Mini-workshop on quantum information theory

Oct 16-18, University of Auckland

Organised by André Nies

Oct 16, **Oct 17, Oct 18**, **2-3** pm

Marco Tomamichel, University of Technology, Sydney
Minicourse on Quantum Information Theory

OGGB (Owen G. Glen Building, the business school)
Monday and Tuesday 260-223, Wednesday 260-325

Oct 17 (Tue) activities all day

10am, 303-610
Cristian Calude, Department of Computer Science, UoA
A Quantum Random Generator Certified by the Kochen-Specker Theorem

11am, 303-B05
Tutorial and discussion session for Marco's lectures

2pm, 260-223 Marco's second lecture

3:10 pm, 303-310
Willem Fouche, Department of Decision Sciences, Unisa, Pretoria
Complexity aspects of the Solovay-Kitaev theorem

4:10 pm, 303-310
Anuradha Mahasinghe, Department of Mathematics, University of Colombo
An introduction to quantum walks on graphs

5:10 pm 303-610
Andre Nies, Department of Computer Science, UoA
Quantum Martin-Löf randomness

Abstracts

Marco Tomamichel, University of Technology, Sydney
Minicourse on Quantum Information Theory

The goal of this lecture series is to recapitulate basic notions of quantum information theory, as well as giving a taste of two of its application areas, quantum Shannon theory and quantum cryptography. I will attempt to be mathematically precise throughout, sacrificing broadness in order to achieve depth by focussing on particular examples.

In the first lecture, which will be supplemented by exercises, I will review the mathematical formalism of quantum information theory: the modeling of observables, states, channels and multipartite quantum systems. I will then put particular emphasis on measures of information: entropy, conditional entropy and mutual information and show how their most important mathematical properties can be derived from a single principle, the data-processing inequality of relative entropy.

The second lecture will give a taste of quantum Shannon theory, following the footsteps of one of its pioneers, Alexander Holevo. Looking at the continuous state space of a single qubit system one might wonder whether it is possible to encode an arbitrary amount of information in a qubit. We will show that this is in fact not possible by leveraging on the mathematical toolkit introduced in the first lecture.

The third lecture will outline the proof of an uncertainty relation expressed in terms of conditional entropies. This relation has conceptual value helping to shape our understanding of quantum mechanics, but it also serves as the basis of the proof of the security of quantum key distribution. We will quickly discuss both of these directions.

The lectures will be accompanied by a short script, and do not build on prior knowledge of quantum or information theory. (Whenever they fail to achieve this goal, the lecturer will be happy to fill in the gaps.)

Reference: arXiv:1504.00233

Cristian Calude, Department of Computer Science, UoA
A Quantum Random Generator Certified by the Kochen-Specker Theorem

We present the theory, realisation and qualitative analysis of a quantum random generator certified by the Kochen-Specker Theorem.
Joint work with A. A. Abbott, C. S. Calude, J. Conder, N. Huang and K. Svozil.

A. A. Abbott, C. S. Calude, J. Conder and K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness, Physical Review A 86, 6 (2012), https://journals.aps.org/pra/abstract/10.1103/PhysRevA.86.062109.
A. A. Abbott, C. S. Calude and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness, Journal of Mathematical Physics 56 (2015), http://dx.doi.org/10.1063/1.4931658.
A. Kulikov, M. Jerger, A. Potocnik, A. Wallraff, A. Fedorov. Realization of a quantum random generator certified with the Kochen-Specker theorem, 2017, https://arxiv.org/pdf/1709.03687.pdf.

Willem Fouche, Department of Decision Sciences, Unisa, Pretoria
Complexity aspects of the Solovay-Kitaev theorem

I consider algorithmic and complexity issues around the effective construction of quantum circuits. We discuss an algorithmic construction which, for any finite but universal set of computable quantum gates and a given measurement basis, will produce a rational quantum circuit whose shortest epsilon-approximations from products of instances of the gates have sizes which grow at least exponentially in the input sizes of the circuits and logarithmically in the reciprocal of epsilon.

I will also discuss the constructive content of the Solovay-Kitaev theorem by considering the algorithmic enumeration of all quantum circuits of a given input size. Finally we introduce the problem of identifying algorithmically random d-dimensional quantum gates.

Anuradha Mahasinghe, University of Colombo
An introduction to quantum walks on graphs

The quantum walk can be regarded a framework for quantum computation. We present several attempts of solving computational problems in the quantum walk framework, particularly the graph isomorphism problem. Then we consider some recent works on the physical implementation of quantum walks, as well as several remarks on the advances in the quantum circuit framework.
References: arXiv:0706.0304, arXiv:1605.07710

Andre Nies, UoA (joint work with Volkher Scholz, ETH Zurich)
Quantum Martin-Löf randomness

We introduce the mathematical background for infinite sequences of quantum bits. They can be seen as states of a certain C* algebra related to spin chains from quantum physics. We then generalise Martin-Loef's notion of randomness to this new setting, discuss examples, universal tests, and an analog of the Levin-Schnorr theorem. arXiv:1709.08422