Workshop: Quantum Information in Scotland 2018a

Organised by the QUISCO Network

January 30th, School of Informatics University of Edinburgh

BOOK OF ABSTRACTS

(alphabetical according to speaker)

Speaker: **Cristian Bonato** (Heriot Watt)

Title: *"Bayesian estimation for quantum sensing"*

Abstract: Sensors based on individual quantum systems hold great promise to deliver measurements of physical quantities combining nanoscale spatial resolution and high-sensitivity. For example, quantum sensing based on single spins associated with nitrogen-vacancy centres in diamond has already reached outstanding milestones in mapping nanoscale magnetic fields of interest for materials science and biology. Bayesian estimation is a natural way to use efficiently all the information available from experimental measurements. Additionally, Bayesian estimation can be easily interfaced with real-time feedback, providing 'on-the-fly' adaptation of the measurement settings to deliver, at each point in time, optimal information extraction based on the knowledge accumulated so far.

In this talk, I will describe our experimental[1] and theoretical work[2] related to the optimization of quantum sensing based on Bayesian estimation and real-time feedback.

[1] C. Bonato et al., Nature Nanotechnology 11, 247 (2016)
[2] C. Bonato et al., Phys Rev A 95, 052348 (2017)

Speaker: **Tom Douce** (Edinburgh)

Title: *"Quantum advantage and fault tolerant quantum computing in continuous variables"*

Abstract: Continuous Variables are a promising platform for demonstrating large scale quantum information effects thanks to the experimental advantages they provide. In this framework, we define a general quantum computational model based on a continuous variables hardware. It consists in vacuum input states, a finite set of gates — including non-Gaussian elements — and homodyne detection. We show that this model enables the encoding of fault tolerant universal quantum computing. Furthermore, when restricted to only commuting gates it turns into a sampling problem that can't be simulated efficiently with a classical computer — unless the polynomial hierarchy collapses. Thus we provide a simple paradigm for short-term experiments relying on Gaussian states, homodyne detection and some form of non-Gaussian evolution.

Speaker: **Kieran Flatt** (Glasgow)

Title: *"Gleason-Busch theorem for sequential measurements"*

Abstract: Gleason's theorem is a statement that, given some reasonable assumptions, the Born rule used to calculate probabilities in quantum mechanics is unique. We show that Gleason's theorem contains within it also the structure of sequential measurements, and along with this the state update rule. We give a small set of axioms, which are physically motivated, from which the familiar Kraus operator form follows.

Speaker: **Andru Gheorghiu** (Edinburgh)

Title: *"On the implausibility of classical client blind quantum computing"*

Abstract: Suppose a large scale quantum computer becomes available over the Internet. Could a client delegate universal quantum computations to this server, using only classical communication, in a way that is information-theoretically blind (i.e., the server learns nothing about the input apart from its size, with no cryptographic assumptions required)? In our work we give indications that the answer is no. This contrasts with the situation where quantum communication between client and server is allowed --- where we now know, from work over the past decade, that such information-theoretically blind quantum computation is possible. It also contrasts with the case where cryptographic assumptions are allowed: there again, it is now known that one can perform quantum fully homomorphic encryption with a classical client.

In more detail, we observe that, if there exist information-theoretically secure classical schemes for performing universal quantum computations on encrypted data, then we get unlikely containments between complexity classes. Specifically, we show that there is an oracle separating the class of problems solvable by certain classical client delegated computation schemes and the class of problems that are efficiently solvable by a quantum computer. We then also show that having such schemes for quantum sampling problems, such as boson sampling, leads to the existence of unlikely circuits for computing the permanent of a matrix.

We also consider encryption schemes which allow one round of quantum communication and polynomially many rounds of classical communication, yielding a generalisation of blind quantum computation. We give a complexity theoretic upper bound on the types of functions that admit such a scheme. This upper bound then lets us show that, under plausible complexity assumptions, such a protocol is no more useful than classical schemes for delegating NP-hard problems to the server. Lastly, we comment on the implications of these results for the prospect of verifying a quantum computation through classical interaction with the server. We argue that if such a procedure is possible, then it must either reveal much of the computation to the quantum computer or rely on computational assumptions.

Speaker: **Chris Heunen** (Edinburgh)

Title: *"How to realise arbitrary (in)compatibilities with quantum observables"*

Abstract: Quantum observables famously need not be compatible, in the sense that they need not be accurately measurable simultaneously. This holds for both projection-valued measures and the more general positive-operator valued measures. Now, if I give you a graph, can you always label the vertices with measurements so that any two are compatible if and only if they are connected by an edge? More generally, if I give you a

hypergraph, can you always label the vertices with measurements so that anu number of them are compatible if and only if they form a hyperedge? The answer is yes: quantum theory realises arbitrary (in)compatibilities. I will explain how.

Speaker: **Marco Piani** (Strathclyde)

Title: *"A formalism for steering with local quantum measurements"*

Abstract: We develop a unified approach to classical, quantum and post-quantum steering. The framework is based on uncharacterised (black-box) parties performing quantum measurements on their share of a (possibly unphysical) quantum state, and its starting point is the characterisation of general no-signalling assemblages via non-positive local hidden-state models. By developing a connection to entanglement witnesses, this formalism allows for new definitions of families of assemblages, in particular via (i) non-decomposable positive maps and (ii) unextendible product bases. The former proves to be useful for constructing post-quantum assemblages with the built-in feature of yielding only quantum correlations in Bell experiments, while the latter always gives certifiably post-quantum assemblages. Finally, our framework is equipped with an inherent quantifier of post-quantum steering, which we call the negativity of post-quantum steering. We postulate that post-quantum steering should not increase under one-way quantum operations from the steered parties to the steering parties, and we show that, in this sense, the negativity of post-quantum steering is a convex post-quantum-steering monotone.

Speaker: **Aidan Strathearn** (St. Andrews)

Title: *"Efficient non-Markovian quantum dynamics using time-evolving matrix product operators"*

Abstract: Modelling realistic quantum devices requires an understanding of quantum systems strongly coupled to their environment. Describing such strong coupling, and the non-Markovianity that accompanies it, analytically is extremely challenging and for consistently reliable results one must turn to numerical methods. To date, the available methods are either restricted to specific special cases or are limited in scope due to huge computational requirements. Here we present a novel and general numerical approach to efficiently describe the time evolution of a quantum system coupled to a non-Markovian environment.

Within the path integral description of open quantum systems, environmental degrees of freedom are integrated out to leave an influence functional of system trajectories only. This influence functional then describes all dissipative and non-Markovian physics occurring in the system due to the environment, though performing the remaining path integration over system trajectories is intractable in general. Here we show that discretising the system trajectories allows the path integral to be written as a tensor network which can be efficiently contracted. We build upon augmented density tensor methods in which the current state of the system and its previous history are stored in a large dimensional tensor. We show that this tensor can be efficiently represented as a matrix product state, and that contracting the tensor network which represents the path integral influence functional can be carried out by iteratively propagating such a matrix product state.

We demonstrate the power and flexibility of our method, which we call ``time-evolving matrix product operators'' (TEMPO), by addressing two contrasting problems. First we identify the the localisation transition in the Ohmic spin-boson model, both for the spin-

1/2 and spin-1 cases, which is numerically challenging due to the transition being of infinite order. Next we look at the problem of a pair of interacting spins embedded in a common environment. Here we can clearly see the effects of excitations traveling between the spins through the environment; a highly non-Markovian phenomenon for which no other methods are suitable for studying.

Based on: A. Strathearn, P. Kirton, D. Kilda, J. Keeling and B. W. Lovett, arXiv:1711.09641

Speaker: **Jacopo Surace** (Strathclyde)

Title: *"Local out-of-equilibrium dynamics of many-body quantum systems"*

Abstract: In order to overcome the exponential complexity inherent to the simulation of the out-of-equilibrium dynamics of many-body quantum systems with classical computers, we devise a strategy that focuses only on local correlations.

We benchmark it in the exactly solvable framework of quadratic fermionic systems and interpret the results in terms of the spreading of correlations.