Certification of quantum state functions under partial information

Leonardo Zambrano[1], Donato Farina[1,2], Egle Pagliaro[1], Márcio M. Taddei[1], and Antonio Acín[1,3]

[1]ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain

[2]Physics Department E. Pancini - Università degli Studi di Napoli Federico II, Complesso Universitario Monte S. Angelo - Via Cintia - I-80126 Napoli, Italy

[3]ICREA - Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain

Convex functions of quantum states play a key role in quantum physics, with examples ranging from Bell inequalities to von Neumann entropy. However, in experimental scenarios, direct measurements of these functions are often impractical. We address this issue by introducing two methods for determining rigorous confidence bounds for convex functions based on informationally incomplete measurements. Our approach outperforms existing protocols by providing tighter bounds for a fixed confidence level and number of measurements. We evaluate the performance of our methods using both numerical and experimental data. Our findings demonstrate the efficacy of our approach, paving the way for improved quantum state certification in real-world applications.

1 Introduction

The value attained by a convex function of a quantum state is generally connected to key concepts in quantum physics [1]. In experimental contexts, though, these values are often not accessible through direct measurements. Even for a linear function of the quantum state, i.e. the expectation value of a generic observable, measurements can be challenging if the observable is highly nonlocal (e.g., a projector on a highly entangled subspace) or requires measurement devices unavailable in experimental setups. How-

Leonardo Zambrano: leonardo.zambrano@icfo.eu, these authors contributed equally to this work.

Donato Farina: donato.farina@unina.it, these authors contributed equally to this work.

ever, it is possible to achieve an indirect estimation of these observables through the measurements of other more accessible quantities. Parallel measurements of local Pauli operators constitute a typical example of feasible measurements for a multiqubit system. A full and perfect tomographic reconstruction, ideally attainable by means of parallel measurements, would naturally lead to the knowledge of any function of the quantum state [2, 3]. Nevertheless, this is unrealistic for two main reasons. First, even considering the case of measuring all the possible multiqubit Pauli strings, such measurements contain an inherent uncertainty due to finite statistics effects, and it is not always clear how to translate this uncertainty to the estimation of the convex function. Second, for large systems a tomographically complete set of measurements is exponentially costly both in time and in experimental resources, hence, infeasible in practice. As a result, it is of utmost importance to be able to reliably estimate the value of convex functions through an incomplete set of measurements, as, for instance, those in compressed sensing quantum tomography [4]. That is, one aims at deriving a confidence interval, i.e. determining a range of feasible values, for the convex function value given the acquired partial information on the state.

The problem, in general, is acquiring increasing interest during the last few years as is related to identifying confidence sets for quantum state tomography [5–13]. These sets are regions within the space of density matrices that contain the experimental state with a certain confidence level. They allow us to establish rigorous bounds for convex functions applied to the state using convex optimization techniques. However, prior research primarily concentrates on scenarios that

require informationally complete measurements, obtainable only through a large number of measurement settings.

The size of the confidence region depends on the desired confidence level and the number of available copies of the experimental state. Since quantum resources are limited, it is critical to devise protocols that use the fewest possible copies of the state for a given confidence level. Here, we present a method to determine the confidence interval of convex functions using informationally incomplete measurements. We demonstrate that, with a fixed confidence level and number of shots, our method yields tighter confidence intervals compared to other previous protocols.

To achieve this objective, we present two approaches: the first is based on the knowledge of a specific number of expectation values of Hermitian operators (e.g. multi-qubit Pauli operators) and assigns confidence intervals to each of these values. The second is a joint approach that considers general measurements, defined by positive operator-valued measures (POVM). Depending on the type of states that we are considering one method might perform better than the other. Both provide useful guidance for certification in realistic experimental settings depending on the input resources.

This article is organized as follows. In Sec. 2 we introduce the certification scheme in the ideal scenario and the problems arising when dealing with experimental data. Our two methods are presented in Sec. 3. Their performances are first tested for Haar pure states' data in Sec. 4 and then for experimental data produced with the `ibm_perth` quantum processor in Sec. 5. We draw our conclusions in Sec. 6 together with possible future developments.

2 Preliminaries

2.1 Certification in ideal scenario

We first discuss the ideal scenario, namely, in the absence of any statistical and experimental uncertainties. Then, under partial information about the state ω given in the form of expectation values of a set of observables $\mathcal{I} = \{O_i\}_i$, certifying that the value of a generic real function of the system state, $\mathcal{F}(\omega)$, is within a certain interval can be

treated with the following optimization problem:

$$
\begin{aligned}
\mathcal{F}_{\text{LB(UB)}} = \quad &\min_\rho \, (\max_\rho) \mathcal{F}(\rho) \\
\text{s.t.} \quad &\text{tr}(\rho) = 1 \\
&\rho \geq 0 \\
&\text{tr}(O_i \rho) = \text{tr}(O_i \omega) \quad \forall i \in \mathcal{I}.
\end{aligned} \tag{1}
$$

This means that any reconstruction ρ compatible with the equality constraints identified by $\mathcal{I}$ will provide a value $\mathcal{F}(\rho)$ which is greater (lower) or equal than the lower (upper) bound $\mathcal{F}_{\text{LB(UB)}}$ determined by Problem (1). More importantly, we are guaranteed that the performance associated to the actual state ω, being also a feasible state, is within such a range,

$$
\mathcal{F}_{\text{LB}} \leq \mathcal{F}(\omega) \leq \mathcal{F}_{\text{UB}}. \tag{2}
$$

If $\mathcal{F}$ is linear,

$$
\mathcal{F}_{\text{lin}}(\omega) = \text{tr}(L\omega), \tag{3}
$$

with $L = L^\dagger$, Problem (1) consists in a semidefinite program (SDP). SDPs are very practical, as they can be efficiently solved with low computational power, and do not feature the problem of local minima [14, 15]. However, data in (1) are perfect, in the sense that do not contain uncertainties, a situation that is unrealistic in experimental scenarios.

2.2 Dealing with experimental data: relaxation of the equality constraints

The main goal of this work is to generalize the certification scheme (1) to a generic situation where the data come from an experiment, taking into account statistical errors.

With the aim of relying completely on the information extracted from the experimental data, we shall relax the equality constraints allowing for fluctuations of the order of the standard errors. As we shall see, in the experimental scenario the range in (2) does not apply deterministically, but, instead, holds true with a probability $\mathcal{P}$ for which we derive appropriate lower bounds $1 - \delta$, namely

$$
\begin{aligned}
\mathcal{F}_{\text{LB}} &\leq \mathcal{F}(\omega) \leq \mathcal{F}_{\text{UB}}, \\
&\text{with probability } \mathcal{P} \geq 1 - \delta.
\end{aligned} \tag{4}
$$

2.3 Operator convex functions

Before presenting our methods for certification under measurement uncertainties, a comment is

in order. As stated below, the results are valid for target functions $\mathcal{F}$ in general. However, they will be most interesting to apply when $\mathcal{F}$ is an (operator) convex function, since the corresponding minimization consists in a convex optimization problem. Convex optimization has the advantage of providing certified lower bounds to the function of interest, as well as that of not having local minima [16]. If $\mathcal{F}$ is *linear*, then both $\mathcal{F}$ and $-\mathcal{F}$ are convex, and both upper and lower bounds can be efficiently and certifiably obtained. Given that linear functions are ubiquitous in quantum mechanics, as they represent the expectation values of operators, we shall apply these methods to several linear functions $\mathcal{F}$ of interest. Additionally, we will show an application to the nonlinear von Neumann entropy (whose negative is convex).

3 Bounds for the feasible set

We now present our two methods in a general formalism.

3.1 Individual-constraint method

Consider an unknown density operator ω describing the state of a system of dimension d. Let O_i be a set of Hermitian operators for $i \in \mathcal{I} = \{1, 2, \ldots, K\}$ with bounded outcomes in $[-1, 1]$, o_i be the corresponding experimental averages obtained with number of measurement shots N_i, and s_i be the associated empirical standard deviations. Then, if $\mathcal{F}$ is a function of the density matrix ρ, and $\delta \in (0, 1]$, the solution to the optimization problem

$$
\begin{aligned}
\mathcal{F}_{\mathrm{LB(UB)}} = \min_{\rho}(\max_{\rho}) \quad & \mathcal{F}(\rho) \\
\text{s.t.} \quad & \operatorname{tr}(\rho) = 1 \\
& \rho \geq 0 \\
& |\operatorname{tr}(O_i\rho) - o_i| \leq \epsilon_i \quad \forall i \in \mathcal{I},
\end{aligned}
$$

is a lower (upper) bound for $\mathcal{F}(\omega)$ with probability at least $1 - \delta$. Here

$$
\epsilon_i := \min(\epsilon_i^{(\mathrm{H})}, \epsilon_i^{(\mathrm{EB})}), \tag{6}
$$

$$
\epsilon_i^{(\mathrm{H})} := \frac{\alpha_{K,\delta}}{\sqrt{N_i}}, \quad \epsilon_i^{(\mathrm{EB})} := s_i \frac{\alpha_{K,\delta/2}}{\sqrt{N_i}} + \frac{7}{3}\frac{\alpha_{K,\delta/2}^2}{N_i - 1} \tag{7}
$$

where $\alpha_{K,\delta} := \sqrt{2\ln(2K/\delta)}$.
The proof of the above statement is based on the application of the Hoeffding or Empirical Bernstein bounds [17, 18], followed by the union

bound, analogously to the proof in [19]. It is reported in Appendix A. Note also that outcomes are taken in $[-1, 1]$ without loss of generality, as the previous result can easily be adapted to an arbitrary bounded operator by adjusting its maximum and minimum eigenvalue.

Discussion.— The need to consider both Hoeffding and Empirical Bernstein bounds, Eqs. (6) and (7), arises because $\epsilon_i^{(\mathrm{EB})}$ allows for fluctuations up to $\alpha_{K,\delta/2}$ times the standard errors $s_i/\sqrt{N_i}$, with a correction term scaling as $\sim 1/N_i$. Neglecting this correction (for sufficiently high N_i) assumes a normal distribution for the averages, resulting in a feasible set contained within the one defined by $\epsilon_i^{(\mathrm{H})}$ for a rescaled δ. In such cases, $\epsilon_i^{(\mathrm{EB})}$ usually yields tighter results than $\epsilon_i^{(\mathrm{H})}$. However, this is not always the case, especially when considering the correction term. Consequently, for not too large N_i, $\epsilon_i^{(\mathrm{EB})}$ may lead to looser bounds than $\epsilon_i^{(\mathrm{H})}$. To obtain a tight general bound, we consider the minimum $\epsilon_i = \min(\epsilon_i^{(\mathrm{H})}, \epsilon_i^{(\mathrm{EB})})$ for each constraint i, as indicated in Eq. (6). For *not huge* numbers N_i, we typically expect the Hoeffding bound to be tighter for random states where most or all standard deviations s_i have non-zero values. However, for specifically chosen states, some of the s_i can be nearly zero, making the EB bound tighter. Furthermore, we stress that this method does not assume statistical independence between the several random variables o_i, opening the way to a broad spectrum of applications. We also mention that, for its derivation, method (5) should be compared with the feasible regions presented in the Supplemental Material of [19] (that, however, were not applied to optimization problems). By construction, method (5) is *tighter* for its selective character in using either Hoeffding's bound or Empirical Bernstein's bound instead of solely Hoeffding's bound. Remarkably, a further improvement of the individual-constraint method is presented in Appendix B showing the possibility of optimizing the step concerning the application of the union bound.

Example.— Let us consider an n-qubit system and let $\{O_i = \otimes_{j=1}^n \sigma_{i_j}\}_i$ be a set of multiqubit Pauli operators for $i \in \mathcal{I} = \{1, 2, \ldots, K\}$, $K \leq 4^n - 1$, o_i be the experimental estimates of $\operatorname{tr}(\omega O_i)$ (correlators for brevity) obtained with number of measurement shots N_i and $s_i =$

Accepted in 〈 〉uantum 2024-07-30, click title to verify. Published under CC-BY 4.0.

3

$\sqrt{N_i/(N_i-1)}\sqrt{1-o_i^2}$ be the associated empirical standard deviations.

The first consideration that comes out is the scaling of the confidence ranges in the number of qubits n. The functional form of $\alpha_{K,\delta}$ implies a worst case scenario scaling $\epsilon_i \sim \sqrt{n}$. Also, with method (5) we account for finite statistics effects, and, in particular, for the fact that correlators that have been estimated with more precision deserve a tighter range of freedom (smaller ϵ_i). In a parallel measurement framework (see Appendix C for details) such correlators are typically the 1-body ones, for which estimations coming from many different measurement settings are typically available. On the contrary, the most imprecise ones are typically the n-body correlators for which only one measurement setting can provide information. In this sense, we remark that correlators extracted from parallel measurements are *not* statistically independent as the estimation of two different correlators can rely on some common shots. This happens when two correlators are related through the following rule: from a higher order correlator, e.g. the four body correlator o_{xxz0y} for a system of 5 qubits, we can obtain a lower order correlator by "substituting" the label of one or more Pauli operators with the identity, obtaining for instance the two-body correlator o_{0x00y}. These two correlators, namely o_{xxz0y} and o_{0x00y}, share some data in their estimation and therefore are *not* statistically independent.

3.2 Joint-constraint method

Consider a density operator ω on a system of dimension d. Let $E = \{E_i\}_{i=1}^m$ define a POVM applied to the system, with $\vec{p} = (tr(\omega E_1), tr(\omega E_2), \ldots, tr(\omega E_m))$ the exact measurement probabilities and $\vec{q}$ the empirical estimation of $\vec{p}$ obtained by measuring E across N copies of ω. Let $\mathcal{F}$ be a function of density matrices, and $\delta \in (0,1]$. Then, the solution to the optimization problem

$$
\begin{aligned}
\mathcal{F}_{\mathrm{LB(UB)}} = \min_\rho \ (\max_\rho) \quad & \mathcal{F}(\rho) \\
\text{s.t.} \quad & tr(\rho) = 1 \\
& \rho \geq 0 \\
& \sum_{i=1}^m |tr(E_i\rho) - q_i| \leq \epsilon \ ,
\end{aligned}
$$
(8)

is a lower (upper) bound for $\mathcal{F}(\omega)$ with probability at least $1 - \delta$. Here

$$
\epsilon = \sqrt{\frac{2}{N} \ln \frac{2^m}{\delta}}.
$$
(9)

This result is based on the Bretagnolle–Huber–Carol inequality [20], that bounds the total variation distance $\|\vec{p} - \vec{q}\|_1$ between a vector of multinomially distributed random variables and its expected values (see Appendix D). The total variation distance has recently been used to define distance measures between quantum states, measurements, and channels based on their statistical distinguishability [21].

3.3 Comparing the two methods

With both methods (5) and (8), we will be interested in the case of the function $\mathcal{F}$ being linear or convex, as they both lead to convex optimization problems.

Let us mention a few differences between methods (5) and (8). In a typical quantum-state measurement scenario, $\vec{q}$ contains information on the counts of each possible outcome of every measurement, whereas in (5), the counts are grouped into expectation values of Hermitian operators. Then, the dimension of $\vec{q}$ is typically larger than the number of Hermitian operators since these operators can be chosen to avoid redundancy. For example, measuring the 9 Pauli basis that are informationally complete for 2 qubits gives a $\vec{q}$ of dimension 36 (we call for brevity *Pauli basis* a particular choice of parallel measurement setting, see Eq. (19) and related discussions in Appendix C). The same information can be grouped into 15 Pauli operators. Another difference between the two methods is that (8) bounds the estimation errors jointly in a single equation, with $\epsilon = \sqrt{\frac{2}{N} \ln \frac{2^m}{\delta}}$, while the local method employs one constraint for each Hermitian operator. As we shall see later the two methods, beyond in general responding to different experimental requests, have different performances in terms of tightness of the resulting bounds. However, as a common feature, regarding the behavior in terms of the confidence level, in both methods the errors in the constraints in Eqs. (7) and (9) are monotonically decreasing with increasing δ, as they are proportional to $\sqrt{\ln \delta^{-1}}$. This implies that having a higher confidence level $1 - \delta$ results in a
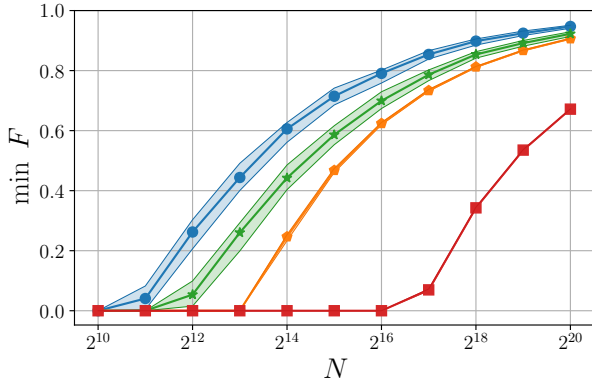
Figure 1: Minimum preparation fidelity of 4-qubit states as a function of the total number of shots N. The confidence level is 0.997. The solid lines represent the median value obtained from 100 Haar-random pure states using the joint-constraint method (blue dots), individual-constraint method (green stars), method from Ref. [13] (orange pentagons) and classical shadows (red squares), while the shaded areas depict the interquartile ranges. When applying our two methods we considered 16 random measurement settings (more precisely, we draw 16 random settings for each drawn random state), while for the method from Ref. [13] all the 81 measurement settings. We remark that N is the total number of shots in the whole simulated experiment, thus, in general, this implies less shots per measurement setting.
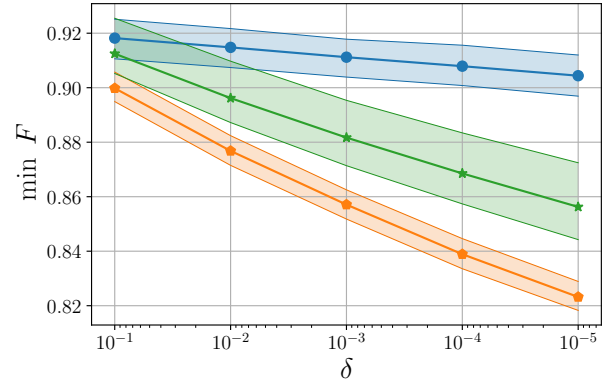
Figure 2: Behaviors in terms of the confidence level. We consider all 9 possible measurement settings for two qubits, a number of shots $N = 16379$ ($N \approx 2^{14}$, ≈ 1820 shots per measurement setting) and plot the median of the minimum preparation fidelity over 100 Haar-random pure states as function of decreasing δ. The shadowed region indicates interquartile ranges. Different curves and associated shadowed regions refer to different methods. Joint-constraint method (blue dots), individual-constraint method (green stars) and method from Ref. [13] (orange pentagons).

decreasing (increasing) behavior for $\mathcal{F}_{\mathrm{LB(UB)}}$, i.e. our bounds become looser but more secure.

Recently de Gois and Kleinmann proposed a method to find confidence regions based on the vector Bernstein inequality [13]. Those regions can also be integrated into convex optimization routines to find bounds for convex functions, but require the measurement of an informationally complete POVM. We show in what follows that for paradigmatic figures of merit in quantum information our bounds outperform the bounds provided by Ref. [13].

4 Numerical simulations

4.1 Certification of state preparation

The first application we discuss involves a certification protocol for preparing quantum states. Let us assume our goal is to prepare a pure quantum state $|\psi\rangle$ within a physical system, and we want to check the quality of the preparation, in terms of the worst-case state preparation. To achieve this, we perform measurements on the system and, given this information, minimize the fidelity

$F(\rho) = \langle\psi|\rho|\psi\rangle$ between the states ρ in the feasibility set Ω, and the desired state $|\psi\rangle$. Therefore, for an experimental state ω, we obtain the lower bound $\langle\psi|\omega|\psi\rangle \geq \min_{\rho\in\Omega} F(\rho)$.

We conducted numerical simulations for this protocol. Specifically, we prepared 100 Haar-random 4-qubit pure states $|\psi\rangle$ and we measured them using 16 randomly chosen Pauli bases, evenly distributing the N copies of the state. Subsequently, we apply our two protocols and protocol A from Ref. [13] for a selected confidence level. In the case of protocol A, we measure the 81 Pauli bases that are informationally complete for 4 qubits. Finally, we calculated the fidelity of the resulting states with the initially prepared states $|\psi\rangle$. We also applied fidelity estimation using classical shadows with random Pauli bases [22]. The minimum fidelity in this case is given by $\hat{f} - \epsilon'$, where $\hat{f}$ is the classical shadows estimator of the fidelity and $\epsilon' = \frac{64 \times 4^4}{N} \ln(2/\delta)$ quantifies the error in the estimation.

In Figure 1, fixing $1 - \delta = 0.997$, we show the behavior of the minimum preparation fidelity in terms of the number of shots. Blue dots and green stars represent the results obtained using the joint-constraint method and individual-constraint method, respectively, while the orange pentagons correspond to the results ob-
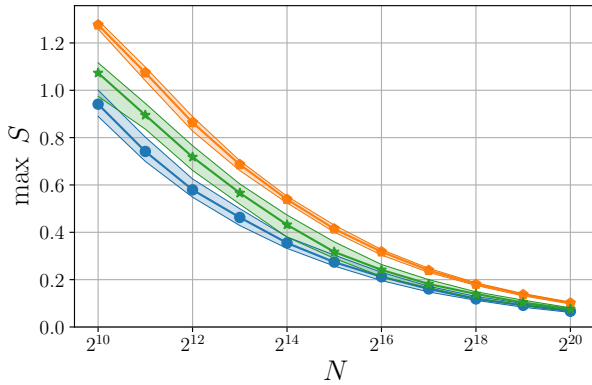
Figure 3: Maximum entropy of 2-qubit pure states as a function of the total number of shots N. The confidence level is 0.997. The solid lines represent the median value obtained from 100 Haar-random pure states using the joint-constraint method (blue dots), individual-constraint method (green stars) and method from Ref. [13] (orange pentagons), while the shaded areas depict the interquartile ranges. We considered all the 9 possible measurement settings.

tained with the method from Ref. [13] and the red squares are the results using classical shadows. We observe that, using the same data, both our bounds outperform the bounds provided by Ref. [13] and classical shadows. In particular, the fidelity bounds are significantly tighter when employing the joint-constraint method, which requires approximately four times fewer quantum resources than method from Ref. [13]. Also the experimental demand is lower, since we only measure around 1/5 of the total number of settings in our protocols.

In Fig. 2, fixing a total of 2^{14} shots, we check the scaling of the protocols with the confidence level $1-\delta$ (decreasing values of δ). Also in this case our two methods provide tighter results with respect to the method from Ref. [13], with the results obtained from the joint-constraint method being the tightest and, remarkably, pretty stable with increasing confidence level.

4.2 Certification of the maximum von Neumann entropy

We now aim to determine an upper bound for the von Neumann entropy S of a state ω. This is a convex optimization problem, since S is a concave function. Then, we perform measurements on the system and maximize the function $S(\rho) = -\text{tr}(\rho \ln \rho)$ over all the states ρ compati-

ble with the feasibility set Ω.

In Fig 3, we prepare 100 Haar-random pure states of 2 qubits, and we measure them using all 9 Pauli observables $\{\sigma^{(1)} \otimes \sigma^{(2)}\}$, with $\sigma = X, Y, Z$. The protocols are then applied with confidence level 0.997. The blue dots and green stars showcase the maximum entropy yielded by methods (8) and (5), respectively, for different numbers of total shots. The orange pentagons are the results using the method A from Ref. [13] with the same data and confidence level. The conclusions we can draw are analogous to the ones extracted from the previous analysis. Both our methods provide tighter results than the method from Ref. [13], with the best performance being reached with the joint-constraint method.

5 Experimental results

We now present results based on actual experimental data. A fundamental difference with respect to the previous analysis is that the target state (the pure state one aims to prepare) and the actual state (the state actually produced in the experiment) do not coincide. We performed experiments using the `ibm_perth` quantum processor. For 4 qubits, we aimed to prepare a random product state, a tensor product of two Bell states, and a GHZ state. We then measured each of these states with a certain number of random Pauli bases, using 2^{14} shots per basis. We compared the experimental state with the theoretical ones in terms of maximum and minimum fidelity, and we also calculated the maximum von Neumann entropy. The results using methods (5) and (8) are displayed in Table 1. We notice that an analysis with the method from Ref. [13] is not possible because the data at our disposal are informationally incomplete.

In contrast to the numerical simulations of Sec. 4, the best performance is obtained here with the individual-constraint method, i.e., it provides tighter values for maximum and minimum preparation fidelity and maximum von Neumann entropy.

On this regard, we notice that the associated target pure states (i.e. what we wanted to theoretically prepare), may possess some structure, an important difference with respect to random Haar states. This implies that they could be described in terms of few relevant Pauli strings. This

state	Individual-constraint			Joint-constraint		
	$\min F$	$\max F$	$\max S$	$\min F$	$\max F$	$\max S$
Product	0.916	0.983	0.397	0.891	0.993	0.492
Bell pair	0.747	0.862	0.986	0.681	0.879	1.102
GHZ	0.730	0.878	1.143	0.671	0.910	1.289

Table 1: Analyzing experimental data produced with `ibm_perth` quantum processor for 4 qubits with both individual-constraint method and joint-constraint method for confidence level 0.997. Given a selected target state we measured with 16 different random settings, performing $N = 2^{18}$ total number of shots. The target states are: Product state, GHZ, Bell pair. We remark that being in the informationally incomplete scenario method from Ref. [13] cannot be applied.

generally makes the individual-constraint method more efficient for these *particular* states, because, at variance with the joint-constraint method, it bounds each Pauli string expectation value independently.

Furthermore, additional factors should be taken into account when examining the data presented in the table. Product states are usually prepared with low error in superconducting platforms. Then, the results for the minimum fidelity are comparable to the value 0.896 obtained by numerical simulations of the joint-constraint method assuming perfect preparation and a total N of 2^{18} shots. Worse performances in preparation are instead obtained in the case of entangled target states. For this reason, when compared with the product state, the results we obtained for minimum and maximum fidelity are smaller in the cases of tensor product of two Bell states and a GHZ state, and, analogously, for maximum von Neumann entropy the last two state preparations yield larger upper bounds.

6   Discussion and conclusions

We faced the problem of identifying a certified interval for a generic function of a quantum state in the informationally incomplete scenario and under finite statistics effects, focusing on the treatable cases of linear functions and the more general operator convex functions. On this regard, we introduced two methods that, considering paradigmatic figures of merit, lead to tighter bounds than the ones extractable from the recent method presented in Ref. [13].
We remark that our schemes are general in the sense that they enable us to find rigorous confidence bounds for the experimental values of convex functions of density matrices using various types of measurements. This flexibility allows the method to be effectively applied to a wide range of different experimental setups, as researchers can conveniently choose the most suitable measurements for their certification task.
Analytical methods like classical shadows [22] or direct fidelity estimation [23] often require new calculations to obtain confidence bounds when the function to certify or the measurements to perform are modified. In contrast, using confidence regions, convex optimization can be directly applied without the need for any additional calculations. Then, the method can be straightforwardly applied to numerous other interesting functions, including the quantum Fisher information [24], Bell inequalities, entanglement witnesses, and more. We mention that one can use our schemes to find a compressed sensing reconstruction by considering the argument of the minimization for any convex function [25], but with rigorous and tight bounds for the constraints provided by our methods.
Furthermore, since finding the quantum state that describes a physical system is not our primary objective, the informational completeness of the measurements is not as crucial as in quantum tomography. In principle, data from any measurement will provide bounds for the convex functions. This contrasts with other results on confidence regions for quantum states, which primarily focus on informationally complete measurements. However, if we intend for the bounds of our method to be non-trivial, we require a reasonable number of settings, as in compressed sensing tomography.
About the joint-constraint method, improvements in confidence regions require tighter bounds for the discrepancy between the experimental and exact probabilities, $||\vec{p} - \vec{q}||_1$. This could be done by trying different concentration

inequalities. Furthermore, it is worth considering that the 1-norm constraint may not always be the best choice. Then, confidence bounds using other p-norms could potentially yield better results. Other concentration inequalities beyond Hoeffding and Empirical Bernstein bounds can also provide improvements in the individual-constraint method by adding their resulting errors in the minimization appearing in (6).

Finally, we notice that the methods can include the case of detection inefficiencies by modifying the POVM elements to include an additional output corresponding to non-detected events, and they might be extended to other estimation tasks, such as, process tomography by means of the Choi-Jamiolkowski isomorphism, or detector tomography.

Acknowledgments

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge university press, 2010).

[2] D. F. V. James, P. G. Kwiat, W. J. Munro and A. G. White, Measurement of qubits, Phys. Rev. A **64**, 052312 (2001).

[3] R. T. Thew, K. Nemoto, A. G. White and W. J. Munro, Qudit quantum-state tomography, Phys. Rev. A **66**, 012303 (2002).

[4] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker and J. Eisert, Quantum State Tomography via Compressed Sensing, Phys. Rev. Lett. **105**, 150401 (2010).

[5] M. Christandl and R. Renner, Reliable Quantum State Tomography, Phys. Rev. Lett. **109**, 120403 (2012).

[6] J. Wang, V. B. Scholz and R. Renner, Confidence Polytopes in Quantum State Tomography, Phys. Rev. Lett. **122**, 190401 (2019).

[7] M. Guţă, J. Kahn, R. Kueng and J. A. Tropp, Fast state tomography with optimal error bounds, Journal of Physics A: Mathematical and Theoretical **53**, 204001 (2020).

[8] K. T. Goh, C. Perumangatt, Z. X. Lee, A. Ling and V. Scarani, Experimental comparison of tomography and self-testing in certifying entanglement, Phys. Rev. A **100**, 022305 (2019).

[9] J. Eisert et al., Quantum certification and benchmarking, Nature Reviews Physics **2**, 382 (2020).

[10] J. O. de Almeida, M. Kleinmann and G. Sentís, Comparison of confidence regions for quantum state tomography, New Journal of Physics **25**, 113018 (2023).

[11] J. Steinberg, H. C. Nguyen and M. Kleinmann, Certifying activation of quantum correlations with finite data (2023), arXiv:2305.03748 .

[12] D. O. Norkin, E. O. Kiktenko and A. K. Fedorov, Reliable confidence regions for quantum tomography using distribution moments, Phys. Rev. A **109**, 032414 (2024).

[13] C. de Gois and M. Kleinmann, User-friendly confidence regions for quantum state tomography, Phys. Rev. A **109**, 062417 (2024).

[14] J. Watrous, Lecture Notes on Quantum Information Theory (2021).

[15] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science*, 2053-2563 (IOP Publishing, 2023).

[16] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

[17] V. Mnih, C. Szepesvári and J.-Y. Audibert, Empirical Bernstein Stopping, in *Proceedings of the 25th International Conference on Machine Learning*, ICML '08 (Association for Computing Machinery, New York, NY, USA, 2008) p. 672–679.

[18] A. Maurer and M. Pontil, Empirical Bernstein Bounds and Sample Variance Penalization (2009), arXiv:0907.3740 .

[19] J. Cotler and F. Wilczek, Quantum Overlapping Tomography, Phys. Rev. Lett. **124**, 100401 (2020).

[20] J. Bretagnolle and C. Huber, Lois empiriques et distance de Prokhorov, Séminaire de probabilités de Strasbourg **12**, 332 (1978).

[21] F. B. Maciejewski, Z. Puchała and M. Oszmaniec, Operational Quantum Average-Case Distances, Quantum **7**, 1106 (2023).

[22] H.-Y. Huang, R. Kueng and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nature Physics **16**, 1050 (2020).

[23] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. **106**, 230501 (2011).

[24] G. Müller-Rigat et al., Certifying the quantum Fisher information from a given set of mean values: a semidefinite programming approach, Quantum **7**, 1152 (2023).

[25] A. Kalev, R. L. Kosut and I. H. Deutsch, Quantum tomography protocols with positivity are compressed sensing protocols, npj Quantum Information **1**, 1 (2015).

[26] S. Boucheron, G. Lugosi and P. Massart, *Concentration inequalities: A nonasymptotic theory of independence* (Oxford university press, 2013).

A   Proof of the individual-constraint method (5)

The proof follows the lines of that given in Appendix A of [19], being, however, valid not only for the Hoeffding bound as in [19], but also for the Empirical Bernstein bound.

The trace and semipositivity conditions in (5) are always obeyed by the actual quantum state ω. Consider N_i shots for the measurement of $\mathbb{E}(o_i) = \operatorname{tr}(O_i\omega)$ for given $i \in \{1, 2, \ldots, K\}$. This entails that there are N_i real-valued i.i.d. random variables for each i. They have, for simplicity, range $R = [-1, 1]$, and their empirical average and standard deviation are o_i and s_i, respectively. Given these data, the probability for a single fluctuation to lie outside a range defined by ϵ_i can in general be upper bounded,

$$\operatorname{Prob}(|\mathbb{E}(o_i) - o_i| > \epsilon_i) \le \delta\,, \tag{10}$$

where concentration inequalities [26] allow finding closed expressions for $\epsilon_i(\delta)$. Defining $\alpha_\delta := \sqrt{2\ln(2/\delta)}$, then

$$\epsilon_i^{(\mathrm{H})}(\delta) \quad := \quad \frac{\alpha_\delta}{\sqrt{N_i}}\,, \tag{11}$$

$$\epsilon_i^{(\mathrm{EB})}(\delta) \quad := \quad s_i\frac{\alpha_{\delta/2}}{\sqrt{N_i}} + \frac{7}{3}\frac{\alpha_{\delta/2}^2}{N_i - 1} \tag{12}$$

are eligible options, corresponding to Hoeffding's and Empirical Bernstein's [17, 18] inequalities, respectively. This implies that to restrict the set as much as possible we can take

$$\epsilon_i(\delta) = \min[\epsilon_i^{(\mathrm{H})}(\delta), \epsilon_i^{(\mathrm{EB})}(\delta)]\,. \tag{13}$$

From the union bound, and using $\mathbb{E}(o_i) = \operatorname{tr}(O_i\omega)$,

$$\operatorname{Prob}\left[\exists i \quad s.t.\, |\operatorname{tr}(O_i\omega) - o_i| > \epsilon_i(\delta')\right] \le \sum_{i=1}^{K} \operatorname{Prob}[\,|\operatorname{tr}(O_i\omega) - o_i| > \epsilon_i(\delta')]\,, \tag{14}$$

we obtain a bound for the violation of any of the K constraints,

$$\operatorname{Prob}\left[\exists i \quad s.t.\, |\operatorname{tr}(O_i\omega) - o_i| > \epsilon_i(\delta')\right] \le K\delta'\,. \tag{15}$$

By rescaling $\delta' = \delta/K$, we conclude that with probability at least $1 - \delta$ all ϵ constraints in (5) are fulfilled by ω. As such, with probability at least $1 - \delta$ the state ω is in the feasible space of Problem (5). Since the minimum (maximum) $\mathcal{F}_{\mathrm{LB(UB)}}$ serves as lower (upper) bound to any state in the feasible space, it bounds $\mathcal{F}(\omega)$ with probability at least $1 - \delta$. $\qquad\square$

We remark that, as the union bound does not assume statistical independence between the several random variables o_i, this implies that the method (5) can be applied for this case too.

B Improving the individual-constraint method (5)

We present here a more involved improved version of the Individual-constraint method (5). We start noticing that for generic

$$\vec{\delta} = (\delta_1, \delta_2, \ldots, \delta_K)^T, \quad \sum_{i=1}^K \delta_i = \delta, \quad \delta_i \geq 0, \tag{16}$$

$$\begin{aligned} \mathcal{F}_{\mathrm{LB(UB)}}(\vec{\delta}) = \min_\rho(\max_\rho) \quad & \mathcal{F}(\rho) \\ \text{s.t.} \quad & \mathrm{tr}(\rho) = 1 \\ & \rho \geq 0 \\ & |\mathrm{tr}(O_i\rho) - o_i| \leq \min(\tfrac{\alpha_{\delta_i}}{\sqrt{N_i}}, \, s_i\tfrac{\alpha_{\delta_i/2}}{\sqrt{N_i}} + \tfrac{7}{3}\tfrac{\alpha_{\delta_i/2}^2}{N_i-1}) \quad \forall i \in \mathcal{I}, \end{aligned} \tag{17}$$

is a lower (upper) bound for $\mathcal{F}(\omega)$ with probability at least $1 - \delta$.

Method (5) sets $\delta_i = \delta/K$, but there are in general non-uniform choices of the vector probabilities $\vec{\delta}$ for which method (17) is tighter.

C Parallel measurements and correlators

In introducing the parallel measurement framework we follow, among others, the introduction of Reference [19].

A common decomposition for the density operator ρ of an n-qubit system is in terms of Pauli operators,

$$\rho = \frac{1}{2^n} \sum_{i=0}^{4^n-1} \mathrm{tr}(O_i\rho)\, O_i, \quad O_i := \sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_n}, \tag{18}$$

with $\sigma_{i_j} \in \{\mathbb{1}_2, \sigma_x, \sigma_y, \sigma_z\}$ and where the term $\mathrm{tr}(O_0\rho) = 1$, as $O_0 := \otimes_{j=1}^n \mathbb{1}_2 = \mathbb{1}_{2^n}$. This means that, in principle, in order to unequivocally identify the quantum state, one should measure the $4^n - 1$ expectation values of the operators (18). However, nowadays parallel measurements are experimentally under control. One can concurrently measure in one shot all the n qubits in different local bases, obtaining n binary outcomes $\vec{a} := (a_1, a_2, \ldots, a_n)$, where $a_j \in \{-1, 1\}$, from a given measurement setting

$$\vec{\alpha} := (\alpha_1, \alpha_2, \ldots \alpha_n), \tag{19}$$

with $\alpha_j \in \{x, y, z\}$. Collecting the corresponding counts $N_{a_1,a_2,\ldots,a_n|\alpha_1,\alpha_2,\ldots,\alpha_n}$ leads to the estimated probabilities

$$p(a_1, a_2, \ldots, a_n|\alpha_1, \alpha_2, \ldots, \alpha_n) \approx \frac{N_{a_1,a_2,\ldots,a_n|\alpha_1,\alpha_2,\ldots,\alpha_n}}{N_{\alpha_1,\alpha_2,\ldots,\alpha_n}} \tag{20}$$

of obtaining the array of outcomes $(a_1, a_2, \ldots, a_n)$ from the measurement setting (19). There are in total 2^n possible outcomes $(a_1, a_2, \ldots, a_n)$ and 3^n possible measurement settings (19).

From the above counts $N_{a_1,a_2,\ldots,a_n|\alpha_1,\alpha_2,\ldots,\alpha_n}$ one can infer the correlators $\mathrm{tr}(O_i\rho)$, by marginalizing the appropriate qubits. For instance, in the case of 4 qubits and from the measurement setting (x, x, y, z), one can estimate the correlator

$$tr(\sigma_x \otimes \mathbb{1} \otimes \sigma_y \otimes \sigma_z\, \rho) \approx \sum_{a_1,a_2,a_3,a_4} a_1 a_3 a_4 \frac{N_{a_1,a_2,a_3,a_4|x,x,y,z}}{N_{x,x,y,z}}. \tag{21}$$

More generally, a given k-body correlator (k counts how many Pauli matrices are not the identity in the string (18)) can be estimated from several measurement settings,

$$\mathrm{tr}(\otimes_{j=1}^n \sigma_{i_j}\, \rho) \approx o_i = \frac{\sum_{\vec{\alpha}|i} \sum_{\vec{a}} (\prod_{j|i} a_j) N_{\vec{a}|\vec{\alpha}}}{\sum_{\vec{\alpha}|i} \sum_{\vec{a}} N_{\vec{a}|\vec{\alpha}}}. \tag{22}$$

10

The $\sum_{\vec{\alpha}|i}$ means that the sum must be taken only over the measurement settings $\vec{\alpha}$ that are "compatible" with the correlator $\text{tr}(\otimes_{j=1}^{n} \sigma_{i_j} \rho)$. More precisely, the number of settings that must be considered for the estimation of a k-body correlator is

$$N_{\text{ms}}(k) = 3^{n-k} . \tag{23}$$

Those settings are the ones that can coincide with the correlator string $(i_1, \ldots, i_n)$ when substituting one or more elements of the measurement setting string $(\alpha_1, \ldots, \alpha_n)$ with the identity (the latter being identified by $i_j = 0$). The $\prod_{j|i} a_j$ imposes instead to consider in the product only the locations j for which $i_j \neq 0$. Hence, the denominator in (22),

$$N_i = \sum_{\vec{\alpha}|i} \sum_{\vec{a}} N_{\vec{a}|\vec{\alpha}} , \tag{24}$$

counts the number of shots used for the estimation of the correlator i. According to our notation, N_0 coincides with the total number of measurement shots in the experiment and $o_0 = 1$ accounts for the normalization condition of the density matrix. Furthermore, the above formalism includes the case where not all the settings are measured (informationally incomplete scenario), as in that case one can set to zero the corresponding counts and apply (22) only when its denominator N_i is non-zero.

D   Proof of the joint-constraint method (8)

The proof follows along the lines of Appendix A, but with a different concentration inequality. Consider we have N copies of a quantum state ω and we measure them using a POVM E with m possible outcomes. With $\vec{p} = (tr(\omega E_1), tr(\omega E_2), ..., tr(\omega E_m))$, let $\vec{Z} = (Z_1, Z_2, \ldots, Z_m)$ be the outcomes (counts) of that measurement. Now, $\vec{Z}$ is a multinomially distributed random vector with parameters $(p_1, p_2, \ldots, p_m)$ such that $\sum_{i=1}^{m} Z_i = N$. The Bretagnolle–Huber–Carol bound [20] holds and can be written as:

$$\text{Prob}\left(\sum_{i=1}^{m} \left| \frac{Z^{(i)}}{N} - p_i \right| \geq \epsilon \right) \leq 2^m e^{-N\epsilon^2/2} =: \delta , \tag{25}$$

bounding the probability for the total ℓ_1-norm error to be above ϵ. Identifying $\vec{q} = \vec{Z}/N$ and solving for ϵ as a function of δ, we can state that, with probability at least $1 - \delta$,

$$\|\vec{p} - \vec{q}\|_1 \leq \epsilon = \sqrt{\frac{2}{N} \ln \frac{2^m}{\delta}} , \tag{26}$$

recovering the ϵ condition from (9). As in Appendix A, with probability $1 - \delta$ the actual state ω is in the feasible space and the bounds $\mathcal{F}_{\text{LB(UB)}}$ hold. $\square$

E   Certification of state preparation II

For sake of illustration, we present a last example concerning maximum fidelity of state preparation. In this application, we receive copies of a quantum state ω, and we are told that this state corresponds to a pure state $|\psi\rangle$. We want to prove that this is false. To achieve this, we perform measurements on the given copies and determine the maximum fidelity $F(\rho) = \langle\psi|\rho|\psi\rangle$ between the states ρ in the feasibility set Ω and the reference state $|\psi\rangle$. If the maximum fidelity differs from 1, we can conclude that the state ω is not equal to $|\psi\rangle$.

In Fig 4, we prepare 100 states of the form $0.9|\psi\rangle\langle\psi| + \frac{0.1}{16}I$, where $|\psi\rangle$ are Haar-random pure states of 4 qubits. We subject these states to measurements using 16 randomly chosen Pauli bases, with varying numbers of total shots. The joint-constraint protocol is then applied with confidence level of 0.997. Blue dots depict the fidelity between the resulting states and the reference states $|\psi\rangle$. We
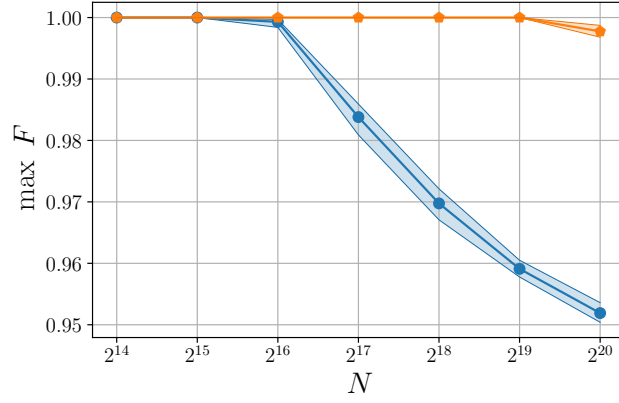
Figure 4: Maximum fidelity between a prepared state $0.9|\psi\rangle\langle\psi| + \frac{0.1}{16}I$ and the reference state $|\psi\rangle$ for 4 qubits. The solid lines represent the median value obtained from 100 Haar-random pure states using our method (blue dots) and method from Ref. [13] (orange pentagons), while the shaded areas depict the interquartile ranges.

compare these results with those obtained using protocol A from Ref. [13], where the same confidence level and total shot count N are used, but in this case, we measure the 81 Pauli strings that are informationally complete for 4 qubits. Our protocol needs around 2^{16} shots to succeed, while Protocol A needs around 2^{20}, 16 times more shots.