Semi-device-independent characterization of quantum measurements under a minimum overlap assumption

Weixu Shi,[1,2] Yu Cai,[2,*] Jonatan Bohr Brask,[3] Hugo Zbinden,[2] and Nicolas Brunner[2]
[1]*Department of Electronic Science, National University of Defense Technology, 410073 Changsha, China*
[2]*Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*
[3]*Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark*

(Received 15 April 2019; published 10 October 2019)

Recently, a novel framework for semi-device-independent quantum prepare-and-measure protocols has been proposed, based on the assumption of a limited distinguishability between the prepared quantum states. Here, we discuss the problem of characterizing an unknown quantum measurement device in this setting. We present several methods to attack the problem. Considering the simplest scenario of two preparations with lower bounded overlap, we show that genuine three-outcome positive-operator valued measures (POVMs) can be certified, even in the presence of noise. Moreover, we show that the optimal POVM for performing unambiguous state discrimination can be self-tested.

DOI: 10.1103/PhysRevA.100.042108

I. INTRODUCTION

The problem of certifying and characterizing quantum systems is a central problem of quantum information science, in particular towards the development of future quantum technologies. It is desirable to develop certification methods that are highly robust to noise and technical imperfections.

The device-independent (DI) approach [1–4] is of strong interest in this context (see, e.g., Refs. [5,6] for recent reviews). The main feature here is that a quantum system (or device) can be certified with minimal assumptions, without the requirement of using previously calibrated devices. In the fully DI approach, the observation of certain measurement statistics can certify a general property of a quantum system (for instance, that a source produces a quantum state that is entangled) and even completely characterize the system, i.e., identify precisely which entangled state is produced. The latter is referred to as "self-testing" (see, e.g., Refs. [7–11]).

While the fully DI approach is conceptually very elegant and provides the strongest possible form of certification for a quantum system, it is challenging to implement in practice. The main difficulty is that fully DI certification methods require a loophole-free Bell inequality violation. This motivated the development of partially DI methods that can be implemented in simple prepare-and-measure type experiments, which do not involve entanglement. The price to pay for this simplification is that an additional assumption on the system is required. First works in this direction used an assumption on the Hilbert space dimension of the quantum states being prepared [12–15]. Self-testing methods have been developed for this setting [16], for characterizing quantum states and measurements [17–22], and for implementing quantum information protocols [23–27]. In practice, however, the assumption of bounded dimension is not straightforward to justify, as dimension is not a directly measurable quantity. One typically needs to assume that the experimental setup is free of extra side-channels. As this is delicate in practice, one would ideally find other solutions allowing one to discard this assumption.

This motivates the study of different approaches to the semi-DI setting, using different types of assumptions. Three promising approaches have been recently put forward. First, Chaves *et al.* [28] suggested to upper bound the entropy of the quantum message (i.e., the set of prepared quantum states). Then, Himbeeck *et al.* [29] proposed an upper bound on the energy of quantum states. Finally, Brask *et al.* [30] assumed a lower bound on the overlap between the prepared quantum states. Moreover, Wang *et al.* [31] has developed a toolbox to characterize the quantum correlation in the prepare-and-measure scenario under the assumption of overlaps of the quantum states. Clearly, the common feature of all these approaches is placing a bound on how distinguishable the quantum states are from each other. In practice these approaches open new perspectives. Indeed, the energy of an optical source can in principle be directly measured, which provides a good justification for an upper bound on the energy or a lower bound on the overlap (using, say, the vacuum and weak coherent states). This approach recently led to promising randomness generation protocols [30,32], combining semi-DI security, high rates, and ease of implementation.

Here we explore further the potential of this new approach to the semi-DI setting. In particular, we consider the problem of characterizing an unknown quantum measurement device in a simple prepare-and-measure scenario, which features only two possible preparations and a fixed ternary measurement. We use the assumption of a lower bound on the indistinguishability between the two prepared quantum states, which we formalize for mixed states in terms of lower bounds on the fidelity. This allows us to certify certain properties of the positive-operator valued measure (POVM)

*caiyu01@gmail.com

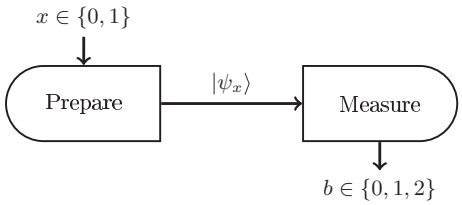

FIG. 1. Schematic representation of the scenario considered.

that is implemented inside the measurement device. In particular, we show that the observation of certain correlations certifies that the measurement is a genuine three-outcome POVM. In order to do so, we develop methods to characterize the set of correlations achievable with binary POVMs and classical postprocessing. Moreover, we show that a particular genuine three-outcome POVM, which allows for unambiguous state discrimination [33–35], can be self-tested. Finally, we discuss the robustness to noise of these methods.

II. DEFINING THE PROBLEM

We consider the prepare-and-measure setup sketched in Fig. 1. The preparation device takes a binary input, $x \in \{0, 1\}$, and the measurement box performs a fixed measurement (hence no input) resulting in a ternary output, $b \in \{0, 1, 2\}$. Upon receiving x, the preparation device sends a quantum system in an unknown state, ρ_x, to the measurement device, which performs an unknown POVM on the system. The POVM elements associated with each outcome are noted M_b. This results in the following statistics:

$$p(b|x) = \mathrm{Tr}[\rho_x M_b], \tag{1}$$

the set of which, $\boldsymbol{p} := \{p(b|x)\}$, is called a *behavior*.

Our goal is to characterize the unknown POVM that is implemented inside the measurement device. This characterization is semi-DI, in the sense that it is based only on the observed behavior, under two assumptions. First, the choice of the input x is independent from the boxes. All the information that the measurement device receives about x comes from the received quantum state ρ_x. Hence, in order to make nontrivial statements, we need to limit the amount of information about x that can be retrieved from the states ρ_x. This leads to our second assumption, namely, a lower bound on the indistinguishability of the two quantum states. Here we use the fidelity [36–38] as a measure of indistinguishability between ρ_0 and ρ_1. Our assumption reads

$$F(\rho_0, \rho_1) = \mathrm{Tr}\sqrt{\rho_0^{1/2}\rho_1\rho_0^{1/2}} \geqslant \delta. \tag{2}$$

For the case of two pure states, we have simply that $F = |\langle\psi_0|\psi_1\rangle| \geqslant \delta$. Note also that when the two states are identical, then $F(\rho_0, \rho_1) = 1$. In the following, without loss of generality, we restrict our analysis to the case of two pure states. This is because the set of behaviors that is achievable under the above assumption (2) can always be reproduced by using two pure states with the same overlap. To see this, suppose a behavior is produced by two mixed states with $F(\rho_0, \rho_1) = \delta$. According to Uhlmann's theorem, there exists a pair of purifications of ρ_0 and ρ_1, denoted by $|\phi_0\rangle$ and $|\phi_1\rangle$, respectively, such that their overlap satisfies $|\langle\phi_0|\phi_1\rangle| = \delta$. Then $p(b|x) = \mathrm{Tr}(\rho_x M_b) = \mathrm{Tr}(\mathrm{Tr}_R(|\phi_x\rangle\langle\phi_x|)M_b) = \mathrm{Tr}(|\phi_x\rangle\langle\phi_x|M_b \otimes \mathbb{I}_R)$, where $\rho_x = \mathrm{Tr}_R(|\phi_x\rangle\langle\phi_x|)$ and R is the ancillary system.

Let us discuss the parametrization of the two pure quantum states. Without loss of generality, we can represent these states in an effective qubit space spanned by the states $|0\rangle$ and $|1\rangle$. Note that we make no assumption on the Hilbert space dimension, but simply use the fact that we can set the reference frame at our convenience. Specifically, we write

$$\begin{aligned} |\psi_0\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |\psi_1\rangle &= \cos\theta|0\rangle - \sin\theta|1\rangle, \end{aligned} \tag{3}$$

with $\delta = \cos 2\theta$ and $0 \leqslant \theta \leqslant \pi/4$, so that the overlap $\langle\psi_0|\psi_1\rangle$ is positive and real. Note that since all the behaviors achievable via pairs of quantum states with a larger overlap are included in the behaviors with a smaller overlap (see Appendix 2 of Ref. [30]), we can take the overlap of the two states to be δ when characterizing the boundary of the sets of behaviors for an overlap larger than or equal to δ.

With the overlap assumption, the first property of the measurement box to be certified is that it performs a *genuine* three-outcome POVM, i.e., a measurement that cannot be decomposed into a convex combination of two-outcome POVMs. Mathematically, if for all b, we can write

$$M_b = \sum_j p_j M_b^j, \tag{4}$$

where each $\{M_b^j\}_{b=0,1,2}$ is a valid POVM with $M_j^j = 0$, and $\{p_j\}_{j=0,1,2}$ is a valid probability distribution, then we say that $\{M_b\}$ is *not* a genuine three-outcome POVM. Physically speaking, this means such an $\{M_b\}$ could be effectively carried out by applying only two-outcome POVMs and classical postprocessing.

Let $\mathcal{P}_3(\delta)$ denote the set of behaviors achievable by three-outcome POVMs for a fixed overlap δ (or larger), and let $\mathcal{P}_2(\delta)$ denote the one achievable by a convex combination of two-outcome POVMs. We should have $\mathcal{P}_2(\delta) \subsetneq \mathcal{P}_3(\delta)$ for any $\delta > 0$, since we know that two-outcome POVMs are special cases of three-outcome POVMs. Moreover it has been shown that, in the regime δ close to 1, behaviors in $\mathcal{P}_3(\delta)$ can certify more randomness than $\mathcal{P}_2(\delta)$ [39]. For completeness, we also introduce another set of behaviors, called the trivial set $\mathcal{P}_t$. Here the input state is ignored (so δ is omitted) and the output is generated at random according to some distribution. Such implementations are called trivial POVMs in the following. Note that this set is different from the set of classical behaviors in Ref. [29]. Mathematically, $\boldsymbol{p} \in \mathcal{P}_t$ implies $p(b|0) = p(b|1)$ for all b. One should note that $\mathcal{P}_3(\delta)$, $\mathcal{P}_2(\delta)$, and $\mathcal{P}_t$ are convex, upon which our arguments are based.

Finally, note that the problem of certifying genuine four-outcome POVMs is not discussed here. While there exist extremal qubit POVM featuring four outcomes, these can never be distinguished from three-outcome POVMs in the present scenario. This is because we can restrict our analysis to POVMs for which all the elements are in a plane of the Bloch sphere [spanned by the two states (3)]. In this case, extremal POVMs feature only three outcomes [39], hence

any behavior can be reproduced via three-outcome POVMs and classical postprocessing. The certification of a genuine four-outcome POVM would require a scenario with three preparations with limited distinguishability, a problem which we leave for future research.

III. RESULTS

In this section, we present different methods for characterizing the sets of behaviors $\mathcal{P}_3(\delta)$, $\mathcal{P}_2(\delta)$, and $\mathcal{P}_t$. First, we show that the problem of determining whether a certain behavior belongs to $\mathcal{P}_2(\delta)$ can be cast as a semidefinite program (SDP). Then we determine the boundary of the various sets for a specific class of behaviors. Finally, we show that various properties of the POVM for performing unambiguous state discrimination (USD) can be certified, in particular that the POVM can be self-tested.

A. Semidefinite programs

Here we show that deciding if a behavior belongs to $\mathcal{P}_2(\delta)$, or whether it must feature a genuine three-outcome POVM, can be cast as an SDP. Let $\boldsymbol{p}$ be the behavior of interest and $\boldsymbol{p}_0$ be arbitrary behavior in $\mathcal{P}_2$. For example, $\boldsymbol{p}_0 = \boldsymbol{p}_{\mathbb{I}} = \{p(b|x) = 1/3\}$. Clearly $\boldsymbol{p}_{\mathbb{I}} \in \mathcal{P}_t$, thus $\boldsymbol{p}_{\mathbb{I}} \in \mathcal{P}_2(\delta)$. Consider the linear combination of these two behaviors, $\boldsymbol{p}' = \omega\boldsymbol{p} + (1-\omega)\boldsymbol{p}_0$, with $\omega > 0$. Let ω^* denote the maximal ω for which $\boldsymbol{p}' \in \mathcal{P}_2(\delta)$. The quantity ω^* tells us how far a behavior can go along the direction from $\boldsymbol{p}_0$ to $\boldsymbol{p}$ while staying in $\mathcal{P}_2(\delta)$. If $\omega^* \geqslant 1$, it means $\boldsymbol{p} \in \mathcal{P}_2(\delta)$, otherwise $\boldsymbol{p} \notin \mathcal{P}_2(\delta)$.

From Eq. (4), we see that the probability to use the jth strategy can be absorbed into the POVM elements, i.e., $\tilde{M}_b^j = p_j M_b^j$. Then computing ω^* can be written as the following optimization problem with linear constraints:

$$
\begin{aligned}
\underset{\tilde{M}_b^j}{\text{maximize}} \quad & \omega \\
\text{subject to} \quad & \tilde{M}_b^j \succeq 0, \ \forall j, b, \\
& \sum_b \tilde{M}_b^j = \frac{1}{2}\mathrm{Tr}\left[\sum_b \tilde{M}_b^j\right]\mathbb{I}, \ \forall j, \\
& \sum_j \frac{1}{2}\mathrm{Tr}\left[\sum_b \tilde{M}_b^j\right] = 1, \\
& \tilde{M}_j^j = 0, \ \forall j, \\
& \omega p(b|x) + (1-\omega)p_0(b|x) \\
& \qquad = \mathrm{Tr}\left[|\psi_x\rangle\langle\psi_x| \sum_j \tilde{M}_b^j\right], \quad \forall x, b,
\end{aligned}
\tag{5}
$$

The first two constraints stem from the positivity and normalization of M_b^j, and the next two constraints guarantee the convex combination of two-outcome POVMs. The last constraint enforces the reproduction of the behavior.

One way to write the dual problem of the SDP above is the following:

$$
\begin{aligned}
\underset{H^j, J^j, v_{b|x}}{\text{maximize}} \quad & \eta = \boldsymbol{v}\cdot(\boldsymbol{p} - \boldsymbol{p}_0) \\
\text{subject to} \quad & H^j = (H^j)^\dagger, \ J^j = (J^j)^\dagger, \\
& \frac{1}{2}\mathbb{I} + H^j - \frac{1}{2}\mathrm{Tr}\big[H^j\big]\mathbb{I} + \frac{1}{2}\sum_{xb'} v_{b'|x} p_0(b'|x)\mathbb{I} \\
& \qquad - \sum_x v_{b|x}|\psi_x\rangle\langle\psi_x| + \delta_{b,j} J^j \succeq 0 \quad \forall j, b
\end{aligned}
\tag{6}
$$

where $\boldsymbol{v} \in \mathbb{R}^6$, and "$\cdot$" denotes the scalar product. The details of deriving the dual problem from the primal are given in Appendix A. Any feasible solution to the dual problem gives an upper bound on ω^* ($\omega^* \leqslant \frac{1}{\eta}$). Let η^* denote the maximal η. Any feasible point $\{H^j, J^j, \boldsymbol{v}\}$ which gives $\eta^* > 1$ provides a witness for genuine three-outcome POVMs, since this feasibility does not depend on $\boldsymbol{p}$. For such a feasible point, for any behavior $\boldsymbol{q}$ that violates the inequality

$$\boldsymbol{v}\cdot(\boldsymbol{q} - \boldsymbol{p}_0) \leqslant 1,$$

we have $\boldsymbol{q} \notin \mathcal{P}_2(\delta)$. These SDP methods are used in the next section in specific examples.

B. Analytical characterization of boundary

Another approach to distinguishing $\mathcal{P}_2(\delta)$ and $\mathcal{P}_3(\delta)$ is to characterize their respective boundaries. Even though determining the boundary of quantum correlation in general is challenging, we are able to characterize them for a specific class of behaviors.

For convenience, we write the vector $\boldsymbol{p}$ of a given behavior in the form

$$\begin{pmatrix} p(0|0) & p(1|0) & p(2|0) \\ p(0|1) & p(1|1) & p(2|1) \end{pmatrix}. \tag{7}$$

We defined $\mathcal{P}_{\mathrm{sym}}(\delta)$ to be the subset of behaviors in $\mathcal{P}_3(\delta)$ that are invariant to the input-output relabeling

$$\Pi : \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \mapsto \begin{pmatrix} e & d & f \\ b & a & c \end{pmatrix}.$$

Notice that the behaviors in $\mathcal{P}_{\mathrm{sym}}(\delta)$ have the form

$$
\begin{aligned}
\boldsymbol{p}(X,Y) = & X\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + Y\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
& + (1-X-Y)\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
\tag{8}
$$

From this we can see $\mathcal{P}_{\mathrm{sym}}(\delta)$ is in the slice S in $\mathbb{R}^6$. Hence the behaviors in $\mathcal{P}_{\mathrm{sym}}(\delta)$ can be parametrized by

$$X = \tfrac{1}{2}[p(0|0) + p(1|1)]$$

and

$$Y = \tfrac{1}{2}[p(0|1) + p(1|0)].$$

Now we introduce a map, T, from a general behavior to a behavior in S: $T(\boldsymbol{p}) = 1/2(\boldsymbol{p} + \Pi(\boldsymbol{p}))$. Apparently,

$T(\mathcal{P}_{\text{sym}}(\delta)) = \mathcal{P}_{\text{sym}}(\delta)$. Our interest lies in the difference of $T(\mathcal{P}_2(\delta))$ and $T(\mathcal{P}_3(\delta))$ in the slice S.

Notice that Π does not change the number of genuine measurement outcomes to reproduce a behavior because it is just relabeling the inputs and outputs. Hence, for any $\boldsymbol{p} \in \mathcal{P}_k(\delta)$, it follows that $\Pi(\boldsymbol{p}) \in \mathcal{P}_k(\delta)$. From the linearity of T and the convexity of $\mathcal{P}_k(\delta)$, we conclude that $T(\boldsymbol{p}) \in \mathcal{P}_k(\delta)$; namely, $\mathcal{P}_k(\delta)$ is closed under T.

To characterize $T(\mathcal{P}_2(\delta))$, we can focus on the extremal points of it because of the linearity of T and the convexity of $\mathcal{P}_2(\delta)$. The extremal points are yielded by projective two-outcome POVMs and trivial POVMs. First note that $\mathcal{P}_t = \mathcal{P}_3(\delta = 1) = \mathcal{P}_2(\delta = 1)$, and it constitutes the line segment connecting (0,0) and (1/2, 1/2). Moreover, $\mathcal{P}_3(\delta = 0) = \mathcal{P}_2(\delta = 0)$ corresponds to the full triangle with extremal points (0,0), (0,1), and (1,0). This is because for perfectly distinguishable states, any statistics can be produced by the measurements. As in Eq. (4), we have three two-outcome strategies, written as $\{0, K_1, \mathbb{I} - K_1\}$, $\{K_2, 0, \mathbb{I} - K_2\}$, and $\{K_3, \mathbb{I} - K_3, 0\}$, where K_i denotes one of the elements of the ith two-outcome measurement. For convenience, we consider projective two-outcome POVMs and trivial POVMs separately.

Strategies $\{0, K_1, \mathbb{I} - K_1\}$ and $\{K_2, 0, \mathbb{I} - K_2\}$ yield the same ellipse:

$$\frac{4(X + Y - 1/2)^2}{\delta^2} + \frac{4(X - Y)^2}{1 - \delta^2} = 1. \tag{9}$$

Strategy $\{K_3, \mathbb{I} - K_3, 0\}$ contributes to the line segment of $X + Y = 1$ between the points

$$\left(\frac{1 - \sqrt{1 - \delta^2}}{2}, \frac{1 + \sqrt{1 - \delta^2}}{2}\right) \tag{10}$$

and

$$\left(\frac{1 + \sqrt{1 - \delta^2}}{2}, \frac{1 - \sqrt{1 - \delta^2}}{2}\right). \tag{11}$$

The details to derive these are given in Appendix B.

Hence, $T(\mathcal{P}_2(\delta))$ is the convex hull of the points (0,0), Eq. (10), Eq. (11), and the ellipse (9). $T(\boldsymbol{p}) \notin T(\mathcal{P}_2(\delta))$ certifies a genuine three-outcome POVM. Note that this is a nonlinear witness, contrary to the witnesses derived from an SDP, which are linear (see Sec. III A).

To characterize $T(\mathcal{P}_3)$, we take advantage of the symmetry of the slice S. Since $\mathcal{P}_k(\delta)$ is closed under T, we have $T(\mathcal{P}_3(\delta)) = \mathcal{P}_{\text{sym}}(\delta)$. Hence we only need to look at the boundary of $\mathcal{P}_{\text{sym}}(\delta)$. To characterize the boundary of $\mathcal{P}_{\text{sym}}(\delta)$, again we only need to consider extremal three-outcome POVMs. An extremal three-outcome POVM, $\{M_0, M_1, M_2\}$, can be parametrized as

$$M_b = \lambda_b(\mathbb{I} + \boldsymbol{u}_b \cdot \boldsymbol{\sigma}), \tag{12}$$

where $|\boldsymbol{u}_b| = 1$, $\sum_{b=0}^{2} \lambda_b = 1$, and $\sum_{b=0}^{2} \lambda_b \boldsymbol{u}_b = 0$. To meet the requirement of normalization, Bloch vectors $\{\boldsymbol{u}_i\}$ of the three-outcome measurement must lie in the same plane. Without loss of generality, we only consider the three-outcome POVMs that lie in the same plane as the two states (since they represent the effects of all possible measurements on the states). Using the SDP method discussed in Sec. III A, we found that to outline $T(\mathcal{P}_3)$, it is enough to consider extremal three-outcome POVMs that have a symmetry in the Bloch vectors as depicted in Fig. 2. Indeed, our analytical constructions based on this observation appear to match precisely the results of the SDP methods over three-outcome POVMs. We can thus characterize all extremal three-outcome POVMs that contribute to the $T(\mathcal{P}_3(\delta))$ only with one parameter. Here we choose the angle between the z axis and one of the two symmetrical Bloch vectors, $\phi \in [-\pi/2, \pi/2]$. Then we have two Bloch vectors, $\boldsymbol{u}_0 = (-\sin\phi, 0, -\cos\phi)$ and $\boldsymbol{u}_1 = (\sin\phi, 0, -\cos\phi)$. And we derive $\lambda_0 = \lambda_1 = 1/[2(1 + \cos\phi)]$. These symmetric three-outcome POVMs can be characterized via a single parameter, namely,

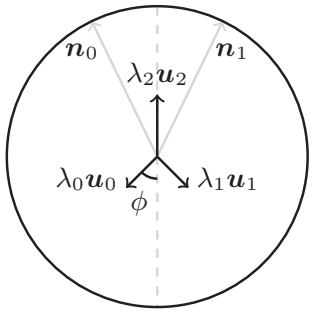

FIG. 2. Schematic representation of the three-outcome POVMs with symmetrical Bloch vectors. The first POVM element has a Bloch vector pointing in the z direction, i.e., intermediate between the Bloch vectors of the two quantum states (3). The other two POVM elements correspond to Bloch vectors distributed symmetrically along the z axis, in the x-z plane of the Bloch sphere.

$$M_0 = \frac{1}{2(1 + \cos\phi)}\begin{pmatrix} 1 - \cos\phi & \sin\phi \\ \sin\phi & 1 + \cos\phi \end{pmatrix},$$
$$M_1 = \frac{1}{2(1 + \cos\phi)}\begin{pmatrix} 1 - \cos\phi & -\sin\phi \\ -\sin\phi & 1 + \cos\phi \end{pmatrix},$$
$$M_2 = \frac{1}{(1 + \cos\phi)}\begin{pmatrix} 2\cos\phi & 0 \\ 0 & 0 \end{pmatrix}. \tag{13}$$

Combined with the states of Eq. (3), we get an equation of the boundary in a parametric form:

$$\begin{cases} X = [1 - \cos(\phi - 2\theta)]/2(1 + \cos\phi), \\ Y = [1 - \cos(\phi + 2\theta)]/2(1 + \cos\phi). \end{cases} \tag{14}$$

Finally, $T(\mathcal{P}_3)$ is the convex hull of the trivial point (0,0) and the curve in Eq. (14), as shown in Fig. 3(a). Figure 3(b) shows $T(\mathcal{P}_2(\delta))$ and $T(\mathcal{P}_3(\delta))$ with $\delta = 0$, 0.7, 0.9, and 1. It again states that the assumption we need to certify is whether it is a genuine three-outcome POVM or merely a lower bound of δ. As δ varies from 0 to 1, $T(\mathcal{P}_2(\delta))$ and $T(\mathcal{P}_3(\delta))$ gradually fills the convex hull of (0,0), (1,0), and (0,1).

Robustness against noise

Next we discuss the three-outcome POVMs that are most robust to white noise, in other words, how much noise we can add to the behavior before it can no longer certify a genuine three-outcome POVM. This can be investigated using the SDP method above.

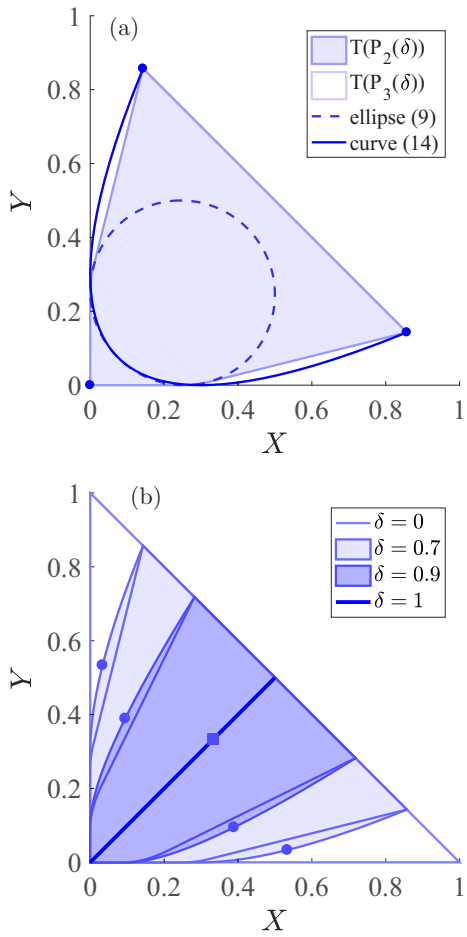

FIG. 3. (a) Geometrical representation of the sets of $T(\mathcal{P}_2(\delta))$ and $T(\mathcal{P}_3(\delta))$ in S at $\delta = 0.7$. (b) $T(\mathcal{P}_2(\delta))$ and $T(\mathcal{P}_3(\delta))$ of $\delta = 0$, 0.7, 0.9, and 1. The regions of smaller overlaps cover the regions of larger overlaps. The behaviors corresponding to the genuine three-outcome POVM that is most robust to noise (M_{rob}) in Sec. III B are marked out here using circles. The square represents the uniformly distributed behavior.

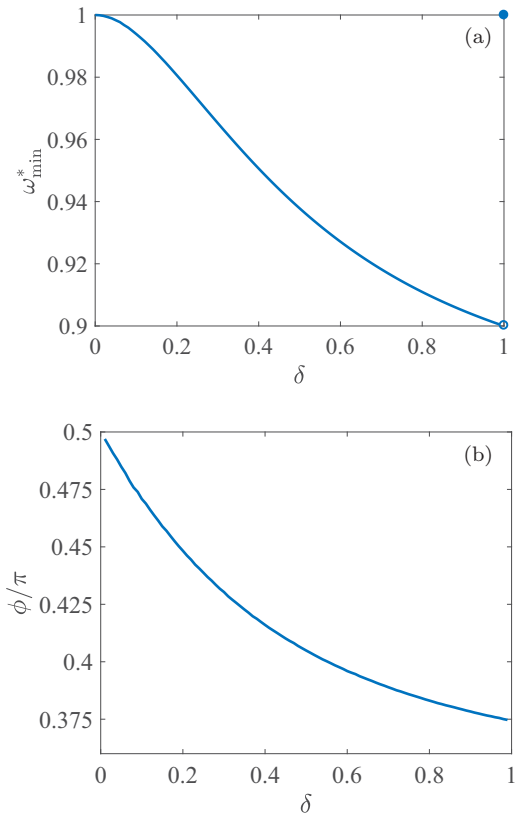

FIG. 4. (a) ω^*_{min}, which characterizes the robustness of the POVMs against white noise in certification, corresponding to different δ. ω^*_{min} cannot go lower than 0.9 no matter how close the quantum states are, which means that up to 10% of white noise can be tolerated. (b) ϕ, the only parameter to define a most robust symmetric extremal three-outcome POVM, as a function of δ.

Here we consider white noise added on the behavior. The robustness against white noise is then characterized by $1 - \omega^*$ when we take $\boldsymbol{p}_0 = \boldsymbol{p}_{\mathbb{I}}$. Through numerical optimization, we found that the larger the overlap between the quantum states is, the more noise the behavior can tolerate before it falls into $\mathcal{P}_2$. In Fig. 4(a), we show the minimal w^* as δ changes. Up to 10% of noise can be tolerated.

Interestingly, numerical results show that the most robust behavior, i.e., the behavior which gives ω^*_{min}, would be on the slice S. Hence the corresponding measurement has the symmetric form given in Eq. (13), as shown in Fig. 2. For given overlap δ, one can then find numerically the optimal value of ϕ, characterizing the most robust measurement [see Fig. 4(b)].

The optimal measurement for USD (in Sec. III C) can tolerate at most 4% of white noise for overlap $\delta = 0.46$. For other values of the overlap, the noise tolerance is weaker.

C. Unambiguous state discrimination

When two states have a nonzero overlap, one cannot perfectly distinguish them. However, if an inconclusive output is allowed in certain instances, this becomes possible via USD [33–35]. Given two states, ψ_0 and ψ_1, the family of POVMs $\{M_0, M_1, M_\varnothing\}$ that can accomplish the USD task must have $\text{Tr}(M_j|\psi_{\bar{j}}\rangle\langle\psi_{\bar{j}}|) = 0$ due to the unambiguity condition. M_0 and M_1 are the elements that correspond to the definite answers, and $M_\varnothing$ is the inconclusive result. The figure-of-merit in USD is the probability of producing a definite answer, i.e., $p_{\text{succ}} = [p(0|0) + p(1|1)]/2$. If $|\langle\psi_0|\psi_1\rangle| = \delta$ and the two states have equal occurrence probability, the maximal p_{succ} is $1 - \delta$ [33–35], denoted by $p_{\text{succ},3}$. This requires a genuine three-outcome POVM (which can be confirmed with the method in Sec. III B).

1. Certifying genuine three-outcome POVM

Intuitively, a high p_{succ} should certify a genuine three-outcome POVM. To show this, we upper bound p_{succ}, restricting ourselves to behaviors in $\mathcal{P}_2$. To achieve USD, the elements of the POVMs must be orthogonal to the states. To maximize p_{succ}, it is enough to consider extremal POVMs. Hence the relevant binary POVMs are of the following

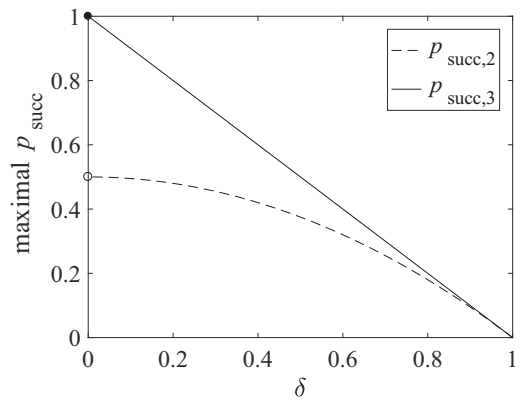

FIG. 5. Maximal USD success probability for different lower bounds on overlap. Note the hollow circle at lower bound 0. In the extreme case where the two input states are orthogonal, they can be perfectly distinguished with a two-outcome POVM as well. No two-outcome measurement can distinguish two states unambiguously with success probability larger than 1/2 when the two states are nonorthogonal ($\delta > 0$).

forms: $\{|\psi_1^\perp\rangle\langle\psi_1^\perp|, 0, \mathbb{I} - |\psi_1^\perp\rangle\langle\psi_1^\perp|\}$ and $\{0, |\psi_0^\perp\rangle\langle\psi_0^\perp|, \mathbb{I} - |\psi_0^\perp\rangle\langle\psi_0^\perp|\}$, where $|\psi_x^\perp\rangle$ is the orthogonal state of $|\psi_x\rangle$. Due to convexity, one can immediately find that for two-outcome POVMs the maximal p_{succ} is

$$p_{\text{succ},2} = \begin{cases} (1-\delta^2)/2, & 0 < \delta \leqslant 1, \\ 1, & \delta = 0. \end{cases} \tag{15}$$

Since $p_{\text{succ},3} > p_{\text{succ},2}$ (see Fig. 5) when $\delta \in (0, 1)$, p_{succ} can be used as a witness for genuine three-outcome POVMs. If the overlap of the states is lower bounded by δ, and p_{succ} exceeds Eq. (15), then it certifies a genuine three-outcome POVM.

Furthermore, one can certify genuine three-outcome POVMs in terms of p_{succ} in a way that is independent from the overlap. For two-outcome POVMs, when $\delta > 0$, $p_{\text{succ}} \leqslant 1/2$. Thus whenever $p_{\text{succ}} \geqslant 1/2$ is observed (and no error occurs), it can be inferred that the measurement box is a genuine three-outcome POVM.

2. *Self-testing*

A high success probability for USD not only certifies genuine three-outcome POVMs, it may even uniquely identify the states and measurement. In this section, we show that under the assumption of bounded overlap $\langle\psi_0|\psi_1\rangle \geqslant \delta$, having $p_{\text{succ}} = 1 - \delta$ *self-tests* two qubit states of overlap δ and the optimal USD measurement. To be precise, following Ref. [15], we say a behavior self-tests the measurement $\{\bar{M}_j\}$ in Hilbert space $\bar{\mathcal{H}}$ if for every quantum realization $(|\psi_0\rangle, |\psi_1\rangle, \{M_j\})$ in Hilbert space $\mathcal{H}$ compatible with the behavior there exists a completely positive and trace-preserving map $\Lambda : \mathcal{B}(\bar{\mathcal{H}}) \to \mathcal{B}(\mathcal{H})$, such that

$$\text{Tr}(M_j \Lambda(|\bar{\psi}\rangle\langle\bar{\psi}|)) = \text{Tr}(\bar{M}_j |\bar{\psi}\rangle\langle\bar{\psi}|) \tag{16}$$

is satisfied for any $|\bar{\psi}\rangle \in \bar{\mathcal{H}}$ and $j = 0, 1, \varnothing$.

In our case, $\bar{\mathcal{H}} = \mathbb{C}^2$, and the ideal states $|\bar{\psi}_x\rangle$ are given in Eq. (3), with overlap δ. For the input states, on the one hand we have $|\langle\psi_0|\psi_1\rangle| \geqslant \delta$ by assumption, and on the other hand $p_{\text{succ}} = 1 - \delta$ implies $|\langle\psi_0|\psi_1\rangle| \leqslant \delta$. Hence, $|\langle\psi_0|\psi_1\rangle| = \delta$.

For the measurements, it is sufficient to construct the map as $\Lambda(\cdot) = K(\cdot)K^\dagger$, where $K : \mathbb{C}^2 \to \mathcal{H}$,

$$\begin{aligned} |0\rangle &\to (|\psi_0\rangle + |\psi_1\rangle)/2c, \\ |1\rangle &\to (|\psi_0\rangle - |\psi_1\rangle)/2s, \end{aligned} \tag{17}$$

and the ideal measurement $\bar{M}$ is

$$\begin{aligned} \bar{M}_0 &= \frac{1}{1+\delta} |\bar{\psi}_1^\perp\rangle\langle\bar{\psi}_1^\perp|, \\ \bar{M}_1 &= \frac{1}{1+\delta} |\bar{\psi}_0^\perp\rangle\langle\bar{\psi}_0^\perp|, \\ \bar{M}_\varnothing &= \mathbb{I} - \bar{M}_0 - \bar{M}_1, \end{aligned} \tag{18}$$

where $|\bar{\psi}_1^\perp\rangle = (s|0\rangle + c|1\rangle)$, $|\bar{\psi}_0^\perp\rangle = (s|0\rangle - c|1\rangle)$. It remains to show that Eq. (16) is satisfied for any qubit states ρ.

Writing an arbitrary qubit state as $\rho = \sum_{i,j} \rho_{ij} |i\rangle\langle j|$, we have

$$\begin{aligned} \Lambda(\rho) = \frac{1}{4} \sum_{i,j=0}^{1} |\psi_i\rangle\langle\psi_j| \Bigg(&\frac{1}{c^2}\rho_{00} + \frac{(-1)^j}{cs}\rho_{01} \\ &+ \frac{(-1)^i}{cs}\rho_{10} + \frac{(-1)^{i+j}}{s^2}\rho_{11} \Bigg). \end{aligned} \tag{19}$$

From the optimal USD behavior

$$p(b|x) = \begin{pmatrix} 1-\delta & 0 & \delta \\ 0 & 1-\delta & \delta \end{pmatrix}$$

[written in the same manner of Eq. (7)], we have $\text{Tr}(M_j |\psi_j\rangle\langle\psi_j|) = 1 - \delta$ and $\text{Tr}(M_j |\psi_{\bar{j}}\rangle\langle\psi_{\bar{j}}|) = 0$. Exploiting the positivity of M_k, we have $\langle\psi_{\bar{j}}|M_j|\psi_{\bar{j}}\rangle = 0 \Leftrightarrow M_j|\psi_{\bar{j}}\rangle = 0$, thus $\text{Tr}(M_k |\psi_j\rangle\langle\psi_{j'}|) = 0$ except

$$\text{Tr}(M_k |\psi_k\rangle\langle\psi_k|) = 1 - \delta. \tag{20}$$

Take $\text{Tr}(M_0 \Lambda(\rho))$ as an example:

$$\text{Tr}(M_0 \Lambda(\rho)) = \frac{1}{1+\delta}(s^2\rho_{00} + cs\rho_{01} + cs\rho_{10} + c^2\rho_{11}). \tag{21}$$

This is achieved by combining Eq. (20) and $\delta = c^2 - s^2$. By rewriting

$$\bar{M}_0 = \frac{1}{1+\delta}(s|0\rangle + c|1\rangle)(s\langle 0| + c\langle 1|),$$

one can arrive at $\text{Tr}(\bar{M}_0\rho) = \text{Tr}(M_0\Lambda(\rho))$. One can check similarly for M_1 with $\bar{M}_1$ and $M_\varnothing$ with $\bar{M}_\varnothing$, which completes the proof.

IV. RANDOMNESS

We briefly discuss the connection between our results and the task of randomness generation. Clearly, the certification of more than one bit of randomness implies a genuine three-outcome POVM [39]. It turns out however that genuine three-outcome measurements do not necessarily imply more randomness. There exist genuine three-outcome POVMs that can certify nearly zero randomness. For example, consider a binary POVM with Bloch vectors aligned with one of the

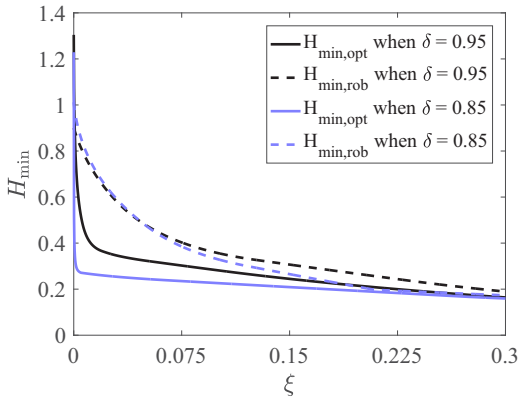

FIG. 6. Randomness certifiable by different POVMs mixed with white noise: dashed line for P_{opt}, and solid line for P_{rob}. The gap between the randomness is more apparent when ξ is small (e.g., at the given overlaps, when ξ is smaller than 0.2). When ξ is larger, the two families of measurements give approximatively the same entropy $H_{\min}$.

quantum states. From this, we can generate a three-outcome POVM by slightly rotating and shrinking the POVM elements, and thus allowing a small weight on a third component. In this case, we can obtain a three-outcome POVM that can be certified to be genuine, but at the same time certifies only little randomness. As a more concrete example, for $\delta = 0.9$, the behavior of the optimal USD measurement can only certify 0.15 bit of randomness (computed via an SDP as in Ref. [30]).

Moreover, we investigated the advantage of the optimal POVM for randomness in Ref. [39], denoted by M_{opt}, over other POVMs in the presence of noise. We compare the randomness that can be certified by M_{opt} with that of the most robust genuine three-outcome POVM (discussed in Sec. III B and now referred to as M_{rob}) in the presence of white noise (see Fig. 6). That is, for behaviors of the form $\boldsymbol{p}'_{\text{opt(rob)}} = (1-\xi)\boldsymbol{p}_{\text{opt(rob)}} + \xi \boldsymbol{p}_{\mathbb{I}}$, we compute the minimal entropy it can certify as a function of ξ. The conclusion is that although M_{opt} can certify the most randomness in the ideal, noiseless case, this advantage vanishes once there is noise.

V. CONCLUSION

We discussed the problem of characterizing an unknown POVM in a semi-DI prepare-and-measure scenario, based on the assumption of a minimum overlap between the prepared quantum states. We developed several methods for this problem and showed how a genuine three-outcome POVM can be certified. Furthermore, we showed that it is possible to self-test the optimal measurement for unambiguous state discrimination in this framework.

It would be interesting to see if other properties of quantum systems can be certified in this setting and if other measurements can be self-tested, in particular in the presence of noise. A relevant problem is the certification of genuine d-outcome POVMs, which would require a scenario with at least $d-1$ preparations. In this case, the assumptions of limited distinguishability of the set of prepared states could be formalized in different possible ways.

ACKNOWLEDGMENTS

We thank Jean-Daniel Bancal, Marie Ioannou, and Davide Rusca for useful discussions. We acknowledge support from the Swiss National Science Foundation (Starting Grant DIAQ, Bridge project "Self-testing QRNG," and NCCR-QSIT). This work is also supported by the National Nature Science Foundation of China (Grant No. 61601476). W.S. is funded by the China Scholarship Council.

APPENDIX A: DUAL PROBLEM

In this section, we show one possible way to dualize the SDP from Eq. (5) to Eq. (6). We use a method similar to that used as in Ref. [30]. First we transform the primal problem. Let $N_b^j = \frac{1}{\omega} p_j M_b^j = \frac{1}{\omega}\tilde{M}_b^j$. From the third constraint of Eq. (5) we immediately have $\frac{1}{\omega} = \frac{1}{2}\text{Tr}\sum_{j,b} N_b^j$. Since maximizing ω is equivalent to minimizing $\frac{1}{\omega}$, which we denote by η, the primal problem can be rewritten as follows:

$$\begin{aligned}
\min_{N_b^j} \quad & \eta = \frac{1}{2}\text{Tr}\sum_{j,b} N_b^j \\
\text{subject to} \quad & N_b^j \succeq 0, \quad \forall j, b, \\
& \sum_b N_b^j = \frac{1}{2}\text{Tr}\left(\sum_b N_b^j\right)\mathbb{I}, \quad \forall j, \\
& N_j^j = 0, \quad \forall j, \\
& p(b|x) + (\eta - 1)p_0(b|x) \\
& \qquad = \text{Tr}\left(|\psi_x\rangle\langle\psi_x| \sum_j N_b^j\right), \quad \forall x, b.
\end{aligned} \tag{A1}$$

Introduce Hermitian matrices G_b^j, H^j, and J^j, and real scalars $v_{b|x}$ as Lagrange multipliers to each constraints in the primal problem. The Lagrangian associated with Eq. (A1) reads

$$\begin{aligned}
\mathcal{L} =& \frac{1}{2}\sum_{j,b}\text{Tr}\left(N_b^j\right) + \sum_{j,b}\text{Tr}\left(G_b^j N_b^j\right) \\
& + \sum_{j,b}\text{Tr}\left\{H^j\left[N_b^j - \frac{1}{2}\text{Tr}\left(N_b^j\right)\mathbb{I}\right]\right\} + \sum_{j,b}\delta_{j,b}\text{Tr}\left(N_b^j J^j\right) \\
& + \sum_{x,b} v_{b|x}\left\{p(b|x) - \text{Tr}\left(|\psi_x\rangle\langle\psi_x| \sum_j N_b^j\right)\right. \\
& \left. + p_0(b|x)\left[\frac{1}{2}\sum_{j,b'}\text{Tr}\left(N_{b'}^j\right) - 1\right]\right\},
\end{aligned} \tag{A2}$$

where j, b, and b' range from 0 to 2, and x ranges from 0 to 1.

We define $\mathcal{S}$ to be the infimum of the Lagrangian over the primal SDP variables, namely, $\mathcal{S} = \inf_{N_b^j}\mathcal{L}$. To let $\mathcal{S}$ be able to lower bound the primal objective function, for any particular solution N_b^j, $\mathcal{L}$ should be smaller than the value of the primal problem. In order to achieve this, the second term of Eq. (A2) should be negative, which requires $G_b^j \leqslant 0$,

while the following three terms vanish automatically for N_b^j that satisfy the constraints in Eq. (A1).

Now we maximize $\mathcal{S}$ over the Lagrangian multipliers to get a tighter lower bound of $\mathcal{L}$. By rearranging the terms of Eq. (A2), we have

$$\mathcal{S} = \sum_{b,x} v_{b|x}[p(b|x) - p_0(b|x)] + \inf_{N_b^j} \sum_{j,b} \mathrm{Tr}\left[N_b^j K_b^j\right], \quad \text{(A3)}$$

where

$$K_b^j = \frac{1}{2}\mathbb{I} + G_b^j + H^j - \frac{1}{2}\mathrm{Tr}(H^j)\mathbb{I} + \frac{1}{2}\sum_{x,b'} v_{b'|x} p_0(b'|x)\mathbb{I} - \sum_x v_{b|x}|\psi_x\rangle\langle\psi_x| + \delta_{j,b}J^j. \quad \text{(A4)}$$

Since there is no constraint on N_b^j in the Lagrangian, to make Eq. (A3) nontrivial, namely, $\mathcal{S} > -\infty$, K_b^j is restricted to be zero. We can solve $K_b^j = 0$ for G_b^j and substitute it into $G_b^j \leqslant 0$, which is the third constraint of Eq. (6).

APPENDIX B: DETAILED CALCULATIONS FOR THE ANALYTIC BOUNDARY OF $\mathcal{P}_2(\delta)$ IN THE SYMMETRIC SLICE

To characterize $T(\mathcal{P}_2(\delta))$, we write the two quantum states as $\{\frac{1}{2}(\mathbb{I} + \boldsymbol{n}_x \cdot \boldsymbol{\sigma})\}_{x=0}^1$ and the projective two-outcome POVMs as $\{\frac{1}{2}(\mathbb{I} \pm \boldsymbol{u} \cdot \boldsymbol{\sigma})\}$, where $\boldsymbol{n}_x$ and $\boldsymbol{u}$ are the Bloch vectors and $\boldsymbol{\sigma}$ is the vector of Pauli operators. According to Eq. (3), $n_x = [(-1)^x \sin 2\theta, 0, \cos 2\theta]$. For strategy $\{0, K_1, \mathbb{I} - K_1\}$, we have

$$X = \tfrac{1}{4}(1 + \boldsymbol{n_1} \cdot \boldsymbol{u}),$$
$$Y = \tfrac{1}{4}(1 + \boldsymbol{n_0} \cdot \boldsymbol{u}). \quad \text{(B1)}$$

We find that

$$X + Y = \tfrac{1}{2} + \tfrac{1}{4}(\boldsymbol{n_0} + \boldsymbol{n_1}) \cdot \boldsymbol{u},$$
$$X - Y = \tfrac{1}{4}(\boldsymbol{n_0} - \boldsymbol{n_1}) \cdot \boldsymbol{u}. \quad \text{(B2)}$$

Since $(\boldsymbol{n_0} + \boldsymbol{n_1}) \perp (\boldsymbol{n_0} - \boldsymbol{n_1})$ and $\boldsymbol{u}$ is a unit vector, we have

$$\left[\frac{\boldsymbol{u} \cdot (\boldsymbol{n_0} + \boldsymbol{n_1})}{|\boldsymbol{n_0} + \boldsymbol{n_1}|}\right]^2 + \left[\frac{\boldsymbol{u} \cdot (\boldsymbol{n_0} - \boldsymbol{n_1})}{|\boldsymbol{n_0} - \boldsymbol{n_1}|}\right]^2 = 1. \quad \text{(B3)}$$

Rewriting Eq. (B3) in terms of Eq. (B2) leads to Eq. (9).

This works for strategy $\{K_2, 0, \mathbb{I} - K_2\}$ also. As to strategy $\{K_3, \mathbb{I} - K_3, 0\}$, immediately we have $X + Y = 1$, but not all the points on the line are accessible. Note that

$$X/Y = \frac{1 + \frac{1}{2}\boldsymbol{u}_0 \cdot (\boldsymbol{n}_0 - \boldsymbol{n}_1)}{1 - \frac{1}{2}\boldsymbol{u}_0 \cdot (\boldsymbol{n}_0 - \boldsymbol{n}_1)} \in \left[\frac{1 - \sqrt{1-\delta^2}}{1 + \sqrt{1-\delta^2}}, \frac{1 + \sqrt{1-\delta^2}}{1 - \sqrt{1-\delta^2}}\right];$$

we have that only the line segment between vertices (10) and (11) is valid. Combined with the vertices contributed by trivial measurements, we know that the (X, Y) allowed by the convex combination of two-outcome POVMs is the convex hull of points $\{(0, 0)$, Eq. (10), Eq. (11)$\}$ and the ellipse (9).

[1] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[3] R. Colbeck, Ph.D. dissertation, University of Cambridge, Cambridge, England, 2007.
[4] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[5] V. Scarani and C. Kurtsiefer, Theor. Comput. Sci. **560**, 27 (2014).
[6] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[7] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).
[8] S. J. Summers and R. Werner, Commun. Math. Phys. **110**, 247 (1987).
[9] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).
[10] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012).
[11] J. Kaniewski, Phys. Rev. Lett. **117**, 070402 (2016).
[12] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
[13] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008).
[14] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 140407 (2014).
[15] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Phys. Rev. Lett. **121**, 180505 (2018).
[16] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Phys. Rev. A **98**, 062307 (2018).
[17] M. Farkas and J. Kaniewski, Phys. Rev. A **99**, 032316 (2019).
[18] A. Tavakoli, D. Rosset, and M.-O. Renou, Phys. Rev. Lett. **122**, 070501 (2019).
[19] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, arXiv:1811.12712.
[20] N. Miklin, J. J. Borkała, and M. Pawłowski, arXiv:1903.12533.
[21] P. Mironowicz and M. Pawłowski, Phys. Rev. A **100**, 030301 (2019).
[22] K. Mohan, A. Tavakoli, and N. Brunner, New J. Phys. **21**, 083034 (2019).
[23] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[24] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[25] T. Lunghi, J. B. Brask, C. Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[26] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, Phys. Rev. Lett. **92**, 087902 (2004).
[27] E. Woodhead and S. Pironio, Phys. Rev. Lett. **115**, 150501 (2015).

[28] R. Chaves, J. B. Brask, and N. Brunner, Phys. Rev. Lett. **115**, 110501 (2015).
[29] T. V. Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Quantum **1**, 33 (2017).
[30] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Appl. **7**, 054018 (2017).
[31] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, npj Quantum Inf. **5**, 17 (2019).
[32] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, arXiv:1904.04819.
[33] I. D. Ivanovic, Phys. Lett. A **123**, 3 (1987).
[34] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[35] A. Peres, Phys. Lett. A **128**, 19 (1988).
[36] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[37] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[38] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University, New York, 2011).
[39] M. Ioannou, J. B. Brask, and N. Brunner, Phys. Rev. A **99**, 052338 (2019).