

Institute for Quantum Information

Findings – 2005-06

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, fault tolerant protocols for quantum information processing, and control of quantum systems. (5) Theory and practice regarding physical implementations of quantum information processing. (6) Connections between quantum information science and other aspects of fundamental physics.

In the nine month period from 1 September 2005 to 31 May 2006, IQI participants have produced 35 publications, which we summarize here.

Quantum algorithms and quantum complexity

Graph isomorphism as a nonabelian hidden shift problems. Andrew Childs and Pawel Wocjan argued that it is more natural to approach the graph isomorphism problem as a hidden shift problem, instead of the more standard view of regarding it as a hidden subgroup problem [1]. However, they concluded that the problem is still hard when approached in this way, in two senses: (1) $\Omega(n)$ copies of the hidden shift state are necessary to solve the problem efficiently (where n is the number of vertices in the graph), and (2) if one is restricted to single-register measurements, then an exponential (in n) number of hidden shift states are required.

Physical limits of heat-bath algorithmic cooling. Leonard Schulman (with Mor and Weinstein), described a new, efficient initialization procedure for open quantum systems [2]. With this procedure, an n -qubit device that is originally maximally mixed, but is in contact with a heat bath of bias $\epsilon \gg 2^{-n}$, can be almost perfectly initialized. This performance is optimal due to a newly discovered threshold effect: for bias $\epsilon \ll 2^{-n}$ no cooling procedure can, even in principle (running indefinitely without any decoherence), significantly initialize even a single qubit.

Efficient algorithm for a quantum analogue of 2-SAT. Sergey Bravyi formulated a quantum analogue of the satisfiability problem (“quantum k -SAT”), and showed that quantum 2-SAT can be solved efficiently by a classical computer [3]. He also showed that for $k \geq 4$ quantum k -SAT is a complete problem for the complexity class QMA with one-sided error. Quantum k -SAT is the problem of determining whether an n -qubit pure state exists whose k -qubit reduced density matrices have support on prescribed subspaces.

Quantum algorithms and applications for the Jones polynomial. Pawel Wocjan and Jon Yard found new quantum algorithms for approximating the evaluations of knot polynomials [4]. Their polynomial-time algorithm achieves an additive approximation at any primitive root of unity to the Jones polynomial for links obtained from a general type of closure of a braid, generalizing recent results of Aharonov, Jones and Landau, and also provides an additive approximation to the HOMFLYPT two-variable polynomial of the trace closure of a braid, evaluated at certain pairs of points. They also found self-contained proofs that a quantum computation can be simulated by an approximate evaluation of the Jones polynomial, that evaluating the Jones polynomial is $\#P$ -hard, and that learning its most significant bit is PP-hard, and they formulated QCMA-complete and PSPACE-complete problems based on braids.

Quantum communication and quantum cryptography

Quantum key distribution based on arbitrarily-weak distillable entangled states. Debbie Leung, with Horodecki, Lo, and Oppenheim, formulated a protocol for the secure distribution of states that encode private correlations, yet have little or no distillable entanglement [5]. The protocol enables two parties to extract from an untrusted bipartite state an arbitrarily long secure key, and establishes that there are quantum channels that have zero capacity for transmitting high-fidelity quantum states, yet have a nonzero capacity for distributing a private key.

Capacities for quantum broadcast channels. Jon Yard, with Hayden and Devetak, proved a variety of results for quantum channels with one sender and two receivers [6]. Building on known classical results, they analyzed a general scenario where Alice sends a personal message to Bob while simultaneously sending a common message to Bob and Charlie. They established achievable rates for several different tasks, obtaining regularized capacity formulas for general channels, while also getting single-letter formulas for certain special classes of broadcast channels.

Improved rates for quantum key distribution based on distillation of twisted states. Graeme Smith, with Renes, found a new method for analyzing the security of quantum key distribution protocols that employ noisy preprocessing and one-way postprocessing of the key [7]. They showed that the security of the protocol is equivalent to that of an associated key distribution protocol in which, instead of the usual maximally-entangled states, a more general type of private state called a twisted state is distilled. The noisy preprocessing allows some phase errors to be left

uncorrected without compromising the privacy of the key, thus improving the rate at which secure final key can be extracted.

Communicating over adversarial quantum channels using quantum list codes. Graeme Smith and Debbie Leung studied communication rates over adversarial quantum channels, in which an adversary who knows the communication protocol can apply any operation that acts on at most a fraction p of the transmitted qubits [8]. (Most previous work on quantum Shannon theory considered the scenario where identical quantum channels are used many times.) They showed that the rate of high-fidelity quantum communication is much higher than would be naively expected, if the sender and receiver use a secret key whose length is logarithmic in the number of qubits sent. To achieve these communication rates, they introduced the concept of a fully quantum list code, where the decoder reduces the number of possible errors to a short list.

Degenerate quantum coding for Pauli channels. Graeme Smith, with Smolin, studied the communication rates achievable over Pauli channels using a family of degenerate quantum codes [9]. (A code is degenerate if it can sometimes correct more errors than can be uniquely identified.) Though there were previously known examples of channels for which degenerate codes achieve a quantum communication rate beyond that achievable with nondegenerate codes, Smith and Smolin found much larger improvements for some channels, and, by studying how the optimal code varies as a function of channel parameters, they reached a deeper understanding of the role of degeneracy in quantum coding.

Quantum entanglement and quantum information theory

Typical entanglement of stabilizer states. Graeme Smith and Debbie Leung characterized the typical entanglement of a randomly chosen bipartite stabilizer state [10]. They showed that if the number of qubits each party holds is large, then the state is close to maximally entangled with probability exponentially close to one. They also showed that typically very few GHZ states can be extracted from a random multipartite stabilizer state via local unitary operations. They obtained these results using a new tool: a concentration inequality that bounds deviations from the mean of random variables that are naturally defined on the Clifford group.

Monogamy of nonlocal quantum correlations. Ben Toner derived upper bounds on the correlations in a bipartite physical system that follow only from the requirement that superluminal signaling is impossible, without assuming the validity of quantum mechanics [11]. He also showed that in a tripartite system ABC , forcing classical correlations between B and C prevents A and B from violating certain Bell inequalities. These results can be applied to find proofs of security for cryptographic protocols, assuming only the impossibility of superluminal signaling.

Review of the theory of entanglement in graph states. Robert Raussendorf, with Hein, Dür, Eisert, Van den Nest, and Briegel, authored a comprehensive review of the multi-

partite entanglement exhibited by graph states [12]. Graph states have a variety of applications in quantum information theory, most prominently as algorithmic resources in the context of the one-way quantum computer, but also in other fields such as quantum error correction and multipartite quantum communication, as well as in the study of foundational issues such as nonlocality and decoherence.

Modeling Pauli measurements on graph states with nearest-neighbor classical communication. Stefano Pironio, with Barrett, Caves, Eastin, and Elliott, introduced a communication-assisted local-hidden-variable model that predicts the outcomes of measurements of arbitrary Pauli operators in arbitrary graph states [13]. Within this model, communication is restricted to a single round of message passing between adjacent nodes of the graph. They also showed that any model of this type is incapable, for at least some graph states, of reproducing the correlations for all subsets of the individual measurements in a Pauli product.

Accurate quantum state estimation via “Keeping the experimentalist honest”. Robin Blume-Kohout, with Hayden, derived a unique procedure for quantum state estimation from a simple, self-evident principle: an experimentalist’s estimate of the quantum state generated by an apparatus should be constrained by honesty [14]. A skeptical observer should subject the estimate to a test that guarantees that a self-interested experimentalist will report the true state as accurately as possible. They also found a non-asymptotic, operational interpretation of the quantum relative entropy function.

Quantum error correction, fault tolerance, and control

Fault-tolerant one-way quantum computer. Robert Raussendorf and Kovid Goyal, with Harrington, proved a quantum accuracy threshold theorem for the one-way quantum computer [15]. Their proof is based on a novel scheme, in which a noisy cluster state in three spatial dimensions is transformed to a high-fidelity topologically encoded two-dimensional cluster state; concatenated quantum codes protect the non-Clifford gates in a universal fault-tolerant gate set.

Fault-tolerant quantum computation with long-range correlated noise. John Preskill and Alexei Kitaev, with Aharonov, found a new proof of the quantum accuracy threshold theorem that applies to non-Markovian noise with algebraically decaying spatial correlations [16]. The proof shows that an arbitrarily long quantum computation can be executed with high reliability in D spatial dimensions, if the perturbation is sufficiently weak and decays with the distance r between the qubits faster than $1/r^D$.

Fault-tolerant quantum computation for local leakage faults. Panos Aliferis, with Terhal, rigorously analyzed fault-tolerant quantum computation in the presence of local leakage faults [17], and proved a quantum accuracy threshold theorem that covers this case. Their proof adapts the methods developed earlier by Aliferis, Gottesman, and Preskill to encompass leakage-reduction

units, such as those based on quantum teleportation. They also described how to optimize the overhead cost of leakage reduction, and showed that measurement-based computation is inherently tolerant against leakage faults.

Universal quantum computation with the $\nu = 5/2$ fractional quantum Hall state. Sergey Bravyi developed the theory of quantum computation using nonabelian anyons, and explained how to achieve universal quantum computation in the simplest realistic model — the Pfaffian state realized in fractional quantum Hall systems at electron filling factor $\nu = 5/2$ [18]. Using distillation schemes for magic states that he had proposed earlier with Kitaev, Bravyi showed that one rather noisy nontopological gate, together with the topological gates, suffices for computational universality. Assuming that all topological operations are implemented perfectly, he proved that the threshold error rate for non-topological operations is above 14%, and that the total number of non-topological computational operations needed to simulate a quantum circuit with L gates scales as $L(\log L)^3$.

Optimal pointers for joint measurement of sigma-x and sigma-z via homodyne detection. Luc Bouten, with Janssens, found the optimal pointers for joint measurement of non-commutative observables of a two-level system that is being observed continuously via homodyne detection [19]. That the optimal pointers depend only on the propagator of the unnormalized (Zakai) quantum filter can be exploited in real-time quantum parameter estimation.

Optimal error tracking via quantum coding and continuous syndrome measurement. Ramon van Handel and Hideo Mabuchi constructed optimal filters for tracking accumulative errors in continuous quantum error detection, and assessed their performance for the bit-flip and five-qubit codes [20]. They showed that a tight upper bound on the stochastic decay of encoded fidelity can be computed from the measurement records.

Separation theorem for quantum control. Luc Bouten and Ramon van Handel developed the rigorous theory of continuous quantum measurements and nonlinear filtering with real-time feedback [21]. They introduced the notion of a controlled quantum flow, where feedback is taken into account by allowing the coefficients of the quantum stochastic differential equation to be adapted processes in the observation algebra. They proved a separation theorem for quantum control: the admissible control that minimizes a given cost function is only a function of the filter, provided that the associated Bellman equation has a sufficiently regular solution.

Introduction to noncommutative quantum filtering theory. Luc Bouten and Ramon van Handel, with James, wrote an introductory article on quantum filtering [22]. They described the construction of Wiener and Poisson processes on Fock space, and the use of the Itô calculus for modeling of physical systems. They also derived quantum filtering equations for system-probe models from quantum optics.

Experiment and implementation

Feedback cooling of atomic motion in cavity QED. Hideo Mabuchi, with Steck, Jacobs, Habib, and Bhattacharya, analyzed the real-time state estimation needed to control the motion of an atom in an optical cavity [23]. They derived an approximate estimation equation for this purpose, and used it in a feedback algorithm designed to cool the atomic motion. They examined the effectiveness of the procedure using full simulations of the cavity QED system, including the quantized motion of the atom in one dimension.

Measurement-induced entanglement for excitation stored in remote atomic ensembles. James Chou, Hugues de Riedmatten, Daniel Felinto, Sergey Polyakov, Steve van Enk, and Jeff Kimble reported observations of entanglement between two atomic ensembles located in distinct apparatuses on different tables [24]. Quantum interference in the detection of a photon emitted by one of the samples projected the otherwise independent ensembles into an entangled state with one joint excitation stored remotely in 10^5 atoms at each site. They confirmed the entanglement by mapping the state of the atoms to optical fields and by measuring mutual coherences and photon statistics for these fields.

Low-lying bifurcations in cavity quantum electrodynamics. Mike Armen and Hideo Mabuchi performed a computational study of some elementary bifurcations that occur in a driven and damped cavity QED model at low intracavity photon number [25]. They used the single-atom cavity QED master equation and associated stochastic Schrödinger equations to characterize the equilibrium distribution and dynamical behavior of the quantized intracavity optical field in parameter regimes near points in the semiclassical bifurcation set, and found that the semiclassical limit sets are qualitatively preserved in the quantum stationary states, although quantum fluctuations apparently induce phase diffusion within periodic orbits and stochastic transitions between attractors.

Efficient retrieval of a single excitation stored in an atomic ensemble. Julien Laurat, Hugues de Riedmatten, Daniel Felinto, James Chou, Erik Schomburg, and Jeff Kimble reported significant improvements in the retrieval efficiency of a single excitation stored in an atomic ensemble and in the subsequent generation of strongly correlated pairs of photons [26]. They demonstrated a 50% probability to transform the stored excitation into one photon in a well-defined spatio-temporal mode; the two-photon component of the emitted states was less than 1% of the value for a coherent state.

Connecting quantum information with the rest of physics

Detecting nonabelian statistics in the $\nu = 5/2$ fractional quantum Hall state. Parsa Bonderson, Alexei Kitaev, and Kirill Shtengel proposed an interferometric test of non-Abelian

statistics in fractional quantum Hall systems, that would provide the first proof of principle in the lab of one of the primitive elements of a topological quantum computer [27]. This paper (and an independent paper by Halperin and Stern that appeared at the same time) set in motion an intense race to confirm the predicted experimental signal, as is featured in the Search and Discovery section of the October 2005 *Physics Today* and in the April 2006 *Scientific American*.

Topological entanglement entropy. Alexei Kitaev and John Preskill discovered a new type of universal “topological quantum entanglement” that arises in topologically ordered gapped two-dimensional media [28]. Using methods borrowed from topological quantum field theory, they found a formula for the entropy that characterizes this topological entanglement, in terms of the properties of the superselection sectors of the medium.

Entanglement renormalization. Guifre Vidal developed a real-space method for renormalizing entangled quantum states of lattice systems in any number of spatial dimensions [29]. Numerical simulations in one dimension show that the resulting coarse-grained site requires a Hilbert space dimension that does not grow with successive scale transformations. With this method one can analyze the ground state of a critical system comprising tens of thousands of quantum spins with a computational effort that scales logarithmically in the system’s size.

Engineered quantum critical points between matrix product states. Frank Verstraete, with Wolf, Ortiz, and Cirac, investigated quantum phase transitions in spin chain systems characterized by local Hamiltonians with matrix product ground states [30]. In particular, they described how to “engineer” quantum critical points that separate phases with specified properties. Some of these quantum critical points depart from the standard paradigm; for example, the ground state energy remains analytic, and the entanglement entropy of a half-chain stays finite. These exotic transitions can occur at the triple point of conventional quantum phase transitions.

Theory of simulated emission by black holes. Greg Ver Steeg, with Adami, showed that rotating black holes clone infalling quantum states with a fidelity that depends on the adsorption coefficient [31]. In particular, perfectly reflecting black holes are optimal universal quantum cloners. For any adsorption probability less than one, the cloning fidelity is nearly optimal for a range of black hole parameters.

Exactly solvable critical quantum models from classical spin models. Frank Verstraete, with Wolf, Perez-Garcia, and Cirac, found that projected entangled-pair states (PEPS) on two-dimensional lattices exhibit a rich variety of quantum many-body phenomena [32]. They showed that coherent versions of thermal states of any local two-dimensional classical spin model correspond to such PEPS, which are ground states of local two-dimensional quantum Hamiltonians. This correspondence leads to the construction of critical quantum models exhibiting a strict area law scaling of the entanglement entropy, despite power-law decaying correlations.

Theory of interferometry for nonabelian anyons. Parsa Bonderson and Kirill Shtengel, with Slingerland, developed a general theory of how two-particle interferometers can detect the

nontrivial braiding statistics of nonabelian anyons [33]. They related the visibility of interference fringes to the topological S -matrix, and found explicit predictions for the case of the Read-Rezayi state (admitting universal topological gates) that is believed to describe the recently observed $\nu = 12/5$ quantum Hall plateau.

Approximating ground states of spin systems with weighted graph states. Frank Verstraete, with Anders, Plenio, Dür, and Briegel, introduced a new variational method, based on superpositions of weighted graph states, for approximating ground states of strongly interacting spin systems in arbitrary geometries and spatial dimensions [34]. All local observables can be efficiently computed in such states, which can have diverging correlation length and unbounded multi-particle entanglement. The approach gives excellent approximations to the ground state energy of the Ising model in one, two, or three dimensions, and also can be applied to lattice field theories.

Time required to establish many-body quantum correlations. Sergey Bravyi and Frank Verstraete, with Hastings, obtained lower bounds on the time required to establish quantum correlations under local Hamiltonian evolution [35]. Using the Lieb-Robinson bound, which establishes an effective light cone with exponentially decaying tails, they showed that there is a finite speed at which correlations and entanglement can be distributed. They also proved lower bounds on the time it takes to convert states without topological quantum order to states with that property, and showed that the rate at which entropy can be created in a block of spins scales with the boundary of that block.

References Cited

- [1] A. Childs and P. Wocjan, On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems, arXiv: quant-ph/0510185 (2005).
- [2] L. Schulman, T. Mor, and Y. Weinstein, Physical limits of heat-bath algorithmic cooling, Physical Review Letters 94, 120501 (2005).
- [3] S. Bravyi, Efficient algorithm for a quantum analogue of 2-SAT, arXiv: quant-ph/0602108 (2006).
- [4] J. Yard and P. Wocjan, The Jones polynomial: quantum algorithms and applications in quantum complexity theory, arXiv: quant-ph/0603069 (2006).
- [5] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Quantum key distribution based on arbitrarily-weak distillable entangled states, Phys. Rev. Lett. 96, 070501 (2006), arXiv: quant-ph/0510067.
- [6] J. Yard, P. Hayden, and I. Devetak, Quantum broadcast channels, arXiv: quant-ph/0603098 (2006).

- [7] J. M. Renes and Graeme Smith, Noisy preprocessing and the distillation of twisted states, arXiv: quant-ph/0603262 (2006).
- [8] D. Leung and G. Smith, Communicating over adversarial quantum channels using quantum list codes, arXiv: quant-ph/0605086 (2006).
- [9] G. Smith and J. A. Smolin, Degenerate coding for Pauli channels, arXiv: quant-ph/0604107 (2006).
- [10] G. Smith and D. Leung, Typical entanglement of stabilizer states, arXiv: quant-ph/0510232 (2005).
- [11] B. Toner, Monogamy of nonlocal quantum correlations, arXiv: quant-ph/0601172 (2006).
- [12] M. Hein, W. Dür, Jens Eisert, Robert Raussendorf, M. Van den Nest, and H. Briegel, Entanglement in graph states and its applications, arXiv: quant-ph/0602096 (2006).
- [13] J. Barrett, C. M. Caves, B. Eastin, M. B. Elliott, and S. Pironio, Modeling Pauli measurements on graph states with nearest-neighbor classical communication, arXiv: quant-ph/0603032 (2006).
- [14] R. Blume-Kohout and P. Hayden, Accurate quantum state estimation via “Keeping the experimentalist honest,” arXiv: quant-ph/0603116 (2006).
- [15] R. Raussendorf, J. Harrington, and K. Goyal, A fault-tolerant one-way quantum computer, arXiv: quant-ph/0510135 (2005).
- [16] Dorit Aharonov, Alexei Kitaev, and John Preskill, Fault-tolerant quantum computation with long-range correlated noise, Phys. Rev. Lett. 96, 050504 (2006), arXiv: quant-ph/0510231.
- [17] P. Aliferis and B. M. Terhal Fault-tolerant quantum computation for local leakage faults, arXiv: quant-ph/0511065 (2005).
- [18] S. Bravyi, Universal quantum computation with the $\nu = 5/2$ fractional quantum Hall state, Phys. Rev. A 73, 042313 (2006), arXiv: quant-ph/0511178.
- [19] B. Janssens and L. Bouten, Optimal pointers for joint measurement of sigma-x and sigma-z via homodyne detection, J. Phys. A: Math. Gen. 39, 2773-2790 (2006), arXiv: quant-ph/0510086 (2005).
- [20] R. van Handel and H. Mabuchi, Optimal error tracking via quantum coding and continuous syndrome measurement, arXiv: quant-ph/0511221 (2005).

- [21] L. Bouten and R. van Handel, On the separation principle of quantum control, arXiv: math-ph/0511021 (2005).
- [22] L. Bouten, R. van Handel, and M. James, An introduction to quantum filtering, arXiv: math.OC/0601741 (2006).
- [23] D. Steck, K. Jacobs, H. Mabuchi, S. Habib, and T. Bhattacharya, Feedback cooling of atomic motion in cavity QED, arXiv: quant-ph/0509039 (2005).
- [24] C.-W. Chou, H. de Riedmatten, D. Felinto, S. Polyakov, S. J. van Enk, and H. Jeff Kimble, Measurement-induced entanglement for excitation stored in remote atomic ensembles, arXiv: quant-ph/0510055 (2005).
- [25] M. A. Armen, H. Mabuchi, Low-lying bifurcations in cavity quantum electrodynamics. arXiv: quant-ph/0602170 (2006).
- [26] J. Laurat, H. de Riedmatten, D. Felinto, C.-W. Chou, E. Schomburg, H. J. Kimble, Efficient retrieval of a single excitation stored in an atomic ensemble, arXiv:quant-ph/0605122 (2006).
- [27] P. Bonderson, A. Kitaev, and K. Shtengel, Detecting non-Abelian statistics in the $\nu = 5/2$ fractional quantum Hall state, Phys. Rev. Lett. 96, 016803 (2006), arXiv: cond-mat/0508616.
- [28] A. Kitaev and J. Preskill, Topological entanglement entropy, Phys. Rev. Lett. 96, 110404 (2006), arXiv: hep-th/0510092.
- [29] G. Vidal, Entanglement renormalization, arXiv: cond-mat/0512165 (2005).
- [30] M. Wolf, G. Ortiz, F. Verstraete, and J. I. Cirac, Quantum phase transitions in matrix product systems, arXiv: cond-mat/0512180 (2005).
- [31] C. Adami and G. L. Ver Steeg, Black holes are almost optimal quantum cloners, arXiv: quant-ph/0601065 (2006).
- [32] F. Verstraete, M. Wolf, D. Perez-Garcia, and J. I. Cirac, Criticality, the area law, and the computational power of PEPS, arXiv: quant-ph/0601075 (2006).
- [33] P. Bonderson, K. Shtengel, and J. K. Slingerland, Probing non-Abelian statistics with two-particle interferometry, arXiv: cond-mat/0601242 (2006).
- [34] S. Anders, M. Plenio, W. Dür, F. Verstraete, and H. Briegel, Ground state approximation for strongly interacting systems in arbitrary dimension, arXiv: quant-ph/0602230 (2006).
- [35] S Bravyi, M. Hastings, and F. Verstraete, Lieb-Robinson bounds and the generation of correlations and topological quantum order, arXiv: quant-ph/0603121 (2006).