

Institute for Quantum Information

Findings – 2000-01

Quantum information science is an exciting emerging field that addresses how fundamental physical laws can be harnessed to dramatically improve the acquisition, transmission, and processing of information. The primary goal of the Institute for Quantum Information (IQI) is to carry out and facilitate research in Quantum Information Science (QIS).

Quantum algorithms

Quantum computers, which process quantum states rather than classical bits, could solve certain problems far faster than any foreseeable digital computers. Our current understanding of the power of quantum computing is very limited. Arguably, the most important theoretical challenge in QIS is to better characterize the capabilities of quantum computers.

Motivated by the recent experimental activity in NMR quantum computation, Leonard Schulman (with Ambainis and Vazirani) has studied the computational power of a quantum computer whose initial state consists of one qubit in a pure state and a large number n of qubits in a highly mixed state [1]. They ask whether such a device is capable of simulating a quantum computation performed by a machine whose initial state consists of many pure qubits, and conclude that for the simulation to be possible n must be *exponentially* large. This is one of the sharpest results currently known about the power of noisy quantum computers.

The best known computational problems for which quantum computers achieve exponential speedups over classical algorithms (such as the factoring and discrete logarithm problems) can be formulated as abelian hidden subgroup problems: an easily computable function defined on an abelian group G is constant and distinct on the cosets of a subgroup H ; the problem is to find H . Schulman (with Grigni, Vazirani, and Vazirani) has investigated how effectively quantum computers can address *nonabelian* hidden subgroup problems [2]. On the positive side they find that the Fourier sampling method that solves the problem when G is abelian can also be effective if the group G is “almost abelian.” But on the negative side, they present evidence that the Fourier sampling cannot distinguish well between subgroups that are related by conjugation, or between certain pairs of nonconjugate pairs of subgroups.

Motivated by the immense success of random walk and Markov chain methods in the design of

classical algorithms, Ashwin Nayak (with Ambainis, Bach, Vishwanath, and Watrous) has studied *quantum* Markov processes [3, 4]. They analyze in detail the behavior of *quantum walks* in one dimension, and show that a quantum walk on a circle mixes in *linear* time, in contrast to the quadratic mixing time for the corresponding classical walk. Their results indicate that quantum analogs of classical Markov processes may provide a new, systematic way of speeding up classical algorithms based on random walk and Markov chain techniques.

Quantum communication and cryptography

The study of quantum communication complexity has produced the surprising result that, although a qubit can carry only one classical bit of information, the communication cost of solving a problem can be reduced exponentially if qubits are exchanged instead of classical bits. With Klauch, Ta-Shma, and Zuckerman, Nayak has studied the relation between the total number of qubits of communication required and the number of *rounds* of communication needed – they find that allowing just one more round can reduce the quantum communication complexity *exponentially* [5]. This result implies that any efficient quantum protocol for certain problems, such as Set Disjointness, must necessarily involve many rounds of communication. A useful by-product of this work has been the development of several techniques which are relevant to quantum cryptography and quantum coin-flipping protocols.

Because it is not possible to acquire information about a quantum state without producing a detectable disturbance of the state, cryptographic protocols that use quantum information rather than classical data can achieve a higher level of security than is possible with classical protocols. With Gottesman, John Preskill has proposed a new method by which two parties can establish unbreakable codes for secure communication [6]. Previous schemes for quantum key distribution are vulnerable to an eavesdropping attack if the parties do not have a reliable source that emits a single photon on demand; the Gottesman-Preskill protocol requires instead a source of *squeezed light*. Adapting a method of proof applied earlier by Preskill and Shor [7], Gottesman and Preskill show that their key distribution scheme is secure against any eavesdropping attack allowed by the laws of quantum physics.

The structure of entangled quantum states can be elucidated by considering what transformations among multipartite quantum states can be achieved with local operations and classical communication. Graduate student Sumit Daftuar (with Klimesh) has studied the properties of the *trumping relation* among bipartite states, characterizing which among such transformations can be implemented by using an entangled *catalyst*. They show that almost all bipartite entangled states are potentially useful as catalysts, and that useful catalysts can have arbitrarily high dimension.

Quantum error correction

Large-scale quantum computers cannot operate reliably unless suitable methods are developed to protect encoded quantum states from decoherence and other potential sources of error. With Gottesman and Kitaev, Preskill has invented novel new types of quantum error-correcting codes [8]. In particular, they described for the first time how quantum information can be robustly encoded in the infinite-dimensional Hilbert space of a system described by *continuous quantum variables*, such as a mode of the electromagnetic field in a small cavity. Furthermore, they have formulated complete protocols whereby a device containing many such modes could execute a quantum computation fault tolerantly — a computation implemented with imperfect hardware could obtain the right answer with a high probability. The experimental tools needed to perform the computation are plausibly available in the quantum optics laboratory: linear optical elements, squeezers, and photon counters.

One of the key problems in quantum information theory is to determine the quantum capacity of a noisy quantum channel. Preskill and Harrington have used new quantum coding methods based on the geometry of numbers to establish lower bounds on the quantum capacity of a particular channel of considerable intrinsic interest – the *Gaussian quantum channel* [9]. Their result offers nontrivial support for an important general conjecture about the quantum channel capacity: that the capacity coincides with the asymptotic coherent information optimized over input states.

Concatenated quantum error-correcting codes are studied to estimate the *accuracy threshold* for fault-tolerant quantum computation, but estimates performed up to now use conservative approximations. Andrew Doherty, John Doyle, Hideo Mabuchi, IQI visitor Salman Habib, and graduate student Ben Rahn (with Jacobs) have produced preliminary results that show promise for improving our ability to simulate and to characterize the performance of concatenated codes [10]. Their approach is to use the symmetries inherent in the quantum code as much as possible to simplify the problem, and then to adopt *minimal realization and model reduction* techniques from control theory to perform approximate simulations that have guaranteed error bounds. They hope to increase the number of concatenation layers that can be used in numerical studies of the performance of quantum codes for realistic error models, and so to improve the estimate of the accuracy threshold.

Quantum teleportation

As part of an ongoing program to delineate the quantum versus classical boundaries for quantum information processing, Jeff Kimble (with Braunstein, Fuchs, and van Loock) has carried out extensive theoretical investigations of the teleportation of coherent states of light [11]. Specifically, they examined the Bell-inequality violation exhibited by continuous-variable EPR states, finding that the threshold for entanglement to serve as a quantum resource for teleportation coincides with

the onset of violation of local realism. These results agree with a previous analysis based on using a classical channel (without entanglement) to simulate teleportation.

The Kimble group is carrying out an ongoing experimental investigation of quantum information processing with continuous quantum variables, including an effort to increase the fidelity for quantum teleportation of coherent states of light. A new optical layout for mode matching of entangled EPR beams has been implemented leading to improved homodyne efficiency (from $\eta^2 = 0.80$ to $\eta^2 = 0.90$, which enters directly into the overall fidelity for teleportation). They have also obtained new nonlinear crystals for parametric down conversion to generate the EPR beams; this has improved the efficiency, but blue-light induced absorption is still the major limiting factor.

Quantum parameter estimation and quantum control

Future quantum technologies will hinge on the ability to control intricate quantum states, but quantum systems are notoriously delicate and difficult to control. To respond to this challenge, IQI researchers are working on connecting quantum formalism with control theory and signal processing. This work aims to develop new practical methods in quantum information technology while elucidating the relationship between physical principles and issues of optimal measurement and control.

Classical physics places no intrinsic limitations on the sensitivity of measurements, but in quantum physics measurements cause an uncontrolled back action on the measured system that imposes a *Standard Quantum Limit* (SQL) on measurement precision. With IQI visiting student Frank Verstraete, Mabuchi and Doherty have developed a new formalism for sensitivity optimization in continuous quantum measurements [12]. Their work synthesizes quantum trajectory theory with the engineering theory of Kalman filtering, and provides a new way of understanding the origin of the SQL for the estimation of a parameter such as a classical force acting on a test mass. They show that improved precision can be attained by varying the measurement sensitivity throughout the course of an extended measurement.

One central challenge in QIS is to devise new experimental protocols that push forward the boundaries of quantum-limited measurement. The Mabuchi group is currently performing an experiment to achieve an *adaptive measurement* of optical phase with a sensitivity below the SQL. Existing theory, which had assumed that the measurement device responds instantaneously, is not adequate to interpret the experimental results; hence Doherty has extended the theory to incorporate the effects of finite bandwidth. The new theory will have many applications to future experiments aimed at realizing quantum communication or computation protocols.

The Kimble group reported an experiment that trapped and tracked single atoms inside an optical resonator, realizing a new form of optical microscopy [13]. An ongoing theoretical effort led by Doherty has been elucidating the trapping dynamics in cavity QED through extensive numerical

simulations. They developed a quasiclassical model for the motion of atoms strongly coupled to the light field in an optical cavity, and showed that the model is in quantitative agreement with recent experiments. The techniques they have developed have broad applications to quantum feedback control in open quantum systems.

Quantum information and fundamental physics

Quantum information science holds promise not only to point the way toward future technologies, but also to shed light on issues in fundamental physics. Preskill and graduate student Dave Beckman (with Gottesman and Nielsen) launched a new approach to classifying and exploring the causality properties of quantum operations in a relativistic setting [14]. Most notably, they discovered a curious gap between the *causal* operations that are consistent with relativistic causality, and the *localizable* operations that can be implemented by spacelike-separated parties who share entangled quantum states that have been prepared in advance. This work raises intriguing questions about the extent to which the principles of relativistic quantum theory are dictated by the requirement that information is forbidden to travel outside the forward light cone.

References Cited

- [1] A. Ambainis, L. J. Schulman and U. Vazirani, Computing with highly mixed states, Proceedings of the Thirty-Second Annual ACM Symposium on the Theory of Computing (2000).
- [2] M. Grigni, L. J. Schulman, M. Vazirani and U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, Proceedings of the Thirty-Third Annual ACM Symposium on the Theory of Computing (2001).
- [3] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous, One-dimensional quantum walks, Proceedings of the Thirty-Third Annual ACM Symposium on the Theory of Computing (2001).
- [4] A. Nayak and A. Vishwanath, Quantum walk on the line, quant-ph/0010117.
- [5] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman, Interaction in quantum communication and the complexity of Set Disjointness, Proceedings of the Thirty-Third Annual ACM Symposium on the Theory of Computing (2001), quant-ph/0005106 and quant-ph/0004100.
- [6] D. Gottesman and J. Preskill, Secure quantum key distribution using squeezed states, Phys. Rev. A 63 (2001) 022309, quant-ph/0008046.
- [7] J. Preskill and P.W. Shor, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441, quant-ph/0003004.

- [8] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, *Phys. Rev. A*, to appear, quant-ph/0008040.
- [9] J. Harrington and J. Preskill, Achievable rates for the Gaussian quantum channel, quant-ph/0105058.
- [10] A. C. Doherty, J. C. Doyle, H. Mabuchi, K. Jacobs, and S. Habib, Robust control in the quantum domain, to appear in Proceedings of the 39th IEEE Conference on Decision and Control (2001), quant-ph/0105018.
- [11] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, Quantum versus classical domain for teleportation with continuous variables, *Phys. Rev. A*, to appear, quant-ph/0012001.
- [12] F. Verstraete, A. C. Doherty, and H. Mabuchi, Sensitivity optimization in quantum parameter estimation, quant-ph/0104116.
- [13] A. C. Doherty, T. W. Lynn, C. J. Hood, and H. J. Kimble, Trapping of single atoms with single photons in cavity QED, *Phys. Rev. A* 63 (2001) 013401, quant-ph/0006015.
- [14] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, Causal and localizable quantum operations, quant-ph/0102043.