Device-independent tests of quantum states

Michele Dall'Arno[*]

Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore

(Received 19 April 2017; published 30 May 2019)

We construct a correspondence between quantum states and the observable input-output correlations they are compatible with. The problem is framed as a game involving an experimenter, claiming to be able to prepare some family of states, and a theoretician, whose aim is to falsify such a claim based on observed correlations only. For any such claim, the optimal strategy consists of providing (i) to the experimenter, *all* the measurements that generate extremal input-output correlations, and (ii) to the theoretician, the *full* characterization of such correlations. Comparing the correlations observed in (i) with those predicted by (ii) corresponds to device-independently testing the states. While no assumption is made about the *actual* states and measurements, we derive the optimal strategy in *closed form* for the case when the *claim* consists of qubit states and the performed measurements are tests, and as applications we specify our results to the case of any pair of pure states and to the case of pure states uniformly distributed on the Bloch equatorial plane.

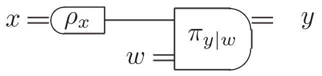
DOI: 10.1103/PhysRevA.99.052353

I. INTRODUCTION

Quantum systems are most generally described by quantum states, abstract vectors in a mathematical space with the property of not being perfectly distinguishable—a property called *superposition* of pure states. However, all an observer can ultimately observe are just correlations among perfectly distinguishable events in usual space and time. Hence, how can quantum states be inferred? Here, we answer this question by constructing a correspondence between quantum states and the observable input-output correlations they are compatible with.

The problem is most generally framed as a game involving an experimenter, claiming to be able to prepare m quantum states $\{\rho_x\}$ and to measure them, and a skeptical theoretician whose aim is to falsify such a claim based on observed correlations only. At each run of the experiment, first the experimenter prepares state ρ_x upon input of x, and then performs measurement $\{\pi_{y|w}\}$ upon input of w. Finally, the theoretician collects outcome y, thus reconstructing correlation $\{p_{y|x,w}\}$. The setup is as follows:

$$p_{y|x,w} := \mathrm{Tr}[\rho_x \pi_{y|w}] \quad =$$



Let us denote with $S_n(\rho_x)$ the set of correlations generated by states $\{\rho_x\}$ for any n-outcomes measurement $\{\pi_y\}$, that is,

$$S_n(\rho_x) := \{p \mid p_{y|x} = \mathrm{Tr}[\rho_x \pi_y]\}$$

(we take $y \in [0, n-2]$ since for $y = n-1$ one simply has $p_{n-1|x} = 1 - \sum_{y=0}^{n-2} p_{y|x}$). On the theoretician's side, the problem amounts to fully characterizing $S_n(\rho_x)$, for any $\{\rho_x\}$, in order to check if $\{p_{y|x,w}\} \in S_n(\rho)$, for any w. On the experimenter's side, the problem amounts to choosing measurements $\{\pi_{y|w}\}$ generating all the extremal correlations of $S_n(\rho_x)$ (of course, the validity of the conclusion itself will be independent of $\{\pi_{y|w}\}$). Therefore, w represents a direction to be probed in the space of correlations in order to reconstruct $S_n(\rho_x)$. Since, as shown later, $S_n(\rho_x)$ is strictly convex, w is a continuous parameter.

Here, we provide a full closed-form solution of this problem for the case when the claim $\{\rho_x\}$ consists of qubit states—notice that this is a *restriction* on the claim to be tested, rather than an *assumption* on the actual states—and the performed measurements are tests, that is, measurements with $n = 2$ outcomes. In particular, for any $\{\rho_x\}$, we explicitly derive (i) the measurements $\{\pi_{y|w}\}$ generating a correlation at the boundary of $S_2(\rho_x)$ for *any arbitrarily given direction* w; and (ii) the *full closed-form characterization* of $S_2(\rho_x)$. It turns out that $S_2(\rho_x)$ is given by the convex hull of the two isolated points 0 and u (vectors with null and unit entries, respectively) and the ellipsoid given by the system:

$$\begin{aligned} &(\mathbb{1} - Q^{-1}Q)(p - \tfrac{1}{2}u) = 0, \\ &(p - \tfrac{1}{2}u)^T Q^{-1}(p - \tfrac{1}{2}u) \leqslant 1, \end{aligned} \tag{1}$$

where $Q_{x_0,x_1} = \frac{1}{2}\mathrm{Tr}[\rho_{x_0}\rho_{x_1}] - \frac{1}{4}$. This situation is represented in Fig. 1. As applications, we explicitly discuss the case where $m = 2$ and $\{\rho_x\}$ are pure states, and the case where $\{\rho_x\}$ are distributed on the m vertices of a regular polygon on the Bloch equatorial plane.

Our results share analogies with previous works on device-independent testing of quantum dimension [1–4]. Notice, however, that therein the aim is to test a specific scalar property of states $\{\rho_x\}$ rather than their most general operatorial form, and the set of correlations is probed along an arbitrarily chosen direction rather than being fully reconstructed. Moreover, the present author has recently addressed the very related problems of device-independent tests of quantum channels [5–7] and measurements [8,9].

[*] cqtmda@nus.edu.sg

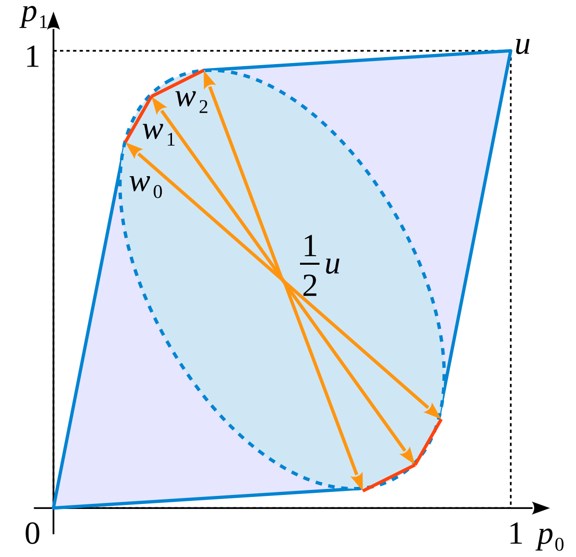


FIG. 1. Our results admit a bidimensional geometrical representation for the case of $m = 2$ states $\{\rho_x\}$. For any direction w (yellow vectors) in the space of correlations, we provide the experimenter with the measurements $\{\pi_{y|w}\}$ generating a correlation that lies on the boundary of $S_2(\rho_x)$ if the measured states are $\{\rho_x\}$. To check if this is the case, we provide the theoretician with a full closed-form characterization of $S_2(\rho_x)$, which turns out to be given by the convex hull (blue area) of 0 and u and the ellipse (blue dashed line) given by Eqs. (1).

II. EXPERIMENTAL OBSERVATIONS

We will make use of standard definitions and results in quantum information theory [10]. Any quantum state is represented by a density matrix ρ, that is, a unit-trace positive semidefinite operator. Any quantum measurement is represented by a positive operator-valued measure (POVM), that is, a collection $\{\pi_y\}$ of positive semidefinite operators such that $\sum_y \pi_y = \mathbb{1}$. The conditional probability $p_{y|x}$ of outcome y given input state ρ_x is given by the Born rule, that is, $p_{y|x} = \mathrm{Tr}[\rho_x \pi_y]$.

The experimenter claims to be able to prepare states $\{\rho_x\}$ and to measure them. Their task is to support such claims by generating all the correlations at the boundary of $S_n(\rho_x)$. To this aim, for any direction w in the space of correlations, the experimenter must measure the POVM $\{\pi_{y|w}\}$ that generates the correlation $p_{y|x} := \mathrm{Tr}[\rho_x \pi_{y|w}]$ that maximizes $p^T w$. In this section, we derive any such POVM for any given $\{\rho_x\}$ and w.

Formally, $\{\pi_{y|w}\}$ is given by the solution of the following optimization problem:

$$W(\rho_x, w) := \max_{\substack{\{\pi_y \geqslant 0\} \\ \sum_y \pi_y = \mathbb{1}}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-2} w_{x,y} \, \mathrm{Tr}[\rho_x \pi_y]. \tag{2}$$

In the following, we make the restriction $n = 2$, hence p and w are column vectors with m entries. Therefore, the maximum in Eq. (2) is attained when π_0 is the projector on $\mathrm{Pos}(\sum_x w_x \rho_x)$, where $\mathrm{Pos}(\cdot)$ denotes the positive part of operator $(\cdot)$, and in this case one has

$$W(\rho_x, w) = \mathrm{Tr}\left[\mathrm{Pos}\left(\sum_x w_x \rho_x\right)\right]. \tag{3}$$

Hence, our first result provides a closed-form characterization of the POVM $\{\pi_{y|w}\}$ achieving the correlation p at the boundary of $S_2(\rho_x)$ that maximizes $p^T w$, for any given family $\{\rho_x\}$ of states and direction w.

Proposition 1. For any family $\{\rho_x\}$ of states and direction w in the space of correlations, the POVM $\{\pi_{y|w}\}$ generating the correlation $p_{y|x} := \mathrm{Tr}[\rho_x \pi_{y|w}]$ on the boundary of $S_2(\rho_x)$ that maximizes $p^T w$ is such that $\pi_{0,w}$ is the projector on $\mathrm{Pos}(\sum_x w_x \rho_x)$ and $\pi_{1|w} = \mathbb{1} - \pi_{0|w}$.

Proposition 1 restricts the set of POVMs $\{\pi_{y|w}\}$ that need to be measured. Indeed, whenever $\mathrm{Pos}\,(\sum_x w_x \rho_x)$ has rank zero or two, the corresponding correlation p is trivial (i.e., $p = 0$ or $p = u$, respectively), thus direction w does not need to be probed.

III. THEORETICAL PREDICTIONS

The theoretician does not believe any of the claims made by the experimenter about the experimental setup, in particular about the set of POVMs $\{\pi_{y|w}\}$. Their task is to test such claims by comparing the observed correlations with $S_2(\rho_x)$. To this aim, in this section we provide a full closed-form characterization of $S_2(\rho_x)$ under the restriction that $\{\rho_x\}$ are qubit states.

The set $S_2(\rho_x)$ is recovered by further optimizing $W(\rho_x, w)$, as given by Eq. (3), over any direction w, that is,

$$S_2(\rho_x) = \{p \mid p = \max_w [p^T w - W(\rho_x, w)] \leqslant 0\}. \tag{4}$$

Upon fixing a computational basis, $\{\rho_x\}$ can be decomposed in terms of Pauli matrices $\{\sigma_k\}$ as follows:

$$\rho_x = \frac{1}{2}\mathbb{1} + \sum_{k=1}^{3} S_{x,k} \sigma_k,$$

where $S_{x,k} := \frac{1}{2}\mathrm{Tr}[\rho_x \sigma_k]$. Of course, our result will be independent of the choice of computational basis.

It is then a simple computation to find that

$$W(\rho_x, w) = \max\left(0,\ ||w||_1,\ \frac{1}{2}||w||_1 + ||S^T w||_2\right),$$

where $||\cdot||_p$ denotes the p norm of vector $(\cdot)$. The maximum is achieved by 0 and $||w||_1$ if $\{\pi_{y|w}\}$ is trivial ($\pi_{0|w} = 0$ and $\pi_{0|w} = \mathbb{1}$, respectively), and by $\frac{1}{2}||w||_1 + ||S^T w||_2$ if $\{\pi_{y|w}\}$ is rank-one projective. If $\{\pi_{y|x}\}$ is trivial, the optimization problem in Eq. (4) becomes

$$\begin{aligned} &\max\nolimits_w p^T w \leqslant 0, && \text{if } \pi_0 = 0, \\ &\max\nolimits_w (p - \tfrac{1}{2}u)^T w \leqslant 0, && \text{if } \pi_0 = \mathbb{1}, \end{aligned}$$

which, as expected, are satisfied if and only if $p = 0$ and $p = u$, respectively.

If, however, $\{\pi_{y|w}\}$ is rank-one projective, the optimization problem in Eq. (4) becomes

$$\max_w \left[\left(p - \frac{1}{2}u\right)^T w - ||S^T w||_2\right] \leqslant 0. \tag{5}$$

This optimization problem is formally equal to that in Eq. (5) of Ref. [8], where the problem of device-independent tests of quantum measurements was addressed. Notice, however, that the operational interpretation and, accordingly, the mathematical representation of the symbols are different. For example, in Ref. [8] p represents the probability distribution of the outcomes of a POVM, and thus $\sum_y p_y = 1$, while here p represents the vector of probabilities of outcome π_0 given states ρ_x, and thus there is no linear constraint on the sum of its elements. Analogous differences hold for u (t in Ref. [8]) and S. The consequences of these differences on the solution of Eq. (5) will be discussed at the end of this section.

Since Eq. (5) is left invariant by the transformation $w \to w = |(p - \frac{1}{2}u)^T w|^{-1} w$ (we recall that w only represents a direction in the space of correlations), without loss of generality one can take $(p - \frac{1}{2}u)^T w = 0, \pm 1$. When $(p - \frac{1}{2}u)^T w = 0, -1$, the inequality in Eq. (5) is of course satisfied, thus let $(p - \frac{1}{2}u)^T w = 1$. Equation (5) becomes

$$\min_{\substack{w \\ [p-(1/2)u]^T w = 1}} \quad ||S^T w||_2^2 \geqslant 1, \tag{6}$$

that is, a linearly constrained quadratic-programming problem.

Let us denote with Q the real symmetric matrix $Q := SS^T$. Upon denoting with $(\cdot)^{-1}$ the Moore-Penrose pseudoinverse [11] of matrix $(\cdot)$, one has that $\mathbb{1} - Q^{-1}Q$ is the orthogonal projector on the kernel of Q.

Let us first show that a necessary condition for $p \in S_2(\rho_x)$ is that $p - \frac{1}{2}u$ is orthogonal to the kernel of Q. Indeed, suppose that $(p - \frac{1}{2}u)^T(\mathbb{1} - Q^{-1}Q)(p - \frac{1}{2}u)>0$. By setting

$$w = \frac{(\mathbb{1} - Q^{-1}Q)\big(p - \frac{1}{2}u\big)}{\big(p - \frac{1}{2}u\big)^T(\mathbb{1} - Q^{-1}Q)\big(p - \frac{1}{2}u\big)},$$

one immediately has that the constraint $(p - \frac{1}{2}u)^T w = 1$ is verified, and that $||S^T w||_2^2 = 0$. Therefore, by Eq. (6) $p \notin S(\rho_x)$.

Let then $p - \frac{1}{2}u$ belong to the kernel of Q. In this case, we can take without loss of generality w in Eq. (6) to have support on the kernel of Q. Then, it is known [12] that Eq. (6) is solved by

$$\begin{aligned} Qw &= -\lambda(p - \tfrac{1}{2}u), \\ (p - \tfrac{1}{2}u)^T w &= 1, \end{aligned} \tag{7}$$

where λ is a Lagrange multiplier. The system in Eq. (7) is solved by [11]

$$\begin{aligned} &w = -\lambda Q^{-1}(p - \tfrac{1}{2}u) + (\mathbb{1} - Q^{-1}Q)v, \\ &(p - \tfrac{1}{2}u)^T\big[(\mathbb{1} - Q^{-1}Q)v - \lambda Q^{-1}(p - \tfrac{1}{2}u)\big] = 1. \end{aligned} \tag{8}$$

If $(p - \frac{1}{2}u)^T Q^{-1}(p - \frac{1}{2}u)>0$, by taking $v = 0$,

$$\lambda = \left[\left(p - \frac{1}{2}u\right)^T Q^{-1}\left(p - \frac{1}{2}u\right)\right]^{-1},$$

and $w = \lambda Q^{-1}(p - \frac{1}{2}u)$, one has that the system in Eq. (8) is verified, as well as the constraint $(p - \frac{1}{2}u)^T w = 1$. Hence, w is the solution of the optimization problem in Eq. (6), and one has $||S^T w||_2^2 = \lambda$, that is, $p \in S_2(\rho_x)$ if and only if $(p - \frac{1}{2}u)^T Q^{-1}(p - \frac{1}{2}u) \leqslant 1$. If instead $(p - \frac{1}{2}u)^T Q^{-1}(p - \frac{1}{2}u) = 0$, one has $p = \frac{1}{2}u$, which is again $p \in S_2(\rho_x)$.

Hence, the solution of the optimization problem in Eq. (6) is given by

$$\begin{aligned} &(\mathbb{1} - Q^{-1}Q)(p - \tfrac{1}{2}u) = 0, \\ &(p - \tfrac{1}{2}u)^T Q^{-1}(p - \tfrac{1}{2}u) \leqslant 1. \end{aligned} \tag{9}$$

Finally, by explicit computation it immediately follows that Q is given by $Q_{x_0,x_1} = \frac{1}{2}\operatorname{Tr}[\rho_{x_0}\rho_{x_1}] - \frac{1}{4}$, thus as expected the system in Eq. (9) does not depend on the choice of computational basis.

Then, our second main result provides a full closed-form characterization of the set $S_2(\rho_x)$ of correlations compatible with any arbitrary given qubit family $\{\rho_x\}$ of states.

Proposition 2. The set $S_2(\rho_x)$ of correlations generated by a given family $\{\rho_x\}$ of qubit states and any test $\{\pi_y\}$ is given by

$$S_2(\rho_x) = \operatorname{conv}\{0, u, \text{Eq. (9)}\},$$

where $Q_{x_0,x_1} = \frac{1}{2}\operatorname{Tr}[\rho_{x_0}\rho_{x_1}] - \frac{1}{4}$.

Let us provide a geometrical interpretation of Proposition 2. The system of equalities in Eq. (9) represents rank$(\mathbb{1} - Q^{-1}Q)$ linear constraints, while the inequality represents an m-dimensional cylinder with (rank Q)-dimensional hyperellipsoidal section. Thus, Eq. (9) represents a (rank Q)-dimensional hyperellipsoid embedded in an m-dimensional space. Since rank $Q \leqslant 3$, we have that Eq. (9) respresents a (possibly degenerate) ellipsoid. Notice as a comparison that, while in this case $S_2(\rho_x)$ includes the two isolated correlations 0 and u, in the case of the device-independent tests of quantum measurements [8] no isolated correlations are included.

IV. COMPARISON

Finally, we discuss the comparison of the set of correlations observed by the experimenter according to Proposition 1 and the set $S_2(\rho_x)$ predicted by the theoretician according to Proposition 2. Notice first that the inclusion relation $S_2(\rho_x) \supseteq S_2(\rho'_x)$ induces a partial ordering among families of quantum states $\{\rho_x\}$ and $\{\rho'_x\}$, that is, $\{\rho_x\} \succeq \{\rho'_x\} \Leftrightarrow S_2(\rho_x) \supseteq S_2(\rho'_x)$. Of course, if the experimenter produces *some* correlation not in $S_2(\rho_x)$, the theoretician must conclude that the prepared states $\{\rho'_x\}$ are such that

$$\{\rho'_x\} \not\preceq \{\rho_x\}. \tag{10}$$

However, if the experimenter produces *all* the extremal correlations of $S_2(\rho_x)$ (as per Proposition 1), the theoretician must conclude that the prepared states $\{\rho'_x\}$ are such that

$$\{\rho'_x\} \succeq \{\rho_x\}. \tag{11}$$

Since the ordering $\succeq$ is partial, Eq. (11) is of course strictly stronger than Eq. (10), that is, Eq. (11) implies Eq. (10) but the vice versa is false. Informally, Eq. (11) allows the theoretician to lower bound the "ability" to create input-output correlations of the states prepared by the experimenter.

An even stronger result can be achieved when $m = 2$. In this case Proposition 2 provides the full closed-form quantum relative Lorenz curve for any pair $\{\rho_0, \rho_1\}$ of qubit state, as illustrated by Fig. 1. Quantum relative Lorenz curves have been recently introduced by Buscemi and Gour [13] in the context of quantum relative majorization. As a consequence of a result therein, in turn based on a previous result by Alberti and Uhlmann [14], under the additional assumption that the prepared states $\{\rho'_0, \rho'_1\}$ are qubit states, Eq. (11) implies the existence of a quantum channel $\mathcal{C}$, that is, a completely positive trace-preserving linear map, such that

$$\mathcal{C}(\rho'_x) = \rho_x, \qquad x = 1, 2. \tag{12}$$

Therefore, Eq. (12) means that the states $\{\rho'_x\}$ prepared by the experimenter are less noisy than the claimed states $\{\rho_x\}$. However, it is known [15] that this implication fails if the assumption that the prepared states $\{\rho'_x\}$ are qubit states is relaxed.

V. APPLICATIONS

As an application of the case $m = 2$, we consider any pair of pure states $\rho_x = |\psi_x\rangle\langle\psi_x|$, that can be written without loss of generality as

$$|\psi_0\rangle = |0\rangle\,, \qquad |\psi_1\rangle = \cos\frac{\alpha}{2}\,|0\rangle + \sin\frac{\alpha}{2}\,|1\rangle\,.$$

Since $|\langle\psi_0|\psi_1\rangle|^2 = \cos^2\frac{\alpha}{2}$, matrix $Q_{x_0,x_1} := \frac{1}{2}|\langle\psi_{x_0}|\psi_{x_1}\rangle|^2 - \frac{1}{4}$ is given by $Q = [(1+\cos\alpha)v_+v_+^\dagger + (1-\cos\alpha)v_-v_-^\dagger]/4$, where $v_\pm = 1/\sqrt{2}(1, \pm 1)^T$. If $\alpha \neq 0, \pi$, the system in Eq. (9) becomes

$$\frac{1}{1+\cos\alpha}(p_0 + p_1 - 1)^2 + \frac{1}{1-\cos\alpha}(p_0 - p_1)^2 \leqslant \frac{1}{2}.$$

If $\alpha = 0$ or $\alpha = \pi$, that is, $|\psi_0\rangle = |\psi_1\rangle$ or $\langle\psi_0|\psi_1\rangle = 0$, respectively, the system in Eq. (9) trivially becomes $p_0 = p_1$ or $p_0 = 1 - p_1$, respectively.

As an application of the general case we consider m pure states $\rho_x = |\phi_x\rangle\langle\phi_x|$ uniformly distributed in the Bloch equatorial plane, that can be written without loss of generality as

$$|\phi_x\rangle = \cos\frac{\pi x}{m}\,|0\rangle + \sin\frac{\pi x}{m}\,|1\rangle\,.$$

Since $|\langle\phi_{x_0}|\phi_{x_1}\rangle|^2 = \cos^2\frac{\pi(x_0 - x_1)}{m}$, matrix $Q_{x_0,x_1} := \frac{1}{2}|\,\langle\phi_{x_0}|\phi_{x_1}\rangle\,|^2 - \frac{1}{4}$ is circulant, that is, $Q_{x_0+k,x_1+k} = Q_{x_0,x_1}$ for any x_0, x_1, and k. Therefore, it is lengthy but not difficult to show that its eigenvalues are given by

$$\begin{aligned}\lambda_j &= \frac{1}{4}\sum_{k=0}^{m-1}\cos\frac{2\pi k}{m}\exp\frac{2\pi i j(m-k)}{m}\\ &= \frac{\left(e^{2\pi i j} - 1\right)\left(e^{2\pi i j/m} + e^{2\pi i(j+2)/m} - 2e^{2\pi i/m}\right)}{8\left(e^{2\pi i/m} - e^{2\pi i j/m}\right)\left(e^{2\pi i(j+1)/m} - 1\right)}.\end{aligned}$$

Hence, one has that $\lambda_1 = \lambda_{m-1} = m/8$ and $\lambda_j = 0$ otherwise, and two eigenvectors $v_\pm$ corresponding to non-null eigenvalues are given by $v_\pm$ where $(v_\pm)_k := \frac{1}{\sqrt{m}}\exp(\pm\frac{2\pi i k}{m})$. Accordingly, one has that $Q = \frac{m}{8}(v_+v_+^\dagger + v_-v_-^\dagger)$, and the system in Eq. (9) becomes

$$\begin{aligned}&(\mathbb{1} - v_+v_+^\dagger - v_-v_-^\dagger)p = 0,\\ &||v_+^\dagger p||_2^2 \leqslant \frac{16}{m}.\end{aligned}$$

For instance, consider the case of two mutually unbiased bases [16] (MUBs), obtained for $m = 4$. MUBs have applications, e.g., in classical communications over quantum channels [17], quantum cryptography [18], and locking of classical information in quantum states [19]. One has that $v_\pm = (1, \pm i, -1, \mp i)^T$, from which the system in Eq. (9) becomes

$$\begin{aligned}&p_0 + p_2 = p_1 + p_3 = 1,\\ &||p||_2^2 \leqslant \tfrac{3}{2}.\end{aligned}$$

VI. CONCLUSION

In this work we have addressed the problem of constructing a correspondence between any given family $\{\rho_x\}$ of m quantum states and the set $S_n(\rho_x)$ of observable correlations they can generate for any POVM $\{\pi_y\}$. The problem has been framed as a game involving an experimenter, claiming to be able to prepare some family $\{\rho_x\}$ of states, and a theoretician, willing to trust observed correlations only. For any such claim $\{\rho_x\}$, the optimal strategy consists of providing (i) to the experimenter, the measurement $\{\pi_{y|w}\}$ that generates a correlation on the boundary of $S_n(\rho_x)$ for *any* given direction w, and (ii) to the theoretician, the *full* characterization of $S_n(\rho_x)$. Comparing the correlations observed in (i) with those predicted by (ii) corresponds to device-independently testing the states. While no assumption has been made about the *actual* states and measurements, we have derived the optimal strategy in *closed form* for the case when the *claim* consists of qubit states and the performed measurements are tests, that is, measurements with $n = 2$ outcomes, and discussed the geometrical interpretation of our results. As applications, we have specified our results to the case of any pair of pure states and to the case of pure states uniformly distributed on the Bloch equatorial plane.

Natural open problems include relaxing some of the restrictions we considered, e.g., considering POVMs with arbitrary number of outcomes and states in arbitrary dimension. Furthermore, the characterization of the set $S_n(\rho_x)$ of correlations compatible with an arbitrary dimensional family $\{\rho_x\}$ of $m = 2$ states might prove to be the key to solve a well-known longstanding conjecture by Shor [20], based on numerical work by Fuchs and Peres: whether the accessible information of any binary ensemble is attained by a von Neumann POVM. Finally, the full closed-form characterization of the quantum relative Lorenz curve for qubit states provided by Proposition 2 naturally leads to applications in quantum resource theories [21], within the general framework provided by the quantum Blackwell theorem [22].

We conclude by noticing that our results are remarkably suitable for experimental implementation. For any family of qubit states that an experimenter claims to be able to prepare, our framework only requires von Neumann measurements to be performed in order to experimentally reconstruct the entire boundary of the set of compatible correlations.

ACKNOWLEDGMENTS

M.D. is grateful to Sarah Brandsen and Francesco Buscemi for valuable discussions, comments, and suggestions. This research is supported by the National Research Fund and the Ministry of Education, Singapore, under the Research Centres of Excellence programme.

[1] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).

[2] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, Nat. Phys. **8**, 588 (2012).

[3] H. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nat. Phys. **8**, 592 (2012).

[4] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, Robustness of device independent dimension witnesses, Phys. Rev. A **86**, 042312 (2012).

[5] M. Dall'Arno, S. Brandsen, and F. Buscemi, Device-independent tests of quantum channels, Proc. R. Soc. A **473**, 20160721 (2017).

[6] F. Buscemi and M. Dall'Arno, Data-driven inference of physical devices: Theory and implementation, arXiv:1805.01159.

[7] I. Agresti, D. Poderini, G. Carvacho, L. Sarra, R. Chaves, F. Buscemi, M. Dall'Arno, and F. Sciarrino, Experimental semi-device-independent tests of quantum channels, Quantum Sci. Technol. **4**, 035004 (2019).

[8] M. Dall'Arno, S. Brandsen, F. Buscemi, and V. Vedral, Device-Independent Tests of Quantum Measurements, Phys. Rev. Lett. **118**, 250501 (2017).

[9] M. Dall'Arno, F. Buscemi, A. Bisio, and A. Tosini, Data-driven inference, reconstruction, and observational completeness of quantum devices, arXiv:1812.08470.

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).

[11] B.-I. Adi and T. N. E. Greville, *Generalized Inverses* (Springer-Verlag, Berlin, 2003).

[12] S. P. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).

[13] F. Buscemi and G. Gour, Quantum relative Lorenz curves, Phys. Rev. A **95**, 012110 (2017).

[14] P. M. Alberti and A. Uhlmann, A problem relating to positive linear maps on matrix algebras, Rep. Math. Phys. **18**, 163 (1980).

[15] K. Matsumoto, An example of a quantum statistical model which cannot be mapped to a less informative one by any trace preserving positive map, arXiv:1409.5658.

[16] A. Klappenecker and M. Roetteler, *Mutually Unbiased Bases are Complex Projective 2-Designs*, Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 2005) (IEEE, NY, 2005), p. 1740.

[17] M. Dall'Arno, Accessible information and informational power of quantum 2-designs, Phys. Rev. A **90**, 052311 (2014).

[18] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[19] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Locking Classical Information in Quantum States, Phys. Rev. Lett. **92**, 067902 (2004).

[20] Peter W. Shor, On the number of elements needed in a POVM attaining the accessible information, Quant. Commun., Comput. Meas. **3**, 107 (2002).

[21] M. Dall'Arno and F. Buscemi (unpublished).

[22] F. Buscemi, Comparison of quantum statistical models: Equivalent conditions for sufficiency, Commun. Math. Phys. **310**, 625 (2012).