Técnico Lisboa
University of Lisbon

Research Seminar in Information Security

(Prof. Paulo MATEUS)

Doctoral Program in Information Security

2023/2024 - 1st Semester

Device-Independent Entanglement Certification with Dishonest Parties

(Gláucia MURTA - November 23, 2023)

Report written by:

- Rúben BARREIRO:
  - *ruben.andre.letra.barreiro@tecnico.ulisboa.pt*

Last updated: February 15, 2024

1 Motivation

One of the tasks of interest in this seminar is to address how to certify some resource states and their quantum properties distributed in a future (experimental) Quantum Communication Network connecting several quantum devices (or quantum nodes) in different places. These quantum properties can be entanglement properties of those resource states distributed on a Quantum Communication Network involving some scenario aspects, such as geographic proximity or political relations. These quantum nodes might be prone to collaborate with each other, so we cannot assume they do their tasks independently. In these scenarios, we would like to certify the entanglement properties even in the presence of some dishonest party. Here, the minimal level of characterization we would want to guarantee for these quantum network systems is that they are Device-Independent (DI). In this characterization scenario, we assume that there might exist some dishonest parties in the quantum network. However, we also want to keep the privacy of the operations and tasks performed by the quantum nodes or devices in that quantum network. Thus, the main goal of a DI scenario would be for these quantum nodes and devices to perform these operations and tasks only based on statistics of inputs and outputs rather than the exact details of the laboratories of the experimental setup for this designed quantum network.

This seminar addresses aspects of a research work published by Gláucia Murta from Heinrich-Heine University of Düsseldorf in collaboration with Flavio Baccari from Max-Planck Institute of Quantum Optics, where they introduced a framework for DI entanglement certification with the presence of dishonest parties, obtaining some self-testing properties and a robust certification of resource states such as GHZ states in these scenarios [1].

2 Entanglement Certification

The first part of this seminar addressed a simple qualitative overview of the scenario previously introduced, with only an entanglement verification of a simple quantum network. In this simple scenario, instead of having several different clusters of collaborating parties, we have only N parties and a subset D of $(N-k+1)$ dishonest parties that could be collaborating. This simple scenario is a little different from the standard DI scenario. Namely, in the DI scenario, we assume we do not know what the quantum devices or

nodes are actually doing. On the other hand, in this scenario variant, some of those quantum devices or nodes could work together and apply some arbitrary joint operations they could communicate. Therefore, in this new scenario, we do not have this overview network separation, and, in fact, we could say one subset of parties is dishonest, although we do not need to know which of them is indeed dishonest. In this quantum communication network, the honest parties only have uncharacterized quantum devices or quantum nodes. On the other hand, the dishonest ones are allowed to communicate among them, apply classical post-processing operations, and perform joint measurements. In this scenario, we assume the dishonest parties can also control their quantum devices. However, in the end, we can obtain the statistics, and we still want to analyze the distributed entanglements.

But the crucial aspect here is that we are actually going to address a DI scenario where we will need a Bell Inequality. The results obtained by the authors demonstrate we can use a particular class of Bell Inequalities to achieve such a strong characterization for this scenario. In this case, the Bell Inequality of interest is called the Svetlichny Inequality, an inequality where each one of the parties gets two inputs and two outputs. This inequality is also known as the Full Correlator Inequality since we only have terms that involve the expected value of the observables of all the parties together. Basically, this correlator results in 1 if the parity of the parties' measurement outcomes is 0 and results in -1 if the parity of the parties' outcomes is 1.

Therefore, this is a family of N-partite Svetlichny Inequalities for any number N of parties. Such as any other Bell Inequality, these Svetlichny Inequalities have a classical bound that Quantum Mechanics can violate, as well as they have a (estimated) quantum bound. However, this classical bound is a little more interesting in the sense that when we have more than $N = 2$ parties, we start having a structure for the outcomes of our parties involved, so we do not have only a separable notion for them (e.g., local or non-local), but also a different structure notion, namely a grouping concept. This classical bound sets a limit for all the probability distributions in a way we cannot decompose them in the following mathematical form below:

From this mathematical form, we can divide the subset of parties into two main groups, where we may have arbitrary collaborations within these groups, but we still have some separate actions. Then, we can take some convex combination of this type of correlation, where we have arbitrary correlations within these groups of parties. And, since these correlations are within this local classical bound, we are able to witness a strong genuine

multipartite non-locality. Thus, we violate the Svetlichny Inequality only when we cannot decompose this probability distribution in this mathematical form. Nowadays, the first proposal for the definition of genuine multipartite non-locality, where Svetlichny allowed this joint probability distribution of the group to be arbitrary, is not used anymore because when we abstract from the considered scenario, we usually want to look at non-locality property as an operational framework, what leads to some inconsistencies if we define locality regarding that operational outlook. To overcome this, people often add some assumptions to these joint probability distributions, often assuming they have to be non-signaling or one-way signaling, but they cannot be arbitrary. However, for our scenario, it turns out that this definition is the one that is interesting because we want to address these collaborating parties that could be realizing an arbitrary action. Another important observation is that this inequality also detects Genuine Multipartite Entanglement (GME) since we would never be able to violate it if the quantum entangled state we want to verify is bi-separable in the standard Bell Inequality scenario.
For the Svetlichny Inequality with dishonest parties, the honest action would be the following observable, which is describing a subtraction between two arbitrary Positive Operator-Valued Measure (POVM) elements, one for each outcome (0 and 1), where, in principle, honest actions should apply local actions, but they will have these two global POVM elements instead:

3 Self-Testing with Dishonest Parties

4 Outlook

References

[1] Gláucia Murta and Flavio Baccari. Self-Testing with Dishonest Parties and Device-Independent Entanglement Certification in Quantum Communication Networks. *Phys. Rev. Lett.*, 131:140201, 2023.