Rigidity of quantum steering and one-sided device-independent verifiable quantum computation

Alexandru Gheorghiu
University of Edinburgh
School of Informatics
Edinburgh, UK
a.gheorghiu@sms.ed.ac.uk

Petros Wallden
University of Edinburgh
School of Informatics
Edinburgh, UK
petros.wallden@ed.ac.uk

Elham Kashefi
University of Edinburgh
School of Informatics
Edinburgh, UK
ekashefi@staffmail.ed.ac.uk

The relationship between correlations and entanglement has played a major role in understanding quantum theory since the work of Einstein, Podolsky and Rosen [3]. Tsirelson proved that Bell states, shared among two parties, when measured suitably achieve the maximum non-local correlations allowed by quantum mechanics [2]. Reichardt, Unger and Vazirani proved the converse [14], which was named *rigidity* of non-local correlations. They showed that observing the maximal non-local correlation value over a sequence of repeated measurements, implies that the underlying quantum state is close to a tensor product of maximally entangled states and, moreover, that it is measured according to an ideal strategy. However, this strong rigidity result comes at a high price, it requires a large overhead in the number of entangled pairs and measurements. In this paper we prove an analogous rigidity result for quantum steering correlations, having smaller overhead. Steering correlations, formally introduced by Schrödinger [15], emerge from the observation that (untrusted) measurements performed on one half of a bipartite entangled state steer the state of the other (trusted) half. A reason for the recent increased interest in steering correlations stems from the practical limitations of protocols which exploit non-locality (device-independent protocols). In fact, practical protocols based on steering correlations have been proposed for quantum key-distribution (QKD) and quantum random number generation (QRNG) [1, 12]. In the same spirit, as an application of our rigidity result, we give a one-sided device independent protocol for verified delegated quantum computation (VDQC).

Recent progress in quantum technologies makes very pressing the issue of verifying the correctness of quantum devices using classical or minimum-quantum abilities. Verification via classical simulation does not seem feasible, as quantum computation is believed to outperform classical computation and so one should resort to techniques such as those of VDQC protocols. It is therefore clear that constructing VDQC protocols with minimal trust assumptions and increased efficiency is crucial. We achieve this, using steering correlations and, in particular, the rigidity result we prove in the first part. Verification appears as the most natural application of this rigidity result. The reason for this is the necessity, when certifying a quantum computation, to characterise the states, operators and Hilbert space used throughout the protocol which is precisely what our rigidity result achieves. This is in contrast to QKD and QRNG where it suffices to bound certain information theoretic quantities such as entropy, mutual information or key-rate from observed correlations.

We prove the rigidity of quantum steering correlations in three steps. First, using maximal steering correlations we obtain robust self-testing of a Bell state. This is done in a manner similar to the work of [10] with the difference that one side (Alice) is trusted and for this reason we use steering rather than Bell inequalities. As in [10] and other works on self-testing [11, 17], we make an independence assumption, i.e. Alice and Bob use the same (unknown) state $|\psi\rangle$ for every set of measurements. We show that if the correlations of their measurement outcomes are saturated up to order $O(\varepsilon)$, the shared state $|\psi\rangle$ is

Submitted to:
QPL 2016

$O(\sqrt{\varepsilon})$-close to a perfect Bell state, under a local isometry. Additionally, we prove that this closeness bound is optimal.

The second step is to remove the independence assumption used in the first part. To do this, we model the measurement process as a martingale and use the Azuma-Hoeffding inequality to get an estimate of the true quantum correlation (of Alice and Bob's observables) from the observed correlations. By combining this with the self-testing result and an optimization argument it follows that a randomly chosen reduced state of Alice and Bob is close to an ideal Bell pair. An important observation is that the technique used is general enough and can therefore be applied to the self-testing results of the fully untrusted setting (device-independent) thus complementing the works of [11, 10, 17].

The third and last step is to extend this result to obtain a tensor product of multiple Bell pairs. It is in this step that trusting one side leads to fewer requirements and makes the rigidity of steering more efficient than the non-local case. To prove the result, we follow a game-based approach, similar to [14, 13]. We define a steering game akin to the CHSH game. Rigidity then follows by showing that if Alice and Bob play according to a strategy that wins in most games, then this strategy is equivalent (up to a local isometry) to the ideal strategy in which Alice and Bob share a tensor product of Bell pairs and perform the ideal measurements.

Finally, we use the rigidity result to create a one-sided device-independent VDQC protocol. This protocol is similar to existing device-independent protocols such as [13, 5, 7]. It consists of a verifier with a trusted single-qubit measurement device, and an untrusted quantum server that can perform universal quantum computations. The verifier will delegate a quantum computation to the server and check its correctness. This is done in two steps:

1. *Verified state preparation* - The server is instructed to prepare Bell states and send one half of each pair to the verifier. By measuring these states and using the rigidity result, the verifier can certify the correct preparation of single qubit states on the server's side.

2. *Verified computation* - We use a version of the protocol of Fitzsimons and Kashefi [4] to verify a computation performed by the server using the qubits prepared in the previous step. Specifically the version we use can be either the one described in [9] or the one in [8]. These ensure optimal communication complexity.

Because of the added trust and use of steering correlations, the protocol has a greatly reduced overhead compared to the existing fully device-independent VDQC protocols, making their actual implementation much more likely.

Our last contribution is to characterise the types of entangled states which are useful for the specific class of VDQC protocols that we considered. We show that these protocols essentially require the use of maximally entangled states. This highlights the necessity of our rigidity result for the verification of quantum computations.

Our full paper can be found here [6]. We acknowledge that an independent work [16], also addressing self-testing from steering correlations, appeared on the arxiv shortly after our paper.

References

[1] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani & Howard M. Wiseman (2012): *One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering*. *Phys. Rev. A* 85, p. 010301, doi:10.1103/PhysRevA.85.010301. Available at `http://link.aps.org/doi/10.1103/PhysRevA.85.010301`.

[2] B.S. Cirel'son (1980): *Quantum generalizations of Bell's inequality*. Letters in Mathematical Physics 4(2), pp. 93–100, doi:10.1007/BF00417500. Available at http://dx.doi.org/10.1007/BF00417500.

[3] A. Einstein, B. Podolsky & N. Rosen (1935): *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. 47, pp. 777–780, doi:10.1103/PhysRev.47.777. Available at http://link.aps.org/doi/10.1103/PhysRev.47.777.

[4] Joseph F. Fitzsimons & Elham Kashefi (2012): *Unconditionally verifiable blind computation*. Eprint:arXiv:1203.5217.

[5] Alexandru Gheorghiu, Elham Kashefi & Petros Wallden (2015): *Robustness and device independence of verifiable blind quantum computing*. New Journal of Physics 17(8), p. 083040. Available at http://stacks.iop.org/1367-2630/17/i=8/a=083040.

[6] Alexandru Gheorghiu, Petros Wallden & Elham Kashefi (2015): *Rigidity of quantum steering and one-sided device-independent verifiable quantum computation*. Eprint:arXiv:1512.07401.

[7] Michal Hajdušek, Carlos A. Pérez-Delgado & Joseph F. Fitzsimons (2015): *Device-Independent Verifiable Blind Quantum Computation*. Eprint:arXiv:1502.02563.

[8] Theodoros Kapourniotis, Vedran Dunjko & Elham Kashefi (2015): *On optimising quantum communication in verifiable quantum computing*. Eprint:arXiv:1506.06943.

[9] Elham Kashefi & Petros Wallden (2015): *Optimised resource construction for verifiable quantum computation*. Eprint:arXiv:1510.07408.

[10] M McKague, T H Yang & V Scarani (2012): *Robust self-testing of the singlet*. Journal of Physics A: Mathematical and Theoretical 45(45), p. 455304. Available at http://stacks.iop.org/1751-8121/45/i=45/a=455304.

[11] Matthew McKague (2013): *Interactive proofs for BQP via self-tested graph states*. Eprint:arXiv:1309.5675.

[12] Elsa Passaro, Daniel Cavalcanti, Paul Skrzypczyk & Antonio Acn (2015): *Optimal randomness certification in the quantum steering and prepare-and-measure scenarios*. New Journal of Physics 17(11), p. 113010. Available at http://stacks.iop.org/1367-2630/17/i=11/a=113010.

[13] Ben W. Reichardt, Falk Unger & Umesh Vazirani (2012): *A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games*. Eprint:arXiv:1209.0448.

[14] Ben W. Reichardt, Reichardt Falk Unger & Umesh Vazirani (2013): *Classical command of quantum systems*. Nature 496, pp. 456–460.

[15] E. Schrödinger (1936): *Probability relations between separated systems*. Mathematical Proceedings of the Cambridge Philosophical Society 32, pp. 446–452, doi:10.1017/S0305004100019137. Available at http://journals.cambridge.org/article_S0305004100019137.

[16] Ivan Šupić & Matty J Hoban (2016): *Self-testing through EPR-steering*. arXiv preprint arXiv:1601.01552.

[17] Tzyh Haur Yang & Miguel Navascués (2013): *Robust self-testing of unknown quantum systems into any entangled two-qubit states*. Phys. Rev. A 87, p. 050102, doi:10.1103/PhysRevA.87.050102. Available at http://link.aps.org/doi/10.1103/PhysRevA.87.050102.