Mathematical Aspects of Quantum Information
Aspects mathématiques de l'informatique quantique

(Org: **Daniel Gottesman** (Perimeter Inst.), **Achim Kempf** (Waterloo), **David Kribs** (Guelph) and/et **Michele Mosca** (Waterloo; Perimeter Inst.))

ANDRIS AMBAINIS, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 2T2
A new proof of quantum adiabatic theorem

Adiabatic quantum algorithms are a new approach to quantum computation. While being equivalent to standard quantum circuit model, they present a completely different way of thinking about quantum algorithms.

Adiabatic algorithms are based on the adiabatic theorem of quantum mechanics. Informally, this theorem says that, when a Hamiltonian of a physical system is slowly transformed to a different Hamiltonian, the lowest energy state of the first Hamiltonian is transformed to the lowest energy state of the second Hamiltonian.

We present a new proof of quantum adiabatic theorem, in terms of discrete mathematics.

ARVID BESSEN, Department of Computer Science, Columbia University, New York, NY 10027, USA
A Lower Bound for the Sturm–Liouville Eigenvalue Problem on a Quantum Computer

We study the complexity of approximating the lowest eigenvalue of a Sturm–Liouville differential equation on a quantum computer. Our main focus is on the special case of computing the ground state energy of a quantum system for a given potential.

Recently Papageorgiou and Woźniakowski proved that quantum computers could achieve exponential speedups compared to classical computers for certain potentials. Papageorgiou's and Woźniakowski's method uses the (discretized) unitary propagator $\exp(i\mathbb{L}_q)$ as a query; here $\mathbb{L}_q$ is the differential operator for the Sturm–Liouville problem. If the operator $\exp(ip\mathbb{L}_q)$ (a "power query") is computable in cost comparable to $\exp(i\mathbb{L}_q)$ for any integer p, one can solve the Sturm-Liouville problem with $\mathcal{O}(\log \epsilon^{-1})$ power queries.

In this paper we will prove a matching lower bound of $\Omega(\log \epsilon^{-1})$ power queries, therefore showing that $\Theta(\log \epsilon^{-1})$ power queries are sufficient and necessary. Our proof is based on a frequency analysis technique, which examines the probability distribution of the final state of a quantum algorithm and the dependence of its Fourier transform on the input. This method was first used to give a lower bound for the number of power queries in the phase estimation problem on quantum computers.

HILARY CARTERET, Université de Montréal, C.P. 6128 succ. Centre-ville, Montréal, Québec H3C 3J7
Noiseless quantum circuits for measuring entanglement

The non-local properties of a density matrix are often defined in terms of the effects of unphysical maps, such as the Partial Transpose on the spectrum of the density matrix (PT-spectrum). Is it possible to measure these functions efficiently, or must we use full state tomography?

Previously proposed methods for measuring these quantities directly relied on the Structural Physical Approximation, which typically produce output states with visibilities that scale poorly with the system size. The moments of the resulting modified density operator must then be measured in a separate procedure, which can be done using a set of generalized Mach-Zehnder interferometers. The spectrum can then be obtained using a little algebra.

I will show how to construct a family of simple quantum circuits that can determine the PT-spectrum for any bipartite state, without incurring any loss of visibility. These circuits measure the minimum amount of information required to determine the PT-spectrum completely. They depend only on the dimension of the state and they will be exact up to the statistical uncertainties inherent in any experimental data. The analysis of the output of these circuits for general bipartite states also raises an interesting eigenspectrum reconstruction problem.

ANDREW CHILDS, California Institute of Technology, Pasadena, CA, USA
The limitations of nice mutually unbiased bases

Mutually unbiased bases of a Hilbert space can be constructed by partitioning a unitary error basis. We consider this construction when the unitary error basis is a nice error basis. We show that the number of resulting mutually unbiased bases can be at most one plus the smallest prime power contained in the dimension, and therefore that this construction cannot improve upon previous approaches. We prove this by establishing a correspondence between nice mutually unbiased bases and abelian subgroups of the index group of a nice error basis and then bounding the number of such subgroups. This bound also has implications for the construction of certain combinatorial objects called nets.

Joint work with Michael Aschbacher and Pawel Wocjan.

J. IGNACIO CIRAC, Max–Planck Institute for Quantum Optics, Hans–Kopferemannstr. 1, D-85748 Garching, Germany
Simulating quantum systems

Many-body quantum systems are very hard to simulate since the dimension of the corresponding Hilbert space scales exponentially with the number of particles N. In practice, however, the quantum states that typically appear in nature may be described with fewer parameters. In this talk I will review a novel description of quantum states which was introduced by F. Verstraete and myself, and it is based on projecting two-particle entangled states of a given dimension D onto subspaces of dimension d, which is the one of the Hilbert spaces corresponding to the original particles. The complexity of these states scales polynomially in d, D and N. Moreover, most of the states that appear in Quantum Information Theory, like cluster, GHZ, W, graphs, *etc.*, have $D = 2$. We have also developed (classical) numerical algorithms based on this description which allow us to simulate quantum many-body systems in 1 and higher spatial dimensions.

RICHARD CLEVE, Universiy of Waterloo
Nonlocality and limits of fault-tolerant computation

We present various results concerning nonlocal behavior in an abstract setting, and then show how to use them to establish upper bounds on the error-threshold below which computations can be made fault-tolerant.

This is joint work with Harry Buhrman, Noah Linden, and Falk Unger.

PATRICK HAYDEN, McGill University, Montreal
On private communication using a shared reference frame

A private shared Cartesian frame is a novel form of private shared correlation that allows for both private classical and quantum communication. Cryptography using a private shared Cartesian frame has the remarkable property that, if perfect security is demanded, the private classical capacity is roughly three times the private quantum capacity. I'll present work done with Stephen Bartlett and Rob Spekkens demonstrating that if the requirement for perfect security is relaxed, then it is possible to use the properties of random subspaces to nearly triple the private quantum capacity.

MARK HILLERY, Hunter College of the City University of New York, Department of Physics, 695 Park Avenue, New York, NY 10020, USA
Programmable quantum circuits

Many quantum circuits are designed to accomplish a single task, such as approximate cloning or teleportation. It is often useful to have more versatile circuits that can perform many tasks. Such a circuit has two inputs, data and a program, both of which are quantum states. The data has an operation performed on it, and the program controls what the operation is. If the circuit is to be able to perform an infinite number of operations with a finite-dimensional program space, it must be either probabilistic or approximate. That is, it either succeeds only part of the time, or the operations are performed to some level of approximation, and not exactly. The operation of probabilistic and approximate programmable circuits will be discussed.

PETER HøYER, Calgary

LOUIS KAUFFMAN, University of Illinois at Chicago
Topological Quantum Computation

This talk will survey joint work with Sam Lomonaco on the use of topology in relation to quantum computation. We begin by a discussion of universal gates based on unitary solutions to the Yang–Baxter equation. We then discuss models based on topological quantum field theory and show, in particular, how to construct the Fibonacci model of Freedman, Kitaev and Wang by using knot theoretic methods based on q-deformations of Penrose spin networks (Temperley Lieb recoupling theory). These methods provide a very direct way to construct representations of the Artin Braid groups that are dense in the unitary groups. Many questions will be discussed in the light of these constructions.

CHRISTOPHER KING, Northeastern University, Boston
Matrix inequalities and multiplicativity results

The multiplicativity of the $q \to p$ norm of a completely positive qubit channel for $q < 2 < p$ follows from some Hanner-type inequalities involving p-norms of positive semidefinite matrices. These inequalities are reviewed, together with their application to the multiplicativity question. Some extensions of the inequalities are described, and some open problems for qubit and higher dimensional channels are also discussed.

GREG KUPERBERG, University of California, Davis
Hybrid quantum memory and its capacity

What is the most general possible kind of memory consistent with quantum mechanics? The only commonly considered kinds are qudits and classical digits, but a hybrid modelled by an arbitrary C^*-algebra is more generally possible. The important Choi–Effros theorem implies that it is the most general possible quantum memory model modulo certain (debatable) assumptions. In particular it generalizes the theory of "decoherence-free subspaces".

Assuming this model, when is one hybrid memory worth more than another? I will give a characterization of when many copies of a memory A embed (or blindly encode with perfect fidelity) into slightly more copies of another memory B. In particular, either there is such an embedding, or A admits a state that does not visibly encode into B with high fidelity. The second half of this alternative depends on a Holder inequality for hybrid memories that generalizes the classical pigeonhole principle.

Reference: quant-ph/0203105.

MAIA LESOSKY, University of Guelph
On Generalized Noiseless Subsystems

A generalized notion of noiseless subsystems was recently introduced by Kribs, Laflamme and Poulin as part of a unified and generalized approach to quantum error correction called *operator quantum error correction*. One advantage to generalized noiseless subsystems is that they are not restricted to unital channels. In this talk I will present some simple examples and outline necessary and sufficient conditions that describe the existence of generalized noiseless subsystems.

DEBBIE LEUNG, University of Waterloo and Caltech
Composition of randomization maps

Recently, various quantum communication tasks have been related to the ability to randomize the state of a quantum system. In this talk, we will see how to obtain communication protocols for multiple receivers by understanding the composition of randomization maps.

ROBERT MARTIN, University of Waterloo, Waterloo, ON N2L 3G1
On the relationship between discrete and continuous representations of quantum information

In classical information theory, sampling theory provides the connection between discrete and continuous representations of information. Here we present a generalization to quantum field theory in which the bandwidth is provided by an ultra-violet cutoff. We investigate, in particular, the role of quantum fluctations as noise and implications for the channel capacity.

ASHWIN NAYAK, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 3G1
A quantum test for group commutativity

We consider the computational problem of testing whether an implicitly specified group is commutative. The group is defined by its k generators, and a procedure that implements group operations. The computational complexity (in terms of k) of this problem was first considered by Pak (2000). We construct a quite optimal quantum algorithm for this problem whose complexity is in $\tilde{O}(k^{2/3})$. The algorithm uses and highlights the power of the quantization method of Szegedy (2004). For the lower bound $\Omega(k^{2/3})$, we introduce a new technique of reduction for quantum query complexity. We also prove an $\Omega(k)$ lower bound for classical algorithms, which shows that the algorithm of Pak is optimal.

This is joint work with Frédéric Magniez (CNRS–LRI, France).

JONATHAN OPPENHEIM, University of Cambridge
Quantum information can be negative

Even the most ignorant among us cannot know less than nothing. What could negative knowledge mean? In the everyday world we are accustomed to, negative knowledge makes no sense. But in the world where the laws of quantum mechanics hold sway, knowledge can be negative. In essence, one can have situations where someone knows more than everything, and it is in these situations where one finds negative knowledge. This negative knowledge turns out to be precisely the right amount to cancel the fact that we can know too much. Negative knowledge is due to exotic features of quantum information theory and by understanding that quantum knowledge can be negative, we gain deeper insights into such phenomena as quantum networks, quantum teleportation, quantum computation, and the very structure of the quantum world.

In more detail, given part of an unknown quantum state, we determine how much quantum communication is needed to obtain the full state. This is the partial information we need conditional on our previous information. It turns out to be given by an extremely simple formula, the conditional entropy. In the classical case, partial information must always be positive, but we find that in the quantum world this physical quantity can be negative. If the partial information is positive, the sender of the partial information needs to communicate this number of quantum bits to the receiver; if it is negative, they instead gain the corresponding potential for quantum communication in the future. The primitive that is introduced—quantum state merging—enables a systematic understanding of quantum network theory, and several such applications will be discussed.

CARLOS PEREZ, University of Waterloo, 200 University Ave. West, Waterloo, ON N2L 3G1
Models of Quantum Cellular Automata

In this talk we present a systematic view of Quantum Cellular Automata (QCA), a mathematical formalism of quantum computation. We present four QCA models, and compare them. One model we discuss is the traditional QCA, similar to those introduced by Shumacher and Werner, Watrous, and Van Dam. We discuss also Margolus QCA, also discussed by Schumacher and Werner. We introduce two new models, Coloured QCA, and Continuous QCA. We also compare our models with the established models. We give proofs of computational equivalence for several of these models. We show the strengths of each model, and provide examples of how our models can be useful to come up with algorithms, and implement them in real-world physical devices.

MARTIN ROETTELER, NEC Laboratories America, Inc.
On the Power of Random Bases in Fourier Sampling: Hidden Subgroup Problem in the Heisenberg Group

The hidden subgroup problem (HSP) provides a unified framework to study problems of group-theoretical nature in quantum computing such as order finding and the discrete logarithm problem. While it is known that Fourier sampling provides an efficient solution in the abelian case, not much is known for general non-abelian groups. Recently, some authors raised the question as to whether post-processing the Fourier spectrum by measuring in a random orthonormal basis helps for solving the HSP. Several negative results on the shortcomings of this random strong method are known. In this talk I will show that the random strong method can be quite powerful under certain conditions on the group G. In particular the HSP for finite Heisenberg groups can be solved using polynomially many random strong Fourier samplings followed by a possibly exponential classical post-processing without further queries.

Joint work with Jaikumar Radhakrishnan and Pranab Sen.

MARY BETH RUSKAI, Tufts University, Medford, MA 02155, USA

Completely bounded p-norms in quantum information theory

Proof of the multiplicativity of maximal p-norms of noisy quantum channels has been conjectured and is known to imply additivity of minimal entropy and several equivalent conjectures. The concept of a completely bounded norm has been defined in the context of operator spaces. A channel is a completely positive, trace-preserving (CPT) map Φ acting on the $d \times d$ matrices, which can be regarded as forming a Banach space associated with the Schatten p-norm. The completely bounded norm of Φ is defined in terms of the action of $I_m \otimes \Phi$ on tensor products of matrices, which generate a non-commutative vector-valued L_p space. The completely bounded norm of a tensor product of CPT maps is multiplicative. This implies that a certain type of minimal conditional entropy is additive.

This talk is based on joint work with I. Devetak, M. Junge and C. King. It is intended to be accessible to both operator algebraists and quantum information theorists.

ANDREAS WINTER, University of Bristol, Department of Mathematics, Bristol BS8 1TW, UK

Random coding for quantum information

In this talk, the conceptual and mathematical ideas in a Lloyd–Shor type proof of the quantum channel capacity theorem will be presented.

To be precise, we will look at a general *quantum channel* $\mathcal{N}$, *i.e.*, a completely positive and trace preserving linear map on density operators, and study block coding of quantum information for n instances $\mathcal{N}^{\otimes n}$ of the channel, for large n. After introducing these concepts in mathematical terms, we will study a specific random coding procedure, which we call *Haar-random codes*. These are akin to P. Shor's proposal [MSRI talk, Nov. 2002; lecture notes online at `http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/`]: the code is (essentially) a subspace of the sender's typical space, chosen according to the unitarily invariant measure.

The "standard" approach to analysing the performance of quantum codes [see S. Lloyd, PRA 1997; I. Devetak, IEEE IT 2005] proceeds by showing

(i) that a basis of the code subspace can be distinguished reliably by the receiver;

(ii) that the channel environment has almost no information about this basis;

(iii) finally, how these two elements imply that superpositions of the basis vectors can be error-corrected with high fidelity.

After highlighting this strategy and some of its technical difficulties, we will demonstrate a new strategy which has the advantage of leading to the result with minimal technical effort, and which is also conceptually nice. It entirely avoids the difficult step (ii), the privacy of the code against the environment, which comes out automatically. Instead, we show

(a) that a basis and its Fourier conjugate basis of the code subspace each can be distinguished reliably by the receiver;

(b) how a recently discovered information uncertainty relation [M. Christandl and AW, `quant-ph/0501090`] then implies that the *quantum mutual information* between sender and receiver is close to maximum—and the quantum mutual information between sender and environment is close to 0;

(c) finally, a simple algebraic reasoning [B. Schumacher and M. Westmoreland, Quantum Inf. Proc. 2002] shows the existence of a decoding procedure.

Time permitting, variations and other applications of the Haar-random coding will be shown.