Robust certification of arbitrary outcome quantum measurements from temporal correlations

Debarshi Das[1,2], Ananda G. Maity[1], Debashis Saha[1], and A. S. Majumdar[1]

[1]S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India
[2]Department of Physics and Astronomy, University College London, Gower Street, WC1E 6BT London, UK

Certification of quantum devices received from unknown providers is a primary requirement before utilizing the devices for any information processing task. Here, we establish a protocol for certification of a particular set of d-outcome quantum measurements (with d being arbitrary) in a setup comprising of a preparation followed by two measurements in sequence. We propose a set of temporal inequalities pertaining to different d involving correlation functions corresponding to successive measurement outcomes, that are not satisfied by quantum devices. Using quantum violations of these inequalities, we certify specific d-outcome quantum measurements under some minimal assumptions which can be met in an experiment efficiently. Our certification protocol neither requires entanglement, nor any prior knowledge about the dimension of the system under consideration. We further show that our protocol is robust against practical non-ideal realizations. Finally, as an offshoot of our protocol, we present a scheme for secure certification of genuine quantum randomness.

1 Introduction

With the rapid development of quantum information science along with its multi-faceted applications in communication and cryptographic protocols, guaranteeing the functioning of quantum devices received from untrusted providers becomes one of the basic requirements for modern quantum technologies. The task of ensuring the proper functioning of the quantum devices can be designed by utilizing the intrinsic features of quantum physics through certification or verification protocols. Several certification protocols have been designed till date with the desiderata of efficiency, security and less resource consumption. Tomography [1, 2, 3], randomized benchmarking [4, 5, 6, 7] and self-testing [8, 9, 10] are notable among them.

Tomography is one of the foremost traditional methodologies for characterizing unknown quantum preparations, measurements, or processes [1, 2, 3]. However, from an operational perspective, wherein a set of unknown quantum devices are intended to perform information processing or computational tasks, quantum tomography is inadequate. In order to carry out tomography of an unknown quantum device, one first needs to know the dimension as well as the relevant degrees of freedom of the physical system that comprises the device, and accordingly, some other fully characterized quantum devices are essential. For instance, for the tomography of an unknown two-outcome qubit measurement, at least three completely known qubit preparations are required. Therefore, tomography of quantum state preparation, process or measurement is a rather resource consuming method. A similar but less resource consuming method is randomized benchmarking which aims to characterize gate errors in an efficient and robust way in terms of the average overlap between the physical quantum states, measurements or processes and their ideal counterparts [7].

Motivated by certain key features of quantum information theory, other ingenious certification methods have been introduced in recent years. These certifications rely upon various non-classical correlations observed only from the statistics that the devices generate. Moreover,

Debarshi Das: dasdebarshi90@gmail.com
Ananda G. Maity: anandamaity289@gmail.com
Debashis Saha: saha@bose.res.in
A. S. Majumdar: archan@bose.res.in

these methods do not require full characterization of any of the devices and, hence, are categorized as device-independent certification protocols. In a fully device-independent scenario, all involved devices are considered as black boxes, thus requiring minimal assumptions on the underlying states and measurements. On the other hand, in a semi device-independent scenario, some assumptions on the devices are required. Apart from their fundamental interests, these certifications have been shown to be immensely useful in many information processing tasks, like quantum key distribution [11], secure randomness expansion [12], quantum computation [13], and so on.

The most complete form of device-independent certification, namely, self-testing, employs entanglement and other non-local correlations. With the requirement of space-like separated systems, self-testing provides the optimal possible characterization of entangled systems and quantum measurements without assuming any internal functioning of the devices. Historically, it was first designed in order to certify certain maximally entangled two-qubit states and non-commuting qubit measurements employing the maximum quantum violation of the Bell-CHSH (Bell-Clauser-Horne-Shimony-Holt) inequality [8, 9]. Since then, several other self-testing protocols have been proposed [14, 15, 16, 17, 18, 19, 20].

Semi device-independent self-testing protocols have also been investigated [21, 22, 23, 24, 25, 26] employing Einstein-Podolsky-Rosen steering. Moreover, semi device-independent certification for prepare and measure scenarios have been studied [27] with the assumptions on the dimension of the underlying Hilbert space. Another class of certification techniques introduced recently, relies on some features of the measurement devices. Out of these, the ones exploiting quantum contextual correlations presume repeatable measurements with certain compatibility relations [28], or without any compatibility relations [29].

Quantum measurements are one of the most important and key resource in quantum technologies and play a crucial role to reveal the counter-intuitive quantum advantages in non-classical phenomena. There are several protocols proposed till date to certify various quantum measurements, but most of them either require entanglement [30, 31, 32, 33, 34], a costly resource, or need certain assumptions or trust on the measurement devices to be certified [27, 35]. Certification of d-outcome measurements (where d is arbitrary) has received attention in a few works [15, 17] involving scenarios that require a large number of measurements by each of the observers sharing the entangled state. Recently, certification of d-outcome measurements has been proposed based on the Salavrakos-Augusiak-Tura-Wittek-Aćin-Pironio (SATWAP) Bell inequalities [36], which involve two measurements on both sides of the shared entangled state [37]. However, the above mentioned Bell-nonlocality based protocols require both entanglement as well as space-like separated subsystems in order to ensure loophole-free Bell violation. Therefore, a more efficient certification protocol involving less resources and minimal assumptions for d-outcome measurements is in order.

With the above motivation, here we aim to present a protocol to certify some specific d-outcome quantum measurements (with d being arbitrary) employing the non-classicality of temporal correlations. Our proposed protocol uniquely (up to some isometry) identifies which set of measurements is being implemented by an unknown device using measurement statistics and some partial (not tomographically complete) information. We consider a scenario involving one preparation device and one measurement device. The preparation device produces a maximally mixed state of an unknown dimension on which the measurement device performs measurements twice in sequence. In this scenario, we propose a set of temporal inequalities (satisfied by classical devices) pertaining to different values of d, containing time separated correlation functions corresponding to successive measurement outcomes. Using quantum violations of these inequalities, we certify a particular set of d-outcome quantum measurements without requiring entanglement or any prior knowledge about the dimension of the system. Our scheme relies on certain minimal assumptions that can be met in practice. We further show that our protocol is robust against non-ideal realizations. Our certification protocol moreover enables us to formulate a scheme for genuine randomness certification.

The rest of the paper is organised as follows. In the next Section, we first present the scenario along with the required assumptions. We next

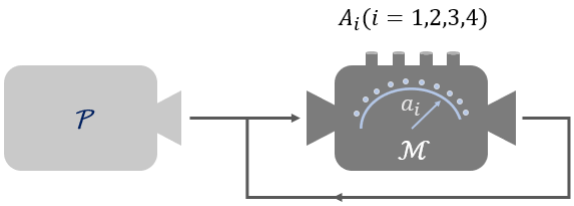

Figure 1: The scenario involves a preparation device $\mathcal{P}$ and a measurement device $\mathcal{M}$ with settings A_i (where $i \in \{1,2,3,4\}$) which returns outcome $a_i \in \{0,1,\cdots,d-1\}$. The state prepared by $\mathcal{P}$ is subjected to $\mathcal{M}$ twice in sequence.

propose a criterion certifying that the measurement effects are projectors. In Section 3, we provide our desired set of temporal inequalities along with their sum-of-squares decompositions under the assumptions considered here. In Section 4, we formulate our scheme for certifying d-outcome quantum measurements and its robustness analyses. Next, we demonstrate in Section 5 the framework for secure randomness certification based on our proposed certification protocol. Finally, Section 6 is reserved for concluding discussions along with some future perspectives.

2 Scenario

Consider the scenario where at first a preparation device $\mathcal{P}$ prepares a state $\rho^{(\mathcal{P})} \in \mathbb{B}(\mathbb{C}^D)$ of an arbitrary dimension D. This prepared state is then subjected to a measurement device $\mathcal{M}$ that performs measurement of the observable A_i upon receiving an input i with $i \in \{1,2,3,4\}$. The post-measurement state is again subjected to the same measurement device $\mathcal{M}$ that receives another input j with $j \in \{1,2,3,4\}$ and performs measurement of the observable A_j. In each experimental run, $\mathcal{M}$ receives the ordered pair of inputs (i,j) randomly. The outcomes of the measurement of A_i are denoted by a_i, where $a_i \in \{0,1,\cdots,d-1\}$. The outcome statistics thus produced are the joint probabilities $p(a_i,a_j|A_iA_j)$ with $i,j,\in \{1,2,3,4\}$ and $a_i,a_j \in \{0,1,\cdots,d-1\}$. Here, $p(a_i,a_j|A_iA_j)$ denotes the joint probability of getting the outcome a_i when the measurement of A_i is performed on the initially prepared state $\rho^{(\mathcal{P})}$, and the outcome of a_j when the measurement of A_j is performed on the post measurement state of A_i. This scenario is depicted in Fig. 1.

2.1 Assumptions

We make the following two assumptions:

Assumption 1. *The preparation device $\mathcal{P}$ prepares the maximally mixed state $\rho^{(\mathcal{P})} = \mathbb{1}/D$, where the dimension D is not required to be known for the realization of the protocol.*

Assumption 2. *The measurement device $\mathcal{M}$ always returns the actual post-measurement state, and does not have any memory.*

Note that one does not need to know the dimension of the state prepared by $\mathcal{P}$ in order to realize the certification protocol. However, one must trust that $\mathcal{P}$ always prepares maximally mixed state. In other words, an unknown supplier provides a preparation device $\mathcal{P}$ producing an input state $\rho^{(\mathcal{P})} \in \mathbb{B}(\mathbb{C}^D)$ and a measurement device $\mathcal{M}$ performing measurements of four possible observables acting on the same Hilbert space $\mathbb{C}^D$ (where $D \geq 2$ can have any integer value). We don't know the dimension D or which particular measurements are performed by $\mathcal{M}$, but we trust that the supplier has devised $\mathcal{P}$ in such a way that $\rho^{(\mathcal{P})}$ is a maximally mixed state. As we show later, such an assumption or trust on the preparation device is necessary, else the measurements cannot be certified uniquely using our proposed temporal inequalities. Since, our motto is not to certify the initial state prepared by the preparation device, we can assume the preparation device to be trusted.

A maximally mixed state can be prepared in the laboratory by subjecting an arbitrary state to a completely depolarizing channel, whose experimental realizations and identification are well-studied [38, 39, 40, 41]. Alternatively, one can prepare a D-dimensional maximally mixed state in optical set-up by subjecting a single photon through a multi-branch Mach-Zehnder interferometer [42, 43] having D number of arms. In each experimental run, one can ensure that the photon passes through a particular arm with unit probability by using specific alignments of a set of mirrors. Hence, this will allow to create mutually orthonormal states in the path degrees of freedom by sending the photons through different arms in different runs. Finally, taking equal mixture of these mutually orthonormal states by using a random number generator to fix the arm through which the photon will pass in each run,

higher dimensional maximally mixed state can be generated.

On the other hand, Assumption 2 has two implications. First, no quantum channel is applied on the post-measurement state before the later measurement A_j, ensuring that the second measurement acts on the actual post-measurement state. Second, the specifics of the later measurement depend only on the second input j, and independent of the first input i as well as the outcome of the first measurement a_i.

Although this scenario for certification of measurements requires some assumption on the preparation state and measurement device, it is efficient in the sense that entanglement or other spatial correlations are not necessary for this scheme.

Next, let us derive the expressions of the measurement statistics produced in the aforementioned scenario under Assumptions 1-2.

In general, the measurement of A_i (where $i \in \{1,2,3,4\}$) is represented by the POVM (Positive Operator Valued Measure) as: $A_i \equiv \{M_i^0, \cdots, M_i^{d-1}\}$ with $M_i^{a_i} \geq 0$ for all $a_i \in \{0, \cdots, d-1\}$ and $\sum_{a_i=0}^{d-1} M_i^{a_i} = \mathbb{1}$. Here, each $M_i^{a_i}$ is called a measurement effect corresponding to outcome a_i. The general form of the respective Kraus operators $\{K_i^{a_i}\}$ of the POVM A_i is given by,

$$K_i^{a_i} = U_i^{a_i} \sqrt{M_i^{a_1}}, \tag{1}$$

where $i \in \{1,2,3,4\}$, $a_i \in \{0, \cdots, d-1\}$, and $U_i^{a_i}$ are some unitary operators.

Using these notations, the unnormalized post-measurement state $\rho_{a_i}^i$, when the outcome a_i is obtained after performing the measurement of A_i on $\rho^{(\mathcal{P})}$, is given by,

$$\rho_i^{a_i} = \left(U_i^{a_i}\sqrt{M_i^{a_i}}\right) \rho^{(\mathcal{P})} \left(U_i^{a_i}\sqrt{M_i^{a_i}}\right)^\dagger \tag{2}$$

In the most distrustful scenario, the joint probability distribution, when the measurement of A_i followed by the measurement of A_j is performed, is given by,

$$p(a_i, a_j | A_i, A_j) = \mathrm{Tr}\left[M_{j,i,a_i}^{a_j} \cdot \Lambda_{i,a_i}\left(\rho_i^{a_i}\right)\right], \tag{3}$$

where the device can apply some quantum channel Λ_{i,a_i} on the post-measurement quantum state and moreover, the specifics of the later measurement, and hence, the measurement effects $\{M_{j,i,a_i}^{a_j}\}$ (where $\sum_{a_j=0}^{d-1} M_{j,i,a_i}^{a_j} = \mathbb{1}$ for all a_i, i, j and $M_{j,i,a_i}^{a_j} \geq 0$ for all i, j, a_i, a_j) may, in general, depend on i and a_i. In such case, for any fixed j, the associated measurement effects of the later measurement might be different for two different choices of i and/or a_i.

However, using Assumption 2, we can consider that the later measurement measurement effects $\{M_j^{a_j}\}$ are independent of i and/or a_i, and there is no quantum channel Λ_{i,a_i}. Further, using Assumption 1, we obtain a simplified form as

$$p(a_i, a_j | A_i, A_j) = \frac{\mathrm{Tr}\left[M_j^{a_j} U_i^{a_i} M_i^{a_i} \left(U_i^{a_i}\right)^\dagger\right]}{D}. \tag{4}$$

Due to the fact that the later measurement of A_j cannot influence the outcome statistics of the first measurement A_i, one can obtain outcome statistics of the first measurement by taking the appropriate marginals as

$$p(a_i|A_i) = \sum_{a_j=0}^{d-1} p(a_i, a_j | A_i, A_j) \quad \forall a_i \in \{0, \cdots d-1\}, i, j \in \{1,2,3,4\}. \tag{5}$$

2.2 Projectivity of the measurement effects

We would now like to present a lemma that introduces an operational criteria certifying the measurement effects to be projectors.

Lemma 1. *Let the measurement of A_i (where $i \in \{1,2,3,4\}$) satisfies the following condition under Assumptions 1-2,*

$$p(a_i, a_i | A_i, A_i) = p(a_i|A_i) \;\; \forall \; a_i \in \{0, \cdots, d-1\}. \tag{6}$$

Then all the measurement effects of A_i are mutually orthogonal projectors, that is, $\forall a_i, \widetilde{a_i} \in \{0, \cdots, d-1\}$

$$M_i^{a_i} M_i^{\widetilde{a_i}} = \delta_{a_i, \widetilde{a_i}} M_i^{a_i}, \tag{7}$$

and moreover, each measurement effect is invariant under the respective unitary associated with Kraus operator (1), that is, $\forall a_i \in \{0, \cdots, d-1\}$

$$\left(U_i^{a_i}\right) M_i^{a_i} \left(U_i^{a_i}\right)^\dagger = M_i^{a_i} \tag{8}$$

for any choice of $U_i^{a_i}$.

A thorough proof of the above Lemma can be found in the Appendix A. For the sake of completeness, here we would like to sketch the outline of the proof.

Without loss of generality, for the POVM $A_i \equiv \{M_i^0, \cdots, M_i^{d-1}\}$, one can take $M_i^{a_i} = \sum_{u=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|$, where $1 \leq m \leq D$, $0 < \lambda_u \leq 1$ for all $u \in \{0, \cdots, m-1\}$ and $\{|\psi_0\rangle, \cdots, |\psi_{D-1}\rangle\}$ forms an orthonormal basis in $\mathbb{C}^D$. However, if the condition $p(a_i, a_i|A_i, A_i) = p(a_i|A_i)$ is achieved under Assumptions 1-2, then a detailed calculation implies that $\lambda_u = 1$ for all $u \in \{0, \cdots, m-1\}$ (see Appendix A). Therefore, $M_i^{a_i} = \sum_{u=0}^{m-1} |\psi_u\rangle\langle\psi_u|$ and hence, $M_i^{a_i}$ must be a projector. Now, if the above condition holds for all $a_i \in \{0, \cdots, d-1\}$, then Eqs.(7)-(8) must hold true.

Next, we will present a set of temporal inequalities that will be used as a tool for certifying A_1, A_2, A_3, A_4.

3 Temporal Inequality with optimal quantum violation

Considering the scenario introduced in Section 2, we would like to design a set of temporal inequalities which can be used as a witness to certify A_1, A_2, A_3, A_4 uniquely (up to some unitary). Nevertheless, it is important to state here that this inequality can be used in the context of any preparation $\rho^{(\mathcal{P})}$ in the scenario mentioned in section 2, without imposing Assumption 2.

Consider now the two-dimensional Fourier transform of the conditional probabilities $p(a_i, a_j|A_i, A_j)$ [44, 45]:

$$\langle A_i^{(k)} A_j^{(l)} \rangle = \sum_{a_i, a_j=0}^{d-1} \omega^{a_i k + a_j l} p(a_i, a_j|A_i, A_j), \quad (9)$$

where ω is the d-th root of unity i.e., $\omega = \exp(2\pi\mathbb{i}/d)$; $k, l \in \{0, \cdots, d-1\}$; $i, j \in \{1, 2, 3, 4\}$. Here, $\{A_x^{(z)}\}$ for each $x \in \{1, 2, 3, 4\}$ are the Fourier transformed operators defined as [25]

$$A_x^{(z)} = \sum_{a_x=0}^{d-1} \omega^{a_x z} M_x^{a_x} \quad \text{with } z = 0, \cdots, d-1, \quad (10)$$

where $A_x \equiv \{M_x^{a_x} | M_x^{a_x} \geq 0 \ \forall\, a_x, \sum_{a_x} M_x^{a_x} = \mathbb{1}\}$ as mentioned earlier. Each $A_x^{(z)}$ can be termed as a generalized observable.

It can be checked that for all $z \in \{0, \cdots, d-1\}$ and $x \in \{1, 2, 3, 4\}$

$$A_x^{(z)\dagger} = A_x^{(d-z)} = A_x^{(-z)},$$
$$A_x^{(z)\dagger} A_x^{(z)} \leq \mathbb{1},$$
$$A_x^{(0)} = \mathbb{1}. \quad (11)$$

Importantly, as a special case, when $M_x^{a_x} M_x^{\widetilde{a_x}} = \delta_{a_x, \widetilde{a_x}} M_x^{a_x}$ for all $a_x, \widetilde{a_x} \in \{0, \cdots, d-1\}$, i.e., all the POVM effects $\{M_x^{a_x}\}$ are mutually orthogonal projectors for each x, then we can define $A_x := A_x^{(1)} = \sum_{a_x=0}^{d-1} \omega^{a_x} \Pi_x^{a_x}$ for each x, where $\{\Pi_x^{a_x}\}$ are the respective projectors. In this case, $\{A_x^{(z)}\}$ for each $x \in \{1, 2, 3, 4\}$ are collections of unitary operators with eigenvalues ω^i $(i = 0, \cdots, d-1)$ defined as

$$A_x^{(z)} = \sum_{a_x=0}^{d-1} \omega^{a_x z} \Pi_x^{a_x} \quad \text{with } z = 0, \cdots, d-1. \quad (12)$$

It is not difficult to see from the above relation (12) that $A_x^{(z)}$ is simply the z-th power of A_x. Thus, in what follows we use the notation $A_x^{(z)}$ or A_x^z interchangeably when the effect operators associated with the measurement of A_x are mutually orthogonal projectors.

3.1 Temporal inequalities

Next, we propose the following set of temporal inequalities,

$$\begin{aligned}\tau_d = \sum_{k=1}^{d-1} \Big[& a_k \left\langle A_1^{(k)} A_3^{(d-k)} \right\rangle + a_k^* \omega^k \left\langle A_1^{(k)} A_4^{(d-k)} \right\rangle \\ & + a_k^* \left\langle A_2^{(k)} A_3^{(d-k)} \right\rangle + a_k \left\langle A_2^{(k)} A_4^{(d-k)} \right\rangle \\ & + a_k \left\langle A_3^{(d-k)} A_1^{(k)} \right\rangle + a_k^* \omega^k \left\langle A_4^{(d-k)} A_1^{(k)} \right\rangle \\ & + a_k^* \left\langle A_3^{(d-k)} A_2^{(k)} \right\rangle + a_k \left\langle A_4^{(d-k)} A_2^{(k)} \right\rangle \Big] \\ \leq C_d, & \quad (13)\end{aligned}$$

where $a_k = \dfrac{1 - \mathbb{i}}{2} \exp\left(\dfrac{\pi \mathbb{i} k}{2d}\right)$ and

$$C_d = 3 \cot\left(\frac{\pi}{4d}\right) - \cot\left(\frac{3\pi}{4d}\right) - 4 \quad (14)$$

are the classical upper bounds of the temporal expressions τ_d. These classical bounds are derived in the Appendix B. In particular, the above temporal inequalities are not only satisfied by classical physics, but also satisfied by any theory consistent with the concept of "macrorealism" [46]

which is the conjunction of the following two assumptions: *(i) Realism:* At any instant, irrespective of any measurement, a system is definitely in any one of the available states such that all its observable properties have definite values. *(ii) Noninvasive measurability:* It is possible, in principle, to determine which of the states the system is in, without affecting the state itself or the system's subsequent evolution. This notion of "macrorealism" is one of the central concepts underpinning the classical world view. The temporal inequalities (13) can be considered as generalized versions of the Leggett-Garg inequality involving measurements with arbitrary number of outcomes whereas the original Leggett-Garg inequality [46] consists of binary outcome measurements. Temporal quantum correlations are inconsistent with macrorealism [46] and, hence, it is possible to violate the above inequalities by quantum mechanical predictions. A point to be stressed here is that (13) represents different temporal inequalities for different d.

It should be mentioned that although the structure of the inequalities (13) is somewhat similar to the structure of the SATWAP Bell inequalities involving measurements with arbitrary number of outcomes [36], these two sets of inequalities are conceptually different. The SATWAP inequalities consist of correlation functions between measurement outcomes of two spatially separated systems [36]. On the other hand, the inequalities (13) proposed here contain correlation functions pertaining to a single system on which different measurements are performed sequentially. Moreover, the above temporal inequalities (13) have twice more terms than the number of terms appearing in SATWAP inequalities. Note further that although the above inequalities (13) are expressed in the Fourier transformed space, these can also be expressed as linear functions of $p(a_i, a_j|A_i, A_j)$ with real coefficients and always take real values as shown in the Appendix B.

Up to now, the details of the Fourier transformed expectation values and the temporal inequalities (13) are discussed for an arbitrary preparation $\rho^{(\mathcal{P})}$. The following discussions will be applicable when Assumptions 1-2 are considered.

Before proceeding, let us point out that the optimal quantum violations of the temporal inequalities (13) under Assumptions 1-2 and condition (6) are relevant for the certification scheme presented here.

Now, suppose that under Assumption 1-2, the condition (6) is satisfied by each of the four observables A_1, A_2, A_3 and A_4. Here, $A_i = A_i^{(1)}$ for all $i \in \{1, 2, 3, 4\}$ with $A_i^{(1)}$ being defined in Eq.(12). Then, it follows from Lemma 1 that each of the measurement of A_i can be represented as $A_i \equiv \{\Pi_i^{a_i}\}$, where $\Pi_i^{a_i}\Pi_i^{\widetilde{a_i}} = \delta_{a_i,\widetilde{a_i}}\Pi_i^{a_i}$ for all $a_i, \widetilde{a_i} \in \{0, \cdots, d-1\}$. Hence, the operator $A_i^{(k)}$ is unitary with $A_i^{(k)} = A_i^k$ for all $i \in \{1, 2, 3, 4\}$ and for all $k \in \{0, \cdots, d-1\}$. Moreover, due to (8), the joint probability expressed in Eq. (4) further reduces to,

$$\begin{aligned} p(a_i, a_j|A_i, A_j) =& \mathrm{Tr}\Big[\Pi_j^{a_j}\,\Pi_i^{a_i}\,\rho^{(\mathcal{P})}\Big] \\ & \forall\, i, j \in \{1, 2, 3, 4\}, \\ & \text{and } \forall\, a_i, a_j \in \{0, \cdots, d-1\}, \end{aligned} \tag{15}$$

in which $\rho^{(\mathcal{P})} = \mathbb{1}/D$.

Consequently, using Eqs.(9) and (12), we can write for all $k, l = 1, \cdots, d-1$ and for all $i, j \in \{1, 2, 3, 4\}$,

$$\begin{aligned} \langle A_i^{(k)}\, A_j^{(l)}\rangle &= \mathrm{Tr}\Big[A_i^k\, A_j^l\, \rho^{(\mathcal{P})}\Big] \\ &= \mathrm{Tr}\Big[A_i^{(k)}\, A_j^{(l)}\, \rho^{(\mathcal{P})}\Big]. \end{aligned}$$

Hence, under Assumptions 1-2 and condition (6), the left hand side of the temporal inequality (13) can be expressed as

$$\tau_d\left(\rho^{(\mathcal{P})} = \mathbb{1}/D\right) = \mathrm{Tr}[\rho^{(\mathcal{P})}\,\hat{\beta}_{\tau_d}], \tag{16}$$

where the operator $\hat{\beta}_{\tau_d}$ is given by,

$$\begin{aligned} \hat{\beta}_{\tau_d} = \sum_{k=1}^{d-1}\Big[& a_k A_1^{(k)}\, A_3^{(d-k)} + a_k^* \omega^k A_1^{(k)}\, A_4^{(d-k)} \\ & + a_k^* A_2^{(k)}\, A_3^{(d-k)} + a_k A_2^{(k)}\, A_4^{(d-k)} \\ & + a_k A_3^{(d-k)}\, A_1^{(k)} + a_k^* \omega^k A_4^{(d-k)}\, A_1^{(k)} \\ & + a_k^* A_3^{(d-k)}\, A_2^{(k)} + a_k A_{(4)}^{(d-k)}\, A_2^{(k)}\Big]. \end{aligned} \tag{17}$$

It should be noted here that (16) is valid under the Assumptions 1-2 and when each of the four observables A_i with $i \in \{1, 2, 3, 4\}$ satisfies the condition (6). In other words, the condition (16) may not be true in general.

3.2 Sum-of-squares decomposition with maximally mixed state

Now, let us derive the sum-of-squares decompositions of the temporal inequalities (13) under Assumptions 1-2, when each of the four observables A_i with $i \in \{1,2,3,4\}$ satisfies condition (6). For this purpose, let us first define

$$\begin{aligned} B_1^{(k)} &= a_k A_3^{(-k)} + a_k^* \omega^k A_4^{(-k)}, \\ B_2^{(k)} &= a_k^* A_3^{(-k)} + a_k A_4^{(-k)}. \end{aligned} \tag{18}$$

Note here that $a_{d-k} = a_k^*$, and therefore $B_x^{(d-k)} = \left[B_x^{(k)}\right]^\dagger$ for any $k = 1, \cdots, d-1$ and $x = 1, 2$.

Since, $(A_i^k)^\dagger = A_i^{d-k}$ and A_i^k is unitary for all $i \in \{1,2,3,4\}$ and for all $k \in \{1, \cdots, d-1\}$, we have $A_i^{-k} = A_i^{d-k}$ for all $i \in \{1,2,3,4\}$ and for all $k \in \{1, \cdots, d-1\}$. Since $A_x^{(k)} = A_x^k$ for all $x \in \{1,2\}$ and for all $k \in \{1, \cdots, d-1\}$, it follows that

$$\begin{aligned} \hat{\beta}_{\tau_d} = \sum_{k=1}^{d-1} \Big[& A_1^{(k)} B_1^{(k)} + A_2^{(k)} B_2^{(k)} \\ & + B_1^{(k)} A_1^{(k)} + B_2^{(k)} A_2^{(k)} \Big]. \end{aligned}$$

Let us also define,

$$\begin{aligned} P_x^{(k)} = \mathbb{1} - A_x^{(k)} B_x^{(k)} \quad & \forall x \in \{1,2\}, \\ & \forall k \in \{1, \cdots, d-1\}. \end{aligned} \tag{19}$$

Using these relations, we have

$$\begin{aligned} & \sum_{k=1}^{d-1} \sum_{x=1}^{2} \left[\left(P_x^{(k)}\right)^\dagger \left(P_x^{(k)}\right) \right] \\ & = \sum_{k=1}^{d-1} \Big[2\,\mathbb{1} - B_1^{(d-k)} A_1^{d-k} - A_1^k B_1^{(k)} \\ & \quad + \left(B_1^{(k)}\right)^\dagger \left(B_1^{(k)}\right) - B_2^{(d-k)} A_2^{d-k} \\ & \quad - A_2^k B_2^{(k)} + \left(B_2^{(k)}\right)^\dagger \left(B_2^{(k)}\right) \Big]. \end{aligned} \tag{20}$$

One can verify that

$$\sum_{k=1}^{d-1} B_x^{(d-k)} A_x^{d-k} = \sum_{k=1}^{d-1} B_x^{(k)} A_x^k \quad \forall x = 1, 2. \tag{21}$$

Now, incorporating the fact that $\left(A_3^{d-k}\right)^\dagger \left(A_3^{d-k}\right) = \left(A_4^{d-k}\right)^\dagger \left(A_4^{d-k}\right) = \mathbb{1}$ and $(a_k)^2 (\omega^k)^* + (a_k^*)^2 = (a_k^*)^2 \omega^k + (a_k)^2 = 0$ for all $k \in \{1, \cdots, d-1\}$ one can evaluate that

$$\left(B_1^{(k)}\right)^\dagger \left(B_1^{(k)}\right) + \left(B_2^{(k)}\right)^\dagger \left(B_2^{(k)}\right) = 2\,\mathbb{1} \;\; \forall k. \tag{22}$$

Using Eqs.(20) (21), (22), we have

$$\sum_{k=1}^{d-1} \sum_{x=1}^{2} \left[\left(P_x^{(k)}\right)^\dagger \left(P_x^{(k)}\right) \right] = 4(d-1)\,\mathbb{1} - \hat{\beta}_{\tau_d}. \tag{23}$$

The left hand side of Eq.(23) is the sum-of-squares decomposition and it is the sum of positive operators. Hence, we have

$$\mathrm{Tr}\left[\rho^{(\mathcal{P})} (4(d-1)\,\mathbb{1} - \hat{\beta}_{\tau_d})\right] \geq 0.$$

The above inequality implies that

$$\mathrm{Tr}\left[\rho^{(\mathcal{P})}\, \hat{\beta}_{\tau_d}\right] \leq 4(d-1). \tag{24}$$

Hence, the upper bounds of the quantum magnitudes of τ_d for all $d \geq 2$ are $4(d-1)$ under Assumptions 1-2 and condition (6). It can be checked that $4(d-1) > C_d$ for all $d \geq 2$ [36], where C_d given by Eq.(14) are the classical upper bounds of the temporal expressions τ_d. Again, it should be noted here that $4(d-1)$ may not be the optimal upper bounds of quantum violations of the temporal inequalities (13) in general.

3.3 Binary outcome ($d = 2$) case

In the case of $d = 2$, the temporal inequality (13) reduces to

$$\begin{aligned} \tau_2 = \frac{1}{\sqrt{2}} \Big[& \langle A_1 A_3 \rangle - \langle A_1 A_4 \rangle + \langle A_2 A_3 \rangle + \langle A_2 A_4 \rangle \\ & + \langle A_3 A_1 \rangle - \langle A_4 A_1 \rangle + \langle A_3 A_2 \rangle + \langle A_4 A_2 \rangle \Big] \\ \leq\; & 2\sqrt{2}, \end{aligned} \tag{25}$$

where the measurement of A_i (with $i \in \{1,2,3,4\}$) has two possible outcomes denotes by $a_i \in \{0,1\}$. This turns out to be the symmetrized version of the temporal inequality proposed in [47]. Interestingly, in this particular binary outcome scenario, the expression (16) for the quantum value of (25) holds for any general input state, that is, for any $\rho^{(\mathcal{P})} \in \mathbb{B}(\mathbb{C}^D)$ (where D is arbitrary),

$$\tau_2\left(\rho^{(\mathcal{P})}\right) = \mathrm{Tr}\left[\rho^{(\mathcal{P})}\, \hat{\beta}_{\tau_2}\right] \;\; \forall\; \rho^{(\mathcal{P})} \in \mathbb{B}(\mathbb{C}^D), \tag{26}$$

where the operator $\hat{\beta}_{\tau_2}$ is given by,

$$\hat{\beta}_{\tau_2} = A_1\,A_3 - A_1\,A_4 + A_2\,A_3 + A_2\,A_4 + A_3\,A_1 - A_4\,A_1 + A_3\,A_2 + A_4\,A_2. \quad (27)$$

To see this, note that there is no restriction on the dimension D of the measurements. Therefore, the Naimark's dilation theorem allows us to consider these measurements to be projective given by,

$$A_i = \Pi_i^0 - \Pi_i^1 \quad \forall i \in \{1,2,3,4\},$$

where $\{\Pi_i^0, \Pi_i^1\}$ are projectors acting on $\mathbb{C}^D$ with

$$\Pi_i^{a_i} = \frac{\mathbb{1} + (-1)^{a_i} A_i}{2} \;\forall\, a_i \in \{0,1\}. \quad (28)$$

The joint probability for any state $\rho^{(\mathcal{P})}$ is given by,

$$p(a_i, a_j|A_i, A_j) = \mathrm{Tr}\left[\Pi_j^{a_j}\Pi_i^{a_i}\rho^{(\mathcal{P})}\Pi_i^{a_i}\right] \quad (29)$$

$\forall i,j \in \{1,2,3,4\}$ and $\forall a_i, a_j \in \{0,1\}$. Using the expression of correlation function

$$\langle A_i\,A_j\rangle = \sum_{a_i,a_j=0}^{1} (-1)^{a_i+a_j} p(a_i,a_j|A_i,A_j), \quad (30)$$

and Eqs. (28)-(29), we get the following

$$\langle A_i\,A_j\rangle + \langle A_j\,A_j\rangle = \mathrm{Tr}\left[\,(A_iA_j + A_jA_i)\,\rho^{(\mathcal{P})}\right] \quad \forall\ \rho^{(\mathcal{P})} \in \mathbb{B}(\mathbb{C}^D). \quad (31)$$

By considering pairs of terms in the temporal expression (25), one can readily verify that the associated quantum operator is given by (27). Subsequently, the sum-of-squares decomposition (23) for $d = 2$ and the quantum upper bound 4 of (25) hold true for any general preparation $\rho^{(\mathcal{P})}$.

4 Certification of quantum measurements

In this section, we would like to state our main results for certifying the d-outcome quantum measurements employing the set of temporal inequalities proposed by us in the previous section along with the sum-of-squares decompositions (23). Before proceeding further, let us first verify that the measurements cannot be certified uniquely using the temporal inequalities (13) if we do not make any assumption on the state preparation. Here, uniqueness encompasses the unitary freedom of the measurements.

Lemma 2. *There exist at least two sets of preparations and binary-outcome projective measurements for which the magnitude of quantum violation of the temporal inequality (25) is 4, but the measurements in these two sets are not unitarily connected. In other words, uniqueness of the measurements cannot be shown employing binary outcome temporal inequality (25) without any assumption on the preparation.*

Proof. Let us first note that the optimal quantum value 4 of (25) holds for arbitrary preparation $\rho^{(\mathcal{P})} \in \mathbb{C}^D$. Now, we show that there exist two different sets of preparations and projective measurements such that the measurements in these two sets are not connected unitarily although $\tau_2 = 4$ is achieved by both of these two sets. Hence, for arbitrary preparations, the measurements cannot be certified uniquely using the inequality (25) without any assumption on the preparation device. The explicit examples of such two different sets of preparations and projective measurements are given in the Appendix C. □

The above lemma implies that some assumption on the preparation device is necessary in order to certify the measurements uniquely using the quantum violation of the temporal inequality (13). Therefore, we have considered Assumption 1 which states that the preparation device produces a maximally mixed state of an unknown dimension.

Before proceeding, let us define the d-dimensional generalization of the σ_z-Pauli matrix in the standard basis given by,

$$Z_d = \sum_{i=0}^{d-1} \omega^i |i\rangle\langle i|. \quad (32)$$

let us also introduce the following d-dimensional unitary observable,

$$T_d = \sum_{i=0}^{d-1} \omega^{i+\frac{1}{2}} |i\rangle\langle i| - \frac{2}{d}\sum_{i,j=0}^{d-1} (-1)^{\delta_{i,0}+\delta_{j,0}} \omega^{\frac{i+j+1}{2}} |i\rangle\langle j|, \quad (33)$$

where $\delta_{i,j}$ is the Kronecker delta function. It can be checked that Z_d and T_d are unitary with eigenvalues ω^i $(i = 0, \cdots, d-1)$ [37].

With these, we present a theorem providing the certification of a specific set of quantum measurements. This theorem states that one can certify the four observables A_1, A_2, A_3, A_4, uniquely (up to some unitary freedom) using the condition (6) and the temporal inequalities (13). Hence, one can indeed certify some particular quantum measurements having arbitrary number of outcomes under certain assumptions employing temporal quantum correlations without using entanglement.

Theorem 1. *Suppose that in the scenario considered by us with any fixed value of d under Assumptions 1-2, the condition (6) is satisfied by each of the four observables A_1, A_2, A_3, A_4, and the magnitude of quantum violation of the temporal inequality (13) is $4(d-1)$. Then, for any d, we have $\mathbb{C}^D = \mathbb{C}^d \otimes \mathcal{H}'$ with some auxiliary Hilbert space $\mathcal{H}'$ of unknown but finite dimension. Further, there exists a unitary transformation $U : \mathbb{C}^d \otimes \mathcal{H}' \to \mathbb{C}^d \otimes \mathcal{H}'$, such that*

$$\begin{aligned} UA_1U^\dagger &= Z_d \otimes \mathbb{1}_{\mathcal{H}'}, \\ UA_2U^\dagger &= T_d \otimes \mathbb{1}_{\mathcal{H}'}, \\ UA_3U^\dagger &= \left(a_1^* Z_d + 2(a_1^*)^3 T_d\right) \otimes \mathbb{1}_{\mathcal{H}'}, \\ UA_4U^\dagger &= \left(a_1 Z_d - a_1^* T_d\right) \otimes \mathbb{1}_{\mathcal{H}'}, \end{aligned} \tag{34}$$

where $a_1 = \frac{1-\mathrm{i}}{2}\omega^{\frac{1}{4}}$, Z_d and T_d are defined earlier and $\mathbb{1}_{\mathcal{H}'}$ is the identity matrix acting on $\mathcal{H}'$.

Proof. Under Assumptions 1 and 2, we can take the measurement effects of each of the observables A_i with $i \in \{1,2,3,4\}$ to be mutually orthogonal projectors as each of these observables satisfies the condition (6). This follows from Lemma 1. Hence, $A_x^{(k)}$ is unitary operator with $A_x^{(k)} = A_x^k$ for all $x \in \{1,2,3,4\}$ and for all $k \in \{0, \cdots, d-1\}$. Also, we can consider that the condition (8) holds true.

Next, since the magnitude of quantum violation of the temporal inequality (13) is $4(d-1)$ under Assumptions 1-2, using Eq.(23), we can write

$$\mathrm{Tr}\left[\rho^{(\mathcal{P})} \left\{ \sum_{k=1}^{d-1} \sum_{x=1}^{2} \left(P_x^{(k)}\right)^\dagger \left(P_x^{(k)}\right) \right\}\right] = 0.$$

Since $\left(P_x^{(k)}\right)^\dagger \left(P_x^{(k)}\right) \geq 0$ for all $k \in \{1, \cdots, d-1\}$ and for all $x \in \{1,2\}$, the above equation implies that

$$\mathrm{Tr}\left[\rho^{(\mathcal{P})} \left(P_x^{(k)}\right)^\dagger \left(P_x^{(k)}\right)\right] = 0 \quad \forall\, k \in \{1, \cdots, d-1\} \text{ and } \forall\, x \in \{1,2\}. \tag{35}$$

As mentioned earlier, $\rho^{(\mathcal{P})} = \sum_{u=0}^{D-1} \frac{1}{D} |\xi_u\rangle\langle\xi_u|$ with $\{|\xi_u\rangle\}$ being an arbitrary orthonormal basis in $\mathbb{C}^D$. Hence, from Eq.(35), we have

$$\left(P_x^{(k)}\right)|\xi_u\rangle = 0, \quad \langle\xi_u|\left(P_x^{(k)}\right)^\dagger = 0 \quad \forall\, x \in \{1,2\},\ \forall\, k \in \{1, \cdots, d-1\},\ \forall\, u \in \{0, \cdots, D-1\}.$$

We can, therefore, write that

$$\left(P_x^{(k)}\right)\rho^{(\mathcal{P})} = 0, \quad \rho^{(\mathcal{P})}\left(P_x^{(k)}\right)^\dagger = 0 \quad \forall\, x \in \{1,2\},\ \forall\, k \in \{1, \cdots, d-1\}. \tag{36}$$

Taking $\rho^{(\mathcal{P})} = \mathbb{1}/D$ and using Eqs.(19) and (36), we get

$$A_x^k\, B_x^{(k)} = \mathbb{1}, \quad \left(B_x^{(k)}\right)^\dagger \left(A_x^k\right)^\dagger = \mathbb{1} \quad \forall\, x \in \{1,2\},\ \forall\, k \in \{1, \cdots, d-1\}. \tag{37}$$

Using the above two equations along with the condition $\left(A_x^k\right)^\dagger \left(A_x^k\right) = \mathbb{1}$, one has

$$\left(B_x^{(k)}\right)^\dagger \left(B_x^{(k)}\right) = \left(B_x^{(d-k)}\right)\left(B_x^{(k)}\right) = \mathbb{1} \quad \forall\, x \in \{1,2\},\ \forall\, k \in \{1, \cdots, d-1\}. \tag{38}$$

Now, taking $x = 1$, the above condition leads to,

$$A_3^k\, A_4^{-k} = \omega^{-k} A_4^k\, A_3^{-k} \quad \forall\, k \in \{1, \cdots, d-1\}. \tag{39}$$

Due to the fact that $A_i^d = \mathbb{1}$ for all $i \in \{1,2,3,4\}$, the above relation (39) can be extended to any integer $k \in \mathbb{Z}$.

Next, Eq.(37) also implies that $B_x^{(k)} = (A_x^k)^\dagger = (A_x^\dagger)^k$ for all $x \in \{1,2\}$ and $k \in \{1, \cdots, d-1\}$. Moreover, with $k = 1$, Eq.(37) implies that $B_x^{(1)} = A_x^\dagger$ for all $x \in \{1,2\}$. Hence, we get

$$\begin{aligned} B_x^{(k)} &= (A_x^\dagger)^k \\ &= (B_x^{(1)})^k \quad \forall\, x \in \{1,2\},\ \forall\, k \in \{1, \cdots, d-1\}. \end{aligned} \tag{40}$$

Eqs.(37), (38), (39) and (40) are sufficient to characterize A_1, A_2 A_3 and A_4. In fact, it can be shown that if the unitary observables A_3 and A_4 satisfy the conditions (38), (39) and (40), then we can draw the following two conclusions (the calculations are the same as presented in the Supplementary Information of [37]):

- The dimension D is a multiple of the number of outcomes d, meaning that

$$\mathbb{C}^D = \mathbb{C}^d \otimes \mathcal{H}',$$

where $\mathcal{H}'$ is some auxiliary Hilbert space of finite dimension D/d which is unknown as D is unknown.

- There exists a unitary transformation $\widetilde{U} : \mathbb{C}^d \otimes \mathcal{H}' \to \mathbb{C}^d \otimes \mathcal{H}'$, such that

$$\widetilde{U} A_3 \widetilde{U}^\dagger = Z_d \otimes \mathbb{1}_{\mathcal{H}'}, \tag{41}$$
$$\widetilde{U} A_4 \widetilde{U}^\dagger = T_d \otimes \mathbb{1}_{\mathcal{H}'}, \tag{42}$$

where Z_d and T_d are defined earlier.

Now, it can be proved that there exists a unitary transformation $W =: \mathbb{C}^d \to \mathbb{C}^d$, such that

$$W Z_d W^\dagger = \Big(a_1^* Z_d + 2(a_1^*)^3 T_d\Big), \tag{43}$$
$$W T_d W^\dagger = \Big(a_1 Z_d - a_1^* T_d\Big), \tag{44}$$

where $a_1 = \dfrac{1-\mathbb{i}}{2}\omega^{\frac{1}{4}}$. The existence of such a unitary W is proved in the Supplementary Information of [37].

Therefore, using Eqs.(41)-(44), we can conclude that there exists a unitary transformation $U = (W \otimes \mathbb{1}_{\mathcal{H}'})\,\widetilde{U} : \mathbb{C}^d \otimes \mathcal{H}' \to \mathbb{C}^d \otimes \mathcal{H}'$, such that

$$U A_3 U^\dagger = \Big(a_1^* Z_d + 2(a_1^*)^3 T_d\Big) \otimes \mathbb{1}_{\mathcal{H}'}, \tag{45}$$
$$U A_4 U^\dagger = \Big(a_1 Z_d - a_1^* T_d\Big) \otimes \mathbb{1}_{\mathcal{H}'}. \tag{46}$$

Now, Eqs. (40), (45) and (46) imply that

$$U B_1^{(k)} U^\dagger = (Z_d^\dagger)^k \otimes \mathbb{1}_{\mathcal{H}'}, \tag{47}$$
$$U B_2^{(k)} U^\dagger = (T_d^\dagger)^k \otimes \mathbb{1}_{\mathcal{H}'}. \tag{48}$$

In particular, if A_3 and A_4 are transformed by applying the unitary U, then $B_1^{(1)} = Z_d^\dagger$ and $B_2^{(1)} = T_d^\dagger$.

Next, Eq.(37) implies that $A_x^k B_x^{(k)} = \mathbb{1}$ for all $x \in \{1,2\}$ and $k \in \{1, \cdots, d-1\}$. Hence, with $k = 1$, we get

$$A_x = \big(B_x^{(1)}\big)^\dagger \qquad \forall\, x \in \{1,2\}. \tag{49}$$

Hence, Eqs.(47)-(49) imply that there exists a unitary transformation $U : \mathbb{C}^d \otimes \mathcal{H}' \to \mathbb{C}^d \otimes \mathcal{H}'$, such that

$$U A_1 U^\dagger = Z_d \otimes \mathbb{1}_{\mathcal{H}'}, \tag{50}$$
$$U A_2 U^\dagger = T_d \otimes \mathbb{1}_{\mathcal{H}'}. \tag{51}$$

Thus, Eqs.(45)-(46) together with Eqs.(50)-(51) complete the proof. □

The above Theorem also implies that $4(d-1)$ is the tight upper bound of the temporal inequality (13) for any fixed d under Assumptions 1-2 when the condition (6) is satisfied by each of the four observables A_1, A_2, A_3, A_4. Let us also remark that the certified operators $(a_1^* Z_d + 2(a_1^*)^3 T_d)$ and $(a_1 Z_d - a_1^* T_d)$ are unitary matrices having d distinct eigenvalues ω^i with $i \in \{0, \cdots, d-1\}$.

One important point to be stressed is that the measurements certified here are the optimal Collins-Gisin-Linden-Massar-Popescu (CGLMP) measurements [36, 48, 49]. Thus these measurements have wide ranges of applications both in quantum information theory and cryptography ranging from witnessing the dimension of a Hilbert-space [50, 51, 52], reducing quantum communication complexity [53, 54], advantages in communication game [55], remote preparation of quantum states [56], distribution of secure key [57, 58] to generating genuine randomness [59]. Further, these measurements have already been realized experimentally [60, 61].

Also note that the measurements certified here have also been self-tested in [37] based on the quantum violation of the SATWAP Bell inequalities. However, as mentioned earlier, this self-testing protocol requires entanglement between two spatially separated particles (spatial separation is required here in order to avoid locality loophole in Bell violation). On the contrary, our certification protocol can be realized using temporal quantum correlation pertaining to a single particle.

4.1 Robustness analysis

So far, we have proposed a certification protocol for the d-outcome ideal measurement settings

given in Theorem 1 employing the maximal quantum violations of the temporal inequalities (13) under Assumptions 1-2 when each of the measurements satisfies condition (6). However, in a real experimental scenario there is always some unavoidable noise and hence, the ideal measurements are hardly realizable. Thus, the condition (6) may not be satisfied and/or one may not get $\tau_d = 4(d-1)$ under Assumptions 1-2. In such cases, we ask the question whether we can certify those measurements up to a certain threshold. The term robustness of the certification protocol implies that the non-ideal measurements are close to the ideal ones if the correlations produced by the non-ideal measurements are close the ideal correlations. In the following, we present the robustness analysis of our certification protocol for the following two cases: • when satisfying the condition (6) is affected by the non-ideal observables, • when the magnitude of the temporal inequality (13) is affected by the non-ideal observables, whereas satisfying the condition (6) remains unaffected.

Suppose that in an experimental situation under Assumptions 1-2, instead of performing measurements of the ideal unitary observables A_i with $i \in \{1,2,3,4\}$ mentioned in the statements of Theorem 1, measurements of the non-ideal observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ are being performed, where each of these non-ideal observables does not satisfy the condition (6).

Now, let us present the following theorem (for proof, see Appendix D) that represents the robustness analysis for any potential imprecision in satisfying the condition (6).

Theorem 2. *Suppose the non-ideal observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ satisfy the following,*

$$p(a_i|\widetilde{A}_i) = p(a_i, a_i|\widetilde{A}_i, \widetilde{A}_i) + \eta_i^{(a_i)} \text{ with } \eta_i^{(a_i)} > 0 \quad \forall\ a_i \in \{0,\cdots,d-1\},\ \forall\ i \in \{1,2,3,4\}. \tag{52}$$

Then we have for all $a_i \in \{0,\cdots,d-1\}$ and for all $i \in \{1,2,3,4\}$

$$\Big|\Big|\rho^{(\mathcal{P})}\left[\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \left(\widetilde{K}_i^{a_i\dagger}\right)^2\left(\widetilde{K}_i^{a_i}\right)^2\right]\rho^{(\mathcal{P})} - \rho^{(\mathcal{P})}\left[K_i^{a_i\dagger}K_i^{a_i} - \left(K_i^{a_i\dagger}\right)^2\left(K_i^{a_i}\right)^2\right]\rho^{(\mathcal{P})}\Big|\Big|_{HS} < \eta_i^{(a_i)}, \tag{53}$$

where $\{\widetilde{K}_i^{a_i}\}$ and $\{K_i^{a_i}\}$ are the Kraus operators defined in (1) of the non-ideal observable $\widetilde{A}_i$ and the ideal observable A_i respectively. Here, $||\cdot||_{HS}$ denotes the Hilbert–Schmidt norm.

In the above theorem, the condition $\eta_i^{a_i} > 0$ for all $a_i \in \{0,\cdots,d-1\}$ and for all $i \in \{1,2,3,4\}$ naturally appears due to the fact that $p(a_i,a_i|A_i,A_i) \leq p(a_i|A_i)$ for all $a_i \in \{0,\cdots,d-1\}$ and for all $i \in \{1,2,3,4\}$ for any input state prepared by $\mathcal{P}$.

Next, let us consider that each of the four non-ideal observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ satisfies the condition (6). Hence, the measurement effects of each of these observables are mutually orthogonal projectors, which implies that these four non-ideal observables are unitary. Now, consider that in the aforementioned scenario with any fixed value of d the magnitude of the temporal inequality (13) with these non-ideal unitary observables is $4(d-1)-\epsilon$, where ϵ is a positive number. Note that the maximum quantum violation of the temporal inequality (13) under Assumptions 1-2 is $4(d-1)$ when each of the four observables satisfies the condition (6), thereby implying that ϵ cannot be negative.

Against the above backdrop, we present the following theorem (for proof, see Appendix E) that represents the robustness analyses of our certification scheme associated with the magnitude of quantum violation of the temporal inequality (13).

Theorem 3. *If the quantum value of the temporal expression τ_d given in (13) for any fixed d realized by unknown unitary (Fourier transformed) observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ satisfying the condition (6) is $[4(d-1)-\epsilon]$ with ϵ being a positive number, then the following relations hold true*

$$(i)\ \Big|\Big|\left[A_1(a_1A_3^\dagger + a_1^*\omega A_4^\dagger)\right]\rho^{(\mathcal{P})} - \left[\widetilde{A}_1(a_1\widetilde{A}_3^\dagger + a_1^*\omega\widetilde{A}_4^\dagger)\right]\rho^{(\mathcal{P})}\Big|\Big|_{HS} < \sqrt{\epsilon}. \tag{54}$$

$$(ii)\ \Big|\Big|\left[A_2(a_1^*A_3^\dagger + a_1A_4^\dagger)\right]\rho^{(\mathcal{P})} - \left[\widetilde{A}_2(a_1^*\widetilde{A}_3^\dagger + a_1\widetilde{A}_4^\dagger)\right]\rho^{(\mathcal{P})}\Big|\Big|_{HS} < \sqrt{\epsilon}. \tag{55}$$

$$(iii)\ \Big\| \left(A_4A_3^\dagger - \omega A_3A_4^\dagger\right)\rho^{(\mathcal{P})} - \left(\widetilde{A}_4\widetilde{A}_3^\dagger - \omega\widetilde{A}_3\widetilde{A}_4^\dagger\right)\rho^{(\mathcal{P})}\Big\|_{HS} \leq 2\sqrt{\epsilon}(2+\sqrt{\epsilon}). \quad (56)$$

$$(iv)\ \Big\| \left(\omega A_2A_1^\dagger - A_1A_2^\dagger\right)\rho^{(\mathcal{P})} - \left(\omega\widetilde{A}_2\widetilde{A}_1^\dagger - \widetilde{A}_1\widetilde{A}_2^\dagger\right)\rho^{(\mathcal{P})}\Big\|_{HS} \leq 2\sqrt{\epsilon}(2+\sqrt{\epsilon}). \quad (57)$$

where A_1, A_2, A_3, A_3 are any set of unitary (Fourier transformed) observables that satisfies the condition (6), achieves $\tau_d = 4(d-1)$ and thus satisfies Theorem 1.

For a more general robustness analysis, one should consider that both the magnitude of the temporal inequality (13) and satisfying the condition (6) are affected simultaneously by the non-ideal measurements. We leave this question for future study.

However, if the difference between the experimentally measured values of $p(a_i, a_i|\widetilde{A}_i, \widetilde{A}_i)$ and $p(a_i|\widetilde{A}_i)$ is within the statistical error range, then it can be approximated that the observables $\widetilde{A}_i$ ($i \in \{1,2,3,4\}$) satisfy the conditions (6). In such cases, Theorem 3 alone presents the complete robustness analysis of our certification protocol.

Another important point to be stressed here is that if an additional assumption is taken into account, then the certification of the measurements presented in Eq.(34) can be demonstrated without requiring the measurements to satisfy the conditions (6) (see the next Sec. 4.2 for details). Hence, in this case, Theorem 2 is not required for demonstrating robustness of our protocol.

4.2 Robust certification without using Lemma 1 or condition (6)

Now, we will show that our certification protocol can be formulated based on the quantum violation of the temporal inequalities (13) alone without using the condition mentioned in Lemma 1 if we consider another assumption as described below together with the Assumptions 1 and 2.

Assumption 3. *The measurements $A_i \equiv \{M_i^{a_i}\}$ with $i \in \{1,2,3,4\}$ are realized in a particular way such that the Kraus operators $K_i^{a_i}$ are Hermitian or, equivalently, $K_i^{a_i} = \sqrt{M_i^{a_i}}$ for all a_i and for all i, where $\{M_i^{a_i}\}$ are the measurement effects. In other words, any state updates due to a measurement following the the Lüders rule.*

Note that the Lüders rule for state evolution due to quantum measurement appears in the context of unsharp measurements [62] and other scenarios [63, 64]. Now, under Assumptions 1-3 the above-mentioned certification protocol using the temporal inequalities (13) alone is robust as stated below.

Theorem 4. *Suppose that in the scenario considered by us with any fixed value of d under Assumptions 1-3, the quantum violation of the temporal inequality (13) is $4(d-1)$, which is achieved by unknown measurements A_1, A_2, A_3, A_4 acting on some $\mathbb{C}^D$. Then, for any d, $\mathbb{C}^D = \mathbb{C}^d \otimes \mathcal{H}'$ and there exists a unitary transformation U such that Eq. (34) holds true.*

Moreover, under Assumptions 1-3, if a quantum violation $4(d-1) - \epsilon$ is achieved by non-ideal measurements $\widetilde{A}_1, \widetilde{A}_2, \widetilde{A}_3, \widetilde{A}_4$ for any non-negative ϵ, then the following two relations hold for all $k \in \{1, \cdots, d-1\}$,

$$\Big\| \left[A_1^{(k)}\left(a_kA_3^{(k)\dagger} + a_k^*\omega^kA_4^{(k)\dagger}\right)\right]\rho^{(\mathcal{P})} - \left[\widetilde{A}_1^{(k)}\left(a_k\widetilde{A}_3^{(k)\dagger} + a_k^*\omega^k\widetilde{A}_4^{(k)\dagger}\right)\right]\rho^{(\mathcal{P})}\Big\|_{HS} < \sqrt{\epsilon}, \quad (58)$$

$$\Big\| \left[A_2^{(k)}\left(a_k^*A_3^{(k)\dagger} + a_kA_4^{(k)\dagger}\right)\right]\rho^{(\mathcal{P})} - \left[\widetilde{A}_2^{(k)}\left(a_k^*\widetilde{A}_3^{(k)\dagger} + a_k\widetilde{A}_4^{(k)\dagger}\right)\right]\rho^{(\mathcal{P})}\Big\|_{HS} < \sqrt{\epsilon}. \quad (59)$$

Proof. Let us first note that the expression of the joint probability $p(a_i, a_j|A_i, A_j)$ given by (4) immediately reduces to

$$p(a_i, a_j|A_i, A_j) = \mathrm{Tr}\left[M_j^{a_j}\, M_i^{a_i}\, \rho^{(\mathcal{P})}\right] \quad \forall\, i,j \in \{1,2,3,4\}, \text{ and } \forall\, a_i, a_j \in \{0, \cdots, d-1\} \quad (60)$$

if each Kraus operator $K_i^{a_i}$ is taken to be $\sqrt{M_i^{a_i}}$. Consequently, using Eqs.(9), (10) and (60), we have for all $k, l = 1, \cdots, d-1$ and for all $i, j \in \{1, 2, 3, 4\}$,

$$\langle A_i^{(k)} A_j^{(l)} \rangle = \mathrm{Tr}\Big[A_i^{(k)} A_j^{(l)} \rho^{(\mathcal{P})}\Big].$$

Therefore, in this case, the left hand sides of the temporal inequalities (13) under Assumptions 1-3 can be expressed in the form (16) without requiring the condition (6) to be satisfied by the four measurements.

The only difference here from the previous calculation is the fact that ${A_i^{(k)}}^\dagger A_i^{(k)} \leq \mathbb{1}$ for all i and k. Following the exact steps done from Eq.(16) to Eq.(23), one obtains

$$\sum_{k=1}^{d-1} \sum_{x=1}^{2} \Big[\Big(P_x^{(k)}\Big)^\dagger \Big(P_x^{(k)}\Big)\Big] \leq 4(d-1)\,\mathbb{1} - \hat{\beta}_{\tau_d}, \tag{61}$$

where $P_x^{(k)}$ is defined in (19) and the equality in (61) holds only if ${A_i^{(k)}}^\dagger A_i^{(k)} = \mathbb{1}$ for all i and k. Since the left hand side of Eq. (61) is sum of positive operators, we also have Eq. (24). Now, we know a quantum realization (34) that achieves $\tau_d = 4(d-1)$ and at the same time satisfies Assumptions 1-3. This implies that, even without condition (6), the maximum quantum magnitude of τ_d is $4(d-1)$ under Assumptions 1-3. More importantly, when $\mathrm{Tr}[\rho^{(\mathcal{P})} \hat{\beta}_{\tau_d}] = 4(d-1)$ is attained, we must have equality in Eq. (61). Consequently, the equality in the sum-of-square decomposition (61) implies ${A_i^{(k)}}^\dagger A_i^{(k)} = \mathbb{1}$ for all i and k.

Now, as shown in [65], ${A_i^{(k)}}^\dagger A_i^{(k)} = \mathbb{1}$ if and only if the measurement effects $\{M_i^{a_i}\}$ are mutually orthogonal projectors. It is, therefore, implied that when the maximal quantum violation of the temporal inequality (13) with any fixed d under the Assumptions 1-3 is attained, then the observables $A_i^{(k)}$ are unitary and $A_i^{(k)} = A_i^k$ for all i and k. Therefore, in this case, the whole proof of Theorem 1 remains valid without invoking the condition (6). In other words, one can certify the observables A_i with $i \in \{1, 2, 3, 4\}$ only using the temporal inequalities (13) under Assumptions 1-3.

For the robustness part, note that the relations (58-59) are similar to the previously derived robustness relations (54-55) in Theorem 3. One can verify that (58-59) can be derived following the exact steps used for deriving (54-55) taking all $k \in \{1, \cdots, d-1\}$. The only difference in the present case is the fact that ${\widetilde{A}_i^{(k)}}^\dagger \widetilde{A}_i^{(k)} \leq \mathbb{1}$ for all $k \in \{1, \cdots, d-1\}$ instead of strict equality in case of each non-ideal observable $\widetilde{A}_i$ with $i \in \{1, 2, 3, 4\}$. □

5 Secure randomness certification

Here, we present a protocol for the secure certification of randomness as a relevant application of our proposed formalism for the certification of d-outcome quantum measurements. In particular, let us consider that the Assumptions 1 and 2 are satisfied in the scenario considered by us with any fixed value of d. Further, we also assume that the condition (6) is satisfied by the each of the four unitary observables A_1, A_2, A_3, A_4 and the magnitude of the temporal inequality (13) is $4(d-1)$ using the above four measurements.

Consider a scenario, where a party, say, Eve prepares the initial state. In other words, the internal functioning of the preparation device $\mathcal{P}$ is controlled by Eve. In each experimental run, Eve prepares a pure state $|\psi_x^{(\mathcal{P})}\rangle$ in such a way that, on average, the initial state becomes $\rho^{(\mathcal{P})} = \mathbb{1}/D$. Let us assume that Eve knows beforehand which two measurements will be performed sequentially in each run. In such a scenario, Eve can always predict the outcome of the first measurement. For example, consider an experimental run in which measurement of A_i is performed at first on the preparation, and then the measurement of A_j is performed (where $i, j \in \{1, 2, 3, 4\}$). In this case, Eve can predict the outcome of the first measurement by preparing an eigenstate of A_i. Hence, no randomness can be certified securely from the first measurement and, therefore, we will focus on randomness certification using the outcome statistics of the second measurement.

Since, we are not interested in the randomness certification using the outcome statistics of the first measurement, it excludes certifying classical randomness associated with the preparation $\rho^{(\mathcal{P})} = \mathbb{1}/D$. In other words, although the preparation device prepares a maximally mixed state, the randomness from the maximally mixed state is not genuine quantum randomness, rather this randomness is a manifestation of the classical convex mixture of different pure states. How-

ever, after the first measurement, the state collapses to a different pure state, and thus the outcome of the second measurement provides genuine quantum randomness. This is why we will certify randomness from $p(a_j|A_i, A_j, a_i) = p(a_i, a_j|A_i, A_j)/p(a_i|A_i)$.

Let us now define the measure of randomness, $\mathcal{H}(A_i, A_j)$ for a fixed set of two observables $\{A_i, A_j\}$ as,

$$\mathcal{H}(A_i, A_j) = \min_{\mathcal{S}} \left[-\sum_{a_i=0}^{d-1} p(a_i|A_i) \sum_{a_j=0}^{d-1} \alpha \log_2 \alpha \right], \quad \text{with } \alpha = p(a_j|A_i, A_j, a_i) \tag{62}$$

and $\mathcal{S}$ denoting all possible strategies of Eve for preparing A_i reproducing the observed probabilities. The above quantification is based on the Shannon entropy that characterizes the average randomness involved in the probability distributions [66]. Further, we have taken average of it over all possible outcomes of the first measurement.

Moreover, to quantify the genuine or guaranteed randomness we have to consider the minimum in (62) over all possible Eve's strategy of preparing the four observables A_i that satisfy the condition (6) and gives $\tau_d = 4(d-1)$ under Assumptions 1-2.

Since, the condition (6) is satisfied by the each of the four unknown observables A_1, A_2, A_3, A_4 and the magnitude of the temporal inequality (13) is $4(d-1)$, Theorem 1 implies that there exists U such that

$$\begin{aligned} U\Pi_1^{a_1}U^\dagger &= \widetilde{\Pi}_1^{a_1} \otimes \mathbb{1}_{\mathcal{H}'} = |Z_d^{a_1}\rangle\langle Z_d^{a_1}| \otimes \mathbb{1}_{\mathcal{H}'}, \\ U\Pi_2^{a_2}U^\dagger &= \widetilde{\Pi}_2^{a_2} \otimes \mathbb{1}_{\mathcal{H}'} = |T_d^{a_2}\rangle\langle T_d^{a_2}| \otimes \mathbb{1}_{\mathcal{H}'}, \\ U\Pi_3^{a_3}U^\dagger &= \widetilde{\Pi}_3^{a_3} \otimes \mathbb{1}_{\mathcal{H}'} = |M_d^{a_3}\rangle\langle M_d^{a_3}| \otimes \mathbb{1}_{\mathcal{H}'}, \\ U\Pi_4^{a_4}U^\dagger &= \widetilde{\Pi}_4^{a_4} \otimes \mathbb{1}_{\mathcal{H}'} = |N_d^{a_4}\rangle\langle N_d^{a_4}| \otimes \mathbb{1}_{\mathcal{H}'}, \\ &\forall\ a_1, a_2, a_3, a_4 \in \{0, 1, \cdots, d-1\}, \end{aligned} \tag{63}$$

where $\{\Pi_i^{a_i}\}$ are the set of mutually orthogonal projectors for measurement of A_i; $|Z_d^{a_1}\rangle$ is the eigenstate of Z_d with eigenvalue ω^{a_1}, $|T_d^{a_2}\rangle$ is the eigenstate of T_d with eigenvalue ω^{a_2}, $|M_d^{a_3}\rangle$ is the eigenstate of $M_d = a_1^* Z_d + 2(a_1^*)^3 T_d$ with eigenvalue ω^{a_3}, $|N_d^{a_4}\rangle$ is the eigenstate of $N_d = a_1 Z_d - a_1^* T_d$ with eigenvalue ω^{a_4}. Note that satisfying the condition (6) by the each of the four observables A_1, A_2, A_3, A_4 implies that the measurement effects of each of these four observables are mutually orthogonal projectors. Moreover, if the magnitude of the temporal inequality (13) is achieved to be $4(d-1)$ using the above four observables, then Theorem 1 implies that these projectors are rank-one. This follows from the fact that each of these four measurements has d number of possible outcomes and the dimension of each of the operators Z_d, T_d, M_d, N_d is d. Thus, we have taken each of the projectors in the above Eq.(63) to be rank-one.

Next, we evaluate the expression of $p(a_j|A_i, A_j, a_i)$ in order to find out $\mathcal{H}(A_i, A_j)$ for a given $\{A_i, A_j\}$. From Eq.(63), we can write the following,

$$p(a_j|A_i, A_j, a_i) = \frac{\mathrm{Tr}\left[\left(\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right)\left(U\rho^{(\mathcal{P})}U^\dagger\right)\left(\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right)\left(\widetilde{\Pi}_j^{a_j} \otimes \mathbb{1}_{\mathcal{H}'}\right)\right]}{\mathrm{Tr}\left[\left(\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right)\left(U\rho^{(\mathcal{P})}U^\dagger\right)\right]}.$$

Since $\rho^{(\mathcal{P})} = \mathbb{1}/D$, the above expression can be simplified as $p(a_j|A_i, A_j, a_i) = \frac{\mathrm{Tr}\left[\widetilde{\Pi}_i^{a_i}\widetilde{\Pi}_j^{a_j}\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right]}{\mathrm{Tr}\left[\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right]} = \mathrm{Tr}\left[\widetilde{\Pi}_i^{a_i}\widetilde{\Pi}_j^{a_j}\right] = \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2$, where $|A_i^{a_i}\rangle$ ($|A_j^{a_j}\rangle$) is the eigenstate of A_i (A_j) with eigenvalue ω^{a_i} (ω^{a_j}). In the above, we have used the fact that $\widetilde{\Pi}_i^{a_i}$ is a rank-one projector, implying that $\mathrm{Tr}\left[\widetilde{\Pi}_i^{a_i}\right] = 1$.

On the other hand, we have for $\rho^{(\mathcal{P})} = \mathbb{1}/D$

$$p(a_i|A_i) = \mathrm{Tr}\left[\left(\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right)\left(U\rho^{(\mathcal{P})}U^\dagger\right)\right]$$

$$= \frac{1}{D}\mathrm{Tr}\left[\left(\widetilde{\Pi}_i^{a_i} \otimes \mathbb{1}_{\mathcal{H}'}\right)\right] = \frac{1}{d},$$

where we have used $\mathrm{Tr}\left[\widetilde{\Pi}_i^{a_i}\right] = 1$ and $\mathrm{Tr}\left[\mathbb{1}_{\mathcal{H}'}\right] = D/d$. Therefore, Eq.(62) becomes

$$\mathcal{H}(A_i, A_j) = \min_{\mathcal{S}} \left[-\sum_{a_j=0}^{d-1} \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2 \log_2 \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2 \right]. \tag{64}$$

As mentioned earlier, $\mathcal{S}$ denotes all possible strategies of Eve for preparing A_i reproducing the observed probabilities. All these strategies are connected unitarily as can be seen from Eq.(63). However, the expression $\sum_{a_j=0}^{d-1} \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2 \log_2 \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2$ is independent of the unitary U. Hence, from Eq.(64), we have for the present case

$$\mathcal{H}(A_i, A_j) = -\sum_{a_j=0}^{d-1} \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2 \log_2 \left|\langle A_i^{a_i}|A_j^{a_j}\rangle\right|^2. \tag{65}$$

Here it should be mentioned that if $i = j$, i.e., if $A_i = A_j$, then from the above Eq.(65), we have $\mathcal{H}(A_i, A_j) = 0$. Hence, no randomness can be certified.

Next, consider that $i \neq j$. At first, let us take $i = 1$ and $j = 2$. In other words, we are considering the case when the measurement of A_1 is performed at first on the initial preparation and then the measurement of A_2 is performed. For this case, Eq. (65) reduces to

$$\mathcal{H}(A_1, A_2) = -\sum_{a_2=0}^{d-1} \left|\langle Z_d^{a_1}|T_d^{a_2}\rangle\right|^2 \log_2 \left|\langle Z_d^{a_1}|T_d^{a_2}\rangle\right|^2. \tag{66}$$

This can be evaluated using the expressions of the eigenstates of Z_d and T_d. The spectral decomposition of Z_d and T_d are given by [37],

$$Z_d = \sum_{q=0}^{d-1} \omega^q |q\rangle\langle q|, \quad \text{and} \quad T_d = \sum_{r=0}^{d-1} \omega^r |r\rangle\langle r|_{T_d}$$

with

$$|r\rangle_{T_d} = \frac{2}{d} \sum_{q=0}^{d-1} (-1)^{\delta_{q,0}} \frac{\omega^{-\frac{q}{2}}}{1-\omega^{r-q-\frac{1}{2}}} |q\rangle$$

Using these, we have

$$\left|\langle Z_d^{a_1}|T_d^{a_2}\rangle\right|^2 = \frac{4}{d^2} \frac{1}{\left|1-\omega^{a_1-a_2-\frac{1}{2}}\right|^2}. \tag{67}$$

Now, replacing the variable $(a_1 - a_2)$ by x and using the fact that $\omega^d = 1$, we get

$$\mathcal{H}(A_1, A_2) = -\sum_{x=0}^{d-1} \frac{4}{d^2} \frac{1}{\left|1-\omega^{x-\frac{1}{2}}\right|^2} \log_2 \frac{4}{d^2} \frac{1}{\left|1-\omega^{x-\frac{1}{2}}\right|^2}. \tag{68}$$

Next, let us take $i = 2$ and $j = 1$. In other words, we are considering the case when the measurement of A_2 is performed at first on the initial preparation and then the measurement of A_1 is performed. In this case, one can easily check that

$$\mathcal{H}(A_2, A_1) = \mathcal{H}(A_1, A_2)$$

We now calculate $\mathcal{H}(A_1, A_2)$ for several values of d and the variation is plotted in Fig. 2. From this figure, it is evident that $\mathcal{H}(A_1, A_2)$ increases

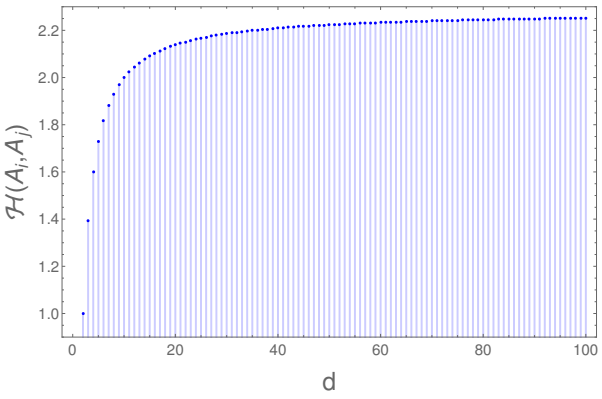

Figure 2: The blue dotted lines demonstrate the variation of the amount of output randomness $\mathcal{H}(A_i, A_j)$ produced in the present certification protocol with the number of outcomes d. Here, $\mathcal{H}(A_i, A_j)$ is the amount of randomness produced from the second measurement when the measurement of A_i is performed at first on the initial preparation and then the measurement of A_j is performed. This plot is for four possible cases- (1) when $i = 1$ and $j = 2$, (2) when $i = 2$ and $j = 1$, (3) when $i = 3$ and $j = 4$, (4) when $i = 4$ and $j = 3$.

with d.

Since $M_d = a_1^* Z_d + 2(a_1^*)^3 T_d$ and $N_d = a_1 Z_d - a_1^* T_d$ are connected to Z_d and T_d, respectively, with the same unitary W (see proof of Theorem 1), we have $\left|\langle A_1^u | A_2^v\rangle\right|^2 = \left|\langle A_3^u | A_4^v\rangle\right|^2$ for all $u, v \in \{0, 1, \cdots, d-1\}$.. Hence, for the case with $i = 3$, $j = 4$ and for the case with $i = 4$, $j = 3$, we have

$$\mathcal{H}(A_3, A_4) = \mathcal{H}(A_4, A_3) = \mathcal{H}(A_1, A_2). \quad (69)$$

For other combinations of $i \neq j \in \{1, 2, 3, 4\}$, we have not evaluated $\mathcal{H}(A_i, A_j)$ in the present study, and we leave it as an open question.

6 Conclusions

Formulating efficient certification protocols for quantum measurements requiring fewer assumptions or trusts on the preparation device is a worthwhile enterprise that will be helpful for establishing secure quantum information theoretic and cryptographic applications. In this work we have proposed a novel framework for certification of a particular set of d-outcome quantum measurements, which does not require entanglement or any other spatial quantum correlation. Further, our protocol does not need any prior knowledge or assumption about the dimension of the system on which the measurements are performed. Importantly, the specific measurements certified in the present study has fundamental significance as well as information theoretic applications. Considering a scenario consisting of a preparation followed by two measurements in sequence, we have first proposed a class of inequalities involving temporal correlations, and have then established their sum-of-squares decompositions. Using quantum violations of these inequalities, we have certified a specific set of d-outcome quantum measurements uniquely up to some unitary freedom. Moreover, we have shown that our certification protocol is robust against non-ideal realizations. As a proposed application, our protocol can be used to generate genuine quantum randomness.

It needs to be emphasized that one cannot certify the measurements uniquely without any assumption whatsoever on the preparation device, employing the quantum violations of our proposed temporal inequalities. Starting with a preparation device producing a maximally mixed states of dimension D, one can certify some particular d-outcome quantum measurements of dimension D with $D \geq d$ following our protocol. Further, no information about D is required for realizing this protocol. Therefore, in our certification scheme, preparing D number of mutually orthogonal pure states in $\mathbb{C}^D$ in different experimental runs randomly by the preparation device is sufficient. In comparison, tomography of such measurements requires $\mathcal{O}(D^2)$ characterized quantum preparations [67]. Hence, the requirement on the preparation device in our protocol is less demanding than that in the case of tomography of quantum measurements. Additionally, tomography also requires some prior knowledge about measurement devices, in contrast to those in our scheme that behave essentially as black boxes without memory.

Unlike certification protocols of d-outcome measurements proposed earlier [37, 68], entanglement between two spatially separated particles is not necessary for the successful realization of our protocol. However, in order to realize our protocol, one must trust that the preparation device produces maximally mixed state of a single particle. Since, for a given dimension, preparing a particular mixed state of a single particle is easier than preparing two spatially separated entangled particles, our protocol is less demanding to be verified experimentally, and should be more

desirable for commercial purposes.

Before concluding, it would be pertinent to mention that the analysis presented in this article for certifying quantum components received from an unknown provider also furnishes a general methodology for introducing new Leggett-Garg type temporal inequalities following the structure of the existing Bell inequalities. Adopting this methodology, certification schemes for quantum devices using temporal correlations without requiring entanglement can be designed based on the existing certification protocols in the Bell scenarios involving entanglement. For example, based on the particular Bell-type inequalities proposed in [68] applicable in the $N - m - d$ scenario (involving N parties, m measurement settings per party, d outcomes per measurement setting) with N, m, d being arbitrary, one can propose Leggett-Garg type temporal inequalities involving m number of d-outcome measurements adopting the methodology described here. Further, one can use our method to propose self-testing/certification protocols of m number of d-outcome quantum measurements using temporal correlations without using entanglement between spatially separated particles based on the self-testing proof derived in [68]. Also, the method presented here can be further applied in the context of self-testing proof proposed in [69] to devise certification scheme of three-outcome mutually unbiased quantum measurements using temporal correlations that may be useful for secure certification of larger amount of randomness.

To summarize, though the present study proposes certification protocol of some specific quantum measurements with arbitrary number of outcomes, the method presented here is quite general and can be immediately applied in different contexts to certify a wide range of quantum measurements employing temporal quantum correlations. Finally, it is worth noting that the certified d-outcome quantum measurements can be rigorously implemented in optical setups [60].

Acknowledgements

DD and DS acknowledge Science and Engineering Research Board (SERB), Government of India for financial support through the National Post Doctoral Fellowship (File Nos.: PDF/2020/001358 and PDF/2020/001682). During the later phase of this work, the research of DD is supported by the Royal Society (United Kingdom) through the Newton International Fellowship (NIF \$R1\212007). ASM acknowledges support from the project no. DST/ICPS/QuEST/2018/79 of the Department of Science and Technology, Government of India.

References

[1] I. L. Chuang and M. A. Nielsen, *Prescription for experimental determination of the dynamics of a quantum black box*, J. Mod. Opt. 44, 2455 (1997).

[2] J. F. Poyatos, J. I. Cirac, and P. Zoller, *Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate*, Phys. Rev. Lett. 78, 390 (1997).

[3] Z. Hradil, *Quantum-state estimation*, Phys. Rev. A, **55**, R1561(R) (1997).

[4] J. Helsen, J. J. Wallman, S. T. Flammia, and S. Wehner, *Multiqubit randomized benchmarking using few samples*, Phys. Rev. A, **100**, 032304 (2019).

[5] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and Robust Randomized Benchmarking of Quantum Processes*, Phys. Rev. Lett., **106**, 180504 (2011).

[6] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized benchmarking of quantum gates*, Phys. Rev. A, **77**, 012307 (2008).

[7] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, Nat Rev Phys **2**, 382 (2020).

[8] D. Mayers, and A. Yao, *Quantum cryptography with imperfect apparatus*, Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), 1998, pp. 503-509.

[9] D. Mayers, and A. Yao, *Self testing quantum apparatus*, Quantum Inf. Comput. **4**, 273 (2004).

[10] I. Supic, and J. Bowles, *Self-testing of quantum systems: a review*, Quantum **4**, 337 (2020).

[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett., **98**, 230501 (2007).

[12] S. Pironio, A. Acín, S. Massar, A. B. Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, *Random numbers certified by Bell's theorem*, Nature, **464**, 1021 (2010).

[13] B. W. Reichardt, F. Unger, and U. Vazirani, *Classical command of quantum systems*, Nature **496**, 456 (2013).

[14] M. McKague, T. H. Yang, and V. Scarani, *Robust self-testing of the singlet*, J. Phys. A: Math. Theor. **45**, 455304 (2012).

[15] T. H. Yang and M. Navascues, *Robust self-testing of unknown quantum systems into any entangled two-qubit states*, Phys. Rev. A **87**, 050102(R) (2013).

[16] C. Bamps and S. Pironio, *Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing*, Phys. Rev. A **91**, 052111 (2015).

[17] A. Coladangelo, K. T. Goh, and V. Scarani, *All pure bipartite entangled states can be self-tested*, Nat Commun **8**, 15485 (2017).

[18] Y. Wang, X. Wu, and V. Scarani, *All the self-testings of the singlet for two binary measurements*, New J. Phys. **18**, 025021 (2016).

[19] I. Supic, R. Augusiak, A Salavrakos, and A. Acín, *Self-testing protocols based on the chained Bell inequalities*, New J. Phys. **18**, 035013 (2016).

[20] I. Supic, A. Coladangelo, R. Augusiak, and A. Acín, *Self-testing multipartite entangled states through projections onto two systems*, New J. Phys. **20**, 083041 (2018).

[21] I. Supic and M. J. Hoban, *Self-testing through EPR-steering*, New J. Phys. **18**, 075006 (2016).

[22] S. Goswami, B. Bhattacharya, D. Das, S. Sasmal, C. Jebaratnam, and A. S. Majumdar, *One-sided device-independent self-testing of any pure two-qubit entangled state*, Phys. Rev. A **98**, 022311 (2018).

[23] Z. Bian, A. S. Majumdar, C. Jebaratnam, K. Wang, L. Xiao, X. Zhan, Y. Zhang, and P. Xue, *Experimental demonstration of one-sided device-independent self-testing for any pure two-qubit entangled state*, Phys. Rev. A **101**, 020301(R) (2020).

[24] H. Shrotriya, K. Bharti, and L.-C. Kwek, *Robust semi-device-independent certification of all pure bipartite maximally entangled states via quantum steering*, Phys. Rev. Research **3**, 033093 (2021).

[25] S. Sarkar, D. Saha, and R. Augusiak, *Certification of incompatible measurements using quantum steering*, arXiv:2107.02937.

[26] S. Sarkar, J. J. Borkała, C. Jebarathinam, O. Makuta, D. Saha, and R. Augusiak *Self-testing of any pure entangled state with minimal number of measurements and optimal randomness certification in one-sided device-independent scenario*, arXiv:2110.15176.

[27] A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner, *Self-testing quantum states and measurements in the prepare-and-measure scenario*, Phys. Rev. A **98**, 062307 (2018).

[28] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, *Robust Self-Testing of Quantum Systems via Noncontextuality Inequalities*, Phys. Rev. Lett. **122**, 250403 (2019).

[29] D. Saha, R. Santos, and R. Augusiak, *Sum-of-squares decompositions for a family of noncontextuality inequalities and self-testing of quantum devices*, Quantum **4**, 302 (2020).

[30] J. D. Bancal, N. Sangouard, and P. Sekatski, *Noise-Resistant Device-Independent Certification of Bell State Measurements*, Phys. Rev. Lett. **121**, 250506 (2018).

[31] M. O. Renou, J. Kaniewski, and N. Brunner, *Self-Testing Entangled Measurements in Quantum Networks*, Phys. Rev. Lett. **121**, 250507 (2018).

[32] J. Kaniewski, *Self-testing of binary observables based on commutation*, Phys. Rev. A **95**, 062323 (2017).

[33] M. McKague and M. Mosca, *Generalized Self-testing and the Security of the 6-State Protocol*, Theory of Quantum Computation,

Communication, and Cryptography, edited by W. van Dam, V. M. Kendon, and S. Severini (Springer-Verlag Berlin Heidelberg, 2011) pp. 113–130.

[34] J. Bowles, I. Supic, D. Cavalcanti, and A. Acín, *Self-testing of Pauli observables for device-independent entanglement certification*, Phys. Rev. A, **98** 042336 (2018).

[35] A. G. Maity, S. Mal, C. Jebarathinam, and A. S. Majumdar, *Self-testing of binary Pauli measurements requiring neither entanglement nor any dimensional restriction*, Phys. Rev. A, **103**, 062604 (2021).

[36] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, *Bell Inequalities Tailored to Maximally Entangled States*, Phys. Rev. Lett. **119**, 040402 (2017).

[37] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, *Self-testing quantum systems of arbitrary local dimension with minimal number of measurements*, npj Quantum Inf **7**, 151 (2021).

[38] P. Imany, J. A. Jaramillo-Villegas, M. S. Alshaykh, J. M. Lukens, O. D. Odele, A. J. Moore, D. E. Leaird, M. Qi, and A. M. Weiner, *High-dimensional optical quantum logic in large operational spaces*, npj Quantum Inf **5**, 59 (2019).

[39] S. Wang, Z.-Q. Yin, H. F. Chau, W. Chen, C. Wang, G.-C. Guo, and Z.-F. Han, *Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme*, Quantum Sci. Technol. **3**, 025006 (2018).

[40] Y.-C. Jeong, J.-C. Lee, and Y.-H. Kim, *Experimental implementation of a fully controllable depolarizing quantum operation*, Phys. Rev. A **87**, 014301 (2013).

[41] M. Frey, D. Collins, and K. Gerlach, *Probing the qudit depolarizing channel*, J. Phys. A: Math. Theor. **44**, 205306 (2011).

[42] M. Ahmed, and L. Young, *Integrated optic series and multibranch interferometers*, Journal of Lightwave Technology, **3**, 77-82 (1985).

[43] A. Melloni, G. Cusmai, R. Costa, F. Morichetti, and M. Martinelli, *Three-arm Mach-Zehnder interferometers*, Integrated Photonics Research and Applications/Nanophotonics, Technical Digest (CD) (Optica Publishing Group, 2006), paper IMC1.

[44] Y.-C. Liang, C.-W. Lim, and D.-L. Deng, *Reexamination of a multisetting Bell inequality for qudits*, Phys. Rev. A **80**, 052116 (2009).

[45] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang, *A framework for the study of symmetric full-correlation Bell-like inequalities*, J. Phys. A: Math. Theor. **45**, 125301 (2012).

[46] A. J. Leggett, and A. Garg, *Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks?* Phys. Rev. Lett. **54**, 857 (1985).

[47] C. Brukner, S. Taylor, S. Cheung, and V. Vedral, *Quantum Entanglement in Time*, arXiv: quant-ph/0402127.

[48] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, Phys. Rev. Lett. **88**, 040404 (2002).

[49] J. Barrett, A. Kent, and S. Pironio, *Maximally Nonlocal and Monogamous Quantum Correlations*, Phys. Rev. Lett. **97**, 170409 (2006).

[50] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, *Testing the Dimension of Hilbert Spaces*, Phys. Rev. Lett. **100**, 210503 (2008).

[51] Y. Cai, J.-D. Bancal, J. Romero and V. Scarani, *A new device-independent dimension witness and its experimental implementation*, J. Phys. A: Math. Theor. **49**, 305301 (2016).

[52] W. Cong, Y. Cai, J.-D. Bancal and V. Scarani, *Witnessing Irreducible Dimension*, Phys. Rev. Lett. **119**, 080401 (2017).

[53] C. Brukner, M. Zukowski, and A. Zeilinger, *Quantum Communication Complexity Protocol with Two Entangled Qutrits*, Phys. Rev. Lett. **89**, 197901 (2002).

[54] D. Martínez, A. Tavakoli, M. Casanova, G. Canas, B. Marques, and G. Lima, *High-Dimensional Quantum Communication Complexity beyond Strategies Based*

on Bell's Theorem, Phys. Rev. Lett. **121**, 150504 (2018).

[55] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, *Communication Games Reveal Preparation Contextuality*, Phys. Rev. Lett. **119**, 220402 (2017).

[56] H. Mikami and T. Kobayashi, *Remote preparation of qutrit states with biphotons*, Phys. Rev. A, **75**, 022325 (2007).

[57] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, Nat. Comm., **2**, 238 (2011).

[58] T. Durt, D. Kaszlikowski, J.-L. Chen, and L. C. Kwek, *Security of quantum key distributions with entangled qudits*, Phys. Rev. A **69**, 032313 (2004).

[59] P. Skrzypczyk, and D. Cavalcanti, *Maximal Randomness Generation from Steering Inequality Violations Using Qudits*, Phys. Rev. Lett., **120**, 260401 (2018).

[60] M. Zukowski, A. Zeilinger, and M. A. Horne, *Realizable higher-dimensional two-particle entanglements via multiport beam splitters*, Phys. Rev. A **55**, 2564 (1997).

[61] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett and E. Andersson, *Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities*, Nat. Phys. **7**, 677 (2011).

[62] P. Busch, *Unsharp reality and joint measurements for spin observables*, Phys. Rev. D **33**, 2253 (1986).

[63] P. Busch, and J. Singh, *Lüders theorem for unsharp quantum measurements*, Phys. Lett. A **249**, 10 (1998).

[64] M. B. Plenio, and P. L. Knight, *The quantum-jump approach to dissipative dynamics in quantum optics*, Rev. Mod. Phys. **70**, 101 (1998).

[65] J. Kaniewski, I. Supic, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, *Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems* Quantum **3**, 198 (2019).

[66] C. E. Shannon, *Communication theory of secrecy systems*, The Bell System Technical Journal, 28, 4 (1949).

[67] I. Gianani, Y. S. Teo, V. Cimini, H. Jeong, G. Leuchs, M. Barbieri, and L. L. Sánchez-Soto, PRX Quantum **1**, 020307 (2020).

[68] S. Sarkar, and R. Augusiak, *Self-testing of multipartite GHZ states of arbitrary local dimension with arbitrary number of measurements per party*, Phys. Rev. A **105**, 032416 (2022).

[69] J. Kaniewski, I. Supic, J, Tura, F. Baccari, A. Salavrakos, and R. Augusiak, *Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems*, Quantum **3**, 198 (2019).

[70] W. N. Anderson, Jr., E. J. Harner, and G. E. Trapp, *Eigenvalues of the difference and product of projections*, Linear Multilinear Algebra **17**, 295-299 (1985).

A Proof of Lemma 1

Consider that the following condition holds under Assumptions 1-2,

$$p(a_i, a_i|A_i, A_i) = p(a_i|A_i). \tag{70}$$

Also, since condition (5) holds for all $|\psi\rangle \in \mathbb{C}^D$ (where D is arbitrary), we have

$$p(a_i, a_i|A_i, A_i) \leq p(a_i|A_i) \quad \forall |\psi\rangle \in \mathbb{C}^D. \tag{71}$$

Hence, the condition (70) for $\rho^{(\mathcal{P})} = \mathbb{1}/D$ together with (71) implies that

$$p(a_i, a_i|A_i, A_i) = p(a_i|A_i) \quad \forall |\psi\rangle \in \mathbb{C}^D. \tag{72}$$

From the above, it follows that

$$\langle\psi| \left(\sqrt{M_i^{a_i}}\right)^\dagger (U_i^{a_i})^\dagger \, M_i^{a_i} U_i^{a_i} \sqrt{M_i^{a_i}} |\psi\rangle = \langle\psi| M_i^{a_i} |\psi\rangle \;\; \forall |\psi\rangle \in \mathbb{C}^D, \tag{73}$$

which implies

$$\left(\sqrt{M_i^{a_i}}\right)^\dagger (U_i^{a_i})^\dagger \, M_i^{a_i} U_i^{a_i} \sqrt{M_i^{a_i}} = M_i^{a_i}. \tag{74}$$

Let $M_i^{a_i} = \sum_{x=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|$ with $0 < \lambda_u \leq 1$ for all $u \in \{0, \cdots, m-1\}$; $\{|\psi_0\rangle, \cdots, |\psi_{D-1}\rangle\}$ being an orthonormal basis in $\mathbb{C}^D$ and m $(1 \leq m \leq D)$ is the rank of $M_i^{a_i}$. Putting this in Eq.(74), we get the following,

$$\left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right) (U_i^{a_i})^\dagger \left(\sum_{u=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|\right) U_i^{a_i} \left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right) = \sum_{u=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|. \tag{75}$$

Let $(U_i^{a_i})^\dagger |\psi_u\rangle = |\phi_u\rangle$ for all $u \in \{0, \cdots, D-1\}$, where $\{|\phi_0\rangle, \cdots, |\phi_{D-1}\rangle\}$ is another orthonormal basis in $\mathbb{C}^D$. Using this, we get from Eq.(75),

$$\left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right) \left(\sum_{u=0}^{m-1} \lambda_u |\phi_u\rangle\langle\phi_u|\right) \left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right) = \sum_{u=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|. \tag{76}$$

Let $|\psi_k\rangle$ belongs to the orthonormal basis $\{|\psi_0\rangle, \cdots, |\psi_{D-1}\rangle\}$ and $k \in \{0, \cdots, m-1\}$. With this, we get the following from Eq.(76),

$$\langle\psi_k| \left[\left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right) \left(\sum_{u=0}^{m-1} \lambda_u |\phi_u\rangle\langle\phi_u|\right) \left(\sum_{u=0}^{m-1} \sqrt{\lambda_u} |\psi_u\rangle\langle\psi_u|\right)\right] |\psi_k\rangle = \langle\psi_k| \left(\sum_{u=0}^{m-1} \lambda_u |\psi_u\rangle\langle\psi_u|\right) |\psi_k\rangle. \tag{77}$$

After simplifying, we get the following condition from Eq.(77),

$$\sum_{u=0}^{m-1} \lambda_u \left|\langle\phi_u|\psi_k\rangle\right|^2 = 1. \tag{78}$$

Since $\{|\phi_0\rangle, \cdots, |\phi_{D-1}\rangle\}$ is an orthonormal basis in $\mathbb{C}^D$, we have

$$\sum_{u=0}^{D-1} \left|\langle\phi_u|\psi_k\rangle\right|^2 = 1. \tag{79}$$

Now, subtracting Eq.(78) from Eq.(79), we get the following,

$$\sum_{u=0}^{m-1}(1-\lambda_u)\Big|\langle\phi_u|\psi_k\rangle\Big|^2+\sum_{u=m}^{D-1}\Big|\langle\phi_u|\psi_k\rangle\Big|^2=0. \tag{80}$$

The left hand side of the above equation is the sum of positive terms. This sum is zero if and only if each term is zero. Hence, we have

$$\langle\phi_u|\psi_k\rangle=0 \quad \forall u\in\{m,\cdots,D-1\}, \tag{81}$$

where the above holds for all $k\in\{0,\cdots,m-1\}$.

On the other hand, it can be shown that for each $u\in\{0,\cdots,m-1\}$, there exists at least one $|\psi_k\rangle$ with $k\in\{0,\cdots,m-1\}$, such that $\Big|\langle\phi_u|\psi_k\rangle\Big|^2\neq 0$. The negation of this leads to a contradiction as follows. Suppose, there exists one particular $u\in\{0,\cdots,m-1\}$, denoted by $\widetilde{u}$, such that $\Big|\langle\phi_{\widetilde{u}}|\psi_k\rangle\Big|^2=0$ for all $k\in\{0,\cdots,m-1\}$. Hence, it is implied that $|\phi_{\widetilde{u}}\rangle$ is mutually orthogonal to $|\psi_k\rangle$ for all $k\in\{0,\cdots,m-1\}$. On the other hand, by definition, $|\phi_{\widetilde{u}}\rangle$ is mutually orthogonal to $|\phi_u\rangle$ for all $u\in\{m,\cdots,D-1\}$. Since, Eq.(81) holds for all $k\in\{0,\cdots,m-1\}$, we can construct the following set: $\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle,|\phi_{\widetilde{u}}\rangle,|\phi_m\rangle,\cdots,|\phi_{D-1}\rangle\}$ consisting of $(D+1)$ number of mutually orthogonal vectors. However, in a Hilbert space of dimension D, one cannot have more than D number of mutually orthogonal vectors. Therefore, for each $u\in\{0,1,\cdots,m-1\}$, there exists at least one $|\psi_k\rangle$ with $k\in\{0,\cdots,m-1\}$, such that $\Big|\langle\phi_u|\psi_k\rangle\Big|^2\neq 0$.

Since Eq.(80) can be derived for all values of $k\in\{0,\cdots,m-1\}$, we know that there exists at least one k for each $u\in\{0,\cdots,m-1\}$ such that

$$(1-\lambda_u)\Big|\langle\phi_u|\psi_k\rangle\Big|^2=0 \quad \text{and} \quad \Big|\langle\phi_u|\psi_k\rangle\Big|^2\neq 0. \tag{82}$$

In other words, we have the following,

$$\lambda_u=1 \quad \forall u\in\{0,\cdots,m-1\}. \tag{83}$$

Hence, we have $M_i^{a_i}=\sum_{u=0}^{m-1}|\psi_u\rangle\langle\psi_u|$. That is, $M_i^{a_i}$ is a projector. Now, if condition (70) holds for all $a_i\in\{0,\cdots,d-1\}$, then each of the POVM elements $\{M_i^{a_i}\}$ is projector, i.e., $(M_i^{a_i})^2=M_i^{a_i}$ for all $a_i\in\{0,\cdots,d-1\}$. Now, it can easily be shown that the projectors $\{M_i^{a_i}\}$ are mutually orthogonal. Multiplying $M_i^{\widetilde{a}_i}$ (with $\widetilde{a}_i\in\{0,\cdots,d-1\}$) on the both sides of the normalization condition $\sum_{a_i=0}^{d-1}M_i^{a_i}=\mathbb{1}$, we get $\left(M_i^{\widetilde{a}_i}\right)^2+\sum_{\substack{a_i=0\\a_i\neq\widetilde{a}_i}}^{d-1}M_i^{a_i}M_i^{\widetilde{a}_i}=M_i^{\widetilde{a}_i}$. Since, as mentioned earlier, $\left(M_i^{\widetilde{a}_i}\right)^2=M_i^{\widetilde{a}_i}$, we have the following,

$$\sum_{\substack{a_i=0\\a_i\neq\widetilde{a}_i}}^{d-1}M_i^{a_i}M_i^{\widetilde{a}_i}=0. \tag{84}$$

The left hand side of this condition (84) is a sum of products of two projectors. Now, product of two projectors is a positive operator [70]. Hence, the left hand side of (84) is a sum of positive operators. Therefore, we have that $M_i^{a_i}M_i^{\widetilde{a}_i}=0$ for all $a_i\neq\widetilde{a}_i\in\{0,\cdots,d-1\}$.

Now, note that the condition (81) is satisfied for all $k\in\{0,\cdots,m-1\}$ by the two orthonormal basis $\{|\psi_0\rangle,\cdots,|\psi_{D-1}\rangle\}$ and $\{|\phi_0\rangle,\cdots,|\phi_{D-1}\rangle\}$ in $\mathbb{C}^D$. Hence, it is implied from (81) that the set $\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle,|\phi_m\rangle,\cdots,|\phi_{D-1}\rangle\}$ is another orthonormal basis in $\mathbb{C}^D$. Therefore, the m-dimensional subspace spanned by the vectors $\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle\}$ and the m-dimensional subspace spanned by the vectors $\{|\phi_0\rangle,\cdots,|\phi_{m-1}\rangle\}$ are the same. It is thus implied that

$$\sum_{u=0}^{m-1}|\psi_u\rangle\langle\psi_u|=\sum_{u=0}^{m-1}|\phi_u\rangle\langle\phi_u|=\widetilde{\mathbb{1}}, \tag{85}$$

where $\widetilde{\mathbb{1}}$ is the identity operator acting on the m-dimensional subspace spanned by the vectors $\{|\psi_0\rangle,\cdots,|\psi_{m-1}\rangle\}$. Since the above analysis holds for all possible choices of $U_i^{a_i}$, we have (8).

B Analysis of the temporal inequality (13) and its classical bound

Consider the following quantity $\widetilde{\tau}_d$ which is a function of several probability distributions as introduced in [36],

$$\widetilde{\tau}_d := \sum_{k=0}^{\lfloor d/2 \rfloor - 1} [\alpha_k(\mathbb{P}_k^1 + \mathbb{P}_k^2) - \beta_k(\mathbb{Q}_k^1 + \mathbb{Q}_k^2)], \tag{86}$$

where the expressions $\mathbb{P}_k^1$, $\mathbb{P}_k^2$, $\mathbb{Q}_k^1$ and $\mathbb{Q}_k^2$ are defined as

$$\mathbb{P}_k^1 = p(A_1 = A_3 + k) + p(A_2 = A_3 - k) + p(A_2 = A_4 + k) + p(A_1 = A_4 - k - 1), \tag{87}$$

$$\mathbb{Q}_k^1 = p(A_1 = A_3 - k - 1) + p(A_2 = A_3 + k + 1) + p(A_2 = A_4 - k - 1) + p(A_1 = A_4 + k), \tag{88}$$

$$\mathbb{P}_k^2 = p(A_3 = A_1 + k) + p(A_3 = A_2 - k) + p(A_4 = A_2 + k) + p(A_4 = A_1 - k - 1), \tag{89}$$

and

$$\mathbb{Q}_k^2 = p(A_3 = A_1 - k - 1) + p(A_3 = A_2 + k + 1) + p(A_4 = A_2 - k - 1) + p(A_4 = A_1 + k), \tag{90}$$

with

$$\alpha_k = \frac{1}{2d}[g(k) + (-1)^d \tan\left(\frac{\pi}{4d}\right)], \qquad \beta_k = \frac{1}{2d}[g(k+1/2) - (-1)^d \tan\left(\frac{\pi}{4d}\right)]. \tag{91}$$

Here, $g(k) = \cot[\pi(k+1/4)/d]$. Also, $p(A_i = A_j + k) := \sum_{m=0}^{d-1} p(a_i = m + k \bmod d, a_j = m | A_i, A_j)$, where $p(a_i = m + k \bmod d, a_j = m|A_i, A_j)$ denotes the joint probability of getting the outcome $a_i = (m + k \bmod d)$ when the measurement of A_i is performed on the initially prepared state $\rho^{(\mathcal{P})}$ and the outcome $a_j = m$ when the measurement of A_j is performed on the post measurement state of A_i. Following this notation, $\mathbb{P}_k^1$ and $\mathbb{Q}_k^1$ involve the probability distributions for the experimental runs in which A_1 or A_2 is measured at first on the initial preparation $\rho^{(\mathcal{P})}$ and then A_3 or A_4 is measured on the post measurement state. Similarly, $\mathbb{P}_k^2$ and $\mathbb{Q}_k^2$ contain the probability distributions for the experimental runs in which A_3 or A_4 is measured at first on the initial preparation $\rho^{(\mathcal{P})}$ and then A_1 or A_2 is measured on the post measurement state.

Now, following the calculations mentioned in the supplementary material of the Ref. [36], it can be shown that

$$\tau_d = d\,\widetilde{\tau}_d - 8S \tag{92}$$

with

$$S = \frac{1}{2}\left\{1 - \cot\left[\frac{\pi}{d}\left(\left\lfloor\frac{d}{2}\right\rfloor + \frac{1}{4}\right)\right]\right\}. \tag{93}$$

Here, τ_d is the left hand sides of the temporal inequalities (13), i.e.,

$$\begin{aligned}\tau_d = \sum_{k=1}^{d-1}\Big[&a_k \left\langle A_1^{(k)} A_3^{(d-k)}\right\rangle + a_k^* \omega^k \left\langle A_1^{(k)} A_4^{(d-k)}\right\rangle + a_k^* \left\langle A_2^{(k)} A_3^{(d-k)}\right\rangle + a_k \left\langle A_2^{(k)} A_4^{(d-k)}\right\rangle \\ &+ a_k \left\langle A_3^{(d-k)} A_1^{(k)}\right\rangle + a_k^* \omega^k \left\langle A_4^{(d-k)} A_1^{(k)}\right\rangle + a_k^* \left\langle A_3^{(d-k)} A_2^{(k)}\right\rangle + a_k \left\langle A_4^{(d-k)} A_2^{(k)}\right\rangle\Big].\end{aligned}$$

One can see that $\widetilde{\tau}_d$ is actually a linear function of probability distributions $p(a_i, a_j|A_i, A_j)$ with real coefficients. Hence, Eq.(92) implies that the left hand side of the temporal inequality (13) always takes real values.

Let us now concentrate on the classical bound of the inequality (13) proposed in the main text. Note that $\widetilde{\tau}_d$ can be expressed in the following alternative form,

$$\widetilde{\tau}_d = \sum_{k=0}^{d-1} \alpha_k \Big[p(A_1 = A_3 + k) + p(A_2 = A_4 + k) + p(A_3 = A_1 + k) + p(A_4 = A_2 + k) \\ + p(A_2 = A_3 - k) + p(A_1 = A_4 - k - 1) + p(A_3 = A_2 - k) + p(A_4 = A_1 - k - 1) \Big]. \tag{94}$$

This can be achieved using the relation that $\alpha_k = -\beta_{d-k-1}$. Hence, the terms of the sum which are attached with β_k can be shifted to indices $k = \lfloor d/2 \rfloor, \cdots, d-1$ and are now associated with an α_k [36]. For the cases where d is odd, the term $k = \lfloor d/2 \rfloor$ disappears, as $\alpha_{\lfloor d/2 \rfloor} = 0$.

Next, we use the notion of "macrorealism" [46] which is the conjunction of the following two assumptions, in order to derive the classical bound of the temporal inequality (13): *(i) Realism:* At any instant, irrespective of any measurement, a system is definitely in any one of the available states such that all its observable properties have definite values. *(ii) Noninvasive measurability:* It is possible, in principle, to determine which of the states the system is in, without affecting the state itself or the system's subsequent evolution. This notion of "macrorealism" is one of the central concepts underpinning the classical world view.

The conjunction of the assumptions 'Realism' and 'Noninvasive measurability' implies that the probability of getting the outcomes a_i and a_j, when the measurements of A_i and A_j, respectively, are performed, does not depend on the order of the two measurements. Mathematically, it implies that $p(a_i, a_j | A_i, A_j) = p(a_j, a_i | A_j, A_i)$. Using this and from the definition of $p(A_i = A_j + k)$, we have

$$\begin{aligned} p(A_j = A_i + k) &= p(A_i = A_j - k) \\ &= p(A_i = A_j + d - k) \quad \forall i, j \in \{1, 2, 3, 4\} \text{ and } \forall k \in \{0, 1, \cdots, d-1\}. \end{aligned}$$

Hence, we have

$$\sum_{k=0}^{d-1} \Big[p(A_i = A_j + k) + p(A_j = A_i + k) \Big] = \sum_{k=0}^{d-1} 2p(A_i = A_j + k) \;\; \forall i, j \in \{1, 2, 3, 4\}. \tag{95}$$

Using (95) and (94), the expression of $\widetilde{\tau}_d$ for classical systems (denoted by $\widetilde{\tau}_{d_C}$) becomes

$$\widetilde{\tau}_{d_C} = \sum_{k=0}^{d-1} 2\alpha_k \Big[p(A_1 = A_3 + k) + p(A_2 = A_4 + k) + p(A_2 = A_3 - k) + p(A_1 = A_4 - k - 1) \Big]. \tag{96}$$

Now, 'Realism' implies that we can assign definite value to each of the observables which is revealed as the outcome of the measurement. Let the assigned value of A_i be denoted by v_i for all $i \in \{1, 2, 3, 4\}$. Also, 'Noninvasive measurability' implies that v_i remains unaffected whether or not any measurement is performed prior to the measurement of A_i. Next, let us assign one value q such that $p(A_i = A_j + k) = \delta_{k,q}$, where $\delta_{k,q}$ is the Kronecker delta function. Here q depends on A_i and A_j but not all pairs of A_i and A_j appearing in $\widetilde{\tau}_{d_C}$. In this way, we can define four variables $q_i \in \{0, 1..., d-1\}$ satisfying the following conditions [36],

$$\begin{aligned} v_1 - v_3 &= q_1, \\ v_3 - v_2 &= q_2, \\ v_2 - v_4 &= q_3, \\ v_4 - v_1 &= q_4 + 1. \end{aligned} \tag{97}$$

Due to the chained character of these equations, we have

$$q_4 = -1 - \sum_{i=1}^{3} q_i \bmod d.$$

With these, $\widetilde{\tau}_{d_C}$ becomes

$$\widetilde{\tau}_{d_C} = 2\left(\sum_{i=1}^{3}\alpha_{q_i} + \alpha_{-1-\sum_{i=1}^{3} q_i \bmod d}\right), \tag{98}$$

where α_k is defined in Eq.(91). Therefore, the classical bound of $\widetilde{\tau}_d$ is given by,

$$\widetilde{C}_d = 2 \max_{0\leq q_1,q_2,q_3\leq d-1}\left(\sum_{i=1}^{3}\alpha_{q_i} + \alpha_{-1-\sum_{i=1}^{3} q_i \bmod d}\right). \tag{99}$$

Next, using Theorem 1 in the supplementary material of the Ref. [36], we have

$$\max_{0\leq q_1,q_2,q_3\leq d-1}\left(\sum_{i=1}^{3}\alpha_{q_i} + \alpha_{-1-\sum_{i=1}^{3} q_i \bmod d}\right) = 3\alpha_0 + \alpha_{d-1} \tag{100}$$

Hence, using Eqs.(91), (92) and (93), the classical bounds C_d of the temporal inequalities (13) are obtained as follows

$$\begin{aligned} C_d &= d\widetilde{C}_d - 8S \\ &= 2d(3\alpha_0 + \alpha_{d-1}) - 8S \\ &= 3\cot\left(\frac{\pi}{4d}\right) - \cot\left(\frac{3\pi}{4d}\right) - 4. \end{aligned} \tag{101}$$

C Proof of Lemma 2

Here we present an example in the case of $d = 2$ to show that if we are not restricted to any assumption on the state preparation, then there exists two different projective measurements such that those two measurements are not connected unitarily although $\tau_d = 4(d-1)$ is achieved.

For the first strategy, the prepared state is of the form

$$\begin{pmatrix} \cos\theta \\ e^{\mathbb{i}\phi}\sin\theta \\ 0 \end{pmatrix}$$

for any θ, ϕ, and the measurements are of the form $A_i = A_i^+ - A_i^-$ such that $A_i^+ = |u_i\rangle\langle u_i|$ and $A_i^- = \mathbb{1} - |u_i\rangle\langle u_i|$ wherein

$$|u_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |u_2\rangle = \begin{pmatrix} \cos\pi/4 \\ \sin\pi/4 \\ 0 \end{pmatrix}, \quad |u_3\rangle = \begin{pmatrix} \cos\pi/8 \\ \sin\pi/8 \\ 0 \end{pmatrix}, \quad |u_4\rangle = \begin{pmatrix} \cos\pi/8 \\ -\sin\pi/8 \\ 0 \end{pmatrix}.$$

For the second strategy, the prepared state is

$$\begin{pmatrix} 0.427 \\ -0.512 - \mathbb{i}0.548 \\ 0.067 + \mathbb{i}0.747 \end{pmatrix}.$$

and the measurements are of the form $A_i = A_i^+ - A_i^-$ such that $A_i^+ = |v_i\rangle\langle v_i|$ and $A_i^- = \mathbb{1} - |v_i\rangle\langle v_i|$ wherein

$$|v_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |v_2\rangle = \begin{pmatrix} 0.582 \\ -0.275 + \mathbb{i}0.308 \\ -0.264 + \mathbb{i}0.317 \end{pmatrix}, \quad |v_3\rangle = \begin{pmatrix} \cos\pi/4 \\ 1/2\ e^{\mathbb{i}\pi/4} \\ 1/2\ e^{\mathbb{i}\pi/4} \end{pmatrix}, \quad |v_4\rangle = \begin{pmatrix} 0.910 \\ -0.135 - \mathbb{i}0.384 \\ -0.104 - \mathbb{i}0.393 \end{pmatrix}.$$

We can verify that $\tau_2 = 4$ is achieved by both the strategies, where τ_2 is defined in (25). If there exists a unitary, say U, that transforms one set of measurements to the another, then the following relations must hold

$$U|u_i\rangle = |v_i\rangle, \quad \forall i = 1, 2, 3, 4. \tag{102}$$

However, the fact that $|\langle u_1|u_3\rangle| \neq |\langle v_1|v_3\rangle|$ implies that such a unitary does not exist. Note that the above example is in the three-dimensional binary outcome projective measurement scenario. Other such examples can easily be constructed in higher dimensions.

D Proof of Theorem 2

Suppose the non-ideal observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ satisfy the following,

$$p(a_i|\widetilde{A}_i) - p(a_i, a_i|\widetilde{A}_i, \widetilde{A}_i) = \eta_i^{(a_i)} \text{ with } \eta_i^{(a_i)} > 0 \quad \forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{103}$$

Since condition (5) holds for all $|\psi\rangle \in \mathbb{C}^D$ (where D is arbitrary), we have

$$p(a_i|\widetilde{A}_i) - p(a_i, a_i|\widetilde{A}_i, \widetilde{A}_i) \geq 0 \quad \forall\, |\psi\rangle \in \mathbb{C}^D. \tag{104}$$

Hence, the condition (103) together with (104) under Assumptions 1-2 implies that

$$0 \leq \langle\psi|\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i}\widetilde{K}_i^{a_i}|\psi\rangle < D\eta_i^{(a_i)} \quad \forall\, |\psi\rangle \in \mathbb{C}^D,\ \forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{105}$$

Hence, condition (105) implies the following,

$$0 \leq \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i}\widetilde{K}_i^{a_i} < D\eta_i^{(a_i)}\mathbb{1} \quad \forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{106}$$

Next, let us define the following positive Hermitian operator acting on $\mathbb{C}^D$ for all $a_i \in \{0, \cdots, d-1\}$ and for all $i \in \{1, 2, 3, 4\}$,

$$W_i^{a_i} = \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i}\widetilde{K}_i^{a_i}. \tag{107}$$

Also, consider that $\lambda_{1_i}^{a_i}, \cdots, \lambda_{D-1_i}^{a_i} \in \mathbb{R}$ are the eigenvalues of $W_i^{a_i}$. Hence, from (106), we can write

$$0 \leq \lambda_{x_i}^{a_i} < D\eta_i^{(a_i)} \quad \forall\, x \in \{0, \cdots, D-1\},\ \forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{108}$$

Now, from the definition of Hilbert Schmidt norm, we have for all $a_i \in \{0, \cdots, d-1\}$ and for all $i \in \{1, 2, 3, 4\}$

$$\left\|W_i^{a_i}\right\|_{\text{HS}} = \sqrt{\sum_{x=0}^{D-1} (\lambda_{x_i}^{a_i})^2} \tag{109}$$

Now, using (107-109), we can write

$$\left\|\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i}\widetilde{K}_i^{a_i}\right\|_{\text{HS}} < \eta_i^{(a_i)} D^{\frac{3}{2}} \quad \forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{110}$$

Next, for the ideal observables A_i (with $i \in \{1, 2, 3, 4\}$) satisfying (6), we have that $K_i^{a_i\dagger}K_i^{a_i} = \left(K_i^{a_i\dagger}\right)^2\left(K_i^{a_i}\right)^2$ for all $a_i \in \{0, \cdots, d-1\}$. This follows from the fact that each of the ideal measurements satisfies the condition (73) mentioned in Appendix A for all $a_i \in \{0, \cdots, d-1\}$. Incorporating this relation into Eq.(110), we have

$$\left\|\rho^{(\mathcal{P})}\left\{\widetilde{K}_i^{a_i\dagger}\widetilde{K}_i^{a_i} - \left(\widetilde{K}_i^{a_i\dagger}\right)^2\left(\widetilde{K}_i^{a_i}\right)^2\right\}\rho^{(\mathcal{P})} - \rho^{(\mathcal{P})}\left\{K_i^{a_i\dagger}K_i^{a_i} - \left(K_i^{a_i\dagger}\right)^2\left(K_i^{a_i}\right)^2\right\}\rho^{(\mathcal{P})}\right\|_{\text{HS}} < \frac{\eta_i^{(a_i)}}{\sqrt{D}} < \eta_i^{(a_i)}$$
$$\forall\, a_i \in \{0, \cdots, d-1\},\ \forall\, i \in \{1, 2, 3, 4\}. \tag{111}$$

E Proof of Theorem 3

We first take the condition (6) to be satisfied by the each of the four non-ideal observables $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$ under Assumptions 1-2. Hence, the measurement effects of each of these observables are mutually orthogonal projectors, which follows from Lemma 1. Hence, $\widetilde{A}_x^{(k)}$ is unitary operator and $\widetilde{A}_x^{(k)} = \widetilde{A}_x^k$ for all $x \in \{1,2,3,4\}$ and for all $k \in \{0,\cdots,d-1\}$. Also it implies that the condition (8) holds true for all the four non-ideal observables. With these non-ideal unitary observables, we have $\mathrm{Tr}[\hat{\beta}_{\tau_d}\rho^{(\mathcal{P})}] = 4(d-1) - \epsilon$ (with $\epsilon > 0$), where $\hat{\beta}_{\tau_d}$ is the operator given by Eq.(17) with $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$. Similar to (18), we define

$$\begin{aligned}\widetilde{B}_1^{(k)} &= a_k \widetilde{A}_3^{-k} + a_k^* \omega^k \widetilde{A}_4^{-k},\\ \widetilde{B}_2^{(k)} &= a_k^* \widetilde{A}_3^{-k} + a_k \widetilde{A}_4^{-k}.\end{aligned} \tag{112}$$

Let us also define the following,

$$\widetilde{P}_x^{(k)} = \mathbb{1} - \widetilde{A}_x^k\, \widetilde{B}_x^{(k)} \quad \forall x \in \{1,2\},\ \forall k \in \{1,\cdots,d-1\}. \tag{113}$$

Now, following the calculation similar to that in Sec. 3.2, we get Eq.(23) involving $\widetilde{P}_x^{(k)}$ and the operator $\hat{\beta}_{\tau_d}$ with $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$, $\widetilde{A}_4$. From this, we have

$$\mathrm{Tr}\Big[\rho^{(\mathcal{P})} \sum_{k=1}^{d-1}\sum_{x=1}^{2}\Big[\Big(\widetilde{P}_x^{(k)}\Big)^\dagger \Big(\widetilde{P}_x^{(k)}\Big)\Big]\Big] = \mathrm{Tr}\Big[\rho^{(\mathcal{P})}(4(d-1)\,\mathbb{1} - \hat{\beta}_{\tau_d})\Big].$$

Since $\rho^{(\mathcal{P})} = \mathbb{1}/D$, we get,

$$\mathrm{Tr}\Big[\sum_{k=1}^{d-1}\sum_{x=1}^{2}\Big[\Big(\widetilde{P}_x^{(k)}\Big)^\dagger \Big(\widetilde{P}_x^{(k)}\Big)\Big]\Big] = D\epsilon. \tag{114}$$

Being the sum of positive numbers, we get for the individual term,

$$\mathrm{Tr}\Big[\Big(\widetilde{P}_x^{(k)}\Big)^\dagger \Big(\widetilde{P}_x^{(k)}\Big)\Big] = f_{k,x}(\epsilon) \leq D\epsilon \quad \forall\ \ k,x. \tag{115}$$

where $\sum_{k,x} f_{k,x}(\epsilon) = D\epsilon$ and $f_{k,x}(\epsilon) \geq 0$ for all k,x. Now, from Eq.(115), we get

$$\Big|\Big|\widetilde{P}_x^{(k)}\Big|\Big|_{\mathrm{HS}} \leq \sqrt{D\epsilon} \quad \forall\ \ k,x. \tag{116}$$

Hence, from Eq.(113), we can write that

$$\Big|\Big|\mathbb{1} - \widetilde{A}_x^k\, \widetilde{B}_x^{(k)}\Big|\Big|_{\mathrm{HS}} \leq \sqrt{D\epsilon} \quad \forall\ \ k,x. \tag{117}$$

Now, for the ideal measurements, Eq.(37) implies that $A_x^k\, B_x^{(k)} = \mathbb{1}$ for all k,x. Thus, from the above relation we get

$$\Big|\Big|A_x^k\, B_x^{(k)} - \widetilde{A}_x^k\, \widetilde{B}_x^{(k)}\Big|\Big|_{\mathrm{HS}} \leq \sqrt{D\epsilon}\ \forall k,x. \tag{118}$$

Since $\rho^{(\mathcal{P})} = \mathbb{1}/D$, we get the following from Eq.(118),

$$\begin{aligned}\Big|\Big|\Big(A_x^k\, B_x^{(k)}\Big)\rho^{(\mathcal{P})} - \Big(\widetilde{A}_x^k\, \widetilde{B}_x^{(k)}\Big)\rho^{(\mathcal{P})}\Big|\Big|_{\mathrm{HS}} &\leq \sqrt{\frac{\epsilon}{D}}\\ &< \sqrt{\epsilon}\ \ \forall k,x.\end{aligned} \tag{119}$$

Putting $x = k = 1$, in Eq.(119), we get Eqs.(54), and putting $x = 2, k = 1$ in Eq.(119), we get (55). These constitute a set of robustness arguments of our certification scheme.

We can derive another set of robustness arguments of our certification scheme as described below. Note that Eq.(115) also implies the following,

$$\begin{aligned}\left|\left|\left(\widetilde{P}_x^{(k)}\right)^\dagger\right|\right|_{\text{HS}} &= \left|\left|\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right|\right|_{\text{HS}} \\ &\leq \sqrt{D\epsilon} \quad \forall \;\; k, x, \end{aligned} \tag{120}$$

Next, we have for all k, x

$$\begin{aligned}\left|\left|\mathbb{1} + \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right|\right|_{\text{HS}} &= \left|\left|2\mathbb{1} - \left[\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right]\right|\right|_{\text{HS}} \\ &\leq 2\left|\left|\mathbb{1}\right|\right|_{\text{HS}} + \left|\left| - \left[\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right]\right|\right|_{\text{HS}} \qquad (121) \\ &\leq \sqrt{D}(2+\sqrt{\epsilon}) \qquad (122)\end{aligned}$$

where we have used the triangle inequality for the Hilbert-Schmidt norm to get (121). We have also used (120) and the fact that $\left|\left|\mathbb{1}\right|\right|_{\text{HS}} = \sqrt{D}$ to get (122).

In a similar way, it can be shown using (117) that

$$\left|\left|\mathbb{1} + \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right|\right|_{\text{HS}} \leq \sqrt{D}(2+\sqrt{\epsilon}) \quad \forall \;\; k, x. \tag{123}$$

Now, we can obtain the following relation for all k, x,

$$\begin{aligned}&\left|\left|\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{B}_x^{(k)}\right)\right|\right|_{\text{HS}} \\ &= \left|\left|\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger \left(\widetilde{A}_x^k\right) \left(\widetilde{B}_x^{(k)}\right)\right|\right|_{\text{HS}} \qquad (124) \\ &= \left|\left|\frac{1}{2}\left[\left(\mathbb{1} + \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right)\left(\mathbb{1} - \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right) + \left(\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right)\left(\mathbb{1} + \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right)\right]\right|\right|_{\text{HS}} \qquad (125) \\ &\leq \frac{1}{2}\left|\left|\left(\mathbb{1} + \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right)\left(\mathbb{1} - \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right)\right|\right|_{\text{HS}} + \frac{1}{2}\left|\left|\left(\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right)\left(\mathbb{1} + \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right)\right|\right|_{\text{HS}} \qquad (126) \\ &\leq \frac{1}{2}\left|\left|\mathbb{1} + \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right|\right|_{\text{HS}} \left|\left|\mathbb{1} - \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right|\right|_{\text{HS}} + \frac{1}{2}\left|\left|\mathbb{1} - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{A}_x^k\right)^\dagger\right|\right|_{\text{HS}} \left|\left|\mathbb{1} + \widetilde{A}_x^k \, \widetilde{B}_x^{(k)}\right|\right|_{\text{HS}} \qquad (127) \\ &\leq D\sqrt{\epsilon}(2+\sqrt{\epsilon}) \qquad (128)\end{aligned}$$

where we have used $\left(\widetilde{A}_x^k\right)^\dagger \left(\widetilde{A}_x^k\right) = \mathbb{1}$ (since, $\widetilde{A}_x^k$ is a unitary operator). Next, the triangle inequality for the Hilbert-Schmidt norm is used to get (126). We obtain (127) as the Hilbert-Schmidt norm is a submultiplicative norm (i.e., for all $n \times n$ square matrices A and B, $||AB||_{\text{HS}} \leq ||A||_{\text{HS}} \, ||B||_{\text{HS}}$). Finally, we have used conditions (117), (120), (122), (123) to get (128) from (127).

Now, for ideal measurements, Eq.(38) implies that $\left(B_x^{(k)}\right)^\dagger \left(B_x^{(k)}\right) = \mathbb{1}$ for all $x \in \{1, 2\}$ and for all $k \in \{1, \cdots, d-1\}$. Hence, from (128), we get

$$\left|\left|\left(B_x^{(k)}\right)^\dagger \left(B_x^{(k)}\right) - \left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{B}_x^{(k)}\right)\right|\right|_{\text{HS}} \leq D\sqrt{\epsilon}(2+\sqrt{\epsilon}). \tag{129}$$

Next, considering $\rho^{(\mathcal{P})} = \mathbb{1}/D$, we get the following from the above inequality,

$$\left|\left|\left[\left(B_x^{(k)}\right)^\dagger \left(B_x^{(k)}\right)\right]\rho^{(\mathcal{P})} - \left[\left(\widetilde{B}_x^{(k)}\right)^\dagger \left(\widetilde{B}_x^{(k)}\right)\right]\rho^{(\mathcal{P})}\right|\right|_{\text{HS}} \leq \sqrt{\epsilon}(2+\sqrt{\epsilon}). \tag{130}$$

Now, putting $x = 1$ and $k = 1$, we get (56) after some simplification. Eq.(56) presents another robustness argument of our certification scheme for A_3 and A_4.

A similar procedure can be followed in order to establish robustness arguments for A_1 and A_2. For this, consider

$$C_1^{(k)} = a_k A_1^{-k} + a_k^* A_2^{-k} \quad \text{and} \quad C_2^{(k)} = \omega_k a_k^* A_1^{-k} + a_k A_2^{-k}.$$

Then, one can have another sum-of-squares decomposition of the inequality (13) as

$$\sum_{k=1}^{d-1} \sum_{x=1}^{2} \left[\left(Q_x^{(k)} \right)^\dagger \left(Q_x^{(k)} \right) \right] = 4(d-1)\,\mathbb{1} - \hat{\beta}_{\tau_d}$$
$$\text{with } Q_x^{(k)} = \mathbb{1} - A_{x+2}^k\, C_x^{(k)} \quad \forall x \in \{1,2\},\, \forall k \in \{1, \cdots, d-1\}. \tag{131}$$

Through a similar analysis as discussed above, we get the following relation for all k, x,

$$\left|\left| \left[\left(C_x^{(k)} \right)^\dagger \left(C_x^{(k)} \right) \right] \rho^{(\mathcal{P})} - \left[\left(\widetilde{C}_x^{(k)} \right)^\dagger \left(\widetilde{C}_x^{(k)} \right) \right] \rho^{(\mathcal{P})} \right|\right|_{\text{HS}} \leq \sqrt{\epsilon}(2 + \sqrt{\epsilon}). \tag{132}$$

Now, putting $x = 1$ and $k = 1$ in (132), we get the robustness expression (57) involving A_1 and A_2.