UNIVERSITÉ LIBRE DE BRUXELLES, UNIVERSITÉ D'EUROPE

ULB

Centre for Quantum Information and Communication

http://quic.ulb.ac.be

Sujets des Mémoires de Fin d'Etudes pour l'année académique 2012-13

Contact général : Prof. Nicolas Cerf (local UA3.217, tél.: 2858, ncerf@ulb.ac.be)

Thème général : Sciences de l'Information Quantique

Etudiants concernés : Ir. Physique ou Ms. Science Physique (sauf projet 6 qui convient également pour des Ir. Informatique ou Ms. Science Informatique)

Pré-requis : Tous les sujets nécessitent des connaissances de base de mécanique quantique, de théorie des probabilités et d'algèbre linéaire. Une connaissance de base de théorie de la complexité est aussi utile pour le projet 6.

Langue : Français ou anglais en fonction de la personne qui supervise le mémoire (par uniformité, tous les sujets sont présentés en anglais ci-dessous)

1. Gaussian quantum bosonic channels with memory

J. Schäffer (joschaef@ulb.ac.be), E. Karpov (ekarpov@ulb.ac.be)

In quantum information theory, the capacity of quantum channels is one major topic of research, just like in Shannon's information theory for classical channels. A particular interest has been devoted to Gaussian bosonic channels as they model common physical links such as the optical transmission via free space or optical fibers. If one considers a system of many modes that are separated spatially, in time or frequency, one needs to take into account possible noise correlations between the modes, also refered to as the "memory" of the channel. The first objective of this project will be to explore new aspects and solve open questions related to memory channels, based on recent research results at QuIC. This will inlcude the study of the capacity of energy-restricted bosonic Gaussian channels. An interesting problem is also the study of a physical model for a memory channel. The goals is to study naturally occurring noise correlations, to develop a mathematical model for such correlations, and to discuss the capacity and optimal encoding of the corresponding channel. A related question is the optimality of a Gaussian encoding for Gaussian channels. The idea is to perform a numerical study of the transmission rates in Gaussian channels, where different, a priori non-Gaussian encodings are used. This could potentially lead to fundamental insights in longstanding open problems

2. Characterization of the concatenation of Gaussian quantum bosonic channels, including the entanglement-assisted capacity

O. Pilyavets (opilyave@ulb.ac.be), E. Karpov (ekarpov@ulb.ac.be)

Information is necessarily transmitted with physical carriers such as, for example, the electromagnetic field, so that it obeys the laws of physics as well as information theory. Modern developments of quantum optics allow the manipulation of electromagnetic signals in a quantum regime, and one can use these quantum signals (quantum states) for information transmission. Therefore, a very important problem of information theory, namely to determine the capacity of information transmission channels, may also be formulated for quantum channels. Although the Gaussian quantum bosonic channels were intensively studied, several important problems are still open. It is known that concatenation of Gaussian channels is a Gaussian channel. However, the properties of concatenated channels, which are obtained by chaining two or more Gaussian bosonic channels, have not yet been systematically analyzed. We propose the study of the information transmission (rates and classical capacity) via such « chains » of several Gaussian quantum channels. In addition, the entanglement-assisted capacity of Gaussian quantum bosonic channels will be investigated. This problem desribes the transmission of classical information in the case where the communicating parties share prior quantum entangled states, which they can use as a resource. In such protocols, the quantum states do not carry the information in itself (this would violate causality), but the combination of a classical channel with quantum entanglement allows increasing the information transmission rate of the classical line.

3. Gaussian quantum key distribution ; alternative schemes, including the application of a noiseless linear amplifier

E. Karpov (ekarpov@ulb.ac.be), C. Gagatsos (Christos.Gagatsos@ulb.ac.be)

Quantum key distribution is a technique that enables a private communication between two authorized parties, the security of which relies on quantum physics. A specific quantum key distribution scheme, called Gaussian and developed by us among others, has the advantage that it can yield high secret key rates as it is based on homodyne detection instead of single-photon detectors. This comes, however, with the disadvantage that the loss-induced vacuum noise severely limits the secure range that can be attained. The key problem is that quantum mechanics precludes the amplification of a signal without adding quantum noise, which is detrimental to quantum key distribution as it can be exploited by an eavesdropper. The objective of this project is to analyze whether the recently invented scheme for heralded noiseless amplification, where the noise of the amplifier is traded for a limited probability of success, could provide a new tool for enhancing the secure range. Alternative schemes may also be envisaged.

4. Majorization theory as a tool in quantum information processing

C. Gagatsos (Christos.Gagatsos@ulb.ac.be), O. Oreshkov (oreshkov@ulb.ac.be)

Majorization is a basic tool of probability theory, which provides a partial order relation between probability distributions. It has been shown, over the last ten years, that majorization is also a very important concept in quantum information theory as it gives a criterion to the possible interconversion between bipartite pure states or to the separability of quantum states. It was also shown by us to play a key role in the information transmission via Gaussian quantum channels, as it is strongly relates to the so-called Gaussian minimum entropy conjecture. The objective of this project is to seek for new applications of this concept in particular within continuous-variable quantum information theory.

5. Quantum paradoxes in the weak-value measurement paradigm.

C. Giarmatzi (cgiarmat@ulb.ac.be), O. Oreshkov (oreshkov@ulb.ac.be)

In a typical quantum thought experiment, one prepares a quantum system at some time and then performs a measurement at a later time. In the weak-value approach (introduced by Aharonov & Vaidman), one considers both the prepared state propagating forwards in time and the postselected state (the one that has been measured) propagating backwards in time. At an intermediate time, one may assign a « weak value » to some observable, which gives rise to paradoxes. This will be investigated in the specific case of Gaussian states of light and Gaussian measurements (homodyne measurement). An information-theoretic interpretation of the paradox will also be sought for, as well as links with the retrodictive approach to quantum mechanics.

6. Optimality of quantum algorithms for the Boolean hidden shift problem

J. Roland (jroland@ulb.ac.be)

Hidden shift problems belong to an important class of problems where quantum computers are known to provide an exponential speedup compared to classical computers. The description of the problem is however very simple : given black-box access to a shifted version f(x+s) of a function f(x), find the hidden shift s. Depending on the domain and range of the function f, different versions of the hidden shift problem may be defined. In particular, the Boolean hidden shift problem considers the case where f is a Boolean function f:$\{0,1\}^n \rightarrow \{0,1\}$. A new quantum algorithm for the Boolean hidden shift problem has recently been proposed by us, and shown to provide an exponential speedup for random Boolean functions. However, the complexity of the algorithm can vary greatly for different functions, for example, if f is a delta function, the problem reduces to Grover's search problem, where only a quadratic speedup is possible. The goal of this projet is to study the complexity of the Boolean hidden shift problem in terms of the Fourier spectrum of the function, which characterizes the cost of the knwown quantum algorithms for this problem, and therefore study their optimality.

7. Information-theoretic concepts for quantum processes without causal order

O. Oreshkov (oreshkov@ulb.ac.be)

Quantum information processes are traditionally expressed in a framework that explicitly includes causal ordering between events. For example, one considers a preparer who sends two entangled systems (e.g. two photons) to two separate observers, each of whom performs a measurement on the system she/he receives. An interesting situation is when the two receivers are spacelike separated, which means that the measurement one performs cannot have a causal influence on the other, while the preparer, of course, can influence the two. This is the standard paradigm where nonlocal quantum correlations can be observed. In a recent work, it was shown by us that one can go beyond this and consider situations where the causal ordering between events is not defined, i.e., we can have a "quantum superposition of causal orders". This new concept will be studied, and an attempt will be made at finding explicit optical setups where such correlations may be observed.

8. Theory and applications of quantum feedback control

O. Oreshkov (oreshkov@ulb.ac.be)

Quantum control is a new and rapidly developing area of quantum information science, which studies methods for control of quantum systems for the purpose of information processing. In quantum feedback control (QFC), the system of interest is monitored continuously via a weak interaction with a measurement device, and the result of the measurement is used to steer the system in real time (for example, by continually modifying the Hamiltonian or the measurement being made). Unlike classical feedback control, however, gaining any information about the system in the quantum case inevitably leads to a disturbance of the system due to the uncertainty principle, which makes the problem of QFC fundamentally different. In particular, a problem of interest is to develop a theoretical framework for QFC for the case where the target is not a state but a general quantum operation. This project will aim at developing theoretical tools for such a framework and investigate the possibility for achieving interesting operations via QFC given a restricted set of simple interactions such as those available in present-day experiments.