# Device-Independent Tests of Quantum Measurements

Michele Dall'Arno,[1,*] Sarah Brandsen,[1,2,†] Francesco Buscemi,[3,‡] and Vlatko Vedral[4,1,§]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2 117543, Singapore*
[2]*California Institute of Technology, 1200 E. California Blvd, Pasadena, California 91125, USA*
[3]*Graduate School of Informatics, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan*
[4]*Atomic and Laser Physics, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX13PU, United Kingdom*

We consider the problem of characterizing the set of input-output correlations that can be generated by an arbitrarily given quantum measurement. Our main result is to provide a closed-form, full characterization of such a set for any qubit measurement, and to discuss its geometrical interpretation. As applications, we further specify our results to the cases of real and complex symmetric, informationally complete measurements and mutually unbiased bases of a qubit, in the presence of isotropic noise. Our results provide the optimal device-independent tests of quantum measurements.

In operational quantum theory, it is a natural question to ask whether a given data sample, provided in the form of a conditional probability distribution representing the measured input-output correlation, is compatible with a particular hypothesis about the theoretical model underlying the experiment. A theoretical model can be more or less specific: for example, it could consist only of a general hypothesis about the theory describing the physics, as in the case in Bell tests [1–3], or it could be extremely detailed, as in the case of a tomographic reconstruction [4–6]. More generally, a hypothesis could be specific about a portion of the underlying model, while leaving the remaining elements completely uncharacterized.

Here, we address hypotheses about the measurement producing the final outcomes of the experiment. This is the problem of characterizing the set $\mathcal{S}(\pi)$ of all input-output correlations $p_{y|x} = \mathrm{Tr}[\rho_x \pi_y]$ compatible with an arbitrarily given quantum measurement $\pi := \{\pi_y\}$ (i.e., the hypothesis) and any family of input quantum states $\{\rho_x\}$, namely,

$$p_{y|x} = \mathrm{Tr}[\rho_x \ \pi_y] \ \longleftrightarrow \ x = \boxed{\rho_x} - \boxed{\pi_y} = y . \quad (1)$$

We first note that a correlation $p$ is compatible with measurement $\pi$ if and only if for any fixed $x$ there exists a state $\rho_x$ such that $p_{y|x} = \mathrm{Tr}[\rho_x \pi_y]$. Hence, $\mathcal{S}(\pi)$ is fully characterized by the range of $\pi$, namely, the set $\mathcal{S}_1(\pi)$ of output distributions $q_y = \mathrm{Tr}[\rho\pi_y]$ generated by $\pi$ for varying input state $\rho$. This is in stark contrast with the analogous problem of characterizing the set of correlations compatible with a given quantum channel, which in general requires more than one input [7].

Our main result is a closed-form characterization of the range $\mathcal{S}_1(\pi)$, and hence of the set $\mathcal{S}(\pi)$ of all compatible correlations, when the hypothesis $\pi$ is a qubit measurement. It turns out that an output distribution $q_y$ belongs to $\mathcal{S}_1(\pi)$ if and only if

$$\begin{cases} (\mathbb{1} - Q^+Q)(q - t) = 0, \\ (q - t)^T Q^+(q - t) \leq 1, \end{cases} \quad (2)$$

where 1 is the identity matrix, $t$ is the vector $t_y := \frac{1}{2}\mathrm{Tr}[\pi_y]$, $Q$ is the matrix $Q_{y_0,y_1} := \frac{1}{2}\mathrm{Tr}[\pi_{y_0}\pi_{y_1}] - \frac{1}{4}\mathrm{Tr}[\pi_{y_0}]\mathrm{Tr}[\pi_{y_1}]$, and $(\cdot)^+$ represents the Moore-Penrose pseudoinverse [8]. Imposing the system of equalities in Eq. (2) causes linear dependencies—if any—among measurement elements $\pi_y$ to emerge as linear constraints on the probabilities. Such linear dependencies are present, for example, in any overcomplete measurement. Provided that these constraints are satisfied, the inequality in Eq. (2) recasts—through the transformation $Q^+$—the set of distributions compatible with $\pi$ as an ellipsoid centered on distribution $t$. This in particular provides a simple and clear geometrical representation for the range of any qubit measurement.

As an application of our general results, we further simplify Eq. (2) for some relevant classes of qubit measurements, i.e., symmetric informationally complete (SIC) measurements [9] and mutually unbiased bases (MUBs) [10], both in the real and complex cases, and in the presence of isotropic noise. SIC measurements play a fundamental role in quantum tomography [4–6], quantum communication [11–17], and foundations of quantum theory [18–22], while MUBs are pivotal elements in quantum cryptography [23], entropic uncertainty relations [24–26], and the locking of classical information in quantum states [27].

Our results represent a further step towards characterizing timelike correlations compatible with quantum theory through device-independent (DI) tests [7]. The aim of DI tests is that of falsifying hypotheses about the underlying physical system, which is considered accessible only through the classical input-output correlations it generates. In particular, no assumptions are made about the underlying physical system or how such correlations have been generated. This approach has been considered in the

previous literature for the problems of falsifying hypotheses about the dimension [28–31] or the average entropy [32] of the input ensemble.

However, while here we provide a full characterization of $\mathcal{S}(\pi)$ [in particular, for the qubit case, the ellipsoid described in Eq. (2) can be plotted], the application of previous results [28–32] would allow one to probe $\mathcal{S}(\pi)$ along a fixed radial direction only. In this sense, our results provide optimal DI tests of quantum measurements, aimed at falsifying the hypothesis that an observed input-output correlation $p_{y|x}$ is generated by a given quantum measurement $\{\pi_y\}$.

*Characterization of $\mathcal{S}(\pi)$.*—We make use of standard results in quantum information theory [33]. Any quantum state $\rho$ is most generally described by a density matrix, namely, a positive semidefinite unit-trace operator. Any quantum measurement $\pi$ is most generally described by a positive operator-valued measure (POVM) $\pi := \{\pi_y\}$, namely, a set of positive semidefinite operators such that $\sum_y \pi_y = \mathbb{1}$.

For any POVM $\pi := \{\pi_y\}_{y=0}^{n-1}$, where $n$ denotes the number of elements, the set $\mathcal{S}(\pi)$ of compatible input-output correlations is formally defined as $\mathcal{S}(\pi) := \bigcup_{m=1}^{\infty} \mathcal{S}_m(\pi)$, where $\mathcal{S}_m(\pi)$ denotes the set of compatible conditional probability distributions $p := \{p_{y|x}\}$, upon the input of any set of $m$ unknown states $\{\rho_x\}$, that is,

$$\mathcal{S}_m(\pi) := \{p| \,\exists\, \{\rho_x\}_{x=0}^{m-1}\text{s.t.}\,p_{y|x} = \text{Tr}[\rho_x\pi_y]\}.$$

First, we notice that, for any fixed $m$, $\mathcal{S}_m(\pi)$ is convex: indeed, for any two sets $\{\rho_x\}$ and $\{\sigma_x\}$ of $m$ states, the conditional probability distribution $\{p_{y|x} := \lambda\text{Tr}[\sigma_x\pi_y] + (1-\lambda)\text{Tr}[\rho_x\pi_y] = \text{Tr}[(\lambda\sigma_x + (1-\lambda)\rho_x)\pi_y]\}$ belongs to $\mathcal{S}_m(\pi)$, since $\{\lambda\sigma_x + (1-\lambda)\rho_x\}$ is itself a set of $m$ states.

Therefore, as a consequence of the hyperplane separation theorem [34], it is possible to detect any conditional probability $p$ lying outside the set $\mathcal{S}_m(\pi)$ through the violation of an inequality involving a linear function of $p$ [35]. More explicitly, $p \in \mathcal{S}_m(\pi)$ if and only if

$$\max_w [\text{Tr}[w^T p] - W(\pi, w)] \leq 0, \qquad (3)$$

where the maximum is over any real matrix $w$ (with the same dimensions as $p$), referred to as a witness, and $W(\pi, w)$ is defined as $\max_{q \in \mathcal{S}_m(\pi)} \text{Tr}[w^T q]$ and is referred to as a witness threshold. Notice that Eq. (3) corresponds to an unconstrained maximin optimization problem.

As a preliminary remark, let us discuss two properties of Eq. (3) that will be relevant in the following. Since $W(\pi, w)$ is a positive homogeneous function, i.e., $W(\pi, \alpha w) = \alpha W(\pi, w)$ for any $\alpha \geq 0$, the rescaling transformation $w \to \alpha w$ for any $\alpha > 0$ leaves Eq. (3) invariant. Moreover, by direct computation it follows that Eq. (3) is invariant under the shifting transformation $w \to w'$, where $w'_{x,y} := w_{x,y} + k_x$, for any $\vec{k}$.

Let us first solve the optimization appearing in the definition of $W(\pi, w)$. One has

$$W(\pi, w) := \sup_{\{\rho_x\}} \sum_x \text{Tr}\left[\rho_x\left(\sum_y w_{x,y}\pi_y\right)\right]$$

$$\leq \sum_x \sup_{\{\rho_x\}} \text{Tr}\left[\rho_x\left(\sum_y w_{x,y}\pi_y\right)\right],$$

where the inequality is saturated if and only if $\{\rho_x := |\phi_x\rangle\langle\phi_x|\}$, where $\{|\phi_x\rangle\}$ are the eigenvectors corresponding to the largest eigenvalue of $\sum_y w_{x,y}\pi_y$. In this case one has $\text{Tr}[\rho_x(\sum_y w_{x,y}\pi_y)] = \lambda_{\max}(\sum_y w_{x,y}\pi_y)$, where $\lambda_{\max}(\cdot)$ denotes the largest eigenvalue of $(\cdot)$. Notice that $\lambda_{\max}(\cdot)$ is a convex function [34]. Then, our first preliminary result immediately follows.

**Proposition 1.** (Witness threshold) For any POVM $\pi$ and any witness $w$, the witness threshold $W(\pi, w)$ is given by

$$W(\pi, w) = \sum_x \lambda_{\max}\left(\sum_y w_{x,y}\pi_y\right). \qquad (4)$$

Proposition 1 recasts the optimization in Eq. (3) as an unconstrained concave maximization problem over any witness $w$.

The transformation $w \to w'$, where $w'_{x,y} := \mu_x w_{x,y}$ with $\mu$ a probability distribution, i.e., $\|\mu\|_1 = 1$ and $\mu \geq 0$ [here and in the following $\|v\|_p := (\sum_k v_k^p)^{1/p}$ denotes the $p$ norm of vector $v$], maps Eq. (3) into

$$\max_{\substack{\mu \geq 0 \\ \|\mu\|_1 = 1}} \max_w \sum_x \mu_x\left[\sum_y p_{y|x}w_{x,y} - \lambda_{\max}\left(\sum_y w_{x,y}\pi_y\right)\right] \leq 0,$$

where the maximum over probability distributions $\mu$ is of course attained when $\mu_x = \delta_{x,x^*}$ with

$$x^* = \arg\max_x \max_w \left[\sum_y p_{y|x}w_{x,y} - \lambda_{\max}\left(\sum_y w_{x,y}\pi_y\right)\right].$$

To summarize, the above calculation shows that the optimization of the witness $w$ can be done independently for each $x$. We therefore obtain our second preliminary result.

**Proposition 2.** For any given POVM $\pi := \{\pi_y\}$, a conditional probability distribution $p_{y|x}$ belongs to $\mathcal{S}(\pi)$ if and only if, for any fixed $x = \bar{x}$, $q_y := \{p_{y|\bar{x}}\}$ belongs to $\mathcal{S}_1(\pi)$.

Because of Proposition 2, without loss of generality we solve the optimization problem in Eq. (3) when $m = 1$. Hence, in the following we will consider output distributions $q = \{q_y\}$ rather than input-output distributions $p = \{p_{y|x}\}$.

*Range of qubit measurements.*—In what follows, we restrict our attention to the case of qubit POVM $\pi$. Let $t \in \mathbb{R}^n$ and $S \in \mathbb{R}^{n \times 3}$ be defined by $t_y := \text{Tr}[\pi_y]/2$ and $S_{y,j} := \text{Tr}[\pi_y\sigma_j]/2$, where $\{\sigma_j\}_{j=1}^3$ are the Pauli matrices $\{\sigma_1 \equiv X, \sigma_2 \equiv Y, \sigma_3 \equiv Z\}$ for some fixed computational basis, so one has $\pi_y = t_y\mathbb{1} + \sum_{k=1}^3 S_{y,k}\sigma_k$. Naturally, our result will be independent of the particular choice of the computational basis. With this parametrization, the witness threshold in Eq. (4) becomes

$$W(\pi, w) = t^T w + \|S^T w\|_2.$$

Accordingly, Eq. (3) becomes

$$\max_w [(q - t)^T w - \|S^T w\|_2] \leq 0. \tag{5}$$

For any $w$ such that $(q - t)^T w \neq 0$, let $\alpha := |(q - t)^T w|$ and $w' := \alpha^{-1} w$, and let $w' = w$ otherwise. The transformation $w \to w'$ leaves Eq. (3) invariant. So Eq. (5) becomes

$$\max_{\substack{w \\ (q-t)^T w = \pm 1, 0}} [(q - t)^T w - \|S^T w\|_2] \leq 0. \tag{6}$$

If $(q - t)^T w = -1$, 0, one has that Eq. (6) is trivially satisfied. Thus, we focus in the following on the case $(q - t)^T w = 1$, when Eq. (6) becomes

$$\min_{\substack{w \\ (q-t)^T w = 1}} \|S^T w\|_2^2 \geq 1. \tag{7}$$

The optimization in Eq. (7) is an equality-constrained quadratic problem. Its solution leads to our second main result.

**Theorem 1** (Range of qubit measurements) An output distribution $q := \{q_y\}$ belongs to the range $\mathcal{S}_1(\pi)$ of any given qubit measurement $\pi := \{\pi_y\}$ if and only if

$$\begin{cases} (\mathbb{1} - Q^+ Q)(q - t) = 0, \\ (q - t)^T Q^+ (q - t) \leq 1, \end{cases} \tag{8}$$

where 1 is the identity matrix, $t$ is the vector $t_y := \frac{1}{2} \mathrm{Tr}[\pi_y]$, $Q$ is the matrix $Q_{y_0, y_1} := \frac{1}{2} \mathrm{Tr}[\pi_{y_0} \pi_{y_1}] - \frac{1}{4} \mathrm{Tr}[\pi_{y_0}] \mathrm{Tr}[\pi_{y_1}]$, and $(\cdot)^+$ represents the Moore-Penrose pseudoinverse.

Before proceeding to prove Theorem 1, let us discuss the role of the matrix $Q$ and provide a geometrical interpretation.

The matrix $Q$, which has a form resembling a covariance matrix, quantifies the statistical overlap of POVM elements. Indeed, as proved in Proposition 3 in the Supplemental Material [36], element $Q_{y_0, y_1}$ is minimized and equal to $-1/4$ if $\pi_{y_0}$ and $\pi_{y_1}$ are rank-1, unit-trace, orthogonal effects. Also, element $Q_{y_0, y_1}$ is maximized and equal to $1/4$ if $y_0 = y_1$ and $\pi_{y_0}$ is a rank-1, unit-trace effect. Finally, element $Q_{y_0, y_1} = 0$ if $\pi_{y_0}$ and $\pi_{y_1}$ are both proportional to the identity operator.

Let us first focus on the system of equalities in Eq. (8). Denoting by $l$ the maximum number of linearly independent elements in $\{\pi_y\}$, the number of equations in the system is $n - l + 1$, each identifying an $(n - 1)$-dimensional hyperplane. This comes from the fact that, by definition, one has $\mathrm{rank} Q^+ Q = l - 1$, which also implies $\mathrm{rank}(\mathbb{1} - Q^+ Q) = n - l + 1$. Moreover, when all POVM elements are linearly independent, namely, $n = l$, the only equation in the system is $\|q\|_1 = \|t\|_1 = 1$. This follows by explicit computation: in this case, $(\mathbb{1} - Q^+ Q)$ turns out to coincide with the rank-1 projector along the vector with all unit entries. Hence, in general, the system of equalities in Eq. (8) represents linear dependencies among POVM elements $\{\pi_y\}$.

Let us now focus on the inequality in Eq. (8), which represents an $n$-dimensional degenerate (hyper)ellipsoid centered on probability $t$. More precisely, the inequality represents the Cartesian product of $\mathbb{R}^{n-3}$ with a three-dimensional ellipsoid, or $\mathbb{R}^{n-2}$ with a two-dimensional ellipse, or $\mathbb{R}^{n-1}$ with a one-dimensional segment, depending on whether $l = 4$, 3, 2, respectively. Accordingly, the solution of Eq. (8) is an ellipsoid, an ellipse, or a segment, respectively, embedded in $\mathbb{R}^n$.

We now turn to the proof of Theorem 1.

*Proof.*—By explicit computation, it immediately follows that matrix $Q$ defined in the statement can be written in terms of matrix $S$ in Eq. (7) as $Q = SS^T$. Indeed, using the decomposition $\pi_y = t_y \mathbb{1} + \sum_{k=1}^3 S_{y,k} \sigma_k$ one immediately has $\frac{1}{2} \mathrm{Tr}[\pi_{y_0} \pi_{y_1}] = t_{y_0} t_{y_1} + \sum_{k=1}^3 S_{y_0, k} S_{y_1, k}$.

Equality-constrained quadratic problems can be solved explicitly [8,34]. In the case of Eq. (7) we thus have

$$\begin{cases} w = -\lambda Q^+ (q - t) + (\mathbb{1} - Q^+ Q) v, \\ \lambda (q - t)^T Q^+ (q - t) = (q - t)(\mathbb{1} - Q^+ Q) v - 1, \end{cases} \tag{9}$$

where $\lambda$ is a Lagrange multiplier and $v$ is an arbitrary vector.

Notice that $(q - t)^T Q^+ (q - t) \geq 0$ since $Q^+ \geq 0$ and that $(q - t)^T (\mathbb{1} - Q^+ Q)(q - t) \geq 0$ since $(\mathbb{1} - Q^+ Q)$ is a projector. We need to distinguish four cases in Eqs. (9).

*First case.* Let $(q - t)^T Q^+ (q - t) > 0$ and $(q - t)^T (\mathbb{1} - Q^+ Q)(q - t) > 0$. Upon taking

$$v = \frac{(\mathbb{1} - Q^+ Q)(q - t)}{(q - t)^T (\mathbb{1} - Q^+ Q)(q - t)},$$

one has $\lambda = 0$ and $w = v$. Therefore, $\|S^T w\|_2^2 = 0$; namely, probability $q$ is incompatible with POVM $\pi$.

*Second case.* Let $(q - t)^T Q^+ (q - t) = 0$ and $(q - t)^T (\mathbb{1} - Q^+ Q)(q - t) > 0$. Upon taking $v$ again as above, one has that $\lambda$ is undetermined and $w = v$. Therefore, $\|S^T w\|_2^2 = 0$; namely, probability $q$ is incompatible with POVM $\pi$.

*Third case.* Let $(q - t)^T Q^+ (q - t) > 0$ and $(q - t)^T (\mathbb{1} - Q^+ Q)(q - t) = 0$. Upon taking $v = 0$ one has

$$\lambda = -\frac{1}{(q - t)^T Q^+ (q - t)}$$

and

$$w = \frac{Q^+ (q - t)}{(q - t)^T Q^+ (q - t)}.$$

Therefore, one has

$$\|S^T w\|_2^2 = [(q - t)^T Q^+ (q - t)]^{-\frac{1}{2}};$$

namely, probability $q$ is compatible with POVM $\pi$ only if Eqs. (8) are satisfied.

*Fourth case.* Let $(q-t)^T Q^+(q-t) = 0$ and $(q-t)^T \times (\mathbb{1} - Q^+ Q)(q-t) = 0$. Condition $(q-t)^T Q^+(q-t) = 0$ implies $|S^+(q-t)|_2 = 0$ and thus $S^+(q-t) = 0$ and thus $QQ^+(q-t) = 0$ and thus $Q^+Q(q-t) = 0$. For the final implication we used the fact that from the definition of the Moore-Penrose pseudoinverse and the symmetry of $Q$ it follows that $Q^+Q = (Q^+Q)^T = Q^T(Q^T)^+ = QQ^+$. Condition $(q-t)^T(\mathbb{1} - Q^+Q)(q-t) = 0$ implies $(\mathbb{1} - Q^+Q)(q-t) = 0$ since $\mathbb{1} - Q^+Q$ is a projector. Therefore, altogether they imply the following system

$$\begin{cases} Q^+Q(q-t) = 0, \\ (\mathbb{1} - Q^+Q)(q-t) = 0. \end{cases}$$

This system in turn implies $q = t$ and therefore probability $q$ is compatible with POVM $\pi$ (upon input of $\mathbb{1}/d$).

Therefore, $(q-t)^T(\mathbb{1} - Q^+Q)(q-t) = 0$ is necessary for probability $p$ to be compatible with POVM $\pi$. Notice also that $(q-t)^T(\mathbb{1} - Q^+Q)(q-t) = 0$ if and only if $(\mathbb{1} - Q^+Q)(q-t) = 0$. Therefore, probability $p$ is compatible with POVM $\pi$ if and only if Eqs. (8) are satisfied.□

*Applications.*—We have provided a full characterization of $\mathcal{S}(\pi)$ in terms of $\mathcal{S}_1(\pi)$ for any POVM in Proposition 2, and a closed-form full characterization of $\mathcal{S}_1(\pi)$ for any qubit POVM in Theorem 1. As an application, let us now specify our general results to the depolarized version $\mathcal{D}_\lambda^\dagger(\pi)$ of any qubit SIC POVM or MUB $\pi := \{\pi_y\}$.

We first recall that the depolarizing channel $\mathcal{D}_\lambda$, modeling isotropic noise, is defined as $\mathcal{D}_\lambda : \rho \to \lambda\rho + (1-\lambda)\mathrm{Tr}[\rho]d^{-1}\mathbb{1}$ for any state $\rho$, and $\mathcal{D}_\lambda^\dagger$ denotes channel $\mathcal{D}$ in the Heisenberg picture, i.e., $\mathrm{Tr}[\mathcal{D}_\lambda(\rho)\pi_y] = \mathrm{Tr}[\rho\mathcal{D}_\lambda^\dagger(\pi_y)]$ for any state $\rho$ and any effect $\pi_y$.

An informationally complete rank-1 POVM $\{\pi_y\}$ such that $\langle\pi_y|\pi_y\rangle = N_d$ and $|\langle\pi_y|\pi_{y'\neq y}\rangle|^2 = N_d^2 C_d^2$, for some $N_d$ and $C_d$ that depend only on the dimension $d$, is called SIC. By trivial computation, it follows that $N_d = 2(d+1)^{-1}$ and $C_d = (d-1)(d^2+d-2)^{-1}$ for real SIC POVMs, and $N_d = d^{-1}$ and $C_d = (d+1)^{-1}$ for complex SIC POVMs. In the qubit case, the only real and complex SIC POVMs are, up to unitaries and antiunitaries, the trine and tetrahedral POVMs, respectively.

Then, the following result follows from Theorem 1, as shown in the Supplemental Material [36].

**Corollary 1.** An output probability distribution $q = \{q_y\}$ belongs to the set $\mathcal{S}_1(\mathcal{D}_\lambda^\dagger(\pi))$ if and only if

$$\|q\|_2^2 \leq \frac{\lambda^2 + 2}{6},$$

if $\pi$ is a real SIC measurement, and

$$\|q\|_2^2 \leq \frac{\lambda^2 + 3}{12},$$

if $\pi$ is a complex SIC measurement.

An informationally complete rank-1 POVM $\{\pi_{z,t}\}$ such that $\{|\pi_{z,t}\rangle\}$ is an orthonormal basis for any $t$, $\langle\pi_{z,t}|\pi_{z,t}\rangle = N_d$, and $|\langle\pi_{z',t'}|\pi_{z,t}\rangle|^2 = N_d^2 C_d^2$ for $t \neq t'$, for some $N_d$ and $C_d$ that depend only on the dimension $d$, is called a mutually unbiased basis (MUB). By trivial computation, it follows that $N_d = \lfloor d/2 + 1 \rfloor^{-1}$ and $C_d = d^{-1}$ for real MUBs, and $N_d = (d+1)^{-1}$ and $C_d = d^{-1}$ for complex MUBs. In the qubit case, the only real and complex MUBs are, up to unitaries and antiunitaries, the square and octahedral POVMs, respectively.

Then, the following result follows from Theorem 3, as shown in the Supplemental Material [36].

**Corollary 2.** An output probability distribution $q = \{q_y\}$ belongs to the set $\mathcal{S}_1(\mathcal{D}_\lambda^\dagger(\pi))$ if and only if

$$\begin{cases} q_{2y} + q_{2y+1} = \frac{1}{2}, & y = 0, 1, \\ \|q\|_2^2 \leq \frac{\lambda^2 + 2}{8}, \end{cases}$$

if $\pi$ is a real MUB, and

$$\begin{cases} q_{2y} + q_{2y+1} = \frac{1}{3}, & y = 0, 1, 2, \\ \|q\|_2^2 \leq \frac{\lambda^2 + 3}{18}, \end{cases}$$

if $\pi$ is a complex MUB.

*Conclusion and outlooks.*—We addressed the problem of characterizing the set $\mathcal{S}(\pi)$ of input-output correlations compatible with any given POVM $\pi$, upon the input of any set of states. We provided as preliminary results a complete characterization of $\mathcal{S}(\pi)$ in terms of $\mathcal{S}_1(\pi)$, i.e., the range of $\pi$, only. This is in stark contrast with the analogous scenario with respect to quantum channels, which in general requires more than one input [7]. Our main result was to conclusively settle the problem for qubit POVMs, by deriving a full characterization of the range $\mathcal{S}_1(\pi)$ for any given qubit POVM $\pi$, geometrically interpreted as an ellipsoid embedded in an $n$-dimensional real space. As applications, we explicitly discussed the particular cases of qubit real and complex SIC POVMs and MUBs in the presence of isotropic noise. Our results represent a further step towards the characterization of timelike correlations compatible with quantum theory [7]. In this sense, our results provide the optimal device-independent test of quantum measurements.

An important problem left open is that of providing a closed-form full characterization of the range $\mathcal{S}_1(\pi)$ for POVMs in dimensions higher than 2. An interesting related problem is that of characterizing the set of correlations compatible with a given family of states, rather than a given POVM. Finally, we would like to mention a possible application of our results in the context of clean POVMs [37], where it has been shown that, for any two POVMs $\pi$ and $\Pi$, whenever $\mathcal{S}_1(\pi) \subseteq \mathcal{S}_1(\Pi)$, one has that $\pi = \mathcal{L}(\Pi)$ for some linear map $\mathcal{L}$ that is positive on the support of $\Pi$. The implications of Theorem 1 in this context will be addressed by the present authors in a forthcoming work.

Remarkably, any observed input-output correlation falsifies some hypothesized POVMs. Thus, the presented

results are particularly suitable for experimental implementation, for example, by using the techniques and statistical analysis discussed in Refs. [29,30], including an analysis of the effects of finite statistics.

---

[*] cqtmda@nus.edu.sg
[†] sbrandse@caltech.edu
[‡] buscemi@is.nagoya-u.ac.jp
[§] phyvv@nus.edu.sg

[1] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Physics **1**, 195 (1964).
[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).
[3] B. S. Cirel'son, Quantum generalizations of Bell's inequality, Lett. Math. Phys. **4**, 93 (1980).
[4] J. F. Poyatos, J. I. Cirac, and P. Zoller, Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate, Phys. Rev. Lett. **78**, 390 (1997).
[5] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, J. Mod. Opt. **44**, 2455 (1997).
[6] G. M. D'Ariano and P. L. Presti, Tomography of Quantum Operations, Phys. Rev. Lett. **86**, 4195 (2001).
[7] M. Dall'Arno, S. Brandsen, and F. Buscemi, Device-independent tests of quantum channels, Proc. R. Soc. A **473**, 20160721 (2017).
[8] B.-I. Adi and T. N. E. Greville, *Generalized Inverses* (Springer-Verlag, Berlin, 2003).
[9] G. Zauner, Dissertation, Universitat Wien, 1999.
[10] A. Klappenecker and M. Roetteler, in *Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 2005), Adelaide (Australia)* (IEEE, New York, 2005), pp. 1740–1744.
[11] M. Dall'Arno, G. M. D'Ariano, and M. F. Sacchi, Informational power of quantum measurements, Phys. Rev. A **83**, 062304 (2011).
[12] W. Słomczyński and A. Szymusiak, Highly symmetric POVMs and their informational power, arXiv:1402.0375.
[13] M. Dall'Arno, F. Buscemi, and M. Ozawa, Tight bounds on accessible information and informational power, J. Phys. A **47**, 235302 (2014).
[14] A. Szymusiak, Maximally informative ensembles for SIC-POVMs in dimension 3, J. Phys. A **47**, 445301 (2014).
[15] M. Dall'Arno, Accessible information and informational power of Quantum 2-designs, Phys. Rev. A **90**, 052311 (2014).
[16] M. Dall'Arno, Hierarchy of bounds on accessible information and informational power, Phys. Rev. A **92**, 012328 (2015).

[17] S. Brandsen, M. Dall'Arno, and A. Szymusiak, Communication capacity of mixed quantum *t*-designs, Phys. Rev. A **94**, 022335 (2016).
[18] C. A. Fuchs and M. Sasaki, Squeezing quantum information through a classical channel: Measuring the quantumness of a set of quantum states, Quantum Inf. Comput. **3**, 377 (2003).
[19] C. A. Fuchs and R. Schack, Quantum-Bayesian coherence, Rev. Mod. Phys. **85**, 1693 (2013).
[20] C. A. Fuchs and R. Schack, A quantum-Bayesian route to quantum state space, Found. Phys. **41**, 345 (2011).
[21] D. M. Appleby, Å. Ericsson, and C. A. Fuchs, Properties of QBist state spaces, Found. Phys. **41**, 564 (2011).
[22] C. Fuchs, Interview with a quantum Bayesian, arXiv:1207.2141.
[23] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (India)* (IEEE, New York, 1984), pp. 175–179.
[24] S. Wehner and A. Winter, Entropic uncertainty relations–a surey, New J. Phys. **12**, 025009 (2010).
[25] I. Bialynicki-Birula and L. Rudnicki, in *Statistical Complexity: Applications in Electronic Structure*, edited by K. D. Sen (Springer, New York, 2011), Chap. 1.
[26] F. Buscemi, M. J. W. Hall, M. Ozawa, and M. M. Wilde, Noise and Disturbance in Quantum Measurements: An Information-Theoretic Approach, Phys. Rev. Lett. **112**, 050401 (2014).
[27] 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).
[28] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).
[29] M. Hendrych, R. Gallego, M. Mićuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, Nat. Phys. **8**, 588 (2012).
[30] H. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nat. Phys. **8**, 592 (2012).
[31] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, Robustness of device independent dimension witnesses, Phys. Rev. A **86**, 042312 (2012).
[32] R. Chaves, J. B. Brask, and N. Brunner, Device-Independent Tests of Entropy, Phys. Rev. Lett. **115**, 110501 (2015).
[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).
[34] S. P. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, England, 2004).
[35] F. Buscemi, Comparison of quantum statistical models: equivalent conditions for sufficiency, Commun. Math. Phys. **310**, 625 (2012).
[36] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.250501, which includes technical derivations, for some of the results presented in the main text.
[37] F. Buscemi, M. Keyl, G. M. D'Ariano, P. Perinotti, and R. F. Werner, Clean positive operator valued measures, J. Math. Phys. (N.Y.) **46**, 082109 (2005).