Self-Testing in Prepare-and-Measure Scenarios and a Robust Version of Wigner's Theorem

Miguel Navascués,[1] Károly F. Pál,[2] Tamás Vértesi,[3] and Mateus Araújo[4]

[1]Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Vienna 1090, Austria
[2]Institute for Nuclear Research, P.O. Box 51, H-4001 Debrecen, Hungary
[3]MTA Atomki Lendület Quantum Correlations Research Group, Institute for Nuclear Research, P.O. Box 51, H-4001 Debrecen, Hungary
[4]Departamento de Física Teórica, Atómica y Óptica, Universidad de Valladolid, 47011 Valladolid, Spain

(Received 13 June 2023; accepted 21 November 2023; published 21 December 2023)

We consider communication scenarios where one party sends quantum states of known dimensionality D, prepared with an untrusted apparatus, to another, distant party, who probes them with uncharacterized measurement devices. We prove that, for any ensemble of reference pure quantum states, there exists one such prepare-and-measure scenario and a linear functional W on its observed measurement probabilities, such that W can only be maximized if the preparations coincide with the reference states, modulo a unitary or an antiunitary transformation. In other words, prepare-and-measure scenarios allow one to "self-test" arbitrary ensembles of pure quantum states. Arbitrary extreme D-dimensional quantum measurements, or sets thereof, can be similarly self-tested. Our results rely on a robust generalization of Wigner's theorem, a well-known result in particle physics that characterizes physical symmetries.

DOI: 10.1103/PhysRevLett.131.250802

All experiments in quantum physics start by setting the lab equipment in a given state and end by conducting a measurement. When we assign different experimenters to each of these two tasks, namely, when one experimenter is asked to prepare certain quantum states and another one to probe them, then we are working in the so-called prepare-and-measure communication scenario [1,2]. This paradigm models many primitives of interest for quantum information theory, such as quantum key distribution [3,4], quantum communication complexity [5], and metrology [6].

A communication protocol that does not rely on a characterization of the measurement and preparation apparatuses is said to be "device-independent" (DI) [7]. The security or success of those protocols is thus guaranteed by their measurement statistics alone [8,9]. Unfortunately, prepare-and-measure scenarios cannot be fully DI, as an arbitrarily large classical memory suffices to explain all conceivable measurement statistics.

It is possible, however, to devise "semidevice independent" (SDI) prepare-and-measure protocols [1]. SDI protocols rely both on the measurement statistics and also on some (generally, weak) promise on the preparation or measurement devices [10–12]. Following most of the literature on SDI protocols (see, e.g., [1,4,13]), in this Letter we will posit a bound on the Hilbert space dimension of the preparations. Note that the SDI paradigm allows certifying properties that the DI approach cannot, e.g., self-testing nonprojective measurements [14]. In addition, SDI protocols are in general experimentally friendlier than their DI counterparts.

Under the assumption that the Hilbert space dimension of the prepared systems is known, it was observed in Ref. [2,14] that certain qubit states and qubit measurements could be "self-tested": namely, the only way to generate certain feasible measurement statistics in a prepare-and-measure scenario is to prepare those quantum states and conduct those measurements, modulo unitary and antiunitary transformations. In the same spirit, the authors of [15] show how to self-test measurements of mutually unbiased bases [16] in arbitrary dimensions. These works leave us with the question of which state ensembles and measurements, in the qubit case, as well as in higher dimensions, can be self-tested.

In this Letter, we answer this question by providing a family of linear witnesses whose maximal value self-tests arbitrary ensembles of pure states and arbitrary sets of extreme positive operator valued measures (POVMs) (or both), in prepare-and-measure scenarios of arbitrary Hilbert space dimension. Since neither state ensembles containing mixed states nor nonextreme POVMs can be self-tested, our result fully characterizes the limits of self-testing in the prepare-and-measure scenario. Note that, prior to our work, general self-testing schemes only existed for scenarios with nondemolition measurements, which should be sequentially applied in the course of a single experimental round [17,18].

To prove our main result, we generalize the famous Wigner's theorem [19], which states that all physical symmetries (i.e., all maps from rays to rays that preserve the absolute value of the scalar product) can be expressed as a unitary or an antiunitary transformation. Our generalization considers "noisy partial symmetries," whose domain is limited to a finite number of rays and which preserve the absolute value of the scalar product up to an error.

The scenario we consider differs from that of other works with a similar flavor, such as Miklin and Oszmaniec's [20]. In that paper, the authors assume that, every time that the experiment is reset, the same state preparations and measurements are available—such scenarios are usually called "independent and identically distributed" (i.i.d.). To the contrary, the statistical tests proposed in this Letter do not rely on the i.i.d. assumption: our results are therefore robust under the miscalibration of the preparation and measurement devices and even allow for correlations between the different experimental rounds.

Prepare-and-measure scenarios.—In a prepare-and-measure scenario, one party, Alice, prepares a D-dimensional quantum state labeled by the index $x = 1, \ldots, X$, and sends it to a second party, Bob, who probes the state with some POVM $y \in \{1, \ldots, Y\}$, obtaining an outcome $b \in \{1, \ldots, B\}$. The scenario is thus specified by the vector of natural numbers (D, X, Y, B).

In the following, we denote Alice's xth state as $\bar{\psi}_x \in B(\mathbb{C}^D)$ and Bob's yth POVM by $\bar{M}_y \coloneqq (\bar{M}_{b|y} \in B(\mathbb{C}^D)\colon b = 1, \ldots, B)$. We will call $\bar{\psi}$ ($\bar{M}$) Alice's collection of states (Bob's collection of POVMs). That is, $\bar{\psi} = \{\bar{\psi}_x\}_{x=1}^X$, $\bar{M} \coloneqq \{\bar{M}_y\}_{y=1}^Y$. Of course, both states and POVMs are subject to the usual positivity and normalization conditions, i.e., $\bar{\psi}_x \geq 0$, $\mathrm{tr}(\bar{\psi}_x) = 1$, $\forall\ x$, $\bar{M}_{b|y} \geq 0$, $\forall\ y, b$ and $\sum_b \bar{M}_{b|y} = \mathbb{I}_D$, $\forall\ y$.

Denoting by $P(b|x,y)$ the probability that Bob observes outcome b when he performs measurement y on state x, the experiment's measurement statistics $P \coloneqq (P(b|x,y)\colon x, y, b)$ are given by

$$P(b|x,y) = \mathrm{tr}(\bar{\psi}_x \bar{M}_{b|y}), \quad \forall\ x, y, b. \tag{1}$$

Note that, for any unitary or antiunitary U, the state ensemble $U\psi U^\dagger$ and the measurements $UMU^\dagger$ generate the same probability distribution $P(b|x,y)$ as the original state ensemble ψ and measurement set M used by Alice and Bob. The realizations $(U\psi U^\dagger, UMU^\dagger)$, (ψ, M) are therefore operationally indistinguishable within the semidevice independent paradigm. We call Q_D the set of all distributions P admitting some D-dimensional realization (ψ, M).

Consider a prepare-and-measure scenario (D, X, Y, B), and let $W\colon \mathbb{R}^{XYB} \to \mathbb{R}$ be a linear functional with $\max_{P \in Q_D} W(P) = W^\star$. For $\mathcal{X} \leq X$, $\mathcal{Y} \leq Y$, we say that *W self-tests* the states $(\psi_x)_{x=1}^{\mathcal{X}}$ and the POVMs $\{M_y\}_{y=1}^{\mathcal{Y}}$ if, for any feasible P realized by $(\bar{\psi}, \bar{M})$ with $W(P) = W^\star$, there exists a unitary or antiunitary map U with the property that

$$\begin{aligned} \bar{\psi}_x &= U\psi_x U^\dagger, \qquad x = 1, \ldots, \mathcal{X}, \\ \bar{M}_{b|y} &= UM_{b|y}U^\dagger, \qquad y = 1, \ldots, \mathcal{Y}, \qquad b = 1, \ldots, B. \end{aligned} \tag{2}$$

We say that *W robustly self-tests* $(\psi_x)_{x=1}^{\mathcal{X}}$, $\{M_y\}_{y=1}^{\mathcal{Y}}$ if, for all $\epsilon > 0$, there exists $\epsilon' > 0$ such that $W^\star - W(P) \leq \epsilon'$ implies that relations (2) are satisfied up to precision ϵ in trace and operator norm, respectively.

No linear functional W can self-test nonextreme states or measurements. Suppose, e.g., that W were maximized by a feasible distribution P whose realization involved a mixed state $\bar{\psi}_x = \sum_j \lambda_j |\bar{\phi}_j\rangle\langle\bar{\phi}_j|$, with $\lambda_j > 0$. Then, the distribution P' generated if we replaced $\bar{\psi}_x$ with $|\bar{\phi}_1\rangle\langle\bar{\phi}_1|$ would also maximize W. However, $|\bar{\phi}_1\rangle\langle\bar{\phi}_1|$ and $\bar{\psi}_x$ are not connected by a unitary or an antiunitary transformation. The same argument holds for extreme POVMs. We arrive at the conclusion that only extreme (pure) states and extreme POVMs can be, in principle, self-tested, modulo unitary or antiunitary transformations.

To prove that a prepare-and-measure experimental system satisfies an inequality of the form $W(P) \geq W^\star - \epsilon$, one would first think of estimating the probabilities $P(b|x,y)$ through repeated experiments and then evaluating the witness. However, such a direct approach is only feasible when the experimental setup satisfies the i.i.d. assumption. When the system is not i.i.d., the goal is to reject the null hypothesis that, in each experimental round, $W(P) < W^\star - \epsilon$. It turns out that, as long as the functional W is linear, it is possible to devise a statistical test that fits the bill and yet does not rely on the i.i.d. assumption [21]. In this test, at each experimental round the inputs x, y are sampled according to some probability distribution and the output b is used to generate a round score. The score of the different rounds is multiplied and a p value for the null hypothesis is derived. If the system violates the hypothesis and is approximately i.i.d., the p value will quickly tend to zero as the number of rounds increases [21].

Reference [14] proposes linear witnesses to self-test some extreme POVMs and state ensembles in the qubit case ($D = 2$). The goal of the rest of this Letter is to generalize the results of Ref. [14] to robustly self-test any ensemble of pure states and collection of extreme POVMs, defined in Hilbert spaces of arbitrary dimension D.

Self-testing of pure state ensembles.—We start by showing how to self-test pure state ensembles. To avoid a cumbersome notation, from now on, whenever we refer to a normalized ket $|\omega\rangle$, we will use ω to denote its corresponding rank-1 projector $|\omega\rangle\langle\omega|$. For fixed dimension D, we call $\mathcal{P} \subset B(\mathbb{C}^D)$ the set of all rank-1 projectors.

Self-testing of state ensembles is based on the following lemma.

Lemma 1.—Let $\Psi \equiv \{\psi_i\}_{i=1}^N \subset \mathcal{P}$ be a collection of pure quantum states such that

$$\sum_i \alpha_i \psi_i = \frac{\mathbb{I}_D}{D}, \tag{3}$$

for some $\{\alpha_i\}_{i=1}^N \subset \mathbb{R}^+$. Consider a prepare-and-measure scenario $\{D, N, [(N^2 - N)/2], 2\}$ with the measurements labeled by $y \in \{(i,j): i > j, i,j = 1,\ldots,N\}$. Define the linear witness

$$W_\Psi(P) \coloneqq \sum_{i>j} \alpha_i \alpha_j \|\psi_i - \psi_j\|_1 S_{i,j}, \tag{4}$$

with

$$S_{i,j} \coloneqq P[2|x=i, y=(i,j)] - P[2|x=j, y=(i,j)]. \tag{5}$$

Then, for all $P \in Q_D$, it holds that

$$W_\Psi(P) \leq 1 - \frac{1}{D}. \tag{6}$$

This inequality is tight and can be saturated by preparing the states Ψ and choosing the dichotomic measurements appropriately.

Moreover, if any feasible distribution P, realized with preparation states $\{\bar{\psi}_i\}_{i=1}^N \subset B(\mathbb{C}^D)$, satisfies $W_\Psi(P) \geq 1-(1/D) - \epsilon$, then it holds that

$$1 - \mathrm{tr}(\bar{\psi}_i^2) \leq O(\epsilon),$$
$$|\mathrm{tr}\{\bar{\psi}_i\bar{\psi}_j\} - \mathrm{tr}\{\psi_i\psi_j\}| \leq O(\sqrt{\epsilon}), \quad \forall \ i,j. \tag{7}$$

In particular, when $\epsilon = 0$, then all the prepared states $\{\bar{\psi}_i\}_{i=1}^N$ are pure and have the same projector overlaps as the reference states ψ.

This lemma can be regarded as a study of the saturation conditions of a variant of the dimension witness proposed in [22]. The reader can find a proof in Sec. I of the Supplemental Material [23], where the exact expressions for the right-hand sides of Eq. (7) are provided.

Now, suppose that we wished to self-test an ensemble of pure-state preparations $\{\psi_i\}_{i=1}^M$. To exploit Lemma 1, we need to find (pure) states $\{\psi_i\}_{i=M+1}^N$ and positive real numbers $\{\alpha_i\}_{i=1}^N$ such that condition (3) holds. Such extra states and positive numbers always exist: consider, for instance, the maximum $\lambda \in \mathbb{R}$ such that the operator $V = (\mathbb{I}/D) - \lambda \sum_{i=1}^M \psi_i$ is positive semidefinite [30]. Let $\sum_{i=M+1}^N \beta_i |\psi_i\rangle\langle\psi_i|$ be the spectral decomposition of V, with $\beta_i > 0$ (we omit the eigenvectors with zero eigenvalue, so $N \leq M + D - 1$). Then we have that $\{\psi_i\}_{i=1}^N$, and $\{\alpha_i\}_{i=1}^N$, with $\alpha_i \coloneqq \lambda$, for $i = 1,\ldots,M$, and $\alpha_i \coloneqq \beta_i$, for $i = M+1,\ldots,N$, satisfy condition (3).

Given $\psi = \{\psi_i\}_{i=1}^N$, $\{\alpha_i\}_{i=1}^N$, we can thus build the witness $W_\psi(P)$. By Lemma 1, if $W_\psi(P)$ is ϵ close to its maximum value, then the prepared states $\{\phi_i\}_{i=1}^N$ will satisfy Eq. (7). The question is whether, for ϵ sufficiently small, this condition implies that $\phi_i \approx U\psi_i U^\dagger$, for all i, for some unitary or antiunitary U.

Note the similarities with the famous Wigner's theorem [19,31,32], whose finite-dimensional version reads [33] as follows.

Theorem 2.—Let the (possibly nonlinear) map $\omega: \mathcal{P} \to \mathcal{P}$ have the property

$$\mathrm{tr}(\phi\phi') = \mathrm{tr}[\omega(\phi)\omega(\phi')], \quad \forall \ \phi, \phi' \in \mathcal{P}. \tag{8}$$

Then, there exists a unitary or antiunitary transformation U such that

$$\omega(\phi) = U\phi U^\dagger, \quad \forall \ \phi \in \mathcal{P}. \tag{9}$$

We wish to generalize this result in two ways. First, in our case the domain of ω only covers a finite set of rank-1 projectors, namely, $\{\psi_i\}_{i=1}^N$. Second, we are interested in situations where Eq. (8) only holds approximately. This leads us to define what from now on we call the "Wigner property."

Definition 3.—We say that a set of pure states $\{\psi_i\}_{i=1}^N \subset \mathcal{P}$ satisfies the Wigner property if, for all $\delta' > 0$ and for any set of (not necessarily pure) states $\{\bar{\psi}_i\}_{i=1}^N \subset B(\mathbb{C}^D)$, there exists $\delta > 0$ such that the relation

$$|\mathrm{tr}(\psi_i\psi_j) - \mathrm{tr}(\bar{\psi}_i\bar{\psi}_j)| \leq \delta, i,j = 1,\ldots,M, \tag{10}$$

implies that there exist a unitary (antiunitary) transformation U with $\|\psi_i - U\bar{\psi}_i U^\dagger\|_1 \leq \delta'$, for $i = 1,\ldots,M$.

As observed in [20], for $D = 2$ all pure state ensembles satisfy the Wigner property. In that case,

$$\psi_i = \frac{\mathbb{I} + \vec{m}^i \cdot \vec{\sigma}}{2}, \qquad \bar{\psi}_i = \frac{\mathbb{I} + \vec{n}^i \cdot \vec{\sigma}}{2}, \tag{11}$$

for some vectors $\{\vec{m}^i, \vec{n}^i: \|\vec{m}^i\|, \|\vec{n}^i\| \leq 1\}_{i=1}^N \subset \mathbb{R}^3$. Here, $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ denotes the three Pauli matrices. Setting $\delta = 0$ in Eq. (10), we have that $\vec{m}^i \cdot \vec{m}^j = \vec{n}^i \cdot \vec{n}^j$, for all i, j. It follows that there exists an orthogonal transformation O such that $\vec{n}^i = O\vec{m}^i$, for all i. Any orthogonal transformation in $\mathbb{R}^3$ can be expressed as either R or TR, where R represents a rotation and T a reflection. In the first case, there exists a unitary U such that $\phi_i = U\psi_i U^\dagger$, for all i. In the second case, there exists an antiunitary operation V such that $\phi_i = V\psi_i V^\dagger$. In Sec. III of the Supplemental Material we provide a robust version of this argument, which proves that any ensemble of pure states in dimension $D = 2$ satisfies the Wigner property with $\delta' = O(\delta^{1/4})$.

How about higher dimensions? Do pure state ensembles in, say, dimension 3, satisfy the Wigner property, too? In general, no. In Sec. V of the Supplemental Material we present several examples of pairs of state ensembles in dimension 3 that, despite having the same overlaps, are not related via unitary or antiunitary transformations. Furthermore, we find that generic ensembles of three two-dimensional pure states, embedded in $B(\mathbb{C}^3)$, do not satisfy the Wigner property, even if we restrict it to the zero-error case ($\delta = 0$).

How can we then certify state ensembles of dimensions greater than two? A possible way to solve this problem is to look for inspiration in the recent literature on Wigner's theorem. In this regard, the proof of Wigner's theorem in [32] relies on the existence of a set of $5D-6$ pure states $\mathcal{T}\subset\mathcal{P}$ with the following property: for any ensemble of pure states $\Psi=\{\psi_i\}_{i=1}^{N}\subset\mathcal{P}$ such that $\langle k|\psi_i|k\rangle>0$, $\forall\ k,i$, the overlaps between the states in $\Psi\cup\mathcal{T}$ uniquely identify this latter set, modulo a unitary (antiunitary) transformation. In Sec. II of the Supplemental Material we make this statement robust. Namely, we prove the following result.

Lemma 4.—Let $\{\psi_i\}_{i=1}^{N}\subset\mathcal{P}$ be such that $\mathrm{tr}(\psi_i|k\rangle\langle k|)\geq f>0$, for $k=1,\ldots,D$. Then, the ensemble of pure states $\mathcal{T}\cup\{\psi_i\}_{i=1}^{N}$ satisfies the Wigner property with $\delta'=O(\sqrt{f}D^{7/4}\delta^{1/8})$.

To arrive at robustness bounds that scale well with D, the proof makes use of Hausladen and Wootters' pretty good measurement [34], duality theory [35], and exactly solvable tridiagonal matrices. The exponent $1/8$ on δ is admittedly very inconvenient. Presumably, one could achieve better robustness bounds by taking a tomographically complete fiducial set $\mathcal{T}'$ instead of $\mathcal{T}$. This is the approach used in [17], which follows more closely the original proof of Wigner's theorem. The tomographic approach has the disadvantage of requiring $O(D^2)$ new state preparations, instead of $O(D)$.

Now, suppose that we wish to self-test the ensemble of preparations $\psi=\{\psi_i\}_{i=1}^{M}\subset\mathcal{P}$. First, we transform the computational basis $\{|k\rangle\}_{k=1}^{D}$ with a unitary to ensure that all M states in ψ satisfy $\mathrm{tr}(\psi_i|k\rangle\langle k|)>0,\ \forall\ k$ (a random unitary will achieve this with probability 1). Next, we consider the ensemble of preparations $\tilde{\psi}\coloneqq\psi\cup\mathcal{T}\cup\mathcal{R}$, where $\mathcal{R}$ are extra states (not to be self-tested) that we might need to add to ensure that the ensemble $\tilde{\psi}$ satisfies condition (3) for some positive numbers $(\alpha_i)_i$.

Suppose that the corresponding dimension witness $W_{\tilde{\psi}}(P)$ is maximized by the set of (necessarily pure) states $\bar{\psi}\cup\bar{\mathcal{T}}\cup\bar{\mathcal{R}}$. Then condition (10) and Lemma 4 guarantee that the ensembles of states $\psi\cup\mathcal{T}$, $\bar{\psi}\cup\bar{\mathcal{T}}$, are related by a unitary or an antiunitary transformation. In particular, the witness $W_{\tilde{\psi}}$ self-tests the reference states $\{\psi_i\}_{i=1}^{M}$. This result can be made robust by applying Lemmas 1 and 4 in sequence. Thus, a value of W_{ψ} that is ϵ short from maximum indicates that $U\bar{\psi}_iU^{\dagger}$ is $O(\epsilon^{1/16})$ away from ψ_i, for all i.

Self-testing of extremal POVMs.—We now turn to the problem of self-testing extremal POVMs. We will rely on the characterization of extreme quantum measurements by D'Arianno *et al.* [36]. Namely, a POVM $(M_b)_b$ is extremal if and only if, for any set of $D\times D$ Hermitian matrices $(H_b)_b$, with $\mathrm{Supp}(H_b)\subset\mathrm{Supp}(M_b)$, $\forall\ b$, the condition $\sum_b H_b=0$ implies that $H_b=0,\ \forall\ b$.

Now, let $(M_b)_b$ be an extreme POVM, and, for each b, let Z_b be a projector onto the kernel of M_b. Then, the only maximizer of the POVM optimization problem $\max_{\bar{M}}-\sum_b\mathrm{tr}(Z_b\bar{M}_b)$ is M. Indeed, first note that the maximum value of the problem is zero, which can, indeed, be achieved by the solution $\bar{M}=M$. Now, suppose that there exists another solution $M^{\star}$ of the optimization problem. Then, $\mathrm{tr}(M_b^{\star}Z_b)=0$, for all a, which implies that $\mathrm{Supp}(M_b^{\star})\subset\mathrm{Kern}(Z_b)=\mathrm{Supp}(M_b)$. Define then $H_b\coloneqq M_b^{\star}-M_b$. Then on one hand we have that $\mathrm{Supp}(H_b)\subset\mathrm{Supp}(M_b)$, for all b. On the other hand, $\sum_b H_b=\sum_b M_b^{\star}-\sum_b M_b=\mathbb{I}-\mathbb{I}=0$. By the extremality of M it thus follows that $H_b=0$, for all b, and so $M^{\star}=M$.

Combined with our tool for self-testing states, this observation is enough to self-test $(M_b)_{b=1}^{B}$. Let Z_b admit a spectral decomposition as $Z_b=\sum_{i=1}^{d_b}|\psi_i^a\rangle\langle\psi_i^a|$ and define the pure state ensemble $\psi\coloneqq\{\psi_i^b\colon i,b\}\cup\mathcal{T}\cup\mathcal{R}$, where $\mathcal{R}$ is again a set of pure states such that ψ satisfies Eq. (3). We define a prepare and measure scenario with $X=\sum_b d_b+|\mathcal{T}|+D-1$, $Y=(X^2-X)/2+1$, where measurements $y=1,\ldots,Y-1$ are dichotomic and measurement $y=Y$ has B outcomes, and consider the witness

$$W_{\bar{M}}(P)=W_{\psi}(P)-\sum_b\sum_{i=1}^{d_b}P(b|x=(i,b),y=Y).\qquad(12)$$

The maximum value of this witness is clearly $1-(1/D)$, achievable by preparing the states ψ, conducting the optimal dichotomic measurements to distinguish every pair of states in ψ and also M as the Yth POVM. Now, suppose that the maximum value of the witness is achieved by preparing states $\bar{\psi}$ and conducting POVM $\bar{M}$ for measurement $y=Y$. Since the witness $W_{\psi}(P)$ is saturated, there exists a unitary (antiunitary) transformation U such that $U\bar{\psi}U^{\dagger}=\psi$. Let us then consider the POVM $M'\coloneqq U\bar{M}U^{\dagger}$. Then this POVM satisfies $\sum_b\mathrm{tr}(Z_bM_b')=0$, and thus, by the previous reasoning, $M_b'=M_b$, for all b. We demonstrate the above construction for self-testing on a specific extremal nonprojective POVM in Sec. VI of the Supplemental Material. On the other hand, in Sec. IV of the Supplemental Material, we present a robust version of this argument. Namely, we show that, if $W_{\bar{M}}(P)>1-(1/D)-\epsilon$, then there exists a unitary or antiunitary U such that $U\tilde{M}_bU^{\dagger}=\bar{M}_a+\delta$, with $\delta=O(\epsilon^{1/16})$ in the $D=2$ case or $\delta=O(\epsilon^{1/32})$, otherwise.

The above construction allows one to self-test several extremal POVMs at a time: indeed, it suffices to add more terms of the form $\sum_b\sum_{i=1}^{d_{b|y}}P[b|x=(i,b,y),y]$ to (12) and update the state preparation witness to self-test the states $\psi_i^{b|y}$ required to express the projector onto the kernel of the desired POVM $(M_{b|y}\colon b)$. In sum, we can devise a prepare-and-measure experiment to self-test as many pure states and extremal POVMs as we wish.

Dealing with higher dimensional leakages.—Throughout this Letter, we were assuming that the Hilbert space where the preparations took place had dimension D. In a realistic experiment, though, it is more plausible that Alice's preparations $\{\bar{\psi}_i\}_i$ actually live in $B(\mathbb{C}^E)$, with $E > D$, possibly with $E = \infty$. Unfortunately, it is impossible to devise a D-dimensional experiment that self-tests preparations and measurements under the assumption that both objects act on a Hilbert space of dimension smaller than or equal to $E > D$, even if $E = D + 1$ [37]. Our results are, however, robust under the assumption that there exists a D-dimensional projector Π_D such that the prepared states satisfy $\mathrm{tr}(\bar{\psi}_i \Pi_D) \geq 1 - \delta, \ \forall \ i$. Indeed, as long as δ is small enough, it is easy to see that a close-to-maximal value of our linear witnesses implies the existence of an isometry (anti-isometry) that approximately transforms the actual states and measurements into the reference ones [38].

Conclusion.—In this Letter, we have completely characterized the limits of robust self-testing in the prepare-and-measure scenario, under a promise on the Hilbert space dimension of the prepared states. Namely, we have proven that, for any ensemble of pure quantum states and any set of extremal POVMs, one can devise a linear witness whose maximal value implies that the underlying states and measurements are related to the reference ones by a unitary or an antiunitary transformation.

Regrettably, the analytic robustness bounds we found, while exhibiting a reasonably good dependence on the Hilbert space dimension, scale with the experimental error ϵ as $\epsilon^{1/32}$. As such, they are impractical for realistic implementations. For small dimensions and a small number of preparation states, it might be feasible, though, to obtain more accurate predictions by combining the swap technique of [39] with standard semidefinite programming relaxations of the set Q_D [40,41].

This project was funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101017733, and from the Austrian Science Fund (FWF), Project No. I-6004. T. V. acknowledges the support of the EU (QuantERA eDICT) and the National Research, Development and Innovation Office NKFIH (No. 2019-2.1.7-ERA-NET-2020-00003). M. A. acknowledges support by the Spanish Ministry of Science and Innovation (MCIN) with funding from the European Union Next Generation EU (PRTRC17.I1) and the Department of Education of Castilla y León (JCyL) through the QCAYLE project, as well as MCIN Projects No. PID2020–113406 GB-I00 and No. RED2022-134301-T.

[1] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

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

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[4] E. Woodhead and S. Pironio, Secrecy in prepare-and-measure Clauser-Horne-Shimony-Holt tests with a qubit bound, Phys. Rev. Lett. **115**, 150501 (2015).

[5] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, J. ACM **49**, 496 (2002).

[6] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum metrology, Phys. Rev. Lett. **96**, 010401 (2006).

[7] 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).

[8] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, arXiv:0911.3814.

[9] 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, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[10] T. V. Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[11] A. Tavakoli, E. Z. Cruzeiro, J. B. Brask, N. Gisin, and N. Brunner, Informationally restricted quantum correlations, Quantum **4**, 332 (2020).

[12] C. L. Jones, S. L. Ludescher, A. Aloy, and M. P. Mueller, Theory-independent randomness generation with spacetime symmetries, arXiv:2210.14811.

[13] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-independent tests of classical and quantum dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[14] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing nonprojective quantum measurements in prepare-and-measure experiments, Sci. Adv. **6**, 16 (2020).

[15] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).

[16] J. Schwinger, Unitary operator bases, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[17] H.-Y. Huang, S. T. Flammia, and J. Preskill, Foundations for learning from noisy quantum experiments, arXiv:2204.13691.

[18] D. Das, A. G. Maity, D. Saha, and A. S. Majumdar, Robust certification of arbitrary outcome quantum measurements from temporal correlations, Quantum **6**, 716 (2022).

[19] E. P. Wigner, *Gruppentheorie und ihre Anwendung auf die Quantenmechanik der Atomspektren* (Springer, New York, 1931).

[20] N. Miklin and M. Oszmaniec, A universal scheme for robust self-testing in the prepare-and-measure scenario, Quantum **5**, 424 (2021).

[21] Y. Zhang, S. Glancy, and E. Knill, Asymptotically optimal data analysis for rejecting local realism, Phys. Rev. A **84**, 062118 (2011).

[22] N. Brunner, M. Navascués, and T. Vértesi, Dimension witnesses and quantum state discrimination, Phys. Rev. Lett. **110**, 150501 (2013).

[23] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.250802 for the proofs of Lemmas 1, 4, and other robustness results, which includes Ref. [24–29].

[24] R. Jozsa, Fidelity for mixed quantum states, J. Mod. Opt. **41**, 2315 (1994).

[25] F. Zhang, *The Schur Complement and Its Applications*, Numerical Methods and Algorithms (Springer US, New York, 2006).

[26] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. (N.Y.) **45**, 2171 (2004).

[27] Y. Aharonov and J. Anandan, Phase change during a cyclic quantum evolution, Phys. Rev. Lett. **58**, 1593 (1987).

[28] N. Mukunda and R. Simon, Quantum kinematic approach to the geometric phase. I. General formalism, Ann. Phys. (N.Y.) **228**, 205 (1993).

[29] E. Haapasalo, T. Heinosaari, and J.-P. Pellonpää, Quantum measurements on finite dimensional systems: Relabeling and mixing, Quantum Inf. Process. **11**, 1751 (2011).

[30] This maximum is always positive, as $\lambda = 1/(MD)$ will already give a positive semidefinite operator.

[31] V. Bargmann, On unitary ray representations of continuous groups, Ann. Math. **59**, 1 (1954).

[32] G. Gehér, An elementary proof for the non-bijective version of Wigner's theorem, Phys. Lett. A **378**, 2054 (2014).

[33] The original version of Wigner's theorem is expressed in terms of Hilbert space rays $|\phi\rangle, |\phi'\rangle$ and the complex modulus of their normalized overlaps $o(\phi, \phi') = (|\langle\phi|\phi'\rangle| / \sqrt{\langle\phi|\phi\rangle}\langle\phi'|\phi'\rangle)$. Note, however, that $\mathrm{tr}(|\tilde{\phi}\rangle\langle\tilde{\phi}||\widetilde{\phi'}\rangle\langle\widetilde{\phi'}|) = o(\phi, \phi')^2$, with $|\tilde{\phi}\rangle = (|\phi\rangle / \sqrt{\langle\phi|\phi\rangle})$. It follows that we can express Wigner's theorem in terms of rank-1 projectors.

[34] P. Hausladen and W. K. Wootters, A 'pretty good' measurement for distinguishing quantum states, J. Mod. Opt. **41**, 2385 (1994).

[35] L. Vandenberghe and S. Boyd, Semidefinite programming, SIAM Rev. **38**, 49 (1996).

[36] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A **38**, 5979 (2005).

[37] Consider, e.g., a 1-shot D-dimensional behavior $P(b|x, y)$ generated by the reference states $\{|\psi_i\rangle\} \in \mathrm{span}(|1\rangle, \ldots, |D\rangle)$ and measurements $\{(M_{b|y})_b \colon y\} \subset B(\mathbb{C}^D)$, and suppose that $\mathrm{tr}(\psi_1\psi_2) \neq 0$. Then, one can obtain the same experimental behavior in a $D + 1$-dimensional state if we replace ψ_1 by $|D+1\rangle\langle D+1|$, and $M_{b|y}$ by $M_{b|y} + P(b|1, y)|D+1\rangle\langle D+1|$. In this new representation, though, the first two preparations are orthogonal and thus not connected by a unitary or an antiunitary transformation.

[38] Note that the D-dimensional ensemble $\tilde{\psi}_i \coloneqq [\Pi_D\psi_i\Pi_D/\mathrm{tr}(\psi_i\Pi_D)]$, $i = 1, \ldots, N$ satisfies $\|\overline{\psi}_i - \tilde{\psi}_i\|_1 \leq O(\sqrt{\delta})$, $\forall\ i$. Thus, the D-dimensional distribution $\tilde{P}(b|x, y) \coloneqq \mathrm{tr}\left(\tilde{\psi}_i\tilde{M}_{b|y}\right)$, with $\tilde{M}_{b|y} \coloneqq \Pi_D M_{b|y}\Pi_D$, is $O(\sqrt{\delta})$ away from the experimental 1-shot distribution $P(b|x, y)$. It follows that $W(P) > W^\star - \epsilon$ implies that $W(\tilde{P}) > W^\star - \epsilon - O(\sqrt{\delta})$. Thus, for ϵ, δ small enough, there exists a unitary (antiunitary) U such that $U\tilde{\psi}U^\dagger \approx \psi_i$ $U\tilde{M}_{b|y}U^\dagger \approx M_{b|y}$. Consequently, the isometry (anti-isometry) $V \coloneqq U\Pi_D$ approximately maps $\{\bar{\psi}_i\}_i$, $\{\bar{M}_{b|y}\}_{b,y}$ to the reference states and measurements $\{\psi_i\}_i$, $\{M_{b|y}\}_{b,y}$.

[39] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Robust and versatile black-box certification of quantum devices, Phys. Rev. Lett. **113**, 040401 (2014).

[40] M. Navascués and T. Vértesi, Bounding the set of finite dimensional quantum correlations, Phys. Rev. Lett. **115**, 020501 (2015).

[41] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Characterizing finite-dimensional quantum behavior, Phys. Rev. A **92**, 042117 (2015).