# Extension of the Alberti-Ulhmann criterion beyond qubit dichotomies

Michele Dall'Arno,[1,*] Francesco Buscemi,[2,†] and Valerio Scarani[1,3,‡]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore*
[2] *Graduate School of Informatics, Nagoya University, Chikusa-ku, 464-8601 Nagoya, Japan*
[3] *Department of Physics, National University of Singapore, 2 Science Drive 3, 117542, Singapore*

(Dated: October 11, 2019)

The Alberti-Ulhmann criterion states that any given qubit dichotomy can be transformed into any other given qubit dichotomy by a quantum channel if and only if the testing region of the former dichotomy includes the testing region of the latter dichotomy. Here, we generalize the Alberti-Ulhmann criterion to the case of arbitrary number of qubit or qutrit states. We also derive an analogous result for the case of qubit or qutrit measurements with arbitrary number of elements. We demonstrate the possibility of applying our criterion in a semi-device independent way.



When quantum states are looked at as resources, it is natural to study which states can be transformed into which others by means of an allowed set of operations. This question has been declined in many ways: entanglement processing, thermal operations... In this paper, we consider generalizations of the following task: given a pair of quantum states $(\rho_0, \rho_1)$, called a *dichotomy*, determine which other dichotomies $(\sigma_0, \sigma_1)$ can be obtained from it by application of a completely positive trace preserving (CPTP) map. The simplicity of the problem is only apparent: very few results are known about this problem. Before reviewing them, and stating our contribution, let us take a detour to consider the analogous task in classical statistics.

A classical dichotomy is a pair of probability distributions $(p_0, p_1)$. It appears naturally in the simplest formulation of hypothesis testing, in which there are two inputs (the *null* and the *alternative* hypotheses) and two outputs (*accept* or *reject*). In this case, any test is represented by a point in the dichotomy's *hypothesis testing region*, defined as the region $\{(p_0, p_1)\} \subset \mathbb{R}^2$ where $p_0$ is the probability of correctly accepting the null hypothesis and $p_1$ is the probability of wrongly accepting the alternative hypothesis with the given test [1]. Tests can be then designed, for instance, to maximise $p_0$ while keeping $p_1$ under a certain threshold. In particular, the wider the testing region, the more "testable", that is, the more "distinguishable" the pair of hypotheses is.

That the testing region is all that matters when dealing with pairs of hypotheses is made particularly clear by the celebrated Blackwell's theorem for dichotomies [2]: given two dichotomies $(p_0, p_1)$ and $(q_0, q_1)$, possibly on different sample spaces, there exists a stochastic transformation that transforms $p_0$ into $q_0$ and $p_1$ into $q_1$ simultaneously ("statistical sufficiency") if and only if the testing region for $(p_0, p_1)$ contains the testing region for $(q_0, q_1)$. In other words, the former dichotomy can be deterministically processed into (or, can deterministically simulate) the latter. In the special case in which $p_1 = q_1 = u$, the uniform distribution, the ordering induced by comparing the testing region coincides with the ubiquitous *majorization ordering*: indeed, the Lorenz curve corresponding to a probability distribution $p$ is nothing but the boundary of the testing region corresponding to the dichotomy $(p, u)$ [1–4].

Such a compact characterisation is not known in the quantum case that concerns us [5–9]: quantum statistical sufficiency is in general expressed in terms of an infinite number of conditions [10–12] that are, therefore, very difficult to check in practice [13]. Some results, based on [14], are known when the conversion is relaxed to be approximate [15, 16], but the problem remains hard in general. A notable exception is the case in which both quantum dichotomies, $(\rho_0, \rho_1)$ and $(\sigma_0, \sigma_1)$, only comprise two-dimensional (i.e., qubit) states. Then, as a consequence of a well-known result by Alberti and Uhlmann, there exists a CPTP map transforming $(\rho_0, \rho_1)$ into $(\sigma_0, \sigma_1)$ if and only if the testing region of the former contains the testing region of the latter [17]. This is the perfect analog of Blackwell's theorem; but counterexamples are known as soon as $(\rho_0, \rho_1)$ is a qutrit dichotomy [5].

In this paper, building upon previous works of some of the present authors [18–22], we derive the following results. First, we show that any family of $n$ qubit states which can all become simultaneously real under a single unitary transformation can be transformed into any other family of $n$ qubit (or, under some conditions, qutrit) states by a CPTP map if the testing region of the former includes the testing region of the latter (the Alberti-Uhlmann case is recovered for $n = 2$, since any pair of qubit states can be made simultaneously real). Second, we show that an analogous result holds for qubit or qutrit measurements with $n$ elements which can all become simultaneously real under a single unitary transformation. We demonstrate the possibility of witnessing statistical sufficiency in a semi-device independent way, that is, without any assumption on the devices except their Hilbert space dimension.

*Formalism.* — We will make use of standard definitions in quantum information theory [23]. A quantum state is represented by a density matrix, that is, a positive semi-definite operator $\rho$ such that $\mathrm{Tr}[\rho] = 1$. A quantum measurement is represented by a positive operator-

valued measure, that is, a family $\{\pi_a\}$ of positive semi-definite operators that satisfy the completeness condition $\sum_a \pi_a = \mathbb{1}$, where $\mathbb{1}$ denotes the identity operator.

A channel is represented by a completely positive trace preserving map, that is, a map $\mathcal{C}$ such that for any state $\rho$ one has $\mathrm{Tr}[\mathcal{C}(\rho)] = \mathrm{Tr}[\rho]$ and $(\mathcal{I} \otimes \mathcal{C})(\rho) \geq 0$. In the Heisenberg picture, a channel is represented by a completely positive unit preserving map, that is, a map $\mathcal{C}$ such that for any $\pi \geq 0$ one has $\mathcal{C}(\mathbb{1}) = \mathbb{1}$ and $(\mathcal{I} \otimes \mathcal{C})(\pi) \geq 0$.

*Simulability of families of states.* — We say that a family $\{\rho_x\}$ of $m$ states simulates another (possibly different dimensional) family $\{\sigma_x\}$ of $m$ states, in formula

$$\{\sigma_x\} \preceq \{\rho_x\}, \tag{1}$$

if and only if there exists a channel $\mathcal{C}$ such that $\sigma_x = \mathcal{C}(\rho_x)$ for any $x$.

If condition (1) is verified, it immediately follows that

$$\mathcal{R}\left(\{\sigma_x\}\right) \subseteq \mathcal{R}\left(\{\rho_x\}\right), \tag{2}$$

where $\mathcal{R}(\{\rho_x\})$ denotes the testing region of family $\{\rho_x\}$, defined as the set of all vectors whose $x$-th entry is the probability $\mathrm{Tr}[\rho_x \pi]$ for any measurement element $\pi$, in formula

$$\mathcal{R}\left(\{\rho_x\}\right) := \left\{ \mathbf{p} \;\middle|\; \exists\, 0 \leq \pi \leq \mathbb{1} \text{ s.t. } \mathbf{p}_x = \mathrm{Tr}\left[\rho_x \pi\right] \right\}.$$

In other words, for any measurement element $\tau$ there exists a measurement element $\pi$ such that $\mathrm{Tr}[\rho_x \pi] = \mathrm{Tr}[\sigma_x \tau]$ for any $x$.

As formally proved in the Supplemental Material, we derive conditions under which the reverse implication is also true, that is Eq. (2) implies Eq. (1). One needs to distinguish two cases. If the family $\{\rho_x\}$ contains the identity operator $\mathbb{1}$ in its linear span, in Lemma 1 we show conditions under which it can be mapped into another family of states by a positive trace preserving map, and in Lemma 2 we specialize this result to the qubit case by using a well-known decomposition [24] of qubit maps due to Woronowicz. If the family $\{\rho_x\}$ does not contain the identity operator $\mathbb{1}$ in its linear span, in Lemmas 3 and 4 we generalize a result [7] by Buscemi and Gour, in turn based on a result [17] by Alberti and Ulhmann. As a result, we have the following Theorem about real families of qubit states, that is, states that have only real entries (in some basis).

**Theorem 1.** *For any family $\{\sigma_x\}$ of qubit states and any real family $\{\rho_x\}$ of qubit states, the following are equivalent:*

- $\{\sigma_x\} \preceq \{\rho_x\}$.
- $\mathcal{R}(\{\sigma_x\}) \subseteq \mathcal{R}(\{\rho_x\})$.

*If $\{\rho_x\}$ contains the identity operator $\mathbb{1}$ in its linear span, the statement holds even if $\{\sigma_x\}$ is a family of qutrit states.*

Notice that the assumption that the family $\{\rho_x\}$ of states is real cannot be relaxed. As a counterexample, take $\{\sigma_x\}$ and $\{\rho_x\}$ to be symmetric informationally complete (or tetrahedral) families of states with $\rho_0 = \sigma_1$ and $\rho_1 = \sigma_0$, while $\rho_k = \sigma_k$ for $k = 2, 3$. A family $\{\rho_x\}$ of four pure qubit states is tetrahedral if and only if $\mathrm{Tr}[\rho_x \rho_z]$ is constant for any $x \neq z$. It immediately follows that there exists a transposition map $\mathcal{T}$ (with respect to some basis) such that $\sigma_x = \mathcal{T}(\rho_x)$ for any $x$. Due to the informational completeness of $\{\sigma_x\}$ and $\{\rho_x\}$, map $\mathcal{T}$ is the only map such that this is the case. However, map $\mathcal{T}$ is not a channel as it is not completely positive.

*Simulability of measurements.* — We say that an $n$-outcome measurement $\{\pi_a\}$ simulates another (possibly, different dimensional) $n$-outcome measurement $\{\tau_a\}$, in formula

$$\{\tau_a\} \preceq \{\pi_a\}, \tag{3}$$

if and only if there exists a channel $\mathcal{C}$ such that $\tau_a = \mathcal{C}^\dagger(\pi_a)$ for any $a$, where $\mathcal{C}^\dagger$ denotes channel $\mathcal{C}$ in the Heisenberg picture.

If condition (3) is verified, it follows immediately that

$$\mathcal{R}\left(\{\tau_a\}\right) \subseteq \mathcal{R}\left(\{\pi_a\}\right), \tag{4}$$

where the range $\mathcal{R}(\{\pi_a\})$ of measurement $\{\pi_a\}$ is defined as the set of all probability distributions $\mathrm{Tr}[\rho \pi_a]$ on the outcomes $a$ for any state $\rho$, in formula

$$\mathcal{R}\left(\{\pi_a\}\right) := \left\{ \mathbf{p} \;\middle|\; \exists\, \rho \geq 0, \mathrm{Tr}\,\rho = 1, \text{ s.t. } \mathbf{p}_a = \mathrm{Tr}\left[\rho \pi_a\right] \right\}.$$

In other words, for any state $\sigma$ there exists a state $\rho$ such that $\mathrm{Tr}[\rho \pi_a] = \mathrm{Tr}[\sigma \tau_a]$ for any $a$.

As formally proved in the Supplemental Material, we derive conditions under which the reverse implication is also true, that is Eq. (4) implies Eq. (3). First, in Lemma 5 we generalize a result [25] by Buscemi et al. on clean measurements. Then, in Lemma 6 we specialize it to the qubit case by using a well-known decomposition [24] of qubit maps due to Woronowicz. As a result, we have the following theorem about real qubit measurements, that is, measurements whose elements have only real entries (in some basis).

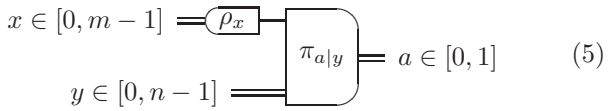
**Theorem 2.** *For any qubit or qutrit measurement $\{\tau_a\}$ and any real qubit measurement $\{\pi_a\}$, the following are equivalent:*

- $\{\tau_a\} \preceq \{\pi_a\}$.
- $\mathcal{R}(\{\tau_a\}) \subseteq \mathcal{R}(\{\pi_a\})$.

Notice that, as before, the assumption that measurement $\{\pi_a\}$ is real cannot be relaxed.

*Semi-device independent simulability of families of states.* — Suppose that a black box preparator with $m$ buttons is given, and let us denote with $\rho_x$ the unknown

state prepared upon the pressure of button $x$. Consider the setup where a black box tester with $n$ buttons is connected to the black box preparator, and let us denote with $\{\pi_{0|y}, \pi_{1|y} := \mathbb{1} - \pi_{0|y}\}$ the test performed upon the pressure of button $y$. One has




(5)

For each $y$, by running the experiment asymptotically many times one collects the vectors $\mathbf{p}_y$ and $\mathbf{u} - \mathbf{p}_y$ ($\mathbf{u}$ denotes the vector with unit entries) whose $x$-th entry are the probabilities $\mathrm{Tr}[\rho_x \pi_{0|y}]$ and $\mathrm{Tr}[\rho_x \pi_{1|y}]$, respectively, that is

$$\left[\mathbf{p}_y\right]_x := \mathrm{Tr}\left[\rho_x \pi_{0|y}\right].$$

We call semi-device independent simulability the problem of characterizing the class of all families of states that can be simulated by the black box $\{\rho_x\}$, for which simulability can be certified based on distributions $\{\mathbf{p}_y\}$ and $\{\mathbf{u} - \mathbf{p}_y\}$ under an assumption on the Hilbert space dimension, without any assumptions on the tests $\{\pi_{a|y}\}$.

Here, we will address the semi-device independent simulability problem under the promise that $\{\rho_x\}$ is a family of qubit states. In this case, the testing region [19, 20] is the convex hull of the isolated points 0 and $\mathbf{u}$ with a (possibly degenerate) ellipsoid centered in $\mathbf{u}/2$. Also, the convex hull of 0 and $\mathbf{u}$ with any (possibly degenerate) ellipsoid centered in $\mathbf{u}/2$ subset of the hypercube $[0, 1]^m$ is the testing region of a qubit family of states. In general, such a testing region identifies the family of states up to unitaries and anti-unitaries.

We will further make the restriction that the black box $\{\rho_x\}$ has $m = 2$ buttons, that is, $\{\rho_x\}$ is a dichotomy. In this case, in the discussion above the (possibly degenerate) ellipsoid becomes a (possibly degenerate) ellipse. Notice also that, since two anti-unitarily related qubit dichotomies are also unitarily-related, a qubit dichotomy is identified by its range up to unitaries only.

Since any qubit dichotomy is necessarily real, due to Theorem 1, we have the following result.

**Corollary 1.** *If the convex hull of points* 0 *and* $\mathbf{u}$ *with any given ellipse centered in* $\mathbf{u}/2$ *is a subset of* $\mathrm{conv}(0, \mathbf{u}, \{\mathbf{p}_x\}, \{\mathbf{u} - \mathbf{p}_x\})$ *it is the testing region of some qubit dichotomy that can be simulated by* $\{\rho_x\}$.

Notice that, on the one hand, the hypothesis of Corollary 1 represents only a sufficient condition for a qubit dichotomy to be simulable by $\{\rho_x\}$. On the other hand, for any other qubit dichotomy that can be simulated by $\{\rho_x\}$ (if any), simulability cannot be certified in a semi-device independent way unless further data is collected.

As an application, consider the case when one of the states prepared by the dichotomy (say $\rho_1$) is the thermal state at infinite temperature, that is $\rho_1 = \mathbb{1}/2$ (for this example we are assuming more than just the Hilber space dimension, although no knowledge of $\rho_0$ is assumed). Consider the problem of finding the dichotomy with maximal free energy among those that can be simulated by $\{\rho_0, \mathbb{1}/2\}$ through a Gibbs-preserving channel (in this case, a unit-preserving channel).

In this case, it immediately follows that the free energy is monotone in the area of the range. This can be seen as follows. First, notice that the free energy in this case is equal to the neg-entropy $-S(\rho_0)$, since the free energy is equal to the relative entropy $S(\rho_0||\mathbb{1}/2)$ and by definition one has $S(\rho_0||\mathbb{1}/2) = -S(\rho_0)$. In turn, $S(\rho_0) = h(\lambda_\pm)$, where $h(\cdot)$ denotes the binary entropy and $\lambda_\pm$ the eigenvalues of $\rho_0$. Since $\lambda_\pm = 1/2 \pm a$, where $a$ is the non-null semi-axis of $\mathcal{E}(\{\rho_x\})$, and the volume of the range of $\{\rho_0, \mathbb{1}/2\}$ is of course a monotone in $a$, the statement remains proved.

Suppose one test is performed on the black box dichotomy and the following probability vectors are observed:

$$\mathbf{p}_0 = \frac{1}{2}\begin{pmatrix} 1-\epsilon \\ 1 \end{pmatrix}, \qquad \mathbf{u} - \mathbf{p}_0 = \frac{1}{2}\begin{pmatrix} 1+\epsilon \\ 1 \end{pmatrix}. \tag{6}$$

for some value of parameter $0 \leq \epsilon \leq 1$. The situation is illustrated in Fig. 1. We assume that the black box implements a qubit dichotomy, a justified assumption since the probability vector in Eq. (6) belongs, for example, to the range of any qubit dichotomy $\{\phi, \mathbb{1}/2\}$, for any pure state $\phi$. It is easy to derive the maximum volume range enclosed in $\mathrm{conv}(0, \mathbf{u}, \mathbf{p}_0, \mathbf{u} - \mathbf{p}_0)$, and to verify using Ref. [18] that it correspond to the range of any $\epsilon$-depolarized dichotomy $\{\mathcal{D}_\epsilon(\phi), \mathbb{1}/2\}$, for any pure state $\phi$.

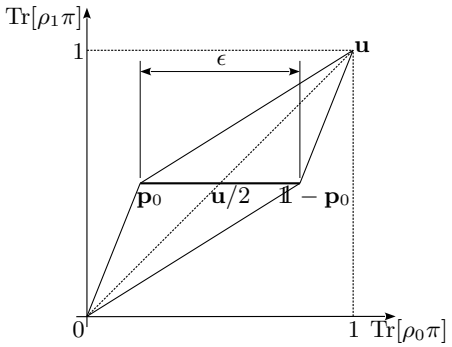



Figure 1. Probability vectors $\mathbf{p}_0$ and $\mathbf{u} - \mathbf{p}_0$ as given by Eq. (6) lie at the vertices of a a line segment of length $\epsilon$ and centered in $\mathbf{u}/2$. The maximally committal testing region for qubit dichotomy $\{\sigma_0, \mathbb{1}/2\}$ enclosed in $\mathrm{conv}(0, \mathbf{u}, \mathbf{p}_0, \mathbf{u} - \mathbf{p}_0)$ is given by $\mathrm{conv}(0, \mathbf{u}, \mathbf{p}_0, \mathbf{u} - \mathbf{p}_0)$ itself.

*Semi-device independent simulability of measurements.* — Suppose that a black box measurement with $n$ outcomes is given, and let us denote with $\pi_y$ the unknown measurement element corresponding to outcome $y$. Consider the setup where a black box preparator with $m$

buttons is connected to the black box measurement, and let us denote with $\rho_x$ the unknown state prepared upon the pressure of button $x$. One has

$$x \in [0, m-1] \; \Longrightarrow \boxed{\rho_x} - \boxed{\pi_a} \Longrightarrow \; a \in [0, n-1] \quad (7)$$

For each $x$, by running the experiment asymptotically many times one collects the probability distribution $\mathbf{p}_x$ of outcome $y$, that is

$$[\mathbf{p}_x]_a := \mathrm{Tr}\left[\rho_x \pi_a\right].$$

We call semi-device independent simulability the problem of characterizing the class of all measurements that can be simulated by the black box $\{\pi_a\}$, for which simulability can be certified based on distributions $\{\mathbf{p}_x\}$ under an assumption on the Hilbert space dimension, without any assumptions on the states $\{\rho_x\}$,

Here, we will address the semi-device independent simulability problem under the promise that $\{\pi_y\}$ is a qubit measurement. In this case, the range [18, 20] is a (possibly degenerate) ellipsoid. Conversely, any (possibly degenerate) ellipsoid subset of the probability simplex is the range of a qubit measurement. In general, such a range identifies the measurement up to unitaries and anti-unitaries.

We will further make the restriction that the black box $\{\pi_a\}$ has $n = 3$ outcomes. In this case, in the discussion above the (possibly degenerate) ellipsoid becomes a (possibly degenerate) ellipse. Notice also that, since three-outcome anti-unitarily related qubit measurements are also unitarily related, a three-outcome measurement is identified by its range up to unitaries only.

Since any three-outcome qubit measurement is necessarily real due to the completeness condition, due to Theorem 2, we have the following result.

**Corollary 2.** *Any ellipse subset of* $\mathrm{conv}(\{\mathbf{p}_x\})$ *is the range of some qubit three-outcome measurement that can be simulated by* $\{\pi_a\}$.

Notice that, on the one hand, the hypothesis of Corollary 2 represents only a sufficient condition for a qubit three-outcome measurement to be simulable by $\{\pi_a\}$. On the other hand, for any other qubit three-outcome measurement that can be simulated by $\{\pi_a\}$ (if any), simulability cannot be certified in a semi-device independent way unless further data is collected.

As an application, consider the problem of finding, among the measurements that can be simulated by the black box $\{\pi_a\}$, the one with maximal simulation power, quantified according to Theorem 2 by the volume of its range. Suppose $m$ states are fed into the black-box measurement and the following distributions are observed:

$$\mathbf{p}_x = \begin{pmatrix} 2 - 2\cos\theta_x \\ 2 + cos\theta_x - \sqrt{3}\sin\theta_x \\ 2 + cos\theta_x + \sqrt{3}\sin\theta_x \end{pmatrix}, \quad (8)$$

where $\theta_x := 2\pi x/m$ and $x \in [0, m-1]$. This situation is depicted in Fig. 2. We assume that the black box implements a qubit measurement, a justified assumption since such distributions belong to the range of, for example, a trine qubit measurement, that is, a measurement whose elements lie on the vertices of a regular triangle oin the Bloch sphere representation. It is easy to derive the maximum volume ellipse [26–29] enclosed in $\mathrm{conv}(\{\mathbf{p}_x\})$, and to verify using Ref. [18] that it corresponds to the range of any $[\cos(\pi/m)]$-depolarized trine measurement.

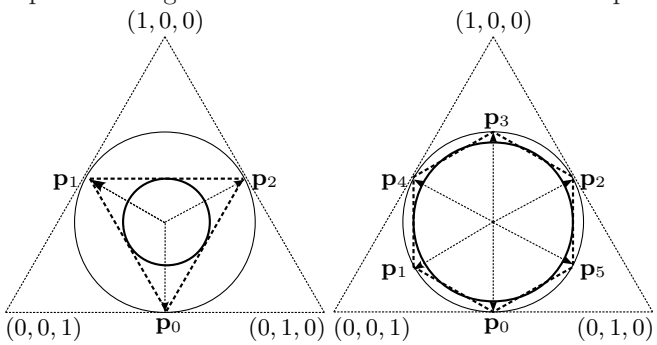



Figure 2. In both left and right figures, the outer dashed triangle represents the simplex of three-outcome probability distributions. The distributions $\{\mathbf{p}_x\}$ given by Eq. (8) lie on the vertices of regular polygons ($m = 3$ and $m = 6$ in left and right figures, respectively). The maximum volume ellipsoid enclosed in $\mathrm{conv}(\{\mathbf{p}_x\})$ is the inner circle, which is the range of a $\epsilon$-depolarized trine qubit measurement ($\epsilon = 1/2$ and $\epsilon = \sqrt{3}/2$ in left and right figures, respectively).

*Conclusion.* — In this work we addressed the problem of quantum simulability, that is, the existence of a quantum channel transforming a given device into another. We considered the cases of families of $n$ qubit or qutrit states and of qubit or qutrit measurements with $n$ elements, thus extending the Alberti-Ulhmann criterion for qubit dichotomies. Based on these results, we demonstrated the possibility of certifying the simulability in a semi-device independent way, that is, without any assumption of the devices except their Hilbert space dimension.

*Acknowledgement.* — M.D. is grateful to A. Bisio, A. Jenčová, and K. Matsumoto for insightful discussions. This work is supported by the National Research Fund and the Ministry of Education, Singapore, under the Research Centres of Excellence programme; and partly supported by the program for FRIAS-Nagoya IAR Joint Project Group. F. B. acknowledges partial support from the Japan Society for the Promotion of Science (JSPS) KAKENHI, Grant No. 19H04066.

* cqtmda@nus.edu.sg
† buscemi@i.nagoya-u.ac.jp
‡ physv@nus.edu.sg

[1] J. M. Renes, *Relative submajorization and its use in*

*quantum resource theories*, J. Math. Phys. **57**, 122202 (2016).
[2] D. Blackwell, *Equivalent Comparisons of Experiments*, The Annals of Mathematical Statistics **24**, 265 (1953).
[3] E. N. Torgersen, *Comparison of statistical experiments* volume **36** (Cambridge University Press, 1991).
[4] E. N. Torgersen, *Comparison of experiments when the parameter space is finite*, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete **16**, 219 (1970).
[5] 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.
[6] K. Matsumoto, *"On the condition of conversion of classical probability distribution families into quantum families"*, arXiv:1412.3680 (2014).
[7] F. Buscemi and G. Gour, *Quantum Relative Lorenz Curves*, Physical Review A **95**, 012110 (9 January 2017).
[8] D. Reeb, M. J. Kastoryano, and M. M. Wolf, *"Hilbert's projective metric in quantum information theory"*, Journal of Mathematical Physics **52**, 082201 (2011).
[9] A. Jenčová, *"Comparison of Quantum Binary Experiments"*, Reports on Mathematical Physics **70**, 237 (2012).
[10] F. Buscemi, *"Comparison of Quantum Statistical Models: Equivalent Conditions for Sufficiency"*, Communications in Mathematical Physics **310**, 625 (2012).
[11] K. Matsumoto, *"A quantum version of randomization criterion"*, arXiv: 1012.2650 (2010).
[12] A. Jenčová, *"Comparison of quantum channels and statistical experiments"*, in 2016 IEEE International Symposium on Information Theory (ISIT), 2249 (2016).
[13] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications* (Springer, 2011).
[14] K. Matsumoto, *"Reverse Test and Characterization of Quantum Relative Entropy"*, arXiv:1010.1030 (2010).
[15] F. Buscemi, D. Sutter, and M. Tomamichel, *An information-theoretic treatment of quantum dichotomies*, arXiv:1907.08539.
[16] X. Wang and M. M. Wilde, *"Resource theory of asymmetric distinguishability"*, arXiv:1905.11629 (2019).
[17] P. M. Alberti and A. Uhlmann, *A problem relating to positive linear maps on matrix algebras*, Reports on Mathematical Physics **18**, 163 (1980).
[18] M. Dall'Arno, S. Brandsen, F. Buscemi, and V. Vedral, *Device-independent tests of quantum measurements*, Phys. Rev. Lett. **118**, 250501 (2017).
[19] M. Dall'Arno, *Device-independent tests of quantum states*, Phys. Rev. A **99**, 052353 (2019).
[20] M. Dall'Arno, F. Buscemi, A. Bisio, and A. Tosini, *Data-driven inference, reconstruction, and observational completeness of quantum devices*, arXiv:1812.08470.
[21] F. Buscemi and M. Dall'Arno, *Data-driven Inference of Physical Devices: Theory and Implementation*, arXiv:1805.01159.
[22] M. Dall'Arno, A. Ho, F. Buscemi, V. Scarani, *Data-driven inference and observational completeness of quantum devices*, arXiv:1905.04895.
[23] M. M. Wilde, *Quantum Information Theory*, (Cambridge University Press, 2017).
[24] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).
[25] F. Buscemi, G. M. D'Ariano, M. Keyl, P. Perinotti, R. Werner, *Clean Positive Operator Valued Measures*, J. Math. Phys. **46**, 082109 (2005).
[26] F. John, *Extremum problems with inequalities as subsidiary conditions*, in *Studies and Essays Presented to R. Courant on his 60th Birthday*, 187–204, (Interscience Publishers, New York, 1948).
[27] K. M. Ball, *Ellipsoids of maximal volume in convex bodies*, Geom. Dedicata. **41**, 241 (1992).
[28] Michael J. Todd, *Minimum-Volume Ellipsoids: Theory and Algorithms*, Minimum-Volume Ellipsoids: Theory and Algorithms (2016).
[29] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press.

### Supplemental Material

Here we provide those technical results reported in the work "Extension of the Alberti-Ulhmann criterion beyond qubit dichotomies" by the present authors (M. DallArno, F. Buscemi, and V. Scarani) that, not being essential for the presentation, were not included in the Main Text.

### Simulability of families of states

For any $n$, a vector $\mathbf{u}_n \in \mathbb{R}^n$ and a set $\mathbb{E}_n \subseteq \mathbb{R}^n$ such that $\operatorname{span}\mathbb{E}_n = \mathbb{R}^n$ are given.

**Definition 1** (Family of states)**.** A linear map $S : \mathbb{R}^\ell \to \mathbb{R}^n$ is a family of states only if $S\mathbf{u}_\ell = \mathbf{u}_n$.

**Definition 2** (Statistical morphism)**.** A linear map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^{\ell_1}$ is a statistical morphism if and only if $C\mathbb{E}_0 \subseteq \mathbb{E}_1$ and $C\mathbf{u}_{\ell_0} = \mathbf{u}_{\ell_1}$. In standard quantum theory, a statistical morphism is a positive unit-preserving (PUP) map.

**Lemma 1.** *For any families of states $S_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^n$ and $S_1 : \mathbb{R}^{\ell_1} \to \mathbb{R}^n$ such that $S_1^+ S_1 \mathbb{E}_1 \subseteq \mathbb{E}_1$ and $S_1^+ S_1 \mathbf{u}_{\ell_1} = \mathbf{u}_{\ell_1}$, the following are equivalent:*

1. *$S_0\mathbb{E}_0 \subseteq S_1\mathbb{E}_1$,*
2. *there exists a statistical morphism $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^{\ell_1}$ such that $S_0 = S_1 C$.*

*Proof.* Implication $1 \Leftarrow 2$ is trivial.

Implication $1 \Rightarrow 2$ can be shown as follows. Let

$$C := S_1^+ S_0. \tag{9}$$

Let us first show that map $C$ is a statistical morphism. One has

$$C\mathbb{E}_0 = S_1^+ S_0 \mathbb{E}_0 \subseteq S_1^+ S_1 \mathbb{E}_1 \subseteq \mathbb{E}_1,$$

where the equality follows from Eq. (9) and the inclusions follow from the hypothesis $S_0\mathbb{E}_0 \subseteq S_1\mathbb{E}_1$ and $S_1^+ S_1 \mathbb{E}_1 \subseteq \mathbb{E}_1$, respectively. Moreover,

$$C\mathbf{u}_{\ell_0} = S_1^+ S_0 \mathbf{u}_{\ell_0} = S_1^+ \mathbf{u}_n,$$

where the equalities follow from Eq. (9) and from the hypothesis $S_0\mathbf{u}_{\ell_0} = \mathbf{u}_n$, respectively. Since by hypothesis $S_1\mathbf{u}_{\ell_1} = \mathbf{u}_n$, one also has $S_1^+ S_1 \mathbf{u}_{\ell_1} = S_1^+ \mathbf{u}_n$, and hence

$$C\mathbf{u}_{\ell_0} = S_1^+ S_1 \mathbf{u}_{\ell_1} = \mathbf{u}_{\ell_1},$$

where the second inequality follows by hypothesis. Hence map $C$ is a statistical morphism.

Let us now show that $S_0 = S_1 C$. By multiplying Eq. (9) from the left by $S_1$ one has

$$S_1 C = S_1 S_1^+ S_0.$$

Since $\operatorname{span}\mathbb{E}_0 = \mathbb{R}^{\ell_0}$ and $\operatorname{span}\mathbb{E}_1 = \mathbb{R}^{\ell_1}$, from $S_0\mathbb{E}_0 \subseteq S_1\mathbb{E}_1$ one has $\operatorname{rng} S_0 \subseteq \operatorname{rng} S_1$. Since $S_1 S_1^+$ is the projector on $\operatorname{rng} S_1$, one has $S_0 = S_1 C$. □

It is easy to see that condition $M_1^+ M_1 \mathbb{S}_1 \subseteq \mathbb{S}_1$ in Lemma 5 is satisfied for any measurement $M_1$ if $\mathbb{E}_1$ is a $\ell_1$–dimensional (hyper)–cone with $(\ell_1 - 1)$–dimensional (hyper)–spherical section with axis along $\mathbf{u}_{\ell_1}$.

**Lemma 2.** *For any qubit or qutrit family $S_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^n$ of states, with $\ell_0 = 4$ or $\ell_0 = 9$, and any qubit family $S_1 : \mathbb{R}^4 \to \mathbb{R}^n$ of states such that $S_1^+ S_1 \mathbf{u}_{\ell_1} = \mathbf{u}_{\ell_1}$ and $S_1 T = S_1$ where $T$ denotes the transposition map with respect to some basis, the following are equivalent:*

1. *$S_0\mathbb{E}_0 \subseteq S_1\mathbb{E}_1$,*
2. *there exists CPTP map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that $S_0 = S_1 C$.*

*Proof.* Implication $1 \Leftarrow 2$ is trivial.

Implication $1 \Rightarrow 2$ can be shown as follows. Due to Lemma 1, there exists a statistical morphism $C' : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$, hence a PUP map, such that $S_0 = S_1 C'$. Let us prove that there exists a CPUP map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that $M_0 = M_1 C$.

For any qubit PUP map $C' : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$, there exists [24] $0 \leq p \leq 1$ and CPUP maps $C_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ and $C_1 : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that

$$C' = pC_0 + (1-p)\, TC_1. \tag{10}$$

One has

$$S_1 C' = S_1 \left[pC_0 + (1-p)\, TC_1\right] = S_1 \left[pC_0 + (1-p)\, C_1\right],$$

where the equalities follow from Eq. (10) and from the hypothesis $S_1 T = S_1$, respectively. Since the convex combination of CPUP maps is CPUP, map $C := pC_0 + (1-p)\, C_1$ is CPUP. □

For any linear map $S$, we denote with $s^k$ its $k$-th row.

**Lemma 3.** *For any families $S_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^n$ and $S_1 : \mathbb{R}^{\ell_1} \to \mathbb{R}^n$ of states such that $S_0\mathbb{E}_0 \subseteq S_1\mathbb{E}_1$, if for some $k$ there exists $\{\lambda_i \in \mathbb{R}\}$ such that*

$$s_1^k = \sum_{i \neq k} \lambda_i s_1^k,$$

*then one has*

$$s_0^k = \sum_{i \neq k} \lambda_i s_0^k.$$

*Proof.* By hypothesis, for any $e_0 \in \mathbb{E}_0$ there exists $e_1 \in \mathbb{E}_1$ such that

$$s_0^k \cdot e_0 = s_1^k \cdot e_1.$$

Hence, for any set $\{e_0^j\} \subseteq \mathbb{E}_0$ one has

$$s_0^k \cdot e_0^j = s_1^k \cdot e_1^j = \sum_{i \neq k} \lambda_i s_1^i \cdot e_1^j = \sum_{i \neq k} \lambda_i s_0^i \cdot e_0^j.$$

Since $\operatorname{span} \mathbb{E}_0 = \mathbb{R}^{\ell_0}$, it is possible to take set $\{e_0^j \in \mathbb{E}_0\}$ a spanning set. Hence the thesis. □

**Lemma 4.** *For any qubit families $S_0 : \mathbb{R}^4 \to \mathbb{R}^n$ and $S_1 : \mathbb{R}^4 \to \mathbb{R}^n$ of states such that $S_1^+ S_1 \mathbf{u}_{\ell_1} \neq \mathbf{u}_{\ell_1}$ and $S_1 T = S_1$ where $T$ denotes the transposition map with respect to some basis, the following are equivalent:*

1. *$S_0 \mathbb{E}_0 \subseteq S_1 \mathbb{E}_1$,*
2. *there exists CPTP map $C : \mathbb{R}^4 \to \mathbb{R}^4$ such that $S_0 = S_1 C$.*

*Proof.* Implication $1 \Leftarrow 2$ is trivial.

Implication $1 \Rightarrow 2$ can be shown as follows.

By the hypothesis $S_0 \mathbb{E}_0 \subseteq S_1 \mathbb{E}_1$, one has that for any $e_0 \in \mathbb{E}_0$ there exists a $e_1 \in \mathbb{E}_1$ such that $s_0^k \cdot e_0 = s_1^k e_1$ for any $k$. Since in particular this holds for $k = 0, 1$, by denoting with $S_0'$ and $S_1'$ the families of states whose rows are $(s_0^0, s_0^1)$ and $(s_1^0, s_1^1)$, respectively, one has

$$S_0' \mathbb{E}_0 \subseteq S_1' \mathbb{E}_1.$$

Hence, due to a result [7] by Buscemi and Gour, in turn based on a result [17] by Alberti and Ulhmann, there exists a CPTP map $C : \mathbb{R}^4 \to \mathbb{R}^4$ such that $S_0' = S_1' C$.

Due to the hypotheses $S_1^+ S_1 \mathbf{u}_{\ell_1} \neq \mathbf{u}_{\ell_1}$ and $S_1 T = S_1$, for any $k$ there exists $\lambda^k \in \mathbb{R}$ such that

$$s_1^k = \lambda^k s_1^0 + (1 - \lambda_k)\, s_1^1.$$

Hence, due to Lemma 3, one also has

$$s_0^k = \lambda^k s_0^0 + (1 - \lambda_k)\, s_0^1.$$

Hence, by linearity, $S_0 = C S_1$. □

### Simulability of measurements

For any $n$, a vector $\mathbf{u}_n \in \mathbb{R}^n$ and a set $\mathbb{S}_n \subseteq \mathbb{R}^n$ such that $\operatorname{span} \mathbb{S}_n = \mathbb{R}^n$ are given.

**Definition 3** (Measurement)**.** A linear map $M : \mathbb{R}^\ell \to \mathbb{R}^n$ is a measurement only if $M^T \mathbf{u}_n = \mathbf{u}_\ell$.

**Definition 4** (State morphism)**.** A linear map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^{\ell_1}$ is a state morphism if and only if $C \mathbb{S}_0 \subseteq \mathbb{S}_1$. In standard quantum theory, a state morphism is any positive trace-preserving (PTP) map.

**Lemma 5.** *For any measurements $M_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^n$ and $M_1 : \mathbb{R}^{\ell_1} \to \mathbb{R}^n$ such that $M_1^+ M_1 \mathbb{S}_1 \subseteq \mathbb{S}_1$, the following are equivalent:*

1. *$M_0 \mathbb{S}_0 \subseteq M_1 \mathbb{S}_1$,*
2. *there exists a state morphism $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^{\ell_1}$ such that $M_0 = M_1 C$.*

*Proof.* Implication $1 \Leftarrow 2$ is trivial.

Implication $1 \Rightarrow 2$ can be shown as follows. Let

$$C := M_1^+ M_0. \tag{11}$$

Let us first show that map $C$ is a state morphism. One has

$$C \mathbb{S}_0 = M_1^+ M_0 \mathbb{S}_0 \subseteq M_1^+ M_1 \mathbb{S}_1 \subseteq \mathbb{S}_1,$$

where the equality follows from Eq. (11) and the inclusions follow from the hypothesis $M_0 \mathbb{S}_0 \subseteq M_1 \mathbb{S}_1$ and $M_1^+ M_1 \mathbb{S}_1 \subseteq \mathbb{S}_1$, respectively. Hence map $C$ is a state morphism.

Let us now show that $M_0 = M_1 C$. By multiplying Eq. (11) from the left by $M_1$ one has

$$M_1 C = M_1 M_1^+ M_0.$$

Since $\operatorname{span} \mathbb{S}_0 = \mathbb{R}^{\ell_0}$ and $\operatorname{span} \mathbb{S}_1 = \mathbb{R}^{\ell_1}$, from $M_0 \mathbb{S}_0 \subseteq M_1 \mathbb{S}_1$ one has $\operatorname{rng} M_0 \subseteq \operatorname{rng} M_1$. Since $M_1 M_1^+$ is the projector on $\operatorname{rng} M_1$, one has $M_0 = M_1 C$. □

It is easy to see that condition $M_1^+ M_1 \mathbb{S}_1 \subseteq \mathbb{S}_1$ in Lemma 5 is satisfied for any measurement $M_1$ if and only if $\mathbb{S}_1$ is a $(\ell - 1)$–dimensional (hyper)–sphere with center along $\mathbf{u}_{\ell_1}$.

To see this, notice that the (hyper)–sphere is the only body for which there exists a point (the center) such that any line through the point is orthogonal to the surface of the body. Hence, the (hyper)–sphere is also the only body for which the projection of the body on any subspace containing such a point is a subset of the body.

Finally, notice that by multiplying condition $M_1^T \mathbf{u}_n = \mathbf{u}_{\ell_1}$ on the left by $M_1^+ M_1$ and using the elementary property of pseudoinverse that $M_1^+ M_1 M_1^T = M_1^T$, one immediately has

$$M_1^+ M_1 \mathbf{u}_{\ell_1} = \mathbf{u}_{\ell_1},$$

that is, $M_1^+ M_1$ is the projector on a subspace that contains the center of the (hyper)–sphere $\mathbb{S}_1$.

**Lemma 6.** *For any qubit or qutrit measurement $M_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^n$, with $\ell_0 = 4$ or $\ell_0 = 9$, and any qubit measurement $M_1 : \mathbb{R}^4 \to \mathbb{R}^n$ such that $M_1 T = M_1$ where $T$ denotes the transposition map with respect to some basis, the following are equivalent:*

1. *$M_0 \mathbb{S}_0 \subseteq M_1 \mathbb{S}_1$,*
2. *there exists CPTP map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that $M_0 = M_1 C$.*

*Proof.* Implication $1 \Leftarrow 2$ is trivial.

Implication $1 \Rightarrow 2$ can be shown as follows. Due to Lemma 5, there exists a state morphism $C' : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$, hence a PTP map, such that $M_0 = M_1 C'$. Let us prove that there exists a CPTP map $C : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that $M_0 = M_1 C$.

For any PTP map $C' : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$, there exists [24] $0 \leq p \leq 1$ and CPTP maps $C_0 : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ and $C_1 : \mathbb{R}^{\ell_0} \to \mathbb{R}^4$ such that

$$C' = pC_0 + (1-p)\,TC_1. \tag{12}$$

One has

$$M_1 C' = M_1 \left[pC_0 + (1-p)\,TC_1\right] = M_1 \left[pC_0 + (1-p)\,C_1\right],$$

where the equalities follow from Eq. (12) and from the hypothesis $M_1 T = M_1$, respectively. Since the convex combination of CPTP maps is CPTP, map $C := pC_0 + (1-p)\,C_1$ is CPTP. □