Journée Informatique Quantique

Paris, 22 septembre 2010
Institut Henri Poincaré, salle 314

Programme

09.30	Coffee	
10.00	Expose de bienvenue	
10.15	Oded Regev	*Quantum One-Way Communication is Exponentially Stronger Than Classical Communication*
11.00	Andre Chailloux	*Lower Bounds for Quantum Oblivious Transfer*
11.30	Loick Magnin	*Deutsch-Josza Algorithm With Continuous Variables*
12.00	LUNCH (not provided)	
14.00	Simon Perdrix	*Quantum Information Processing with Graphs*
14.30	Damian Markham	*Measurement Based Quantum Computation on Fractal Lattices*
15.00	Pablo Arrighi	*A quantum extension of Gandy's theorem: Church-Turing thesis and quantum theory*
15.30	Discussions/Coffee	
16.15	Frederic Magniez	*Finding is as easy as detecting for quantum walks*
16.45	Ansis Rosmanis	*Quantum snake walk on the glued trees graph*

Abstracts

Title: Quantum One-Way Communication is Exponentially Stronger Than Classical Communication
Speaker: Oded Regev, Tel Aviv University (joint work with Boaz Klartag)

In STOC 1999, Raz presented a (partial) function for which there is a quantum protocol communicating only $O(\log n)$ qubits, but for which any classical (randomized, bounded-error) protocol requires $\poly(n)$ bits of communication. That quantum protocol requires two rounds of communication. Ever since Raz's paper it was open whether the same exponential separation can be achieved with a quantum protocol that uses only one round of communication. In other words, can quantum one-way communication be exponentially stronger than classical two-way communication? Here we settle this question in the affirmative.

NOTE: This talk is about lower bounds for *classical* communication complexity, so it does not require any knowledge in quantum communication complexity

Title: Lower Bounds for Quantum Oblivious Transfer
Speaker: André Chailloux, LRI-Univ Paris Sud (joint work with Iordanis Kerenidis, Jamie Sikora)

Oblivious transfer is a fundamental primitive in cryptography. While perfect information theoretic security is impossible, quantum oblivious transfer protocols can limit the dishonest players' cheating. Finding the optimal security parameters in such protocols is an important open question. In this paper we show that every 1-out-of-2 oblivious transfer protocol allows a dishonest party to cheat with probability bounded below by a constant strictly larger than 1/2. Alice's cheating is defined as her probability of guessing Bob's index, and Bob's cheating is defined as his probability of guessing both input bits of Alice. In our proof, we relate these cheating probabilities to the cheating probabilities of a coin flipping protocol and conclude by using Kitaev's coin flipping lower bound. Then, we present an oblivious transfer protocol with two messages and cheating probabilities at most 3/4.

Title: Deutsch-Josza Algorithm With Continuous Variables
Speaker: Loick Magnin, LRI - Univ Paris Sud (Joint work with Nicolas J. Cerf, Peter Hoyer and Bary C. Sanders.)

We investigate oracle problems in the context of continuous variables. The problem being discrete the work focus on the encoding of qubits into system described by infinite dimensional Hilbert spaces and the analysis of the errors resulting of such an encoding. This setup can be applied to a large family of problems, and we show that for the Deutsch-Josza problem, we can restrict ourselves to the use of Gaussian resources but the oracle.

Title: Quantum Information Processing with Graphs
Speaker: Simon Perdrix, LIG Univ Grenoble, CNRS (joint work with Mehdi Mhalla, Mio Murao, Masato Someya, Peter S. Turner)

Graph states are an elegant and powerful quantum resource for measurement based quantum computation (MBQC). They are also used for many quantum protocols (error correction, secret sharing, etc.). The main focus of this paper is to provide a structural characterization of the graph states that can be used for quantum information processing. The existence of a gflow (generalized flow) is known to be a requirement for open graphs (graph, input set and output set) to perform uniformly and strongly deterministic computations. We weaken the gflow conditions to define two new more general types of MBQC: uniform equiprobability and constant probability. These classes can be useful from a cryptographic and information point of view because even though we can not do a deterministic computation in general we can preserve the information and transfer it perfectly from the inputs to the outputs. We derive simple graph characterizations for these classes and prove that the deterministic and uniform equiprobability classes collapse when the cardinalities of inputs and outputs are the same. We also prove the reversibility of gflow in that case. The new graphical characterizations allow us to go from open graphs to graphs in general and to consider this question: given a graph with no inputs or outputs fixed, which vertices can be chosen as input and output for quantum information processing? We present a characterization of the sets of possible inputs and outputs for the equiprobability class, which is also valid for deterministic computations with inputs and outputs of the same cardinality.

Title: Measurement Based Quantum Computation on Fractal Lattices
Speaker: Damian Markham, LTCI Telecom ParisTech, CNRS (joint work with Vlatko Vedral, Janet Anders and Michel Hajdusek)

In this work we investigate how fractal lattices can be used to perform measurement based quantum computation. We find fractal lattices of arbitrary dimension greater than one which do all act as good resources for one-way quantum computation, and sets of fractal lattices with dimension greater than one all of which do not. The difference is put down to other topological factors such as ramification and connectivity. This is in direct analogy to the tendency of lattices to observe criticality in spin systems. The anaology between thermodynamics and one-way computation in this context will be discussed also. This work adds confidence to the analogy and highlights new features to what we require for universal resources for one-way quantum computation.

Title: A quantum extension of Gandy's theorem: Church-Turing thesis and quantum theory
Speaker: Pablo Arrighi, ENS Lyon (joint work with Gilles Dowek)

We tackle the question of the interplay between computability and quantum theory, in a way that is inspired by Gandy. Gandy formulates postulates about physics, such as homogeneity of space and time, bounded density and velocity of information --- and proves that the physical Church-Turing thesis is a consequence of these postulates. The authors provide a quantum extension of the result.

Title: Finding is as easy as detecting for quantum walks.
Speaker: Frédéric Magniez, LRI Univ Paris Sud, CNRS (joint work with Hari Krovi, Maris Ozols, Jérémie Roland)

We solve an open problem by constructing quantum walks that not only detect but also find marked vertices in a graph. The number of steps of the quantum walk is quadratically smaller than the classical hitting time of any reversible random walk P on the graph. Our approach is new, simpler and more general than previous ones. Contrary to previous approaches, our results remain valid when the random walk P is not state-transitive, and in the presence of multiple marked vertices. As a consequence we make a progress on an open problem related to the spatial search on the 2D-grid.

Title: Quantum snake walk on the glued trees graph
Speaker: Ansis Rosmanis, Univ Waterloo

We introduced the continuous-time quantum snake walk in order to construct a quantum algorithm efficiently solving a particular pathfinding problem on the glued trees graph, that is, finding a path connecting both roots of the glued trees graph. I will start this talk by analyzing the behavior of the continuous-time quantum snake walk on a simple graph - the infinite line. Then I will show that a very similar analysis helps us to understand how this walk behaves on the glued trees graph, and how to exploit it to construct an algorithm solving our problem. However, it is still not clear if the proposed algorithm works efficiently. Finally, I will present recently obtained numerical data which, unfortunately, suggest that this might not be the case.