Quantum superiority for verifying NP-complete problems with coherent states and linear optics

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

[1]*LIP6, CNRS, Université Pierre et Marie Curie, Sorbonne Universités, 75005 Paris, France*
[2]*IRIF, CNRS, Université Paris Diderot, Sorbonne Paris Cité, 75013 Paris, France*

The task of demonstrating quantum superiority for various computational tasks has been a topic of interest ever since the famous Shor's prime factoring algorithm. However most of these tasks require a universal quantum computer. Here on contrary we investigate the power of linear optics which is still powerful enough tool to demonstrate quantum superiority for some tasks. One such task studied in detail is Boson Sampling. In our work, we study a different kind of computational task, namely verifying NP-complete problems. In particular we look at the quantum proofs for 2-out-of-4 SAT problem as introduced by Aaronson et.al [1].

The 2-out-of-4 SAT is satisfying formula over N binary variables consisting of a conjugation of many clauses, each of which consists of exactly four variables. The clauses are satisfiable if exactly two variables are equal to 1. The problem is to decide if there is a truth assignment $x = x_1x_2..x_N$ to the formula. When Merlin(prover) and Arthur(verifier) use a quantum channel, the verification task can be done with on $K = \mathcal{O}(\sqrt{N})$ unentangled proofs with each proof revealing $\mathcal{O}(\log N)$ bits of information. This can be verified in polynomial time by Arthur. Whereas, in the classical case, any verification proof revealing $\mathcal{O}(\sqrt{N}\log N)$ bits of information requires exponential time for Arthur to verify. Recently, Arrazola et.al [2] showed that the quantum proof states can be implemented with single photon states in an equal superposition over many optical modes. Similarly, the tests can be performed using linear-optical transformations consisting of: permutation of modes interferometers, and measurement using single-photon detectors. The work in [2] shows that for an advantage over the classical proof, $N \geq 512$. Nevertheless, it is generally difficult to test these results experimentally and demonstrate the quantum superiority in practice since the quantum protocols typically necessitate creation and maintenance of large superposition states, which are out of the reach of current photonic technologies.

In this work, we come up with an alternative encoding of quantum proofs via time-bin sequences of coherent states. These states mimic the operation of single photon states with the same linear optics circuit. These offer us three primary advantages over the single photon implementation. (1) They are highly easy to produce and to sustain over a period of time for any size N. (2) With coherent states, the prover has to just send one proof state with $\sqrt{N}$ average photons over N time-bin modes. This enables us to remove the previous assumptions of unentanglement among the $\mathcal{O}(\sqrt{N})$ quantum proofs which was central to the working of the proof. (3) Sending one coherent state proof also enables Arthur to perform one less test of *symmetricity* which he otherwise performs probabilistically in the qubit proof structure.

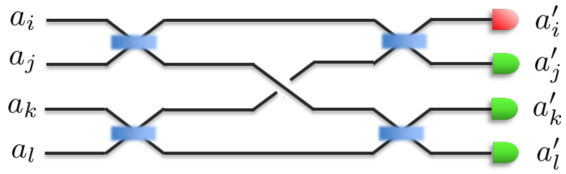

Figure 1: Interferometer for testing is the clauses are satisfiable. The input time-bin coherent states are rearranged as (i,j,k,l) and passed through this interferometer setting. In the ideal case, no photon is detected in the red detector if the clause is correct. Whereas if the clause is incorrect, then the probability of click in the red detector is almost double than the probability of click in the other 3 detectors

References

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor, in *23rd Annual IEEE Conference on Computational Complexity, 2008*. (IEEE, 2008), pp. 223-236.

[2] Juan Miguel Arrazola, Eleni Diamanti and Iordanis Kerenidis, arXiv:1711.02200 [quant-ph] 2017.