Semi-device-independent certification of the number of measurements

Isadora Veeren,[1] Martin Plávala,[2] Leevi Leppäjärvi,[3] and Roope Uola[4]
[1]*Centro Brasileiro de Pesquisas Físicas, Rua Dr. Xavier Sigaud, 150, Rio de Janeiro, RJ, Brasil*
[2]*Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany*
[3]*RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 84511 Bratislava, Slovakia*
[4]*Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*

(Received 18 August 2023; revised 19 January 2024; accepted 8 May 2024; published 3 June 2024)

We develop a method for semi-device-independent certification of the number of measurements. We achieve this by testing whether Bob's steering equivalent observables can be simulated by k measurements, which we do by testing whether they are k-compatible with separable joint observable. This test can be performed with the aid of hierarchy of semidefinite programs, and whenever it fails one can conclude that Alice must have access to at least $(k+1)$-incompatible measurements.

DOI: 10.1103/PhysRevA.109.062203

I. INTRODUCTION

Quantum measurement theory, pivotal in our comprehension of quantum mechanics, was originally devised to explain measurements at a foundational level. While its applications in quantum information processing have become apparent, particularly in the realm of quantum networks (see [1,2] for reviews on the topic), the focus has primarily been on single-system measurements. This is despite the fact that quantum networks have gone through a rapid development recently [3], and the investigation of such platforms necessitates the use of multipartite measurements. On top of fundamental achievements, such as disproving real-number-based models of quantum theory [4], the approach has improved our understanding of measurements on compound systems, e.g., in the form of the elegant joint measurement [5]. However, the full theory of quantum measurements on such systems is still developing, and the exact role of known concepts, such as entangled measurements and measurements simulable by local operations supported by classical communication [6,7], in networks remains unclear.

This paper contributes to the evolving theory of compound system measurements by establishing a connection between two central concepts: simulability of measurements and compatibility of measurements on many copies, resulting in a hierarchy for certifying the number of measurements in a semi-device-independent manner. On one hand, simulability examines whether the statistics of a set of quantum measurements can be explained using a predetermined set of measurements, aided by randomness and classical data processing. Recently, the concept was used to improve bounds on the Grothendieck constant $K_G(3)$ [8] in cases of sharp measurements [9]; to show the existence of truly nonprojective measurements in quantum theory [10] for measurements with fixed number of outcomes [11,12]; or yet to allow for a record high semi-device-independent certification of entanglement dimensionality [13]. Here we consider a fixed number of simulating measurements [11].

On the other hand, compatibility on many copies investigates the recovery of measurement statistics from a single measurement on a compound system [14], a generalization of compatibility of measurements, which is recovered when a single system is considered. This special case has found connections with an advantage in quantum correlations in bipartite [15–17], prepare-and-measure [18–20], and temporal [21–28] scenarios, but the more general many-copy case has not yet found applications in such setting.

We demonstrate the use of the proposed hierarchy in a quantum steering scenario. Steering manifests itself in asymmetric scenarios where Alice and Bob cannot be interexchanged [29–35] (cf. Fig. 1). Consequently, it can be exploited for practical applications, such as quantum key distribution [36], randomness certification [37–39], or secret sharing [40,41], where such asymmetry is advantageous.

Beyond applicability, steering has a considerable role in foundations of quantum mechanics. Although a distinct and independent phenomenon, it is closely related to Bell nonlocality, entanglement, and measurement incompatibility [42,43]. Indeed, steering can only be observed if the shared state is entangled and Alice's measurements are incompatible [16,17]. Such requirement makes steering detection a strategy that certifies measurements incompatibility in a semi-device-independent approach [44,45], a feat relevant on its own since incompatibility is central in many protocols.

Using our results on measurements, we go beyond witnessing incompatibility of measurements through the violation of a steering inequality, providing a strategy to actually certify the number of incompatible measurements one of the parties can access. Consider the following steering scenario: Alice and Bob share a bipartite quantum state and Alice has access to some set of measurement devices acting on her part of the state (cf. Fig. 1). Alice performs a measurement corresponding to an input x and outputs the measurement outcome a. Bob's task is to certify the cardinality of the set of the measurements settings $\{x\}_x$. In particular, we will construct a hierarchy of tests such that if one of them is successful, Bob will be able to give a lower bound for the number of (incompatible) measurements at Alice's possession. Our method also displays the main advantage of admitting a semidefinite

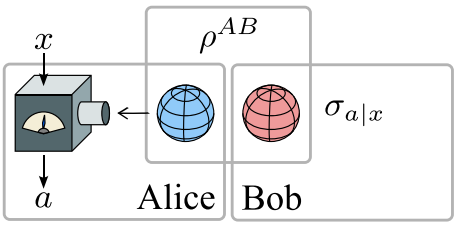

FIG. 1. The steering scenario. Alice performs local measurements x suggested by Bob and reports the outcomes a. Our aim is to set lower bounds on the cardinality of x based only on the updated local states $\sigma_{a|x}$ on Bob's side. In the scenario, Alice is treated as a black box and Bob's measurements are fully characterized.

programming (SDP) formulation, and our hierarchy of tests can, consequently, be efficiently computed with well-established methods.

II. COMPATIBILITY AND SIMULABILITY

Joint measurability of a set of positive-operator valued measures (POVMs) encapsulates the notion of whether a set of measurements can be performed simultaneously by a single device. Let $\{M_{a|x}\}_{a,x}$ be a measurement assemblage, i.e., a set of POVMs obeying $M_{a|x} \geqslant 0$ and $\sum_a M_{a|x} = \mathbb{1}$ for all a, x. This way, the set $\{M_{a|x}\}_a$ forms a POVM for every value of x, which labels the measurement setting while a labels its associated outcome. Formally, an assemblage is said to be compatible or jointly measurable if there exist a POVM $\{G_\lambda\}_\lambda$ and a probability distribution p such that, for any state ρ and all a, x,

$$\mathrm{tr}[\rho M_{a|x}] = \sum_\lambda p(a|x,\lambda)\mathrm{tr}[\rho G_\lambda]. \tag{1}$$

When this condition is met, the observable $\{G_\lambda\}_\lambda$ represents a joint measurement of $\{M_{a|x}\}_{a,x}$, as it can recover its statistics through a suitable postprocessing given by p. Equivalently, this condition can be put in terms of the marginalization of some joint measurement. In this case, there must be a POVM G with effects $G_{a_1,\ldots,a_n}$ such that $M_{a|x} = \sum_{a_i, i\neq x} G_{a_1,\ldots,a_{x-1},a,a_{x+1},\ldots,a_n}$. Then it is said that $M_{a|x}$ can be recovered as the xth marginal of G.

The notion of joint measurability can be extended to the concept of k-compatibility [14], that is central for our work. The idea is that we are allowed to perform the joint measurement on k copies of the state ρ. A set of measurements $\{M_{a|x}\}_{a,x}$ is said to be k-compatible if there exists a joint observable $\{G_\lambda\}_\lambda$ such that for any state ρ and all a, x we have

$$\mathrm{tr}[\rho M_{a|x}] = \sum_\lambda p(a|x,\lambda)\mathrm{tr}[\rho^{\otimes k} G_\lambda]. \tag{2}$$

G is called a k-copy joint observable of $\{M_{a|x}\}_{a,x}$. This is a relaxation of the usual concept of compatibility, recovered when one has access to only one copy of ρ, meaning $k = 1$. Also, notice that any set of k measurements is k-compatible. An example of incompatible but 2-compatible POVMs is given in [46], by a set of 3-incompatible POVMs that are compatible pairwise. Such triplet of POVMs is clearly 2-compatible, as one can construct the 2-copy joint POVM by measuring one of the POVMs on one copy of ρ and measuring the joint observable of the other two on the other copy of ρ.

Another central concept for our work is k-simulability [11]. In contrast to having many copies of the state, in k-simulability one has k measurements. Also, on top of classical postprocessing, in k-simulability one is allowed to use classical preprocessing. Formally, a set of measurements given by POVM elements $\{M_{a|x}\}_{a,x}$ is k-simulable if there exist probability distributions p and q, as well as k POVMs with elements $B_{b|y}$ such that for all a and x

$$M_{a|x} = \sum_{y=1}^{k} p(y|x) \sum_b q(a|b,x,y) B_{b|y}. \tag{3}$$

The interpretation of the simulation scheme is the following: given a measurement setting x the system is first measured with a POVM $\{B_{b|y}\}_b$ with probability $p(x|y)$ after which the measurement b outcome is postprocessed to a new outcome a with probability $q(a|b,x,y)$. When this scheme results in the POVMs $\{M_{a|x}\}_{a,x}$, the POVMs $\{B_{b|y}\}_{b,y}$ are called k-simulators of $\{M_{a|x}\}_{a,x}$. Notice that, similarly to k-compatibility, any set of k POVMs is k-simulable since one can always choose the k-simulators to be the same k measurements of the POVM set, i.e., any set of POVMs can be trivially simulated by itself. Furthermore, we recover the notion of usual compatibility when $k = 1$. As an example of 2-simulable but incompatible measurements one can again take the same POVMs from [46] and apply a construction analogous to the previous one.

III. STEERING AND STEERING EQUIVALENT OBSERVABLES

Consider a scenario where two parties, Alice and Bob, share a quantum state ρ_{AB}, upon which they can perform measurements and classically exchange results. On Alice's side, she has access to a set of measurements labeled by x with outcomes a, described by the POVM effects $\{M_{a|x}\}_{a,x}$. After Alice measures, Bob is left with reduced states conditioned to Alice's measurement choice and measurement outcome, i.e., Bob has access to a state assemblage $\{\rho_{a|x}\}_{a,x}$ given as $\rho_{a|x} = \mathrm{tr}_A[(M_{a|x} \otimes \mathbb{1})\rho_{AB}]$. Upon determining his state assemblage, Bob can check whether the assemblage can be explained by a local hidden state (LHS) model. An assemblage is said to allow LHS model if there are probabilities $p(a|x,\lambda)$ and subnormalized states σ_λ such that $\rho_{a|x} = \sum_\lambda p(a|x,\lambda)\sigma_\lambda$. In this case, Bob could just claim the states he observes come from local states σ_λ in his laboratory whose probability distributions are simply updated by finding out Alice's measurement outcomes. When that is not the case, Bob concludes that Alice is able to steer his states, i.e., the state assemblage cannot be realized using a separable state.

Steerability of any state assemblage can be put in terms of a joint measurability problem. Let $\rho_B = \mathrm{tr}_A[\rho_{AB}]$ be Bob's reduced state and Π_B be the projection onto range(ρ_B), i.e., the subspace spanned by the column vectors of ρ_B. The steering equivalent observables (SEO) of Bob's state assemblage $\{\rho_{a|x}\}_{a,x}$ are defined as $S_{a|x} = \tilde{\rho}_B^{-\frac{1}{2}} \tilde{\rho}_{a|x} \tilde{\rho}_B^{-\frac{1}{2}}$, where $\tilde{\rho}_{a|x} = \Pi_B \rho_{a|x} \Pi_B^\dagger$ and $\tilde{\rho}_B = \Pi_B \rho_B \Pi_B^\dagger$. It is known that $\{\rho_{a|x}\}_{a,x}$ has LHS model if and only if $\{S_{a|x}\}_{a|x}$ is jointly measurable [47].

IV. CONSTRUCTING THE TEST

We now introduce a string of implications that leads to a test certifying that Alice must have access to more than k-incompatible measurements. We start showing that if a measurement assemblage is k-simulable, then the SEO of the corresponding state assemblage is also k-simulable. Consider a measurement assemblage $\{M_{a|x}\}_{a,x}$. If $\{M_{a|x}\}_{a,x}$ is k-simulable, then there exist probability distributions p and q, as well as k POVMs with effects $\{B_{b|y}\}_{b,y}$, that satisfy Eq. (3). Bob's SEO are given by

$$S_{a|x} = \tilde{\rho}_B^{-\frac{1}{2}} \Pi_B \mathrm{tr}_A[(M_{a|x} \otimes \mathbb{1})\rho_{AB}]\Pi_B^\dagger \tilde{\rho}_B^{-\frac{1}{2}}. \tag{4}$$

Using Eq. (3) we have

$$S_{a|x} = \sum_{y=1}^{k} \sum_b p(y|x)q(a|b,x,y) \times \tilde{\rho}_B^{-\frac{1}{2}} \Pi_B \mathrm{tr}_A[(B_{b|y} \otimes \mathbb{1})\rho_{AB}]\Pi_B^\dagger \tilde{\rho}_B^{-\frac{1}{2}}. \tag{5}$$

We can simply identify $\tilde{B}_{b|y}$, the simulators of $S_{a|x}$, as

$$\tilde{B}_{b|y} = \tilde{\rho}_B^{-\frac{1}{2}} \Pi_B \mathrm{tr}_A[(B_{b|y} \otimes \mathbb{1})\rho_{AB}]\Pi_B^\dagger \tilde{\rho}_B^{-\frac{1}{2}}. \tag{6}$$

We assume p, q to be probability distributions, so if $\{\tilde{B}_{b|y}\}_{b,y}$ is a measurement assemblage of k POVMs then, by definition, $S_{a|x}$ is k-simulable. All that is left is to show that $\tilde{B}_{b|y} \geqslant 0$ and $\sum_b \tilde{B}_{b|y} = \mathbb{1}$ for all b, y.

One easily sees that the first condition holds since $B_{b|y} \geqslant 0$, we only need to check that $\sum_b \tilde{B}_{b|y} = \mathbb{1}$. We have

$$\sum_b \tilde{B}_{b|y} = \tilde{\rho}_B^{-\frac{1}{2}} \Pi_B \rho_B \Pi_B^\dagger \tilde{\rho}_B^{-\frac{1}{2}} = \tilde{\rho}_B^{-\frac{1}{2}} \tilde{\rho}_B \tilde{\rho}_B^{-\frac{1}{2}} = \mathbb{1}. \tag{7}$$

With that we conclude that if a measurement assemblage is k-simulable, then the steering equivalent observables of the state assemblage it generates will also be k-simulable. Notice that the converse is not true: if the SEO of a state assemblage is k-simulable, it does not mean that the measurement assemblage that generated it is also k-simulable. As a counterexample, whenever Alice and Bob share a separable state, Bob's steering equivalent observables will be k-simulable for any $k \geqslant 1$, regardless of whether Alice's measurement assemblage is k-simulable.

We now recall a result of [48] where it was shown (in the framework of general probabilistic theories) that k-simulability implies k-compatibility of the measurement assemblage. Furthermore, in this case the k-copy joint measurement can be chosen to be of the product form. For completeness, we formulate the proof in the case of quantum theory. We prove it by directly constructing a joint measurement for the assemblage. Consider the set $\{M_{a|x}\}_{a,x}$ that is k-simulable, meaning there must exist probability distributions p, q and measurement assemblage $\{B_{b|y}\}_{b,y}$ of k POVMs that satisfy (3). Define

$$N_{b|y} = \underbrace{\mathbb{1} \otimes \cdots \otimes \overbrace{B_{b|y}}^{y\text{th term}} \otimes \cdots \otimes \mathbb{1}}_{k \text{ terms}}, \tag{8}$$

it follows that

$$\mathrm{tr}[\rho M_{a|x}] = \sum_{y=1}^{k} \sum_b p(y|x)q(a|b,x,y)\mathrm{tr}[\rho^{\otimes k} N_{b|y}]. \tag{9}$$

Now, notice that the POVM elements $N_{b|y}$ can be obtained as yth marginal of $\tilde{N}_{\vec{b}} = B_{b_1|1} \otimes \cdots \otimes B_{b_y|y} \otimes \cdots \otimes B_{b_k|k}$, where $\vec{b} = (b_1, \ldots, b_k)$. Indeed,

$$N_{b|y} = \sum_{b_i, i \neq y} B_{b_1|1} \otimes \cdots \otimes B_{b|y} \otimes \cdots \otimes B_{b_k|k}. \tag{10}$$

So one can derive that

$$\mathrm{tr}[\rho M_{a|x}] = \sum_{y=1}^{k} \sum_{b_1 \ldots b_k} p(y|x)q(a|b_y,x,y)\mathrm{tr}[\rho^{\otimes k} \tilde{N}_{\vec{b}}]. \tag{11}$$

One can identify $\sum_{y=1}^{k} p(y|x)q(a|b_y,x,y)$ with a probability distribution $p'(a|x,\vec{b})$, and easily check that this object obeys $p'(a|x,\vec{b}) \geqslant 0 \; \forall \, a, x, \vec{b}$ and $\sum_a p'(a|x,\vec{b}) = 1 \; \forall \, x, \vec{b}$. We thus conclude that the set $\{M_{a|x}\}_{a,x}$ must be k-compatible with k-copy joint observable in a product form.

In our context, this implication requires that if Bob's SEO are k-simulable they will also admit a k-copy joint measurement in a product form. The conditions that we have derived here are necessary and will, in the following section, enable us to develop a hierarchy of conditions to check k-simulability in a semi-device-independent scenario. It is an open question whether the conditions are also sufficient, or whether one needs to consider additional conditions. We present sufficient conditions for 2-compatibility in the Appendix and we relegate the question of necessary and sufficient conditions to future research.

V. CONSTRUCTING THE SDP HIERARCHY

Given Bob's state assemblage $\{\rho_{a|x}\}_{a,x}$, one can construct its SEO $\{S_{a|x}\}_{a,x}$. We know that if Alice's measurement assemblage $\{M_{a|x}\}_{a,x}$ is k-simulable then so is Bob's SEO, which means that if $\{S_{a|x}\}_{a,x}$ is not k-simulable then neither is $\{M_{a|x}\}_{a,x}$. Additionally, recall that any set of k POVMs is k-simulable, i.e., if $\{M_{a|x}\}_{a,x}$ is not k-simulable it must consist of more than k measurements. Furthermore, the POVMs must be incompatible since otherwise they would be compatible, i.e., 1-simulable and thus also k-simulable. Thus, by checking the k-simulability of $\{S_{a|x}\}_{a,x}$ one can extract information about Alice's measurements: if Bob's SEO are k-simulable the test is inconclusive, but if $\{S_{a|x}\}_{a,x}$ is not k-simulable then we conclude that Alice's measurement assemblage must consist of at least $k+1$ incompatible measurements.

The task of directly checking the k-simulability of a set of POVMs cannot in general be easily computed, as the corresponding problem deals with nonlinear constraints, for which there is no known SDP formulation. However, it is still possible to perform different tests, and one can, for instance, simply check the k-compatibility of $\{S_{a|x}\}_{a,x}$ using an SDP. Alternatively, one can test the k-compatibility of $\{S_{a|x}\}_{a,x}$ and

enforce that the k-copy joint observable has positive partial transpose also using an SDP. Lastly, one can test whether $\{S_{a|x}\}_{a,x}$ is k-compatible with k-copy joint observable in a separable form through an SDP hierarchy. These SDPs give a series of tests and if any of these programs is not feasible, then we know that Alice's assemblage must consist of at least $(k+1)$-incompatible measurements. If all these SDPs are feasible, then the test's result is inconclusive since the existence of a separable k-copy joint observable does not imply that it can be selected to be in a product form.

Even though SDPs for computing the joint measurability of a set $\{M_{a|x}\}_{a,x}$ can be directly written from the definition of compatibility, it takes further investigation to be able to formulate an analogous construction to k-compatibility. We must recall the main result in [14], stating that the k-compatibility of a set $\{M_{a|x}\}_{a,x}$ is equivalent to compatibility of the set $\{\tilde{M}^k_{a|x}\}_{a,x}$, defined as

$$\tilde{M}^k_{a|x} = \frac{1}{k}\sum_{\ell=0}^{k-1} \mathbb{1}^{\ell} \otimes M_{a|x} \otimes \mathbb{1}^{\otimes k-\ell-1}. \tag{12}$$

With this, one can construct an SDP to check the k-compatibility of Bob's SEO. All that is left is to also require that the k-copy joint observables are separable. From Eq. (12) it is clear that if the k-copy joint observable of $\{M_{a|x}\}_{a,x}$ is of the product form then the joint observable of $\{\tilde{M}_{a|x}\}_{a,x}$ is separable.

A bipartite operator $X \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$, where $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ denotes the set of linear operators on the tensor product of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, is said to be separable if it can be written as $X = \sum_i Y_i \otimes Z_i$, where Y_i, Z_i are positive operators on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Determining whether an operator can be put in this form is an NP-hard problem but there are many separability criteria that can be used, most famously the positive partial transpose (PPT) criterion, stating that if X is separable then its partial transpose must be positive, i.e., $X^{T_A} \geqslant 0$. Here T_A denotes the partial transpose over the system A, defined as $(X_A \otimes X_B)^{T_A} = X_A^T \otimes X_B$.

One can consider the hierarchy of criteria established in [49] by Doherty, Parrilo, and Spedalieri, known as the DPS hierarchy, where symmetric extensions of $X \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_{B_1})$ are constructed, namely, operators $\tilde{X}_N \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_N})$ such that $\mathrm{tr}_{B_2,\ldots,B_N}[\tilde{X}_N] = X$ and $\tilde{X}_N = P\tilde{X}_N P$, where P is the operator that performs any permutation of $\mathcal{H}_{B_1}, \ldots, \mathcal{H}_{B_N}$. If a certain operator X has symmetric extension for arbitrary $N \in \mathbb{N}$, then X is separable. This construction is easily generalized to proving full separability of multipartite operators. In this case one needs to search for symmetric extensions over all parties but one (see [50]).

With this construction, one can build an SDP hierarchy to test whether Bob's SEO is k-compatible with separable k-copy joint observable. Since the Nth level of the hierarchy corresponds to symmetrically extending its POVM elements to N copies, we can also apply the PPT criterion to them to improve convergence of the hierarchy. Whenever the test fails one is sure that $\{S_{a|x}\}_{a,x}$ are not k-compatible with k-copy joint observable in a product form and, hence, after evaluating the string of implications we constructed, Alice must have access to at least $(k+1)$-incompatible measurements. For $N = 2$ we obtain the following SDP:

given	$\{\tilde{S}^k_{a\|x}\}_{a,x}$
find	$\{\tilde{G}_\lambda\}_\lambda$
s.t.	
k-compatibility	$\begin{cases} \tilde{S}^k_{a\|x} = \sum_\lambda p(a\|x,\lambda) G_\lambda, \forall\, a, x \\ \sum_\lambda G_\lambda = \mathbb{1} \\ G_\lambda \geqslant 0, \forall\, \lambda \end{cases}$
PPT	$\{\tilde{G}_\lambda^{T_X} \geqslant 0, X = \{A, B_1, B_2\}$
first level of DPS	$\begin{cases} \mathrm{tr}_{B_2}[\tilde{G}_\lambda] = \mathrm{tr}_{B_1}[\tilde{G}_\lambda] = G_\lambda \\ \tilde{G}_\lambda \geqslant 0. \end{cases}$

Recall that $\{\tilde{S}^k_{a|x}\}_{a,x}$ are constructed from $\{S_{a|x}\}_{a,x}$ according to (12), and the variables of the SDP are the operators $\{\tilde{G}_\lambda\}_\lambda$. Whenever this task has no solution one can conclude that Alice has access to at least $(k+1)$-incompatible measurements. If there are $\{\tilde{G}_\lambda\}_\lambda$ that obey these constraints the test is inconclusive and one can consider higher levels of the separability hierarchy.

VI. EXAMPLES

To test the efficiency in certifying a lower bound for the number of Alice's measurements, one can investigate the typical example of measurements in mutually unbiased bases (MUB), considering that Alice and Bob share a maximally entangled state. Consider the noisy version of Alice's measurement assemblage $\{M_{a|x}\}_{a,x}$, consisting of n_x measurements with n_a outcomes each, parametrized by the visibility $t \in [0,1]$ as $M^t_{a|x} = tM_{a|x} + (1-t)\frac{\mathbb{1}}{n_a}$. For $t = 0$ we have simply a trivial set of measurements, which is clearly k-compatible with separable k-copy joint measurement, and for $t = 1$ we recover the original MUB measurements. One can evaluate what is the critical visibility t_c for which $\{M^t_{a|x}\}_{a,x}$ passes the test, meaning for $t \geqslant t_c$ we can certify that Alice's assemblage consists of at least $(k+1)$-incompatible measurements.

For qubits we do not need to consider the DPS hierarchy since in this case an operator is separable if and only if it is PPT. We thus obtain that for all three MUBs, the critical visibility for 2-compatibility is $\frac{\sqrt{3}}{2}$, while the critical visibility for 2-compatibility with separable k-copy joint observable is $\sqrt{\frac{2}{3}}$.

For qutrits our findings are summarized in Fig. 2. The full criteria to be evaluated is that the set $\{S^k_{a|x}\}_{a,x}$ must be k-compatible with separable k-copy joint observable. We provide three upper estimates: k-compatibility, k-compatibility with PPT, that is, the case when we enforce that the k-copy joint observable is PPT, and k-compatibility with PPT and first level DPS, that is, we enforce that the k-copy joint observable is PPT and satisfies the first level of the DPS hierarchy.

VII. CONCLUSION

We developed a hierarchy of conditions that enable semi-device-independent certification of the number of measurements, establishing a lower bound for this quantity. We

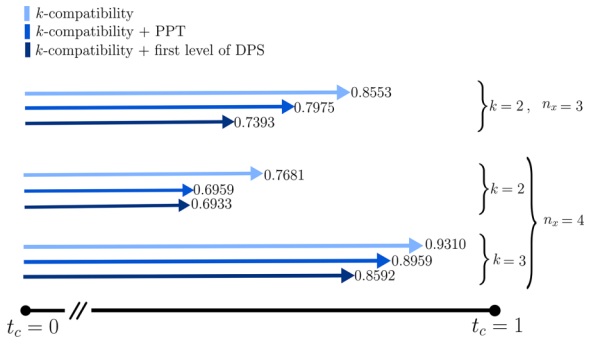

FIG. 2. Critical values t_c for the visibility below which the set $\{S^k_{a|x}\}_{a,x}$ is k-compatible, k-compatible with PPT, i.e., we enforce that the k-copy joint observable is PPT, and k-compatible with PPT and first-level DPS, i.e., the k-copy joint observable is PPT and satisfies the first level of the DPS hierarchy. The number of measurements used to generate $\{S^k_{a|x}\}_{a,x}$ is denoted by n_x, the state was taken to be a maximally entangled state. For visibility values above the critical t_c depicted for the different analyses, one certifies that the number of Alice's measurements must be at least $k+1$.

implemented the first levels of the hierarchy using CVXPY [51], a freely accessible software. Particularly, we investigated noisy MUBs measured on a maximally entangled state, a setting well in reach of today's experimental techniques. Specifically, our results show that Bob can verify Alice's access to more than two measurements in presence of significant background noise. A potential bottleneck of our methods is that for a bigger number of measurements acting on multiple qubits the resulting SDP may be too large to be solved numerically; addressing this, symmetry-reduction techniques [52] and optimizing the SDP implementation and solver choice are suggested.

Our results extend to checking k-simulability of POVMs, establishing necessary conditions for k-simulability that can be cast as SDPs, filling a prior knowledge gap before this work. For future directions, we highlight finding conditions for k-simulability that are both necessary and sufficient, and can be efficiently checked numerically.

This work has broad implications in quantum information scenarios, as demonstrated by some examples: A main obstacle in applying device-independent quantum key distribution protocols [53,54] is low robustness to experimental noise. It is known that using higher-dimensional Bell inequalities and Bell inequalities with more than two inputs and outcomes [55–59] can improve the noise thresholds necessary for secure quantum key distribution. Our methods can be used by the parties to mutually certify that they have the necessary number of incompatible measurements to implement these protocols. Also, the results hint at the possibility of semi-device-independent cryptography based on more than two measurements, which may improve feasibility of experimental applications. Another potential use is attacking an unknown quantum device, where there is a discovery phase and the attacker aims to learn as much as possible about the target. Our results indicate that an attacker able to send entangled states to the device could bound the number of incompatible measurements it can perform. Furthermore, we envision that applications in randomness certification [38] hold promise for future developments. Finally, there are potential applications within the prepare-and-measure scenario, notably the receiver-device-independent quantum key distribution protocol [60,61].

ACKNOWLEDGMENTS

I.V. acknowledges the financial support of National Council for Scientific and Technological Development, CNPq Brazil, and thanks C. de Gois and T.-A. Ohst for discussions. M.P. acknowledges support from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, Projects No. 447948357 and No. 440958198), the Sino-German Center for Research Promotion (Project No. M-0294), the ERC (Consolidator Grant No. 683107/TempoQ), the German Ministry of Education and Research (Project QuKuK, BMBF Grant No. 16KIS1618K), and the Alexander von Humboldt Foundation. L.L. acknowledges support from the European Union's Horizon 2020 Research and Innovation Programme under the Programme SASPRO 2 COFUND Marie Sklodowska-Curie Grant Agreement No. 945478 as well as from projects APVV-22-0570 (DeQHOST) and VEGA 2/0183/21 (DESCOM). R.U. is thankful for the financial support from the Swiss National Science Foundation (Ambizione Grant No. PZ00P2-202179).

APPENDIX: SUFFICIENT CONDITIONS FOR 2-SIMULABILITY BASED ON 2-COMPATIBILITY

We make the following simple observation: Consider a set of k-compatible measurements $\{M_{a|x}\}_{a,x}$ with a k-copy joint observable G_λ so that

$$\mathrm{tr}[\rho M_{a|x}] = \sum_\lambda p(a|x,\lambda)\mathrm{tr}[\rho^{\otimes k} G_\lambda] \tag{A1}$$

for all states ρ for some conditional probability distributions p. Suppose now that the POVM $\{G_\lambda\}_\lambda$ is a mixture of k POVMs $\{\mathbb{1}^{\otimes y-1}\otimes B_{\lambda|y}\otimes \mathbb{1}^{\otimes k-y}\}_{\lambda,y}$, where $y\in\{1,\ldots,k\}$ and $\{B_{\lambda|y}\}_{b,y}$ are some k POVMs. Thus, there exists a probability distribution q such that

$$G_\lambda = \sum_{y=1}^{k} q(y)\left(\mathbb{1}^{\otimes y-1}\otimes B_{\lambda|y}\otimes \mathbb{1}^{\otimes k-y}\right). \tag{A2}$$

Now we see that the original measurements $\{M_{a|x}\}_{a,x}$ are in fact k-simulable:

$$\begin{aligned}\mathrm{tr}[\rho M_{a|x}] &= \sum_\lambda p(a|x,\lambda)\mathrm{tr}[\rho^{\otimes k} G_\lambda] \\ &= \mathrm{tr}\left[\rho\left(\sum_{y=1}^{k} q(y)\sum_\lambda p(a|x,\lambda)B_{\lambda|y}\right)\right].\end{aligned} \tag{A3}$$

Consider now a set of 2-compatible measurements $\{M_{a|x}\}_{a,x}$ with a joint observable G_λ. Let us take any two different states ρ_1 and ρ_2 and consider their mixture $\rho = \mu\rho_1 + (1-\mu)\rho_2$ by some weight $\mu\in(0,1)$. By the linearity of the trace we naturally have that $\mathrm{tr}[\rho M_{a|x}] = \mu\,\mathrm{tr}[\rho_1 M_{a|x}] + (1-\mu)\mathrm{tr}[\rho_2 M_{a|x}]$ and by using Eq. (A1) for $k=2$ one can

easily rephrase the condition as

$$\sum_{\lambda} p(a|x,\lambda)\mathrm{tr}[(\rho_1-\rho_2)^{\otimes 2}G_\lambda]=0. \tag{A4}$$

Since this must hold for any two states ρ_1 and ρ_2, we must have that for all a,x,λ such that $p(a|x,\lambda)\neq 0$ we have that $G_\lambda=\tilde{B}_{\lambda|1}\otimes\mathbb{1}_B+\mathbb{1}_A\otimes\tilde{B}_{\lambda|2}+W_\lambda$ for some operators $\tilde{B}_{\lambda|1},\tilde{B}_{\lambda|2},W_\lambda$ such that in particular $\mathrm{tr}[(\rho_1-\rho_2)^{\otimes 2}W_\lambda]=0$. In the case when $W_\lambda=0$ and the operators $\tilde{B}_{\lambda|1}$ and $\tilde{B}_{\lambda|2}$ are self-adjoint we can show that the observation described above applies.

Proposition 1. Let $\{M_{a|x}\}_{a,x}$ be a set of 2-compatible POVMs with a 2-copy joint POMV G. If $G_\lambda\in\mathrm{span}(\{B_1\otimes\mathbb{1}_B+\mathbb{1}_A\otimes B_2 : B_1\in\mathcal{L}(\mathcal{H}_A), B_2\in\mathcal{L}(\mathcal{H}_B), B_1,B_2 \text{ are self-adjoint}\})$ for all λ, then $\{M_{a|x}\}_{a,x}$ are 2-simulable.

Proof. Since G is a 2-copy joint POVM for $\{M_{a|x}\}_{a,x}$, there exists a conditional probability distribution p such that $\mathrm{tr}[\rho M_{a|x}]=\sum_\lambda p(a|x,\lambda)\mathrm{tr}[\rho^{\otimes 2}G_\lambda]$ for all a,x. If now $G\in\mathrm{span}(\{B_1\otimes\mathbb{1}_B+\mathbb{1}_A\otimes B_2 : B_1\in\mathcal{L}(\mathcal{H}_A), B_2\in\mathcal{L}(\mathcal{H}_B), B_1,B_2 \text{ are self-adjoint}\})$, then there exists some self-adjoint $\tilde{A}_\lambda\in\mathcal{L}(\mathcal{H}_A),\tilde{B}_\lambda\in\mathcal{L}(\mathcal{H}_B)$ such that $G_\lambda=\tilde{A}_\lambda\otimes\mathbb{1}_B+\mathbb{1}_A\otimes\tilde{B}_\lambda$. We see that in fact we can choose another decomposition $G_\lambda=A_\lambda\otimes\mathbb{1}_B+\mathbb{1}_A\otimes B_\lambda$ such that A_λ and B_λ are positive semidefinite: Namely, let us consider the spectral decompositions $\tilde{A}_\lambda=\sum_i\nu_\lambda^{(i)}|\phi_\lambda^{(i)}\rangle\langle\phi_\lambda^{(i)}|$ and $\tilde{B}_\lambda=\sum_j\mu_\lambda^{(j)}|\psi_\lambda^{(j)}\rangle\langle\psi_\lambda^{(j)}|$ for some real numbers $\nu_\lambda^{(i)},\mu_\lambda^{(j)}$ and some orthonormal bases $\{\phi_\lambda^{(i)}\}_i$ and $\{\psi_\lambda^{(j)}\}_j$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then we clearly have that

$$\begin{aligned}G_\lambda&=\tilde{A}_\lambda\otimes\mathbb{1}_B+\mathbb{1}_A\otimes\tilde{B}_\lambda\\&=\sum_{i,j}\left(\nu_\lambda^{(i)}+\mu_\lambda^{(j)}\right)|\phi_\lambda^{(i)}\rangle|\psi_\lambda^{(j)}\rangle\langle\psi_\lambda^{(j)}|\langle\phi_\lambda^{(i)}|.\end{aligned} \tag{A5}$$

The above equation defines a spectral decomposition for G_λ so that from the positive semidefiniteness of G_λ it follows that $\nu_\lambda^{(i)}+\mu_\lambda^{(j)}\geqslant 0$ for all i,j,λ. Thus, in particular we must have that either $\tilde{A}_\lambda$ or $\tilde{B}_\lambda$ or both of them are positive semidefinite for all λ. Without loss of generality, we assume that $\tilde{A}_\lambda\geqslant 0$ so that $\nu_\lambda^{(i)}\geqslant 0$ for all i,λ. By denoting $\nu_\lambda^{\min}:=\min_i\nu_\lambda^{(i)}$ and defining $A_\lambda:=\tilde{A}_\lambda-\nu_\lambda^{\min}\mathbb{1}_A$ we see that also $A_\lambda\geqslant 0$. Now we see that

$$\begin{aligned}G_\lambda&=\tilde{A}_\lambda\otimes\mathbb{1}_B+\mathbb{1}_A\otimes\tilde{B}_\lambda=A_\lambda\otimes\mathbb{1}_B+\nu_\lambda^{\min}\mathbb{1}_A\otimes\mathbb{1}_B+\mathbb{1}_A\\&\otimes\tilde{B}_\lambda=A_\lambda\otimes\mathbb{1}_B+\mathbb{1}_A\otimes\left(\nu_\lambda^{\min}\mathbb{1}_B+\tilde{B}_\lambda\right)\end{aligned}$$

so that by denoting $B_\lambda:=\nu_\lambda^{\min}\mathbb{1}_B+\tilde{B}_\lambda$ we must have that B_λ is positive semidefinite because $\nu_\lambda^{\min}+\mu_\lambda^{(j)}\geqslant 0$ for all j.

By taking the partial traces separately with respect to $\mathcal{H}_A$ and $\mathcal{H}_B$ from the normalization condition $\sum_\lambda G_\lambda=\mathbb{1}_A\otimes\mathbb{1}_B$ we see now that

$$\sum_\lambda A_\lambda=\left(1-\frac{\sum_\lambda\mathrm{tr}[B_\lambda]}{d_B}\right)\mathbb{1}_A, \tag{A6}$$

$$\sum_\lambda B_\lambda=\left(1-\frac{\sum_\lambda\mathrm{tr}[A_\lambda]}{d_A}\right)\mathbb{1}_B\,. \tag{A7}$$

Since A_λ and B_λ are positive semidefinite, we must have that $q:=(1-\frac{\sum_\lambda\mathrm{tr}[B_\lambda]}{d_B})\geqslant 0$ and $q':=(1-\frac{\sum_\lambda\mathrm{tr}[A_\lambda]}{d_A})\geqslant 0$, and from the normalization of G it also follows that $q'=1-q$. By denoting $C_\lambda:=\frac{1}{q}A_\lambda$ and $D_\lambda:=\frac{1}{1-q}B_\lambda$ whenever $q,1-q\neq 0$ and $C_\lambda:=0=:D_\lambda$ otherwise, we have that $\{C_\lambda\}_\lambda$ and $\{D_\lambda\}_\lambda$ are in fact two POVMs such that

$$G_\lambda=qC_\lambda\otimes\mathbb{1}_B+(1-q)\mathbb{1}_A\otimes D_\lambda \tag{A8}$$

for all λ. Now we see that we are in the case described by the observation in the beginning of this section so that $\{M_{a|x}\}_{a,x}$ are 2-simulable. ■

We note that both the 2-compatibility and the previously described condition for the 2-copy joint POVM can be checked by using SDPs.

[1] T. Heinosaari, T. Miyadera, and M. Ziman, J. Phys. A: Math. Theor. **49**, 123001 (2016).

[2] O. Gühne, E. Haapasalo, T. Kraft, J.-P. Pellonpää, and R. Uola, Rev. Mod. Phys. **95**, 011003 (2023).

[3] A. Tavakoli, A. Pozas-Kerstjens, M.-X. Luo, and M.-O. Renou, Rep. Prog. Phys. **85**, 056001 (2022).

[4] M.-O. Renou, D. Trillo, M. Weilenmann, T. P. Le, A. Tavakoli, N. Gisin, A. Acín, and M. Navascués, Nature (London) **600**, 625 (2021).

[5] N. Gisin, Entropy **21**, 325 (2019).

[6] J. Czartowski, D. Goyeneche, M. Grassl, and K. Życzkowski, Phys. Rev. Lett. **124**, 090503 (2020).

[7] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Commun. Math. Phys. **328**, 303 (2014).

[8] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, Quantum **1**, 3 (2017).

[9] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Phys. Rev. Lett. **119**, 190501 (2017).

[10] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Phys. Rev. Lett. **117**, 260401 (2016).

[11] L. Guerini, J. Bavaresco, M. Terra Cunha, and A. Acín, J. Math. Phys. **58**, 092102 (2017).

[12] W. Shi and C. Tang, Quantum Inf. Proc. **19**, 393 (2020).

[13] S. Designolle, V. Srivastav, R. Uola, N. H. Valencia, W. McCutcheon, M. Malik, and N. Brunner, Phys. Rev. Lett. **126**, 200404 (2021).

[14] C. Carmeli, T. Heinosaari, D. Reitzner, J. Schultz, and A. Toigo, Mathematics **4**, 54 (2016).

[15] M. M. Wolf, D. Perez-Garcia, and C. Fernandez, Phys. Rev. Lett. **103**, 230402 (2009).

[16] M. T. Quintino, T. Vértesi, and N. Brunner, Phys. Rev. Lett. **113**, 160402 (2014).

[17] R. Uola, T. Moroder, and O. Gühne, Phys. Rev. Lett. **113**, 160403 (2014).

[18] A. Tavakoli and R. Uola, Phys. Rev. Res. **2**, 013011 (2020).

[19] C. Vieira, C. de Gois, L. Pollyceno, and R. Rabelo, New J. Phys. **25**, 113004 (2023).

[20] D. Saha, D. Das, A. K. Das, B. Bhattacharya, and A. S. Majumdar, Phys. Rev. A **107**, 062210 (2023).

[21] C. Carmeli, T. Heinosaari, and A. Toigo, Phys. Rev. Lett. **122**, 130402 (2019).

[22] P. Skrzypczyk, I. Šupić, and D. Cavalcanti, Phys. Rev. Lett. **122**, 130403 (2019).
[23] R. Uola, T. Kraft, J. Shang, X.-D. Yu, and O. Gühne, Phys. Rev. Lett. **122**, 130404 (2019).
[24] R. Uola, G. Vitagliano, and C. Budroni, Phys. Rev. A **100**, 042117 (2019).
[25] M. Oszmaniec and T. Biswas, Quantum **3**, 133 (2019).
[26] R. Uola, T. Bullock, T. Kraft, J.-P. Pellonpää, and N. Brunner, Phys. Rev. Lett. **125**, 110402 (2020).
[27] F. Buscemi, E. Chitambar, and W. Zhou, Phys. Rev. Lett. **124**, 120401 (2020).
[28] R. Uola, E. Haapasalo, J.-P. Pellonpää, and T. Kuusela, arXiv:2212.02815.
[29] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A **81**, 022101 (2010).
[30] M. K. Olsen, Phys. Rev. A **88**, 051802(R) (2013).
[31] J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 200402 (2014).
[32] D. A. Evans and H. M. Wiseman, Phys. Rev. A **90**, 012114 (2014).
[33] P. Skrzypczyk, M. Navascués, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).
[34] J. Bowles, F. Hirsch, M. T. Quintino, and N. Brunner, Phys. Rev. A **93**, 022121 (2016).
[35] P. Sekatski, F. Giraud, R. Uola, and N. Brunner, arXiv:2304.03888.
[36] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
[37] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, J. Phys. A: Math. Theor. **47**, 424028 (2014).
[38] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, New J. Phys. **17**, 113010 (2015).
[39] P. Skrzypczyk and D. Cavalcanti, Phys. Rev. Lett. **120**, 260401 (2018).
[40] Y. Xiang, I. Kogias, G. Adesso, and Q. He, Phys. Rev. A **95**, 010101(R) (2017).
[41] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).
[42] D. Cavalcanti and P. Skrzypczyk, Rep. Prog. Phys. **80**, 024001 (2017).
[43] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Rev. Mod. Phys. **92**, 015001 (2020).
[44] S.-L. Chen, C. Budroni, Y.-C. Liang, and Y.-N. Chen, Phys. Rev. Lett. **116**, 240401 (2016).
[45] D. Cavalcanti and P. Skrzypczyk, Phys. Rev. A **93**, 052112 (2016).
[46] T. Heinosaari, D. Reitzner, and P. Stano, Found. Phys. **38**, 1133 (2008).
[47] R. Uola, C. Budroni, O. Gühne, and J.-P. Pellonpää, Phys. Rev. Lett. **115**, 230402 (2015).
[48] S. N. Filippov, T. Heinosaari, and L. Leppäjärvi, Phys. Rev. A **97**, 062102 (2018).
[49] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[50] G. Aubrun, A. Müller-Hermes, and M. Plávala, arXiv:2206.11805.
[51] S. Diamond and S. Boyd, J. Machine Learn. Res. **17**, 1 (2016).
[52] H. C. Nguyen, S. Designolle, M. Barakat, and O. Gühne, arXiv:2003.12553.
[53] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E.-Z. Tan *et al.*, Nature (London) **607**, 682 (2022).
[54] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim *et al.*, Nature (London) **607**, 687 (2022).
[55] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, npj Quantum Inf. **9**, 10 (2023).
[56] N. Miklin, A. Chaturvedi, M. Bourennane, M. Pawłowski, and A. Cabello, Phys. Rev. Lett. **129**, 230403 (2022).
[57] Z.-P. Xu, J. Steinberg, J. Singh, A. J. López-Tarrida, J. R. Portillo, and A. Cabello, Quantum **7**, 922 (2023).
[58] P. Brown, H. Fawzi, and O. Fawzi, Nat. Commun. **12**, 575 (2021).
[59] J. R. Gonzales-Ureta, A. Predojević, and A. Cabello, Phys. Rev. A **103**, 052436 (2021).
[60] M. Ioannou, M. A. Pereira, D. Rusca, F. Grünenfelder, A. Boaron, M. Perrenoud, A. A. Abbott, P. Sekatski, J.-D. Bancal, N. Maring, H. Zbinden, and N. Brunner, Quantum **6**, 718 (2022).
[61] M. Ioannou, P. Sekatski, A. A. Abbott, D. Rosset, J.-D. Bancal, and N. Brunner, New J. Phys. **24**, 063006 (2022).