Warszawa, 15.09.2023

Rafael Freitas dos Santos
ul. Gen. W. Andersa 24/7
00-201 Warszawa

Summary of the doctoral thesis

"Certification of quantum states and measurements in contextuality scenarios"

Quantum theory is a probabilistic theory that provides a description of small-scale physical systems such as atoms or photons and it is one of the most successful physical theories that have been verified experimentally with a high degree of accuracy. At the same time it predicts phenomena such as quantum entanglement, Bell non-locality or more generally quantum contextuality that have been harnessed as resources for certain applications that are not accessible within classical physics. What is more, quantum phenomena are responsible for the recent rapid development of the new quantum technologies, just to mention the quantum computing machines. However, as far as the possibility of full exploitation of quantum technologies is concerned, this development has to be followed by designation of suitable certification tools that would enable the user to verify or certify that a given device operates according to its specification and generates the correct output. Such certification tools are particularly relevant in the context of quantum cryptography where the communicating parties need to verify that the state shared by the parties as well as the measurements performed by them are the correct one.

While there exist methods that serve the above purpose such as for instance the well-known quantum tomography, these rely on certain assumptions such as that the measuring devices used to test the state are fully characterized and that the user can trust that they perform correct measurements. While in certain situations such assumptions are justified, they are not when it comes to such tasks as quantum cryptography. As a remedy to this problem the idea of self-testing was put forward by Mayers and Yao. It allows for almost complete characterization of the underlying quantum systems based on the nonclassical correlations they produce, without the need of making strong assumptions about them. It thus falls into the category of device-independent certification in which quantum devices are treated as black boxes whose internal working is unknown to the user and the nonclassicality they generate is used to make nontrivial statements about them.

Self-testing as originally put forward by Mayers and Yao is based on Bell nonlocality and allows for certification of entangled states and the measurement performed on them. While many self-testing methods have already been proposed for entangled quantum states both in the bipartite and multipartite case, most of them, in particular, in the multipartite case, are devoted to systems that are locally qubits. Moreover, this type of certification methods have barely been explored for systems that do not have spatially separated subsystems and thus do not give rise to Bell nonlocality. Our aim here is to fill the above gaps. On one hand, we explore the possibility of exploiting quantum contextuality for certification purposes. In this direction we provide a class of scalable noncontextuality inequalities whose maximal violations can be used for certification of quantum systems consisting of N qubits and sets of binary measurements that obey certain commutation and anticommutation relations and generate the N-qubit Pauli group. Second, we propose a scheme, which is a modification of the standard quantum contextuality scenario, which allows for making certification statements about quantum systems from the observed correlations, however, without making any assumptions about the compatibility structure of the involved measurements which are made in contextuality-based approaches. On the other hand, we

introduce the first, to the best our knowledge, general class of Bell inequalities that are maximally violated by the multipartite graph states of arbitrary prime local dimension and show that in the qutrit case the maximal quantum violation of these inequalities allows for self-testing of the graph states. Again, our inequalities are scalable in the sense that the number of expectation values they consist of scales linearly with the number of parties which is relevant from the point of view of their experimental exploitation.

Rafael Freitas dos Santos