Reliable Quantum State Tomography

Matthias Christandl* and Renato Renner†

Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Strasse 27, CH-8093 Zurich, Switzerland

(Received 11 March 2012; published 19 September 2012; publisher error corrected 24 September 2012)

Quantum state tomography is the task of inferring the state of a quantum system by appropriate measurements. Since the frequency distributions of the outcomes of any finite number of measurements will generally deviate from their asymptotic limits, the estimates computed by standard methods do not in general coincide with the true state and, therefore, have no operational significance unless their accuracy is defined in terms of error bounds. Here we show that quantum state tomography, together with an appropriate data analysis procedure, yields reliable and tight error bounds, specified in terms of confidence regions—a concept originating from classical statistics. Confidence regions are subsets of the state space in which the true state lies with high probability, independently of any prior assumption on the distribution of the possible states. Our method for computing confidence regions can be applied to arbitrary measurements including fully coherent ones; it is practical and particularly well suited for tomography on systems consisting of a small number of qubits, which are currently in the focus of interest in experimental quantum information science.

DOI: 10.1103/PhysRevLett.109.120403 PACS numbers: 03.65.Wj, 02.50.−r, 03.67.−a

The state of a classical system can, in principle, be determined to arbitrary precision by applying a single measurement to it. Any imprecisions are due solely to inaccuracies of the measurement technique but not of fundamental nature. This is different in quantum theory. It follows from Heisenberg's uncertainty principle that measurements generally have a random component and that individual measurement outcomes only give limited information about the state of the system—even if an ideal measurement device is used. To illustrate this difference, it is useful to take an information-theoretic perspective. Assume, for instance, that we are presented with a two-level system about which we have no prior information except that it has been prepared in a pure state, and our task is to determine this state. If the system was classical, there are only two possible pure states, and one single bit of information is therefore sufficient for its full description. Furthermore, a single measurement of the system suffices to retrieve this bit. If the system was quantum, however, the situation becomes more interesting. A two-level quantum system (a qubit) admits a continuum of pure states that can, for example, be parametrized by a point on the Bloch sphere. To determine this point to a given accuracy Δ, at least $\log_2(4/\Delta^2)$ bits of information are necessary [1]. Conversely, according to Holevo's bound [2], any measurement applied to a single qubit will provide us with at most one bit of information. And even if n identically prepared copies of the qubit were measured, at most $\log_2(n+1)$ bits of information about their state can be obtained [3]. Hence, the accuracy, Δ, to which the state can be determined always remains finite ($\Delta \geq 2/\sqrt{n+1}$), necessitating the specification of error bars.

The impact that randomness in measurement data has on the accuracy of estimates has been studied extensively in statistics and, in particular, estimation theory [4]. The latter is concerned with the general problem of estimating the values of parameters from data that depend probabilistically on them. The data may be obtained from measurements on a quantum system with parameter-dependent state, as considered in quantum estimation theory [5]. Quantum state tomography can be seen as a special instance of quantum estimation, where one aims to estimate a set of parameters large enough to determine the system's state completely [6–12].

An obvious choice of parameters are the matrix elements of a density operator representation of the state. Because of the finite accuracy, however, the individual estimates for the matrix elements do not generally correspond to a valid density operator (for instance, the matrix may have negative eigenvalues). This problem is avoided with other techniques, such as maximum likelihood estimation (MLE) [10,13,14], which has been widely used in experiments [15–21], or Bayesian estimation [5,22–27].

In MLE, an estimate for the error bars can be obtained from the width of the likelihood function, which is approximated by the Fisher information matrix [12,13,28–31]. In current experiments, one also uses numerical plausibility tests known as "bootstrapping" or, more generally, "resampling" [20,32] in order to obtain bounds on the errors. However, despite being reasonable in many practical situations, these bounds are not known to have a well-defined operational interpretation and, in the case of the resampling method, may lead to an underestimate of the errors [33].

In contrast, Bayesian methods can be used to calculate "credibility regions", i.e., subsets of the state space in which the state is found with high probability. This probability, however, depends on the choice of a "prior", corresponding to an assumption about the distribution

of the states before the measurements (in particular, the assumption can not be justified by the experimental data). Furthermore, we remark that most known techniques are based on the assumption of independent and identical measurements (a notable exception is the one-qubit adaptive tomography analysis of Ref. [34]). We refer to Ref. [26] for a further discussion of currently used approaches to quantum state tomography, including pedagogical examples illustrating their limitations.

In this Letter, we introduce a method to obtain confidence regions, that is, regions in state space which contain the true state with high probability. A point in the region may then serve as estimate, and the maximal distance of the point to the border of the region as error bar. Our method allows us to analyze data obtained from arbitrary quantum measurements, including fully coherent ones. The method does not rely on any assumptions about the prior distribution of the states to be measured. This makes it highly robust so that it can, for instance, be applied in the context of quantum cryptography, where the states to be estimated are chosen adversarially.

The remainder of this Letter is organized as follows: We first describe a very general setup for tomography of quantum states prepared in a sequence of experiments, where we do not make the typical assumption that the states are independent and identically distributed (IID). We then show that, nevertheless, properties of the states can be inferred reliably using a suitable tomographic data analysis procedure (Theorem). In motivation and spirit, this result relates to recent research efforts on quantum de Finetti representations. We then specialize our setup to the case where, in principle, the experiments may be run an arbitrary number of times (while still only finitely many runs are used to generate data). This special case is (by the quantum de Finetti theorem) equivalent to an IID preparation of the states, thereby justifying the common IID assumption in data analysis. The theorem, applied to this special case, then results in a construction for confidence regions for quantum state tomography (Corollary).

General scenario.—Consider a collection $\mathcal{S}_1, \ldots, \mathcal{S}_{n+k}$ of finite-dimensional quantum systems with associated Hilbert space $\mathcal{H}$, as depicted in Fig. 1 (see also Refs. [35,36], where a similar setup is considered). We denote by d the dimension of $\mathcal{H}$. For example, one may think of $n + k$ particles prepared in a series of experiments, where $\mathcal{H}$ could correspond to the spin degree of freedom. From this collection, a sample consisting of n systems is selected at random and measured according to an (arbitrary) positive operator valued measure (POVM) $\{B^n\}$, a family of positive semidefinite operators B^n on $\mathcal{H}^{\otimes n}$ such that $\sum_{B^n} B^n = 1_{\mathcal{H}}^{\otimes n}$. That is, each POVM element B^n corresponds to a possible sequence of outcomes resulting from (not necessarily independent) measurements on the n systems. The goal of quantum state tomography is to infer the state of the remaining k systems, using the outcomes of these measurements.

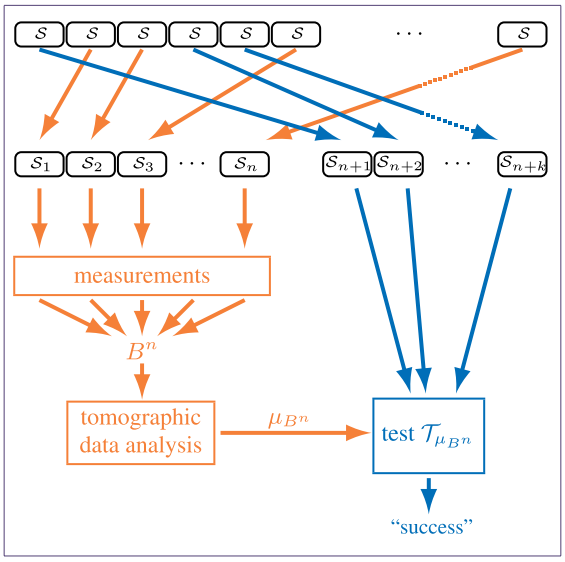

FIG. 1 (color online). General scenario. Measurements are applied to a sample $\mathcal{S}_1, \ldots, \mathcal{S}_n$ consisting of n systems, chosen at random from a collection of $n + k$ systems. The outcomes of the measurements are collected and given as input, B^n, to a data analysis procedure (left orange part). The aim of quantum state tomography is to make reliable predictions about the state of the remaining k (non-measured) systems $\mathcal{S}_{n+1}, \ldots, \mathcal{S}_{n+k}$. To model such predictions, we consider hypothetical tests, which output "success" whenever their input has a desired property (right blue part). Given only the output of the data analysis procedure, μ_{B^n}, it is possible to characterize the tests $\mathcal{T}_{\mu_{B^n}}$ that are passed with high probability—independently of the initial state of the $n + k$ systems (Theorem).

Note that the k extra systems are not measured during data acquisition. Nevertheless, they play a role in the above scenario, as they are used to define operationally what state we are inferring. (In the special case of IID states, the extra systems are simply copies of the measured systems—see below.) We also remark that, instead of measuring a sample of n systems chosen at random, one may equivalently permute the initial collection of $n + k$ systems at random and then measure the first n of them, i.e., $\mathcal{S}_1, \ldots, \mathcal{S}_n$. We will use this alternative description for our theoretical analysis.

In order to describe our main results, we imagine that the measurement outcomes B^n are processed by a data analysis routine that outputs a probability distribution μ_{B^n} on the set of mixed states, defined by

$$\mu_{B^n}(\sigma)d\sigma = \frac{1}{c_{B^n}} \operatorname{tr}[\sigma^{\otimes n} B^n] d\sigma$$

(see Fig. 2 for an illustration). Here $d\sigma$ denotes the Hilbert-Schmidt measure with $\int d\sigma = 1$. Furthermore, $c_{B^n} = \operatorname{tr}[B^n \otimes 1_{\mathcal{K}}^{\otimes n} \cdot 1_{\mathrm{Sym}^n(\mathcal{H}\otimes\mathcal{K})}]/\binom{n+d^2-1}{d^2-1}$ is a normalization constant, where $\mathcal{K} \cong \mathcal{H} \cong \mathbb{C}^d$ and where $1_{\mathrm{Sym}^n(\mathcal{H}\otimes\mathcal{K})}$ is the projector onto the symmetric subspace of $(\mathcal{H} \otimes \mathcal{K})^{\otimes n}$. Note that, in Bayesian statistics, $\mu_{B^n}(\sigma)d\sigma$ corresponds to the *a posteriori* distribution when updating

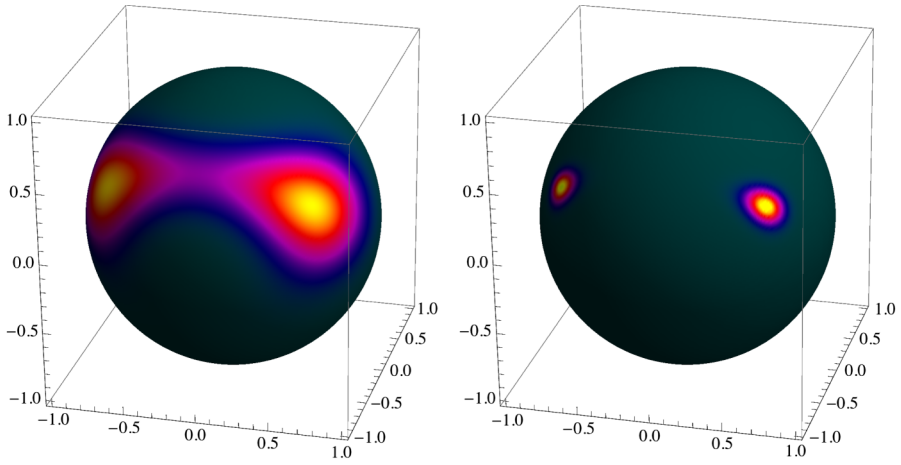

FIG. 2 (color online). Illustration of μ_{B^n}. The graphs show μ_{B^n} for measurements performed on $n = 20$ and $n = 240$ qubits (for illustration purposes, we only depict the density μ_{B^n} on the surface of the Bloch ball). Half of the qubits have been measured in the z direction and half in the y direction with relative frequencies of (0.2, 0.8) and (0.7, 0.3), respectively. One observes a rapid decrease in the size of the bright regions (which are connected by a bright tube inside the Bloch ball), which correspond to large values of μ_{B^n}.

a Hilbert-Schmidt prior $d\sigma$. Furthermore, in MLE, $\sigma \mapsto \mathrm{tr}[\sigma^{\otimes n} B^n]$ is known as the likelihood function. Since our work is not based on either of these approaches, however, we will not use this terminology and simply refer to μ_{B^n}.

Reliable predictions.—We now show that μ_{B^n} contains all information that is necessary in order to make reliable predictions about the state of the remaining systems $\mathcal{S}_{n+1}, \ldots, \mathcal{S}_{n+k}$. To specify these predictions, we consider hypothetical tests, a quantum version of a similar concept used in classical statistics. Any such test acts on the joint system consisting of $\mathcal{S}_{n+1}, \ldots, \mathcal{S}_{n+k}$ (see Fig. 1). Mathematically, a test is simply a measurement with a binary outcome, "success" or "failure", specified by a joint POVM $\{T^{\mathrm{fail}}, 1_{\mathcal{H}}^{\otimes k} - T^{\mathrm{fail}}\}$ on $\mathcal{H}^{\otimes k}$ [37]. Note that the state of $\mathcal{S}_{n+1}, \ldots, \mathcal{S}_{n+k}$ could be inferred if we knew which hypothetical tests it would pass. Hence, instead of estimating this state directly, we can equivalently consider the task of predicting the outcomes of the hypothetical tests.

Assume now that we carry out a test $\mathcal{T}_{\mu_{B^n}} = \{T^{\mathrm{fail}}_{\mu_{B^n}}, 1_{\mathcal{H}}^{\otimes k} - T^{\mathrm{fail}}_{\mu_{B^n}}\}$ depending on μ_{B^n}. We denote by ρ^{n+k} the (unknown) joint state of the systems $\mathcal{S}_1, \ldots, \mathcal{S}_{n+k}$ before the tomographic measurements. (As described above, we can assume without loss of generality that the systems are permuted at random, so that ρ^{n+k} is permutation invariant.) If the outcome of the tomographic measurement is B^n, then the postmeasurement state of the remaining systems is given explicitly by $\rho^k_{B^n} = [1/\mathrm{tr}(B^n \rho^n)]\mathrm{tr}_{\mathcal{H}^{\otimes n}}[B^n \otimes 1_{\mathcal{H}}^{\otimes k} \cdot \rho^{n+k}]$, where $\mathrm{tr}_{\mathcal{H}^{\otimes n}}$ denotes the partial trace over the n measured systems. Hence, the probability that the test $\mathcal{T}_{\mu_{B^n}}$ fails for the above state $\rho^k_{B^n}$ equals $\mathrm{tr}[T^{\mathrm{fail}}_{\mu_{B^n}} \rho^k_{B^n}]$. The following theorem now provides a criterion under which this failure probability is upper bounded by any given $\epsilon > 0$. Crucially, the criterion only depends on μ_{B^n}, which is obtained by the tomographic data analysis. In other words, μ_{B^n} allows us to determine which hypothetical tests the state $\rho^k_{B^n}$ would pass.

Theorem (reliable predictions from μ_{B^n}).—For all B^n let $T^{\mathrm{fail}}_{\mu_{B^n}}$ be a POVM element on $\mathcal{H}^{\otimes k}$ such that

$$\int \mu_{B^n}(\sigma)\mathrm{tr}[T^{\mathrm{fail}}_{\mu_{B^n}} \sigma^{\otimes k}] d\sigma \leq \epsilon c^{-1}_{n+k,d},$$

where $c_{N,d} = \binom{N+d^2-1}{d^2-1}$. Then, for any ρ^{n+k},

$$\langle \mathrm{tr}[T^{\mathrm{fail}}_{\mu_{B^n}} \rho^k_{B^n}] \rangle_{B^n} \leq \epsilon,$$

where $\langle \cdot \rangle_{B^n}$ denotes the expectation taken over all possible measurement outcomes B^n when measuring ρ^n (i.e., outcome B^n has probability $\mathrm{tr}[B^n \rho^n]$).

As we shall see, the tests are typically chosen such that the integral over $d\sigma$ decreases exponentially with n. The additional factor $c^{-1}_{n+k,d}$, which is inverse polynomial in $n + k$, plays, therefore, only a minor role in the criterion. We also emphasize that the theorem is valid independently of how the systems $\mathcal{S}_1, \ldots, \mathcal{S}_{n+k}$ have been prepared. In particular, the (commonly made) assumption that they all contain identical copies of a single-system state is not necessary.

The proof of the theorem, together with a slightly more general formulation, is provided in the Supplemental Material [38]. It makes crucial use of the following fact, which has also been used in quantum-cryptographic security proofs: there exists a so-called *de Finetti state* τ^N, i.e., a convex combination of tensor products, such that $\rho^N \leq c_{N,d} \cdot \tau^N$ holds for all permutation-invariant states ρ^N on $\mathcal{H}^{\otimes N}$ [39,40].

Confidence regions.—A confidence region is a subset of the single-particle state space which is likely to contain the "true" state. In order to formalize this, we consider the practically relevant case of an experiment that can, in

principle, be repeated arbitrarily often. Within the above-described general scenario, this corresponds to the limit where k approaches infinity while n, the number of actual runs of the experiment (whose data is analyzed), is still finite and may be small.

Since the initial state ρ^{n+k} of all $n+k$ systems can without loss of generality be assumed to be permutation invariant (see above), the quantum de Finetti theorem [35,41–44] implies that, for fixed $n, k' \in \mathbb{N}$, the marginal state $\rho^{n+k'}$ on $n+k'$ systems is approximated by a mixture of product states, i.e.,

$$\rho^{n+k'} = \mathrm{tr}_{k-k'}(\rho^{n+k}) \approx \int P(\sigma)\sigma^{\otimes(n+k')}d\sigma, \qquad (1)$$

for some probability density function P and approximation error proportional to $1/k$. In the limit of large k, the marginal state $\rho^{n+k'}$ is thus fully specified by P. We can therefore equivalently imagine that all systems were prepared in the same unknown "true" state σ, which is distributed according to P (see Fig. 3). This corresponds to the IID assumption commonly made in the literature on quantum state tomography, which is therefore rigorously justified within our general setup.

As before, we assume that tomographic measurements are applied to the systems $\mathcal{S}_1, \ldots, \mathcal{S}_n$, whereas the remaining systems, $\mathcal{S}_{n+1}, \ldots, \mathcal{S}_{n+k'}$, undergo a test (depending on the output μ_{B^n} of the data analysis procedure). We may now consider tests that are passed if and only if the true state σ is contained in a given subset $\Gamma^{\delta}_{\mu_{B^n}}$ of the state space. The following corollary provides a sufficient criterion under which the tests are passed, so that $\Gamma^{\delta}_{\mu_{B^n}}$ are confidence regions. (Note that the criterion refers to additional sets $\Gamma_{\mu_{B^n}}$ that are related to the confidence regions $\Gamma^{\delta}_{\mu_{B^n}}$; see Supplemental Material [38] for an illustration.)

Corollary (confidence regions from μ_{B^n}).—For all B^n let $\Gamma_{\mu_{B^n}}$ be a set of states on $\mathcal{H}$ such that

$$\int_{\Gamma_{\mu_{B^n}}} \mu_{B^n}(\sigma)d\sigma \geq 1 - \frac{\epsilon}{2}c^{-1}_{2n,d}. \qquad (2)$$

Then, for any σ,

$$\mathrm{Prob}_{B^n}[\sigma \in \Gamma^{\delta}_{\mu_{B^n}}] \geq 1 - \epsilon,$$

where Prob_{B^n} refers to the distribution of the measurement outcomes B^n when measuring $\sigma^{\otimes n}$ (i.e., outcome B^n has probability $\mathrm{tr}[B^n\sigma^{\otimes n}]$) and where

$$\Gamma^{\delta}_{\mu_{B^n}} = \{\sigma: \exists\, \sigma' \in \Gamma_{\mu_{B^n}} \text{ with } F(\sigma,\sigma')^2 \geq 1-\delta^2\}, \qquad (3)$$

with $\delta^2 = \frac{2}{n}(\ln\frac{2}{\epsilon} + 2\ln c_{2n,d})$ and $F(\sigma,\sigma') = \|\sqrt{\sigma}\sqrt{\sigma'}\|_1$ the fidelity.

The main idea for the proof of the corollary is to apply the above theorem to tests (acting on $k' = n$ systems) derived from Holevo's optimal covariant measurement [45]. We refer to the Supplemental Material [38] for the technical proof.

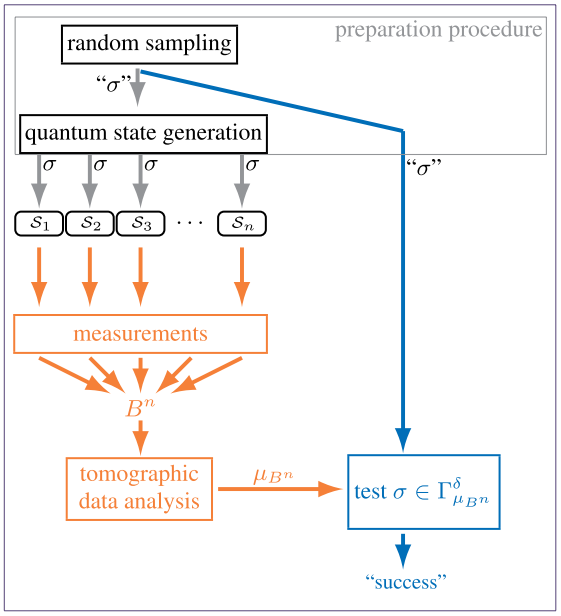

FIG. 3 (color online). Tomography of identically prepared systems. This scenario falls into the framework depicted in Fig. 1, corresponding to the limit where the number of extra systems, k, approaches infinity. In this case, we can assume without loss of generality that the systems have been prepared in a two-step process: first, a description "σ" of a single-system state is sampled at random (according to some probability density P); second, n identical systems $\mathcal{S}_1, \ldots, \mathcal{S}_n$ are prepared in state σ. The k extra systems of Fig. 1 are replaced by a classical variable carrying the description "σ". Given only the output of the tomographic data analysis, μ_{B^n}, it is possible to decide whether σ is (with probability at least $1-\epsilon$) contained in a given set $\Gamma^{\delta}_{\mu_{B^n}}$ (Corollary). If this is the case then $\Gamma^{\delta}_{\mu_{B^n}}$ is a confidence region (with confidence level $1-\epsilon$).

Note that $1-\epsilon$ can be interpreted as the confidence level of the statement that the true state σ is contained in the set $\Gamma^{\delta}_{\mu_{B^n}}$. Crucially, the claim is valid for all σ. In particular, it is independent of any initial probability distribution, P, according to which σ may have been chosen [see Eq. (1)]. In other words, the operational interpretation of the sets $\Gamma^{\delta}_{\mu_{B^n}}$ as confidence regions does not depend on any extra assumptions about the preparation procedure or on the specification of a prior. In fact, σ could even be chosen "maliciously", for example, in a quantum cryptographic context, where an adversary may try to pretend that a system has certain properties (e.g., that its state is entangled while in reality it is not).

Obviously, the assertion that a state σ is contained in a certain set Γ^{δ}_{μ} can only be considered a good approximation of σ if the set Γ^{δ}_{μ} is small. This is indeed the case for reasonable choices of the measurement $\{B^n\}$. For instance, in the practically important case where each system is measured independently and identically with POVM $\{E_i\}$, the confidence region is, for generic states, asymptotically of size proportional to $\frac{1}{\sqrt{n}}$ in the (semi)norm on the set

of quantum states induced by the POVM: $\|\cdot\|_{\{E_i\}} = \sum_i |\mathrm{tr}(E_i \cdot)|$ [38,46].

Conclusion.—Despite conceptual differences, our technique is not unrelated to MLE and Bayesian estimation. As mentioned before, $\mu(\sigma)$ is proportional to the likelihood function, and therefore, methods to construct confidence regions with our technique are likely to use adaptations of techniques from MLE. Also, $\mu_{B^n}(\sigma)d\sigma$ corresponds to the probability measure obtained from applying Bayes's updating rule to the Hilbert-Schmidt measure; a fact that implies near optimality [47] of our method in the practically most relevant case of independent tomographically complete measurements [25].

Recently, another novel approach to quantum state tomography has been proposed [48,49], which yields reliable error bounds similar to ours. A central difference between this approach and ours is the level of generality. In Refs. [48,49], a specific sequence of measurement operations is proposed, which is adapted to systems whose states are fairly pure. Under this condition, the estimate converges fast and, in addition, can be computed efficiently. In contrast, our method can be applied to arbitrary measurements (i.e., any tomographic data may be analyzed). Accordingly, the convergence of the confidence region depends on the choice of these measurements. However, we do not propose any specific algorithm for the efficient computation of confidence regions.

Finally, we refer to the very recent work of Blume-Kohout [33] for an excellent discussion of the notion of confidence regions in quantum state tomography. In particular, he shows that confidence regions, as considered here, can be defined via likelihood ratios.

We thank Robin Blume-Kohout for useful comments on earlier versions of this work. We acknowledge support from the Swiss National Science Foundation (Grants No. PP00P2-128455 and No. 200020-135048 and through the National Centre of Competence in Research "Quantum Science and Technology"), the German Science Foundation (Grant No. CH 843/2-1), and the European Research Council (Grant No. 258932).

*christandl@phys.ethz.ch
†renner@phys.ethz.ch

[1] A disk with (great-circle) radius Δ on the Bloch sphere has area $2\pi(1-\cos\Delta) \leq \pi\Delta^2$, whereas the full Bloch sphere has area 4π. Consequently, there are at least $(4\pi)/(\pi\Delta^2) = 4/\Delta^2$ such disks. Note also that the (great-circle) distance Δ between two pure states ϕ and ψ is related to their fidelity, $F(\phi,\psi) = |\langle\phi\psi\rangle| = |\cos\frac{\Delta}{2}|$, as well as to their trace distance, $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 = 2|\sin\frac{\Delta}{2}| \approx \Delta$.

[2] A. Holevo, Prob. Peredachi Inf. **9**, 31 (1973).

[3] The bound follows from the fact that the joint state of n identically prepared copies of a pure state in $\mathcal{H} = \mathbb{C}^2$ lies in the symmetric subspace of $\mathcal{H}^{\otimes n}$, which has dimension $n+1$.

[4] S. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory* (Prentice-Hall, Englewood Cliffs, 1993), Vol. 1.
[5] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[6] U. Fano, Rev. Mod. Phys. **29**, 74 (1957).
[7] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).
[8] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
[9] U. Leonhardt, H. Paul, and G. M. D'Ariano, Phys. Rev. A **52**, 4899 (1995).
[10] Z. Hradil, Phys. Rev. A **55**, R1561 (1997).
[11] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, in *Advances in Imaging and Electron Physics*, edited by P. W. Hawkes (Elsevier, New York, 2003), Vol. 128, pp. 205–308.
[12] T. Sugiyama, P. S. Turner, and M. Murao, Phys. Rev. A **83**, 012105 (2011).
[13] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, Phys. Rev. A **61**, 010304 (1999).
[14] Z. Hradil, J. Řeháček, J. Fiurášek, and M. Ježek, in *Quantum State Estimation*, edited by M. Paris and J. Řeháček (Springer, New York, 2004), pp. 59–112.
[15] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).
[16] C. F. Roos, G. P. T. Lancaster, M. Riebe, H. Häffner, W. Hänsel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. Lett. **92**, 220402 (2004).
[17] K. J. Resch, P. Walther, and A. Zeilinger, Phys. Rev. Lett. **94**, 070402 (2005).
[18] R. Blatt and D. Wineland, Nature (London) **453**, 1008 (2008).
[19] S. Filipp, P. Maurer, P. J. Leek, M. Baur, R. Bianchetti, J. M. Fink, M. Göppl, L. Steffen, J. M. Gambetta, A. Blais *et al.*, Phys. Rev. Lett. **102**, 200402 (2009).
[20] J. P. Home, D. Hanneke, J. D. Jost, J. M. Amini, D. Leibfried, and D. J. Wineland, Science **325**, 1227 (2009).
[21] J. T. Barreiro, M. Müller, P. Schindler, D. Nigg, T. Monz, M. Chwalla, M. Hennrich, C. F. Roos, P. Zoller, and R. Blatt, Nature (London) **470**, 486 (2011).
[22] K. R. W. Jones, Ann. Phys. (N.Y.) **207**, 140 (1991).
[23] V. Bužek, R. Derka, G. Adam, and P. Knight, Ann. Phys. (N.Y.) **266**, 454 (1998).
[24] R. Schack, T. A. Brun, and C. M. Caves, Phys. Rev. A **64**, 014305 (2001).
[25] F. Tanaka and F. Komaki, Phys. Rev. A **71**, 052323 (2005).
[26] R. Blume-Kohout, New J. Phys. **12**, 043034 (2010).
[27] K. Audenaert and S. Scheel, New J. Phys. **11**, 023028 (2009).
[28] K. Usami, Y. Nambu, Y. Tsuda, K. Matsumoto, and K. Nakamura, Phys. Rev. A **68**, 022314 (2003).
[29] Z. Hradil, D. Mogilevtsev, and J. Řeháček, Phys. Rev. Lett. **96**, 230401 (2006).
[30] M. D. de Burgh, N. K. Langford, A. C. Doherty, and A. Gilchrist, Phys. Rev. A **78**, 052122 (2008).
[31] J. Řeháček, D. Mogilevtsev, and Z. Hradil, New J. Phys. **10**, 043022 (2008).
[32] R. J. T. B. Efron, *An Introduction to the Bootstrap* (Chapman and Hall, London, 1993).

[33] R. Blume-Kohout, arXiv:1202.5270.
[34] T. Sugiyama, P. S. Turner, and M. Murao, Phys. Rev. A **85**, 052107 (2012).
[35] R. Renner, Nature Phys. **3**, 645 (2007).
[36] G. Chiribella, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. Kendon, and S. Severini, Lecture Notes in Computer Science Vol. 6519 (Springer-Verlag, Berlin, 2011), pp. 9–25.
[37] For our technical treatment in the Supplemental Material [38], we also consider tests that act on a larger space, $(\mathcal{H} \otimes \mathcal{K})^{\otimes k}$, which includes purifications of the systems.
[38] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.109.120403 for precise statements and proofs of our technical results and a discussion of the practically important case of independent measurments.
[39] M. Hayashi, Commun. Math. Phys. **293**, 171 (2009).
[40] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[41] R. L. Hudson and G. R. Moody, Z. Wahrsch. Verw. Geb. **33**, 343 (1976).
[42] G. A. Raggio and R. F. Werner, Helv. Phys. Acta **62**, 980 (1989).
[43] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. (N.Y.) **43**, 4537 (2002).
[44] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[45] A. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[46] W. Matthews, S. Wehner, and A. Winter, Commun. Math. Phys. **291**, 813 (2009).
[47] More precisely, the bound on the parameter ϵ, which is usually exponentially decreasing in the size of the confidence region $\Gamma_{\mu_{B^n}}$, is tight up to a polynomial factor.
[48] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Phys. Rev. Lett. **105**, 150401 (2010).
[49] M. Cramer, M. B. Plenio, S. Flammia, D. Gross, S. Bartlett, R. Somma, O. Landon-Cardinal, Y.-K. Liu, and D. Poulin, Nature Commun. **1**, 149 (2010).