Efficient verification of continuous-variable quantum states & devices without assuming independent and identical operations

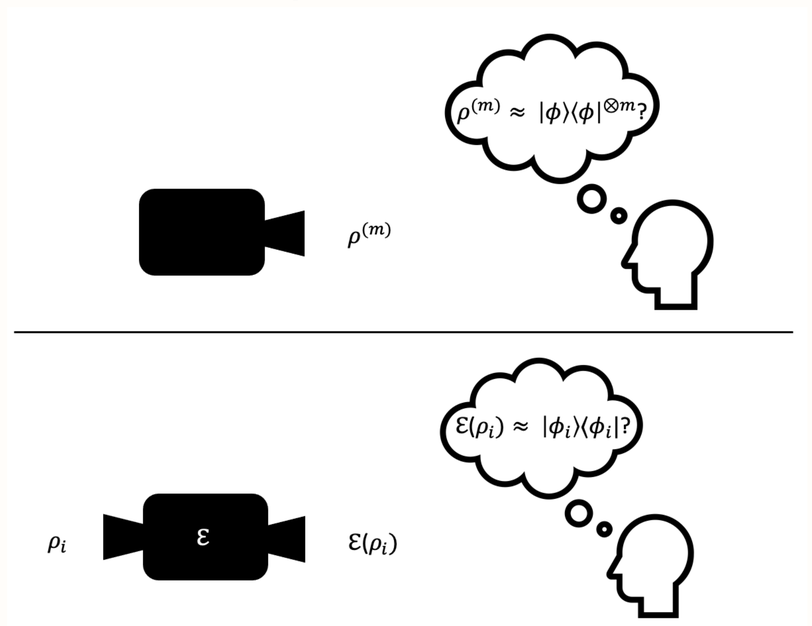
Ya-Dong Wu[1], Ge Bai[1], Giulio Chiribella[1], Nana Liu[2]

[1]Department of Computer Science, The University of Hong Kong

[2]Institute of Natural Sciences, Shanghai Jiao Tong University

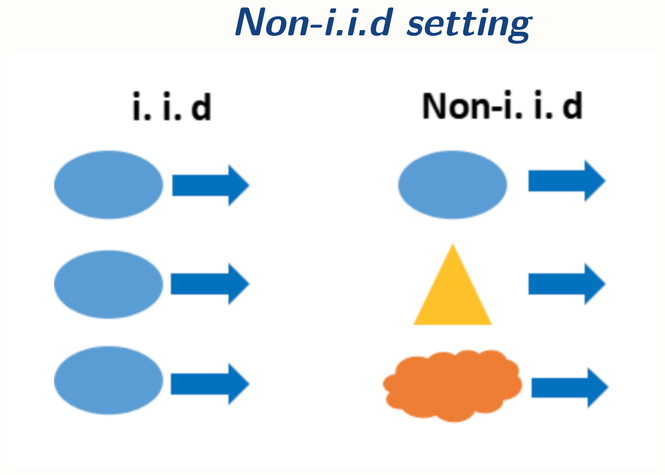
Introduction

Verification of quantum states & devices



One of the crucial problems in quantum technologies is verifying whether or not a correct quantum state or quantum device has been realized, to be used either for quantum computation, sensing or communication. State verification [2] addresses the problem of whether or not a state generated by a quantum device is close enough to a specified target state. Quantum device verification [3] is the problem of determining whether the outputs of a quantum device is close to associated target output states, averaged over all possible input states.

Non-i.i.d setting



Multiple copies of the quantum system are required to gather a sufficient number of measurement results to enable verification. This multiple measurement process of many identical copies of the quantum state or device is called the i.i.d (independent and identical) scenario and most quantum verification protocols are built upon this assumption.

However, we know that the i.i.d assumption do not hold in many realistic scenarios. For instance, there may be time-dependent noise in a quantum device, which can exhibit correlations between subsequent uses of the same device. In the context of quantum technologies in future quantum networks, we need to consider the role of adversaries, who have the power of disturbing the states and devices prior to verification. We cannot trust that the adversaries will necessarily allow us access to multiple copies of the same state, or to multiple uses of the same quantum device.

Background & framework

Continuous-variable (CV) quantum information

A CV state lies on an infinite dimensional Hilbert space, equipped with observables with a continuous spectrum, such as the position and momentum observables of a quantum particle. CV states are usually implemented by bosonic systems, described by quantum harmonic oscillators. CV quantum information is encoded in tensor product $\mathcal{H}^{\otimes k}$ of Hilbert space $\mathcal{H} = \mathrm{Span}\{|n\rangle\}_{n\in\mathbb{N}}$, where $\hat{n}|n\rangle = n|n\rangle$ is a particle number eigenstate with particle number operator $\hat{n} = \hat{a}^\dagger\hat{a}$.

Reliable state verification

In state verification, a verifier has to test the preparation of a target state, denoted by $|\phi\rangle \in \mathcal{H}^{\otimes k}$, where $k \in \mathbb{N}^+$. The verifier is given n quantum registers, whose state is claimed to consist of n identical copies of the target state. The actual state of the n registers is unknown to the verifier, and is denoted by $\rho^{(n)} \in \mathcal{S}(\mathcal{H}^{\otimes k\cdot n})$. The verifier then chooses $n - m$ quantum registers uniformly at random, and performs measurements on each register, to decide whether the reduced state at the remaining m registers is close enough to $|\phi\rangle\langle\phi|^{\otimes m}$ or not.

Denote T as the POVM element on $\mathcal{H}^{\otimes k(n-m)}$ that corresponds to the verification test flagged as passed, and $0 < \epsilon < \frac{1}{2}$ as failure probability. A reliable quantum state verification scheme must satisfy

Completeness

$$\mathrm{tr}\left[T|\phi\rangle\langle\phi|^{\otimes(n-m)}\right] \geq 1-\epsilon.$$

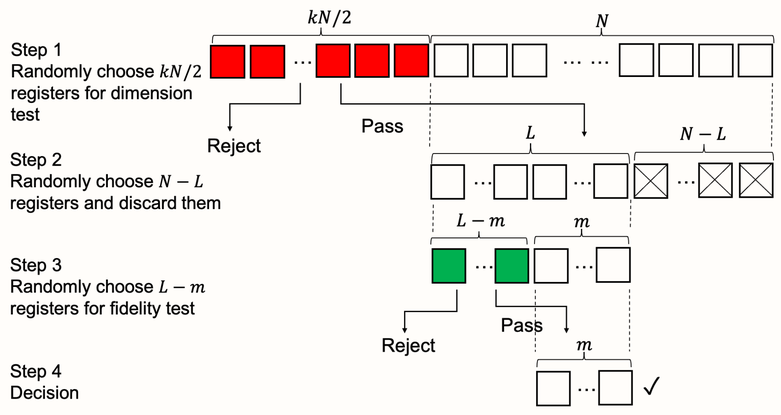
Soundness

For any permutation-invariant $\rho \in \mathcal{S}(\mathcal{H}^{\otimes kn})$,

$$\mathrm{tr}\left[T \otimes (1-|\phi\rangle\langle\phi|^{\otimes m})\rho\right] \leq \epsilon.$$

Results

State verification protocol



In general non-i.i.d settings, CV quantum state verification comprises of two subprotocols: the dimension test and the fidelity test. The dimension test [4] is used to bound the dimension d. In the dimension test, the measurement outcomes of homodyne detection are compared with a certain threshold. If the measurement outcomes are always less than the threshold, this gives a strong guarantee that each subsystem is confined in a subspace spanned by Fock states $|n\rangle$ with n less than d. Through discarding a large fraction of the subsystems of the randomized non-i.i.d state, one can treat the state at the remaining subsystems as approximately i.i.d, due to a finite-d de Finetti theorem [5]. After getting an i.i.d approximation, the fidelity test, similar to the test under i.i.d assumption, is to certify the fidelity between the state at each remaining subsystem and the target state, by detecting the fidelity witness [6] at partial subsystems. The above figure summarises the key steps of the scheme. This scheme works for verification of multi-mode entangled Gaussian states and non-Gaussian CV hypergraph states.

Sample complexity

The sample complexity of the above verification scheme, to satisfy both completeness and soundness, is

$$(k/2+1)N = O\left(\frac{k^7m^4}{\epsilon^6}\mathrm{Poly}\left(\ln\frac{km}{\epsilon}\right)\right). \qquad (1)$$

Compared to the sample complexity $L = O\left(\frac{k^2m^2}{\epsilon^2}\mathrm{Poly}\left(\ln\frac{km}{\epsilon}\right)\right)$ in the i.i.d case, at most L^4 samples are sufficient for CV-state verification in non-i.i.d scenario.

Device verification

These same state verification techniques can also be used to implement the verification of quantum devices. We begin with the observation that any test of quantum devices can be realized by preparing one entangled state on the input and an ancillary system, and then jointly measuring the output and the ancillary system [7]. The observable to be measured can then be chosen to be (average) fidelity witness as in a state verification task. By adding a dimension test and rotational symmetry in the fidelity test, we get our quantum-device verification schemes. Verification protocols of amplification, attenuation, and purification of noisy coherent states can be found in the supplemental material.

Conclusions

We have proposed the first protocols that can verify both multimode CV entangled states and CV quantum devices without the assumption of i.i.d state and device operations. Through bypassing the i.i.d assumption for multimode states, our results can be applied to CV blind quantum computing [8], where a potentially malicious server may deceive an agent or steer the computational results by preparing entangled states. Our results can also be applied to performance benchmarks of quantum devices [9], in a broader setting where the devices may undergo arbitrary correlated noise processes in subsequent uses, and may contain an internal memory that affects their behavior on later inputs.

References

[1] Wu, Bai, Chiribella, & Liu, PRL **126**, 240503 (2021)

[2] Pallister, Linden, & Montanaro, PRL **120**, 170502 (2018); Takeuchi, & Morimae, PRX **8**, 021060(2018); Zhu, & Hayashi, PRL **123**, 260504 (2019); Takeuchi, Mantri, Morimae, Mizutani, & Fitzsimons, npjQI **5**, 1 (2019); Chabaud, Douce, Grosshans, Kashefi, & Markham, TQC 2020

[3] Wu, & Sanders, NJP **21**, 073026 (2019); Farias, & Aolita QST **6**, 035014 (2021)

[4] Renner & Cirac, PRL **102**, 110504 (2009). Leverrier, García-Patrón, Renner, & Cerf, PRL **110**, 030502 (2013).

[5] Christandl, Konig, Mitchison & Renner, CMP **273**, 473 (2007)

[6] Aolita, Gogolin, Kliesch, & Eisert, NC **6**, 1 (2015); Gluza, Kliesch, Eisert & Aolita PRL **120**, 190501 (2018)

[7] Bai & Chiribella, PRL **120**, 150502 (2018).

[8] Morimae, PRL **109**, 230502 (2012); Liu, Demarie, Tan, Aolita, & Fitzsimons, PRA **100**, 062309 (2019)

[9] Chiribella, & Xie, PRL **110**, 213602 (2013); Yang, Chiribella, & Adesso, PRA **90**, 042319 (2014)

QCrypt, 23-27 August 2021