PhD Thesis Defense GONZALO DE LA TORRE CARAZO 'From Quantum Foundations to Quantum Information Protocols and back '

GONZALO DE LA TORRE CARAZO

September 23, 2015

Wednesday, September 23, 11:00. ICFO Auditorium

GONZALO DE LA TORRE CARAZO

Quantum Information Theory

ICFO-The Institute of Photonic Sciences

Physics has two main ambitions: to predict and to understand. Indeed, physics aims for the prediction of all natural phenomena.Prediction entails modeling the correlation between an action, the input, and what is subsequently observed, the output.

Understanding, on the other hand, involves developing insightful principles and models that can explain the widest possible varietyof correlations present in nature. Remarkably, advances in both prediction and understanding foster our physical intuition and, as a consequence, novel and powerful applications are discovered. Quantum mechanics is a very successful physical theory both in terms of its predictive power as well as in its wide applicability. Nonetheless and despite many decades of development, we do not yet have a proper physical intuition of quantum phenomena. I believe that improvements in our understanding of quantum theory will yield better, and more innovative, protocols and vice versa.This dissertation aims at advancing our understanding and developing novel protocols. This is done through four approaches.

The first one is to study quantum theory within a broad family of theories. In particular, we study quantum theory within the family of locally quantum theories. We found out that the principle that singles out quantum theory out of this family, thus connecting quantum local and nonlocal structure, is dynamical reversibility. This implies that the viability of large scale quantum computing can be based on concrete physical principles that can be experimentally tested at a local level without needing to test millions of qubits simultaneously.

The second approach is to study quantum correlations from a black box perspective thus making as few assumptions as possible. The strategy is to study the completeness of quantum predictions by benchmarking them against alternative models. Three main results and applications come out of our study. Firstly, we prove that performing complete amplification of randomness starting from a source of arbitrarily weak randomness - a task that is impossible with classical resources - is indeed possible via nonlocality. This establishes in our opinion the strongest evidence for a truly random event in nature so far. Secondly, we prove that there exist finite events where quantum theory gives predictions as complete as any no-signaling theory can give, showing that the completeness of quantum theory is not an asymptotic property. Finally, we prove that maximally nonlocal theories can never be maximally random while quantum theory can, showing a trade-off between the nonlocality of a theory and its randomness capabilities. We also prove that quantum theory is not unique in this respect.

The third approach we follow is to study quantum correlations in scenarios where some parties have a restriction on the available quantum degrees of freedom. The future progress of semi-device-independent quantum information depends crucially on our ability to bound the strength of these correlations. Here we provide a full characterization via a complete hierarchy of sets that approximate the target set from the outside. Each set can be in turn characterized using standard numerical techniques. One application of our work is certifying multidimensional entanglement device-independently.

The fourth approach is to confront quantum theory with computer science principles. In particular, we establish two interesting implications for quantum theory results of raising the Church-Turing thesis to the level of postulate. Firstly, we show how different preparations of the same mixed state, indistinguishable according to the quantum postulates, become distinguishable when prepared computably.Secondly, we identify a new loophole for Bell-like experiments: if some parties in a Bell-like experiment use private pseudorandomness to choose their measurement inputs, the computational resources of an eavesdropper have to be limited to observe a proper violation of non locality.

Wednesday, September 23, 11:00. ICFO Auditorium

Thesis Advisor: Prof. Antonio Acin