PhD Thesis Defense ALEXIA SALAVRAKOS 'Bell Inequalities for Device-Independent Protocols'

ALEXIA SALAVRAKOS

March 26, 2019

Tuesday, March 26, 11:00. ICFO Auditorium

ALEXIA SALAVRAKOS

Quantum Information Theory

ICFO-The Institute of Photonic Sciences

The technological era that we live in is sometimes described as the Information Age. Colossal amounts of data are generated every day and considerable effort is put into creating technologies to process, store and transmit information in a secure way. Quantum Information Science relies on quantum systems to develop new information technologies by exploiting the non-classical properties of those systems, such as entanglement or

superposition. Quantum computing has recently received substantial investment, and quantum random number generators and cryptography systems are already available commercially.

Entanglement is one of the counter-intuitive, mysterious phenomena that quantum theory is known to describe. Two entangled particles are such that, even when they are spatially separated, their quantum state can only be described for the system as a whole, and not as two independent quantum states.

This implies that when making measurements on entangled particles, particular correlations between the measurement outcomes may appear which cannot be obtained with pre-shared classical information. Such correlations, termed nonlocal, can be detected using mathematical objects called Bell inequalities, that correspond to hyperplanes in the set of correlations obtained in a so-called Bell scenario. Many Bell experiments were conducted in which violations of Bell inequalities were measured, thus confirming the existence of nonlocality in Nature.

The last decade has seen the development of a new paradigm in quantum information theory, called the device-independent paradigm. The security and success of a device-independent protocol relies on the observation of nonlocal correlations in a Bell experiment. Moreover, the nature of Bell scenarios is such that very few assumptions on the experimental apparatus are needed, hence the name device-independent. In this framework, Bell inequalities serve as certificates that guarantee properties and quantities such as the randomness of a series of numbers or the security of a secret key shared between users. It is even possible to certify which quantum state and measurements were used in the experiment based solely on the correlations they produce: this task is called self-testing.

The goal of this thesis is the study of Bell inequalities, both as fundamental objects and as tools for device-independent protocols. We consider in particular protocols for randomness certification, quantum key distribution and self-testing.

In Chapter 3, we develop robust self-testing procedures for the chained Bell inequalities, which also imply randomness certification. The chained Bell inequalities are a family of Bell inequalities that are relevant for a scenario with an arbitrary number of measurement

choices. In Chapter 4, we introduce a family of Bell inequalities maximally violated by the maximally entangled states, valid for a scenario with any number of measurement choices as well as any number of measurement outcomes. We study the properties of these Bell inequalities in depth, and discuss through examples their applications to self-testing, randomness certification and quantum key distribution. We also present an extension of our results to any number of parties, as well as experimental results obtained in an international collaboration, where we measure violations of our Bell inequalities for local dimension up to 15. In Chapter 5, we consider the question of randomness certification from partially entangled states. We show, through self-testing results, that maximal randomness can be certified from any partially entangled state of two qubits, using the Clauser-Horne-Shimony-Holt inequality and its tilted version.

Tuesday, March 26, 11:00. ICFO Auditorium

Thesis Advisor: Prof Dr Antonio Acin