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

Ya-Dong Wu,[1] Ge Bai,[1] Giulio Chiribella,[1,2,3,4] and Nana Liu[5,6,7]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *The University of Hong Kong Shenzhen Institute of Research and Innovation, 5/F, Key Laboratory Platform Building, No.6, Yuexing 2nd Rd., Nanshan, Shenzhen 518057, China*
[3] *Department of Computer Science, Parks Road, Oxford, OX1 3QD, UK*
[4] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[5] *Institute of Natural Sciences, Shanghai Jiao Tong University, Shanghai 200240, China*
[6] *Ministry of Education, Key Laboratory in Scientific and Engineering Computing, Shanghai Jiao Tong University, Shanghai 200240, China*
[7] *University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai 200240, China*

Continuous-variable (CV) quantum information, encoded in an infinite-dimensional Hilbert space, is widely used in many quantum information protocols [1, 2]. To demonstrate quantum advantage in these protocols, certification of realistic implementations of quantum states and quantum devices is an essential step [3]. However, in realistic scenarios, we cannot guarantee identical and independent (i.i.d) state and device preparation. Important examples include adversarial scenarios, where one cannot trust if one is given the same state or device in each subsequent run. For instance, in verifiable blind quantum computing [4], the potential existence of a malicious server sending arbitrary entangled states to steer computational results makes state verification in adversarial scenarios important. Also, in the presence of time-dependent noise, correlated noise can be created between subsequent uses of quantum devices, so one cannot trust that a realistic quantum device outputs identical and independent states in each run. In this paper, we propose verification protocols for CV entangled states and CV quantum devices in these non-i.i.d scenarios.

State verification [5–13] addresses the problem of whether or not a state generated by a quantum device is close enough to a specified target pure state. Most proposed methods work well and efficiently when states have i.i.d preparation [5, 6, 8]. In the non-i.i.d setting, one powerful method is to employ the quantum de Finetti theorem [14], which enables us to approximate a collection of non-i.i.d states with a smaller set of i.i.d states after a randomising procedure followed by tracing out some subsystems [7, 12, 13]. This then allows us to use known verification methods on those i.i.d states. In the CV setting, there are two main classes of quantum de Finetti theorems and they are separated into the infinite dimension $d \to \infty$ setting [15] relying on rotational randomization on multimode phase space, and the finite d case [16, 17] relying only on permutation randomization. However, in the $d \to \infty$ case, the rotational randomising procedure to enable the state after randomization to be approximated by an i.i.d state is not easily implementable. To enable the use of a finite d de Finetti theorem in the CV setting, which is infinite dimensional, one must filter those CV states, which are close to finite d states, using CV measurements and such tests have been shown to work for single-mode CV states [12] and certain photonic states [13]. However, for this method, the approximation error between the permutation randomised state and an almost i.i.d state scales exponentially with d [16, 17], implying that this method is not preferable for the multimode setting. In our approach, we propose an alternative test utilizing the finite d de Finetti theorem [14], which relies not only on permutation randomization, but also rotational randomization at each single-mode phase space. This rotational randomization at each mode, unlike multimode rotational randomization, is easily implemented by random choices of quadrature basis for homodyne detections. This test allows us to have a quadratic scaling of the approximation error between the state after randomization and an i.i.d state with respect to d, preferable for verification of multimode entangled CV states, which are crucial for many quantum protocols to provide a quantum advantage.

For a verification test to be reliable, we also need to ensure that the completeness and soundness of the protocol is good enough. Completeness refers to a high probability that the correct state is flagged as correct by our protocol and soundness is a low probability of a false positive. Our new technique allows us to guarantee both the completeness and soundness of our protocol. We also extend our state verification protocol to CV non-i.i.d quantum-device verification using the fact that any test on a quantum channel can be done via preparing an entangled input state and applying tests at both the output and the ancillary system [18]. Quantum device verification [19] 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.

Our CV quantum state and device verification schemes comprise of a dimension test and a fidelity test. The dimension test is to filter the CV states so that we can apply the finite d quantum de Finetti theorem. The fidelity test is the verification protocol used on the resulting approximated i.i.d state. Our verification scheme can be used to verify any multimode Gaussian pure states and one particular type of non-Gaussian states: CV hypergraph states [11, 20]. The sample complexity of this verification scheme is $O\left(\frac{k^7m^4}{\epsilon^6}\text{Poly}\left(\ln\frac{km}{\epsilon}\right)\right)$, where k is the number of modes, m is the number of copies we want of the target state, and ϵ is a maximal error probability. Compared to the sample complexity $O\left(\frac{k^2m^2}{\epsilon^2}\text{Poly}\left(\ln\frac{km}{\epsilon}\right)\right)$ in i.i.d scenario, we see that a polynomial increase in k, m and ϵ are required to relax the i.i.d assumption. Similar results hold for device verification.

[1] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. , 1 (2020).
[4] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Syst. **63**, 715 (2019).
[5] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Nat. Commun. **6**, 1 (2015).
[6] S. Pallister, N. Linden, and A. Montanaro, Phys. Rev. Lett. **120**, 170502 (2018).
[7] Y. Takeuchi and T. Morimae, Phys. Rev. X **8**, 021060 (2018).
[8] N. Liu, T. F. Demarie, S.-H. Tan, L. Aolita, and J. F. Fitzsimons, Phys. Rev. A **100**, 062309 (2019).
[9] H. Zhu and M. Hayashi, Phys. Rev. Lett. **123**, 260504 (2019).
[10] H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).
[11] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, npj Quantum Inf. **5**, 1 (2019).
[12] U. Chabaud, T. Douce, F. Grosshans, E. Kashefi, and D. Markham, in *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 158, edited by S. T. Flammia (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020) pp. 3:1–3:15.
[13] U. Chabaud, F. Grosshans, E. Kashefi, and D. Markham, arXiv preprint arXiv:2006.03520 (2020).
[14] M. Christandl, R. König, G. Mitchison, and R. Renner, Comm. Math. Phys. **273**, 473 (2007).
[15] A. Leverrier, Journal of Mathematical Physics **59**, 042202 (2018).
[16] R. Renner and J. I. Cirac, arXiv preprint arXiv:0809.2243 (2008).
[17] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[18] G. Bai and G. Chiribella, Phys. Rev. Lett. **120**, 150502 (2018).
[19] Y.-D. Wu and B. C. Sanders, New J. Phys. **21**, 073026 (2019).
[20] D. W. Moore, Phys. Rev. A **100**, 062301 (2019).