Aspen Winter Conference:

Aspen Winter Conference:
Advances in Quantum Algorithms and Computation
March 20-26, 2016
PROGRAM

SUNDAY - March 20

5:00 – 7:00 Opening Reception – Aspen Center for Physics

MONDAY - March 21
Session Chair: Krysta Svore

8:00 – 8:05 Welcome

8:05 – 8:45 Charlie Marcus – “Hybrid Qubits: Gatemons and Majoranas”

8:45 – 9:25 Robin Kothari – “Quantum linear systems algorithm with exponentially improved dependence on precision”

9:25 – 9:40 COFFEE BREAK

Session Chair: Neil Ross

9:40- 10:20 Stacey Jeffery – “nand-Trees, Average Choice Complexity and Effective Resistance”

10:20 – 10:40 Vadym Kliuchnikov – “Quaternion algebras and compiling”

MIDDAY BREAK

Session Chair: Sergio Boixo

4:15 – 4:55 Bettina Heim – “Numerical simulations as a tool for designing quantum annealing algorithms and hardware”

4:55 – 5:15 Helmut Katzgraber – “Weaknesses and strengths of weak-strong cluster problems”

5:15 – 5:30 COFFEE BREAK

Session Chair: Travis Humble

5:30 – 6:10 Vadim Smelyanskiy – “Scaling analysis and instantons for thermally-assisted tunneling and Quantum Monte Carlo simulations”

6:10 – 6:50 Wim van Dam – “Quantum Monte Carlo Simulations of Tunneling in Quantum Adiabatic Optimization”

TUESDAY - March 22
Session Chair: Cody Jones

8:00 – 8:40 Tim Taminiau – “Active quantum error correction in a diamond quantum processor”

8:40 – 9:20 Hector Bombin – “Resilience to time-correlated noise in quantum computation”

9:20 – 9:40 COFFEE BREAK

Session Chair: Will Zeng

9:40- 10:20 Ken Brown – “Error Models and Error Thresholds”

10:20 – 10:40 Tomas Jochym O’Connor – “Stacked codes: universal fault-tolerant quantum computation in a two-dimensional layout”

MIDDAY BREAK

Session Chair: Ryan Babbush

4:15 – 4:55 Alan Aspuru-Guzik – “Quantum simulation for chemistry: new advances and perspectives”

4:55 – 5:35 Joerg Schmiedmayer – “What can we learn from correlation measurements about quantum many body systems”

5:35 – 5:50 COFFEE BREAK

5:50 – 7:00 Poster Session

7:30 Group Dinner – Aspen Meadows

WEDNESDAY - March 23

Session Chair: Martin Roetteler

8:00 – 8:40 Rami Barends – “Digitized adiabatic quantum computing with a superconducting circuit”

8:40 – 9:20 Peter Love – “A quantum algorithm for the Moebius function”

9:20 – 9:40 COFFEE BREAK

Session Chair: Dave Clader

9:40- 10:20 Edward Farhi – “The Quantum Approximate Optimization Algorithm: A Good Choice for a Near Term Quantum Computer”

10:20 – 11:00 Dave Wecker – “LIQUi|> Tutorial”

1:00 – 3:00 Ski Race – Aspen Mountain

MIDDAY BREAK

4:30 – 5:30 Physics Café, Wheeler Opera House: Edward Farhi and Charlie Marcus

5:30 – 6:30 Public Lecture, Wheeler Opera House

THURSDAY - March 24
Session Chair: Robert Joynt

8:00 – 8:40 Andreas Wallraff – “Exploring Quantum Computation and Simulation with Superconducting Circuits”

8:40 – 9:20 Matthias Christandl – “Nondeterministic quantum communication complexity: the cyclic equality game and iterated matrix multiplication”

9:20 – 9:40 COFFEE BREAK

Session Chair: Nike Dattani

9:40 – 10:20 Shalev Ben-David – “Separations in Query Complexity using Cheat Sheets”

10:20 – 10:40 Barry Sanders – “Classical Heuristic-Based Machine Learning for Fast High-Fidelity Multi-Qubit Gates”

MIDDAY BREAK

Session Chair: Masoud Mohseni

4:15 – 4:55 Matt Hastings – “Towards Practical Quantum Variational Algorithms”

4:55 – 5:35 Sergey Bravyi – “Improved classical simulation of quantum circuits with a small T-count”

5:35 – 5:50 COFFEE BREAK

Session Chair: Aram Harrow

5:50 – 6:10 Ted Yoder – “Universal fault-tolerant gates on nondegenerate stabilizer codes”

6:10 – 6:30 Leonie Mueck – “Quantum Information at Nature and its sister journals”

7:30 Banquet Dinner – Aspen Meadows

FRIDAY - March 25
Session Chair: Ulrich Schollwoeck

8:00 – 8:40 Phillip Schindler – “Quantum algorithms and simulations with trapped ions”

8:40 – 9:20 Bela Bauer – “Hybrid quantum-classical approach to correlated materials”

9:20 – 9:40 COFFEE BREAK

Session Chair: Peter Hoyer

9:40 – 10:20 Scott Aaronson – “Three Paths to Quantum Supremacy”

10:20 – 10:40 Juan Bermejo-Vega – “Contextuality as a resource for qubit quantum computation”

MIDDAY BREAK

Session Chair:	Sean Hallgren
4:15 – 4:55	Benoit Valiron – “Quantum algorithms from the programmer's perspective”
4:55 – 5:15	Gorjan Alagic – “Quantum encryption and obfuscation”
5:15 – 5:30	COFFEE BREAK
Session Chair:	Matthias Troyer
5:30 – 6:10	Nathan Wiebe – “Quantum Bootstrapping”
6:10 – 6:50	Discussion – “What do experimentalists need from theorists (and vice versa)?”

SATURDAY - March 26

8:30 – 10:30	Discussion: Future applications of quantum computing

Aspen Winter Conference:
Advances in Quantum Algorithms and Computation
March 20-26, 2016
ABSTRACTS

Speaker: **Charlie Marcus**
Title: Hybrid Qubits: Gatemons and Majoranas

Abstract: This talk will review recent progress at the Center for Quantum Devices making use of hybrid materials made of epitaxially grown superconductors and semiconductors. I will focus on applications toward scalable quantum information hardware, future plans, novel aspects of these materials, and known unknowns.

Speaker: **Robin Kothari**
Title: Quantum linear systems algorithm with exponentially improved dependence on precision

Abstract: Harrow, Hassidim, and Lloyd showed that for a suitably specified N×N matrix A and N-dimensional vector b, there is a quantum algorithm that outputs a quantum state proportional to the solution of the linear system of equations Ax=b. If A is sparse and well-conditioned, their algorithm runs in time poly (log N, 1/ε), where ε is the desired precision in the output state. We improve this to an algorithm whose running time is polynomial in log(1/ε), exponentially improving the dependence on precision while keeping essentially the same dependence on other parameters. Our algorithm is based on a general technique for implementing any operator with a suitable Fourier or Chebyshev series representation. This allows us to bypass the quantum phase estimation algorithm, whose dependence on ε is prohibitive.

Speaker: **Stacey Jeffery**
Title: nand-Trees, Average Choice Complexity and Effective Resistance

Abstract: We show that the quantum query complexity of evaluating nand-tree instances with average choice complexity at most W is O(W), where average choice complexity is a measure of the difficulty of winning the associated two-player game. This generalizes a superpolynomial speedup over classical query complexity due to Zhan et al. We further show that the player with a winning strategy for the two-player game associated with the nand-tree can win the game with an expected O(N^{1/4}\sqrt{C(x)}) quantum queries against a random opponent, where C(x) is the average choice complexity of the instance. This gives an improvement over the query complexity of the naive strategy, which costs O(\sqrt{N}) queries.

The results rely on a connection between nand-tree evaluation and st-connectivity problems on certain graphs, and span programs for st-connectivity problems. Our results follow from relating average choice complexity to the effective resistance of these graphs, which itself corresponds to the span program witness size. Joint work with Shelby Kimmel.

Speaker: **Vadym Kliuchnikov**

Title: Quaternion algebras and compiling

Abstract: "We present an algorithm for efficiently approximating qubit unitaries over gate sets derived from totally definite quaternion algebras. It achieves ε-approximations using circuits of length O(log(1/ε)), which is asymptotically optimal. The algorithm achieves the same quality of approximation as previously-known algorithms for Clifford+T [arXiv:1212.6253], V-basis [arXiv:1303.1411] and Clifford+π/12 [arXiv:1409.3552], running on average in time polynomial in O(log(1/ε)) (conditional on a number-theoretic conjecture). Ours is the first such algorithm that works for a wide range of gate sets and provides insight into what should constitute a \""good\"" gate set for a fault-tolerant quantum computer. Our results also extend to finding provably optimal approximations and designing circuits with fallback.

Based on http://arxiv.org/abs/1510.03888, http://arxiv.org/abs/1504.04350 and new results in preparation. "

Speaker: **Bettina Heim**
Title: Numerical simulations as a tool for designing quantum annealing algorithms and hardware

Abstract: With quantum technology rapidly progressing, more sophisticated quantum annealing devices are starting to become available. While they promise new possibilities for solving classically hard optimization problems, their true potential remains a debated topic. Numerical simulations provide an indispensable tool not only for its assessment but also for designing annealing algorithms. As a good understanding of this tool is crucial, we discuss the difference between simulated quantum annealing as a classical optimization algorithm and its application for simulating quantum hardware.
We examine the traveling salesman problem to illustrate the value of simulations in the quest for problem classes that benefit from quantum effects, and discuss the aspects and challenges to consider when solving discrete optimization problems on quantum annealing hardware. We argue that a need for inequality constraints, in particular, presents a major hurdle for the implementation on analog devices.

Speaker: **Helmut Katzgraber**
Title: Weaknesses and strengths of weak-strong cluster problems

Abstract: To date, a conclusive detection of quantum speedup remains elusive.
Recently, a team by Google Inc. [arXiv:1512.02206] proposed weak-strong cluster problems tailored to have tall and narrow energy barriers separating local minima and to highlight the value of finite-range tunneling. In particular, results from quantum Monte Carlo simulations, as well as the D-Wave 2X quantum annealer scale considerably better than state-of-the-art simulated annealing simulations. Moreover, the D-Wave 2X quantum annealer is 10^8 times faster than simulated annealing on conventional computer hardware for problems with approximately 950 variables. Here, an overview of different sequential, standard, as well as specialized algorithms on the Google instances is given. We show that the quantum speedup is limited and study the typical complexity of the benchmark problems using insights from the study of spin glasses.

Work done in collaboration with Salvatore Mandra (Harvard University), Alejandro Perdomo-Ortiz (NASA), Zheng Zhu (Texas A&M University), Wenlong Wang (Texas A&M University)

Speaker: **Vadim Smelyanskiy**
Title: Scaling analysis and instantons for thermally-assisted tunneling and Quantum Monte Carlo simulations

Abstract:

Speaker: **Wim van Dam**
Title: Quantum Monte Carlo Simulations of Tunneling in Quantum Adiabatic Optimization

Abstract: We explore to what extent path-integral quantum Monte Carlo methods can efficiently simulate the tunneling behavior of quantum adiabatic optimization algorithms. Specifically we look at symmetric cost functions defined over n bits with a single potential barrier that a successful optimization algorithm will have to tunnel through. The height and width of this barrier depend on n, and by tuning these dependencies, we can make the optimization algorithm succeed or fail in polynomial time. In this article we compare the strength of quantum adiabatic tunneling with that of path-integral quantum Monte Carlo methods. We find numerical evidence that quantum Monte Carlo algorithms will succeed in the same regimes where quantum adiabatic optimization succeeds.

Speaker: **Tim Taminiau**
Title: Active quantum error correction in a diamond quantum processor

Abstract: Reliable quantum information processing in the face of errors is a major fundamental and technological challenge. Quantum error correction protects quantum states by encoding a logical quantum bit (qubit) in multiple physical qubits. To be compatible with universal fault-tolerant computations, it is essential that states remain encoded at all times and that errors are actively corrected. Here we demonstrate such active error correction on a continuously protected logical qubit using a diamond quantum processor. We encode the logical qubit in three long-lived nuclear spins, repeatedly detect phase errors by non-destructive measurements, and apply corrections by real-time feedback. The actively error-corrected qubit is robust against errors and encoded quantum superposition states are preserved beyond the natural dephasing time of the best physical qubit in the encoding. These results establish a powerful platform to investigate error correction under different types of noise and mark a step towards fault-tolerant quantum information processing.

Speaker: **Hector Bombin**
Title: Resilience to time-correlated noise in quantum computation

Abstract: Fault-tolerant quantum computation techniques rely on the noise being weakly correlated both in time and space. I will show that it is enough to assume weak spatial correlations. In particular, there exists a noise threshold for quantum memories under spatially local stochastic Pauli noise.

Speaker: **Ken Brown**
Title: Error Models and Error Thresholds

Abstract: The error threshold for fault-tolerant quantum computation depends strongly on the error model. Most calculations assume a depolarizing model, which allows for efficient calculations based on random applications of Pauli errors. We have been exploring how the threshold changes for both non-unital and coherent operations. I will present our results based on exact calculations of the Steane code pseudothreshold for different error models. I will also discuss whether the two-qubit depolarizing error model is an appropriate model for realistic two-qubit gates and how realistic models can lead to simpler fault-tolerant constructions.

Speaker: **Tomas Jochym O'Connor**
Title: Stacked codes: universal fault-tolerant quantum computation in a two-dimensional layout

Abstract: We introduce a new class of 3D color codes, which we call stacked codes, together with a fault-tolerant transformation that will map logical qubits encoded in 2D color codes into stacked codes and back. The stacked code allows for the transversal implementation of a non-Clifford logical T gate, which when combined with the logical Clifford gates that are transversal in the 2D color code give a gate set which is both fault-tolerant and universal without requiring non-stabilizer magic states. We then show that the layers forming the stacked code can be unfolded and arranged in a 2D layout. As only Clifford gates can be implemented transversally for 2D topological stabilizer codes, a non-local operation must be incorporated in order to allow for this transversal application of a non-Clifford gate. Our code achieves this operation through the transformation from a 2D color code to the unfolded stacked code induced by measuring only geometrically local stabilizers and gauge operators within the bulk of 2D color codes together with a non-local operator that has support on a 1D boundary between such 2D codes. We believe that this proposed method to implement the non-local operation is a realistic one for 2D stabilizer layouts and would be beneficial in avoiding the large overheads caused by magic state distillation.

Speaker: **Alan Aspuru-Guzik**
Title: Quantum simulation for chemistry: new advances and perspectives

Abstract: Since our last Aspen workshop, several new developments in the field of quantum computation and simulation and chemistry have been made by several research groups. I will try to provide an overview of the different developments. I will then focus on new sparse algorithms that our group has developed in collaboration with Dominic Berry and Peter Love, as they represent (as of the writing of the abstract) perhaps the best algorithms in the asymptotic limit for simulating molecules and matter in general. I will then move on to discuss the progress in the variational quantum eigensolver algorithm, both in the theory of it, as well as on progress towards several experimental realizations of it. I will conclude with a perspective of what to expect in the next year(s), and hopefully there will be much more to discuss at the next Aspen meeting."

Speaker: **Joerg Schmiedmayer**
Title: What can we learn from correlation measurements about quantum many body systems

Abstract: The knowledge of all correlation functions of a system is equivalent to solving the corresponding quantum many-body problem. If one can identify the relevant degrees of freedom, the knowledge of a finite set of correlation functions is in many cases sufficient to determine a sufficiently accurate solution of the corresponding field theory. Complete factorization is equivalent to identifying the relevant degrees of freedom where the Hamiltonian becomes diagonal. I will give examples how one can apply this powerful theoretical concept in experiment.

Speaker: **Rami Barends**
Title: Digitized adiabatic quantum computing with a superconducting circuit

Abstract: A major challenge in quantum computing is to solve general problems with limited physical hardware. We implement digitized adiabatic quantum computing, combining the generality of the adiabatic algorithm with the universality of the digital approach, using a superconducting circuit with nine qubits. We probe the adiabatic evolutions, explore the scaling of errors with system size, and quantify the success of the algorithm for random spin problems. We find that the system can approximate the solutions to both frustrated Ising problems and non-stoquastic problem Hamiltonians with a performance that is comparable.

Speaker: **Peter Love**
Title: A quantum algorithm for the Moebius function

Abstract: In this talk I will describe an efficient quantum algorithm for the Moebius function from the natural numbers to {-1,0,1} and discuss the algorithmic techniques used in this algorithm. While the Moebius function was previously known to be in BQP, I will present an algorithm that does not rely on factorization via Shor's algorithm as an intermediate step.

Speaker: **Edward Farhi**
Title: The Quantum Approximate Optimization Algorithm: A Good Choice for a Near Term Quantum Computer

Abstract: I will describe a quantum algorithm for approximate optimization and explain how to analyze its performance on all instances of particular combinatorial optimization problems. I will explain why this algorithm is well suited to run on small scale quantum computers because of its low circuit depth and simple gate structure. I will also explain that running this algorithm can demonstrate Quantum Supremacy because if a classical algorithm could efficiently sample its output then the Polynomial Hierarchy would collapse.

Speaker: **Dave Wecker**
Title: Quantum simulator for Academia

Abstract: We are releasing our state of the art quantum simulator (LIQUi|>) for academic use. The scope of the release and how the system may be used by classes and individuals will be presented.

Speaker: **Andreas Wallraff**
Title: Exploring Quantum Computation and Simulation with Superconducting Circuits

Abstract: The high level of control achievable over quantized degrees of freedom have turned superconducting circuits into one of the prime physical architectures for quantum computing and simulation. While conventional approaches mostly rely on unitary time evolution more recently open-system dynamics are considered for quantum information processing and simulations as well. In this talk, I will first give an introduction to superconducting quantum circuits. Then I will discuss a set of experiments in which we simulated the physics of interacting spins using a digital approach [1]. In a second set of experiments [2] we made use of an open cavity quantum electrodynamics (QED) system with tunable interactions to simulate the ground state of an interacting Bose gas confined in one dimension [3,4]. These experiments rely on our ability to efficiently measure higher order photon correlations of propagating microwave fields. To facilitate these measurements we developed a quantum limited amplifier achieving phase-preserving amplification at large bandwidth and high dynamic range [5]. Our results demonstrate an alternative path towards simulating complex quantum many-body physics based on the controlled generation and detection of non-classical radiation in open quantum systems.

[1] Y. Salathe et al., Phys. Rev. X 5, 021027 (2015).
[2] C. Eichler et al., Phys. Rev. X 5, 041044 (2015).
[3] S. Barrett et al., Phys. Rev. Lett. 110, 090501 (2013).
[4] F. Verstraete and J. I. Cirac, Phys. Rev. Lett. 104, 190405 (2010).
[5] C. Eichler et al., Phys. Rev. Lett. 113, 110502 (2014).

Speaker: **Matthias Christandl**
Title: Nondeterministic quantum communication complexity: the cyclic equality game and iterated matrix multiplication

Abstract: We study nondeterministic multiparty quantum communication with a quantum generalization of broadcasts. We show that, with number-in-hand classical inputs, the communication complexity of a Boolean function in this communication model equals the logarithm of the support rank of the corresponding tensor, whereas the `approximation' complexity in this model is characterized by the border support rank. This characterisation allows us to prove a log-rank conjecture posed by Villagra et al. for nondeterministic multiparty quantum communication with message-passing.

The support rank characterization of the communication model connects quantum communication complexity intimately to the theory of asymptotic entanglement transformation and algebraic complexity theory. In this context, we introduce the graphwise equality problem. For a cycle graph, the complexity of this communication problem is closely related to the complexity of the computational problem of multiplying matrices, or more precisely, it equals the asymptotic support rank of the iterated matrix multiplication tensor. We employ Strassen's laser method to show that asymptotically there exist nontrivial protocols for every odd-player cyclic equality problem. We exhibit an efficient protocol for the 5-player problem for small inputs, and we show how Young flattenings yield nontrivial complexity lower bounds. This is joint work with Harry Buhrman and Jeroen Zuiddam.

Speaker: **Shalev Ben-David**
Title: Separations in Query Complexity using Cheat Sheets

Abstract: We show a power 2.5 separation between bounded-error randomized and quantum query complexity for a total Boolean function, refuting the widely believed conjecture that the best such separation could only be quadratic (from Grover\'s algorithm). We also present a total function with a power 4 separation between quantum query complexity and approximate polynomial degree, showing severe limitations on the power of the polynomial method. Finally, we exhibit a total function with a quadratic gap between quantum query complexity and certificate complexity, which is optimal (up to log factors). These separations are shown using a new, general technique that we call the cheat sheet technique. The technique is based on a generic transformation that converts any (possibly partial) function into a new total function with desirable properties for showing separations. The framework also allows many known separations, including some recent breakthrough results of Ambainis et al., to be shown in a unified manner.

Speaker: **Barry Sanders**
Title: Classical Heuristic-Based Machine Learning for Fast High-Fidelity Multi-Qubit Gates

Abstract: We develop classical heuristic-based machine learning algorithms to devise quantum-control policies for designing fast multi-qubit logic gates. Our modified differential evolution algorithm enabled us to devise a policy for a fast high-fidelity single-shot Toffoli gate.

Speaker: **Matt Hastings**
Title: Towards Practical Quantum Variational Algorithms

Abstract: There is a long history of proposals to produce classes of variational states on a quantum computer, ranging from preparing PEPS and other tensor network states to more recently preparing unitary coupled cluster states. However, there has been little numerical work studying the actual performance of these schemes. We present such a study and we develop a new class of states, which we call "Hamiltonian variational", that offers improved performance; the improvement is most notable on larger systems entering the strongly interacting regime where a quantum computer would be most useful. Despite this, we argue that even with very optimistic speculations about future theoretical and hardware advances, variational methods will not be useful for problems in quantum chemistry, partly due to the large number of terms in the Hamiltonian which increases the statistical error. We suggest other applications where they may be useful, including strongly interacting model systems of condensed matter such as the Hubbard model and other uses inside other quantum algorithms. The Hamiltonian variational scheme is especially useful for models such as the Hubbard model where it allows a short circuit depth and small number of variational parameters. Joint work with Dave Wecker and Matthias Troyer.

Speaker: **Sergey Bravyi**
Title: Improved classical simulation of quantum circuits with a small T-count

Abstract: The famous Gottesman-Knill theorem asserts that a quantum circuit composed of Clifford gates can be efficiently simulated on a classical computer. We revisit this theorem and extend it to quantum circuits in the Clifford+T basis. We assume that the circuit outputs a bit string x obtained by measuring some subset of w qubits. Two simulation tasks are considered: (1) computing the probability of a given output x, and (2) sampling x from the output probability distribution.
We show that these tasks can be solved on a classical computer in time $poly(n,m)+2^{0.5 t} t^3$ and

$poly(n,m)+2^{0.23 t} t^3 w^3$ respectively, where t is the number of T-gates, m is the total number of gates, and n is the number of qubits. The new algorithms may serve as a verification tool for medium-size quantum computations that are dominated by Clifford gates. The main ingredient of both algorithms is a new subroutine for approximating the norm of a multi-qubit state which is given as a linear combination of stabilizer states. We also develop new techniques for approximating tensor products of magic states by linear combinations of stabilizer states.

Based on a joint work with David Gosset (Caltech)

Speaker: **Ted Yoder**
Title: Universal fault-tolerant gates on nondegenerate stabilizer codes

Abstract: It is an oft cited fact that no quantum code can support a set of fault-tolerant logical gates that is both universal and transversal. This no-go theorem is generally responsible for the interest in alternative universality constructions including magic state distillation. Widely overlooked, however, is the possibility of non-transversal, yet still fault-tolerant, gates that work directly on small quantum codes. Here we demonstrate precisely the existence of such gates. In particular, we show how the limits of non-transversality can be overcome by performing rounds of intermediate error-correction to create logical gates on stabilizer codes that use no ancillas other than those required for syndrome measurement. Moreover, the logical gates we construct, the most prominent examples being Toffoli and controlled-controlled-Z, often complete universal gate sets on their codes. We detail such universal constructions for the smallest quantum codes, the 5-qubit and 7-qubit codes, and then proceed to generalize the approach. One remarkable result of this generalization is that any nondegenerate stabilizer code with a complete set of fault-tolerant single-qubit Clifford gates has a universal set of fault-tolerant gates. Another is the interaction of logical qubits across different stabilizer codes, which, for instance, implies a broadly applicable method of code switching.

Speaker: **Leonie Mueck**
Title: Quantum Information at Nature and its sister journals

Abstract: Ever since its launch in 1869, the multidisciplinary journal Nature has striven to provide scientists with a communication platform to publish and discuss exciting results. Focussing on quantum information science, I will explain how to navigate the publication process at Nature and its sister journals, including choice of journal, editorial criteria and policy issues. I will discuss current publishing trends, especially measures to promote transparency in the dissemination of scientific results. Finally, I will talk about a current programme on entrepreneurship in quantum technology that Nature is running together with Entrepreneur First and Innovate UK.

Speaker: **Phillip Schindler**
Title: Quantum algorithms and simulations with trapped ions

Abstract: Trapped ions are a promising platform to realize engineered quantum systems such as quantum information processors and quantum simulators. In this talk, the physics of ion trap quantum information processing are introduced by describing our extended toolbox consisting of coherent as well as dissipative operations. This toolbox allows us to directly simulate paradigmatic quantum systems, such as pair creation in the lattice gauge formalism. More general, a universal quantum information processor is able to realize any given algorithm as a sequence of these toolbox operations. I will present an approach to find an optimal decomposition, illustrated by the example of Shor's algorithm. In the long run, it will be necessary to employ quantum error correction to engineer a large-scale quantum information processor. I will review past proof-of-concept experiments and outline a path towards a medium scale quantum error correction procedure, where the logical qubit will outperform its physical constituents.

Speaker: **Bela Bauer**
Title: Hybrid quantum-classical approach to correlated materials

Abstract: Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade. While it has been shown that such a quantum computer can in principle solve certain small electronic structure problems and idealized model Hamiltonians, the highly relevant problem of directly solving a complex correlated material appears to require a prohibitive amount of resources. Here, we show that by using a hybrid quantum-classical algorithm that incorporates the power of a small quantum computer into a framework of classical embedding algorithms, the electronic structure of complex correlated materials can be efficiently tackled using a quantum computer. In our approach, the quantum computer solves a small effective quantum impurity problem that is self-consistently determined via a feedback loop between the quantum and classical computation. Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around one hundred logical qubits becomes available.

Speaker: **Scott Aaronson**
Title: Three Paths to Quantum Supremacy

Abstract: With high-quality ~40-qubit machines on the horizon, attention has turned to the question of what we could do with them that would unambiguously demonstrate a complexity advantage over classical computing. In the last 6-7 years, a paradigm has emerged for arguing that certain quantumly-samplable probability distributions are hard to sample classically, unless (say) PostBPP=PostBQP and the polynomial hierarchy collapses. In this talk, I'll discuss three examples of this paradigm -- BosonSampling, random quantum circuits, and IQP / Fourier Sampling -- with a focus on brand-new results that could be relevant to experiments. In particular, I'll explain:
(1) How to prove classical/quantum separations for sampling-like tasks with classically verifiable outcomes, assuming the classical hardness of guessing a quantum amplitude with even slightly-better-than-chance success probability
(2) Time-space tradeoffs for classically simulating a quantum circuit with n qubits and m gates, with applications to the hardness conjectures in (1)
(3) "Gray-box" classical hardness results for IQP / Fourier Sampling -- which are better than black-box hardness, though still not as good as hardness for fully explicit problems -- and which assume nothing more than the existence of secure one-way functions and pseudorandom generators
I'll mention numerous open problems. This is joint work with Lijie Chen.

Speaker: **Juan Bermejo-Vega**
Title: Contextuality as a resource for qubit quantum computation

Abstract: We describe a scheme of quantum computation with magic states on qubits for which contextuality is a necessary resource possessed by the magic states. More generally, we establish contextuality as a necessary resource for all schemes of quantum computation with magic states on qubits that satisfy three simple postulates. Furthermore, we identify stringent consistency conditions on such computational schemes, revealing the general structure by which negativity of Wigner functions, hardness of classical simulation of the computation, and contextuality are connected.

Based on joint work with Robert Raussendorf, Dan E. Browne, Nicolas Delfosse and Cihan Okay.

Speaker: **Benoit Valiron**
Title: Quantum algorithms from the programmer's perspective

Abstract: In this talk I will present the design and implementation of the quantum programming language Quipper. Designed with scalability and expressiveness in mind, Quipper has been used to program several non-trivial quantum algorithms whose quantum gate representation use trillions of gates. Based on a generalized circuit model, it is not dependent on any particular model of quantum hardware. Quipper has proven effective and easy to use, and opens the door towards using formal methods to analyze quantum algorithms.

Speaker: **Gorjan Alagic**
Title: Quantum encryption and obfuscation

Abstract: Encryption of data is fundamental to secure communication. Beyond encryption of data lies obfuscation, i.e., encryption of functionality. It has been known for some time that the most powerful form of classical obfuscation (black-box obfuscation) is impossible. In this work, we initialize the rigorous study of obfuscating programs via quantum-mechanical means. We prove quantum analogues of several foundational results in obfuscation, including the aforementioned impossibility result.

In its most powerful “quantum black-box” instantiation, a quantum obfuscator would turn a description of a quantum program P into a quantum state S, such that anyone in possession of S can repeatedly evaluate P on inputs of their choice, but never learn anything else about P. We formalize this notion of obfuscation, and prove that it is only possible in a setting where the adversary has access to just one obfuscation. Our proof involves a novel technical idea: chosen-ciphertext-secure encryption for quantum states. In addition, we show that the surviving form of obfuscation may still have powerful applications, including quantum fully-homomorphic encryption and quantum money. We also define quantum versions of indistinguishability obfuscation and best-possible obfuscation, show that they are equivalent, and that their perfect and statistical variants would imply an unlikely complexity-theoretic collapse.

Speaker: **Nathan Wiebe**
Title: Quantum Bootstrapping

Abstract: A major problem facing the development of quantum computers or large scale quantum simulators is that general methods for characterizing and controlling are intractable. We provide a new approach to this problem that uses small quantum simulators to efficiently characterize and learn control models for larger devices. Our protocol achieves this by using Bayesian inference in concert with Lieb–Robinson bounds and interactive quantum learning methods to achieve compressed simulations for characterization. We also show that the Lieb–Robinson velocity is epistemic for our protocol, meaning that information propagates at a rate that depends on the uncertainty in the system Hamiltonian. We illustrate the efficiency of our bootstrapping protocol by showing numerically that an 8 qubit Ising model simulator can be used to calibrate and control a 50 qubit Ising simulator while using only about 750 kilobits of experimental data. Finally, we provide upper bounds for the Fisher information that show that the number of experiments needed to characterize a system rapidly diverges as the duration of the experiments used in the characterization shrinks, which motivates the use of methods such as ours that do not require short evolution times.