Abstracts

Monday

Jamie Batuwantudawe

A Look at a Three-State Quantum Key Distribution Protocol

Quantum key distribution (QKD) protocols allow two parties, Alice and Bob, to establish secure keys. The most well-known protocol is BB84, using four distinct states. Recently, Phoenix et al. proposed a three state protocol. We explain the protocol and discuss its security proof. The proof follows the Shor and Preskill structure, invoking Azuma's Inequality for phase error estimation.The three-state protocol also has an interesting structure that allows for bit error estimation from the inconclusive results (ie. where Alice and Bob choose different bases).

Christian Schaffner

Cryptography in the Bounded Quantum-Storage Model

We initiate the study of two-party cryptographic primitives with unconditional security, assuming that the adversary's quantum memory is of bounded size. We show that oblivious transfer and bit commitment can be implemented in this model using protocols where honest parties need no quantum memory, whereas an adversarial player needs quantum memory of size larger than n/2 in order to break the protocol, where n is the number of qubits transmitted. This is in sharp contrast to the classical bounded memory model, where we can only tolerate adversaries with memory of size quadratic in honest players' memory size. Our protocols are efficient, non-interactive and can be implemented using today's technology. On the technical side, a new entropic uncertainty relation involving min-entropy is established.

Christoph Dankert

Efficient Noise Estimation with MUBs

In joint work with Richard Cleve (UW), Etera Livine (PI), and Joseph Emerson (PI), I am investigating methods to estimate noise in an implementation of a quantum algorithm and in a quantum channel. We came up with a nice way to characterize the average gate fidelity using mutually unbiased basis (MUB) vectors. Other techniques relied on costly averages over the Haar measure on the set of all states of some d-dimensional state space or had to

make use of state tomography. Our result provides an efficient way to estimate the average gate fidelity. This might give experimentalists a practical method for noise estimation.

Nathan Babcock

Magic States

The Gottesman-Knill theorem states that quantum computations consisting only of preparations of the $|0\rangle$ state, unitary operations from the Clifford group, and Pauli measurements can be simulated efficiently on a classical computer and are therefore not sufficient to do universal quantum computation (UQC). Recently, Bravyi and Kitaev proposed a novel scheme for UQC based on a modification to the Clifford group model (quant-ph/0403025). They show that known quantum error correction algorithms will distill certain "magic" mixed states into pure states allowing UQC. I will provide a brief review of quantum error correction and its "stabilizer" formalism before giving a detailed explanation of the distillation algorithm. Finally, I will discuss a "proof-of-concept" implementation of the algorithm on a nuclear magnetic resonance quantum computer.

Tuesday

Zeng Bin Wang

Large Interaction of Two Photons

Some ideas to introduce large nonlinear interaction between photons will be discussed. In particular a novel scheme to achieve strong coupling between single photons in EIT (Electromagnetically Induced Transparency) regime. The talk will conclude with possible applications of this nonlinearity.

Eden Figueroa

Quantum Information Storage in Atomic Media

The answer to the atom-light interface problem could be given by the recently developed technique of storage of light by means of electromagnetically-induced transparency. EIT is a quantum interference effect that permits light to propagate through an otherwise opaque medium. Observed in gaseous atomic media, EIT is associated with high linear dispersion which leads to a tremendous reduction of the group velocity of light. Reducing this velocity to zero will stop and store the light pulse in the medium. The process can be reversed and the light pulse regenerated in its original quantum state, thus implementing a quantum memory cell for light.

Theoretically, this method is good for storing quantum and classical information alike; the regenerated pulse should possess exactly the same quantum properties as the one initially stored. Existing experimental tests are however limited to the classical domain. The next step extending the EIT storage technique to nonclassical states of light is the goal of our project. Our non-classical states will be single photons the actual carriers of quantum bits in the hypothetical optical quantum computer.

The idea is to generate a photon pair by means of parametric down-conversion; one photon in a pair will be detected immediately to serve as a reference while the other one will be stored in an EIT medium. The second photon will be detected upon its release; nonclassical correlations between the two photons will verify whether the EIT storage preserves the single-photon state.

The experiment is rather complicated due to some special requirements a photon must meet in order to be stored. Namely, its line width must be on the order of hundreds of kHz. Such narrowband single photons have not yet been produced.

The idea is to use an optical parametric amplifier a nonlinear optical cavity pumped by a continuous-wave laser source below its threshold. This cavity must be stabilized so that the signal photon wavelength is exactly the same as that of the desired atomic transition.

We report in our present experimental results together with a global overview of future experiments.

Simon Poole

Mode Theory and its Application to Quantum Information

Qubits can be realized by the usage of photons and can be manipulated in a variety of ways with linear optical elements. Under strongly idealizing assumptions, a laser prepares a many-photon state in which all photons are in the same mode. For some applications, it is convenient and sufficient to use a single plane wave laser mode to analyze the system. However, a better description of the laser beam can be given using the paraxial approximation to Maxwell's equations, this allows for the analysis of transverse electromagnetic laser modes. In practicality, lasers emit photons in different modes as a mixed state, however, the idealized mode model provides a convenient description employing linear optical elements and, to some degree, nonlinear crystals. An introduction to non-orthogonal modes will be used to describe the Hong-Ou-Mandel dip and how it relates to quantum fingerprinting.

Marcus Silva

A Markov Chain Description of Error-correction

Using symmetries inherent in the [[7,1,3]] code and circuitry used to perform fault-tolerant computation, I demonstrate how to calculate the exact error distribution in an erasure error

model using Markov chains. This approach, although complex, can be automated and is an alternative to Monte Carlo simulation if the code and circuits have enough symmetry.

Osama Moussa

Refrigeration by Quantum Computation

Preparation of a quantum computer in a known state is essential for quantum computation. This is required in initializing a quantum computer for computation, and in dynamically supplying ancilla qubits to achieve fault-tolerance. Heat-bath algorithmic cooling is an implementation-independent procedure, which has been proposed as means to purify the initially mixed state for computation. In this talk, I present numerical simulations of the heat-bath algorithmic cooling procedure, and highlight the theoretical limits on achievable cooling using this algorithm. I will also report the implementation of this algorithm on a 3-qubit processor as a proof of principle. The experiment is performed using the nuclear magnetic resonance (NMR) of single-crystal Malonic acid (C3H4O4) in the solid state. Using the algorithm, and starting from the totally mixed state on the computational qubits, we are able to cool one of the qubits below the effective heat-bath temperature.

Wednesday

Jon Walgate

Local Information and Nonorthogonal States

Measurements of quantum systems extract only classical information. This dichotomy between physically real and physically discoverable information underlies many of the conceptual and metaphysical challenges of quantum theory. In particular, nonorthogonal quantum states can never be reliably distinguished; this simple fact has wide ranging implications, such as the nocloning theorem and the security of quantum cryptography. Another quantum mechanical novelty is nonlocality - the existence of physical systems whose correlated behavior violates local realism. Nonlocality arises when quantum systems parts are measured and studied separately, even when the results of such measurements are public. I study the information which can be extracted from nonorthogonal systems under exactly this constraint. By focusing upon simple qubit-based systems, some primitive properties emerge which demonstrate both the drawbacks and the advantages of nonorthogonally encoded information. Although they can never be perfectly distinguished, nonorthogonal systems can nevertheless reliably store and yield classical information, and this is particularly apparent in a local framework. For example, all locally indistinguishable sets quantum states can be rendered perfectly distinguishable by the addition of one system in a complementary set of purely nonorthogonal states. In fact, arbitrarily large sets of arbitrarily multipartite

nonorthogonal states can always be found such that just one copy always suffices to reduce the set of possible states of a system to just two. I discuss a number of protocols whereby such nonorthogonal states can be used to locally encode and process classical information in a reliable fashion.

Anne Broadbent

On the Power of Nonlocal Boxes

We study quantum information through the use of a virtual two-party device, the nonlocal box. Through the analysis of pseudo-telepathy games, we show the power of the nonlocal box in entanglement simulation. We also show limits on the power of the nonlocal box and conclude that nonlocality and entanglement are fundamentally different resources.

Andre Methot

Is a Maximally Entangled State Maximally Entangled?

We reveal an anomaly which arises in many measures of entanglement, where non-maximally entangled states appear more entangled than maximally entangled ones. We ask the question: why is it so?

Sibasish Ghosh

Entangling Power of Permutations

The notion of entangling power of unitary matrices was introduced by Zanardi, Zalka and Faoro, where the linearized entropy of subsystem's density matrix was used as a measure of entanglement of the density matrix of the whole system. Using the same measure of entanglement, we study the entangling power of permutations, given in terms of a combinatorial formula. We show that the permutation matrices with zero entangling power are, up to local unitaries, the identity and the swap. We construct the permutations with the minimum nonzero entangling power for every dimension. With the use of orthogonal latin squares, we construct the permutations with the maximum entangling power for every dimension. Moreover, we show that the value obtained is maximum over all unitaries of the same dimension, with possible exception for 36. Our result enables us to construct generic examples of 4-qudits maximally entangled states for all dimensions except for 2 and 6. We numerically classify, according to their entangling power, the permutation matrices of dimension 4 and 9, and we give some estimates for higher dimensions. Taking the 'disentangling' power of any unitary operator, acting on a two-qudit system, as the average (over all maximally entangled states) of the linearized entropy of one subsystem of the two-qudit system which

is in a state obtained after the action of the unitary operator on a maximally entangled state of the system, we show that the permutations having maximal entangling powers are also having minimal 'disentangling' powers over the set of all unitaries with possible exceptions for dimensions 2 and 6.

Thursday

Lana Sheridan

Quantum Walks, Entanglement, and the Measurement-based Model

This talk focuses on quantum walks, but in two parts. First, the standard quantum walk model will be introduced, then the effects of entangling pairs of walkers in the walk will be presented. In the second part, I will discuss the current effort to frame the quantum walk in the measurement-based model.

Heath Gerhardt

Spatial Search by Phased Continuous-time Quantum Walks

In this talk I will introduce a new type of continuous-time quantum walk (cqw), which I call the phased continuous-time quantum walk (pcqw). The pcqw differs from the previously studied ctw in that the edges of the graphs can be associated with arbitrary elements of the complex unit circle (the phases). Numerical results on the application of pcqw's to spatial search will be discussed.

Eric Paquette

Towards Quantum Types

In this talk I will introduce the notion of a formal type theory and show why someone cannot develop a formal 'pure' quantum type theory (by pure, I mean a theory which would contain only quantum types). I will then introduce a type system which is augmented with quantum types and models the notion of quantum computation with classical control. I will also show that quantum types not only type the information but are also carriers of topological information. I will discuss the possible relations of topology with computational complexity.

Nathan Wiebe

Quantum Chaos and Measurement in Quantum Information Science

Quantum Chaos is the study of the behavior of quantum systems whose classical analogs exhibit chaos. In this talk I will discuss the properties of chaotic time evolution for various systems, and mention the possible utility that these systems might have in the field of quantum information. In addition I will discuss coarse grained observations, and how these can make quantum chaos less useful for quantum protocols.

Friday

Gus Gutoski

Classical Upper Bounds for Quantum Interaction

I will prove classical upper bounds on the power of several variants of the quantum interactive proof system model. In particular, I will review an existing semidefinite programming technique used to decide single-prover quantum interactive proofs in deterministic exponential time. I will observe that this technique extends naturally to yield a nondeterministic exponential-time algorithm to decide competing-prover quantum interactive proofs. Finally, I will combine this technique with the ellipsoid method to decide one-round competing-prover quantum interactive proofs in deterministic exponential time.

Rick Zhang

Classical Measures and Quantum Query Complexity on Boolean Functions

I will introduce several complexity measures for Boolean functions: certificate complexity, sensitivity, block sensitivity, and the degree of a representing or approximating polynomial. Some relationships and biggest gaps known between these measures will be discussed. I will show how these measures give bounds for the decision tree complexity of Boolean functions on deterministic, randomized, and quantum computers. I will also introduce the techniques used for finding lower-bounds of quantum query complexity on boolean functions.

Dmitry Gavinsky

Auxiliary Shared Resources in Quantum and Classical Communication

Quantum computers are being intensively studied in the last decade, it is widely believed that the laws of Nature described by quantum mechanics give rise to significantly more powerful model of computation than that of (classical) Turing Machine. The notion of (classical) communication complexity was first studied by Yao in 1979, since then this complexity measure has found many application in different areas of Computer Sciences. In 1993 Yao defined the notion of quantum communication complexity. More recently it has been shown that using the laws of quantum mechanics it is sometimes possible to construct considerably more efficient communication protocols.

In this talk I will try to compare communication efficiency of several classical and quantum models. I will describe the following results:
- We demonstrate a communication problem where 0-error classical simultaneous message passing with public coin is exponentially more efficient than 0-error quantum simultaneous message passing. Together with a separation in the other direction due to Bar-Yossef et al., this shows that the quantum SMP model is, in some sense, incomparable with the classical public coin SMP model.
- We "almost separate" the models of quantum simultaneous message passing with shared entanglement and the model of quantum simultaneous message passing with shared randomness. We define a relation which can be efficiently exactly solved in the first model but cannot be solved efficiently, either exactly or in 0-error setup in the second model.
- We strengthen a result by Yao that a "very short" protocol from the model of classical simultaneous message passing with shared randomness can be simulated in the model of quantum simultaneous message passing with at most exponential slowdown. We show a similar result for protocols from the (stronger) model of classical 1-way message passing with shared randomness.

In the end of the talk I will mention a number of open problems and describe possible direction for further research.

Alexis Morris

Topological Quantum Computation

I will begin my presentation by a general overview of current proposals for implementing quantum circuits in real physical systems such as ions traps and optical cavities. I will then discuss issues such as what kind of requirements are needed in order for such systems to be able to perform universal quantum computations. Most notable is a need for great accuracy in the individual quantum gates. Since the advent of error correction codes, it is theoretically possible to perform quantum computations to any desired accuracy, provided that the failure rate for the quantum gates is smaller than a certain threshold value. However,

for the physical systems that I have just discussed, it will still be some time (if ever!) before experimental techniques can be perfected in order to satisfy the threshold error rate. I will then introduce the ideas behind topological quantum computation (TQC). TQC is a very exciting way to do quantum computations because it is intrinsically extremely robust against many types of error. I will explain why this is so, and conclude by showing how topological quantum gates can be implemented by braiding anyonic quasi-particles.