Quantum Information Processing (2023) 22:419
https://doi.org/10.1007/s11128-023-04167-y

Optimizing measurements sequences for quantum state verification

Weichao Liang[1] · **Francesco Ticozzi**[1] · **Giuseppe Vallone**[1]

Received: 5 July 2023 / Accepted: 24 October 2023 / Published online: 22 November 2023

Abstract
We consider the problem of deciding whether a given state preparation, i.e., a source of quantum states, is accurate; namely, it produces states close to a target one within a prescribed threshold. While most of the result in the literature considers the case in which the measurement operators can be arbitrarily chosen depending on the target state, obtaining favorable (Heisenberg) scaling, we focus on the case in which the measurements can be only chosen from a given set. We show that, in this case, the order of measurements is critical for quickly assessing accuracy. We propose and compare different strategies to compute optimal or suboptimal measurement sequences either relying solely on *a priori* information, i.e., the target state for state preparation, or actively adapting the sequence to the previously obtained measurements. Numerical simulations show that the proposed algorithms reduce significantly the number of measurements needed for verification and indicate an advantage for the adaptive protocol especially assessing faulty preparations.

Keywords Quantum state verification · Optimal measurement sequence · Off-line and adaptive strategies · Optimization

1 Introduction

Due to the unavoidable errors, noise or decoherence, realistic quantum devices do not always behave as expected. Various metrics can be used to characterize and benchmark a quantum device [1]. In this work, we focus on devices expected to reliably produce

✉ Weichao Liang
weichao.liang@yahoo.com

Francesco Ticozzi
ticozzi@dei.unipd.it

Giuseppe Vallone
vallone@dei.unipd.it

[1] Department of Information Engineering, University of Padova, 35131 Padova, Italy

some target state. Given an unknown quantum state in a d-dimensional Hilbert space $\mathcal{H}_d$, d^2-1 measurements are necessary in general for a full tomographic reconstruction of the corresponding density matrix [2].

However, in many situations, such as quantum telecommunication, quantum state preparation and quantum computation, we are more concerned with whether some experimentally accessible quantum state ρ_{exp} is accurate enough with respect to a target state ρ_0, representing the intended result of the preparation, processing or communication task, rather than fully reconstructing it. This problem is referred to as *quantum state certification* [3] and has been considered in the literature from multiple viewpoint.

Most of the research on state verification builds upon an hypothesis-testing framework [3, 4]. The main results show that the hypothesis "the unknown state is the target state" can be answered using strategies that achieve a Heisenberg scaling between the precision and the sample complexity. A key hypothesis to obtain these extremely favorable scaling is that the measurement operators used to test need leave the target state invariant, which directly translates in having false negatives with zero probability, so the errors come only from false positive. Moreover, if the measurement can be chosen depending on the state to be verified, these verification protocols only require two measurement settings for assessing an arbitrary bipartite pure state (see, e.g., [5]). The basic strategy can then be extended to include locality constraints, specific classes of target states, adversarial choices in the states to be tested, classical communication and more [4, 6–12].

In this work, we reconsider this task, in a different, more taxing scenario: We assume that *only a finite set of measurement is available and given, independently of the target state.* Under this assumption, the previously proposed optimal verification strategies cannot be applied in general, as it is possible that no measurement in the set leaves the target invariant. For this reason, we are going to need more measurements, and worse scaling between accuracy and sample complexity than the situation.

Of course, one way to tackle the problem would be to proceed with a full tomography of ρ [2] and then decide accuracy consequently. This is in general, however, not efficient as it requires to obtain averages for at least $d^2 - 1$ independent observables, and it does not leverage on prior information about the target state ρ_0. For example, if the target state is known to be pure, a smaller number of measurements are required via compressed sensing techniques [13].

In order to improve the verification performance, we here propose procedures that decide whether the state ρ is accurate within a prescribed tolerance, without necessarily obtaining a full tomography and thus still reducing the number of required observables. The central idea is to order the measurement sequence using the *a priori* information, so that the first measurements are the most informative when the state to be measured is indeed ρ_0. The procedure can also be seen as a way to optimize the order of the measured observables in a tomography depending on the best available estimate of the state at hand, in the spirit of [14].

The procedure we propose is of two types: The first ones compute the whole measurement sequence off-line and then uses it choose which measurements to actually perform, stopping as soon as verification can be decided. A crucial aspect, in practice, is in fact the computation of the optimal sequence. The latter is a nontrivial

optimization problem that has to be solved in a number of instances that scale combinatorially with the number of measurements, which in turn grows at least quadratically in the dimension of the space. For this reason, even off-line calculation becomes of optimal sequences becomes rapidly impractical. In order to address this problem, we propose iterative algorithms, which determine the best next measurements given the previously chosen ones. Two versions are provided, where the second one relies on a relaxation of the constraints that allows for an analytic treatment. These ways of constructing the sequence, albeit suboptimal, are computationally treatable and offer another advantage: They lend themselves to be used as adaptive strategies, which rely on the previously obtained actual measurements rather than just the target state. In fact, the second type of verification method we propose is an *adaptive* strategy, where the next measurement is chosen based on the best available estimate given the actual measurement performed to that point. The different methods are tested with a paradigmatic example: a two-qubit state where only local Pauli measurements are available. The results highlight the flexibility of the adaptive method, which performs well even in the case of inaccurate priors.

2 Problem setting and verification criteria

We denote by $\mathcal{B}(\mathcal{H})$ the set of all linear operators on a finite-dimensional Hilbert space $\mathcal{H}$. Define $\mathcal{B}_*(\mathcal{H}):=\{X \in \mathcal{B}(\mathcal{H}) | X = X^\dagger\}$ and $\mathcal{B}_{>0}(\mathcal{H}):=\{X \in \mathcal{B}(\mathcal{H}) | X > 0\}$. $\mathrm{Tr}(A)$ indicates the trace of $A \in \mathcal{B}(\mathcal{H})$. We define $\mathcal{S}(\mathcal{H}_d):=\{\rho \in \mathcal{B}_*(\mathcal{H}_d) |\, \rho \geq 0, \mathrm{Tr}(\rho) = 1\}$ as the set of all physical density matrices on $\mathcal{H}_d$.

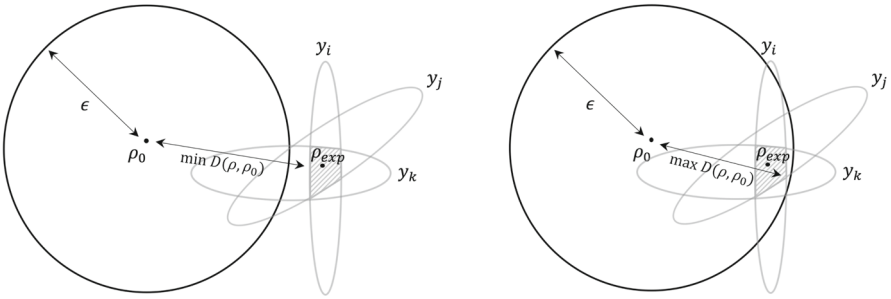
In order to precisely specify the verification task, we introduce the following definition, which depends on the choice of a relevant distance-like function.

Definition 1 ((ϵ, D, ρ_0)-accurate) Given a target state $\rho_0 \in \mathcal{S}(\mathcal{H}_d)$ and a (pseudo-)distance function D on $\mathcal{S}(\mathcal{H}_d)$, the density matrix $\rho \in \mathcal{S}(\mathcal{H}_d)$ is called (ϵ, D, ρ_0)-accurate if $D(\rho, \rho_0) \leq \epsilon$ with $\epsilon \geq 0$.

Consider a set of observables, represented by Hermitian matrices $\{A_i\}_{i=1}^R$, where R is a positive integer. This set of observables is called information-complete if $\{A_i\}_{i=1}^R$ generate the set of all d-dimensional traceless Hermitian matrices. Note that a necessary condition for the observables to be information-complete is $R \geq d^2$. If $\{A_i\}_{i=1}^R$ is information-complete and the measurement statistics $\{\hat{y}_i\}_{i=1}^R$ are known exactly, i.e., $\hat{y}_i = y_i := \mathrm{Tr}(\rho_{\mathrm{exp}} A_i)$ with $i \in \{1, \ldots, R\}$, then there is a unique state compatible with the constraints, that is, the generated state ρ_{exp}. Throughout this paper, we suppose that set of observables is *finite, information-complete and fixed.* The problem we will be concerned with is the following,

Problem 1 *Based on the* a priori *state ρ_0 and available data $\{\hat{y}_i\}_{i=1}^K$ with $K \leq R$, determine the optimal order of A_k to verify if the generated state ρ_{exp} is (ϵ, D, ρ_0)-accurate via as few measurements as possible.*

In order to introduce the central idea of the work, let us assume for now that a certain sequence of the available observables has been decided. There are two cases



(a) **C1**: $\rho_{\rm exp}$ is determined not to be (ϵ, D, ρ_0)-accurate

(b) **C2**: $\rho_{\rm exp}$ is determined to be (ϵ, D, ρ_0)-accurate

Fig. 1 Diagrams corresponding to the quantum state verification criteria **C1** and **C2**. The gray area represents $\bar{\mathbf{S}}_i \cap \bar{\mathbf{S}}_j \cap \bar{\mathbf{S}}_k$, i.e., the states compatible with the measurement data y_i, y_j and y_k

in which the verification process can be terminated, establishing whether the generate state is (ϵ, D, ρ_0)-accurate or not with a minimum of measurements. Suppose that the measurements are perfect, namely the available data y_i satisfy $y_i = \mathrm{Tr}(A_i \rho_{\rm exp})$. Denote by $\bar{\mathbf{S}}_i := \{\rho \in \mathcal{S}(\mathcal{H}_d) | \, \mathrm{Tr}(\rho A_i) = y_i\}$ the set of states compatible with the measurement data y_i. Based on $\{y_i\}_{i=1}^K$, two criteria can be used to verify if the generated state $\rho_{\rm exp}$ is (ϵ, D, ρ_0)-accurate in each step:

C1. If $\min_{\rho \in \bigcap_{i=1}^K \bar{\mathbf{S}}_i} D(\rho, \rho_0) > \epsilon$, $\rho_{\rm exp}$ is not (ϵ, D, ρ_0)-accurate;

C2. If $\max_{\rho \in \bigcap_{i=1}^K \bar{\mathbf{S}}_i} D(\rho, \rho_0) \leq \epsilon$, $\rho_{\rm exp}$ is (ϵ, D, ρ_0)-accurate.

Depictions of the situations corresponding to the above two criteria **C1** and **C2** are shown in Figure 1. **C1** guarantees that all states compatible with the measurement data are outside of the ball of radius ϵ around the target state ρ_0, while **C2** ensures that the same states are all inside.

In the following sections, we shall leverage the criteria above in order to devise optimal measurement sequences, or suboptimal ones that present computational advantages and can be adapted to the actual measurement outcomes.

3 Verification of quantum state based on the *a priori* state

In this section, we first introduce a strategy of determining the measurement sequence M off-line based only on the *a priori* target state ρ_0, i.e., without using the measurement data. We next use the sequence M to verify that the generated state $\rho_{\rm exp}$ is or is not (ϵ, D, ρ_0) accurate according to the criteria **C1** and **C2**. The objective is to perform as few measurements as possible to achieve verification.

3.1 Off-line construction of the optimal measurement sequence

From an experimental point of view, it is arguably easier to determine the whole sequence of measurements before performing them. We shall start by exploring this

approach, while the adaptive approach, in which the next measurement is chosen depending on the outcome of the previous ones, will be treated in Section 4.

Denote by $\mathbf{S}_i(\rho_0) := \{\rho \in \mathcal{S}(\mathcal{H}_d) | \operatorname{Tr}(\rho A_i) = \operatorname{Tr}(\rho_0 A_i)\}$, the set of density matrices compatible with the measurement A_i that we would have if the state was actually $\rho_0 \in \mathcal{S}(\mathcal{H}_d)$. While relying only on prior information, with no true measurements data available, we use $\mathbf{S}_i(\rho_0)$ to replace the constraints $\bar{\mathbf{S}}_i$ in the criteria **C1** and **C2**. Note that $\mathbf{S}_i(\rho_0) = \bar{\mathbf{S}}_i$ if the state is perfect generated, i.e., $\operatorname{Tr}(\rho_0 A_i) = y_i$.

Obviously, since $\rho_0 \in \mathbf{S}_i(\rho_0)$ for all $i \in \{1, \ldots, R\}$ by construction, then in this scenario **C1** can never be satisfied. Thus, we only exploit **C2** to determine the order of measurements. Suppose that the distance function D is continuous on $\mathcal{S}(\mathcal{H}_d)$, e.g., any matrix norm, quantum relative entropy, etc., (see [15, Chapter 9, 11] for standard options), due to the compactness of $\bigcap_i \mathbf{S}_i(\rho_0)$, $\max_{\rho \in \bigcap_i \mathbf{S}_i(\rho_0)} D(\rho, \rho_0)$ exists.

If the state was actually ρ_0, the minimal amount of measurements that allow to determine that the preparation was indeed accurate would correspond, according to **C2**, to the minimum n for which there exists a set of measurements indexes $\mathsf{M}_n \subset \{1, \ldots, R\}$ such that

$$\max_{\rho \in \bigcap_{i \in \mathsf{M}_n} \mathbf{S}_i(\rho_0)} D(\rho, \rho_0) \leq \epsilon,$$

and the optimal sequence would be any permutation of the M_n.

The Algorithm OS could be used to generate one such optimal sequence.

Algorithm OS: Optimal verification Sequence based on ρ_0

- **Initialization:** Define the set $\mathsf{S} = \{1, \ldots, R\}$ and set $k = 1$.
- **Step 1:** Denote a k elements sequence by $\mathsf{M}_k := (m_{k,1}, \ldots, m_{k,k}) \in \mathsf{S}^k$. Compute $\overline{\mathsf{M}}_k \in \arg\min_{\mathsf{M}_k \in \mathsf{S}^k} \left(\max_{\rho \in \bigcap_{i \in \mathsf{M}_k} \mathbf{S}_i(\rho_0)} D(\rho, \rho_0) \right)$.
  If $\max_{\rho \in \bigcap_{i \in \overline{\mathsf{M}}_k} \mathbf{S}_i(\rho_0)} D(\rho, \rho_0) \leq \epsilon$ **stop the procedure**. Otherwise, update $k = k + 1$.
- **Step 2:** Repeat **Step 1** until $k = d^2$.

Note that each step of above algorithm is independent, thus for some $i < j$, $\overline{\mathsf{M}}_i \not\subset \overline{\mathsf{M}}_j$. At the end of process, we obtain a sequence of measurements $\overline{\mathsf{M}}_n$ containing $n \leq R$ elements, whose corresponding observables are the optimal choice for the verification of (ϵ, D, ρ_0) accuracy of $\rho_{\text{exp}} = \rho_0$. The order of the elements belonging to $\overline{\mathsf{M}}_n$ is not important. However, the computational complexity of the above algorithm is too large; in order to determine $\overline{\mathsf{M}}_n$, it needs to solve $\sum_{k=1}^{n} \binom{n}{k} = 2^n - 1$ optimization problems. Moreover, in practice, the generated state ρ_{exp} is usually different from the target state ρ_0, and thus, the generated measurement sequence $\overline{\mathsf{M}}_n$ by Algorithm OS with respect to ϵ may not be able to verify the accuracy of ρ_{exp}. To obtain a tomographically complete sequence, one needs to add $d^2 - n$ linearly independent measurements operators from the available set.

3.2 Iterative construction of verification sequences

In order to address the above issues, we propose to construct the sequence of measurements iteratively, based on the previous determined measurement indexes, which can greatly reduce the computational complexity and allow to extend the procedure to the full observable set. The resulting sequence will be in general suboptimal with respect to ρ_0, but still yields an advantage with respect to a random sequence of observables, as shown in Section 5.

3.2.1 Optimization-based approach

The general algorithm we propose works as follows: It starts by evaluating, for each measurement A_i, the maximal distance α_i with respect to ρ_0 of the states ρ belonging to $\mathbf{S}_i(\rho_0)$, the set of states that are compatible with the measurement outcome $\mathrm{Tr}(\rho A_i) = \mathrm{Tr}(\rho_0 A_i)$. The measurement giving the minimum value of α_i is selected as first measurement A_{m_1}, and the corresponding maximum distance is $\alpha^1_{m_1}$. Now, the next measurement $A_{m_{i+1}}$ is chosen so that it is linearly independent on the previously chosen ones and at the same time minimizes the maximum distance of the new compatible set with the measurement of *all the previously selected* $A_{m_1}, \ldots, A_{m_i}$. The minimum worst-case distance among compatible states α^n_i, with n indicating the iteration and i the selected measurement, is chosen as an indicator of how likely it is that checking **C2** will allow us to determine whether the actual state is (ϵ, D, ρ_0)-accurate.

A more formal form of the above algorithm is summarized as Algorithm IOS.

Algorithm IOS: Iteratively Optimized Sequence based on ρ_0

- **Initialization:** Define the sets $\mathsf{M} = \emptyset$ and $\mathsf{S} = \{1, \ldots, R\}$. Set $k = 0$.
- **Step 1:** Define $\bar{\mathsf{S}}$ as the set of all $i \in \mathsf{S}$ such that $A_i \notin \mathrm{span}\{A_n\}_{n\in\mathsf{M}}$. Set $k = k + 1$. For all $i \in \bar{\mathsf{S}}$, compute $\alpha^k_i := \max_{\rho\in\bigcap_{n\in\mathsf{M}} \mathbf{S}_n(\rho_0)\cap\mathbf{S}_i(\rho_0)} D(\rho, \rho_0)$.

  If $\min_{i\in\bar{\mathsf{S}}}\alpha^k_i = 0$, set $\mathsf{M} = \mathsf{M} \cup \bar{\mathsf{S}}$ and **stop the process**: In this case, ρ_0 must belong to the span of the selected measurements.

  Otherwise, compute $\mathrm{argmin}_{i\in\bar{\mathsf{S}}}\alpha^k_i$. If arg min output a single integer, set $m_k = \arg\min_{i\in\bar{\mathsf{S}}}\alpha^k_i$. If arg min output multiple integers, designate a unique m_k in that set, according to some deterministic rule or at random: In this case, the criteria we consider do not lead to a preferred choice.

  Update $\mathsf{M} = \mathsf{M} \cup \{m_k\}$, $\mathsf{S} = \mathsf{S} \setminus \{m_k\}$.
- **Step 2:** Repeat **Step 1** until $\mathrm{card}(\mathsf{M}) = d^2$

At the end of the procedure, M is a ordered sequence of measurements, from the most to the less informative based on *a priori* state. Note that, at the end of Step 2, we obtain a sequence of measurements containing n linearly independent observables, from which the target state ρ_0 can be reconstructed via tomography. By construction $\alpha^1_{m_1} \geq \alpha^2_{m_2} \geq \cdots \geq \alpha^n_{m_n}$ is a decreasing sequence of the maximum distance from ρ_0 of the states compatible with the measurement. However, in practice $\rho_{\mathrm{exp}} \neq \rho_0$, for the case of $n < d^2$, the n observables may not be sufficient to verify the accuracy of ρ_{exp}. Thus, we need to complete the sequence with additional $d^2 - n$ linearly independent observables, which we can choose at random or according to other criteria.

3.2.2 Analytic approach based on distance bound

The computational complexity of Algorithm IOS is still highly dependent on the number of optimization problems to be solved that, albeit reduced with respect to the optimal *a priori* sequence, still increases quadratically with the dimension of the Hilbert space. To address this issue, we provide an approximation of Algorithm IOS when the Hilbert–Schmidt distance is chosen as the distance function. In this case, we are not ordering the measurements by evaluating the exact maximal distance of the set of states compatible with the measurement (i.e., the α_i^k values), but instead by evaluating an upper bound of such distance that can be expressed analytically.

The Hilbert–Schmidt distance is defined as

$$d_{HS}(\rho_0, \sigma) := \sqrt{\mathrm{Tr}(\rho_0 - \sigma)^2}, \quad \forall\, \rho_0, \sigma \in \mathcal{S}(\mathcal{H}_d),$$

In the following proposition, we provide an upper bound of the distance on the target state ρ_0 for states σ that are compatible with ρ_0 according to a set of observables $\{A_i\}_{i=1}^K$ where $K \leq R$.

Proposition 1 *Given a state $\rho_0 \in \mathcal{S}(\mathcal{H}_d)$ and a set of observables $A_i \in \mathcal{B}_*(\mathcal{H}_d)$ with $i \in \{1, \ldots, K\}$, for any $\sigma \in \bigcap_{i=1}^K \mathbf{S}_i(\rho_0)$, then*

$$d_{HS}(\rho_0, \sigma) \leq \sqrt{1 - \mathrm{Tr}(\varrho_K^2)} + \sqrt{\mathrm{Tr}(\rho_0^2) - \mathrm{Tr}(\varrho_K^2)} \tag{1}$$

where ϱ_K is the projection of ρ_0 in the subspace spanned by the operators $\{A_i\}_{i=1}^K$.

Proof The square of the Hilbert–Schmidt distance can be written as $d_{HS}^2(\sigma, \rho_0) = \mathrm{Tr}(\rho_0^2) + \mathrm{Tr}(\sigma^2) - 2\mathrm{Tr}(\sigma\rho_0) \leq 1 + \mathrm{Tr}(\rho_0^2) - 2\mathrm{Tr}(\sigma\rho_0)$. Any state $\sigma \in \bigcap_i \mathbf{S}_i(\rho_0)$ satisfies $\mathrm{Tr}(\sigma A_i) = \mathrm{Tr}(\rho_0 A_i)$ for all $i \in \{1, \ldots, K\}$. Therefore, the orthogonal projection of ρ_0 and σ on the space spanned by the operators $\{A_i\}_{i=1}^K$ is the same: We can defined it as ϱ_K. We can thus write $\rho_0 = \varrho_K + \varrho_K^\perp$ and $\sigma = \varrho_K + \varsigma_K^\perp$ with $\varrho_K^\perp$ and $\varsigma_K^\perp$ orthogonal to ϱ_K according to the Hilbert–Schmidt inner product, i.e., $\langle \rho, \sigma \rangle_{HS} = \mathrm{Tr}(\rho^* \sigma)$. Therefore, $\mathrm{Tr}(\rho_0\sigma) = \mathrm{Tr}(\varrho_K^2) + \mathrm{Tr}(\varrho_K^\perp \varsigma_K^\perp)$. Moreover, the equations $\mathrm{Tr}(\rho_0^2) = \mathrm{Tr}(\varrho_K^2) + \mathrm{Tr}[(\varrho_K^\perp)^2]$ and $\mathrm{Tr}(\sigma^2) = \mathrm{Tr}(\varrho_K^2) + \mathrm{Tr}[(\varsigma_K^\perp)^2] \leq 1$ imply that $\mathrm{Tr}[(\varrho_K^\perp)^2] = \mathrm{Tr}(\rho_0^2) - \mathrm{Tr}(\varrho_K^2)$ and $\mathrm{Tr}[(\varsigma_K^\perp)^2] \leq 1 - \mathrm{Tr}(\varrho_K^2)$. From the Cauchy–Schwarz inequality, we have that $\mathrm{Tr}(\varrho_K^\perp \varsigma_K^\perp) \geq -\sqrt{\mathrm{Tr}[(\varrho_K^\perp)^2]\mathrm{Tr}[(\varsigma_K^\perp)^2]} \geq -\sqrt{\mathrm{Tr}(\rho_0^2) - \mathrm{Tr}(\varrho_K^2)}\sqrt{1 - \mathrm{Tr}(\varrho_K^2)}$. We have therefore proved that

$$\mathrm{Tr}(\rho_0\sigma) \geq \mathrm{Tr}(\varrho_K^2) - \sqrt{\mathrm{Tr}(\rho_0^2) - \mathrm{Tr}(\varrho_K^2)}\sqrt{1 - \mathrm{Tr}(\varrho_K^2)} \tag{2}$$

and the main proposition follows. □

Remark 1 We would like to point out that if the target state ρ_0 is pure (i.e., $\mathrm{Tr}(\rho_0^2) = 1$), the upper bound given in (1) simplifies to

$$d_{HS}(\rho_0, \sigma) \leq 2\sqrt{1 - \mathrm{Tr}(\varrho_K^2)}. \tag{3}$$

Moreover, a similar bound also holds when the Bures metric is employed and the target state ρ_0 is pure. Indeed, when ρ_0 is pure, the Bures distance is written as $d_B(\rho_0,\sigma)=\sqrt{2(1-\sqrt{\mathrm{Tr}(\rho_0\sigma)}}$. Therefore, by following similar step it is possible to demonstrate that, for pure ρ_0 for which $\mathrm{Tr}(\varrho_K^2)\geq 1/2$ we have

$$d_B^2(\rho_0,\sigma)\leq 2(1-\sqrt{2\mathrm{Tr}(\varrho_K^2)-1}). \tag{4}$$

Lastly, the bound (1) can be interpreted geometrically. The states σ are written as $\sigma=\varrho_K+\varsigma_K^{\perp}$ with fixed ϱ_K. Therefore, the states σ are contained within a ball centered in ϱ_K and radius $R_K=\max\sqrt{\mathrm{Tr}[(\varsigma_K^{\perp})^2]}=\sqrt{1-\mathrm{Tr}(\varrho_K^2)}$. The state $\rho_0=\varrho_K+\varrho_K^{\perp}$ also belongs to such ball, but its distance from the center is given by $d_K=d_{HS}(\rho_0,\varrho_K)=\sqrt{\mathrm{Tr}[(\varrho_K^{\perp})^2]}=\sqrt{\mathrm{Tr}(\rho_0^2)-\mathrm{Tr}(\varrho_K^2)}$. Therefore, the maximum distance between ρ_0 and σ is indeed bounded by R_K+d_K, as in (1). Notice that, by starting from a set of linear independent observables $\{A_i\}$, adding an extra observable A_j will improve the bound.

Proposition 2 *Assume we have fixed the first $\{A_i\}_{i=1}^K$ and we add a further measurement operator A_{K+1}. Let $\{\Gamma_i\}$ be an orthonormal basis of the space spanned by the $\{A_i\}_{i=1}^K$. Define $A_{K+1}^{\perp}=A_{K+1}-\sum_i\mathrm{Tr}(\Gamma_i A_{K+1})\Gamma_i$. Then, the projected state becomes:*

$$\varrho_{K+1}=\varrho_K+\frac{\mathrm{Tr}(\rho_0 A_{K+1}^{\perp})}{\mathrm{Tr}[(A_{K+1}^{\perp})^2]}A_{K+1}^{\perp} \tag{5}$$

The latter also implies $\|\varrho_{K+1}\|_{HS}^2=\|\varrho_K\|_{HS}^2+\frac{\mathrm{Tr}^2(\rho_0 A_{K+1}^{\perp})}{\|A_{K+1}^{\perp}\|_{HS}^2}$.

Proof We can write $\rho_0=\varrho_K+\alpha A_{K+1}^{\perp}+\tau_{K+1}^{\perp}$, with $A_{K+1}^{\perp}$ orthogonal to all A_i's and $\tau_{K+1}^{\perp}$ orthogonal to both ϱ_K and $A_{K+1}^{\perp}$. Since $\mathrm{Tr}(\rho_0 A_{K+1})=\mathrm{Tr}(\varrho_K A_{K+1})+\alpha\mathrm{Tr}(A_{K+1}A_{K+1}^{\perp})$, we can determine $\alpha=\mathrm{Tr}[(\rho_0-\varrho_K)A_{K+1}]/\mathrm{Tr}(A_{K+1}A_{K+1}^{\perp})$. Thus, the projection of ρ_0 into the subspace spanned by the $\{A_i\}$ and A_{K+1} is given by:

$$\varrho_{K+1}=\varrho_K+\frac{\mathrm{Tr}[(\rho_0-\varrho_K)A_{K+1}]}{\mathrm{Tr}(A_{K+1}^2)-\sum_i[\mathrm{Tr}(A_{K+1}\Gamma_i)]^2}A_{K+1}^{\perp}. \tag{6}$$

More in detail, write $\varrho_K:=\sum_n\mathrm{Tr}(\rho_0\Gamma_n)\Gamma_n$ and $A_{K+1}=A_{K+1}^{\perp}+\Omega_{K+1}$ with $\Omega_{K+1}:=\sum_n\mathrm{Tr}(A_{K+1}\Gamma_n)\Gamma_n$, where $\mathrm{Tr}(\Gamma_n\Gamma_m)=\delta_{n,m}$. We have $\mathrm{Tr}(\varrho_K A_{K+1}^{\perp})=0$, $\mathrm{Tr}(\rho_0\Omega_{K+1})=\sum_n\mathrm{Tr}(A_{K+1}\Gamma_n)\mathrm{Tr}(\rho_0\Gamma_n)$ and

$$\begin{aligned}\mathrm{Tr}(\varrho_K\Omega_{K+1})&=\textstyle\sum_n\mathrm{Tr}(\rho_0\Gamma_n)\mathrm{Tr}(\Omega_{K+1}\Gamma_n)\\&=\textstyle\sum_n\mathrm{Tr}(\rho_0\Gamma_n)\mathrm{Tr}\big(\sum_m\mathrm{Tr}(A_{K+1}\Gamma_m)\Gamma_m\Gamma_n\big)\\&=\textstyle\sum_{n,m}\mathrm{Tr}(\rho_0\Gamma_n)\mathrm{Tr}(A_{K+1}\Gamma_m)\mathrm{Tr}(\Gamma_m\Gamma_n)\\&=\textstyle\sum_n\mathrm{Tr}(\rho_0\Gamma_n)\mathrm{Tr}(A_{K+1}\Gamma_n)=\mathrm{Tr}(\rho_0\Omega_{K+1}).\end{aligned}$$

From the latter, we have that:

$$\begin{aligned}\mathrm{Tr}\big((\rho_0-\varrho_K)A_{K+1}\big) &= \mathrm{Tr}\big((\rho_0-\varrho_K)(A_{K+1}^{\perp}+\Omega_{K+1})\big)\\ &= \mathrm{Tr}(\rho_0 A_{K+1}^{\perp}) - \mathrm{Tr}(\varrho_K A_{K+1}^{\perp}) + \mathrm{Tr}(\rho_0\Omega_{K+1}) - \mathrm{Tr}(\varrho_K\Omega_{K+1})\\ &= \mathrm{Tr}(\rho_0 A_{K+1}^{\perp}).\end{aligned}$$

Hence,

$$\varrho_{K+1} = \varrho_K + \frac{\mathrm{Tr}[(\rho_0-\varrho_K)A_{K+1}]}{\mathrm{Tr}(A_{K+1}^2) - \sum_i[\mathrm{Tr}(A_{K+1}\Gamma_i)]^2}A_{K+1}^{\perp} = \varrho_K + \frac{\mathrm{Tr}(\rho_0 A_{K+1}^{\perp})A_{K+1}^{\perp}}{\|A_{K+1}^{\perp}\|_{HS}^2}.$$

□

Notice that the rhs of (1) represents an upper bound on the parameter α_i^k defined in Algorithm IOS. Since $\|\varrho_K\|_{HS} = \sqrt{\mathrm{Tr}(\varrho_K^2)}$, according to Proposition 1, the norm $\|\varrho_K\|_{HS}$ of the projection ϱ_K of ρ_0 over the subspace spanned by a subset of observables $\{A_i\}$ is an useful parameter to optimize the sequence of the measurements. The larger is $\|\varrho_K\|_{HS}$, the lower the upper bound on $d_{HS}(\rho_0,\sigma)$. Therefore, the measurement sequence should be chosen in order to maximize the norm of such projection at each step, since the upper bound (1) is monotonically non-increasing with respect to the norm of the projection. To this aim, it is sufficient to select an observable A_{K+1} which maximizes the value of $\frac{\mathrm{Tr}^2(\rho_0 A_{K+1}^{\perp})}{\|A_{K+1}^{\perp}\|_{HS}^2}$ at each step.

A more formal form of the above algorithm is summarized as Algorithm IAS.

Algorithm IAS: Iterative Sequence based on ρ_0 and the Analytic bound

- **Initialization:** Define the sets $\mathsf{M} = \emptyset$ and $\mathsf{S} = \{1,\ldots,R\}$. Set $k = 1$.
- **Step 1:** For all $j \in \mathsf{S}$, compute $A_j^{\perp} = A_j - \sum_{i\in\mathsf{M}}\mathrm{Tr}(A_j\Gamma_i)\Gamma_i$, and $\omega_j^{(k)} = \frac{\mathrm{Tr}^2(\rho_0 A_j^{\perp})}{\|A_j^{\perp}\|_{HS}^2}$ for all $j \in \mathsf{S}$. Then, define the index $m_k \in \arg\max_{j\in\mathsf{S}}\omega_j^{(k)}$, and the matrix $\Gamma_{m_k} = \frac{A_{m_k}^{\perp}}{\|A_{m_k}^{\perp}\|_{HS}}$. Update $\mathsf{M} = \mathsf{M}\cup\{m_k\}$, $\mathsf{S} = \mathsf{S}\setminus\{m_k\}$. Set $k = k+1$.
- **Step 2:** Repeat **Step 1** until $\mathrm{card}(\mathsf{M}) = d^2$.

Note that if $\omega_j^{(k)} = 0$, then $\rho_0 \in \mathrm{span}\{\Gamma_{m_1},\ldots,\Gamma_{m_{k-1}}\}$. If the arg max in the algorithm above produces more than a single index, one is chosen at random in the set. The sequence is generated by increasing as much as possible in each cycle the value of $\|\varrho_k\|_{HS}$. At the end of the procedure, M corresponds to an ordered sequence of d^2 linearly independent measurement operators based on the upper bound on the distance from ρ_0 provided above.

3.3 Verification algorithm based on the measurement sequence

Once we obtained the measurement sequence M using one of the algorithms above, we can perform the Algorithm VM to verify whether the generated state ρ_{exp} is (ϵ, D, ρ_0)-accurate according to **C1** and **C2**.

Algorithm VM: Verification of the quantum state based on M

- **Initialization:** Set $\mathsf{N} = \{m_1\}$ and $k = 1$.
- **Step 1:** Perform the measurements of A_{m_k} and collect the sampled average output y_{m_k}. Compute $\gamma_k := \min_{\rho \in \bigcap_{n\in\mathsf{N}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$, $\Gamma_k := \max_{\rho \in \bigcap_{n\in\mathsf{N}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$.
  - If $\gamma_k > \epsilon$, then ρ_{exp} is not (ϵ, D, ρ_0)-accurate and **stop the procedure**;
  - If $\Gamma_k \leq \epsilon$, then ρ_{exp} is (ϵ, D, ρ_0)-accurate and **stop the procedure**;
  - Otherwise, update $k = k + 1$ and $\mathsf{N} = \mathsf{N} \cup \{m_k\}$.
- **Step 2:** Repeat **Step 1** until $k = d^2$.

Remark 2 At the end of the above algorithm, if the procedure ends with $k = d^2$, we can reconstruct the generated state $\rho_{\text{exp}} = \sum_{i\in\mathsf{N}} c_i A_i$ where $\{c_i\}_{i\in\mathsf{N}}$ can be computed, for example, by

$$\begin{bmatrix} c_1 \\ \vdots \\ c_K \end{bmatrix} = \begin{bmatrix} \text{Tr}(A_1 A_1) & \dots & \text{Tr}(A_1 A_K) \\ \vdots & \ddots & \vdots \\ \text{Tr}(A_K A_1) & \dots & \text{Tr}(A_K A_K) \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ \vdots \\ y_K \end{bmatrix}. \tag{7}$$

While all measurements need to be performed in this case, and there is no advantage in having ordered them, it is of course not possible to know in advanced that this will be the case. Moreover, the computational overhead from ordering measurements becomes negligible if the verification task has to be performed many times.

4 Adaptive quantum state verification

In the previously proposed algorithms, the measurement sequence was determined off-line (i.e., without performing any measurement) by only leveraging the information on the a priori state ρ_0. Here, we optimize the verification procedure Algorithm IOS and Algorithm IAS by also exploiting the measurement data at each step in addition to the *a priori* state to determine the next measurement and then verify the state. We call such protocol *adaptive verification.*

For now, suppose that the *measurements are perfect*: Namely the sampled output averages correspond to the true expected values for the actual state. We initialize the algorithm as same as in Algorithm IOS, since before perform the measurements, the *a priori* state is the only accessible information. Compute $\alpha_i^1 := \max_{\rho\in\mathbf{S}_i(\rho_0)} D(\rho, \rho_0)$ for all $i \in \{1, \dots, R\}$ and $m_1 \in \arg\min_{i\in\{1,\dots,R\}} \alpha_i^1$. If arg min cannot assign an unique m_1, then we consider the following rule: select an observable at random

among those indicated by the criterion of Algorithm IAS, namely those maximizing $\mathrm{Tr}^2(\rho_0 A_j^{\perp})/\|A_j^{\perp}\|_{HS}^2$. Then, we perform the measurement A_{m_1} and obtain an empirical estimate of $y_{m_1} = \mathrm{Tr}(\rho_{\mathrm{exp}} A_{m_1})$. For the sake of simplicity in presenting the algorithm, we shall here assume we actually obtain the exact value y_{m_1}. The case of imperfect estimates can be treated along the same lines. In order to test both criteria **C1** and **C2**, we compute

$$\omega_1 := \min_{\rho \in \bar{\mathbf{S}}_{m_1}} D(\rho, \rho_0), \qquad \Omega_1 := \max_{\rho \in \bar{\mathbf{S}}_{m_1}} D(\rho, \rho_0).$$

If $\omega_1 > \epsilon$, then ρ_{exp} is not (ϵ, D, ρ_0)-accurate and if $\Omega_1 \leq \epsilon$, then ρ_{exp} is (ϵ, D, ρ_0)-accurate. Otherwise, we determine an estimate of ρ_{exp} based on the measurement data y_{m_1} by $\rho_1 = \arg\min_{\rho \in \bar{\mathbf{S}}_{m_1}} f_{\rho_0}(\rho)$, where $f_{\rho_0}(\rho)$ is a continuous function such that $\rho_0 = \arg\min_{\rho \in \mathcal{S}(\mathcal{H}_d)} f_{\rho_0}(\rho)$, quantifying information distance between $\rho \in \mathcal{S}(\mathcal{H}_d)$ and $\rho_0 \in \mathcal{S}(\mathcal{H}_d)$. Common choices for f can be the quantum relative entropy [14], or any distance function on $\mathcal{S}(\mathcal{H}_d)$ [15, Chapter 9]. Strictly convex functions guarantee the uniqueness of the minimum. For all $i \in \{1, \ldots, R\} \setminus \{m_1\}$, according to the criteria **C1** and **C2**, we compute

$$\delta_i^1 := \min_{\rho \in \mathbf{S}_i(\rho_1) \cap \bar{\mathbf{S}}_{m_1}} D(\rho, \rho_0), \qquad \Delta_i^1 := \max_{\rho \in \mathbf{S}_i(\rho_1) \cap \bar{\mathbf{S}}_{m_1}} D(\rho, \rho_0),$$

where $\Delta_i^1 \geq \delta_i^1 \geq 0$ and $\mathbf{S}_i(\rho_1) = \{\rho \in \mathcal{S}(\mathcal{H}_d) | \, \mathrm{Tr}(\rho A_i) = \mathrm{Tr}(\rho_1 A_i)\}$. Notice that the constrained set now is computed for ρ_1, which depends on the actual measurement outcomes. Intuitively, the smaller $\epsilon - \delta_i^1$ (resp. $\Delta_i^1 - \epsilon$) is, the more likely **C1** (resp. **C2**) is verified (see Figure 2).

If for some i we have that $\Delta_i^1 \geq \delta_i^1 > \epsilon$ or $\epsilon > \Delta_i^1 \geq \delta_i^1$, it means that choosing the corresponding measurement is expected to bring the compatible set closer to verify criteria **C1** or **C2**, respectively. However, if there exists i such that $\delta_i^1 = 0$, it implies that $\min\{\epsilon - \delta_i^1, \Delta_i^1 - \epsilon\} = \epsilon$ and $\rho_0 \in \mathbf{S}_i(\rho_1) \cap \bar{\mathbf{S}}_{m_1}$, which means that **C1** cannot yield the conclusion. Thus, if $\delta_i^1 = 0$ for all i, only Δ_i^1 provides the information for the selection of the next measurement. Therefore, in order to maximize the possibility of the successful verification, we set

$$m_2 \in \begin{cases} \arg\min_{i \in \mathsf{S}} \Delta_i^1, & \delta_i^1 = 0, \forall i \\ \arg\min_{i \in \mathsf{S}} \left\{ \min\{\epsilon - \delta_i^1, \Delta_i^1 - \epsilon\} \right\}, & \text{else.} \end{cases}$$

If arg min cannot assign an unique m_2, then we can select one by employing the idea of Algorithm IAS, that is to select an observable at random among those which maximize $\mathrm{Tr}^2(\rho_1 A_j^{\perp})/\|A_j^{\perp}\|_{HS}^2$.

Then, the whole procedure of verification can be defined recursively.

Remark 3 Note that, at each step, determining an estimate ρ_k of ρ_{exp} solves the quantum state tomography [2] based on the partial information, the obtained sequence $\{\rho_k\}_{k=1}^R$ converges to ρ_{exp}, since $\rho_R = \bigcap_{i=1}^R \bar{\mathbf{S}}_i = \rho_{\mathrm{exp}}$ and the measurements are supposed to be perfect.

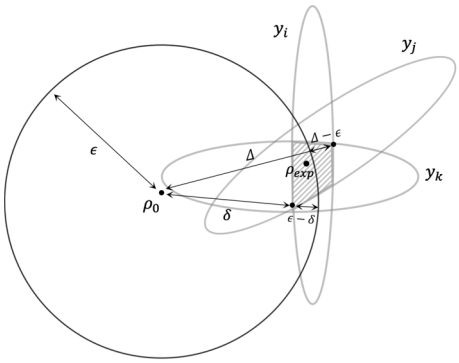


Fig. 2 Diagrams corresponding to the option of quantum state verification criteria **C1** and **C2**. The gray area represents $\bar{\mathbf{S}}_i \cap \bar{\mathbf{S}}_j \cap \bar{\mathbf{S}}_k$, i.e., the states compatible with the measurement data y_i, y_j and y_k

We summarize the algorithm of adaptive verification with perfect measurements as Algorithm AV.

Algorithm AV: Adaptive Verification

- **Initialization:** Define the sets $\mathsf{M} = \emptyset$ and $\mathsf{S} = \{1, \ldots, R\}$, and compute
  $\alpha_i^1 := \max_{\rho \in \mathbf{S}_i(\rho_0)} D(\rho, \rho_0)$
  for all $i \in \mathsf{S}$ and $\arg\min_{i \in \mathsf{S}} \alpha_i^1$.
  If arg min output a single integer, set $m_1 = \text{argmin}_{i \in \mathsf{S}} \alpha_i^1$. If arg min output multiple integers, choose at random a $m_1 \in \arg\min_{i \in \mathsf{S}} \mathrm{Tr}^2(\rho_0 A_i^\perp)/\|A_i^\perp\|_{HS}^2$. Set $\Gamma_{m_1} = A_{m_1}/\|A_{m_1}\|_{HS}$ and $k = 1$.
- **Step 1:** Perform the measurements corresponding to A_{m_k} and collect the sampled average output y_{m_k}. Update $\mathsf{M} = \mathsf{M} \cup \{m_k\}$ and $\mathsf{S} = \mathsf{S} \setminus \{m_k\}$. Compute
  $\omega_k := \min_{\rho \in \bigcap_{n \in \mathsf{M}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$, $\Omega_k := \max_{\rho \in \bigcap_{n \in \mathsf{M}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$.
  – If $\omega_k > \epsilon$, then ρ_{exp} is not (ϵ, D, ρ_0)-accurate and **stop the procedure**;
  – If $\Omega_k \leq \epsilon$, then ρ_{exp} is (ϵ, D, ρ_0)-accurate and **stop the procedure**;
  – Otherwise, set $\rho_k \in \arg\min_{\rho \in \bigcap_{n \in \mathsf{M}} \bar{\mathbf{S}}_n} f_{\rho_0}(\rho)$.
- **Step 2:** Collect all $i \in \mathsf{S}$ such that $A_i \notin \text{span}\{A_i\}_{i \in \mathsf{M}}$ in $\bar{\mathsf{S}}$. For all $i \in \bar{\mathsf{S}}$, compute
  $\delta_i^k := \min_{\rho \in \mathbf{S}_i(\rho_k) \cap \bigcap_{n \in \mathsf{M}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$,
  $\Delta_i^k := \max_{\rho \in \mathbf{S}_i(\rho_k) \cap \bigcap_{n \in \mathsf{M}} \bar{\mathbf{S}}_n} D(\rho, \rho_0)$,
  where $\mathbf{S}_i(\rho_k) = \{\rho \in \mathcal{S}(\mathcal{H}_d) | \, \mathrm{Tr}(\rho A_i) = \mathrm{Tr}(\rho_k A_i)\}$.
  If $\delta_i^k = 0$ for all $i \in \mathsf{S}$, compute $\arg\min_{i \in \bar{\mathsf{S}}} \Delta_i^k$.
  – If arg min outputs a single integer, set $m_{k+1} = \arg\min_{i \in \bar{\mathsf{S}}} \Delta_i^k$;
  – If arg min outputs multiple integers, compute $A_j^\perp = A_j - \sum_{i \in \mathsf{M}} \mathrm{Tr}(A_j \Gamma_i)\Gamma_i$ for all $j \in \bar{\mathsf{S}}$ and choose at random $m_k \in \arg\max_{j \in \bar{\mathsf{S}}} \mathrm{Tr}^2(\rho_0 A_j^\perp)/\|A_j^\perp\|_{HS}^2$. Set $\Gamma_{m_k} = A_{m_k}^\perp/\|A_{m_k}^\perp\|_{HS}$.
  Otherwise, compute
  $\arg\min_{i \in \bar{\mathsf{S}}} \{\min\{\epsilon - \delta_i^k, \Delta_i^k - \epsilon\}\}$.
  – If arg min outputs a single integer, set $m_{k+1} = \arg\min_{i \in \bar{\mathsf{S}}} \{\min\{\epsilon - \delta_i^k, \Delta_i^k - \epsilon\}\}$;
  – If arg min outputs multiple integers, compute $A_j^\perp = A_j - \sum_{i \in \mathsf{M}} \mathrm{Tr}(A_j \Gamma_i)\Gamma_i$ for all $j \in \bar{\mathsf{S}}$ and choose at random $m_k \in \arg\max_{j \in \bar{\mathsf{S}}} \mathrm{Tr}^2(\rho_0 A_j^\perp)/\|A_j^\perp\|_{HS}^2$. Set $\Gamma_{m_k} = A_{m_k}^\perp/\|A_{m_k}^\perp\|_{HS}$.
  Update $k = k + 1$.
- **Step 3:** Repeat **Step 1** and **Step 2** until $\text{card}(\mathsf{M}) = d^2$.

Due to the perfect measurements, we can always obtain the verification results when the above algorithm ends. In Step 2, we specifically consider the case $\delta_i^k = 0$ for all $i \in$

S, in which ρ_0 belongs to the compatible sets, i.e., **C1** is always verified. Thus, we can only apply **C2** to determine the next measurement. If $\rho_{\text{exp}} = \rho_0$, in Step 1 of Algorithm 4, we have $\rho_k \equiv \rho_0$ for any $k \in \{1, \ldots, R\}$ since $\rho_0 = \arg\min_{\rho \in \mathcal{S}(\mathcal{H}_d)} f_{\rho_0}(\rho)$, which implies $\delta_i^k \equiv 0$. Thus, in this case, Algorithm 4 is equivalent to the combination of Algorithm IOS and Algorithm IAS.

Note that Algorithm AV can also be applied to the imperfect measurement case. However, if the sample size is not big enough or there are errors and bias, one may obtain $\bigcap_{i=1}^{K} \hat{\mathbf{S}}_{m_i} = \emptyset$. In this case, we need to stop the verification process and re-measure ρ_{exp}.

5 Application: two-qubit systems

In the following, we test the proposed algorithm simulating measurements to verify the accuracy of preparation of randomized pure states in a two-qubit system. We summarize the key elements of the numerical experiments we ran.

Target states: According to the normal distribution, we pick 100 sets of 4 independent complex random numbers with real and imaginary parts belonging to $[-100, 100]$, i.e., $|\psi_i\rangle \in \mathbb{C}^4$ with $i = 1, \ldots, 100$. Then, we generate 100 pure target states by $\rho_{0,i} = \frac{|\psi_i\rangle\langle\psi_i|}{\text{Tr}(|\psi_i\rangle\langle\psi_i|)}$.

Bures distance: The distance we employ is the Bures distance, which reduces to $d_B(\rho, \rho_0) = \sqrt{2(1 - \sqrt{F(\rho, \rho_0)})} = \sqrt{2(1 - \sqrt{\text{Tr}(\rho\rho_0)})}$ for the case of ρ_0 being a pure state. Obviously, $d_B(\rho, \rho_0)$ is strictly monotonically decreasing with respect to $\text{Tr}(\rho\rho_0)$. Due to the linearity, we can apply the convex optimization (CVX-SDP [16]) in the simulation for searching the minimum and maximum value of $\text{Tr}(\rho\rho_0)$ under constraints.

Accuracy: $\epsilon = \sqrt{2(1 - \sqrt{\tilde{\epsilon}})}$, where $\tilde{\epsilon}$ is the desired precision for the fidelity $\text{Tr}(\rho\rho_0)$. We consider $\tilde{\epsilon} = 0.95$ so that $\epsilon = 0.2250$.

Measurements: We apply projective measurements into Pauli eigenstates. Let $\Pi_1 \ldots \Pi_6$ be the eigenprojectors of Pauli matrices corresponding to the eigenvalue 1 and -1, respectively, i.e., $\sigma_x\Pi_1 = \Pi_1, \sigma_x\Pi_2 = -\Pi_2, \ldots, \sigma_z\Pi_6 = -\Pi_6$. We denote by $A_{6(i-1)+j} = \Pi_i \otimes \Pi_j$ with $i, j \in \{1, \ldots, 6\}$ the 36 observables for the two-qubit system. The set of observables $\{A_i\}_{i=1}^{36}$ is information-complete.

Generated state: We generate 100 full rank $(\epsilon, d_B, \rho_{0,k})$-accurate states $\rho_{\text{exp},k}^a$ and 100 full rank $(\epsilon, d_B, \rho_{0,k})$-non-accurate states $\rho_{\text{exp},k}^n$ by perturbing the target state $\rho_{0,k}$ with $k \in 1, \ldots, 100$ as

$$\rho_{\text{exp},k} = e^{i\eta H_k}\Big((1-\lambda)\rho_{0,k} + \frac{\lambda}{4}\mathbb{1}_4\Big)e^{-i\eta H_k}, \tag{8}$$

where $\lambda \in (0, 1)$, $\eta > 0$ and H_k are random Hermitian matrix. We generate the random $H_k \in \mathcal{B}_*(\mathbb{C}^4)$ in the following way and express $H_k = \sum_{j=0}^{15} h_{j,k}\Gamma_n$ where $\Gamma_0 = \mathbb{1}_4$ and $\{\Gamma_j\}_{j=1}^{15}$ are generators of the Lie algebra SU(4) satisfying $\text{Tr}(\Gamma_j) = 0$ and $\text{Tr}(\Gamma_m\Gamma_j) = 2\delta_{jm}$ with $j, m \in \{1, \ldots, 15\}$, $\{h_{j,k}\}_{n=0}^{16}$ are random scalars drawn

from the uniform distribution in the intervals $(-1, 1)$. We set $\eta = 0.1$, $\lambda = 0.0001$ for the accurate case and $\lambda = 0.1$ for the non-accurate case.

5.1 Before measurements: Algorithm IOS versus Algorithm IAS

Algorithm IOS: We use CVX-SDP mode to apply semidefinite programming, and obtain 100 measurement sequences, $\mathsf{M}_k = [m_{k,j}]_{j\leq 16}$ for $k \in \{1, \ldots, 100\}$.

Algorithm IAS: We obtain 100 measurement sequences, $\mathsf{R}_k = [r_{k,j}]_{j\leq 16}$ for $k \in \{1, \ldots, 100\}$.

Comparison: Based on the measurement sequences R_k generated by Algorithm IOS, we apply semidefinite programming (CVX-SDP mode) to compute the following

$$\beta_{k,l} = \max_{\rho \in \bigcap_{j\in[\mathsf{R}_k]_l} \mathbf{S}_j(\rho_{0,k})} d_B(\rho, \rho_{0,k}),$$

where $[\mathsf{R}_k]_l$ denotes the first l elements of R_k. The value β_k can be considered as an indicator of how well Algorithm IAS approximates Algorithm IOS. The upper diagram of Figure 3 draws error bars of $\beta_k - \alpha_k$ which represents the mean value and standard deviation, where α_k are defined in Algorithm IOS; the lower diagram draws the number of measurements required by Algorithm IAS minus the one required by Algorithm IOS for reconstructing $\rho_{0,k}$. Taking the machine precision into account, reconstruction of $\rho_{0,k}$ means $d_B(\rho, \rho_{0,k}) \leq 10^{-6}$ for ρ belonging to the compatible set. For 100 target states $\rho_{0,k}$, the mean values and the standard deviations of the number of measurements required by Algorithm IOS and Algorithm IAS for the reconstruction are $(5.69, 0.5449)$ and $(6.47, 0.6884)$, respectively. It is worth noting that more measurements are required by Algorithm IOS than Algorithm IAS in few cases, since Algorithm IOS does not always provide the optimal measurement sequence, being itself an approximation of Algorithm OS.

5.2 Accurate $\rho_{\mathbf{exp}}$: Algorithm IOS versus Algorithm IAS versus Algorithm AV versus control groups

Control groups: Since the set of measurements considered here is information-overcomplete, we generate 5 random measurement sequences for each accurate generated state $\rho^a_{\mathrm{exp},k}$, and every sequence contains 16 linearly independent observables.

Numerical Test: We apply the verification protocol (Algorithm VM) on the measurement sequences generated off-line by Algorithm IOS, Algorithm IAS and randomized control groups and run the adaptive protocol (Algorithm AV) with $f_{\rho_0}(\rho) = d_B(\rho, \rho_0)$.

Remark 4 In the case of multiple measurements with the same index of merit, Algorithm IAS selects one measurement at random, while Algorithms IOS and AV use the following rule, inspired by Algorithm IAS: Select an observable at random among those which maximize $\mathrm{Tr}^2(\rho_1 A_j^{\perp})/\|A_j^{\perp}\|^2_{HS}$. The further optimization step is based

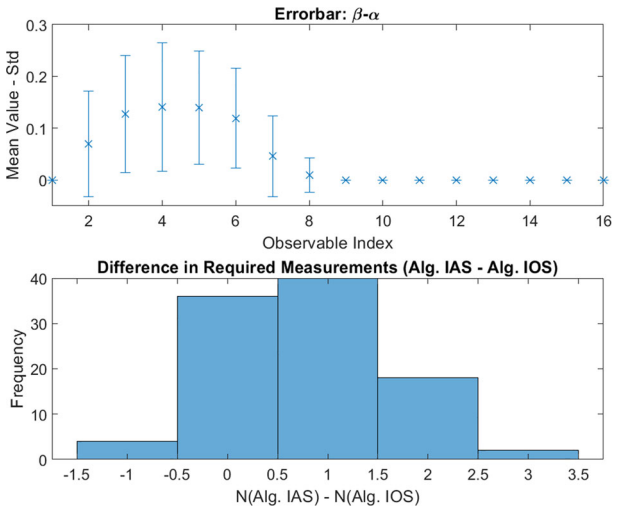


Fig. 3 Comparison of Algorithm IOS and Algorithm IAS on the reconstruction of $\rho_{0,k}$ with $k \in \{1, \ldots, 100\}$

on analytic formulas so it is not computationally intensive. The same rule will be used in the next set of simulations as well.

The main results are summarized in Figure 4 and Table 1. The first diagram of Figure 4 shows the histogram of the number of measurements required for the verification of accuracy by Algorithm IOS, Algorithm IAS, Algorithm AV and control groups. This diagram and Table 1 confirm the efficiency of our algorithms in verification of accuracy. The rest diagrams show the histogram of difference of the number of measurements required by different algorithms. In this situation, Algorithm IOS exhibits an advantage with respect to Algorithm IAS. In this case, the performance of Algorithm AV is almost equal to Algorithm IOS. This results are not surprising: When the state to be verified is indeed close to the target one, Algorithm IOS is expected to provide the best iteratively built sequence. Nonetheless, Algorithm IAS performance is fairly close (one extra measurement operator is needed on average) and has the advantage of avoiding iterated optimization procedures as it relies only on analytic formulas.

Remark 5 It is worth noticing that the performance of Algorithm AV strongly depends on the choice of the function f_{ρ_0}. Here, we only consider the basic choice $f_{\rho_0}(\rho) = d_B(\rho, \rho_0)$: The optimization of f_{ρ_0} will be the focus of the future work.

5.3 Non-accurate ρ_{exp}: Algorithm IOS versus Algorithm IAS versus Algorithm AV versus control groups

Control groups: We generate 5 random measurement sequences for each non-accurate generated state $\rho^n_{\text{exp},k}$, and every sequence contains 16 linearly independent observables.

Table 1 Verification of accuracy

Alg. IOS	Alg. IAS	Alg. AV	Control gr. 1
(4.76,1.46)	(5.73,1.42)	(4.83,1.10)	(8.68,1.38)
Control gr. 2	Control gr. 3	Control gr. 4	Control gr. 5
(8.74,1.52)	(8.82, 1.38)	(8.75,1.38)	(8.71,1.37)

The mean value and the standard deviation (m, σ) of the number of measurements are required for verifying the accuracy of $\rho^a_{\text{exp},k}$ for $k = 1, \ldots, 100$

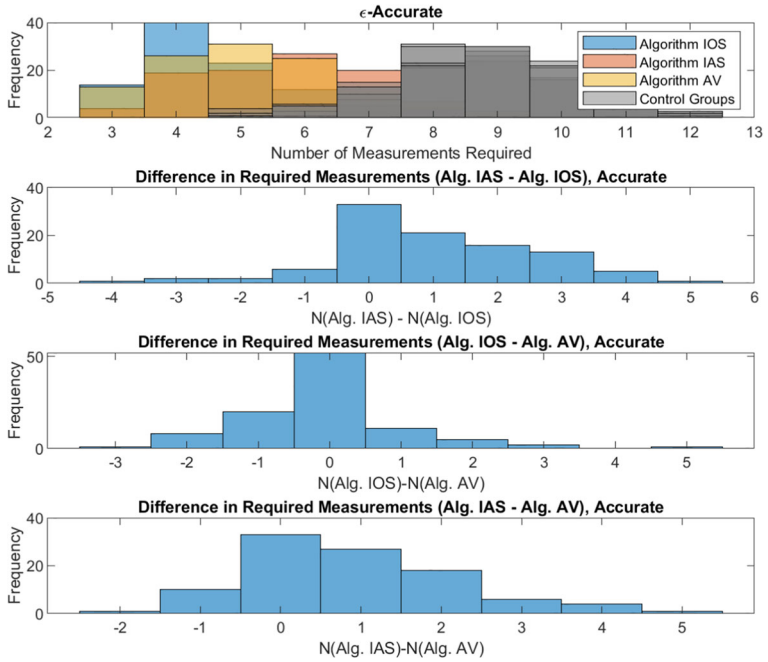


Fig. 4 The first histogram displays the distribution of the number of measurements required to verify the accuracy of $\rho^a_{\text{exp},k}$ for $k = 1, \ldots, 100$. The other three show the distribution of the difference between the lengths of the sequences of two algorithms for the same set of generated measurements: For example, if the displayed $N(\text{Alg. X}) - N(\text{Alg. Y})$ is negative, it indicates an advantage for (Alg. X)

Numerical Test: We apply the verification protocol (Algorithm VM) on the measurement sequences generated off-line by Algorithm IOS, Algorithm IAS and randomized control groups and also run the adaptive protocol (Algorithm AV) with $f_{\rho_0}(\rho) = d_B(\rho, \rho_0)$.

The main results are summarized in Figure 5 and Table 2. The first diagram of Figure 5 shows the histogram of the number of measurements required for the verification of non-accuracy by Algorithm IOS, Algorithm IAS, Algorithm AV and control groups. This diagram and Table 2 confirm the efficiency of our algorithms in verification of non-accuracy with respect to random sequences. The rest diagrams show the histogram of difference of the number of measurements required by different algorithms. We can observe that the performance is similar, with a slight advantage for the

Table 2 Verification of non-accuracy

Alg. IOS	Alg. IAS	Alg. AV	Contr. gr. 1
(5.14,1.65)	(5.28,1.25)	(5.06,1.11)	(8.38,1.80)
Contr. gr. 2	Contr. gr. 3	Contr. gr. 4	Contr. gr. 5
(8.34,1.72)	(8.71,1.73)	(8.48, 1.8504)	(8.57,1.83)

The mean value and the standard deviation of the number of measurements are required for verifying the non-accuracy of $\rho^{n}_{\mathrm{exp},k}$ for $k = 1, \ldots, 100$

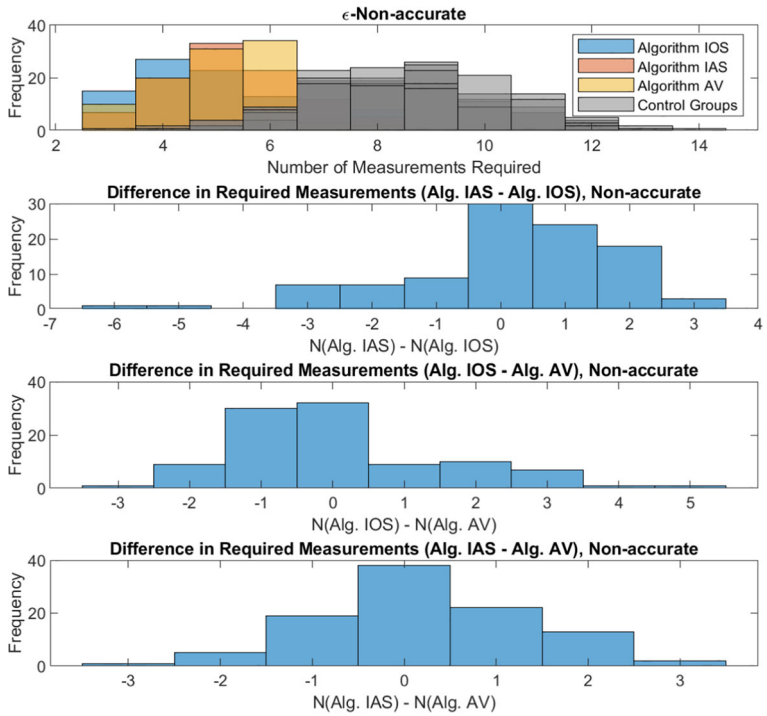


Fig. 5 The first histogram displays the distribution of the number of measurements required to verify the non-accuracy of $\rho^{n,1}_{\mathrm{exp},k}$ for $k = 1, \ldots, 100$. The other three show the distribution of the difference between the lengths of the sequences of two algorithms for the same set of generated measurements

adaptive protocol, Algorithm AV. Other numerical experiments indicate that the difference in performance becomes more relevant if the needed number of measurements grows.

6 Conclusions

In this work, we define and study *quantum state verification*, a key task to test the effectiveness of quantum state preparation procedures, quantum communication channels, quantum memories and a variety of quantum control algorithms.

Assuming that i.i.d. copies of the system can be produced, the resulting state can be identified by tomographic techniques: Sampled averages of a basis of observables are sufficient to determine an estimate of the state and thus to decide if it is compatible with given accuracy requirements. We propose improved strategies to select the observables to be measured, so that a decision on the accuracy of the preparation can be reached well before the full set of measurement is completed. The protocols rely on prior information about the target state and either provide a full ordered list of observables to be performed or adaptively decide the next observable based on the previously obtained ones.

Let us briefly compare the sample complexity of our method with the verification techniques that optimize the measurements with respect to the target state. In [3], by tuning the measurements for a specific target state ρ_0, Proposition 16 and Proposition 20 established that we need sample complexity $m > 1/\epsilon$ to guarantee:

$$\text{Prob}\{\text{“accept”}|F(\rho_{exp}, \rho_0) \leq 1-\epsilon\} \leq \delta, \quad \text{Prob}\{\text{“reject”}|\rho_{exp} = \rho_0\} = 0$$

In our strategy, the errors in the algorithms emerge from the substitution of the exact expected output for measuring the observable A_{m_k}, namely y_{m_k} with the empirical mean estimation using n-measurements, expressed as $Y_{m_k} := 1/n \sum_{i=1}^{n} A_{m_k}^{(i)}$, where $A_{m_k}^{(i)}$ represents the outcome of the i-th measurement of A_{m_k} in the state ρ_{exp}. Consequently, the primary errors in our paper come from $|Y_{m_k} - y_{m_k}|$, whose scaling can be characterized as in Proposition 10 of [3]: The latter states that

$$\text{Prob}\{|Y_{m_k} - y_{m_k}| \leq \epsilon\} \geq 1 - \delta,$$

for sample size $m > k/\epsilon^2 \log(2/\delta)$. In our scheme, these errors may sum over a finite number of measurements, thus maintaining the $1/\epsilon^2$ scaling.

Note that in the first case ϵ denotes the distance with respect to perfect fidelity, while in our case is the distance between true and estimated averages. However, the two can be related using standard quantum information bounds, obtaining the same scaling.

While our approach unfavorably scales as a linear function of $1/\epsilon^2$, all strategies obtaining $1/\epsilon$ scaling rely on the ability of tuning the measurements for the specific target. Here, on the other hand, we are limited to a fixed, finite set of general measurements, a situation motivated by typical experimentally-available setups.

Numerical tests indicate that, for example, a fidelity of 0.95 can be tested on a qubit system with just 5 measurement of joint Pauli operators, when using randomized sequences requires at least 8. While the solution of the problem leads to solve and compare multiple optimization problems, we also propose an iterative, suboptimal algorithm whose solution can be computed analytically, based on a geometric approximation of the set of states compatible with given measurement outcomes. The adaptive strategy holds an advantage, especially when the needed number of measurements grows, albeit it requires a more involved implementation. Further work will address the use of optimized measurement sequences for fast tomography, the use of different distance functions for the adaptive strategies and the application to real data from experimental systems of interest.

Acknowledgements F.T. and G.V. acknowledge partial funding from the European Union - NextGenerationEU, within the National Center for HPC, Big Data and Quantum Computing (Project No. CN00000013, CN 1, Spoke 10) and from the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, grant agreement No. 101114043). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them.

Funding Open access funding provided by Università degli Studi di Padova

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose. The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

1. Eisert, J., Hangleiter, D., Walk, N., Roth, I., Markham, D., Parekh, R., Chabaud, U., Kashefi, E.: Quantum certification and benchmarking. Nat. Rev. Phys. **2**(7), 382–390 (2020)
2. Paris, M., Rehacek, J.: Quantum State Estimation, vol. 649. Springer, Berlin/Heidelberg (2004)
3. Kliesch, M., Roth, I.: Theory of quantum system certification. PRX Quantum **2**, 010201 (2021)
4. Pallister, S., Linden, N., Montanaro, A.: Optimal verification of entangled states with local measurements. Phys. Rev. Lett. **120**(17), 170502 (2018)
5. Li, Y., Zhang, H., Li, Z., Zhu, H.: Minimum number of experimental settings required to verify bipartite pure states and unitaries. Phys. Rev. A **104**, 062439 (2021)
6. Wang, K., Hayashi, M.: Optimal verification of two-qubit pure states. Phys. Rev. A **100**(3), 032315 (2019)
7. Dangniam, N., Han, Y.-G., Zhu, H.: Optimal verification of stabilizer states. Phys. Rev. Res. **2**(4), 043323 (2020)
8. Yu, X.-D., Shang, J., Gühne, O.: Optimal verification of general bipartite pure states. Npj Quantum Inf. **5**(1), 112 (2019)
9. Jiang, X., Wang, K., Qian, K., Chen, Z., Chen, Z., Lu, L., Xia, L., Song, F., Zhu, S., Ma, X.: Towards the standardization of quantum state verification using optimal strategies. Npj Quantum Inf. **6**(1), 90 (2020)
10. Li, Z., Han, Y.-G., Zhu, H.: Optimal verification of greenberger-horne-zeilinger states. Phys. Rev. Appl. **13**(5), 054002 (2020)
11. Liu, Y.-C., Yu, X.-D., Shang, J., Zhu, H., Zhang, X.: Efficient verification of dicke states. Phys. Rev. Appl. **12**(4), 044020 (2019)
12. Liu, Y.-C., Shang, J., Yu, X.-D., Zhang, X.: Efficient verification of quantum processes. Phys. Rev. A **101**(4), 042315 (2020)
13. Gross, D., Liu, Y.-K., Flammia, S.T., Becker, S., Eisert, J.: Quantum state tomography via compressed sensing. Phys. Rev. Lett. **105**, 150401 (2010)
14. Zorzi, M., Ticozzi, F., Ferrante, A.: Minimum relative entropy for quantum estimation: feasibility and general solution. IEEE Trans. Inf. Theory **60**(1), 357–367 (2013)

15. Nielsen, M.A., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
16. Grant, M., Boyd, S.: CVX: Matlab Software for Disciplined Convex Programming, version 2.1. http://cvxr.com/cvx (2014)