

Institute for Quantum Information

Findings – 2001-02

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. Our research covers six broad areas: (1) Quantum algorithms that achieve speedups relative to classical algorithms, and limits on such algorithms. (2) Quantum cryptographic protocols, and other types of communication using quantum states. (3) Quantum entanglement and the theory of transformations among quantum states. (4) Protection of quantum information using quantum error correcting codes and fault tolerant protocols for quantum information processing. (5) Theory and practice regarding physical implementations of quantum information processing. (6) Connections between quantum information science and other aspects of fundamental physics.

Quantum algorithms and quantum complexity

Efficient quantum algorithm for Pell's equation. 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 quantum information science is to better characterize the capabilities of quantum computers.

Sean Hallgren recently has formulated an efficient quantum algorithm for the principle ideal problem over real quadratic number fields [1]. An important application of Hallgren's method is to a problem that has been studied for over 1000 years: finding integer solutions (x, y) to Pell's equation $x^2 - dy^2 = 1$, where d is an integer that is not a perfect square. This problem is at least as hard as factoring integers, and the best known classical algorithm for solving Pell's equation is exponentially slower than the best known classical algorithm for factoring. In fact, a cryptosystem based on Pell's equation has been constructed which it had been hoped would be stronger than cryptosystems based on the difficulty of factoring. Hallgren's new algorithm breaks this cryptosystem.

Tight quantum lower bound for the collision problem. To better understand the capabilities of

quantum computers, it is important to establish *lower bounds* that place limits on what a quantum computer can do. Yaoyun Shi has found a tight lower bound on the *collision problem*: Given a function f , the problem is to find x and y such that $f(x) = f(y)$, under the promise that such inputs exist. Since the security of fundamental cryptographic primitives depends on the difficulty of finding collisions, quantum lower bounds for the collision problem provide evidence for the existence of cryptographic primitives that are immune to quantum cryptanalysis.

Classically, of order $n^{1/2}$ evaluations of the function are necessary and sufficient, where n is the number of possible values of the input. Shi's new bound establishes that of order $n^{1/3}$ evaluations are necessary and sufficient in the quantum case [2]. Shi's tight bound improved on an weaker lower bound found earlier by IQI visitor Scott Aaronson [3].

BQNP. Alexei Kitaev's recently published book (with Shen and Vyalvi) contains many new results concerning quantum algorithms and quantum complexity [4]. For example, a new proof of the Solovay-Kitaev theorem is presented, which establishes an accurate complexity bound on the approximation of a unitary transformation by a circuit constructed from universal gates. Kitaev also defined a new computational class BQNP (a quantum analog of NP or MA) and gave an example of a BQNP-complete problem; this could be regarded as the quantum analog of the Cook-Levin theorem, the fundamental result of classical complexity theory.

Quantum simulation with homogeneous operations. One important application for quantum computers is to the simulation of other quantum systems. Guifre Vidal, with Masanes and Latorre, investigated how quantum simulation can be achieved with suitable control operations [5]. In particular, they discussed how Hamiltonian evolution can be simulated using homogeneous operations (operations that act identically on all qubits). Their findings have interesting applications, since homogeneous operations are readily available in some solid-state implementations of quantum computation.

Quantum communication and quantum cryptography

Same-sided bias in quantum coin flipping. In some cases, like key exchange, it is known that cryptographic protocols can achieve a higher level of security if the parties communicate by sending quantum states rather than classical bits. A particularly important cryptographic primitive is coin tossing. Consider a game in which Alice and Bob perform local quantum computation and send qubits back and forth. At the end of the game, both players are to make measurements that determine the outcome of a fair coin toss. Is there a way to design the game so that the coin toss is fair, where neither party by cheating can bias the outcome? It was already known that no classical or quantum protocol can accomplish this task perfectly. But do protocols exist such that the bias is arbitrarily small?

Kitaev has recently obtained an important negative result: that *any* quantum coin tossing

protocol is susceptible to same-sided bias [6]. Specifically, let p_A be the maximum probability that Bob finds the outcome “heads” when Alice cheats and let p_B be the maximum probability that Alice finds the outcome “heads” when Bob cheats. Kitaev shows that the product $p_A p_B$ is greater or equal to $1/2$. Thus in a symmetric protocol $p_A = p_B = 1/\sqrt{2}$.

Limits on entanglement-assisted communication. It has long been known that if Alice and Bob share quantum entanglement, then Alice can send classical information to Bob with improved efficiency: sending a single qubit can convey two bits (“superdense coding”). However optimal bounds on the probability of error in entanglement-assisted communication had been elusive. Recently, Ashwin Nayak with IQI visiting student Julia Salzman derived such a bound, which applies irrespective of the number of rounds of communication or the amount of entanglement consumed (all that matters is the number of bits being conveyed, and the number of qubits that travel from Alice to Bob) [7]. Their bound is obtained from surprisingly simple linear algebra techniques; an immediate consequence is a near-optimal lower bound on the communication complexity of the Inner Product function.

Hiding quantum data. Recent work has shown how to use the laws of quantum mechanics to keep classical and quantum bits secret in a number of different circumstances, such as private quantum channels, quantum secret sharing and quantum data hiding. Now Patrick Hayden, Barbara Terhal, and IQI long-term visitor David DiVincenzo have shown that a method for keeping two classical bits hidden in any such scenario can be used to construct a method for keeping one quantum bit hidden, and vice-versa [8]. This gives a simple proof that two bits of shared randomness are required to construct a private quantum channel hiding one qubit. Furthermore, bipartite and multipartite hiding schemes for qubits can be constructed from the previously known constructions for hiding bits. The only constraints on the authorized sets for these multipartite hiding schemes are the same as those for quantum secret sharing, namely, monotonicity and the no-cloning theorem.

Quantum entanglement and quantum information theory

Trading quantum for classical resources in data compression. One of the fundamental challenges in quantum information theory is to identify and quantify the basic resources that can be used for communication in quantum theory. The basic resources are classical communication (in bits), quantum communication (in qubits) and entanglement (in ebits), and it is interesting to see how these resources are related. Patrick Hayden, with Jozsa and Winter, has established the precise rate at which qubits and bits can be traded against each other for the task of “visible” quantum data compression [9]. The techniques are quite generally applicable; for example they can also be used to establish the optimal trade-off between bits and ebits for the task of remotely preparing quantum states.

Embezzling quantum states. The study of distributed processing in quantum mechanics invari-

ably leads to questions about the nature of entanglement and the resources required to transform a given state shared between two or more parties into a different state. A surprising phenomenon in the theory of entanglement transformations is “catalysis” — the presence of a catalytic state may enable a transformation between two other states to occur, even though the catalyst remains intact at the end of the transformation. Hayden, with van Dam, demonstrated that if the choice of catalysts is unrestricted and arbitrarily small errors are tolerated, then it becomes possible to create entanglement out of nothing; that is entanglement can be “embezzled” from the catalyst without damaging it noticeably [10]. This result demonstrates that allowing arbitrary catalysts (as had been commonplace in previous work) is essentially unphysical.

Entanglement transformations with limited communication. In most studies of entanglement transformations achieved with local operations and classical communication (LOCC) it is assumed that classical communication is free and unlimited. In recent work with Winter and with van Dam, Hayden has quantified the *amount* of classical (or quantum) communication needed to accomplish various tasks [11, 12]. In particular, they proved a tight bound on the amount of communication required to perform entanglement dilution (the conversion of the standard form of entanglement into a desired type). This work established for the first time a fundamental asymmetry between the tasks of entanglement concentration and dilution.

Bell inequalities with classical communication. Bell inequalities, by quantifying the sense in which quantum entanglement is a stronger resource than shared classical randomness, characterize a fundamental distinction between quantum and classical information. Dave Bacon and graduate student Ben Toner have studied generalizations of Bell inequalities that take into account the amount of classical communication that is needed to simulate quantum correlations with classical correlations [13, 14]. In particular, they find that the correlations between measurements made on a two-qubit Bell state can be explained by augmenting shared classical randomness with a single bit of communication. That “correlations between 1 Bell pair = classical shared randomness + 1 bit” is a new and significant way to quantify the power of quantum entanglement.

Entanglement of purification. A major task in quantum information theory is to find useful ways to quantify quantum entanglement. Terhal and DiVincenzo, with Debbie Leung (who will join IQI later this year) and Michal Horodecki have laid the foundations for a unified theory that attaches value to *all* correlations, both quantum and classical [15]. Their new measure, the entanglement of purification, is a natural analog of standard measures of entanglement, but can be applied in broader settings, and suggests new approaches to the important problem of quantifying correlations in many-particle systems.

Structure of entanglement generating sets. A goal of quantum information theory is to identify and classify the distinct types of multi-partite entanglement. What minimal set of entangled states is sufficient for reversibly generating, via LOCC, all of the possible states that could be shared by n parties? This problem remains open, but recent work by Vidal with Acin and Cirac has sharpened

and clarified the question. They identified a conservation law respected by asymptotically reversible entanglement transformations, and used it to show that Bell pairs and three-party Greenberger-Horne-Zeilinger (GHZ) states are not adequate for reversibly generating all three-part states [16]. This work emphasizes the elusiveness of a full understanding of many-party entanglement.

Tests for entanglement. If a bipartite mixed quantum state is specified, can we determine whether the state is entangled? No efficient algorithm is known that is guaranteed to answer this question for all states. Andrew Doherty, and students Federico Spedalieri and Pablo Parrilo, have constructed a hierarchy of new efficient tests for entanglement that work for a broader class of states than previous tests [17]. They observe that a family of simple properties of separable (unentangled) states may be checked using semidefinite programming, a computationally tractable class of convex optimization. Using analytic properties of semidefinite programs, one can construct observables (“entanglement witnesses”) that could in principle be measured in the laboratory in order to prove that a state is entangled.

Quantum error correction and fault tolerance

Phase transition in noisy quantum computers. Large-scale quantum computers cannot operate reliably unless quantum states are suitably protected from damage that could be caused by decoherence and other potential sources of error. Quantum error-correcting codes and fault tolerant protocols have been developed for this purpose, but these methods are ineffective if the noise afflicting the computer is too strong. Kitaev and John Preskill, with students Eric Dennis and Andrew Landahl, have identified a sharp phase transition between the low-noise regime in which error correction can succeed and the high-noise regime in which error correction is ineffective, and they have formulated powerful methods for analyzing the properties of this transition [18]. They considered *topological* codes in which error recovery can easily be executed using only local quantum gates, found that the phase transition can be identified with a phase boundary in a lattice gauge theory with quenched disorder, and estimated the critical noise strength. Their work suggests that topological codes provide a promising framework for quantum computing architectures.

Nonabelian anyons in a simple spin model. A related approach to building a decoherence-resistant quantum memory has been explored by Kitaev [19]. He constructed an exactly solvable but highly nontrivial quantum spin model in two dimensions, and showed that the spectrum of the model contains nonabelian anyons, quasiparticles that exhibit an exotic type of identical-particle statistics. Because the long-range statistical interactions of these particles are impervious to local noise, the charges carried by the particles can encode robust quantum information.

Continuous quantum error correction. As usually formulated, the implementation of quantum error correction requires fast projective measurements and fast unitary gates, which might not be available in many laboratory settings. With student Charlene Ahn, Doherty and Landahl

have proposed new methods for protecting quantum states from a noisy environment, based on weak but continuous measurements (like those available in optical cavity quantum electrodynamics experiments) and feedback conditioned on measurement results [20]. Their protocol outperforms conventional methods in protecting quantum states if the time between error correction cycles is limited.

Model reduction for concatenated quantum codes. One way to achieve robust processing of quantum information is to employ concatenated quantum codes, a hierarchy of error-correcting codes within codes. Doherty, Hideo Mabuchi, and student Ben Rahn have developed new tools for analyzing the performance of concatenated codes [21]. They have shown that the effect of adding a level of concatenation can be expressed as an iterative map acting on an error model for encoded quantum information, and they have found unstable fixed points of these maps corresponding to the accuracy threshold for quantum storage. They have also adapted the control theory method of balanced truncation to analyze codes with many levels of concatenation. These tools provide new insights into how codes can be matched to the special features of a particular error model.

Experiment and implementation

Challenging quantum limits on measurement precision with real-time feedback. 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.

Mabuchi and Doherty, with students Michael Armen, John Au, and John Stockton, have demonstrated the power of real-time feedback in quantum metrology, by confirming the superior performance of an adaptive homodyne technique for single-shot measurement of optical phase [22]. For phase measurements performed on weak coherent states with no prior knowledge of the signal phase, they found that the variance of adaptive homodyne estimation approaches closer to the fundamental quantum uncertainty limit than any previously demonstrated technique. Current work aims to extend these results on adaptive quantum measurement to feedback control of the conditional quantum dynamics of collective spin states in optical lattices.

Quantum noise in gravitational wave detectors. In the next decade, exquisitely sensitive interferometric detectors may open a new window on the universe by detecting the gravitational wave signals emitted during the cataclysmic coalescence of very distant sources such as neutron star and black hole binaries. A great challenge for the science of quantum measurement will be to conceive, design, and construct new detectors that will achieve the sensitivity needed to acquire detailed information about these spectacular astrophysical events. Kip Thorne and IQI visitors

Vladimir Braginsky, Farid Khalili, Sergey Vyatchanin, with their collaborators, have carried out a definitive analysis of the quantum noise that limits the sensitivity of interferometric gravitational-wave detectors [23], showing that limitations due to quantum behavior of the test masses used in an interferometer are already fully accounted for by photon shot noise and radiation-pressure back-action noise. This work will help to point the way toward optimal designs for future advanced interferometers.

Storing quantum information in atomic ensembles. Many methods for implementing quantum information processing in the laboratory have been proposed and are being actively pursued, but all are difficult. A serious problem for most methods is that decoherence is too rapid to be effectively resisted with active error control. Luming Duan has been exploring approaches to quantum computation that use macroscopic *ensembles* of atoms to store and manipulate quantum states, a method with some naturally fault tolerant features. These methods seem to be feasible with current technology, and scalable to systems with many encoded qubits. In particular, Duan has proposed an experimentally feasible scheme to generate multiqubit entangled “cat states” based on simple linear optical operations and single-photon detection [24]. These states can be used for demonstrations of quantum nonlocality, for high-precision spectroscopy, and for more general types of quantum information processing.

Until recently, calculations of the properties of interactions between atomic ensembles and light have used simplified one-dimensional models, which are not adequate for accurately describing realistic experimental situations. Recently, Duan with Cirac and Zoller developed a three-dimensional theory that confirms the collective enhancement of the signal-to-noise ratio, which is believed to be one of the main advantages of the ensemble-based quantum information processing schemes [25].

Design of photonic crystals for quantum computation. Combining photonic crystals with cavity QED methods is a promising path toward scalable quantum information processing. But the design of these photonic crystals is challenging, because of the small cavity volume and low loss required for cavity QED experiments. Recently Mabuchi, JM Geremia and Jon Williams have posed photonic crystal design as a formal inverse problem and applied mathematical analysis tools roughly based on optimal control theory [26]. This approach led to an analytical solution for the two-dimensional photonic crystal design problem and a concise numerical algorithm for optimizing more complex structures, such as photonic crystal slabs. The approach should apply equally well to photonic crystal design problems beyond cavity QED.

Quantum information and fundamental physics

Observables of gauge field theories. Quantum information science holds promise not only to point the way toward future technologies, but also to shed light on issues in fundamental physics. Kitaev and Preskill, with Daniel Gottesman and student David Beckman, have been investigating the

implications of the theory of quantum operations for the algebra of observables in relativistic quantum field theories, including the gauge theories that are used to describe the fundamental interactions of elementary particles [27].

The basic observables of nonabelian gauge theories are Wilson loop operators, which encode the effect on the color of a quark due to covariant transport around a closed path. Among the surprising conclusions found by these authors is that the nondemolition measurement of a spacelike Wilson loop operator is impossible in a relativistic nonabelian gauge theory. They also found that abelian electric charge (but not nonabelian charge) can be transported superluminally, without any accompanying transmission of information. These studies raise provocative 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] S. Hallgren, Polynomial-time algorithms for Pell's equation and the principal ideal problem, Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing (2002).
- [2] Y. Shi, Quantum lower bounds for the collision and the element distinctness problems, quant-ph/0112086 (2002).
- [3] S. Aaronson, Quantum lower bound for the collision problem, Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing (2002), quant-ph/0111102.
- [4] A. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics, Volume 47 (American Mathematical Society, 2002), 257 pages.
- [5] L. Masanes, G. Vidal, and J. I. Latorre, Time-optimal Hamiltonian simulation and gate synthesis using homogeneous local unitaries, quant-ph/0202042 (2002).
- [6] A. Kitaev, Any quantum coin tossing protocol is susceptible to same-sided bias, unpublished (2002).
- [7] A. Nayak and J. Salzman On communication over an entanglement-assisted quantum channel, Proceedings of the Thirty-Fourth Annual ACM Symposium on the Theory of Computing (2002).
- [8] D. DiVincenzo, P. Hayden, and B. M. Terhal, Hiding quantum data, unpublished (2002).
- [9] P. Hayden, R. Jozsa, and A. Winter, Trading quantum for classical resources in quantum data compression, quant-ph/0204038 (2002).
- [10] W. van Dam and P. Hayden, Embezzling entangled quantum states, quant-ph/0201041 (2002).

- [11] P. Hayden and A. Winter, On the communication cost of entanglement transformations, quant-ph/0204092 (2002).
- [12] W. van Dam and P. Hayden Renyi-entropic bounds on quantum communication, quant-ph/0204093 (2002).
- [13] D. Bacon, Bell inequalities with communication, unpublished (2002).
- [14] D. Bacon and B. Toner, The cost of quantum correlations, unpublished (2002).
- [15] B. M. Terhal, M. Horodecki, D. W. Leung, D. P. DiVincenzo, The entanglement of purification, J. Math. Phys., accepted, quant-ph/0202044 (2002).
- [16] A. Acin, G. Vidal, J. I. Cirac, On the structure of a reversible entanglement generating set for three-partite states, quant-ph/0202056 (2002).
- [17] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Distinguishing separable and entangled states, Phys. Rev. Lett. 88, 187904 (2002), quant-ph/0112007.
- [18] E. Dennis, Alexei Kitaev, A. Landahl, and J. Preskill, Topological quantum memory, J. Math. Phys., accepted, quant-ph/0110143 (2002).
- [19] A. Kitaev, Anyons in a spin model on the honeycomb lattice, unpublished (2002).
- [20] C. Ahn, A. C. Doherty, A. J. Landahl, Continuous quantum error correction via quantum feedback control, Phys. Rev. A 65, 042301 (2002), quant-ph/0110111.
- [21] B. Rahn, A. C. Doherty, and H. Mabuchi, Exact and approximate performance of concatenated quantum codes, quant-ph/0111003 (2002).
- [22] M. A. Armen, J. K. Au, J. K. Stockton, A. C. Doherty, H. Mabuchi, Adaptive homodyne measurement of optical phase, quant-ph/0204005 (2002).
- [23] V. B. Braginsky, M. L. Gorodetsky, F. Ya. Khalili, A. B. Matsko, K. S. Thorne, and S. P. Vyatchanin, The noise in gravitational-wave detectors and other classical-force measurements is not influenced by test-mass quantization, gr-qc/0109003 (2001).
- [24] L.-M. Duan, Entangling many atomic ensembles through laser manipulation, Phys. Rev. Lett. 88, 170402 (2002), quant-ph/0201128.
- [25] L.-M. Duan, J. I. Cirac, and P. Zoller, Three-dimensional theory for interaction between atomic ensembles and free-space light, quant-ph/0205005 (2002).
- [26] JM Geremia, J. Williams and H. Mabuchi, An inverse problem approach to designing photonic crystals for cavity QED, unpublished (2002).

- [27] D. Beckman, D. Gottesman, A. Kitaev, and J. Preskill, Measurability of Wilson loop operators, Phys. Rev. D 65, 065022 (2002), hep-th/0110205.