

Institute for Quantum Information

Findings – 2003-04

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

Quantum Schur transform. 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. Dave Bacon, with Chuang and Harrow, has found an efficient quantum circuit for the unitary transform known as the *Schur transform* [1]. The Schur transform is useful for numerous quantum information tasks — optimal spectrum estimation, entanglement concentration, and hypothesis testing, among others. Previously these schemes were known to be optimal in a particular sense, but whether each optimal protocol could be efficiently implemented was not known.

Spatial search via the Dirac equation. Long-term IQI visitor Jeffrey Goldstone, with IQI visiting student Andrew Childs, studied the problem of quantumly searching a d -dimensional lattice of N sites for a single marked location, finding a Hamiltonian that solves this problem in time of order \sqrt{N} for $d > 2$ and of order $\sqrt{N} \log N$ in the critical dimension $d = 2$ [2]. This algorithm, using a lattice version of the Dirac Hamiltonian, matches the performance of a corresponding discrete-time

quantum walk algorithm.

NP problems from quantum codes. Sergey Bravyi and IQI visitor Mike Vyalyi studied generalized stabilizer quantum codes defined for a system of n qudits, and showed that these provide an efficient classical description for a class of quantum states [3]. This description has a length only polynomial in n , but requires additional information needed for a consistency check. They formulated a formal decision problem based on this observation, and proved that the problem belongs to the class NP.

Entanglement and interactive proof systems. Interactive proof systems provide a natural framework for studying quantum nonlocality. Student Ben Toner, with Cleve, Høyer and IQI visitor John Watrous, have exhibited two-prover interactive proof systems that are sound for classical provers, but are no longer sound if the provers are allowed to share entanglement [4]. For several simple games, they obtained bounds on the extent to which entangled provers can cheat, and on the amount of entanglement required for optimal and nearly optimal quantum strategies.

Universality of multi-body interactions. Bacon, with IQI visitor Michael Nielsen and visiting students Mick Bremner and Jennifer Dodd, addressed the power of multi-body interactions (along with local control) to produce a universal set of quantum interactions [5, 6], thus extending previous work where only two-body interactions were considered. They showed that for the case of systems comprised entirely of qubits, there are exactly two different universality classes for these interactions, given local control of the qubits. These two classes are either fully universal or can be made universal through suitable encodings. Furthermore, for multi-body interactions among systems with more than two levels (“qudits”) they showed that there is only one universality class.

Improvements in measurement-based quantum computation. Debbie Leung, with Childs and Nielsen, formulated simple and efficient schemes, based on the concept of “one-bit teleportation,” for realizing universal quantum computing using only one-qubit and two-qubit projective measurements [7]. They also obtained the first systematic derivations of schemes for universal “one-way quantum computing,” in which a quantum circuit is simulated using only one-qubit measurements performed on a “cluster state” that is prepared in advanced. Furthermore, Leung discovered that measurement-based universal quantum computing can be achieved with a deterministic number of steps [8]. In addition, Leung and student Panos Aliferis, erected a comprehensive theory that provides a unified understanding of both measurement-based quantum computing and one-way quantum computing, finding many further improvements in the efficiency of both models [9].

Optimal decomposition of two-qubit gates into controlled-not gates and single-qubit gates. One standard set of quantum gates that suffices for universal quantum computation contains a single two-qubit gate, the controlled-not, and arbitrary single-qubit gates. Guifre Vidal, with IQI visiting student Chris Dawson, studied the implementation of arbitrary two-qubit unitary transformations using this gate set [10]. They showed by an explicit construction that three controlled-not gates always suffice, and that this number is optimal. They also identified the subset of two-qubit gates that can be performed using only two controlled-not gates.

Quantum communication and quantum cryptography

Oblivious transfer in quantum cryptography. Another central topic in quantum information science is quantum cryptography, which unlike quantum computation is already realizable with existing technology. One significant distinction between quantum and classical cryptography is that in a quantum setting, two parties with access to a black box that realizes perfect bit commitment can use it to achieve secure quantum oblivious transfer, and hence secure two-party computation. But what if the bit commitment scheme is only (quantum) computationally secure? IQI Senior Scientist Dominic Mayers, with Crépeau, Dumais, and L. Salvail, has made progress on this important question by proving the security of a primitive called “quantum measurement commitment” when it is constructed from a commitment that is unconditionally concealing but computationally binding [11].

Self-testing of quantum devices. When analyzing the security of cryptographic protocols, we usually assume that the equipment used in the protocol can be trusted. But Mayers, with Yao, has observed that quantum nonlocality can be exploited to ensure that *local* flaws of detectors used in a quantum protocol cannot fool two parties into falsely believing they share an entangled state [12]. Therefore, the equipment can be “self-tested” and need not be trusted by the parties. Furthermore, Mayers, with Magniez, Mosca, and Ollivier, has extended this idea to the self-testing of quantum circuits, provided that gates that are synchronous in the ideal circuit are also synchronous in the circuit to be tested [13].

Key recycling in quantum authentication. In quantum authentication, the recipient of a quantum message uses a private key shared with the sender to verify that the message has not been modified during transmission. Patrick Hayden, Leung, and Mayers have shown that when authentication is successful, most of the classical key can be safely reused in further rounds of authentication [14]. Their proof uses the concept of “universal composability; — it is shown that authentication with key recycling can be used as a subroutine in other protocols without compromising security. It is known that quantum message authentication requires the message to be encrypted. Hayden, Leung, and Mayers also showed that for authentication of *pure* states, *approximate* encryption methods (discovered by Hayden, Leung, Shor, and Winter [15]) can be used in place of exact encryption, reducing the size of the initial key by a factor of two.

Improved quantum coin flipping protocols. Coin flipping is an example of a “post-cold-war” cryptographic task, where two mutually distrustful persons are trying to achieve a common goal. It was already known that quantum coin flipping protocols are more resistant to cheating than classical protocols. Student Carlos Mochon invented a new protocol for (weak) quantum coin-flipping, establishing a tighter bound on the effectiveness of cheating than had previously been known [16]. Mochon also analyzed the security of protocols in which many coins are flipped sequentially, and found improved bounds on the cheat sensitivity of quantum bit commitment protocols [17].

Unified approach to quantum Shannon theory. As compared to classical information theory, quantum information theory provides a bewildering zoo of new resources such as entanglement and quantum communication; indeed, due to the Heisenberg uncertainty principle, even knowledge of the task to be performed becomes a resource in quantum mechanics. Therefore, as our technical ability to solve various noisy communication and resource conversion problems improved over the past few years, we were nonetheless daunted by the number of possible ways these incommensurate resources could be combined and put to different uses. But advances during the past year have greatly simplified the emerging picture of two-party communication in quantum mechanics. Specifically, Hayden and Leung, with Devetak, have found the optimal ways to trade entanglement, noiseless bit communication, and noiseless qubit communication in order to make use of noisy entanglement and noisy channels [18]. These problems include as special cases entanglement distillation, hybrid quantum-classical channel capacities, entanglement-assisted channel capacities, and both teleportation and superdense coding through noisy states. The solution involves constructing a pair of “grandmother” and “grandfather” protocols that generate the optimal protocols for all these other tasks. These operational links demonstrate that the seemingly unrelated tasks are all equivalent to each other; basic questions, like the structure of the optimal encoding, can be answered for the easiest case and then exported to the rest.

Superdense coding of entangled quantum states. One of the basic tasks of quantum information theory is to send quantum states from one location to another. When the sender knows which state she is trying to send, the task is known as “remote state preparation” [19]. Last year’s report described work of Hayden and student Anura Abeyesinghe that calculated the optimal methods to use entanglement, classical, and quantum communication to perform remote state preparation [20]. Insights from that unification effort have led to the formulation of a “father” protocol for this task: superdense coding of entangled quantum states. A previous method for constructing this father protocol, devised by Hayden, Leung, and IQI visitor Aram Harrow [21], was indirect. Now Abeyesinghe, Hayden, student Graeme Smith, and IQI visitor Andreas Winter [22] have found a much more transparent direct construction that is universal in a way that the indirect version was not — it can be used to send *any* quantum state, not just one of the highly structured type that appears in block compression. One consequence is that for large n , a receiver can identify $2n$ qubits using n “entangled bits” and a sublinear amount of forward communication. (Identification means correctly answering the question, “Is this state the one I think it is, or not?”)

Distributed compression of quantum information. Hayden and Winter, with Andrew Doherty and student Charlene Ahn, have completed a long-standing project on the compression of correlated quantum sources [23]. This work should provide a starting point for the development of methods for manipulating quantum information in a distributed environment. In contrast to the analogous classical theorem of Slepian and Wolf, they found a surprising variety of different regimes. Under some quite general conditions, no interesting compression is possible, while under other conditions,

compression using techniques related to entanglement distillation can be performed.

Multipart quantum data hiding. Data hiding is a cryptographic task in which information is shared among multiple parties in such a way that only particular authorized subsets of the parties can access the shared information. Hayden, Leung, and Smith developed protocols for multipart quantum data hiding such that very little information about a shared quantum state can be recovered by groups of up to $k - 1$ parties who are limited to local operations and classical communication (LOCC), yet the state can be almost perfectly reconstructed by LOCC among all parties together with quantum communication among any k parties [24]. These protocols achieve an asymptotic rate of one hidden qubit per local physical qubit, a substantial improvement over previously known quantum data hiding protocols.

Tradeoff between forward and backward communication using bidirectional channels. Bidirectional channels (nonlocal bipartite gates or Hamiltonians) can communicate quantum or classical messages simultaneously in both directions. Using the concepts of coherent classical communication and entanglement recycling, Leung and Harrow characterized the tradeoff between the forward and backward communication of four kinds (classical-classical, classical-quantum, quantum-classical, quantum-quantum) in terms of the tradeoff for forward and backward classical communication.

Quantum communication in a spin chain. Might “naturally occurring” local interactions be exploited to achieve reliable quantum communication? Leung and Sougato Bose, with IQI visiting student Man-Hong Yung, described how a two-qubit gate acting on the two spins at the ends of a three-qubit XY chain can be realized [26]. In their protocol, the spin in the middle is initialized once, and no further manipulation is needed. The gate can generate one ebit, or transfer a qubit in one direction, or simultaneously transfer one classical bit in each direction.

Fermionic Gaussian channels. Sergey Bravyi introduced and classified fermionic Gaussian channels, which map fermionic Gaussian states into Gaussian states [27]. These channels can be naturally described in terms of Gaussian integrals over Grassmann variables. Bravyi used this formalism to calculate explicitly how a measurement of occupation numbers affects a fermionic Gaussian state.

Quantum entanglement and quantum information theory

Maximally entangled subspaces. The crucial feature that distinguishes quantum information and classical information is quantum entanglement, the nonlocal correlations among the parts of a quantum system that have no classical analog. Hayden, Leung, and Winter [28] have discovered exotic quantum states whose entanglement of formation is nearly as large as that of a maximally entangled state, yet with negligible entanglement of distillation. These states are entanglement “black holes” — virtually none of the entanglement required for their creation can ever be recovered.

Kochen-Specker theorem for generalized measurements. The Kochen-Specker theorem is a basic result in the foundations of quantum theory stating that any hidden variable theory seeking

to reproduce quantum theory must be *contextual*. Traditionally the Kochen-Specker theorem has been applied to projective measurements, but Bacon, Toner, and IQI visitor Michael Ben-Or have proved it for generalized measurements [29]. Their new proof applies to two-dimensional quantum systems, for which the original Kochen-Specker theorem with projective measurements did not hold. Furthermore, by formulating the Kochen-Specker theorem in the language of classical communication complexity, Bacon, Toner, and Ben-Or have proposed a method for *quantifying* contextuality; this makes it possible to state precisely the information-processing advantages that contextuality confers.

Simulating joint correlation observables. Continuing their earlier work on the classical communication cost of simulating quantum correlations, Bacon and Toner have shown that all two-party joint correlation observables can be simulated using an amount of communication bounded by a *polynomial* in the dimension of the entangled state [30]. This new result gives further evidence supporting the conjecture that all correlations produced by measuring entangled quantum states can be exactly simulated using infinite shared randomness and an amount of communication *proportional* to the dimension of the entangled state.

Locally unconvertible bound entangled states. Bound entangled states are states that require entanglement for their creation, but where no entanglement can be distilled using LOCC. Is it possible to use LOCC to convert one bound entangled state to another? Sergey Bravyi studied interconvertibility of multipartite entangled states [31], proving among other things that there exist three-qubit bound entangled states that cannot be converted into one another by LOCC [32]. This conclusion holds even for approximate non-deterministic conversion.

Quantum error correction and fault tolerance

Distillation of quantum software. 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, and a key ingredient in these protocols is the off-line preparation of “quantum software” that is subsequently consumed during the execution of certain quantum gates that are needed to complete a universal set. Bravyi and Alexei Kitaev [33] have discovered purification protocols that can be used to create high fidelity quantum software states. One interesting application of their protocols establishes that universal quantum computation is achievable in a model in which symplectic gates can be executed reliably, and a suitable supply of *noisy* ancilla states is provided (where the noise rate for the ancilla can be as large as about 20%). These results suggest that a sharp boundary can be identified between the “classical” and “quantum” phases of such models.

Improved depth blowup for quantum fault tolerance. With fault-tolerant methods, we can faith-

fully simulate an ideal quantum circuit using noisy quantum gates. But to protect against errors, quantum information must be encoded redundantly, which causes a blowup in the circuit size (number of gates needed) and the circuit depth (the time needed to execute the circuit). In previous work it had been shown that the depth of the circuit using noisy gates need be no larger than the depth of the ideal circuit times a power of the $\log L$, where L is the size of the ideal circuit. Ahn and John Preskill [34] have shown that this cost in depth can be reduced to a factor of $\log \log L$. Their proof combines ideas about topological encoding of quantum information with methods that had been developed to ensure the robustness of classical cellular automata.

Stabilization of topological quantum memory using local rules. Topological coding provides a particularly powerful way to protect quantum information from damage. In work reported last year, Preskill and student Jim Harrington had analyzed the accuracy threshold for toric codes, assuming that quantum processing to measure error syndromes is local, but allowing fast nonlocal classical processing of the measurement outcomes. Now Ahn and Harrington [35] have extended the analysis to the case in which all quantum and classical processing is local, by developing procedures for error recovery that require only local communication. They proved the existence of an accuracy threshold in this model, with the critical error rate larger than 10^{-11} ; numerical results suggest that the actual threshold is at least 10^{-4} .

Anyon computation with smaller groups. Mochon has continued to pursue another approach to protecting a quantum computation from decoherence — computing with *anyons* [36]. After showing last year that anyonic magnetic fluxes taking values in a non-solvable finite group are adequate for universal quantum computation, Mochon developed new techniques to establish a stronger result: it suffices that the group not be nilpotent [37]. Mochon’s new constructions are based on using charged particles to achieve the fault-tolerant preparation of suitable quantum software.

Continuous-time quantum error correction using weak measurements. Typical theoretical studies of quantum fault tolerance assume tools such as fast projective measurements that are not always available in realistic laboratory settings. Continuing work cited in previous reports, Charlene Ahn has studied error correction protocols using more plausible tools, such as weak measurements accompanied by quantum feedback. With Wiseman and Jacobs [38], she formulated more general schemes that recover from errors that are detected by performing suitable measurements on the environment, and with Sarovar, Jacobs, and Milburn [39], she formulated feedback schemes that require less classical processing of measurement results than previous protocols.

Experiment and implementation

Strongly-coupled one-atom laser. One promising approach to quantum information processing is based on establishing strong coupling between single atoms and single photons. For several years, Jeff Kimble’s group has been working to achieve improved isolation of single atoms inside high

finesse optical cavities. Now McKeever, Boca, Boozer, Buck and Kimble have reported the experimental realization of a one-atom laser that generates light with strongly nonclassical properties such as photon antibunching and sub-Poissonian photon statistics [40]. In a follow-up theoretical paper, the authors developed the theory of the strongly-coupled laser pumped by coherent external fields, and made quantitative comparisons of the theory with experimental results [41].

Generation of single photons using atomic ensembles. The production of single photons on demand is a critical capability for linear optics quantum computing and quantum cryptography. Chou, Polyakov, Kuzmich, and Kimble have realized a scheme for generating single photons based on transferring quantum information from a collective excitation of a cold atomic ensemble to an electromagnetic field mode [42]. The single-quantum properties of the pulse were confirmed through measurements of the field correlations.

Scalable photonic quantum computation through cavity-assisted interaction. Luming Duan and Kimble proposed a scheme for scalable photonic quantum computation based on cavity assisted interactions between single-photon pulses [43]. A quantum controlled phase-flip gate between the single-photon pulses is achieved by successively reflecting the pulses from an optical cavity with a single-trapped atom. They demonstrated that the proposal is robust against practical noise and experimental imperfections in current cavity-QED setups.

Experimental demonstration of quantum feedback control. JM Geremia and student John Stockton, with Hideo Mabuchi, demonstrated experimentally the use of real-time feedback to stabilize conditional preparation of entangled (spin-squeezed) states of large numbers of atoms [44]. They used continuous optical Faraday rotation to monitor one Cartesian component of the net magnetization vector of a cloud of cold atoms, and showed that they could achieve sensitivity at the level of the quantum projection noise. They also demonstrated the use of real-time feedback via a transverse magnetic field to remove the projection offset, resulting in the first demonstration of unconditional preparation of spin-squeezing.

Feedback control of quantum state reduction. Stockton and fellow student Ramon van Handel, with Mabuchi, analyzed the problem of using continuous quantum non-demolition measurement and real-time feedback to stabilize quantum state preparation for a single qubit [45]. This appears to be the simplest problem in which issues of quantum-mechanical measurement backaction and coherent control can be brought together in a scenario that is both experimentally relevant and amenable to mathematical analysis. They introduced a new method for proving global stability of a feedback law, based on mathematical tools from the classical theory of stochastic nonlinear control. This work shows for the first time that strong analytic proofs are possible in quantum feedback control theory, and in particular that continuous measurement and real-time feedback control can be proven to be more robust than analogous discrete operations, for the purpose of high-fidelity qubit or ancilla initialization in quantum computation.

Deterministic Dicke state preparation with continuous measurement and control. Further work

by Stockton, van Handel and Mabuchi [46] established concrete connections between the theoretical work on global stability and the ongoing experimental effort to apply real-time feedback to spin-squeezed states. Through numerical simulations, they found compelling evidence that real-time feedback can be used for *deterministic* preparation of entangled states. Previous work had proposed schemes for non-deterministic generation of entangled states via measurement and conditioning, where the states are obtained randomly and with low probability. The new results show that if continuous measurements rather than discrete measurements are used, feedback can ensure that the desired outcome occurs with high probability.

Connecting quantum information with the rest of physics

Efficient algorithms for simulation of quantum many-body systems. Quantum information science holds promise not only to point the way toward future technologies, but also to shed light on issues closer to the core of physics. A particularly exciting field in which ideas about quantum information may prove to be fruitful is quantum many-body physics, in which collective entangled states of many qubits can exhibit exotic behavior that can be probed in experiments. Continuing to pursue work reported last year in which he discovered that slightly entangled quantum computations can be simulated efficiently by classical computers [47], Guifre Vidal formulated a new efficient method for simulating the real-time evolution of one-dimensional many-body systems with quite general local interactions [48]. This method is founded on a clear and simple description of how the parts of the system are entangled with one another. Recently Vidal in collaboration with Daley, Kollath, and Schollwoeck, has clarified the connections between his algorithm and established density-matrix-renormalization-group (DMRG) methods [49], and the new methods are being eagerly accepted, refined, and exploited by the sizable DMRG community.

Evolution of quantum entanglement along renormalization-group flows. Quantum systems evolve *irreversibly* when “coarse-grained” to study their long-distance properties, because information about short distance fluctuations is irretrievably lost. However, no satisfying information-theoretic description of this irreversibility has ever been formulated. Now Vidal, extending work reported last year with Latorre and Rico [50], has calculated how the quantum entanglement of a block of contiguous spins decreases along a renormalization group trajectory in the critical Ising spin chain [51]. Their calculations connect the loss of entanglement with a systematic reordering of the eigenvalues of the reduced density matrix of the block.

Quantum computational complexity in the presence of closed timelike curves. Is time travel possible? One way to probe this fascinating question about fundamental physics is to examine the impact of time travel on the foundations of computer science. Dave Bacon has shown that if one builds a quantum computer that has access to some qubits that traverse closed timelike curves, then this quantum computer can efficiently solve hard computational problems — namely those in

the class NP [52]. Bacon also demonstrated the robustness of this computational power against slight imperfections in the computer’s hardware.

Superselection rules and quantum protocols. We say that a game is *secure* if a cheater who breaks the rules is unable to alter the outcome of the game. Kitaev, Mayers, and Preskill studied the impact of local conservation laws (superselection rules) on the security of quantum games [53]. Naively, it seems that in an *invariant* world subject to a superselection rule, a cheater would have less power than in the *unrestricted* world, not subject to a superselection rule. But on the contrary, Kitaev, Mayers, and Preskill showed that any cheating strategy in the unrestricted world can be accurately simulated in the invariant world. Aside from clarifying general issues regarding the security of quantum protocols, by explaining how the physics of the invariant world can be simulated in the unrestricted world and vice versa, the authors also clarified the physical implications of superselection rules, which have a central role in modern quantum field theory.

Quantum circuits for black hole information flow. Do black holes destroy information? No question about fundamental physics is more vexing, or has deeper implications for the foundations of quantum theory. With IQI visitor Daniel Gottesman, Preskill studied whether the black hole information paradox can be resolved by imposing a suitable boundary condition at the singularity inside the black hole [54]. Drawing on the theory of quantum entanglement and quantum circuits, they concluded that in this setting the restoration of unitarity in black hole evaporation requires an implausible fine tuning of particle interactions — weak deformations of the interactions result unavoidably in weak violations of unitarity.

References Cited

- [1] D. Bacon, A. Harrow, and I. Chuang, An efficient quantum circuit for the Schur transform, in preparation.
- [2] A. Childs and J. Goldstone, Spatial search and the Dirac equation, arXiv: quant-ph/0405120 (2004).
- [3] S. Bravyi and M. Vyalyi, Commutative version of the k-local Hamiltonian problem and non-triviality check for quantum codes, arXiv: quant-ph/0308021 (2003).
- [4] R. Cleve, P. Høyer, B. Toner, and J. Watrous, Consequences and limits of nonlocal strategies, Proceedings of the 19th IEEE Conference on Computational Complexity (CCC 2004), arXiv: quant-ph/0404076.
- [5] M. J. Bremner, J. L. Dodd, M. A. Nielsen, and D. Bacon, Fungible dynamics: There are only two types of entangling multiple-qubit interactions, Phys. Rev. A, 69, 012313 (2004)

- [6] M. J. Bremner, M. A. Nielsen, and D. Bacon, Simulating Hamiltonian dynamics using many-qudit Hamiltonians and local unitary control, arXiv: quant-ph/0405115 (2004).
- [7] A.M. Childs, D. W. Leung, and M. A. Nielsen, Unified derivations of measurement-based schemes for quantum computation, arXiv: quant-ph/0404132 (2004).
- [8] D. W. Leung, Quantum computation by measurements, *Int. Jour. Quant. Inf.* 2, No. 1, 33-43 (2004), arXiv: quant-ph/0310189.
- [9] P. Aliferis and D. W. Leung, Computation by measurements: a unifying picture, arXiv: quant-ph/0404082 (2004).
- [10] G. Vidal and C. M. Dawson, A universal quantum circuit for two-qubit transformations with three CNOT gates, *Phys. Rev. A* 69, 010301 (2004), arXiv: quant-ph/0307177.
- [11] C. Crépeau, P. Dumais, D. Mayers and L. Salvail, Computational collapse of quantum state with application to oblivious transfer, in *Proceedings of First Theory of Cryptography Conference*, *Lecture Notes in Computer Science* 2951, February 2004.
- [12] D. Mayers and A. Yao, Self testing quantum apparatus, arXiv: quant-ph/0307205 (2003).
- [13] F. Magniez, D. Mayers, M. Mosca and H. Ollivier, Self testing quantum circuits, in preparation.
- [14] P. Hayden, D. Leung and D. Mayers, The composability of quantum authentication with key recycling, in preparation.
- [15] P. Hayden, D. Leung, P. Shor and A. Winter, Randomizing quantum states: Constructions and applications *Comm. Math. Phys.*, accepted (2004), arXiv: quant-ph/0307104.
- [16] C. Mochon, Quantum weak coin-flipping with bias of 0.192, arXiv: quant-ph/0403193 (2004).
- [17] C. Mochon, Serial composition of quantum coin-flipping, and bounds on cheat detection for bit-commitment, arXiv: quant-ph/0311165 (2003).
- [18] I. Devetak, P. Hayden and D. Leung, Towards a unification of quantum Shannon theory, in preparation.
- [19] C. Bennett, P. Hayden, D. Leung, P. Shor and A. Winter, Remote preparation of quantum states, *IEEE Trans. Inf. Theory*, accepted (2004), arXiv: quant-ph/0307100.
- [20] A. Abeyesinghe and P. Hayden, Generalized remote state preparation: Trading qubits and ebits in quantum communication, *Phys. Rev. A* 68:062319 (2003), arXiv: quant-ph/0308143.
- [21] A. Harrow, P. Hayden and D. Leung, Superdense coding of quantum states, *Phys. Rev. Lett.*, accepted (2004), arXiv: quant-ph/0308143.

- [22] A. Abeyesinghe, P. Hayden, G. Smith, A. Winter, Superdense coding of entangled quantum states, in preparation.
- [23] Charlene Ahn, Andrew Doherty, Patrick Hayden and Andreas Winter, On the distributed compression of quantum information, arXiv: quant-ph/0403042.
- [24] P. Hayden, D. Leung, and G. Smith, Multiparty quantum data hiding, in preparation.
- [25] A Harrow and D. Leung, Tradeoff between forward and backward communication using bidirectional channels, in preparation.
- [26] M.-H. Yung, D. W. Leung, Sougato Bose, An exact effective two-qubit gate in a chain of three spins, arXiv: quant-ph/0312105(2003).
- [27] S. Bravyi, Lagrangian representation for fermionic linear optics, arXiv: quant-ph/0404180 (2004).
- [28] P. Hayden, D. Leung and A. Winter, Maximally entangled subspaces, in preparation.
- [29] B. Toner, D. Bacon, and M. Ben-Or, Extending the Kochen-Specker theorem for generalized measurements, in preparation.
- [30] B. Toner and D. Bacon, The communication cost of simulating joint observable correlations, in preparation.
- [31] S. Bravyi, Requirements for compatibility between local and multipartite quantum states, Quantum Information Computation, Vol. 4, No. 1, p. 12 (2004) arXiv: quant-ph/0301014.
- [32] S. Bravyi, Unextendible product bases and locally unconvertible bound entangled states, aXiv: quant-ph/0310172 (2003).
- [33] S. Bravyi and A. Kitaev, Universal quantum computation based on magic states distillation, arXiv: quant-ph/0403025 (2004).
- [34] C. Ahn, Extending quantum error correction: new continuous measurement protocols and improved fault-tolerant overhead, Caltech Ph.D. thesis (2004).
- [35] J. Harrington, Analysis of quantum error-correcting codes: symplectic lattice codes and toric codes, Caltech Ph.D. thesis (2004).
- [36] C. Mochon, Anyons from non-solvable finite groups are sufficient for universal quantum computation, Phys. Rev. A 67, 022315 (2003), arXiv: quant-ph/0206128.
- [37] C. Mochon, Anyon computers with smaller groups, Phys. Rev. A 69, 032306 (2004). arXiv: quant-ph/0306063.

- [38] C. Ahn, H. Wiseman, K. Jacobs, Quantum error correction for continuously detected errors with any number of error channels per qubit, *Phys. Rev. A*, accepted (2004), quant-ph/0402067.
- [39] M. Sarovar, C. Ahn, K. Jacobs, G. J. Milburn, A practical scheme for error control using feedback, *Phys. Rev. A*, accepted (2004), quant-ph/0402017.
- [40] J. McKeever, A. Boca, A. D. Boozer, J. R. Buck, and H. J. Kimble, A One-atom laser in a regime of strong coupling, *Nature* 425, 268-271 (2003), arXiv: quant-ph/0309199.
- [41] A. D. Boozer, A. Boca, J. R. Buck, J. McKeever, and H. J. Kimble, Comparison of theory and experiment for a one-atom laser in a regime of strong coupling, arXiv: quant-ph/0309133 (2003).
- [42] C. W. Chou, S. V. Polyakov, A. Kuzmich, and H. J. Kimble, Single-photon generation from stored excitation in an atomic ensemble, arXiv: quant-ph/0401147 (2004).
- [43] L.-M. Duan and H. J. Kimble, Scalable photonic quantum computation through cavity-assisted interaction, arXiv: quant-ph/0309187 (2003).
- [44] JM Geremia, J. K. Stockton, and H. Mabuchi, Real-time quantum feedback control of atomic spin-squeezing, *Science* 304, 270 (2004).
- [45] R. van Handel, J. K. Stockton, and H. Mabuchi, Feedback control of quantum state reduction, arXiv: quant-ph/0402136 (2004).
- [46] J. K. Stockton, R. van Handel, and H. Mabuchi, Deterministic Dicke state preparation with continuous measurement and control, arXiv: quant-ph/0402137 (2004).
- [47] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, *Phys. Rev. Lett.* 91, 147902 (2003), arXiv: quant-ph/0301063.
- [48] G. Vidal, Efficient simulation of one-dimensional quantum many-body systems, arXiv: quant-ph/0310089 (2003).
- [49] A. J. Daley, C. Kollath, U. Schollwoeck, and G. Vidal, Time-dependent density-matrix renormalization-group using adaptive effective Hilbert spaces, *J. Stat. Mech.: Theor. Exp.* P04005 (2004), arXiv: cond-mat/0403313.
- [50] J. I. Latorre, E. Rico, and G. Vidal, Ground state entanglement in quantum spin chains J. I. Latorre, E. Rico, G. Vidal, *Quant. Inf. and Comp.* vol.4 no.1 pp.048-092 (2004), arXiv: quant-ph/0304098.

- [51] J.I. Latorre, C.A. Lutken, E. Rico, and G. Vidal, Fine-grained entanglement loss along renormalization group flows, arXiv: quant-ph/0404120 (2004).
- [52] D. Bacon, Quantum Computational Complexity in the Presence of Closed Timelike Curves, quant-ph/0309189 (2003).
- [53] A. Kitaev, D. Mayers, and J. Preskill, Superselection rules and quantum protocols, Phys. Rev. A 69, 052326 (2004), arXiv: quant-ph/0310088.
- [54] D. Gottesman and J. Preskill, Comment on “The black hole final state,” JHEP 0403, 026 (2004), arXiv: hep-th/0311269.