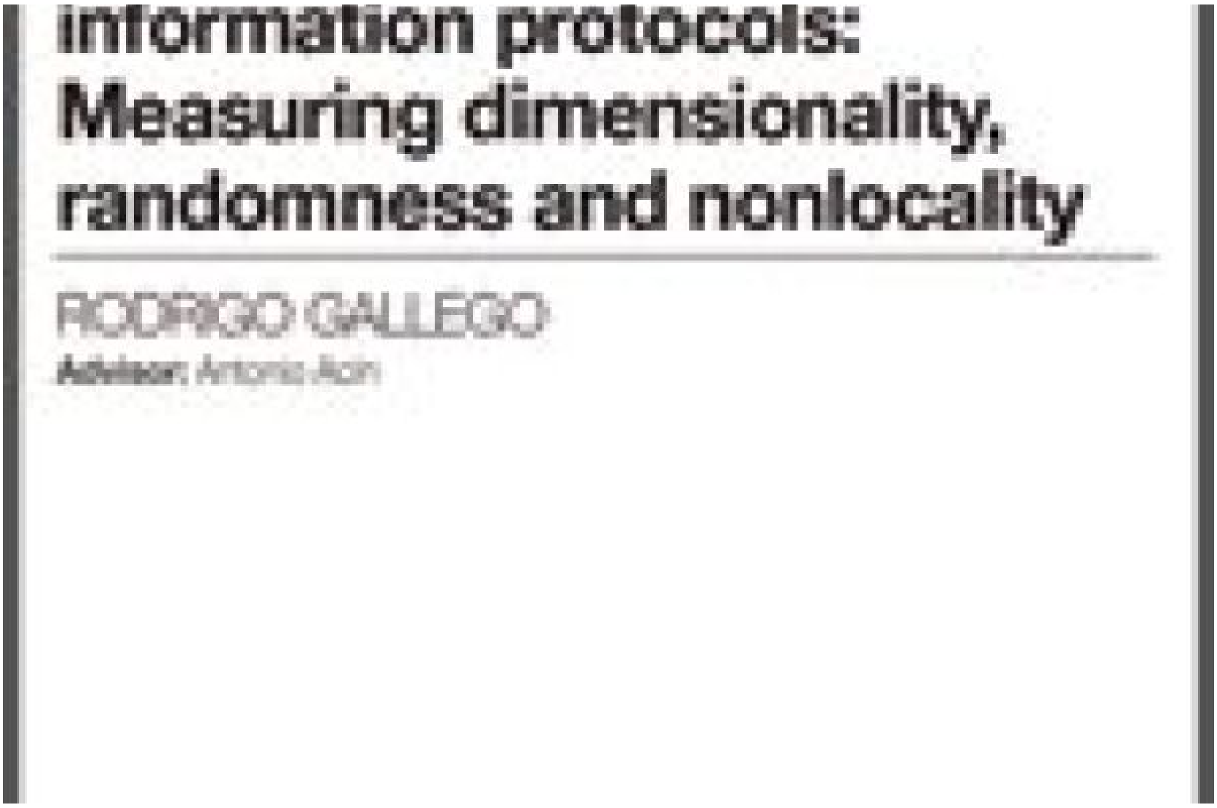

information protocols: Measuring dimensionality, randomness and nonlocality

RODRIGO GALLEGO

Advisor: Antonio Acín

PhD Thesis Defense RODRIGO GALLEGO 'Device-independent information protocols: Measuring dimensionality, randomness and nonlocality'

RODRIGO GALLEGO

February 22, 2013

Friday, February 22, 11:00. ICFO Auditorium

RODRIGO GALLEGO

QUANTUM INFORMATION THEORY

ICFO-The Institute of Photonic Sciences, SPAIN

The device-independent formalism is a set of tools to analyze experimental data and infer properties about systems, while avoiding almost any assumption about the functioning of

devices. It has found applications both in fundamental and applied physics: some examples are the characterization of quantum nonlocality and information protocols for secure cryptography or randomness generation. This thesis contains novel results on these topics and also new applications such as deviceindependent test for dimensionality.

After an introduction to the field, the thesis is divided in four parts. In the first we study device-independent tests for classical and quantum dimensionality. We investigate a scenario with a source and a measurement device. The goal is to infer, solely from the measurement statistics, the dimensionality required to describe the system. To this end, we exploit the concept of dimension witnesses. These are functions of the measurement statistics whose value allows one to bound the dimension. We study also the robustness of our tests in more realistic experimental situations, in which devices are affected by noise and losses. Lastly, we report on an experimental implementation of dimension witnesses. We conducted the experiment on photons manipulated in polarization and orbital angular momentum. This allowed us to generate ensembles of classical and quantum systems of dimension up to four. We then certified their dimension as well as its quantum nature by using dimension witnesses.

The second part focuses on nonlocality. The local content is a nonlocality quantifier that represents the fraction of events that admit a local description. We focus on Systems that exhibit, in that sense, maximal nonlocality. By exploiting the link between Kochen-Specker theorems and nonlocality, we derive a systematic recipe to construct maximally nonlocal correlations. We report on the experimental implementation of correlations with a high degree on nonlocality in comparison with all previous experiments on nonlocality. We also study maximally nonlocal correlations in the multipartite setting, and show that the so-called GHZ-state can be used to obtain correlations suitable for multipartite information protocols, such as secret-sharing.

The third part studies nonlocality from an operational perspective. We study the set of operations that do not create nonlocality and characterize nonlocality as a resource theory. Our framework is consistent with the canonical definitions of nonlocality in the bipartite setting. However, we find that the well-established definition of multipartite nonlocality is inconsistent with the operational framework. We derive and analyze alternative definitions of

multipartite nonlocality to recover consistency. Furthermore, the novel definitions of multipartite nonlocality allows us to analyze the validity of information principles to bound quantum correlations. We show that ?information causality' and `non-trivial communication complexity' are insufficient to characterize the set of quantum correlations.

In the fourth part we present the first quantum protocol attaining full randomness amplification. The protocol uses as input a source of imperfect random bits and produces full random bits by exploiting nonlocality. Randomness amplification is impossible in the classical regime and it was known to be possible with quantum system only if the initial source was almost fully random. Here, we prove that full randomness can indeed be certified using quantum non-locality under the minimal possible assumptions: the existence of a source of arbitrarily weak (but non-zero) randomness and the impossibility of instantaneous signaling. This implies that one is left with a strict dichotomic choice regarding randomness: either our world is fully deterministic or there exist events in nature that are fully random.

Friday, February 22, 11:00. ICFO Auditorium

Thesis Advisor: Prof. Antonio Acin