9:00-10:00 Short talks (20min × 3)

Tyson Jones (Oxford University)

Title: Eigensolving in imaginary time

Abstract: Finding the energy spectrum of a quantum system is an important task, useful for example in analysing chemical reactions. While diagonalising the Hamiltonian is prohibitively expensive on a classical computer, it may soon become possible on near-future quantum-classical hybrid computers. Previous algorithms for eigensolving using such hardware required deep circuits or many measurements. We introduce a low depth, variational eigensolver based on imaginary time evolution which drives the system into energy eigenstates, which are subsequently penalised with the recently proposed swap-test. We test our algorithm on molecular and optimisation problem Hamiltonians, where it outperforms canonical gradient-based methods.

Suguru Endo (Oxford University)

Title: Practical error mitigation for near-future applications

Abstract: It is vital to minimize the impact of errors for near-future quantum devices that will lack the resources for full fault tolerance. Two quantum error mitigation (QEM) techniques have been introduced recently, namely, error extrapolation [Y. Li and S. C. Benjamin, Phys. Rev. X 7, 021050 (2017); K. Temme et al., Phys. Rev. Lett. 119, 180509 (2017)] and quasiprobability decomposition [K. Temme et al., Phys. Rev. Lett. 119, 180509 (2017)]. To enable practical implementation of these ideas, here we account for the inevitable imperfections in the experimentalist's knowledge of the error model itself. We describe a protocol for systematically measuring the effect of errors so as to design efficient QEM circuits. We find that the effect of localized Markovian errors can be fully eliminated by inserting or replacing some gates with certain single-qubit Clifford gates and measurements. Also, we also verify that algorithmic errors in the Trotter decomposition due to the insufficiency of the discritization of the simulated time can be mitigated by using extrapolation method.

Kosuke Mitarai (Osaka University)

Title: Improving Efficiency of Variational Quantum Eigensolver

Abstract: Recent progress in experimental realization of quantum computers are stimulating the research of their possible applications. Quantum computers which might realize in near-future are conveniently called noisy intermediate-scale quantum (NISQ) device. Among possible applications of NISQ, variational quantum algorithms have recently attracted much attention. Probably the most famous one is variational quantum eigensolver (VQE). VQE aims to find a ground state of a given

Hamiltonian, by optimizing the parameter implemented on a quantum circuit to generate ansatz states. We propose a new approach that improves efficiency of VQE to make it more practical.

10:00-10:45 Michael Bremner

Title: The challenge of developing post-classical applications with noisy quantum computers

Abstract: Over the last few years significant attention has been devoted to devising experimental demonstrations of quantum computational supremacy: namely using a quantum computer to perform a computational task in a regime that goes beyond what is possible on a classical, digital, machine. This is, in part, driven by the hope that a clear demonstration of post-classical computation can be performed with a device that is intermediate between the small quantum circuits that can currently be built and a full-scale, fault-tolerant, quantum computer. The theoretical challenge that this poses is twofold: firstly we must identify the physically least expensive quantum computations that are classically unachievable; and we must also determine if this advantage can be maintained in realistic physical systems. In this talk I will discuss the IQP, Boson Sampling, and chaotic circuit approaches to quantum computational supremacy, how they can be generalized to other intermediate quantum computing models, and to what extent the experimental resource requirements of these problems can be reduced.

This talk is based on joint work with:

[1] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Achieving quantum supremacy with sparse and noisy commuting quantum computations", Quantum 1, 8 (2017). arXiv:1610.01808

[2] M. J. Bremner, A. Montanaro, and D. J. Shepherd "Average-case complexity versus approximate simulation of commuting quantum computations", Phys. Rev. Lett. 117, 080501 (2016). arXiv:1504.07999

[3] S. Boixo, et al, "Characterizing quantum supremacy in near-term devices", Nature Physics 4, 595 (2018). arXiv:1608.00263.

[4] A. Lund, M. J. Bremner, T. C. Ralph "Quantum sampling problems, BosonSampling and quantum supremacy", npj Quantum Information 3, Article number: 15 (2017). arXiv:1702.03061

[5] R. Mann and M. J. Bremner, "On the Complexity of Random Quantum Computations and the Jones Polynomial", arXiv:1711.00686.

10:45-11:30 Bill Fefferman

Title: "Quantum Supremacy" and the Complexity of Random Circuit Sampling

Abstract: A critical goal for the field of quantum computing is quantum supremacy -- a demonstration of a quantum computation that is prohibitively hard for classical computers. Besides dispelling any skepticism about the experimental viability of quantum computers, quantum supremacy also provides a test of quantum theory in the realm of high complexity. A leading near-term candidate, put forth by the Google/UCSB team, is sampling from the probability distributions of randomly chosen quantum circuits, called Random Circuit Sampling (RCS). While RCS was defined with experimental realization in mind, we give complexity-theoretic evidence of classical hardness of RCS, placing it on par with the best theoretical proposals for supremacy. Specifically, we show that RCS satisfies an average-case hardness condition -- computing output probabilities of typical quantum circuits is as hard as computing them in the worst-case, and therefore #P-hard. Our reduction exploits the polynomial structure in the output amplitudes of random quantum circuits, enabled by the Feynman path integral. We also describe a new verification measure which in some formal sense maximizes the information gained from experimental samples.
Based on joint work with Adam Bouland, Chinmay Nirkhe and Umesh Vazirani.

11:30-13:30 lunch

13:30-14:15 Dominik Hangleiter

Title: Verification vs. Approximate sampling: How hard is it to verify "quantum supremacy"?

Abstract: Devising schemes showing a quantum speedup that are feasible in the near future has become a central milestone in the field of quantum simulation and computation. Most of the suggested schemes are based on the natural quantum task of *sampling* from the output distribution of certain unitaries applied to a reference state. In this talk, I will discuss how two properties required of such schemes of "quantum supremacy" are related: the hardness results need to be robust against errors and a (quantum) device sampling from the relevant distributions should efficiently verifiable. I will show that a single property of the sampled distribution, namely, its second moments, is crucial for both of these properties to be satisfied. The result shows that for prominent examples of approximate-sampling "supremacy" schemes, verification from polynomially many classical samples is impossible. This is the case, in particular, for Boson Sampling, universal random circuit sampling and IQP circuit

sampling. In the last part of the talk, I will sketch how using structure specific to a quantum sampler or a particular architecture may give rise to feasible schemes with both properties: approximate sampling is classically intractable and they are efficiently verifiable.
Joint work with Martin Kliesch, Jens Eisert, and Christian Gogolin.

14:15-15:00 Zhenfeng Ji

Title: A Complexity-Theoretic Bell Inequality
Abstract: The Bell inequality is one of the most important and foundational results of quantum physics named after its inventor John Stewart Bell. The inequality proves Einstein wrong and provides a concrete method to distinguish quantum mechanics from classical theories. We study Bell inequalities from a complexity theory perspective and show that the classical and quantum violations of a Bell inequality are not only different in value but are also different in terms of their computational complexity.

15:00-15:15 break

15:15-16:00 Masahito Hayashi

Title: Verification of Measurement-Based Quantum Computation
Abstract: Quantum computation offers a novel way of processing information and promises solution of some classically intractable problems. However, if the component of the quantum computer has some errors, it does not output a correct computation outcome. Since the quantum computer is composed of several components, the unexpected correlation causes unexpected error that cannot be corrected by error correction. To resolve this problem, we need to verify the quantum computer. If a problem is in NP, we can verify the correctness of a solution, but a problem that we want to solve with a quantum computer is not necessarily in NP. We need to verify quantum computer. Usually a quantum computer is composed of a combination of so many quantum circuits. It is not easy to predict the outcome of the combination of so many quantum circuits. That is, since we do not know the computation outcome, we cannot verify the computation outcome by itself. To resolve this problem, we employ measurement-based quantum computation (MBQC). MBQC is composed of graph state

and local measurements, which are known to us. In particular, the computation resource is given as the quantum correlation of the graph state, which is in a known form. Hence, we can verify these components by using the method of statistical hypothesis testing. In this talk, we consider the following three settings.

(1) We perfectly trust our local measurement. So, we need to verify only the graph state.

(2) We trust local measurement, but it is noisy. The noise can be converted to noise of graph state. So, we need to verify only the noisy graph state. This protocol works with noisy graph state.

(3) We do not trust measurement as well as graph state. However, it accept only the case when the measurement and the graph state are noiseless.

Setting (3) has weakest assumption, but it works with ideal case. Setting (2) has stronger assumption, but it works with realistic case. Further, our verification scheme can be applied to the blind quantum computation. In addition, as an extension of (1), we consider the following topic.

(4) MBQC with hypergraph state, and its verification.

This talk is based on joint works with T. Morimae, K. Fujii, M. Hajdusek, Y. Takeuchi, and H. Zhu. The detail is available in

Phys. Rev. Lett. 115, 220502 (2015), Phys. Rev. A 96, 030301(R) (2017), Phys. Rev. A 96, 062321 (2017), Phys. Rev. A 97, 052308 (2018), and arXiv:1806.05565

16:00-16:45 Sevag Gharibian

Title: Towards Quantum One-Time Memories from Stateless Hardware

Abstract: A central tenet of theoretical cryptography is the study of the minimal assumptions required to implement a given cryptographic primitive. One such primitive is the one-time memory (OTM), introduced by Goldwasser, Kalai, and Rothblum [CRYPTO 2008], with applications in areas ranging from software protection to money. It is known that secure OTMs do not exist in the "plain" classical and quantum computation models. Hence, we ask: What are the minimal additional assumptions needed in order to enable OTMs?

In this work, we propose a scheme for using quantum information, together with the assumption of stateless hardware tokens, to build statistically secure OTMs. Via the semidefinite programming-based quantum games framework of Gutoski and Watrous [STOC 2007], we prove our scheme is secure against an arbitrary quantum adversary making a linear number of adaptive queries to the token. We conjecture our scheme is secure against a polynomial number of adversarial queries. Our scheme is technologically simple, being of the “prepare-and-measure” type, and our security proof is in the desirable quantum universal composability framework, ensuring composability with other cryptographic primitives. Finally, we show our scheme is "tight” according to two scenarios.

Joint work with Anne Broadbent (University of Ottawa) and Hong-Sheng Zhou (Virginia Commonwealth University).

16:45-17:45 Short talks (20min × 3)

Yuki Takeuchi (NTT)

Title: Resource-efficient verification of quantum computing using Serfling‘s bound

Abstract: In measurement-based quantum computing, checking whether correct graph states are generated or not is essential for reliable quantum computing. Several verification protocols for graph states have been proposed, but none of these are particularly resource efficient: Many copies are required in order to extract a single state that is guaranteed to be close to the ideal graph state. For example, the best protocol currently known requires $O(n^{15})$ copies of the state, where n is the size of the graph state [D. Markham {¥it et al}., arXiv:1801.05057 (2018)]. In this talk, we propose a significantly more resource-efficient verification protocol for graph states that needs only $O(n^5 ¥log{n})$ copies. The key idea that achieves such a drastic improvement is to employ Serfling’s bound, which is a probability inequality in classical statistics. Utilizing Serfling’s bound also enables us to generalize our protocol for qudit graph states and continuous-variable weighted hypergraph states.

This talk is based on joint work with Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, and Joseph F. Fitzsimons. The detail is given in arXiv:1806.09138.

Xiao Yuan (Oxford University)

Titile: Hypothesis testing and relative entropy of quantum channels

Abstract: Hypothesis testing is an important task in mathematics, physics, computer science, etc. Hypothesis testing of two random variables is related to the Kullback-Leibler divergence of the two corresponding distributions. Similarly, quantum hypothesis testing of two quantum states is characterised by the quantum relative entropy. In this talk, we extend hypothesis testing to general quantum channels. In both the one-shot and asymptotic scenario, we propose several quantifiers for hypothesis testing under different assumptions of how the channels are used. As the quantifiers are analog to the quantum relative entropy of states, we also call them the quantum relative entropy of channels. We investigate the properties that the quantum relative entropy of channels should satisfy and study its interplay with entanglement. We also consider several special examples for unitary channels and demolition measurements.

Andrew Darmawan (Kyoto University)

Title: Linear-time general decoding algorithm for the surface code

Abstract: A quantum error correcting protocol can be substantially improved by taking into account features of the physical noise process. We present an efficient decoder for the surface code which can account for general noise features, including coherences and correlations. We demonstrate that the decoder significantly outperforms the conventional matching algorithm on a variety of noise models, including non-Pauli noise and spatially correlated noise. The algorithm is based on an approximate calculation of the logical channel using a tensor-network description of the noisy state.