Building Trust for Continuous Variable Quantum States

Ulysse Chabaud[1]
Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université,
4 place Jussieu, 75005 Paris, France
ulysse.chabaud@gmail.com

Tom Douce
School of Informatics, University of Edinburgh,
10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom

Frédéric Grosshans
Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université,
4 place Jussieu, 75005 Paris, France
Laboratoire Aimé Cotton, CNRS, Université Paris-Sud, ENS Cachan, Université Paris-Saclay, 91405 Orsay Cedex, France

Elham Kashefi
Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université,
4 place Jussieu, 75005 Paris, France
School of Informatics, University of Edinburgh,
10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom

Damian Markham
Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université,
4 place Jussieu, 75005 Paris, France

Abstract

In this work we develop new methods for the characterisation of continuous variable quantum states using heterodyne measurement in both the trusted and untrusted settings. First, building on quantum state tomography with heterodyne detection, we introduce a reliable method for continuous variable quantum state certification, which directly yields the elements of the density matrix of the state considered with analytical confidence intervals. This method neither needs mathematical reconstruction of the data nor discrete binning of the sample space and uses a single Gaussian measurement setting. Second, beyond quantum state tomography and without its identical copies assumption, we promote our reliable tomography method to a general efficient protocol for verifying continuous variable pure quantum states with Gaussian measurements against fully malicious adversaries, i.e., making no assumptions whatsoever on the state generated by the adversary. These results are obtained using a new analytical estimator for the expected value of any operator acting on a continuous variable quantum state with bounded support over the Fock basis, computed with samples from heterodyne detection of the state.

2012 ACM Subject Classification Theory of computation → Quantum information theory

Keywords and phrases Continuous variable quantum information, reliable state tomography, certification, verification

Digital Object Identifier 10.4230/LIPIcs.TQC.2020.3

Related Version A full version of the paper is available at `https://arxiv.org/abs/1905.12700`

Acknowledgements We thank N. Treps, V. Parigi, and especially M. Walschaers for stimulating discussions. We also thank A. Leverrier for interesting discussion on de Finetti reductions, and useful comments on previous versions of this work. This work was supported by the ANR project ANR-13-BS04-0014 COMB.

[1] Corresponding author

1 Introduction

Out of the many properties featured by quantum physics, the impossibility to perfectly determine an unknown state [8] is specially interesting. This property is at the heart of quantum cryptography protocols such as quantum key distribution [3]. On the other hand, it makes certification of the correct functioning of quantum devices a challenge, since the output of such devices can only be determined approximately, through repeated measurements over numerous copies of the output states. With rapidly developing quantum technologies for communication, simulation, computation and sensing, the ability to assess the correct functioning of quantum devices is of major importance, for near-term systems, the so-called Noisy Intermediate-Scale Quantum (NISQ) devices [23], and for the more sophisticated devices.

Depending on the desired level of trust, various methods are available for certifying the output of quantum devices. In the following, the task of checking the output state of a quantum device is denoted *tomography* for state independent methods, when i.i.d. behaviour is assumed, *certification* for a given a target state, when i.i.d. behaviour is assumed, and *verification* for a given target state, with no assumption whatsoever, and in particular without the i.i.d. assumption.

Quantum state tomography [9] is an important technique which aims at reconstructing a good approximation of the output state of a quantum device by performing multiple rounds of measurements on several copies of said output states. Given an ensemble of identically prepared systems, with measurement outcomes from the same observable, one can build up a histogram, from which a probability density can be estimated. According to Born's rule, this probability density is the square modulus of the state coefficients, taken in the basis corresponding to the measurement. However, a single measurement setting cannot yield the full state information since the phase of its coefficients are then lost. Many sets of measurements on many subensembles must be performed and combined to reconstruct the density matrix of the state. The data do not yield the state directly, but rather indirectly through data analysis. Quantum state tomography assumes an *independent and identically distributed* (i.i.d.) behaviour for the device, i.e., that the density matrix of the output state considered is the same at each round of measurement. This assumption may be relaxed with a tradeoff in the efficiency of the protocol [7].

A certification task corresponds to a setting where one wants to benchmark an industrial quantum device, or check the output of a physical experiment. On the other hand, a verification task corresponds to a cryptographic scenario, where the device to be tested is untrusted, or the quantum data is given by a potentially malicious party, for example in the context of delegated quantum computing. In the latter case, the task of quantum verification is to ensure that either the device behaved properly, or the computation aborts with high probability. While delegated computing is a natural platform for the emerging NISQ devices, one can provide a physical interpretation to this adversarial setting by emphasising that we aim for deriving verification schemes that make no assumptions whatsoever about the noise model of the underlying systems. Various methods for verification of quantum devices have been investigated, in particular for discrete variable quantum information [14], and they provide different efficiencies and security parameters depending on the computational power of the verifier. The common feature for all of these approaches is to utilise some basic obfuscation scheme that allows to reduce the problem of dealing with a fully general noise model, or a fully general adversarial deviation of the device, to a simple error detection scheme [27].

In this work, we consider the setting of quantum information with continuous variables [18], in which quantum states live in an infinite-dimensional Hilbert space. Using continuous variable systems for quantum computation and more general quantum information processing is a powerful alternative to the discrete variable case. *Firstly*, it is compatible with standard network optics technology, where more efficient measurements are available. *Secondly*, it allows for unprecedented scaling in entanglement, with entangled states of up to tens of thousands of subsystems reported [30] generated deterministically.

A continuous variable quantum process or state can be described by a quasi-probability distribution in phase space, often the Wigner function [28], but also the Husimi Q function or the Glauber–Sudarshan P function [5]. This allows for a simple and experimentally relevant classification of quantum states: those with a Gaussian quasiprobability distibutions are called Gaussian states, and the others non-Gaussian states. By extension, operations mapping Gaussian states to Gaussian states are also called Gaussian. These Gaussian operations and states are the ones implementable with linear optics and quadratic non-linearities [4], and are hence relatively easy to construct experimentally. However, it is well known that for many important applications, Gaussian operations and Gaussian states are not sufficient. This takes the forms of no-go theorems for distillation and error correction [10, 12, 20], and the fact that all Gaussian computations can be simulated efficiently classically [2]. Furthermore, it is not possible to demonstrate non-locality or contextuality – which are increasingly understood to be important resources in quantum information – in the Gaussian regime.

For continuous variable quantum devices, checking that the output state is close to a target state may be done with linear optics using optical homodyne tomography [19]. This method allows to reconstruct the Wigner function of a generic state using only Gaussian measurements, namely homodyne detection. Because of the continuous character of its outcomes, one must proceed to a discrete binning of the sample space, in order to build probability histograms. Then, the state representation in phase space is determined by a mathematical reconstruction.

For cases where we have a specific target state, more efficient options are possible. For multimode Gaussian states, more efficient certification methods have been derived with Gaussian measurements [1]. These methods involve the computation of a fidelity witness, i.e., a lower bound on the fidelity, from the measured samples. The cubic phase state certification protocol of [17] also introduces a fidelity witness and is an example of certification of a specific non-Gaussian state with Gaussian measurements, which assumes an i.i.d. state preparation. The verification protocol for Gaussian continuous variable weighted hypergraph states of [25] removes this assumption, again for this specific family of states.

2 Results

In this work we address two main issues. *Firstly*, existing continuous variable state tomography methods are not reliable in the sense of [7], because errors coming from the reconstruction procedure are indistinguishable from errors coming from the data. *Secondly*, to the best of our knowledge there is no Gaussian verification protocol for non-Gaussian states without i.i.d. assumption (a possible route using Serfling's bound was mentioned in Ref. [17] for removing the i.i.d. assumption for their protocol).

We thus introduce a general *receive-and-measure* protocol for building trust for continuous variable quantum states, using solely Gaussian measurements, namely heterodyne detection [11, 26]. This protocol allows to perform reliable continuous variable quantum state tomography based on heterodyne detection, with analytical confidence intervals, which we

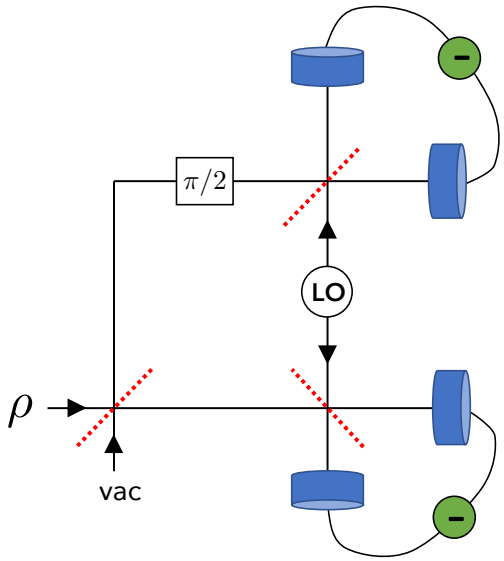

Figure 1 A schematic representation of heterodyne measurement of a state ρ. The dashed red lines represent balanced beamsplitters. *LO* stands for local oscillator, i.e., strong coherent state, and *vac* for vacuum state. The blue circles are photodiode detectors.

refer to as *heterodyne tomography* in what follows. This tomography technique only requires a single fixed measurement setting, compared to homodyne tomography. This protocol also provides a means for certifying continuous variable quantum states with an energy test, under the i.i.d. assumption. Finally, the same protocol also allows to verify continuous variable states, without the i.i.d. assumption. For these three applications, the measurements performed are the same. It is only the number of subsystems to be measured and the classical post-processing performed that differ from one application to another.

We detail the structure of the protocol in the following. We give an estimator for the expected value of any operator acting on a state with bounded support over the Fock basis (Theorem 1) by deriving an approximate version of the optical equivalence theorem for antinormal ordering [5]. The estimate is expressed as an expected value under heterodyne detection. Similar estimates have been obtained in the context of imperfect heterodyne detection [21, 22]. We go beyond these works in different respects: using this result, we introduce a reliable heterodyne tomography method and compute analytical bounds on its efficiency (Theorem 3). We then derive a *receive-and-measure* certification protocol (against i.i.d. adversary) for continuous variable quantum states, with Gaussian measurements (Theorem 4). We further promote this certification technique to a verification protocol against fully malicious adversary (Theorem 5), using a de Finetti reduction for infinite-dimensional systems [24].

3 Description of the protocol

Continuous variable quantum states live in an infinite-dimensional Hilbert space $\mathcal{H}$, spanned by the Fock basis $\{|n\rangle\}_{n\in\mathbb{N}}$, and are equivalently represented in phase space by their Husimi Q function [5], a smoother relative of the Wigner function. Given a single-mode state ρ, its Q function is defined as:

$$Q_\rho(\alpha) = \frac{1}{\pi}\,\mathrm{Tr}\left(|\alpha\rangle\langle\alpha|\,\rho\right) = \mathrm{Tr}\left(\Pi_\alpha \rho\right), \tag{1}$$

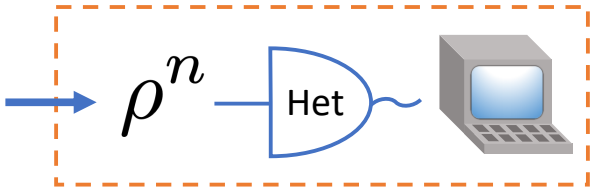

Figure 2 A schematic representation of the protocol. The tester (within the dashed rectangle) receives a continuous variable quantum state ρ^n over n subsystems. This state could be for example the outcome of n successive runs of a physical experiment, the output of a commercial quantum device, or directly sent by some untrusted quantum server. The tester measures with heterodyne detection some of the subsystems of ρ^n, and uses the samples and efficient classical post-processing to deduce information about the remaining subsystems.

for all $\alpha \in \mathbb{C}$, where $|\alpha\rangle$ is a coherent state and where $\{\Pi_\alpha\}_{\alpha\in\mathbb{C}} = \left\{\frac{1}{\pi}|\alpha\rangle\langle\alpha|\right\}_{\alpha\in\mathbb{C}}$ is the Positive Operator Valued Measure for heterodyne detection.

This detection, also called double homodyne or eight-port homodyne [11], consists in splitting the measured state with a beamsplitter, and measuring both ends with homodyne detection (Fig. 1). This corresponds to a joint noisy measurement of quadratures q and p. This is a Gaussian measurement, which yields two real outcomes, corresponding to the real and imaginary parts of α. The Q function of a single-mode state thus is a probability density function over $\mathbb{C}$ and measuring a state with heterodyne detection amounts to sampling from its Q function.

Using this detection, one may acquire knowledge about an unknown continuous variable quantum state. More precisely, we define the following *receive-and-measure* protocol, depicted in Fig. 2: given a quantum state ρ^n over n subsystems, measure some of the subsystems with heterodyne detection. Then, post-process the samples obtained to retrieve information about the remaining subsystems. The number subsystems to be measured and the post-processing performed depend on the application considered.

We show in the following sections how this protocol may be used to perform reliable tomography, certification and verification of continuous variable quantum states, and we detail the corresponding choices of subsystems and the classical post-processing for each task.

4 Heterodyne estimator

This section contains our main technical result, an estimator for the expected value of an operator acting on a state with bounded support over the Fock basis, from samples of heterodyne detection of the state. From this result, we derive various protocols in the following sections, ranging from tomography to state verification.

We denote by $\mathop{\mathbb{E}}_{\alpha\leftarrow D}[f(\alpha)]$ the expected value of a function f for samples drawn from a distribution D. Let us introduce for $k, l \geq 0$ the polynomials

$$\mathcal{L}_{k,l}(z) = e^{zz^*} \frac{(-1)^{k+l}}{\sqrt{k!}\sqrt{l!}} \frac{\partial^{k+l}}{\partial z^k \partial z^{*l}} e^{-zz^*}, \tag{2}$$

for $z \in \mathbb{C}$, which are, up to a normalisation, the Laguerre 2D polynomials, appearing in particular in the expressions of Wigner function of Fock states [29]. For any operator

$A = \sum_{k,l=0}^{+\infty} A_{kl} |k\rangle\langle l|$ and all $E \in \mathbb{N}$, we define with these polynomials the function

$$f_A(z,\eta) = \frac{1}{\eta} e^{\left(1-\frac{1}{\eta}\right)zz^*} \sum_{k,l=0}^{E} \frac{A_{kl}}{\sqrt{\eta^{k+l}}} \mathcal{L}_{k,l}\left(\frac{z}{\sqrt{\eta}}\right), \tag{3}$$

for all $z \in \mathbb{C}$, and all $0 < \eta < 1$. We omit the dependency in E for brevity. The function $z \mapsto f_A(z,\eta)$, being a polynomial multiplied by a converging Gaussian function, is bounded over $\mathbb{C}$. With the same notations, we also define the following constant:

$$K_A = \sum_{k,l=0}^{E} |A_{kl}| \sqrt{(k+1)(l+1)}. \tag{4}$$

The optical equivalence theorem for antinormal ordering [5] gives an equivalence between the expectation value of an operator in Hilbert space and the expectation value of its Glauber-Sudarshan P function. The P function is however highly singular in general and our results are based instead on the following approximate version of this equivalence when the P function is replaced by the bounded function f:

▶ **Theorem 1.** *Let $E \in \mathbb{N}$ and let $0 < \eta < \frac{2}{E}$. Let also $A = \sum_{k,l=0}^{+\infty} A_{kl} |k\rangle\langle l|$ be an operator and let $\rho = \sum_{k,l=0}^{E} \rho_{kl} |k\rangle\langle l|$ be a density operator with bounded support. Then,*

$$\left| \mathrm{Tr}\,(A\rho) - \mathop{\mathbb{E}}_{\alpha \leftarrow Q_\rho}[f_A(\alpha,\eta)] \right| \leq \eta K_A, \tag{5}$$

where the function f and the constant K are defined in Eqs. (3) and (4).

For all theorems, the proof techniques are given in appendix A and the detailed proofs may be found in [6]. This result provides an estimator for the expected value of any operator A acting on a continuous variable state ρ with bounded support over the Fock basis. This estimator is the expected value of a bounded function f_A over samples drawn from the probability density corresponding to a Gaussian measurement of ρ, namely heterodyne detection. The optical equivalence theorem for antinormal ordering corresponds to the limit $\eta \to 0$. The right hand side of Eq. (5) is an energy bound, which depends on the operator A, the value E and the precision parameter η.

When the operator A is the density matrix of a continuous variable pure state $|\Psi\rangle$, the previous estimator approximates the fidelity $F(\Psi,\rho) = \langle\Psi|\rho|\Psi\rangle$ between $|\Psi\rangle\langle\Psi|$ and ρ. With the same notations:

▶ **Corollary 2.** *Let $E \in \mathbb{N}$ and let $0 < \eta < \frac{2}{E}$. Let also $|\Psi\rangle\langle\Psi| = \sum_{k,l=0}^{+\infty} \psi_k \psi_l^* |k\rangle\langle l|$ be a normalised pure state and let $\rho = \sum_{k,l=0}^{E} \rho_{kl} |k\rangle\langle l|$ be a density operator with bounded support. Then,*

$$\left| F\,(\Psi,\rho) - \mathop{\mathbb{E}}_{\alpha \leftarrow Q_\rho}[f_\Psi(\alpha,\eta)] \right| \leq \eta K_\Psi \leq \frac{\eta}{2}(E+1)(E+2), \tag{6}$$

where the function f_A and the constant K_A are defined in Eqs. (3) and (4), for $A = |\Psi\rangle\langle\Psi|$.

This result provides an estimator for the fidelity between any target pure state $|\Psi\rangle$ and any continuous variable (mixed) state ρ with bounded support over the Fock basis. This estimator is the expected value of a bounded function f_Ψ over samples drawn from the probability density corresponding to a Gaussian measurement of ρ, namely heterodyne detection. The right hand side of Eq. (6) is an energy bound, which may be refined depending on the

expression of $|\Psi\rangle$. In particular, the second bound is independent of the target state $|\Psi\rangle$. The assumption of bounded support makes sense for tomography, but not necessarily in an adversarial setting. We will relax this condition for the certification and verification protocols in the following, and indeed estimate the energy bound from the heterodyne measurements. Errors in this estimation are taken into account in the confidence statements.

Given these results, one may choose a target pure state $|\Psi\rangle$, and measure with heterodyne detection various copies of the output (mixed) state ρ of a quantum device with bounded support over the Fock basis. Then, using the samples obtained, one may estimate the expected value of f_Ψ, thus obtaining an estimate of the fidelity between the states $|\Psi\rangle\langle\Psi|$ and ρ. Using this result, we introduce a reliable method for performing continuous variable quantum state tomography using heterodyne detection.

5 Reliable continuous variable state tomography

Continuous variable quantum state tomography methods usually make two assumptions: firstly that the measured states are independent identical copies (i.i.d. assumption, for *independently and identically distributed*), and secondly that the measured states have a bounded support over the Fock basis [19]. With the same assumptions, we present a reliable method for state tomography with heterodyne detection which has the advantage of providing analytical confidence intervals. Our method directly provides estimates of the elements of the state density matrix, phase included. As such, neither mathematical reconstruction of the phase, nor binning of the sample space is needed, since the samples are used only to compute expected values of bounded functions. Moreover, only a single fixed Gaussian measurement setting is needed, namely heterodyne detection (Fig. 1).

For tomographic application, all copies of the state are measured. For $n \geq 1$, let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be samples from heterodyne detection of n copies of a quantum state ρ. For $\epsilon > 0$ and $k, l \in \mathbb{N}$, we define

$$\rho^\epsilon_{kl} = \frac{1}{n} \sum_{i=1}^{n} f_{|l\rangle\langle k|} \left(\alpha_i, \epsilon / K_{|l\rangle\langle k|}\right), \tag{7}$$

where the function f_A and the constant K_A are defined in Eqs. (3) and (4), for $A = |l\rangle\langle k|$, and where $\epsilon > 0$ is a free parameter. The quantity ρ^ϵ_{kl} is the average of the function $f_{|l\rangle\langle k|}$ over the samples $\alpha_1, \ldots, \alpha_n$. The next result shows that this estimator approximates the matrix element k, l of this state with high probability. We use the notations of Theorem 1.

▶ **Theorem 3** (Reliable heterodyne tomography). *Let $\epsilon, \epsilon' > 0$, $n \geq 1$ and $\alpha_1, \ldots, \alpha_n$ be samples obtained by measuring with heterodyne detection n copies of a state $\rho = \sum_{k,l=0}^{E} \rho_{kl} |k\rangle\langle l|$ with bounded support, for $E \in \mathbb{N}$. Then*

$$|\rho_{kl} - \rho^\epsilon_{kl}| \leq \epsilon + \epsilon', \tag{8}$$

for all $0 \leq k, l \leq E$, with probability greater than

$$1 - 4 \sum_{0 \leq k \leq l \leq E} \exp\left[-\frac{n\epsilon^{2+k+l}\epsilon'^2}{4C_{kl}}\right], \tag{9}$$

where the estimate ρ^ϵ_{kl} is defined in Eq. (7) and where

$$C_{kl} = [(k+1)(l+1)]^{1+\frac{k+l}{2}} \, 2^{|l-k|} \binom{\max(k,l)}{\min(k,l)} \tag{10}$$

is a constant independent of ρ.

In light of this result, the principle for performing reliable heterodyne tomography is straightforward and as follows: n identical copies $\rho^{\otimes n}$ of the output quantum state of a physical experiment or quantum device are measured with heterodyne detection, yielding the values $\alpha_1, \ldots, \alpha_n$. These values are used to compute the estimates ρ^{ϵ}_{kl}, defined in Eq. (7), for all k, l in the range of energy of the experiment. Then, Theorem 3 directly provides confidence intervals for all these estimates of ρ_{kl}, the matrix elements of the density operator ρ, without the need for a binning of the sample space or any additional data reconstruction, using a single measurement setting. For a desired precision ϵ and a failure probability δ, the number of samples needed scales as $n = \text{poly}(1/\epsilon, \log(1/\delta))$.

Both homodyne and heterodyne quantum state tomography assume a bounded support over the Fock basis for the output state considered, i.e., that all matrix elements are equal to zero beyond a certain value, and that the output quantum states are i.i.d., i.e., that all measured output states are independent and identical. While these assumptions are natural when looking at the output of a physical experiment, corresponding to a noisy partially trusted quantum device with bounded energy, they may be questionable in the context of untrusted devices. We remove these assumptions in what follows: we first drop the bounded support assumption, deriving a certification protocol for continuous variable quantum states of an i.i.d. device with heterodyne detection ; then, we drop both assumptions, deriving a general verification protocol for continuous variable quantum states against an adversary who can potentially be fully malicious.

6 State certification with Gaussian measurements

Given an untrusted source of quantum states, the purpose of state certification and state verification protocols is to check whether if its output state is close to a given target state, or far from it. To achieve this, a verifier tests the output state of the source. Ideally, one would like to obtain an upper bound on the probability that the state is not close from the target state, given that it passed a test. However, this is known to be impossible without prior knowledge of the tested state distribution [14]. Indeed, writing this conditional probability

$$\Pr[\text{incorrect}|\text{accept}] = \frac{\Pr[\text{incorrect} \cap \text{accept}]}{\Pr[\text{accept}]}, \tag{11}$$

in a situation where the device always produces a bad output state, it is rejected by the verifier's test most of the time, so the acceptance probability is very small and the conditional probability is equal to 1. Therefore, the quantity that will always be bounded in certification and verification protocols, in which one does not have prior knowledge of the device, is the joint probability that the tested state is not close to the target state *and* that it passes the test. Equivalently, we obtain lower bounds on the probability that the tested state is close to the target state or that it fails the test.

We first consider the certification of the output of an i.i.d. quantum device, i.e., which output state is the same at each round. However, we do not assume that the output states of the device have bounded support over the Fock basis anymore. This is instead ensured probabilistically using the samples from heterodyne detection.

Our continuous variable quantum state certification protocol is then as follows: let $|\Psi\rangle$ be a target pure state, of which one wants to certify m copies. The values s and E are free parameters of the protocol. One instructs the i.i.d. device to prepare $n+m$ copies of $|\Psi\rangle$, and the device outputs an i.i.d. (mixed) state $\rho^{\otimes(n+m)}$. One keeps m copies $\rho^{\otimes m}$, and measures the n others with heterodyne detection, obtaining the samples $\alpha_1, \ldots, \alpha_n$. One records the

number r of samples such that $|\alpha_i|^2 > E$. We refer to this step as *support estimation*. For a given $\epsilon > 0$, one also computes with the same samples the estimate

$$F_\Psi(\rho) = \left[\frac{1}{n}\sum_{i=1}^{n} f_\Psi\left(\alpha_i, \epsilon/(mK_\Psi)\right)\right]^m, \tag{12}$$

where the function f_A and the constant K_A are defined in Eqs. (3) and (4), for $A = |\Psi\rangle\langle\Psi|$, and where $\epsilon > 0$ is a free parameter. The next result quantifies how close this estimate is from the fidelity between the remaining m copies of the output state $\rho^{\otimes m}$ of the tested device and m copies of the target state $|\Psi\rangle\langle\Psi|^{\otimes m}$.

▶ **Theorem 4** (Gaussian certification of continuous variable quantum states)**.** *Let $\epsilon, \epsilon' > 0$, let $s \leq n$, and let $\alpha_1, \ldots, \alpha_n$ be samples obtained by measuring with heterodyne detection n copies of a state ρ. Let E in $\mathbb{N}$, and let r be the number of samples such that $|\alpha_i|^2 > E$. Let also $|\Psi\rangle$ be a pure state. Then for all $m \in \mathbb{N}^*$,*

$$\left|F(\Psi^{\otimes m}, \rho^{\otimes m}) - F_\Psi(\rho)\right| \leq \epsilon + \epsilon', \tag{13}$$

or $r > s$, with probability greater than

$$1 - \left(P^{iid}_{Support} + P^{iid}_{Hoeffding}\right), \tag{14}$$

where

$$P^{iid}_{Support} = \frac{(s+1)^{3/2}}{n} \exp\left[\frac{(s+1)^2}{n+1}\right], \tag{15}$$

$$P^{iid}_{Hoeffding} = 2\exp\left[-\frac{n\epsilon^{2+2E}\epsilon'^2}{2m^{4+2E}C_\Psi^2}\right], \tag{16}$$

where the estimate $F_\Psi(\rho)$ is defined in Eq. (12), and where

$$C_\Psi = \sum_{k,l=0}^{E} |\psi_k\psi_l| \left(\frac{\epsilon}{m}\right)^{E-\frac{k+l}{2}} K_\psi^{1+\frac{k+l}{2}} \sqrt{2^{|l-k|}\binom{\max(k,l)}{\min(k,l)}} \tag{17}$$

is a constant independent of ρ, with the constant K defined in Eq. (4).

This results implies that the quantity $F_\Psi(\rho)$ is a good estimate of the fidelity $F(\Psi^{\otimes m}, \rho^{\otimes m})$, or the score at the support estimation step is higher than s, with high probability. The values of the energy parameters E and s should be chosen to guarantee completeness, i.e., that if the correct state $|\Psi\rangle$ is sent, then $r \leq s$ with high probability.

This theorem is valid for all continuous variable target pure states $|\Psi\rangle$, and the failure probability may be greatly reduced depending on the expression of $|\Psi\rangle$. The number of samples needed for certifying a given number of copies m with a precision ϵ and a failure probability δ scales as $n = \mathrm{poly}(m, 1/\epsilon, 1/\delta)$. Note that the same protocol may be used to obtain reliable estimates of $\mathrm{Tr}(A\rho)$ for any operator A under the i.i.d. assumption, by setting $m = 1$ and replacing Ψ by A in Eq. (12).

This certification protocol is promoted to a verification protocol in the following section, by removing the i.i.d. assumption.

7 State verification with Gaussian measurements

We now consider an adversarial setting, where a verifier delegates the preparation of a continuous variable quantum state to a potentially malicious party, called the *prover*. One could see the verifier as the experimentalist in the laboratory and the prover as the noisy device, where we aim not to make any assumptions about its correct functionality or noise model. Given the absence of any direct error correction mechanism that permits a fault tolerant run of the device, the aim of verification is to ensure that a wrong outcome is not being accepted. In the context of state verification, this amounts to making sure that the output state of the tested device is close to an ideal target state.

The prover is not supposed to have i.i.d. behaviour. In particular, when asked for various copies of the same state, the prover may actually send a large state entangled over all subsystems, possibly also entangled with a quantum system on his side. In that case, the certification protocol derived in the previous section is not reliable. With usual tomography measurements, the number of samples needed for a given precision of the fidelity estimate scales exponentially in the number of copies to verify. This is an essential limitation of quantum tomography techniques, because they check all possible correlations between the different subsystems.

However we prove that, because of the symmetry of the protocol, the verifier can assume that the prover is sending permutation-invariant states, i.e., states that are invariant under any permutation of their subsystems. With a specific support estimation step, reduced states of permutation-invariant states are close to mixture almost-i.i.d. states, i.e., states that are i.i.d. on almost all subsystems. At the heart of this reduction is the de Finetti theorem for infinite-dimensional systems of [24], which allows restricting to an almost-i.i.d. prover.

Our verification protocol is then as follows: the verifier wants to verify m copies of a target pure state $|\Psi\rangle$. The values n, k, q, s and E are free parameters of the protocol. The prover is instructed to prepare $n+k$ copies of $|\Psi\rangle$ and send them to the verifier. The verifier picks k subsystems at random and measures them with heterodyne detection, obtaining the samples $\beta_1, \ldots, \beta_k$, and records the number r of values $|\beta_i|^2 > E$. The verifier discards $4q$ subsystems at random and measures all the others but m chosen at random with heterodyne detection, obtaining the samples $\alpha_1, \ldots, \alpha_{n-4q-m}$. Finally, the verifier computes with these samples the estimate

$$F_\Psi(\rho) = \left[\frac{1}{n-4q-m} \sum_{i=1}^{n-4q-m} f_\Psi\left(\alpha_i, \epsilon/(mK_\Psi)\right) \right]^m , \tag{18}$$

where the function f_A and the constant K_A are defined in Eqs. (3) and (4), for $A = |\Psi\rangle\langle\Psi|$ and where $\epsilon > 0$ is a free parameter. Note that this estimate is identical to the one defined in Eq. (12), replacing n by $n-4q-m$.

▶ **Theorem 5** (Gaussian verification of continuous variable quantum states)**.** *Let $n \geq 1$, let $s \leq k$, and let ρ^{n+k} be a state over $n+k$ subsystems. Let $\beta_1, \ldots, \beta_k$ be samples obtained by measuring k subsystems at random with heterodyne detection and let ρ^n be the remaining state after the measurement. Let E in $\mathbb{N}$, and let r be the number of samples such that $|\beta_i|^2 > E$. Let also $q \geq m$, and let ρ^m be the state remaining after discarding $4q$ subsystems of ρ^n at random, and measuring $n-4q-m$ other subsystems at random with heterodyne detection, yielding the samples $\alpha_1, \ldots, \alpha_{n-4q-m}$. Let $\epsilon, \epsilon' > 0$ and let $\epsilon'' = \sqrt{\frac{m(4q+m-1)}{n-4q}}$. Let $|\Psi\rangle$ be a target pure state. Then,*

$$\left| F\left(\Psi^{\otimes m}, \rho^m\right) - F_\Psi(\rho) \right| \leq \epsilon + \epsilon' + \epsilon'' + P_{deFinetti}, \tag{19}$$

or $r > s$, with probability greater than

$$1 - (P_{support} + P_{deFinetti} + P_{Hoeffding}), \tag{20}$$

where

$$P_{support} = 8k^{3/2} \exp\left[-\frac{k}{9}\left(\frac{q}{n} - \frac{2s}{k}\right)^2\right], \tag{21}$$

$$P_{deFinetti} = q^{(E+1)^2/2} \exp\left[-\frac{2q(q+1)}{n}\right], \tag{22}$$

$$P_{Hoeffding} = 2\binom{n-4q}{4q} \exp\left[-\frac{n-8q}{2m^{4+2E}}\left(\frac{\epsilon^{1+E}\epsilon'}{C_\Psi} - \frac{8qm^{2+E}}{n-4q-m}\right)^2\right], \tag{23}$$

where the estimate $F_\Psi(\rho)$ is defined in Eq. (18), and where C_Ψ is a constant independent of ρ defined in Eq. (17).

This result implies that the quantity $F_\Psi(\rho)$ is a good estimate of the fidelity $F(\Psi^{\otimes m}, \rho^m)$, or the score at the support estimation step is higher than s, with high probability. Like for the certification protocol, the values of the energy parameters E and s should be chosen by the verifier to guarantee completeness, i.e., that if the prover sends the correct state $|\Psi\rangle$, then $r \leq s$ with high probability.

For specific choices of the free parameters of the protocol either the estimate $F_\Psi(\rho)$ is polynomially precise in m, or $r > s$, with exponential probability in m, with $n, k, q = \text{poly}(m)$. In particular, the efficiency of the protocol may be greatly refined by taking into account the expression of $|\Psi\rangle$ in the Fock basis, and optimizing over the free parameters.

This verification protocol let the verifier gain confidence about the precision of the estimate of the fidelity in Eq. (18). If the value of the estimate is close enough to 1, the verifier may decide to use the state to run a computation. Indeed, statements on the fidelity of a state allow inferring the correctness of any trusted computation done afterwards using this state. Let $\beta > 0$, and let $\mathcal{O}$ be the observable corresponding to the result of the trusted computation performed on ρ^m, the reduced state over m subsystems instead of $|\Psi\rangle^{\otimes m}$, m copies of the target state $|\Psi\rangle$. In other words, $\mathcal{O}$ encodes the resources which the verifier can perform perfectly (ancillary states, evolution and measurements), the imperfections being encoded in ρ. Then, $F(\Psi^{\otimes m}, \rho^m) \geq 1 - \beta$ implies the following bound on the total variation distance between the probability densities of the computation output of the actual and the target computations:

$$\|P^{\mathcal{O}}_{\Psi^{\otimes m}} - P^{\mathcal{O}}_{\rho^m}\|_{tvd} \leq D(\Psi^{\otimes m}, \rho^m) \leq \sqrt{\beta}, \tag{24}$$

by standard properties of the trace distance D [13]. What this means is that the distribution of outcomes for the state ρ^m sent by the prover is almost indistinguishable from the distribution of outcomes for m copies of the ideal state $|\Psi\rangle$, when the fidelity is close enough to one.

8 Discussion

Determining an unknown continuous variable quantum state is especially difficult since it is described by possibly infinitely many complex parameters. Existing methods like homodyne quantum state tomography require many different measurement settings, and

heavy classical post-processing. For that purpose, we have introduced a reliable method for heterodyne quantum state tomography, which uses heterodyne detection as a single Gaussian measurement setting, and allows the retrieval of the density matrix of an unknown quantum state without the need for data reconstruction nor binning of the sample space. For data reconstruction methods such as Maximum Likelihood, errors from the reconstruction procedure are usually indistinguishable from errors coming from the tested quantum device. For that reason, such methods do not extend well to the task of verification, unlike our method.

Building on these tomography techniques, and with the addition of cryptographic techniques such as the de Finetti theorem, we have derived a protocol for verifying various copies of a continuous variable quantum state, without i.i.d. assumption, with Gaussian measurements. This protocol is robust, as it directly gives a confidence interval on an estimate of the fidelity between the tested state and the target pure state. We emphasize that, while the target state is pure, the tested state is not required to be pure.

Our verification protocol is complementary to the approach of [25], in which a measurement-only verifier performs continuous variable quantum computing by delegating the preparation of Gaussian cluster states to a prover, and has to perform non-Gaussian measurements. In our approach, the measurement-only verifier may perform continuous variable quantum computing by delegating the preparation of non-Gaussian states to the prover, and has to perform Gaussian measurement, which are much easier to perform experimentally.

Our protocol may be tailored to different uses and assumptions, from tomography to verification, simply by changing the classical post-processing. We expect this protocol to be useful for the validation of continuous variable quantum devices in the NISQ [23] era and onwards.

In particular, an interesting perspective would be fine-tuning the various parameters of the protocol for specific target states in order to optimise its efficiency, thus reducing the number of samples needed for a given confidence interval. Another interesting prospect would be extending our main technical result, Theorem 1, which applies to operators, to quantum maps. Also, in the case where the operator is the density matrix of a target pure state, our result provide an estimate for the fidelity, and it would be interesting to extend this to target mixed states.

References

1 Leandro Aolita, Christian Gogolin, Martin Kliesch, and Jens Eisert. Reliable quantum certification of photonic state preparations. *Nature communications*, 6:8498, 2015. doi:10.1038/ncomms9498.

2 Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein, and Kae Nemoto. Efficient classical simulation of continuous variable quantum information processes. *Phys. Rev. Lett.*, 88:097904, February 2002. doi:10.1103/PhysRevLett.88.097904.

3 C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, Bangalore, December 1984. doi:10.1016/j.tcs.2011.08.039.

4 Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, June 2005. doi:10.1103/RevModPhys.77.513.

5 Kevin E Cahill and Roy J Glauber. Density operators and quasiprobability distributions. *Physical Review*, 177(5):1882, 1969. doi:10.1103/PhysRev.177.1882.

6 Ulysse Chabaud, Tom Douce, Frédéric Grosshans, Elham Kashefi, and Damian Markham. Building trust for continuous variable quantum states. *quant-ph*, 2019. arXiv:1905.12700.

7 Matthias Christandl and Renato Renner. Reliable quantum state tomography. *Physical Review Letters*, 109(12):120403, 2012. doi:10.1103/PhysRevLett.109.120403.

8 G. M. D'Ariano and H. P. Yuen. Impossibility of measuring the wave function of a single quantum system. *Physical review letters*, 76(16):2832, 1996. doi:10.1103/PhysRevLett.76.2832.

9 G Mauro D'Ariano, Matteo GA Paris, and Massimiliano F Sacchi. Quantum tomography. *Advances in Imaging and Electron Physics*, 128:206–309, 2003. arXiv:quant-ph/0302028.

10 Jens Eisert, Stefan Scheel, and Martin B Plenio. Distilling gaussian states with gaussian operations is impossible. *Physical review letters*, 89(13):137903, 2002. doi:10.1103/PhysRevLett.89.137903.

11 Alessandro Ferraro, Stefano Olivares, and Matteo GA Paris. Gaussian states in continuous variable quantum information. *quant-ph*, 2005. arXiv:quant-ph/0503237.

12 Jaromír Fiurášek. Gaussian transformations and distillation of entangled gaussian states. *Physical review letters*, 89(13):137904, 2002. doi:10.1103/PhysRevLett.89.137904.

13 Christopher A Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

14 Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems*, 4:715–808, 2019. doi:10.1007/s00224-018-9872-3.

15 Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American statistical association*, 58(301):13–30, 1963. doi:10.1080/01621459.1963.10500830.

16 Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J Cerf. Security of continuous-variable quantum key distribution against general attacks. *Physical review letters*, 110(3):030502, 2013. doi:10.1103/PhysRevLett.110.030502.

17 Nana Liu, Tommaso F Demarie, Si-Hui Tan, Leandro Aolita, and Joseph F Fitzsimons. Client-friendly continuous-variable blind and verifiable quantum computing. *Physical Review A*, 100(6):062309, 2019. doi:PhysRevA.100.062309.

18 Seth Lloyd and Samuel L Braunstein. Quantum computation over continuous variables. In *Quantum Information with Continuous Variables*, pages 9–17. Springer, 1999. doi:10.1103/PhysRevLett.82.1784.

19 Alexander I Lvovsky and Michael G Raymer. Continuous-variable optical quantum-state tomography. *Reviews of Modern Physics*, 81(1):299, 2009. doi:10.1103/RevModPhys.81.299.

20 Julien Niset, Jaromír Fiurášek, and Nicolas J Cerf. No-go theorem for gaussian quantum error correction. *Physical review letters*, 102(12):120501, 2009. doi:10.1103/PhysRevLett.102.120501.

21 Matteo GA Paris. On density matrix reconstruction from measured distributions. *Optics communications*, 124(3-4):277–282, 1996. doi:10.1016/0030-4018(96)00019-3.

22 Matteo GA Paris. Quantum state measurement by realistic heterodyne detection. *Physical Review A*, 53(4):2658, 1996. doi:10.1103/PhysRevA.53.2658.

23 John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018. doi:10.22331/q-2018-08-06-79.

24 Renato Renner and J Ignacio Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical review letters*, 102(11):110504, 2009. doi:10.1103/PhysRevLett.102.110504.

25 Yuki Takeuchi, Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, and Joseph F Fitzsimons. Resource-efficient verification of quantum computing using serfling's bound. *npj Quantum Information*, 5:27, 2019. doi:10.1038/s41534-019-0142-2.

26 Yong Siah Teo, Christian R Muller, Hyunseok Jeong, Zdenek Hradil, Jaroslav Rehacek, and Luis L Sanchez-Soto. When heterodyning beats homodyning: an assessment with quadrature moments. *quant-ph*, 2017. arXiv:1701.07539.

27 Thomas Vidick. http://users.cms.caltech.edu/~vidick/verification_bulletin.pdf, 2018.

28 Eugene Paul Wigner. On the quantum correction for thermodynamic equilibrium. In *Part I: Physical Chemistry. Part II: Solid State Physics*, pages 110–120. Springer, 1997. doi:10.1103/PhysRev.40.749.

29 Alfred Wünsche. Laguerre 2d-functions and their application in quantum optics. *Journal of Physics A: Mathematical and General*, 31(40):8267, 1998. doi:10.1088/0305-4470/31/40/017.

30 Shota Yokoyama, Ryuji Ukai, Seiji C Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Jun-ichi Yoshikawa, Hidehiro Yonezawa, Nicolas C Menicucci, and Akira Furusawa. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nature Photonics*, 7(12):982, 2013. doi:10.1038/nphoton.2013.287.

A Proof techniques

This section details the primary mathematical tools used in the proofs of the theorems, along with some intuition. The full technical proofs can be found in [6].

The function $z \mapsto f_A(z, \eta)$ defined in Eq. (3) for $\eta > 0$ is a bounded approximation of the Glauber-Sudarshan function P_A of the operator A. This approximation is parametrised by a precision η, and a cutoff value E. The optical equivalence theorem for antinormal ordering [5] reads

$$\mathrm{Tr}(A\rho) = \int Q_\rho(\alpha) P_A(\alpha) d^2\alpha. \tag{25}$$

Given that

$$\mathop{\mathbb{E}}_{\alpha \leftarrow Q_\rho}[f_A(\alpha, \eta)] = \int Q_\rho(\alpha) f_A(\alpha, \eta) d^2\alpha, \tag{26}$$

we can expect that $\mathop{\mathbb{E}}_{\alpha \leftarrow Q_\rho}[f_A(\alpha, \eta)]$ is an approximation of $\mathrm{Tr}(A\rho)$ parametrised by η and E. Theorem 1 formalises this statement.

The proof of Theorem 3 combines Theorem 1 with Hoeffding inequality [15], which quantifies the speed of convergence of the sample mean towards the expected value of a bounded i.i.d. random variable:

▶ **Lemma 6** (Hoeffding). *Let $\lambda > 0$, let $n \geq 1$, let $z_1, \ldots, z_n$ be i.i.d. complex random variables from a probability density D over $\mathbb{R}$, and let $f : \mathbb{C} \mapsto \mathbb{R}$ such that $|f(z)| \leq M$, for $M > 0$ and all $z \in \mathbb{C}$. Then*

$$\Pr\left[\left|\frac{1}{n}\sum_{i=1}^{n} f(z_i) - \mathop{\mathbb{E}}_{z \leftarrow D}[f(z)]\right| \geq \lambda\right] \leq 2\exp\left[-\frac{n\lambda^2}{2M^2}\right]. \tag{27}$$

The proof then follows by applying this inequality for $D = Q_\rho$, and $f = f_{|k\rangle\langle l|}$, for all values of k, l between 0 and E, together with the union bound.

Theorem 4 removes the bounded support assumption and its proof is similar to the one of Theorem 3, with the addition of a support estimation step, using samples from heterodyne detection. The main result utilised here is the fact that for all E [16]

$$1 - \Pi_{\leq E} = \sum_{n=E+1}^{+\infty} |n\rangle\langle n| \leq \frac{2}{\pi} \int_{|\alpha|^2 \geq E} |\alpha\rangle\langle\alpha| \, d^2\alpha, \tag{28}$$

where $\Pi_{\leq E}$ is the projector onto the space of states of support bounded by E. This result allows to bound the probability of having a large support and obtaining a low score at the support estimation step.

The proof of Theorem 5 is the most technical. This proof combines three main ingredients: a support estimation step for permutation-invariant states using samples from heterodyne detection, the de Finetti reduction from [24] and a refined version of Hoeffding inequality for superpositions of almost-i.i.d. states under a product measurement. The three terms appearing in the expression of the probability in the theorem correspond to these three ingredients, respectively.