Extended Abstract for: "Efficient Characterization of Multi-Qubit States and their Application to Demonstrate Measurement Only Blind Quantum Computing"

Chiara Greganti[1], Marie-Christine Roehsner[1], Stefanie Barz[1,2],
Tomoyuki Morimae[3], Mordecai Waegell[4], Philip Walther[1]
[1] *University of Vienna, Faculty of Physics, Austria,* [2] *Present address: University of Oxford, Clarendon Laboratory, UK,* [3] *ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan,*
[3] *Institute for Quantum Studies, Chapman University, Orange, CA, US*

Multi-qubit states are a basic resource for present and future generations of quantum information science experiments. In particular, N-qubit stabilizer (or graph) states have well-proved utility for one-way quantum computation and quantum information processing [1–4]. As the number of particles increases, the system and its properties become significantly more complex. In order to manipulate and exploit such entangled systems, it is crucial to certify the generated states with respect to the ideal stabilizer states.

This problem is approached using a new method based on Identity Products (IDs) [5, 6] scaling linearly with the number of qubits, that can be used to efficiently characterize important properties of multi-qubit stabilizer states. The method is compared to other common methods for estimating quantum state fidelity for an N-qubit state. These methods are based on quantum state tomography [7] (QST - requires 3^N measurement settings), the stabilizer group [8, 9] (SG - requires 2^N measurement settings), the generators of the stabilizer group [10, 11] (GoSG - requires N measurement settings) and a witness [12](Wit - requires $N+1$ measurement settings). A comparison of results is shown in Figure 1.

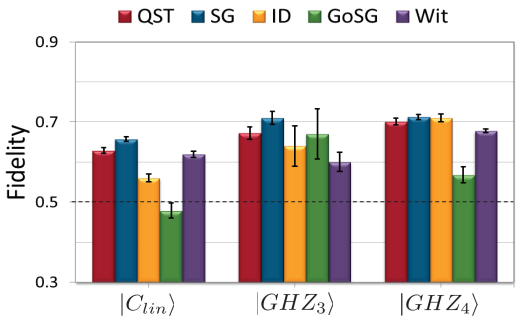

Figure 1: Comparison of fidelities obtained with different methods for a four-qubit linear cluster state, a four-qubit GHZ state, and a three-qubit GHZ state. The methods of QST (red/first bar) and SG (blue/second bar) scale exponentially, while our ID method (yellow/third bar), the GoSG (green/fourth bar), and Wit (purple/fifth bar) approaches scale linearly with the number of qubits. Within the error bars the IDs set lower bounds, in agreement with the QST results. The SG fidelities tend to overestimate the QST ones. The GoSG and Wit bounds, like the IDs, are consistent with the rest of the methods. Note that $F_{GoSG} < 0.5$ for the four-qubit linear cluster, so it is not sufficient to certify that the state can violate a Bell-type inequality. The error bars derive from Poissonian statistics and thus correspond to a lower limit.

Another challenge and a possible application for the characterized states is the protection of data privacy in quantum computing. Even today complex computations are often delegated to distant providers, which is known as cloud computing. Should powerful quantum computers be available in such manner Alice, a (quasi-classical) client, might want to use the quantum resources of Bob, the operator of a powerful quantum computer, even though she does not trust him. Blind quantum computing (BQC) first introduced in 2009 [13] allows Alice to delegate her computation to Bob without leaking any of her information to him. Additionally, even without a quantum computer on her side, she can verify if Bob is honest and provides her with the correct results or resources for her computation [14, 15]. A new protocol was proposed by Morimae [16] which increases the security and simplifies the BQC for Alice as it only requires her to perform single qubit measurements. It is therefore referred to as "measurement only blind quantum computation" (MBQC). Bob generates a resource state, and sends the corresponding qubits, one by one, through a one-way quantum channel to Alice. She measures each qubit according to her program. For any kind of a malicious Bob, he cannot learn anything about Alice's quantum computation, because information is sent only in one direction. The no-signaling principle then ensures that if Alice and Bob share a system (classical or quantum) and she measures her part, this does not transmit any information to Bob. Moreover, the concept of secure quantum computing has opened-up feasible verification methods [14, 15, 17]. This means that Alice can test whether Bob is performing the computation correctly even though her resources are limited. We practically realize a proof-of-principle implementation of the protocol using photons, computing two-qubit entangling gates and verifying two single trap qubits.The four-qubit resource for measurement-only BQC, is produced in Bobs laboratory via a photonic set-up in a so-called railway-crossing configuration. A double spontaneous parametric down

conversion process allows to generate two pairs of polarization entangled photons. Interferometers with polarizing beam splitters entangle the four photons. Additional half-wave plates on both pairs directions enable the generation of a four-qubit linear cluster state as well as a four-qubit star cluster state.

The four-qubit linear cluster allows verifying computation with only two different trap measurements and is especially suited for the verification protocol. The results for this state are presented in Figure 2.

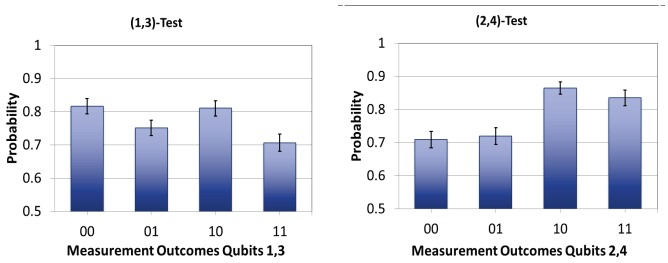

Figure 2: Probability that Alice receives the expected outcomes for the two possible tests she can perform, the (1,3)-test and (2,4)-test on a linear cluster state. According to the measurement outcomes of the non-trap qubits (shown on the abscissa) we report the probability that measurements on each of Alice's trap qubits return the expected result (i.e. Alice trusts the state Bob sent).

More detailed information can be found at `http://arxiv.org/abs/1601.02451` [18] and `http://arxiv.org/abs/1502.06549` [19].

[1] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, Caltech, 1997.

[2] R. Raussendorf and H.J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001.

[3] F. Verstraete and J. I. Cirac. Valence-bond states for quantum computation. *Phys. Rev. A*, 70:060302, Dec 2004.

[4] H.-J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Phys.*, 5(1):19–26, 2009.

[5] M. Waegell and P. K. Aravind. Proofs of the kochen-specker theorem based on a system of three qubits. *Journal of Physics A: Mathematical and Theoretical*, 45(40):405301, 2012.

[6] M. Waegell. *Nonclassical Structures within the N-qubit Pauli Group.* PhD thesis, Worcester Polytechnic Institute, 2013.

[7] D.F.V. James, P.G. Kwiat, W.J. Munro, and A.G. White. Measurement of qubits. *Phys. Rev. A*, 64(5):52312, 2001.

[8] G. Tóth and O. Gühne. Entanglement detection in the stabilizer formalism. *Phys. Rev. A*, 72:022340, Aug 2005.

[9] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter. Experimental analysis of a four-qubit photon cluster state. *Phys. Rev. Lett.*, 95:210502, 2005.

[10] H. Wunderlich and M. B. Plenio. Quantitative verification of entanglement and fidelities from incomplete measurement data. *Journal of Modern Optics*, 56(18-19):2100–2105, 2009.

[11] H. Wunderlich, G. Vallone, P. Mataloni, and M. B. Plenio. Optimal verification of entanglement in a photonic cluster state experiment. *New Journal of Physics*, 13(3):033033, 2011.

[12] Yuuki Tokunaga, Takashi Yamamoto, Masato Koashi, and Nobuyuki Imoto. Fidelity estimation and entanglement verification for experimentally produced four-qubit cluster states. *Phys. Rev. A*, 74:020301, Aug 2006.

[13] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science*, pages 517–526, 2009.

[14] J.F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind computation. *arXiv:1203.5217*, 2012.

[15] T. Morimae. Verification for measurement-only blind quantum computing. *Phys. Rev. A*, 89:060302, Jun 2014.

[16] T. Morimae and K. Fujii. Blind quantum computation protocol in which alice only makes measurements. *Phys. Rev. A*, 87(5):050301, 2013.

[17] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther. Experimental verification of quantum computation. *Nature Physics*, 9:727–731, 2013.

[18] Chiara Greganti, Marie-Christine Roehsner, Stefanie Barz, Mordecai Waegell, and Philip Walther. Practical and efficient experimental characterization of multiqubit stabilizer states. *Phys. Rev. A*, 91:022325, Feb 2015.

[19] Chiara Greganti, Marie-Christine Roehsner, Stefanie Barz, Tomoyuki Morimae, and Philip Walther. Demonstration of measurement-only blind quantum computing. *New Journal of Physics*, 18(1):013020, 2016.