Partial-indistinguishability obfuscation using braids
Stephen Jordan, NIST
Tuesday, January 8, 2013, 3:00 pm, 107 Annenberg

A circuit obfuscator is an algorithm that translates logic circuits into functionally-equivalent similarly-sized logic circuits that are hard to understand. While ad hoc obfuscators exist, theoretical progress has mainly been limited to no-go results. In this work, we propose a new notion of circuit obfuscation, which we call partial indistinguishability. We then prove that, in contrast to previous definitions of obfuscation, partial indistinguishability obfuscation can be achieved by a polynomial-time algorithm. Specifically, our algorithm re-compiles the given circuit using a gate that satisfies the relations of the braid group, and then reduces to a braid normal form. A variant of our obfuscation algorithm can also be applied to quantum circuits.

Quantum computational matter
Stephen Bartlett, University of Sydney
Tuesday, January 29, 2013, 3:00 pm, 107 Annenberg

Low-temperature phases of strongly-interacting quantum many-body systems can exhibit a range of exotic quantum phenomena, from superconductivity to fractionalized particles. One exciting prospect is that the ground or low-temperature thermal state of an engineered quantum system can function as a quantum computer. For this idea to be sensible, the usefulness of a ground or low-temperature thermal state for quantum computation cannot be critically dependent on the details of the system's Hamiltonian; if so, engineering such systems would be difficult or even impossible. A much more powerful result would be the existence of a robust ordered phase which is characterised by its ability to perform quantum computation.

I'll discuss some recent results on the existence of such a quantum computational phase of matter, working within the measurement-based (cluster state) model of quantum computation. I will show that the ability to perform certain logic gates such as the identity gate over long distances in the model corresponds precisely to the recently-proposed notion of 'symmetry-protected topological order' for an appropriate symmetry group. Using some techniques from fault-tolerance, we can then prove that any perturbation of the cluster state model will result in a ground state that remains universal for quantum computation, provided the perturbation is sufficiently small and respects a certain symmetry.

References:
http://arxiv.org/abs/1201.4877
http://arxiv.org/abs/1207.4805

Device-independent physics: randomness good, communication bad

Valerio Scarani, Centre for Quantum Technologies and Department of Physics, National University of Singapore

Tuesday, February 5, 2013, 3:00 pm, 107 Annenberg

Bell's theorem rules out the explanation of quantum correlations through pre-established agreement. Most physicists, including the present speaker, view this result as a confirmation of the existence of intrinsic randomness in nature. In the past five years, this lofty view has developed into an unexpected connection with applied quantum information science, hinting to the possibility of "device-independent certification". In the first half of the talk, I shall review some of these developments.
In the second half, I shall try and put myself in the skin of the die-hard of determinism, who have to deny one of the two other assumptions of Bell's theorem. I shall rapidly argue that no scientist can abandon "measurement independence" and shall then focus on abandoning no-signaling. I shall prove a strong result which can be seen as a twin of Bell's theorem (http://arxiv.org/abs/1110.3795): if one tries to explain quantum correlations by a hidden, superluminal influence, this influence must propagate at infinite speed. In other words, any finite-speed influence cannot be hidden and would lead to the possibility of superluminal signaling. This goes as far as one can to prove that, even if intrinsic randomness is puzzling, the alternatives are probably much worse.

Quantum information theory as a proof technique

Fernando Brandao, ETH Zurich, Institute for Theoretical Physics

Friday, February 8, 2013, 3:00 pm, 213 Annenberg **Note room change**

Quantum information theory emerges naturally from our desire to understand the capabilities of quantum mechanical systems for information processing. However, as for its classical counterpart, the theory turns out to have applications much beyond analysing the efficiency of communication protocols with quantum systems. In this talk I will present two results in this direction.

First I will discuss how the Sum-Of-Squares (Parrilo/Lasserre) hierarchy, one of the most powerful hierarchies of semidefinite programs for approximating optimisation problems, is intimately connected to quantum information theory, with the latter providing a convenient framework for understanding the efficiency of the former. This leads to new fast algorithms for important quantum-related problems, such as determining whether there is entanglement in a quantum state, as well as improved running-time bounds for approximating problems of interest in theoretical computer science, such as unique games and the small set expansion problem.

Second I will discuss the use of techniques from quantum information theory to understand better the efficiency of mean-field theory, a very useful heuristics in computing properties of certain physical systems (such as in the context of quantum chemistry), and link it to the problem of obtaining a quantum counterpart of the celebrated PCP theorem, which is the central tool in the theory of hardness of approximation.

Both results show how ideas from quantum information theory are useful even outside the quest of building new quantum technologies, forming a powerful new method for arguing about problems ranging from optimization theory and computational complexity theory to numerical physics. No background on quantum information will be assumed.

Based on joint works with Boaz Barak (MRS New England), Matthias Christandl (ETH), Aram Harrow (MIT), Jonathan Kelner (MIT), David Steurer (Cornell), Yuan Zhou (CMU), and Jon Yard (MRS Station Q).

Exponential decay of correlations implies area law
Fernando Brandao, ETH Zurich, Institute for Theoretical Physics
Tuesday, February 12, 2013, 3:00 pm, 107 Annenberg

Quantum states of many particles are fundamental to our understanding of many-body physics. Yet they are extremely daunting objects, requiring in the worst case an exponential number of parameters in the number of subsystems to be even approximately described. How then can multi-particle states be useful for giving predictions to physical observables? The intuitive explanation is that physically relevant quantum states, defined as the ones appearing in nature, are usually much simpler than generic quantum states. In this talk I will discuss a very recent theorem that gives further justification to this intuition. The theorem states that exponential decay of correlations, a physically motivated restriction on the set of multi-particle quantum states, implies an area law for the entanglement entropy of systems defined on a line, and thus also an efficient classical description for such systems. The result can be seen as a rigorous justification to the intuition that states with exponential decay of correlations, usually associated with non-critical phases of matter, are simple to describe. I will outline the main steps in the proof, that relies on several previous tools from quantum information theory and that can also be seen as providing a limitation to the phenomenon of data hiding in quantum states. Based on joint work with Michal Horodecki.

Sequential decoding of general quantum communication channels
Mark Wilde, Louisiana State University
Tuesday, April 9, 2013, 3:00 pm, 107 Annenberg

Despite the fact that a quantum measurement generally disturbs the state of a quantum system, recent work of Seth Lloyd and collaborators demonstrates that a sender and receiver can communicate at the Holevo rate even when the receiver performs a large number of sequential measurements to determine the message of the sender. The present work contributes to this direction, by addressing three questions that have arisen from the work on sequential decoding. First, we show that Pranab Sen's non-commutative union bound applies for a sequence of general measurements (not merely projective ones). Next, we use this result to prove that sequential decoding works well even in the "one-shot" regime, where we are given a single instance of a channel and wish to determine the maximal number of bits that can be communicated up to a small failure probability. Finally, we demonstrate two ways in

which a receiver can recover a state close to the original state after it has been decoded by a sequence of measurements that each succeed with high probability. The second of these methods will be useful in realizing an efficient decoder for fully quantum polar codes, should a method ever be found to realize an efficient decoder for classical-quantum polar codes. This work is available as arXiv:1303.0808.

Equilibrium value method for optimization problems and its applications in quantum computation
Xiaodi Wu, University of Michigan
Tuesday, April 16, 2013, 3:00 pm, 107 Annenberg

Semidefinite programming (SDP) is a powerful technique from both an analytic and computational point of view for optimization problems. It is also intimately related to quantum computation, as many optimization problems over density operators (quantum states) could be naturally formulated as SDPs. In spite of the existence of polynomial time solvers for general SDPs (e.g., interior point method), the black-box use of these solvers is, however, unsatisfactory for many purposes. For instance, the lack of explicitness makes it hard to adapt (or optimize) these solvers for special instances of SDPs. Moreover, these polynomial time solvers provide no guarantee when one requires stronger efficiency, such as space efficiency (or equivalently, efficient computability by a parallel machine).
In this talk, I will present a new approach called "Equilibrium Value Method" (EVM) that provides an explicit and time/space efficient solution to a substantial class of SDPs, which, in particular, includes many examples that arise naturally in quantum computation. The main idea behind EVM is to characterize the procedure to solve a SDP as a zero-sum game, in which one player tries to provide an optimal solution of the SDP while the other player tries to find anything wrong with that solution.
I will focus on the main application of EVM, which serves as a way to obtain PSPACE upper bounds of quantum complexity classes. First, I will show how EVM could lead to a simple and intuitive alternative proof to the recent celebrated result QIP=PSPACE. Second, I will illustrate how EVM could extend to a much more general setting, by proving that the quantum refereed games (i.e., the competing-prover variant of QIP) with two turns (QRG(2)) coincide with PSPACE.
I will also talk about a few additional features of this approach and discuss a little bit about how it can extend to convex optimizations beyond SDPs. No background on either SDP or computational complexity will be assumed.
Based on results by myself and a joint result with Gus Gutoski (IQC, U Waterloo).

Continuous-variable quantum cryptography: Current status and future directions
Christian Weedbrook, University of Toronto
Tuesday, April 23, 2013, 3:00 pm, 107 Annenberg

Quantum cryptography allows two people to communicate in absolute secrecy using unbreakable codes. In this talk I introduce the basics of the continuous-variable version of quantum cryptography and detail recent works and advances along with future opportunities in this exciting field of research.

Building one-time memories from isolated qubits

Yi-Kai Liu, NIST

Tuesday, April 30, 2013, 3:00 pm, 107 Annenberg

One-time memories (OTM's) are a simple type of tamper-resistant cryptographic hardware, which can be used to implement one-time programs, a strong form of secure computation. Here we investigate the possibility of building OTM's using "isolated qubits" -- qubits that can only be accessed using local operations and classical communication (LOCC). Isolated qubits can be implemented using current technologies, such as nitrogen vacancy centers in diamond.

We construct OTM's that are information-theoretically secure against one-pass LOCC adversaries using 2-outcome measurements. (Also, these OTM's can be prepared and accessed by honest parties using only LOCC operations.) This result is somewhat surprising, as OTM's cannot exist in a fully-quantum world or in a fully-classical world; yet they can be built from the combination of a quantum resource (single-qubit measurements) with a classical restriction (on communication between qubits).

Our construction resembles Wiesner's old idea of quantum conjugate coding, implemented using random error-correcting codes. Our proof of security uses entropy chaining to bound the supremum of a suitable empirical process. An interesting open problem is to replace our random codes with efficiently-decodable codes, which may yield computationally-efficient OTM's that are secure against computationally-bounded LOCC adversaries. In addition, we construct data-hiding states, which allow an LOCC sender to encode an (n-O(1))-bit messsage into n qubits, such that at most half of the message can be extracted by a one-pass LOCC receiver, but the whole message can be extracted by a general quantum receiver.

http://arxiv.org/abs/1304.5007

Quantum sparse-graph codes for future quantum computers

Leonid Pryadko, UCR

Tuesday, May 7, 2013, 3:00 pm, 107 Annenberg

Research in quantum error correction has been heavily dominated by just two classes of codes: concatenated and surface codes. Both code families can only encode a limited number of qubits per block and thus require huge redundancy for any useful quantum computation. I will discuss recently discovered quantum hypergraph-product codes (QHPCs) which generalize the surface codes but can encode many more qubits per block. Just like the surface codes, QHPCs have convenient planar representations, with each encoded qubit corresponding to a pair of topologically non-trivial patterned strings. The allowed patterns correspond to codewords of two classical binary codes which form the QHPC. Further, each of the quantum measurements needed for error correction can involve just a few qubits, these measurements can be done in parallel, and almost all errors affecting a finite fraction of qubits can be corrected.

Is there life beyond Quantum Mechanics?
Anton Kapustin, Caltech
Tuesday, May 14, 2013, 3:00 pm, 107 Annenberg

I formulate a system of axioms for a physical theory which are common to both classical and quantum mechanics and incorporate some basic intuition about the laws of physics, such as the existence of composite systems and the relation between symmetries and conservation laws. I prove that if systems with finite-dimensional spaces of observables exist, then Quantum Mechanics is the only possible theory of this sort. Even if some of the axioms are dropped, one can show that Quantum Mechanics cannot be deformed by a small parameter. These results show that the laws of Quantum Mechanics are exact, unless some deeply cherished assumptions about the structure of physical laws are wrong.

Quantum metrology and many-body physics with optical lattice clocks
Michael J. Martin, JILA, University of Colorado
Tuesday, May 21, 2013, 4:00 pm, 107 Annenberg **Note time change**

Optical clocks have revolutionized the science of timekeeping, permitting frequency measurements at (and even below) the level of a part in 1017 systematic uncertainty. Neutral atom optical standards based on ultracold lattice-trapped atoms promise an order of magnitude increase in measurement precision over frequency standards based on single ions, but require the highest levels of laser precision to fully realize this improvement and operate near the limit set by quantum fluctuations. In this seminar, I will introduce alkaline earth atoms in the context of precision frequency measurement and describe the features that make this class of neutral atoms desirable for optical frequency standards. I will then describe the JILA 87Sr optical lattice clock, where thousands of essentially decoherence-free 87Sr atoms are probed by a laser with <30 mHz linewidth. This level of precision allows access to a regime in which quantum fluctuations play a significant role, enabling near quantum-limited clock operation and the study of quantum many-body physics, which I will discuss. Such precise atom-laser interactions should permit direct characterization and manipulation of many-body states and explorations of the SU(N) symmetry exhibited by the nuclear spin of fermionic alkaline earth atoms

Fourier sparsity, spectral norm, and the Log-rank conjecture
Shengyu Zhang, The Chinese University of Hong Kong
Tuesday, May 28, 2013, 3:00 pm, 107 Annenberg

We study Boolean functions with sparse Fourier coefficients or small spectral norm, and show their applications to the Log-rank Conjecture for XOR functions f(x\oplus y) --- a fairly large class of functions including well-studied ones such as Equality and Hamming Distance. The rank of the communication matrix M_f for such functions is exactly the Fourier sparsity of f. Let d be the F2-degree of f and D(f) stand for the deterministic communication complexity for f(x\oplus y). We show that 1. D(f) = O(2^{d^2/2} log^{d-2} ||\hat f||_1). In particular, the Log-rank conjecture holds for XOR functions with constant F2-degree. 2. D(f) = O(d ||\hat f||_1) = O(\sqrt{rank(M_f)}\logrank(M_f)). We obtain our

results through a degree-reduction protocol based on a variant of polynomial rank, and actually conjecture that its communication cost is already \log^{O(1)}rank(M_f). The above bounds also hold for the parity decision tree complexity of f, a measure that is no less than the communication complexity (up to a factor of 2).

Along the way we also show several structural results about Boolean functions with small F2-degree or small spectral norm, which could be of independent interest. For functions f with constant F2-degree: 1) f can be written as the summation of quasi-polynomially many indicator functions of subspaces with \pm-signs, improving the previous doubly exponential upper bound by Green and Sanders; 2) being sparse in Fourier domain is polynomially equivalent to having a small parity decision tree complexity; 3) f depends only on polylog||\hat f||_1 linear functions of input variables. For functions f with small spectral norm: 1) there is an affine subspace with co-dimension O(||\hat f||_1) on which f is a constant; 2) there is a parity decision tree with depth O(||\hat f||_1 log ||\hat f||_0).

Error models in quantum computation: an application of model selection
Steven van Enk, University of Oregon
Tuesday, July 9, 2013, 3:00 pm, 107 Annenberg

Threshold theorems for fault-tolerant quantum computing assume that errors are of certain types. But how would one detect whether errors of the ''wrong'' type occur in one's experiment, especially if one does not even know what type of error to look for? The problem is that for many qubits a full state description is impossible to analyze, and a full process description is even more impossible to analyze. As a result, one simply cannot detect all types of errors.

Here we show through a quantum state estimation example (on up to 25 qubits) how to attack this problem using model selection. We use, in particular, the Akaike Information Criterion. The example also indicates that the number of measurements that one has to perform before noticing errors of the wrong type scales polynomially both with the number of qubits and with the error size.

This is joint work with Lucia Schwarz.

Nested quantum walks with quantum data structures
Robin Kothari, University of Waterloo
Tuesday, September 24, 2013, 3:00 pm, 107 Annenberg

I'll talk about a new framework for designing quantum algorithms that extends the quantum walk framework of Magniez, Nayak, Roland, and Santha, by utilizing the idea of quantum data structures to construct an efficient method of nesting quantum walks. The new framework extends the known quantum walk framework while retaining its advantages: simplicity, ease of use, and a straightforward understanding of all resources used by the algorithm, such as queries, time or space.

The new framework is also powerful. In particular, the recently proposed learning graph framework of Belovs has yielded improved upper bounds for several problems, including the triangle finding problem and more general subgraph detection problems. I will exhibit the power of the new framework by giving simple explicit constructions that reproduce both the O(n^{35/27}) and O(n^{9/7}) learning graph upper bounds (up to logarithmic factors) for triangle finding.

This is joint work with Stacey Jeffery and Frédéric Magniez.

Simulation of dynamical abelian and no-abelian lattice gauge theories with cold atoms
Benni Reznik, Tel-Aviv University
Tuesday, October 8, 2013, 3:00 pm, 107 Annenberg

Quantum simulations of High Energy Physics, and of gauge field theories, is an emerging and exciting direction in quantum simulations. Compared with condensed matter simulations however, such simulations are more demanding because of the additional requirements involving local gauge symmetries, Lorentz invariance, and the inclusion of both Fermions and Bosons, that are needed for describing matter and force mediators. Explicit models of analog simulators of LGT have been recently proposed for systems of cold atoms in optical lattices. In particular, it turns out that local gauge invariance, can be based and derived from the fundamental symmetries of the given atomic cold atomic interactions and conservation laws.

This then provides methods for simulating elementary gauge invariant field theories, such as compact-QED (U(1)), and SU(N) Yang-Mills theories. It suggests that fundamental HEP phonomena, such as dynamical quark confinement, and exotic QCD phases, that are currently inaccessible to classical simulations, can be explored in “table-top” experiments with cold atoms.

Exponential Improvement in Precision for Hamiltonian-Evolution Simulation
Rolando Somma, Los Alamos National Laboratory
Tuesday, November 12, 2013, 3:00 pm, 105 Annenberg (different location, this term only)

I will present a quantum method for simulating Hamiltonian evolution with complexity polynomial in the logarithm of the inverse error. This is an exponential improvement over existing methods for Hamiltonian simulation. In addition, its scaling with respect to time is close to linear, and its scaling with respect to the time derivative of the Hamiltonian is logarithmic. These scalings improve upon most existing methods. Our method is to use a compressed Lie-Trotter formula, based on recent ideas for efficient discrete-time simulations of continuous-time quantum query algorithms.

This is joint work with Dominic Berry and Richard Cleve.

The Bose-Hubbard model on a graph is QMA-complete
David Gosset, University of Waterloo
Tuesday, November 19, 2013, 3:00 pm, 105 Annenberg (different location, this term only)

The Bose-Hubbard model is a system of interacting bosons that live on the vertices of a graph. The particles can move between adjacent vertices and experience a repulsive on-site interaction. We prove that approximating the ground energy of the Bose-Hubbard model on a graph (at fixed particle number) is QMA-complete. Our QMA-hardness proof encodes an n-qubit computation in the subspace of n hard-core bosons with at most one particle per site, so it holds for any fixed repulsive interaction strength. This feature, along with the well-known mapping between hard-core bosons and spin systems, also allows us to prove a related result for a class of 2-local Hamiltonians defined by graphs (a generalization of the XY model).

This is joint work with Andrew Childs and Zak Webb.

Simplified Quantum Compiling with Complex Gate Distillation
Guillaume Duclos-Cianci, University of Sherbrooke
Tuesday, December 3, 2013, 3:00 pm, 105 Annenberg (different location, this term only)

I will present a scheme to compile complex quantum gates that uses significantly fewer resources than existing schemes. In standard fault-tolerant protocols, a magic state is distilled from noisy resources, and copies of this magic state are then assembled into produced complex gates using the Solovay-Kitaev theorem or variants thereof. In our approach, we instead directly distill magic states associated to complex gates from noisy resources, leading to a reduction of the compiling overhead of several orders of magnitude.