

Institute for Quantum Information

Findings – 2002-03

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 algorithms for hidden shift problems. 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.

Most known examples of problems for which quantum computers can achieve an exponential speedup relative to classical computers are hidden subgroup problems, in which a function is constant and distinct on the cosets of an unknown subgroup H of a group G , and the problem is to exhibit a generating set for H . Sean Hallgren, with van Dam and Ip, has generalized this framework to include “hidden coset” and “hidden shift” problems that can also be solved efficiently on a quantum computer using the quantum Fourier transform [1]. In the hidden shift problem, two functions f and g are given such that $f(x) = g(x + s)$, and the problem is to find the value of the shift s . The algorithms of Hallgren et al. have interesting cryptographic applications, as they can predict the behavior of pseudo-random functions that are intractable classically.

Basis selection in Fourier sampling. While Shor’s factoring and discrete log algorithms solve

hidden subgroup problems in which the group G is abelian, nonabelian hidden subgroup problems have many interesting applications; for example, both the graph isomorphism problem and the problem of finding the shortest vector on a lattice can be reduced to nonabelian hidden subgroup problems. Leonard Schulman, with Moore, Rockmore, and Russell, has studied the efficacy of the Fourier sampling method applied to nonabelian hidden subgroup problems [2]. They find that in some cases a complete measurement after executing the Fourier transform suffices for reconstruction of the hidden subgroup, while a measurement that reveals only the name of an irreducible representation of the group does not suffice. An important example to which this observation applies is the case where G is a semidirect product of Z_p by Z_q where q divides $(p - 1)$.

Diameters of homogeneous spaces. Alexei Kitaev, with Freedman and Lurie, has shown that if a subgroup of a compact semisimple Lie group intersects with any ball of a certain radius r , then the subgroup is dense [3]. The metric on the group is given by the operator norm of the adjoint action. An important point is that the constant r does not depend on the group; the value $r = .12$ will suffice. This result provides an efficient way to check universality of a quantum gate set.

Reversible simulation of bipartite product Hamiltonians. Debbie Leung and Guifre Vidal, with Childs, showed that any two bipartite product Hamiltonians can simulate each other reversibly with the help of local unitary operations and local ancillas [4]. This result completely characterizes the nonlocal behavior of any bipartite product Hamiltonian, in that all non-local features — including the rate at which the Hamiltonian can be used to produce entanglement, transmit classical or quantum information, or simulate other Hamiltonians — depend only upon a single parameter.

Time-optimal two-qubit Hamiltonian simulation. IQI visitor Michael Nielsen and visiting student Henry Haselgrove, with Osborne, have investigated the time-optimal simulation of a two-qubit quantum gate using a fixed interaction Hamiltonian and fast local control over individual qubits, showing that for most Hamiltonians, achieving the optimal simulation requires infinitely many infinitesimally small steps, and thus is physically impractical [5]. However, they also show that if the number of steps is fixed at a finite value, then the cost in simulation time is not very large.

Quantum and classical complexity classes. Michael Vyalıy has considered the relation between quantum and classical complexity classes, in particular relations between gap-definable classes and the class QMA (the smallest among the classes of quantum interactive proof systems) [6]. Previously it was known that QMA (as well as BQP) is contained in the class PP. Vyalıy found a new gap-definable class A0PP that possibly separates QMA and the class PP. Namely, QMA is contained in A0PP and if A0PP=PP then PP contains the polynomial hierarchy.

Hardness of approximating the weight enumerator. In an effort to relate the complexity issues in coding theory to quantum computation, Vyalıy has considered the problem of approximating the weight enumerator of a binary linear code [7]. For a specified code description (e.g. by a generator matrix), the problem is to evaluate the code's weight enumerator to a specified precision. Vyalıy finds that this problem is hard for the polynomial hierarchy, and in fact as hard as the whole class

of gap functions.

Quantum cellular automata. Ben Schumacher, with Werner, has been working to characterize quantum cellular automata. By considering mappings on the algebra of local observables of the cellular automaton, they aim to give a general classification of unitary quantum cellular automata (at least for 1-D qubit arrays).

Quantum communication and quantum cryptography

Security of quantum key distribution with imperfect equipment. Another important topic in quantum information science is quantum cryptography, which unlike quantum computation is already realizable with existing technology. John Preskill has studied quantum key distribution, proving its information theoretic security against arbitrary attacks by an eavesdropper. In [8], Preskill, with Koashi, showed that security is uncompromised even if the source of quantum states used in the protocol is completely unreliable, as long as the detector is perfect and the source leaks no information to the eavesdropper about the basis used in the protocol. The proof, which uses a new and remarkably simple method, also applies to the case where the source is perfect and the detector has arbitrary flaws (a case treated earlier by Mayers). In [9] Preskill, with D. Gottesman, H.-K. Lo, and N. Lütkenhaus, investigated the impact on security of small flaws in both the source and the detector used, showing that secure key can still be extracted if the flaws are small enough, and estimating the impact of the flaws on the rate of key generation. This analysis applies, in particular, to the case where the source emits weak coherent states instead of single photons, revealing a little bit of information about the basis.

Quantum state randomization. The one-time pad is perhaps the simplest and most basic cryptographic construction: two parties can use a number of secret shared random bits as key to securely encrypt and decrypt a message of the same length. An analogous construction exists in the quantum realm, with the twist that the number of bits of key required to perfectly encrypt the message is now twice the length of the message itself. The need for this extra factor of two is related to the ability of a quantum channel to communicate two bits for every qubit transmitted. Patrick Hayden, Debbie Leung, and their collaborators investigated what happens if a negligible but non-zero amount of information is allowed to remain available to an eavesdropper. Astonishingly, the extra factor of two disappears entirely: using a probabilistic construction they showed that it is possible to encrypt quantum data using half the resources that had previously been thought necessary [10]. The quantum information is concealed by applying a unitary transformation chosen at random from an ensemble, and the efficacy of the procedure is analyzed using large deviation methods.

Quantum data hiding. A more complicated cryptographic task is known as quantum data hiding. In this setting, a number of parties share a secret such that local operations and classical communication within unauthorized groups is insufficient to reconstruct the secret. Conversely,

quantum communication within authorized groups of parties should be sufficient to reconstruct the secret. Previous work had shown how to accomplish this goal for hiding classical bits. Hayden, with DiVincenzo and Terhal, showed that any method for hiding bits automatically provides a method for hiding qubits and vice-versa [11]. More recently, further developing the methods used to construct the quantum one-time pad, Hayden, Leung, and collaborators have developed schemes for bipartite data hiding at a rate of one hidden qubit per pair of physical qubits [10]. For moderate levels of security, previous constructions required dozens of times more physical qubits, and worse.

Remote state preparation and superdense coding of quantum states. The new results on efficient randomization of quantum states have further applications. One example is remote state preparation, a version of teleportation in which Alice knows the quantum state that is to be sent to Bob. Hayden, Leung, and collaborators have shown that in this case a qubit can be sent to Bob with arbitrarily good fidelity consuming one ebit of entanglement and transmitting one cbit of classical information asymptotically, just half the cost in classical communication of teleporting an unknown quantum state [12]. Another example is “superdense coding of quantum states,” the transmission of a d^2 -dimensional quantum system using $\log d$ ebits of entanglement and $\log d$ qubits of quantum communication, assisted by $\log d$ bits of shared randomness [13].

Unlocking classical correlations. New insights into state randomization lead to still other new protocols for cryptographic tasks. Leung, Hayden, and collaborators were able to use the new methods to demonstrate the existence of quantum states whose classical correlations are large but “locked”. Local measurements on the bipartite state yield a proportionately negligible amount of correlation but, after sending a negligibly small key, that correlation can be made arbitrarily large [14, 10]. Such constructions might ultimately yield protocols for quantum cryptography more efficient than those currently known.

Resource tradeoffs in quantum communication. Hayden and student Anura Abeyesinghe have been studying the ways in which quantum states can be communicated using the resources of classical communication, quantum communication and entanglement [15], extending the analysis begun in [16]. In their model, the sender has knowledge of the state she is trying to transmit. When the amount of quantum communication is zero, the task is remote state preparation, where one ebit and one cbit suffice asymptotically to send a qubit. Eliminating classical communication instead, the task is superdense coding of quantum states, where one qubit of communication and one ebit of entanglement suffice to send two qubits worth of quantum information. Hayden and Abeyesinghe have completely characterized the way in which the three resources interact, in the form of an easily computable formula for the trade-off surface. The results apply to sending pure entangled states as well as to establishing entangled states between sender and receiver. Among other surprises, the latter task provides a new operational interpretation of the Holevo chi quantity that is very different than the classical capacity of a quantum channel.

Spin chain as quantum channel. Sougato Bose has proposed using a quantum spin chain as a

channel for quantum communication [17]. In this proposal, a quantum state is placed on a spin at one end of a magnet and is received with some fidelity at the other end at a later time. For a Heisenberg chain, Bose found that a qubit can be transmitted in a reasonable time with fidelity better than is achievable classically for chains of up to 80 spins. Moreover, significant entanglement can be transferred over chains of as many as 1000 spins in the same amount of time. This scheme is a viable option for short distance quantum communication between two quantum computers, avoiding the need for an optical interface to create flying qubits.

Classical capacities of quantum channels. Student John Cortese has analyzed the capacity of a quantum channel for sending classical information, deriving an expression for the Holevo-Schumacher-Westmoreland capacity in terms of the relative entropy [18], and obtaining an explicit formula for a class of unital qudit channels [19].

Quantum entanglement and quantum information theory

Quantifying nonlocality. The crucial feature that distinguishes quantum information and classical information is quantum entanglement, the nonlocal correlation between the parts of a quantum system that has no classical analog [20]. While much prior work has focused solely on demonstrating the nonlocal nature of quantum correlations, Dave Bacon and student Ben Toner have investigated different measures which *quantify* the amount of this nonlocally, extending work described in last year's report [21, 22]. They have focused in particular on the amount of communication needed (together with shared classical randomness) to simulate quantum correlations, discovering for example that projective measurements on a Bell pair can be simulated with a single bit of communication. One particular implication is that there is a local hidden variable model describing certain quantum teleportation experiments, which therefore fail to prove the validity of quantum theory. Bacon and Toner have also devised a protocol for simulating a class of projective measurements on maximally entangled states using an amount of communication proportional to the dimension of the state. A further implication of their work is a new bound for the detector inefficiency loophole in certain Bell experiments.

Distinguishing separable and entangled states. The task of distinguishing whether a bipartite mixed state is entangled or not is a hard problem in general, and until recently there were no efficient computational methods known that could detect the entanglement of an arbitrary state. Such a method has been developed by Andrew Doherty, Pablo Parrilo and student Federico Spedalieri [23], extending their results described in last year's report [24, 25]. Their program exploits the observation that a bipartite state is separable if and only if it has an n -fold symmetric extension with positive partial transpose for all positive integers n . For each n determining whether such an extension exists is a semidefinite program that can be solved efficiently, and if the extension does not exist for some n , an explicit construction is obtained of an entanglement witness, an observable that

could in principle be measured to prove that the state is nonseparable. This project exemplifies the IQI’s interdisciplinary character — Parrilo, a control theorist and expert on convex optimization, teamed with physicists to solve an important problem in quantum information theory.

Local hidden variable theories for quantum states. One of the most important features of entangled quantum systems is that measurements on them violate Bell inequalities and thus do not have any description in terms of local hidden variables. All pure entangled states violate some Bell inequality, but, surprisingly, there are entangled mixed states that do not violate any Bell inequality. Barbara Terhal and Andrew Doherty, with student David Schwab, have found a general procedure for constructing local hidden variable descriptions for mixed quantum states, for a fixed number of local observables that can be measured in the Bell experiment [26]. The construction is a semidefinite program, and thus can be implemented either analytically or numerically for typical quantum states of interest. This program always succeeds for states that are not entangled. For entangled states it does not always succeed (there are of course states that *do* violate Bell inequalities) but in this case a closely related construction provides an entanglement witness.

Sharability of quantum states. Ben Schumacher, with Werner, has studied how joint quantum states can be “copied” or “shared” among many parties [27]. They have characterized all “copyable” joint states and rediscovered the theorem that all infinitely sharable states are separable. (The latter closely parallels the work of Doherty, Parrilo, and Spedalieri, but using different techniques.) In addition, Schumacher and Werner have established that, for all n , there exist states sharable by n parties that are not sharable by $n + 1$ parties.

Progress on additivity conjectures. Schumacher and Cortese, with Westmoreland, have been attacking a cluster of related additivity conjectures. These include the additivity of entanglement of formation for product states, the additivity of the classical capacity for quantum channels, the additivity of minimum output entropy for quantum channels, and the so-called “strong superadditivity” for entanglement of formation. They found that all of these follow from the last one, a result now superseded by Shor’s result that all are completely equivalent. They verified the conjectures with many numerical searches and for several special cases. Nevertheless, the central question remains unresolved.

Entanglement of spin-squeezed many-particle states. States of ensembles of two-level atoms such as spin-squeezed states have been of recent experimental interest since they are relatively easy to prepare, represent entangled states of the atoms, and are thus attractive test-beds for experiments in quantum communication. JM Geremia, Hideo Mabuchi, Doherty, and student John Stockton investigated this entanglement quantitatively for ensembles as large as a thousand atoms by taking advantage of the very high symmetry of the states used in these experiments [28]. They imagined a scenario in which a certain number of atoms are lost to the sample (one simple source of decoherence), and the remaining atoms are physically separated into two groups. Several simple measures of the entanglement between these two atomic ensembles were then calculated.

They investigated an apparent trade-off between the maximum achievable entanglement and the robustness of this entanglement to the loss of atoms from the sample.

Compatibility between local and multipartite states. Another approach to the entanglement of many-particle pure states was developed by visiting student Sergey Bravyi [29]. A specified multiparticle state determines a “mean field state” — a collection of local density matrices, one for each part, that encodes the expectation values of all single-particle observables. Bravyi determined the necessary and sufficient conditions for a mean field state to be compatible with at least one multipartite pure state, for the case of n qubits, and for the tripartite system with Hilbert space of dimension $2 \times 2 \times 4$.

Communication complexity of entanglement transformations. One approach to the study of entanglement is to characterize quantum states by the resources required to interconvert them. In such studies, classical communication is usually idealized to be free in order to isolate the intrinsically quantum-mechanical correlation. The conversion of one state into another might, however, require very large amounts of classical communication. Therefore, Hayden and student Sumit Datta have taken a different approach [30], which has the advantage that it treats all correlations uniformly while still being tractable, if only just so. Specifically, they have determined how to find the minimum amount of quantum communication required to convert one pure bipartite state into another. The solution to the problem lies at the intersection of representation theory, symplectic geometry and algebraic geometry, providing an exciting link between quantum information theory and an active area of research in pure mathematics.

Conditions for equality in strong subadditivity. In quantum information, a single inequality known as strong subadditivity encodes our most basic intuitions about the nature of quantum states. The inequality plays a pivotal role in almost every important result in the field, including every channel capacity theorem. While the inequality was formulated as a conjecture and then proved in the 1970’s, the conditions for equality had never been obtained. Hayden and his collaborators have found an explicit characterization of all states that satisfy strong subadditivity with equality, a condition that turns out to characterize the states that can be thought of as arising from quantum Markov chains [31]. Roughly speaking, the strong subadditivity inequality expresses the fact that discarding a subsystem of a quantum system is a dissipative operation, in the sense that it can only destroy correlations with an environment. Their new result, therefore, can be interpreted as providing a detailed description of the conditions under which the act of discarding a quantum system can be locally reversed on a particular input. As special cases, they recover the conditions for quantum error correction and saturation of the Holevo bound.

Quantum error correction and fault tolerance

Quantum error correction for continuously detected errors. 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 in its usual formulation quantum error correction requires fast projective measurements and fast unitary gates, which might not be available in some laboratory settings. Student Charlene Ahn, with Wiseman and Milburn, has shown that quantum feedback control can be used as a quantum error correction process if the environment is monitored continuously [32]. Using the stabilizer formalism, they derived an explicit scheme, involving feedback and an additional constant Hamiltonian, to protect an $(n - 1)$ -qubit logical state encoded in n physical qubits; universal quantum computation is possible within this scheme.

Anyons from non-solvable finite groups. Another approach to protecting a quantum computation from decoherence, computing with anyons, has been pursued by student Carlos Mochon [33]. He found a constructive proof that anyonic magnetic charges with fluxes in a non-solvable finite group can perform universal quantum computation. In Mochon’s construction, the gates are built out of the elementary operations of braiding, fusion, and vacuum pair creation, supplemented by a reservoir of ancillas of known flux, and a universal gate set ideally suited for anyons is presented.

Toward naturally fault-tolerant quantum computation. Dave Bacon has been developing the idea of natural fault tolerance — that we might engineer many-body systems whose size guarantees that they can serve as robust quantum computers, thus overcoming the difficulties faced by the “traditional” approach to building a quantum computer [34]. Seeking systems whose dynamics naturally enforces quantum error correction, Bacon has investigated a system of qubits on a cubic lattice with two-qubit interactions, whose degenerate ground state can encode quantum information. Monte Carlo simulations of this system are underway to determine whether it has a naturally fault-tolerant phase.

Experiment and implementation

Controlling spin exchange interactions in optical lattices. Many methods for implementing quantum information processing in the laboratory have been proposed and are being actively pursued, but all are difficult. However, one exciting application of “quantum computing” is already a reality — simulating coherent many-body physics with ultracold atoms in optical lattices. Luming Duan, with Demler and Lukin, has proposed an efficient way to engineer many-body spin Hamiltonians in optical lattices [35]. In this proposal, the lattice geometry and spin-dependent tunneling interactions between the atoms are specified by controlling interfering laser beams. Hamiltonians realized with this technique have wide applications, such as probing various quantum phase transitions relevant to quantum magnetism. In particular, Duan et al. have suggested a way to realize a model proposed by Kitaev that supports both abelian and nonabelian anyons.

Simulation of quantum dynamics with quantum optical systems. Guifre Vidal and collaborators have proposed other schemes for achieving quantum simulation that can be realized by either neutral atoms stored in optical lattices or ions stored in micro-traps [36]. In either case, local unitary operations can be performed on each atom or ion with laser beams, and two-qubit gates are achieved by displacing the atoms or ions. A large class of Hamiltonians can be simulated by this method.

Engineering of multi-atom entanglement through single-photon detections. Duan and Jeff Kimble have proposed a scheme to engineer multi-atom entanglement by detecting the decay light from an optical cavity [37]. This scheme is very efficient, yet inherently robust to practical noise and imperfections. Furthermore, the scheme prepares a broad type of multi-atom entanglement as well as two-atom entanglement. For its realization, it does not require full localization and separate addressing of the atoms inside the optical cavity; thus it is well matched to current experimental capabilities.

Quantum information processing with “hot” trapped atoms. Duan, Kimble, and Kuzmich have proposed a method to implement quantum information processing in high-Q cavities with a single trapped but non-localized atom [38]. Their method is based on adiabatic passage, which makes the relevant dynamics insensitive to the randomness of the atom position with an appropriate interaction configuration. They demonstrated the validity of the method with both approximate analytical calculations and exact numerical simulations.

Quantum computing with an “always-on” Heisenberg interaction. Sougato Bose, with Benjamin, has proposed using an array of spins in a one-dimensional magnet for quantum computation [39]. Such a magnet is modeled as a Heisenberg spin chain with “always-on” (untunable) interactions. They found a protocol where any quantum algorithm can be executed in this system by controlling a switch with only six settings.

Photon pairs for scalable quantum communication with atomic ensembles. Two years ago, Luming Duan and his collaborators proposed a scheme for robust long-distance quantum communication through the manipulation of atomic ensembles. Recently, Kuzmich et al. have demonstrated a key ingredient in this scheme: entangled photon pairs generated by collective emission from the ensemble [40]. In the experiment, a “write” pulse produces a (probabilistic) forward-scattered Raman photon, preparing a symmetrized state of the vapor (with a single excited atom). Then a “read” pulse produces, with high efficiency, a second photon entangled with the first and in a specified mode, with a programmable direction, pulse shape, and time delay. The results indicate that long-distance entanglement is not far beyond the reach of current experiments.

Quantum teleportation of light beams. Zhang et al. experimentally demonstrated quantum teleportation for continuous variables using squeezed-state entanglement [41]. They inferred that teleportation of coherent states was achieved with fidelity $F = .62$. This is an improvement over the experiment reported by the Kimble group in 1998, thanks to stronger entanglement and higher

detection efficiency.

Spin squeezing via real-time feedback. JM Geremia, John Stockton, and Hideo Mabuchi are using feedback to generate entanglement in atomic ensembles. Continuous measurement and real-time feedback on symmetric spin ensembles have already been achieved. These experiments should soon be able to attain the quantum noise limit for a continuously monitored spin.

Connecting quantum information with the rest of physics

Entanglement in quantum critical phenomena. 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 the theory of quantum phase transitions. Quantum phase transitions occur at zero temperature and involve the appearance of long-range correlations. These correlations are not due to thermal fluctuations but to the intricate structure of a strongly entangled ground state of the system. Vidal and Kitaev, with Latorre and Rico, have presented a microscopic computation of the ground-state entanglement in several one-dimensional spin chain models, using both analytic and numeric methods [42, 43]. They quantify the ground state entanglement by studying the density operator of a segment of L consecutive spins on the chain, finding that the entropy of this segment diverges logarithmically with L at the critical point, with a coefficient that is related to the central charge of the corresponding conformal theory. For an infinite chain near the critical regime, they also find logarithmic dependence on the deviation from the transition point.

Efficient classical simulation of slightly entangled quantum systems. A typical quantum state of n qubits has no succinct classical description — its expansion in a standard basis has of the order of 2^n terms. On the other hand, a product state of n qubits can be described by a number of parameters of order n . Guifre Vidal has observed that if a quantum state of n qubits has the property that the bipartite entanglement for any way of splitting the system into two parts is bounded above by a constant, then a description of the state with only $O(n)$ parameters can be formulated using an iterated Schmidt decomposition [44]. Furthermore, it is easy to update the description when a quantum gate is executed on a pair of qubits. Therefore, any quantum computation such that the bipartite entanglement remains bounded can be simulated efficiently on a classical computer. This observation can be exploited to formulate an efficient classical simulation of the Schrödinger dynamics of many interesting quantum systems, such as spin chains with nonvanishing correlation length.

Quantum many-body physics and quantum codes. IQI visitor Michael Nielsen and visiting student Henry Haselgrove, with Osborne, have used the theory of quantum codes to construct interesting classes of entangled many-body states [45]. Specifically, they exhibited quantum states that cannot possibly be the ground state of any system with local interactions. Such states are

instructive because they realize a type of non-locality that cannot be produced by minimizing any local energy function of the system.

Quantum analogues of closed timelike curves. IQI visitor Ben Schumacher, with Bennett, has conceived a variant of quantum teleportation that they call “conditional quantum time travel.” By considering post-selected ensembles, they describe situations in which a system can interact with a future copy of itself, a kind of behavior that has been discussed previously in connection with spacetimes that admit closed timelike curves. One outcome of this work is a theorem asserting that every operator is a partial trace of a unitary operator.

Disordered gauge theories and the quantum accuracy threshold. John Preskill, with students Chenyang Wang and Jim Harrington, has been exploring some intriguing connections between fault-tolerant quantum computation and phase transitions in disordered systems [46]. Following up on work described in last year’s report [47], they considered topological quantum codes in which error recovery can be executed easily using only local quantum gates, and found that the accuracy threshold for quantum storage can be identified with the confinement-Higgs phase boundary in a three-dimensional lattice gauge theory with quenched disorder. Using a combination of analytic methods and Monte Carlo simulations, they mapped out the phase diagram of this model, establishing that confinement can be driven by magnetic disorder even at zero temperature (that is, without any quantum fluctuations of the magnetic field). Their analysis yields improved numerical estimates of the accuracy threshold. In passing, they also studied the random-bond Ising model in two dimensions (which has very similar features), disproving the widely accepted conjecture that the disorder strength at the boundary between the ferromagnetic and paramagnetic phases is a temperature-independent constant at low temperature.

References Cited

- [1] S. Hallgren, W. van Dam, and L. Ip, Quantum Algorithms for Hidden Coset Problems, Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA, 2003), quant-ph/0211140.
- [2] C. Moore, D. Rockmore, A. Russell, and L. J. Schulman, The hidden subgroup problem in affine groups: basis selection in Fourier Sampling, quant-ph/0211124 (2002).
- [3] M. Freedman, A. Kitaev, and J. Lurie, Diameters of Homogeneous Spaces, Mathematical Research Letters, 10 (1), 11-20 (2003), quant-ph/0209113.
- [4] A. M. Childs, D. Leung, and G. Vidal, Reversible simulation of bipartite product Hamiltonians, quant-ph/0303097.

- [5] H. L. Haselgrove, M. A. Nielsen, and T. J. Osborne, On the practicality of time-optimal two-qubit Hamiltonian simulation, quant-ph/0303070 (2003).
- [6] M. N. Vyalyi, QMA=PP implies that PP contains PH, Electronic Colloquium on Computational Complexity, TR03-21 (2003).
- [7] M. N. Vyalyi, Hardness of approximating the weight enumerator of a binary linear code, cs.CC/0304044 (2003).
- [8] M. Koashi and J. Preskill, Secure quantum key distribution with an uncharacterized source, Phys. Rev. Lett. 90, 057902 (2003), quant-ph/0208155.
- [9] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, quant-ph/0212066 (2002).
- [10] C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, Randomizing quantum states: Constructions and applications, in preparation (2003).
- [11] D. P. DiVincenzo, P. Hayden and B. M. Terhal, Hiding quantum data, to appear in Foundations of Physics (2003), quant-ph/0207147.
- [12] C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, and A. Winter, Remote state preparation, in preparation (2003).
- [13] A. Harrow, P. Hayden, and D. Leung, Superdense coding of quantum states, in preparation (2003).
- [14] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Locking classical correlation in quantum states, quant-ph/0303088 (2003).
- [15] A. Abeyesinghe and P. Hayden, Bits, ebits and qubits in quantum data compression, in preparation (2003).
- [16] P. Hayden, R. Jozsa, and A. Winter, Trading quantum for classical resources in quantum data compression, J. Math. Phys. 43(9):4404-4444 (2002), quant-ph/0204038.
- [17] S. Bose, Quantum communication through an unmodulated spin chain, quant-ph/0212041 (2002).
- [18] J. A. Cortese, Relative entropy and single qubit Holevo-Schumacher-Westmoreland channel capacity, quant-ph/0207128 (2002).
- [19] J. A. Cortese, The Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels, quant-ph/0211093 (2002).

- [20] B. M. Terhal, M. M. Wolf and A. C. Doherty, Quantum entanglement: A modern perspective, *Physics Today*, April 2003.
- [21] D. Bacon and B. F. Toner, Bell inequalities with auxiliary communication, *Phys. Rev. Lett.* 90, 157904 (2003), quant-ph/0207147.
- [22] D. Bacon and B. F. Toner, The communication cost of simulating bell correlations, accepted by *Phys. Rev. Lett.* (2003), quant-ph/0304076.
- [23] F. Spedalieri, Characterizing entanglement in quantum information, Caltech Ph.D. thesis, June 2003, 108 pages.
- [24] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Distinguishing separable and entangled states, *Phys. Rev. Lett.* 88, 187904 (2002), quant-ph/0112007.
- [25] P. A. Parrilo, A. C. Doherty and F. M. Spedalieri, Entanglement witnesses and semidefinite programming, *Proceedings of the 41st IEEE Conference of Decision and Control* (2002).
- [26] B. M. Terhal, A. C. Doherty, D. Schwab, Local hidden variable theories for quantum states, *Phys. Rev. Lett.* 90 157903 (2003).
- [27] B. Schumacher and R. Werner, Sharable, copyable, classical, in preparation (2003).
- [28] J. K. Stockton, JM Geremia, A. C. Doherty, H. Mabuchi, Characterizing the entanglement of symmetric many-particle spin-1/2 systems, *Phys. Rev. A* 67 022112 (2003), quant-ph/0210117.
- [29] S. Bravyi, Requirements for compatibility between local and multipartite quantum states, quant-ph/0301014 (2003).
- [30] S. Daftuar and P. Hayden, The communication complexity of entanglement transformation, in preparation (2003).
- [31] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Structure of states which satisfy strong subadditivity of quantum entropy with equality, quant-ph/0304007 (2003).
- [32] C. Ahn, H. W. Wiseman, and G. J. Milburn, Quantum error correction for continuously detected errors, quant-ph/0302006 (2003).
- [33] C. Mochon, Anyons from non-solvable discrete groups are sufficient for universal quantum computation, *Phys. Rev. A* 67, 022315 (2003), quant-ph/0206128.
- [34] D. Bacon, Naturally fault-tolerant quantum computation, in preparation (2003).
- [35] L.-M. Duan, E. Demler, M. Lukin, Controlling spin exchange interactions of ultracold atoms in optical lattices, cond-mat/021056 (2002).

- [36] E. Jané, G. Vidal, W. Dür, P. Zoller, J.I. Cirac, Simulation of quantum dynamics with quantum optical systems, *Q. Inf. and Comp.* 3, 38-47 (2003), quant-ph/0207011.
- [37] L.-M. Duan, H. J. Kimble, Efficient engineering of multi-atom entanglement through single-photon detections, accepted by *Phys. Rev Lett.* (2003), quant-ph/0301164.
- [38] L.-M. Duan, A. Kuzmich, and H. J. Kimble, Cavity QED and quantum-information processing with “hot” trapped atoms, *Phys. Rev A* 67, 032305 (2003), quant-ph/0208051.
- [39] S. C. Benjamin and S. Bose, Quantum computing with an “always on” Heisenberg interaction, accepted by *Phys. Rev. Lett.* (2003), quant-ph/0210157.
- [40] A. Kuzmich, W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L.-M. Duan, and H. J. Kimble, Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles, accepted by *Nature* (2003), quant-ph/0305162.
- [41] T. C. Zhang, K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, Quantum teleportation of light beams, *Phys. Rev A* 67, 033802 (2003), quant-ph/0207076.
- [42] G. Vidal, J.I. Latorre, E. Rico and A. Kitaev, Entanglement in quantum critical phenomena , accepted by *Phys. Rev. Lett.* (2003), quant-ph/0211074.
- [43] J. I. Latorre, E. Rico, and G. Vidal, Ground state entanglement in quantum spin chains, quant-ph/0304098 (2003).
- [44] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, quant-ph/0301063 (2003).
- [45] H. L. Haselgrove, M. A. Nielsen, T. J. Osborne, Quantum states far from the energy eigenstates of any local Hamiltonian, quant-ph/0303022 (2003).
- [46] C. Wang, J. Harrington, and J. Preskill, Confinement-Higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory, *Annals Phys.* 303, 065022 (2003), quant-ph/0207088.
- [47] E. Dennis, A. Landahl, A. Kitaev, and J. Preskill, Topological quantum memory, *J. Math. Phys.* 43 4452-4505 (2002), quant-ph/0110143.