} \tag{5}$$

Certification requires minimizing p_{II} under the condition $p_{\mathrm{I}} \leq \delta$, where δ is the desired significance level. It leads to the following optimization problem:

$$p_{\mathrm{II}}(U, V) := \min\{p_{\mathrm{II}}(\Omega, \rho) : p_{\mathrm{I}}(\Omega, \rho) \leq \delta, \rho, \Omega \in \texttt{LOCC}\}. \tag{6}$$

The remainder of this section is devoted to proving the following theorem. This result shows the relation between two-party certification and the product numerical range.

Theorem 1 *Consider the problem of two-point certification of unitary channels with hypotheses*

- H_0*: The operation is* Ψ_U.
- H_1*: The operation is* Ψ_V*.defined as in Section 3.1 for unitary matrices U and V of size* $d_1 \cdot d_2$*, and statistical significance* $\delta \in [0, 1]$*. Let z be the euclidean distance between* 0 *and* $W^{\otimes}_{d_1:d_2}(V^\dagger U)$*, that is*

$$z := \min\{|x| : x \in W^{\otimes}_{d_1:d_2}(V^\dagger U)\}. \tag{7}$$

Then, for the most powerful test utilizing LOCC operations, the probability of the type II error yields

$$p_{\mathrm{II}}(U, V) = \begin{cases} 0, & z \leq \sqrt{\delta}, \\ \left(z\sqrt{1-\delta} - \sqrt{1-z^2}\sqrt{\delta}\right)^2, & z > \sqrt{\delta}. \end{cases} \tag{8}$$

Proof By utilizing local quantum operations and classical communication, Alice and Bob can prepare any separable quantum state $\rho = \sum_j p_j |a_j\rangle\langle a_j| \otimes |b_j\rangle\langle b_j|$, where $|a_j\rangle\langle a_j|$ are defined on $\mathcal{A}_I \otimes \mathcal{A}_E$ and $|b_j\rangle\langle b_j|$ on $\mathcal{B}_I \otimes \mathcal{B}_E$.

Let us assume that Alice and Bob take a product state, that is $\rho = |a,b\rangle\langle a,b| = |a\rangle\langle a| \otimes |b\rangle\langle b|$. Then, depending which hypothesis is true, we obtain the one of the following pure states

$$\begin{aligned} H_0: &\quad |h_0\rangle\langle h_0| := (\Psi_U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E})(\rho), \\ H_1: &\quad |h_1\rangle\langle h_1| := (\Psi_V \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E})(\rho). \end{aligned} \tag{9}$$

We consider two cases. If $|\langle h_0|h_1\rangle| \leq \sqrt{\delta}$, then according to[21], Theorem 1 & Corollary 1 the best pure states certification strategy $\widetilde{\Omega}$ with significance level δ is of the form: $\widetilde{\Omega} = \{\widetilde{\Omega_0}, \widetilde{\Omega_1}\}$, where $\widetilde{\Omega_0} = |\omega\rangle\langle\omega|$ for $|\omega\rangle = \frac{|\widetilde{\omega}\rangle}{\||\widetilde{\omega}\rangle\|}$ and $|\widetilde{\omega}\rangle = |h_0\rangle - \langle h_1|h_0\rangle|h_1\rangle$. The operator $|\omega\rangle\langle\omega|$ satisfies $|\langle h_1|\omega\rangle|^2 = 0$ and $|\langle h_0|\omega\rangle|^2 \geq 1-\delta$. Therefore, the states $|h_1\rangle\langle h_1|$ and $|\omega\rangle\langle\omega|$ are orthogonal and we can find a LOCC measurement $\Omega = \{\Omega_0, \Omega_1\}$[22], such that $\mathrm{tr}(\Omega_0|\omega\rangle\langle\omega|) = 1$ and $\mathrm{tr}(\Omega_1|h_1\rangle\langle h_1|) = 1$. Alice and Bob choose Ω as their measurement and achieve $p_{\mathrm{I}}(\Omega,\rho) = \mathrm{tr}(\Omega_1|h_0\rangle\langle h_0|) \leq 1 - \mathrm{tr}(|\omega\rangle\langle\omega||h_0\rangle\langle h_0|) \leq \delta$ and $p_{\mathrm{II}}(\Omega,\rho) = 1 - \mathrm{tr}(\Omega_1|h_1\rangle\langle h_1|) = 0$, which is the optimal solution in that case.

If $|\langle h_0|h_1\rangle| > \sqrt{\delta}$, then according to[21], Theorem 1 & Corollary 1 the best pure states certification strategy $\widetilde{\Omega}$ with significance level δ is of the form: $\widetilde{\Omega} = \{\widetilde{\Omega_0}, \widetilde{\Omega_1}\}$, where $\widetilde{\Omega_0} = |\omega\rangle\langle\omega|$ for $|\omega\rangle = \sqrt{1-\delta}\frac{\langle h_0|h_1\rangle}{|\langle h_0|h_1\rangle|}|h_0\rangle - \sqrt{\delta}|h_0^{\perp}\rangle$ and $|h_0^{\perp}\rangle = |\widetilde{h_0^{\perp}}\rangle / \||\widetilde{h_0^{\perp}}\rangle\|$, where $|\widetilde{h_0^{\perp}}\rangle = |h_1\rangle - \langle h_0|h_1\rangle|h_0\rangle$. The operator $|\omega\rangle\langle\omega|$ satisfies $|\langle h_1|\omega\rangle|^2 = (\sqrt{1-\delta}|\langle h_0|h_1\rangle| - \sqrt{\delta}\sqrt{1-|\langle h_0|h_1\rangle|^2})^2$ and $|\langle h_0|\omega\rangle|^2 = 1-\delta$. Here, for the orthogonal states $|\omega\rangle\langle\omega|$ and $|\omega^{\perp}\rangle\langle\omega^{\perp}|$, where $|\omega^{\perp}\rangle = \sqrt{\delta}|h_0\rangle + \sqrt{1-\delta}\frac{\langle h_1|h_0\rangle}{|\langle h_0|h_1\rangle|}|h_0^{\perp}\rangle$ we can find a LOCC measurement $\Omega = \{\Omega_0, \Omega_1\}$ [22], such that $\mathrm{tr}(\Omega_0|\omega\rangle\langle\omega|) = 1$ and $\mathrm{tr}(\Omega_1|\omega^{\perp}\rangle\langle\omega^{\perp}|) = 1$. Alice and Bob choose Ω as their measurement and achieve $p_{\mathrm{I}}(\Omega,\rho) = \mathrm{tr}(\Omega_1|h_0\rangle\langle h_0|) \leq 1 - \mathrm{tr}(|\omega\rangle\langle\omega||h_0\rangle\langle h_0|) = \delta$. To calculate $p_{\mathrm{II}}(\Omega,\rho)$ notice that $|h_1\rangle$ is spanned in the basis $|\omega\rangle, |\omega^{\perp}\rangle$, that is $|h_1\rangle = c_1|\omega\rangle + c_2|\omega^{\perp}\rangle$. Therefore, we get $p_{\mathrm{II}}(\Omega,\rho) = \mathrm{tr}(\Omega_0|h_1\rangle\langle h_1|) = |c_1|^2\mathrm{tr}(\Omega_0|\omega\rangle\langle\omega|) = |c_1|^2$, where we used $\Omega_0|\omega^{\perp}\rangle = |\omega^{\perp}\rangle - \Omega_1|\omega^{\perp}\rangle = |\omega^{\perp}\rangle - |\omega^{\perp}\rangle = 0$. Eventually, $p_{\mathrm{II}}(\Omega,\rho) = |c_1|^2 = |\langle h_1|\omega\rangle|^2$, which is the optimal solution in that case.

We have showed that the optimal measurement Ω for product state ρ gives

$$p_{\mathrm{II}}(\Omega,\rho) = \begin{cases} 0, & |x| \leq \sqrt{\delta}, \\ (\sqrt{1-\delta}|x| - \sqrt{\delta}\sqrt{1-|x|^2})^2, & |x| > \sqrt{\delta}, \end{cases} \tag{10}$$

where $x := \langle h_1|h_0\rangle = \langle a,b|\left(V^{\dagger}U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E}\right)|a,b\rangle$. As the function $|x| \mapsto p_{\mathrm{II}}(\Omega,\rho)$ is non-decreasing, Alice and Bob choose $|a,b\rangle$ that minimizes $|x|$.

Observe, the choice of the optimal product input state $\rho = |a,b\rangle\langle a,b|$ is independent of the significance level δ. Therefore, no separable state ρ will provide better result than product state.

Finally, let us assume that $\rho = |a_0,b_0\rangle\langle a_0,b_0|$ is the optimal product input state - it minimizes $|a,b\rangle\langle a,b| \mapsto |\langle a,b|\left(V^{\dagger}U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E}\right)|a,b\rangle|$. Let $\mathcal{A}_E = \mathbb{C}^{e_1}$ and $\mathcal{B}_E = \mathbb{C}^{e_2}$. Using the result from[13], Lemma 2 we get

$$\begin{aligned} &\langle a_0,b_0|\left(V^{\dagger}U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E}\right)|a_0,b_0\rangle \\ \in &W^{\otimes}_{d_1 e_1 : d_2 e_2}(V^{\dagger}U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E}) \\ = &W^{\otimes}_{d_1:d_2}(V^{\dagger}U). \end{aligned} \tag{11}$$

Hence, there is a quantum state $|A_0\rangle\langle A_0|$ defined on the space $\mathcal{A}_I$ and a quantum state $|B_0\rangle\langle B_0|$ on the space $\mathcal{B}_I$, such that $\langle a_0,b_0|\left(V^{\dagger}U \otimes \mathbb{1}_{\mathcal{A}_E \otimes \mathcal{B}_E}\right)|a_0,b_0\rangle = \langle A_0,B_0|V^{\dagger}U|A_0,B_0\rangle$. Eventually, we observe that to minimize $|x|$ Alice and Bob do not need to use auxiliary systems $\mathcal{A}_E$ and $\mathcal{B}_E$ and the optimal state can be chosen as $\rho = |A_0,B_0\rangle\langle A_0,B_0|$, which is defined on $\mathcal{A}_I \otimes \mathcal{B}_I$. Hence, for $z = \min\{\left|\langle a,b|V^{\dagger}U|a,b\rangle\right| : \langle a|a\rangle = \langle b|b\rangle = 1, |a\rangle \in \mathbb{C}^{d_1}, |b\rangle \in \mathbb{C}^{d_2}\} = \min\{|x| : x \in W^{\otimes}_{d_1:d_2}(V^{\dagger}U)\}$ we achieve the desired result

$$p_{\mathrm{II}}(U,V) = \begin{cases} 0, & z \leq \sqrt{\delta}, \\ (\sqrt{1-\delta}z - \sqrt{\delta}\sqrt{1-z^2})^2, & z > \sqrt{\delta}. \end{cases} \tag{12}$$

□

Optimal certification strategy

The proof of Theorem 1 provides insight of the best certification strategy that Alice and Bob can utilize. Starting from the input state $\rho \in \mathtt{LOCC}$, we see that Alice does not have to create any entanglement between $\mathcal{A}_I$ and $\mathcal{A}_E$, what is more - she does not need to use auxiliary system $\mathcal{A}_E$ at all. The same holds for Bob's systems. That optimal input state $\rho = |a,b\rangle\langle a,b|$ defined on $\mathcal{A}_I \otimes \mathcal{B}_I$ is pure and product as well it minimizes $|\langle a,b|V^{\dagger}U|a,b\rangle|$. It is independent from the significance level δ.

The explicit form of the optimal measurement $\Omega \in \mathtt{LOCC}$ is more complicated and relies heavily on the construction provided in[22] and the proof of Theorem 1. Also, its description changes with δ. Nevertheless, from the operational point of view, Ω can be simply realized by Alice and Bob. One party, let's say Alice, prepares an appropriate Von Neumann measurement P_{R_A} on system $\mathcal{A}_O$, where R_A is an unitary rotation and sends the

measurement result i as a classical information to Bob. Then, he prepares a Von Neumann measurement $P_{R_B|_i}$ on $\mathcal{B}_O$, conditioned on the information gained from Alice, where $R_B|_i$ is an unitary rotation. Bob's measurement result j after classical post-processing $j \mapsto f(j) \in \{0,1\}$ indicates if the hypothesis H_0 should be accepted or rejected. We provide a schematic representation of the optimal strategy in Fig. 2.

Local vs global certification of unitary channels

In the case where a single party controls both inputs and outputs, the party can create entanglement between compound systems $\mathcal{A}_I \otimes \mathcal{A}_E$ and $\mathcal{B}_I \otimes \mathcal{B}_E$ (similarly between $\mathcal{A}_O \otimes \mathcal{A}_E$ and $\mathcal{B}_O \otimes \mathcal{B}_E$). In other words, the input state ρ can be chosen arbitrarily, also the measurement $\Omega = \{\Omega_0, \Omega_1\}$. The certification result $p^*_{\text{II}}(U,V)$ is expressed as[21]:

$$p^*_{\text{II}}(U,V) = \begin{cases} 0, & v \leq \sqrt{\delta}, \\ \left(v\sqrt{1-\delta} - \sqrt{1-v^2}\sqrt{\delta}\right)^2, & v > \sqrt{\delta}, \end{cases} \tag{13}$$

where

$$v := \min\{|x| : x \in W(V^\dagger U)\}. \tag{14}$$

As we can see, the certification results differ in local and global scenarios. Observe, that both results depend on the product $V^\dagger U$, hence, the results are unitarily invariant and we may assume that $V = \mathbb{1}$ for the remainder of this section. In the global case we are interested in computing the distance $v(U) := \min\{|x| : x \in W(U)\}$, while for the local case we compute the distance $z_{d_1:d_2}(U) := \min\{|x| : x \in W^{\otimes}_{d_1:d_2}(U)\}$. The forthcoming comparison of $z_{d_1:d_2}(U)$ and $v(U)$ will enable a comparative analysis between single-party and two-party certification scenarios.

From the definition, for all unitary matrices U of size $d_1 \cdot d_2$ it holds $v(U) \leq z_{d_1:d_2}(U)$. The questions arise, can $v(U)$ be strictly lower than $z_{d_1:d_2}(U)$ and how much lower it can be?

Let $d = d_1 = d_2$. Define

$$U = \mathbb{1}_{d^2} - \frac{2}{d}|\mathbb{1}_d\rangle\langle\mathbb{1}_d|, \tag{15}$$

where $|\mathbb{1}_d\rangle = \sum_{i=1}^{d} |i,i\rangle$. Observe that the eigenvalues of U are ± 1, so $v(U) = 0$ and therefore, $p^*_{\text{II}}(U, \mathbb{1}_{d^2}) = 0$. On the other hand, for any normed vectors $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^d$ we have

$$|\langle\psi_1,\psi_2|U|\psi_1,\psi_2\rangle| = \left|1 - \frac{2}{d}|\langle\psi_1|\overline{\psi_2}\rangle|^2\right| \geq \frac{d-2}{d}, \tag{16}$$

where to saturate the last inequality we take $|\psi_1\rangle = |\psi_2\rangle = |1\rangle$. That means, $z_{d_1:d_2}(U) = (d-2)/d$ and when the local dimension goes to infinity, $d \to \infty$, then we have $p_{\text{II}}(U, \mathbb{1}_{d^2}) \to 1 - \delta$.

We showed that in the extremal case, local and global strategies differ significantly. But what about a typical case? For the incoming analysis we assume that U is Haar-random unitary matrix[23]. We have the following theorem.

Theorem 2 *Let U be a Haar-random unitary matrix of size $d_1 \cdot d_2$. For large enough product $d_1 d_2$ we have*

$$\mathbb{P}\left(z_{d_1:d_2}(U) = 0\right) \geq 1 - \exp\left(-\frac{\log 2}{2}\max(d_1^2, d_2^2)\right). \tag{17}$$

Proof Without loss of the generality let us assume that $d_2 \geq d_1$. For a fixed state $|1\rangle \in \mathbb{C}^{d_1}$ denote $M = (\langle 1| \otimes \mathbb{1})U(|1\rangle \otimes \mathbb{1})$. We have then $W(M) \subset W^{\otimes}_{d_1:d_2}(U)$. As U is Haar distributed the matrix M has the same distribution as VM, where V is a Haar-random unitary matrix of size d_2 independent of U. The matrix M is a truncation of U, hence, almost surely it has full rank[24]. Continuing the reasoning, if $M = U_M Q_M$ is the polar decomposition of M, then VM has the same distribution as VQ_M. Let λ_i be eigenvalues of V with corresponding eigenvectors $|x_i\rangle$. Then $\langle x_i|VQ_M|x_i\rangle = \lambda_i\langle x_i|Q_M|x_i\rangle \in W(VQ_M)$ for each i, where almost surely $\langle x_i|Q_M|x_i\rangle > 0$. Therefore, if $0 \in W(V)$, then there is a probability vector $(p_i)_i$ such that $\sum_i \lambda_i p_i = 0$. Let us

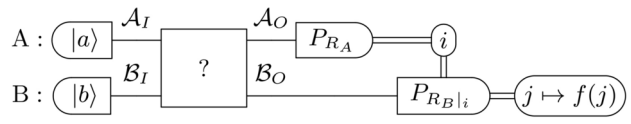

Fig. 2. Schematic representation of the optimal operational scenario for unitary channel certification. Alice (**A**) prepares the initial pure state $|a\rangle\langle a|$ and Bob (**B**) prepares $|b\rangle\langle b|$. The final measurement consists of Alice preparing P_{R_A} and sending the result label i to Bob, who prepares the measurement $P_{R_B|_i}$. The post-processed label $j \mapsto f(j) \in \{0,1\}$ of Bob's measurement certificate if $? = \Psi_U$ or $? = \Psi_V$.

define a probability vector $(q_i)_i$ given by $q_i = \frac{p_i}{\langle x_i|Q_M|x_i\rangle}\left(\sum_j \frac{p_j}{\langle x_j|Q_M|x_j\rangle}\right)^{-1}$. We obtain $\sum_i q_i\lambda_i\langle x_i|Q_M|x_i\rangle = 0$ which implies $0 \in W(VQ_M)$. Combining all together we get

$$\begin{aligned}\mathbb{P}\left(z_{d_1:d_2}(U)=0\right) &\geq \mathbb{P}\left(0\in W(M)\right) = \mathbb{P}\left(0\in W(VQ_M)\right)\\ &\geq \mathbb{P}\left(0\in W(V)\right) \geq 1-\exp\left(-\frac{\log 2}{2}d_2^2\right),\end{aligned} \tag{18}$$

where the last inequality was proven in[25], Proposition 19 for large enough d_2. □

According to Theorem 2, when we are dealing with high-dimensional unitary channels Ψ_U and Ψ_V, most of them can be perfectly certified. What is more, the optimal strategy is local, uses only once one-way classical communication channel and does not need auxiliary systems (see Fig. 2). Such strategies are the most desirable in terms of used resources such as quantum entanglement[26].

In this section, we learned that the gap between $\nu(U)$ and $z_{d_1:d_2}(U)$ may be huge in extremal cases. Also, we observed that typically in high dimensions both quantities are equal to zero. We provide more examples comparing local and global strategies in the Supplementary Material.

Application to Von Neumann measurement certification

In the domain of von Neumann measurements certification, we are given two unitary matrices U and V of size $d_1 \cdot d_2$ and consider two hypotheses:

- H_0: The operation is P_U.
- H_1: The operation is P_V.The operational paradigm is similar, yet it harbors a critical distinction: the output transitions to a classical domain. Upon executing a joint measurement on their respective quantum states, a classical label *i* is generated. This label, mutually acknowledged by Alice and Bob, serves as the foundational element for subsequent certification processes. Thereafter, both parties then measure their auxiliary systems, guided by the known label *i*, to ascertain whether the joint measurement was null of the alternative hypothesis. As in the unitary channel certification Alice and Bob strategy is similar (see Fig. 1). They can prepare the input state $\rho \in \texttt{LOCC}$ and the measurement $\Omega = \{\Omega_0, \Omega_1\} \in \texttt{LOCC}$ while having access to auxiliary systems $\mathcal{A}_E$ and $\mathcal{B}_E$ of arbitrary dimension. Let $\widetilde{p_{\text{II}}}(U,V)$ indicates minimized probability of type II error under the condition that δ is given significance level for the introduced certification scheme of Von Neumann measurements. Then, we summarize our findings with the following proposition:

Proposition 3 *Consider the problem of two-point certification of Von Neumann measurements defined for unitary matrices U and V of size $d_1 \cdot d_2$, and statistical significance $\delta \in [0,1]$ with hypotheses*

- *H_0: The operation is P_U.*
- *H_1: The operation is P_V.The most powerful test utilizing LOCC operations provides*

$$\begin{aligned}\widetilde{p_{\text{II}}}(U,V) \geq \max\{p_{\text{II}}(UE,VF) : E,F \text{ is unitary}\\ \text{and diagonal}\}.\end{aligned} \tag{19}$$

Proof Observe that action of each von Neumann measurement P_U, can be expressed as $P_U = \Delta\Psi_{(UE)^\dagger}$. Here, Δ is the completely dephasing channel $\Delta(X) = \sum_i \langle i|X|i\rangle|i\rangle\langle i|$ and E is a diagonal unitary matrix. The channel Δ acting on $\mathcal{A}_O \otimes \mathcal{B}_O$ is equivalent to $\Delta = \Delta_A \otimes \Delta_B$, where Δ_A, Δ_B are completely dephasing channels acting on $\mathcal{A}_O$ and $\mathcal{B}_O$, respectively. Let us fix $\rho_*, \Omega_* \in \texttt{LOCC}$ as the optimal certification strategy achieving $\widetilde{p_{\text{II}}}(U,V)$. For the unitary channel certification between $\Psi_{(UE)^\dagger}$ and $\Psi_{(VF)^\dagger}$, where E, F are diagonal, unitary matrices, we have

$$p_{\text{II}}(\Omega_*(\Delta_A \otimes \Delta_B \otimes \mathbb{1}_{\mathcal{A}_E\otimes\mathcal{B}_E}), \rho_*) = \widetilde{p_{\text{II}}}(P_U, P_V). \tag{20}$$

Eventually, we get $p_{\text{II}}(UE,VF) \leq \widetilde{p_{\text{II}}}(P_U,P_V)$, which ends the proof. □

Summary

In this study, we explored a scenario where two parties, having access to a shared quantum unitary channel, engage in its certification. Each party conducts individual measurements on their respective systems following channel utilization. We demonstrated in Theorem 1 that the certification challenge can be effectively transformed into an optimization problem involving the product numerical range. Following the proof of Theorem 1, we concluded that the optimal local strategy does not need usage of auxiliary systems and parties involved need to utilize one-way classical communication channel. We provided the original considered scheme in Fig. 1 and the optimal and resource efficient scheme in Fig. 2.

In Section 3.3 we compared local certification strategies with global ones. We observed that in the extremal case a global (single party) strategy can make no type II errors, while for the best local strategy the probability of making type II error approaches $1-\delta$, where δ is the significance level. However, in Theorem 2 we proved that typically, for high-dimensional unitary channels, local certification strategies are optimal and what is more, they make no type II errors. Assuming Haar distribution of unitary channels of size *d*, the probability of perfect local certification is no smaller than $1-\exp(-\frac{\log 2}{2}d)$, which is approaching exponentially fast to 1 as $d \to \infty$.

Regarding von Neumann measurements, our findings in Proposition 3 provide insights into the lower bound of the type II error, thus contributing partial but significant knowledge to the field of quantum measurement certification.

Our work opens new paths for future research. They could include more advanced comparison of $\nu(U)$ and $z_{d_1:d_2}(U)$ as well as finding effective ways of computing $z_{d_1:d_2}(U)$ for arbitrary U. From the operational point of view, the scenario where many players are involved in the local certification process seems to be interesting to explore. As the results of our work are based strongly on LOCC measurements' construction provided in[22] which is also valid in many players scenario, quick analysis suggests that the Eq. (8) will be valid in that case, but with replaced

$$z \leftarrow \min\{|x| : x \in W^{\otimes}_{d_1:\ldots:d_N}(V^{\dagger}U)\}, \tag{21}$$

where $W^{\otimes}_{d_1:\ldots:d_N}$ is the product numerical range defined for N parties[13].

Availability of data and materials

The authors declare that the data supporting the findings of this study are available within the paper and its supplementary information files. The code used to create the plots in the Supplementary Material is available at https://github.com/iitis/NumericalShadow.jl

Received: 31 January 2024; Accepted: 3 October 2024
Published online: 04 November 2024

References

1. Helstrom, C. W. Quantum detection and estimation theory. *J. Stat. Phys.* **1**, 231. https://doi.org/10.1007/BF01007479 (1970).
2. Ghosh, S., Kar, G., Roy, A. & Sarkar, D. Distinguishability of maximally entangled states. *Phys. Rev. A-Atomic Molecular Optical Phys.* **70**, 022304 (2004).
3. Nathanson, M. Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases. *J. Math. Phys.*[SPACE]https://doi.org/10.1063/1.1914731 (2005).
4. Duan, R., Feng, Y., Xin, Y. & Ying, M. Distinguishability of quantum states by separable operations. *IEEE Trans. Inf. Theory* **55**, 1320 (2009).
5. Childs, A. M., Leung, D., Mančinska, L. & Ozols, M. A framework for bounding nonlocality of state discrimination. *Commun. Math. Phys.* **323**, 1121 (2013).
6. Zhang, X., Guo, C., Luo, W. & Tan, X. Local distinguishability of quantum states in bipartite systems arXiv preprint arXiv:1712.08830 (2017)
7. Fan, H. Distinguishability and indistinguishability by local operations and classical communication. *Phys. Rev. Lett.* **92**, 177905 (2004).
8. Zhang, Z.-C., Gao, F., Cao, Y., Qin, S.-J. & Wen, Q.-Y. Local indistinguishability of orthogonal product states. *Phys. Rev. A* **93**, 012314 (2016).
9. Calsamiglia, J., De Vicente, J., Muñoz-Tapia, R. & Bagan, E. Local discrimination of mixed states. *Phys. Rev. Lett.* **105**, 080504 (2010).
10. Matthews, W., Piani, M. & Watrous, J. Entanglement in channel discrimination with restricted measurements. *Phys. Rev. A-Atomic Molecular Opt. Phys.* **82**, 032302 (2010).
11. Bae, J. Discrimination of two-qubit unitaries via local operations and classical communication. *Sci. Rep.* **5**, 18270 (2015).
12. Duan, R., Feng, Y. & Ying, M. Entanglement is not necessary for perfect discrimination between unitary operations. *Phys. Rev. Lett.* **98**, 100503 (2007).
13. Duan, R., Feng, Y. & Ying, M. Local distinguishability of multipartite unitary operations. *Phys. Rev. Lett.* **100**, 020503 (2008).
14. Cao, T.-Q. et al. Minimal number of runs and the sequential scheme for local discrimination between special unitary operations. *Sci. Rep.* **6**, 26696 (2016).
15. Emmert-Streib, F. & Dehmer, M. Understanding statistical hypothesis testing: The logic of statistical inference. *Machine Learning Knowl. Extraction* **1**, 945. https://doi.org/10.3390/make1030054 (2019).
16. Gawron, P., Puchała, Z., Miszczak, J. A., Skowronek, Ł & Życzkowski, K. Restricted numerical range: a versatile tool in the theory of quantum information. *J. Math. Phys.* **51**, 102204. https://doi.org/10.1063/1.3496900 (2010).
17. Watrous, J. The theory of quantum information *title The theory of quantum information* (publisher Cambridge University Press, 2018)
18. Fiedler, M. Geometry of the numerical range of matrices. *Linear Algebra Appl.* **37**, 81. https://doi.org/10.1016/0024-3795(81)90169-5 (1981).
19. Dunkl, C. F. et al. Numerical shadow and geometry of quantum states. *J. Phys. A: Math. Theor.* **44**, 335301. https://doi.org/10.1088/1751-8113/44/33/335301 (2011).
20. Puchała, Z. et al. Product numerical range in a space with tensor product structure. *Linear Algebra Appl.* **434**, 327. https://doi.org/10.1016/j.laa.2010.08.026 (2011).
21. Lewandowska, P., Krawiec, A., Kukulski, R., Pawela, Ł & Puchała, Z. On the optimal certification of von Neumann measurements. *Sci. Rep.* **11**, 1. https://doi.org/10.1038/s41598-021-81325-1 (2021).
22. Walgate, J., Short, A. J., Hardy, L. & Vedral, V. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.* **85**, 4972 (2000).
23. Życzkowski, K. & Kuś, M. Random unitary matrices. *J. Phys. A: Math. Gen.* **27**, 4235 (1994).
24. Życzkowski, K. & Sommers, H.-J. Truncations of random unitary matrices. *J. Phys. A: Math. Gen.* **33**, 2045 (2000).
25. Nechita, I., Puchała, Z., Pawela, Ł & Życzkowski, K. Almost all quantum channels are equidistant. *J. Math. Phys.*[SPACE]https://doi.org/10.1063/1.5019322 (2018).
26. Chitambar, E. & Gour, G. Quantum resource theories. *Rev. Mod. Phys.* **91**, 025001 (2019).

Acknowledgements

MS and KH acknowledge support received from The National Centre for Research and Development (NCBR), Poland, under Project No. POIR.01.01.01-00-0061/22, titled *VeloxQ: Utilizing Dynamic Systems in Decision-Making Processes Based on Knowledge Acquired Through Machine Learning, Across Various Levels of Complexity, in*

Industrial Process Optimization, that aims to develop digital solutions for solving combinatorial optimization problems. The focus is on leveraging quantum-inspired algorithms and artificial intelligence to enhance decision-making processes in industrial optimization contexts. The insights and knowledge gained during the research phase of this project have significantly shaped the content and findings of this article. RK acknowledges financial support by the National Science Centre, Poland, under the contract number 2021/03/Y/ST2/00193 within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101017733. This project was supported by the National Science Center (NCN), Poland, under Projects: SONATA BIS 10, No. 2020/38/E/ST3/00269 (LP, BG) and OPUS, No 2022/47/B/ST6/02380 (ZP).

Author contributions

ZP set the research goal. LP and MS performed numerical simulations. MS prepared the figures. RK and LP prepared revised version of main result. All authors wrote the main manuscript text. All authors reviewed the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-024-75148-z.

Correspondence and requests for materials should be addressed to Ł.P.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.