

Device-independent tests of quantum measurements

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

¹Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore

²California Institute of Technology, 1200 E. California Blvd, Pasadena, CA 91125, United States

³Graduate School of Information Science, Nagoya University, Chikusa-ku, Nagoya, 464-8601, Japan

⁴Atomic and Laser Physics, Clarendon Laboratory,

University of Oxford, Parks Road, Oxford OX13PU, United Kingdom

(Dated: 27th September 2016)

We consider the problem of characterizing the set of input-output correlations that can be generated by an arbitrarily given quantum measurement. We first show that it is not necessary to consider multiple inputs, but that it is sufficient to characterize only the range of the measurement, namely, the set of output distributions that can be obtained by varying a single input state. We then derive a closed-form, full characterization of the range of any qubit measurement, and discuss its geometrical interpretation. 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 only consist of a general hypothesis about the theory describing the physics, as it is the case in Bell tests [1–3], or it could be extremely detailed, as it happens 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 the case, in which the hypothesis is 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 $p_{y|x} = \text{Tr}[\rho_x \pi_y]$ compatible with an arbitrarily given quantum measurement $\pi := \{\pi_y\}$ (i.e., the hypothesis) and any family of input quantum states $\{\rho_x\}$, namely,

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

Our first result is to show that $\mathcal{S}(\pi)$ is fully characterized by the range of π , namely, the set $\mathcal{S}_1(\pi)$ of output distributions $p_y = \text{Tr}[\rho \pi_y]$ generated by π for varying input state ρ . In other words, correlation $p_{y|x}$ belongs to $\mathcal{S}(\pi)$ if and only if, for any fixed x , $p_{y|x}$ belongs to $\mathcal{S}_1(\pi)$. 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].

When the hypothesis π is a qubit measurement, our second 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: an output distribution $p = \{p_y\}$ belongs to

$\mathcal{S}_1(\pi)$ if and only if

$$\begin{cases} (\mathbb{1} - SS^+)(p - t) = 0, \\ \|S^+(p - t)\|_2 \leq 1, \end{cases} \quad (2)$$

where $\mathbb{1}$ is the identity matrix, S is the matrix $S_{y,k} := \text{Tr}[\pi_y \sigma_k]/2$ representing a decomposition of π over Pauli matrices $\{\sigma_1 \equiv X, \sigma_2 \equiv Y, \sigma_3 \equiv Z\}$, $t_y := \text{Tr}[\pi_y]/2$, and $(\cdot)^+$ represents the Moore-Penrose pseudoinverse [8]. Imposing the system of equalities in Eq. (2) causes linear dependencies (if any) among measurement elements π_y to emerge as linear constraints on the probabilities. Provided that these constraints are satisfied, the inequality in Eq. (2) recasts – through the transformation S^+ – the set of distributions compatible with π 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 (MUB) bases [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 MUB are pivotal elements in quantum cryptography [23], entropic uncertainty relations [24–26], and locking of classical information in quantum states [27].

Our results represent a further step towards the characterization, through device-independent (DI) tests [7], of time-like correlations compatible with quantum theory. The aim of DI tests is that of falsifying hypotheses about the underlying physical model, which is considered accessible only through the *classical* input-output correlations it generates. This approach has been considered in 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 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 ρ is most generally described by a density matrix, namely a positive semidefinite unit-trace operator. Any quantum measurement π 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 π , 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

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

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

$$\max_w [w^T \cdot p - W(\pi, w)] \leq 0, \quad (3)$$

where the maximum is over any $m \times n$ real matrix w , referred to as a *witness*, and $W(\pi, w)$ is defined as $\max_{q \in \mathcal{S}_m(\pi)} w^T \cdot q$ 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 $w \rightarrow \alpha w$ for any $\alpha > 0$ leaves Eq. (3) invariant. Moreover, by direct computation it follows that Eq. (3) is invariant under the *shifting* transformation $w \rightarrow w'$, 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

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

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

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

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

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

The transformation $w \rightarrow w'$, where $w'_{x,y} := \mu_x w_{x,y}$ with μ a probability distribution, i.e. $\|\mu\|_1 = 1$ and $\mu \geq 0$, 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 μ 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 reach therefore our first main result:

Theorem 1. *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 , $p_{y|x}$ belongs to $\mathcal{S}_1(\pi)$.*

Range of qubit measurements — Due to Theorem 1, without loss of generality we solve the optimization problem in Eq. (3) when $m = 1$. In what follows, we restrict our attention to the case of qubit POVM π . 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. With this parametrization, the witness threshold in Eq. (4) becomes

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

Accordingly, Eq. (3) becomes

$$\max_w [(p-t)^T \cdot w - \|S^T w\|_2] \leq 0. \quad (5)$$

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

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

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

$$\min_{(p-t)^T \cdot w = 1} \|S^T w\|_2^2 \geq 1. \quad (7)$$

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

Theorem 2 (Range of qubit measurements). *An output distribution $p := \{p_y\}$ belongs to the range $\mathcal{S}_1(\pi)$ of any given qubit measurement $\pi := \{\pi_y\}$ if and only if*

$$\begin{cases} (\mathbb{1} - SS^+)(p-t) = 0, \\ \|S^+(p-t)\|_2 \leq 1, \end{cases} \quad (8)$$

where $\mathbb{1}$ is the identity matrix, S is the matrix $S_{y,k} := \text{Tr}[\pi_y \sigma_k]/2$ representing a decomposition of π over Pauli matrices $\{\sigma_1 \equiv X, \sigma_2 \equiv Y, \sigma_3 \equiv Z\}$, $t_y := \text{Tr}[\pi_y]/2$, and $(\cdot)^+$ represents the Moore-Penrose pseudoinverse.

Before proceeding to prove Theorem 2, let us provide a geometrical interpretation.

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 $\text{rank } S = \text{rank } SS^+ = l-1$, which also implies $\text{rank}(\mathbb{1} - SS^+) = n-l+1$. Moreover, when all POVM elements are linearly independent, namely $n=l$, the only equation in the system is $\|p\|_1 = \|t\|_1 = 1$. This follows by explicit computation: in this case, $(\mathbb{1} - SS^+)$ turns out to coincide with the rank-one projector along the vector with all unit entries. Hence, in general, the system of equalities in (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 2.

Proof. Equality-constrained quadratic problem can be solved explicitly [8, 34]. In this case we have

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

where $Q := SS^T$, λ is a Lagrange multiplier and v is an arbitrary vectors.

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

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

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

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

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

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

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

and

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

Therefore one has

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

namely probability p is compatible with POVM π only if Eqs. (8) are satisfied.

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

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

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

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

Applications — We have provided a full characterization of $\mathcal{S}(\pi)$ in terms of $\mathcal{S}_1(\pi)$ for *any* POVM in Theorem 1, and a closed-form full characterization of $\mathcal{S}_1(\pi)$ for *any qubit* POVM in Theorem 2. 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}_λ , representing the simplest model of isotropic noise, is defined as $\mathcal{D}_\lambda : \rho \rightarrow \lambda\rho + (1 - \lambda)\text{Tr}[\rho]d^{-1}\mathbb{1}$ for any state ρ , and $\mathcal{D}_\lambda^\dagger$ denotes channel \mathcal{D} in the Heisenberg picture, i.e. $\text{Tr}[\mathcal{D}_\lambda(\rho) \pi_y] = \text{Tr}[\rho \mathcal{D}_\lambda^\dagger(\pi_y)]$ for any state ρ and any effect π_y .

An informationally complete rank-one POVM $\{\pi_y\}$ such that $\langle \pi_y \rangle \pi_y = N_d$ and $|\langle \pi_y \rangle \pi_{y' \neq y}|^2 = N_d^2 C_d^2$, for some N_d and C_d that depend only on the dimension d , is called symmetric, informationally complete (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 anti-unitaries, the trine and tetrahedral POVMs, respectively.

Then, the following result follows from Theorems 1 and 2, as shown in the Supplemental Material [36].

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

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

if π is a real SIC, and

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

if π is a complex SIC.

An informationally complete rank-one POVM $\{\pi_{z,t}\}$ such that $\{|\pi_{z,t}\rangle\}$ is an orthonormal basis for any t , $\langle \pi_{z,t} \rangle \pi_{z,t} = N_d$, and $|\langle \pi_{z',t'} \rangle \pi_{z,t}|^2 = N_d^2 C_d^2$ for $t \neq t'$, for some N_d and C_d that depend only on the dimension d , is called mutually unbiased basis (MUB). By trivial computation, it follows that $N_d = [d/2 + 1]^{-1}$ 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 anti-unitaries, the square and octahedral POVMs, respectively.

Then, the following result follows from Theorems 1 and 2, as shown in the Supplemental Material [36].

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

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

if π is a real MUB, and

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

if π 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 π , upon the input of any set of states. Our first result is a complete characterization of $\mathcal{S}(\pi)$ in terms of $\mathcal{S}_1(\pi)$, i.e. the range of π , only. This is in stark contrast with the analogous scenario of tests of quantum channels, which in general requires more than one input [7]. Then, we conclusively settled the problem for qubit POVMs, by deriving a full characterization of the range $\mathcal{S}_1(\pi)$ for any given qubit POVM π , 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 and MUB POVMs in the presence of isotropic noise. Our results represent a further step towards the characterization of time-like 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 two. 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 about a possible application of our results is in the context of *clean POVMs* [37], where it has been shown that, for any two POVMs π and Π , whenever $\mathcal{S}_1(\pi) \subseteq \mathcal{S}_1(\Pi)$, one has that $\pi = \mathcal{L}(\Pi)$ for some linear map \mathcal{L} which is positive on the support of Π . The implications of Theorem 2 in this context will be addressed by the present authors in a forthcoming work.

Remarkably, any observed input-output correlation (except the uncorrelated one, i.e. when $p_{y|x} = p_y$ for any x) 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].

Acknowledgements M. D. acknowledges support from the Singapore Ministry of Education Academic Research Fund Tier 3 (Grant No. MOE2012-T3-1-009). F. B

acknowledges support from the JSPS KAKENHI, No. 26247016. V. V. acknowledges support from the Ministry of Education and the Ministry of Manpower (Singapore).

* 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; 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, P. Lo Presti, *Tomography of Quantum Operations*, *Phys. Rev. Lett.* **86**, 4195 (2001).
- [7] M. Dall'Arno, S. Brandsen, F. Buscemi, arXiv:1606.02799.
- [8] B.-I. Adi, T. N. E. Greville, *Generalized Inverses* (Springer-Verlag, 2003).
- [9] G. Zauner, *Quantendesigns – Grundzuge einer nichtkommutativen Designtheorie*. Dissertation, Universitat Wien, 1999.
- [10] A. Klappenecker and M. Roetteler, *Mutually unbiased bases are complex projective 2-designs* Proceedings 2005 IEEE International Symposium on Information Theory (ISIT 2005), 1740 (2005).
- [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: Math. Theor.* **47**, 235302 (2014).
- [14] A. Szymusiak, *Maximally informative ensembles for SIC-POVMs in dimension 3*, *J. Phys. A: Math. Theor.* **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*, *Quant. Inf. Comp.* **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* *Foundations of Physics* **41**, 345 (2011).
- [21] D. M. Appleby, Å. Ericsson, and C. A. Fuchs, *Properties of QBist state spaces* *Foundations of Physics* **41**, 564 (2011).
- [22] C. Fuchs, *Interview with a Quantum Bayesian* arXiv:1207.2141
- [23] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 175, 8 (1984).
- [24] S. Wehner and A. Winter, *Entropic uncertainty relations—a surety*, *New J. Phys.* **12**, 025009 (2010).
- [25] I. Białynicki-Birula and L. Rudnicki, *Statistical Complexity: Applications in Electronic Structure*, Ed. K. D. Sen, (Springer, U.K., 2011), chapter 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. Mičuda, N. Brunner, A. Acín, and J. P. Torres, *Experimental estimation of the dimension of classical and quantum systems*, *Nature Phys.* **8**, 588-591 (2012).
- [30] H. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, *Experimental Device-independent Tests of Classical and Quantum Dimensions*, *Nature Physics* **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. Bohr 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, 2010).
- [34] S. P. Boyd, L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).
- [35] F. Buscemi, *Comparison of quantum statistical models: equivalent conditions for sufficiency*, *Comm. Math. Phys.* **310**(3), 625 (2012).
- [36] See the attached supplemental material.
- [37] F. Buscemi, M. Keyl, G. M. D'Ariano, P. Perinotti, and R. F. Werner, *Clean positive operator valued measures*, *J. Math. Phys.* **46**, 82109 (2005).

SUPPLEMENTAL MATERIAL

Here we prove those results reported in the article ‘‘Device-independent tests of quantum measurements’’ by the present authors (M. Dall’Arno, S. Brandsen, F. Buscemi, and V. Vedral) whose proofs, being lengthy but relatively straightforward, has only been outlined in the main text. The numbering of statements follows that of the article.

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

$$\|p\|_2^2 \leq \frac{\lambda^2 + 2}{6}, \quad (10)$$

if π is a real SIC, and

$$\|p\|_2^2 \leq \frac{\lambda^2 + 3}{12}, \quad (11)$$

if π is a complex SIC.

Proof. Let us first prove the real case. The POVM $\pi_y = |\pi_y\rangle\langle\pi_y|$ with $|\pi_y\rangle = U^y|0\rangle$ where $U := e^{-i\frac{\pi}{3}Y}$ is the unique (up to unitaries and anti-unitaries) real SIC POVM of a qubit. Thus, t and S are given by

$$t = \frac{1}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad S = \frac{\lambda}{6} \begin{pmatrix} 2 & 0 & 0 \\ -1 & \sqrt{3} & 0 \\ -1 & -\sqrt{3} & 0 \end{pmatrix}.$$

Let us first take $\lambda > 0$. The equality in Eqs. (8) becomes $\sum_{y=0}^2 p_y = 1$. The inequality in Eqs. (8) becomes

$$(p-t)^T(S^T)^+S^+(p-t) = \lambda^{-2} \left(6 \sum_{y=0}^2 p_y^2 - 2 \right) \leq 1,$$

through use of the identity $\sum_{y<z} p_y p_z = \frac{1}{2}(1 - \sum_y p_y^2)$.

Let us now take $\lambda = 0$. The equality in Eqs. (8) becomes $p = t$. The inequality in Eqs. (8) is trivially satisfied. Then Eq. (10) immediately follows.

Let us then prove the complex case. The POVM $\pi_y = \frac{1}{2}|\pi_y\rangle\langle\pi_y|$ with

$$|\pi_y\rangle := \sigma_y \left(\cos \frac{\arctan \sqrt{2}}{2} |0\rangle + e^{i\frac{\pi}{4}} \sin \frac{\arctan \sqrt{2}}{2} |1\rangle \right),$$

where $\sigma := (\mathbb{1}_2, \sigma_X, \sigma_Y, \sigma_Z)$ are the Pauli matrices, is the unique (up to unitaries and anti-unitaries) SIC POVM of a qubit. Thus, t and S are given by

$$t = \frac{1}{4} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad S = \frac{\lambda}{12} \begin{pmatrix} 3 & 0 & 0 \\ -1 & 2\sqrt{2} & 0 \\ -1 & -\sqrt{2} & \sqrt{6} \\ -1 & -\sqrt{2} & -\sqrt{6} \end{pmatrix}.$$

Let us first take $\lambda > 0$. The equality in Eqs. (8) becomes $\sum_{y=0}^3 p_y = 1$. The inequality in Eqs. (8) becomes

$$(p-t)^T(S^T)^+S^+(p-t) = \lambda^{-2} \left(12 \sum_{y=0}^2 p_y^2 - 3 \right) \leq 1,$$

through use of the identity $\sum_{y<z} p_y p_z = \frac{1}{2}(1 - \sum_y p_y^2)$.

Let us now take $\lambda = 0$. The equality in Eqs. (8) becomes $p = t$. The inequality in Eqs. (8) is trivially satisfied. Then Eq. (11) immediately follows. \square

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

$$\begin{cases} p_{2y} + p_{2y+1} = \frac{1}{2}, & y = 0, 1, \\ \|p\|_2^2 \leq \frac{\lambda^2 + 2}{8}, \end{cases} \quad (12)$$

if π is a real MUB, and

$$\begin{cases} p_{2y} + p_{2y+1} = \frac{1}{3}, & y = 0, 1, 2, \\ \|p\|_2^2 \leq \frac{\lambda^2 + 3}{18}, \end{cases} \quad (13)$$

if π is a complex MUB.

Proof. Let us first prove the real case. The POVM $\pi_y = |\pi_y\rangle\langle\pi_y|$ with $\sigma_k |\pi_{2k, 2k+1}\rangle = \pm |\pi_{2k, 2k+1}\rangle$ with $k = 0, 1$ is the unique (up to unitaries and anti-unitaries) real SIC POVM of a qubit. Thus, t and S are given by

$$t = \frac{1}{4} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad S = \frac{1}{4} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

Let us first take $\lambda > 0$. The equality in Eqs. (8) becomes $p_0 + p_1 = p_2 + p_3 = 1/2$. The inequality in Eqs. (8) becomes

$$(p-t)^T(S^T)^+S^+(p-t) = \lambda^{-2} \left(8 \sum_{y=0}^2 p_y^2 - 2 \right) \leq 1,$$

through use of the identity $p_0 p_1 = -\frac{1}{2}(p_0^2 + p_1^2) + \frac{1}{8}$.

Let us now take $\lambda = 0$. The equality in Eqs. (8) becomes $p = t$. The inequality in Eqs. (8) is trivially satisfied. Then Eq. (12) immediately follows.

Let us then prove the complex case. The POVM $\pi_y = |\pi_y\rangle\langle\pi_y|$ with $\sigma_k |\pi_{2k, 2k+1}\rangle = \pm |\pi_{2k, 2k+1}\rangle$ with $k = 0, 1, 2$ is the unique (up to unitaries and anti-unitaries) real SIC POVM of a qubit. Thus, t and S are given by

$$t = \frac{1}{6} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad S = \frac{1}{6} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Let us now take $\lambda > 0$. The equality in Eqs. (8) becomes $p_0 + p_1 = p_2 + p_3 = p_4 + p_5 = 1/3$. The inequality

in Eqs. (8) becomes

$$(p - t)^T (S^T)^+ S^+ (p - t) = \lambda^{-2} \left(18 \sum_{y=0}^2 p_y^2 - 3 \right) \leq 1,$$

through use of the identity $p_0 p_1 = -\frac{1}{2}(p_0^2 + p_1^2) + \frac{1}{18}$.

Let us now take $\lambda = 0$. The equality in Eqs. (8) becomes $p = t$. The inequality in Eqs. (8) is trivially satisfied. Then Eq. (13) immediately follows. \square