UNIVERSITÉ LIBRE DE BRUXELLES, UNIVERSITÉ D'EUROPE

Centre for Quantum Information and Communication

http://quic.ulb.ac.be

Sujets des Mémoires de Fin d'Etudes pour l'année académique 2015-16

Contact général : Prof. Nicolas Cerf (local UA3.217, tél: 2858, ncerf@ulb.ac.be)
Prof. Jérémie Roland (local UA3.212, tél: 2875, jroland@ulb.ac.be)

Thème général : Sciences de l'Information Quantique

Etudiants concernés : Ir. Physique ou Ms. Science Physique (tous les projets)
Ir. Informatique ou Ms. Science Informatique (projets 2-4)

Pré-requis : Tous les sujets nécessitent des connaissances de base de mécanique quantique, de théorie des probabilités et d'algèbre linéaire.

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. Capacity of Gaussian quantum channels

E. Karpov (ekarpov@ulb.ac.be) and N. Cerf (ncerf@ulb.ac.be)

In communication networks, information is transmitted by physical carriers, such as the photons mediating the electromagnetic field. Modern developments in quantum optics enable the manipulation of electromagnetic signals in a quantum regime, i.e., at the level of single photons, and one uses quantum states of light as signals for encoding information. Therefore, a central problem of Shannon's information theory, namely to determine the capacity of communication channels, may also be formulated for quantum channels. In this context, a particular effort has been devoted to quantum bosonic Gaussian channels as they model most common physical links, such as information transmission via optical fibers. Although these channels have been intensively studied, several important problems have remained open today.

The goal of this project is to investigate one particular problem, which can be reduced to the energy-constrained minimization of the output entropy of a lossy channel that couples the input state with a squeezed vacuum state. Proving that the optimal input state is Gaussian, in analogy to the situation in Shannon's information theory, would bring a big progress in the determination of the capacity of phasesensitive bosonic channels (below some energy threshold). The idea is to seek a possible analytical treatment of the optimization problem, guided by a numerical analysis. A second objective will be to address the power constraint « worst case » and « optimal » channel noise in case of quantum Gaussian channels with memory or parallel quantum Gaussian channels.

2. Adiabatic quantum query algorithms

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

Quantum computers promise to solve certain problems more efficiently than classical computers. The standard model of quantum computation works by applying a sequence of quantum gates (or unitary operations) on a set of qubits. An alternative model, which is equivalent in computational power, is adiabatic quantum computing. In this model, the quantum computer is initially prepared in the ground state of a specific Hamiltonian, and the computation works by slowly turning off this Hamiltonian while at the same time turning on another one whose ground state encodes the solution of the computational problem. If this interpolation is performed slowly enough, the quantum adiabatic theorem guarantees that the initial ground state will be transformed into the final ground state.

Many (if not most) of known quantum algorithms are based on the so-called quantum query model, where the input of the problem is accessible via a black box. These algorithms are usually described as quantum circuits, but researchers at QuIC have recently shown that any such problem can also be solved optimally by an adiabatic algorithm. The goal of this project will be to explicitly apply this new construction in order to derive adiabatic formulations of standard quantum algorithms, such as Deutsch's, Deutsch-Jozsa's, Simon's and Shor's algorithms.

3. Search algorithms by random (or quantum) walks in the presence of multiple solutions

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

Random walks or Markov chains describe the dynamics of a memoryless particle moving on a graph and have many applications ranging from statistical physics to computer science. For example, the dynamics of a physical system coupled with a thermal bath can be modeled as a Markov chain where each step corresponds to a transition from one state to another due to the absorption or emission of energy. This process converges to the so-called Gibbs distribution which, for low temperatures, favors low energy states. In computer science, this physical process can be simulated to solve optimization problems by mapping the objective function that has to be minimized to energy levels of a physical system: this is the basic idea behind the famous Metropolis algorithm.

Besides optimization problems, many search problems in computer science can be solved by walking randomly on a graph until a certain marked vertex, corresponding to the solution, is reached. In this case, the relevant property of the random walk is its hitting time, that is, the expected number of steps necessary to reach the marked vertex. In the presence of multiple marked vertices (that is, multiple solutions), the algorithm can easily be adapted by stopping as soon as any marked vertex is reached, leading to a notion of hitting time for sets of marked vertices. One disadvantage of this modified algorithm is that it might not provide a fair sampling of solutions, favoring some easily reachable solutions over others.

The goal of this project will be to study how this random walk search algorithm could be modified to provide a fair sampling of solutions. One possible inspiration for this might be the Metropolis algorithm which, by coupling to a thermal bath, allows to escape local minima and uniformly sample global minima. The interested student could also extend his project to the case of quantum walks, which are the quantum equivalents of random walks, and can be used to solve the same search problems.

4. The information complexity of quantum non-locality

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

One of the most intriguing aspects of quantum mechanics is quantum non-locality, which arises when two distant systems are measured. Indeed, it can happen that the measurement outcomes are so strongly correlated that, considering a model of the experiment based on classical physics, only faster-than-light communication could explain the outcomes. The correct explanation can only be given by quantum physics, which implies that if two quantum particles have interacted in the past, they can share a special connection called entanglement, which remains even when the particles are separated, and explain these classically impossible correlations.

Non-locality was first considered as an oddity of quantum mechanics, but has now been found the be an invaluable resource for many informational tasks, in particular in the context of cryptography, such as key distribution or randomness generation. For this reason, a natural question is how to quantify the non-locality of an entangled system, and many approaches have been proposed to answer this question. One approach is based on the model of communication complexity. In theoretical computer science, the goal of communication complexity is to quantify the amount of communication required for two distant parties to compute a function f(x,y), if one of them knows x and the other y. In order to quantify non-locality, one might ask how much faster-than-light communication is required to simulate the correlations between the measurement outcomes of the entangled state, which can be shown to reduce to a problem very similar to the standard problem of computing a function.

Recently, the model of communication complexity led to the idea of information complexity, where instead of counting the number of bits sent back and forth between the parties, we count the information content of the messages. This new model has been intensively studied in the last few years and led to a flurry of results, dramatically improving the understanding of the usual communication complexity model.

The goal of this project will be the study the information complexity of quantum non-locality, starting with the case of a maximally entangled pair of qubits. This is the simplest and also most studied system, in particular its communication complexity has been fully characterized as it is known that 1 bit of communication is necessary and sufficient to simulate it. On the other hand, not much is known about its information complexity, except that it is strictly less than one, which is enough to conclude that the question is not trivial and might therefore lead to interesting results.

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

O. Oreshkov (oreshkov@ulb.ac.be) and N. Cerf (ncerf@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.

6. Adiabatic quantum computing via Markovian dynamics

O. Oreshkov (oreshkov@ulb.ac.be), J. Roland (jroland@ulb.ac.be), and N. Cerf (ncerf@ulb.ac.be)

Quantum computers promise to solve certain problems more efficiently than classical computers. The standard model of quantum computation works by applying a sequence of quantum gates (or unitary operations) on a set of qubits. An alternative model, which is equivalent in computational power, is Adiabatic Quantum Computing. In this model, the quantum computer is initially prepared in the ground state of a specific Hamiltonian, and the computation works by slowly turning off this Hamiltonian while at the same time turning on another one whose ground state encodes the solution of the computational problem. If this interpolation is performed slowly enough, the quantum adiabatic theorem guarantees that the initial ground state will be transformed into the final ground state. Recently, the adiabaticatic theorem was extended from the case of closed quantum system undergoing

Hamiltonian dynamics to the case of open quantum systems undergoing dissipative Markovian dynamics, and it was shown that this more general type of adiabatic dynamics can be used to perform various tasks. This project will explore the possibility to perform adiabatic quantum computation via adiabatic Markovian dynamics

7. Distributing classical randomness over a quantum channel

R. Garcia-Patron (raulgarciapatron@gmail.com) and N. Cerf (ncerf@ulb.ac.be)

The ability to distribute randomness over a channel appears to be a weaker resource than distributing information, as transmitting a meaningful message (e.g. a page of a book) gives the capability of distributing randomness, while the opposite is not necessarily true. In contrats with Shannon's classical theory of communication, where randomness and information are treated on a same footing, quantum theory of communication seems to indicate that randomness and information are truly inequivalent resources. This is shown by exhibiting quantum channels that are noisy for information communication, but behave as virtually noiseless channels for randomness distribution. In this project, we propose to transform this initial evidence into a final rigourous proof and to expand the family of quantum channels where this phenomenon is observed.

8. New representation of the boson sampling problem

R. Garcia-Patron (raulgarciapatron@gmail.com) and N. Cerf (ncerf@ulb.ac.be)

Quantum computers hold the promise to solve important computational problems much faster than today's computers. Despite its most elementary building blocks (quantum gates) have been experimentally demonstrated, it has proven to be very challenging to scale a quantum computer up to a size that would be relevant to solve real-life problems. It was recently been shown that a restricted quantum computational model, called boson sampling, seems to be sufficient to demonstrate a separation between the power of quantum and classical computers, even if it does not reach the full power of quantum computation. The boson sampler works by combining single-photon sources, linear optical circuits (a multimode interferometer composed of beamsplitters and phase shifters) and single-photon detectors. Despite the simplicity of this scheme, accessing its amplitude probabilities boils down to compute the permanent of a matrix (akin to its determinant but without alternating signs), which is a computationally hard task (in contrast to computing the determinant). In this project we will use the connection (isomorphism) between a system of N photons scattered over M modes and a system of N ions with M distinct level states in order to simplify some elements of the boson-sampling proof. In a second step, we will buid a toolbox of operations to simulate boson-sampling into an ion-trap.

9. Multiple-access and broadcast capacities of quantum optical channels

R. Garcia-Patron (raulgarciapatron@gmail.com), M. Jabbour (mjabbour@ulb.ac.be), and N. Cerf (ncerf@ulb.ac.be)

In order to find the fundamental limits that physics imposes to our communication capabilities over optical channels, it is indispensable to consider the potential advantage obtained by exploiting quantum effects. Indeed, light is ultimately made of photons, which must be described within a quantum formalism. Recently, the solution of the ultimate capacity of a single-mode optical link between an emitter and a receiver was obtained by members of QuIC/ULB and collaborators, showing that a set of simple quantum optical gaussian states gives the optimal encoding strategy. In this project, we will extend this recent result to the more general setting of a single emitter communicating to multiple receivers (also called *broadcasting* scenario), and to the dual situation of a single receiver but multiple emitters (also called *multiple-access* scenario).

10. Application of the replica method in quantum optics

M. Jabbour (mjabbour@ulb.ac.be) and N. Cerf (ncerf@ulb.ac.be)

The replica method has been introduced in statistical physics, as a tool to access the particition function of disordered systems. It has also been proven successul in quantum field theory as a means to calculate the von Neumann entropy of a quantum system that circumvents the need for diagonalizing its density matrix. It relies on finding an analytical expression for tr(ρ^n) with an integer number n of replicas. Then, by analytical continuation, the variable n is considered real and the entropy is accessed via the derivative of -tr(ρ^n) with respect to n at $n=1$. The mathematical justification is connected to Hausdorf's moment problem (translated for density matrices), which gives necessary and sufficient conditions for the moments of a distribution to uniquely determine this distribution, hence its entropy which is the expectation value of the -ln(ρ).

The replica method has been applied to a quantum optics problem for the first time by researchers at QuIC/ULB, and the present project aims at pursuing this recent and promising research direction. The replica method gives a invaluable method to access the entropy of the reduced state at the output of an optical parametric amplifier, which cannot be accessed otherwise as a result of the infinite dimension of the Fock space. In this master project, we will apply the replica method to the entropic characterization of general quantum Gaussian channels. In particular, we expect that some simple, yet unproven conjectures may become solvable using this technique. For example, we will address the entropic photon-number inequality that is conjectured to hold for quantum Gaussian channels.