Experimental Quantum Advantage for NP Verification [1]

Federico Centrone[1,2], Niraj Kumar[3], Eleni Diamanti[2], and Iordanis Kerenidis[1]

[1] *Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France.*
[2] *Université de Paris, CNRS, IRIF, 8 Place Aurélie Nemours, 75013 Paris, France.*
[3] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK.*

Abstract. We show the first experimental demonstration of a computational quantum advantage with linear optics, by studying the computational task of the verification of an NP-complete problem by a verifier who only gets limited information about the proof. We provide a simple linear optical implementation that can perform this task efficiently, while we also provide strong evidence that a classical computer would take time greater than the age of the universe. The verification of NP-complete problems with limited informationbrings us a step closer to real-world useful applications, such as server-client quantum computing.

Keywords: Quantum advantage, Photonics, Verification

Quantum Advantage is the quest for an evidence of a quantum device outperforming the best existing classical computer in time resources for some specific computational task. Such a long-standing goal in the field of Quantum Information was recently attained, as revealed in an article produced by a scientific collaboration of NASA and Google, showing the performance of their 53 qubits superconducting quantum processor in sampling randoms quantum circuits [2]. This first experimental proof of such advantage, although its practical applications may be limited, represents a milestone for the research in this area.

However, it might not always be necessary to step on cutting-edge quantum technologies inorder to accomplish a task classically unachievable and with an appealing set of handy employments. Recently, we could observe experimental evidence for a quantum advantage in the verification of NP-complete problems through the implementation of a Quantum Merlin Arthur (QMA) instance in arather simple optical setup. QMA is a Quantum Interactive Proof system in which a computationallyunbounded untrusted *prover*, Merlin, wants to convince the *verifier*, Arthur, that he can solve a given satisfiability problem, by sending him *unentangled* quantum proofs [3]. If in the classical case Arthur receives only K bits out of N of the complete solution, he would need exponential time in the number of N−K missing bits to verify the problem, whereas our quantum protocol takes linear time in the input size N. Hence, even though the information received by the verifier is bounded, if a solution exists, he would accept the proof in polynomial time with high probability (completeness) and otherwise he would reject, still in polynomial time and with high probability (soundness).

In order to render this computational task realizable with current technology, we had to greatly simplify our theoretical verification protocol of [4], since that one was inherently not realisable due to the number of quantum devices needed (in the thousands). On the other hand, our experimental implementation [1] highlights the power of linear optics, and in particular of coherent state mappings, for computational tasks. By encoding the information in weak coherent pulses and allowing Merlin's quantum proofs to live in an infinite dimensional Hilbert space, we could generalize this complexity class to a regime that was never explored before. The power of the theoretical simplification in this work allowed for an experimental implementation that requires only a standard laser source, a handful of passive optical elements independent of the input size of the problem and single photon detectors, thus technologies available in almost any optical laboratory.

While previous proposals for quantum supremacy experiments are still based on non-standard computational assumptions, we use the most standard and widely accepted computational assumption, the fact that classical computers take exponential time to solve NP complete problems. As aconsequence, we estimate that this task, taking into account the experimental imperfections, can verify a NP-complete problem of arbitrary input size with high probability of success in a fraction ofa second, whereas the classical analog to achieve the same level of confidence with the same amountof information would take a time that exceeds the age of the Universe even employing the most advanced state-of-the-art classical technology.

Link to the pre-print: https://arxiv.org/abs/2007.15876

References

[1] Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis. Experimental demonstration of quantum advantage for np verification.arXiv preprint arXiv:2007.15876, 2020.
[2] F. Arute, K. Arya, R. Babbush, and et al. Quantum supremacy using a programmable superconducting processor.Nature, 574:505–510, 2019.
[3] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. In2008 23rd Annual IEEE Conference on Computational Complexity, pages 223–236. IEEE, 2008.
[4] Juan Miguel Arrazola, Eleni Diamanti, and Iordanis Kerenidis. Quantum superiority for verifying np-complete problems with linear optics. npj Quantum Information, 4(1):1–8, 2018