A semi-device-independent framework based on natural physical assumptions and its application to random number generation

T. Van Himbeeck[1,2], E. Woodhead[3], N. J. Cerf[2], R. García-Patrón[2], and S. Pironio[1]

[1]Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium
[2]Centre for Quantum Information and Communication,
Université libre de Bruxelles (ULB), Belgium
[3]ICFO – Institut de Ciències Fotòniques, The Barcelona Institute of Science
and Technology,, 08860 Castelldefels (Barcelona), Spain

In the device-independent (DI) approach to quantum information, correlations that are observed between separate quantum devices provide a guarantee that the protocol performs as expected. This guarantee follows independently of any assumptions on the local behavior of the quantum devices but it must necessarily rely on some specific constraints on the information that they exchange. Indeed, if arbitrary, unlimited communication is allowed between the devices, any kind of correlations can be generated, even in a scenario restricted to classical physics.

In the standard DI framework based on Bell non-locality, the constraint on communication is maximal: the separate devices are not allowed to communicate any type of information, neither classical nor quantum. This no-communication constraint has the conceptual advantage of having a clear physical and operational significance. In particular, it is in principle possible to enforce it without knowledge of the internal behavior of the devices, i.e., by adequate shielding or space-like separation of the devices. However, the generation of useful, non-classical correlations in the absence of quantum communication must then necessarily rely on (loophole-free) entanglement, which presently represents a serious obstacle to practical DI applications.

This difficulty has motivated the development of an alternative framework for DI applications, which is inspired by the traditional prepare-and-measure implementation of quantum key distribution and where communication is allowed between the quantum devices. As noted above, a constraint, though, must be put on this communication and it is usually formulated as a bound on the Hilbert space dimension of the exchanged quantum messages. With such a constraint, useful non-classical correlations can already be generated by restricting the communication to qubits or qutrits in a purely prepare-and-measure scenario, without the need of entanglement, which provides a clear advantage from the implementation point of view. Several protocols for randomness generation (RNG) and quantum key distribution (QKD) have been introduced within this framework, which is usually referred to as "semi-device-independent" (semi-DI). The downside, however, is that the dimension assumption, even if it represents a convenient abstraction for a theorist, is only an idealization. Carriers of quantum information, such as photons, live in an infinite Hilbert space, and assuming that information is encoded in only a few degrees of freedom is not justified without some intricate characterization of the devices (hence the terminology "semi-device-independent").

In this talk, we propose a physically better motivated approach for constraining the exchanged quantum messages in a semi-DI framework. We express the restriction on the exchanged states in terms of the mean values of some well-chosen observable, such as the energy.

As a simple example, consider the case where the Hilbert space carrying the quantum messages is the Fock space of several quantum optical modes. This is the appropriate space to describe quantum optics experiments, including those attempting to demonstrate results based on dimension bounds, in which attenuated laser sources or non-ideal heralded photon sources are used. In this context, the emitted states can in principle occupy an infinite-dimensional space so that, instead of putting a limit on the dimension, it is much more natural to constrain the average number of photons. The corresponding observable would then be the photon-number operator, which has a clear physical significance. Alternatively, we could constrain the energy contained in one or more frequency modes containing the quantum message, as the two are closely related. This is thus a natural substitute for the dimension of a finite Hilbert space. Moreover, designing devices in such a way that the average photon number does not exceed a given threshold or verifying experimentally that it does not exceed such a threshold will typically require a less detailed modeling of the devices than would be needed to verify, e.g., that the emitted states span a Hilbert space of a given dimension.

A prerequisite for the development of any DI or semi-DI protocol is to examine the set of correlations that are available under the assumptions considered. Much work has been done specifically on this question in the standard settings based on non-locality and dimension bounds. In this talk, we first present a full analytical characterization of the set of available correlations in the simplest scenario compatible with our general framework.

This scenario involves the following two ingredients: a source that can emits one of two states depending on the value of a binary input and a measurement device that performs a single measurement with binary outcome on the state that is received. Interestingly, this prepare-and-measure scenario is simpler than any possible scenario based on a dimension bound. In our analysis, the behaviors of the source and measurement device are not characterized and could even depend on shared hidden parameters in the possession of an adversary. But we trust that the prepared states satisfy constraints expressed in term of the expectations of some observable with non-degenerate ground state and finite gap. A particular example of such constraints could correspond in quantum optics implementations to upper-bounds on the expected number of photon of the states emitted by the source (this is the main application that we have in mind, but our formalism is more general).

We have determined analytically the set of available quantum correlations in this simple scenario. In particular, we have identified analogues of Bell inequalities, which are able to distinguish genuinely quantum devices from those behaving in a purely classically pre-determined fashion. We present a few simple potential implementations using currently accessible quantum optics technology that generate correlations in the genuinely quantum region. Our simplest optical scheme works by the on-off keying of an attenuated laser source followed by photocounting.

A more complete discussion and motivation of our approach and the technical details of the results mentioned above can be found in arXiv:1612.06828.

In addition to arXiv:1612.06828, this talk will also present results from a second paper that we are currently writing. This paper contains two new main contributions. First, we provide a characterization of the quantum region that is alternative to the one presented in arXiv:1612.06828 and which is based on a simple semidefinite program. This alternative characterization is obtained by establishing an isomorphism between the set of correlations in our prepare-and-measure scenario and the correlations of an entanglement-based protocol corresponding to a bipartite XOR game with two binary inputs and outputs. This relation between our prepare-and-measure scenario and an entanglement-based one is not only conceptually interesting, but is also technically useful for quantifying the amount of randomness that can be certified in our semi-DI setting.

Computing lower-bounds on the randomness produced by an arbitrary implementation represents our second new contribution beyond the results already presented in arXiv:1612.06828. Using the new formulation of the quantum region, this problem can be cast as a semidefinite program and can thus easily solved numerically. For several cases of physical interest, we also provide a complete analytical solution to the corresponding optimization problem. Such lower bounds on the amount of randomness generated can then be directly exploited to design protocols for semi-DI random number generation. We will discuss the resulting semi-DI RNG protocols, with a special focus on the on-off keying implementation.