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.

Since our last annual report in May 2008, IQI participants have produced 37 publications, which we summarize here.

Quantum algorithms and quantum complexity

Quantum Algorithms using the curvelet transform. The curvelet transform is a directional wavelet transform over $\mathbb{R}^n$. In [1], postdoc Yi-Kai Liu constructed an efficient implementation of a quantum curvelet transform, together with two applications to quantum algorithms: a single-shot measurement procedure for approximately finding the center of a ball in $\mathbb{R}^n$, given a single quantum sample over the ball, and a quantum algorithm for finding the center of a radial function over $\mathbb{R}^n$, given oracle access to the function. These algorithms are conjectured to succeed with constant probability, using one quantum sample and $O(1)$ oracle queries, respectively, independent of the dimension $n$. In contrast, the best classical algorithm for approximately finding the center of a ball succeeds with probability exponentially small in $n$, and a classical algorithm for finding the center of a radial function requires $\Omega(n)$ queries. The conjectures are supported by rigorous proofs showing that the algorithms work in an idealized continuous model.

Quantum and classical complexity of translationally-invariant tiling and Hamiltonian problems. Long-term visitor Sandy Irani, with Gottesman, studied the computational
complexity of computing the ground energy of translationally-invariant one-dimensional quantum systems where the Hamiltonian is a sum of two-body terms, each acting on a pair of neighboring particles [2]. In the problem they formulated, the two-body Hamiltonian is fixed, and the input to the problem, an integer $N$, is the size of the one-dimensional system. They showed that this problem, for open chains or closed cycles of particles, is complete for the class $\text{QMA}_{\text{EXP}}$ (problems that can be solved in exponential time by a quantum computer if a suitable quantum witness is provided). This result provides strong evidence that no quantum algorithm can compute the ground state energy in time polynomial in $N$ (i.e., exponential in the number of input bits). They also showed that a closely related classical tiling problem in two dimensions is complete for the class $\text{NEXP}$ (non-deterministic exponential time).

**Universal quantum computation by quantum walk.** In some of the earliest work on quantum-mechanical computers, Feynman showed how to implement universal quantum computation using the dynamics of a time-independent Hamiltonian. Postdoc Andrew Childs showed that this remains possible even if the Hamiltonian is restricted to be a sparse matrix with all entries equal to 0 or 1, i.e., the adjacency matrix of a low-degree graph [3]. Thus quantum walk can be regarded as a universal computational primitive, with any desired quantum computation encoded entirely in some underlying graph. The main idea of the construction is to implement quantum gates by scattering processes. Most of this work was done at Caltech, before Childs departed for a faculty position at the University of Waterloo.

**Preparing ground states of quantum many-body systems on a quantum computer.** Preparing the ground state of a system of interacting classical particles is an NP-hard problem. Thus, there is in general no better algorithm to solve this problem than exhaustively going through all $N$ configurations of the system to determine the one with lowest energy, requiring a running time proportional to $N$. A quantum computer could solve this problem in time $\sqrt{N}$. Postdoc David Poulin, with former IQI postdoc Pawel Wocjan, presented a powerful extension of this result to the case of interacting quantum particles, demonstrating that a quantum computer can prepare the ground state of a quantum system as efficiently as it does for classical systems [4].

**Approximating group representations.** Postdoc Stephen Jordan found polynomial time quantum algorithms for approximating matrix elements from irreducible representations of the symmetric, alternating, unitary, special unitary, and special orthogonal groups [5]. No polynomial-time classical algorithms for these problems are known. For Lie groups, the quantum algorithms make novel use of techniques originally developed for simulating time evolution governed by local Hamiltonians.

**Quantum state preparation by phase randomization.** Postdoc Sergio Boixo, with Knill and Somma, formulated a method for adiabatic quantum computation and quantum state preparation based on randomizing the evolution time under the corresponding Hamiltonian [6]. The resulting phase decoherence effectively implements a sequence of projections that traverses the
adiabatic path. The cost of the algorithm is quadratic in the length of the path and inversely proportional to the minimum energy gap along the path, a logarithmic improvement over previous algorithms of this type. Among other applications, these methods can provide quantum speedups for quantum sampling and solving combinatorial optimization problems.

**Implementing sparse unitaries.** Jordan, with Wocjan, obtained a general method for implementing sparse unitary transformations using quantum circuits [7]. This method can realize any exponentially high-dimensional unitary transformation provided that the number of nonzero matrix elements in any row and in any column is polynomial, and the individual matrix elements are efficiently computable. The technique builds on existing methods for the simulation of sparse Hamiltonians, and may provide a broadly useful primitive for quantum algorithms.

**Classical Ising test for quantum circuit.** Long-term visitor Lidar, with Geraci, showed that quantum circuits corresponding to certain planar graphs can be efficiently simulated classically [8]. Their proof builds upon a previously recognized connection between the Ising model partition function and quadratically signed weight enumerators, which are bivariate polynomials arising in expansions of quantum circuits in terms of rotations involving Pauli matrices. As examples, they exhibited classically simulable quantum circuits with small numbers of non-nearest neighbor gates.

**Quantum communication and quantum cryptography**

**Robust cryptography in the noisy-quantum-storage model.** Extending work described in last year’s report, postdoc Stephanie Wehner, with Schaffner and Terhal, showed that cryptographic primitives can be implemented based on the assumption that it is difficult to store quantum states without errors [9]. They analyzed a protocol achieving oblivious transfer that can be implemented using existing quantum-key-distribution hardware, and in a practical setting where honest participants are unable to perform noise-free operations. They derived trade-offs among the amount of storage noise, the amount of noise in the operations performed by the honest participants, and the security of oblivious transfer, greatly improving on their previously reported results. For example, they showed that for the case of depolarizing storage noise oblivious transfer is secure provided the quantum bit-error rate of the channel does not exceed 11% and the channel noise is weaker than the storage noise, which is optimal for the protocol they considered.

**Post-selection technique for quantum channels with applications to quantum cryptography.** Postdoc Robert König, with Christandl and Renner, studied channels which are covariant with respect to the action of a group [10]. They showed that certain properties of such channels can be established by considering only one particular input state. When applied to channels which are covariant with respect to the symmetric group, this result provides a simple proof that security of a discrete-variable QKD protocol against collective attacks implies security of the protocol against the most general attacks. This security analysis circumvents the need for an exponential
de Finetti theorem, and provides tighter security bounds for concrete protocols than previously known.

**A strong converse for classical channel coding using entangled inputs.** König and Wehner showed that for a large class of quantum channels, the probability of successful decoding decays exponentially when transmitting classical information at rates exceeding the classical capacity of the quantum channel [11]. Such a “strong converse,” which strengthens the interpretation of the capacity as a sharp threshold for information transmission, was previously known only for classical channels and the quantum identity channel. The result has useful applications to quantum cryptography, particularly in the noisy-quantum-storage model.

Quantum entanglement and quantum information theory

**Information processing in generalized theories.** Wehner and student Greg Ver Steeg studied generalized probabilistic theories that include quantum mechanics as a special case, which in general admit nonlocal correlations that are stronger than those realized by entangled quantum states [12]. They showed that the resource requirements for information processing tasks can be drastically different in a world with superstrong correlations compared to the quantum world. In particular, they found that “learning” even approximately the properties of a superstrongly correlated state requires a vast number of measurements.

**The operational meaning of min- and max-entropy.** König, with Schaffner and Renner, found simple operational interpretations for entropic quantities commonly used in single-shot quantum information theory [13]. The conditional min-entropy $H_{\text{min}}(A|B)$ of a bipartite state $\rho_{AB}$ was shown to be directly related to the maximal singlet fraction achievable if only local actions on part $B$ are allowed. It is also equal to the guessing probability in hypothesis testing if $A$ is classical. Similarly, the max-entropy $H_{\text{max}}(A|B)$ was shown to be equivalent to the fidelity of $\rho_{AB}$ with a product state that is completely mixed on $A$, and is therefore a measure of security when $A$ is used as a key.

**Lower bound on the dimension of a quantum system given measured data.** Wehner, with Christandl and Doherty, proved a lower bound on the dimension of a quantum system that is compatible with the results of experiments performed on the system [14]. The experimenter can prepare the system in various ways labeled by an index $\rho$, and can perform measurements labeled by $M$ that yield outcomes labeled by $a$; Repeated experiments determine the conditional probability distribution $p(a|M, \rho)$, and Wehner et al. determined how large the dimension of the system’s Hilbert space must be to accommodate this distribution. Their result has applications to state estimation, Bell inequalities, and interactive proof systems with entangled provers.

**Distinguishing quantum states with a restricted family of measurements.** Wehner, with Matthews and Winter, constructed a framework for characterizing how well two quantum
states can be distinguished using a restricted class of measurements [15]. In particular, they have found bounds on performance for measurements based on 2-designs and 4-designs, and for measurements implemented using local operations and classical communication. Their results imply the optimality of proposed quantum data hiding schemes.

**Area law for entanglement with a fractal boundary.** If a quantum system with short-range interactions is divided into two parts, the entanglement entropy scales with the “area” of the boundary between the parts. Lidar, with Hamma and Severini, studied the case in which the boundary is a fractal [16]. For a topologically ordered two-dimensional system, they showed that the entanglement entropy depends on the boundary’s fractal dimension.

**Quantum error correction, fault tolerance, and control**

**Fault-tolerant quantum computation versus Gaussian noise.** Though characterizing the noise in a quantum computer in terms of an error rate per gate is natural and useful for the analysis of fault-tolerant quantum circuits, it is not a very realistic way to describe the noise in actual devices. From a physics perspective, it is more natural to describe the noise using a non-Markovian Hamiltonian model that includes a coupling between the computing hardware and a “bath” or environment. John Preskill and student Hui Khoon Ng investigated the robustness of a fault-tolerant quantum computer coupled to a bath with Gaussian thermal or quantum fluctuations, and they showed that scalable quantum computation is possible if the noise power spectrum satisfies an appropriate “threshold condition” [17]. This new condition has several advantages over the threshold conditions derived in previous work; in particular, it can be related more directly to experimentally measurable quantities, and it is less sensitive to very-high-frequency noise.

**The Fibonacci scheme for fault-tolerant quantum computation.** Preskill and former IQI student Panos Aliferis developed and analyzed an approach to fault-tolerant quantum computing [18] based on ideas suggested earlier by Emanuel Knill. In this “Fibonacci scheme,” protected quantum gates are executed using quantum teleportation, and most of the computational resources are expended during the preparation and testing of the maximally entangled pairs of encoded qubits that are consumed by the teleportation. For an independent depolarizing noise model, Aliferis and Preskill proved that the scheme works effectively if the fundamental gates in the quantum computer fail with probability per gate below 0.1%.

**Fault-tolerant computing with biased-noise superconducting qubits.** For many of the proposed schemes for implementing quantum computation, the noise is expected to be highly biased — dephasing in the energy eigenstate basis is much more likely than jumps from one energy eigenstate to another. Preskill, with the IBM group, formulated a scheme for fault-tolerant quantum computation that works effectively against highly biased noise, and explored applications of this scheme to the superconducting qubits being developed by the IBM team [19]. Numerical simulations
combined with analytic studies indicate that the noise in these devices is highly biased and can be substantially suppressed using suitable fault-tolerant methods. Ongoing experiments at IBM will test how well these methods work in practice.

**Topological phases and quantum computation.** Alexei Kitaev, with Laumann, published a series of lectures reviewing the theory of topological phases of matter and their applications to fault-tolerant quantum computing [20]. The lectures provide a pedagogical introduction to topological phenomena in one-dimensional superconductors and in two-dimensional media, covering in particular the properties of abelian and nonabelian anyons and the exactly solvable honeycomb lattice model.

**Fault-tolerant holonomic quantum computing.** Lidar, with Oreshkov and Brun, proposed and developed a scheme for fault-tolerant holonomic quantum computing [21]. In the holonomic model, universal quantum gates are realized using purely geometric transformations. In the fault-tolerant scheme, encoded gates are realized by adiabatically transported the code space around a nontrivial closed path.

**Quantum error correction for noise that is not completely positive.** Lidar, with Shabani, showed that quantum error correction will work for noise that is not described by a completely positive map [22]. They classified the conditions under which open quantum systems can be described by linear maps, and by completely positive maps in particular. They showed that a necessary and sufficient condition for complete positivity is that the initial correlations between system and environment are purely classical, and that the dynamics can always be described by a Hermitian linear map irrespective of the initial correlations.

**Experiment and implementation**

**Verifying multi-partite mode entanglement of W states.** The Kimble group developed a method for verifying quantum entanglement in a W state of $N$ bosonic modes [23]. The ideal W state contains exactly one excitation symmetrically shared between $N$ bosonic modes, but their method takes into account the possible presence of additional excitations, as well as other deviations from the ideal state. Moreover, the method distinguishes between states with full $N$-part entanglement and states with only $M$-part entanglement where $M < N$. In the optical case, where the excitations are photons, the method can be implemented using linear optics.

**Near-field nanoscale traps for neutral atoms.** Postdoc Darrick Chang and collaborators proposed a scheme to interface individual neutral atoms with nanoscale solid-state systems by optically trapping the atom using the strong near-field generated by a sharp metallic nanotip [24]. Under realistic conditions, the atom can be trapped with position uncertainties of just a few nanometers. They also proposed using the guided surface plasmon modes of the nanotip for efficient optical manipulation and collection of fluorescence photons. This technique can be
applied to place atoms near micro-photonic and nano-photonic structures (such as microtoroidal resonators or photonic crystal cavities), or to bring an atom close to a charged or magnetized solid-state quantum system for direct coupling.

**Spectral control of single-photon sources.** Chang and collaborators developed a technique for controlling the emission wavelength and bandwidth of single-photon quantum emitters using a nonlinear photonic crystal cavity [25]. The emission wavelength can be shifted by hundreds of nanometers, potentially allowing direct optical coupling between different types of quantum emitters (enabling hybrid quantum networks), direct emission into low-loss telecom bands, and shifts to wavelengths where high-efficiency single-photon detectors are available. They designed novel double-mode photonic crystal cavity structures for this purpose where each mode exhibits exceptionally high figures of merit.

**Strong coupling of a mechanical oscillator and a single atom.** Kimble and collaborators proposed and analyzed a setup to achieve strong coupling between a single trapped atom and a mechanical oscillator [26]. The interaction between the motion of the atom and the mechanical oscillator is mediated by a quantized light field in a laser driven high-finesse cavity. In particular, they showed that high fidelity transfer of quantum states between the atom and the mechanical oscillator is achievable for existing or near-future experimental parameters. Their proposal provides a basic toolbox for coherent manipulation, preparation, and measurement of nanomechanical oscillators using methods from atomic physics.

**Optical interferometers with reduced sensitivity to thermal noise.** A fundamental limit to the sensitivity of an optical interferometer arises from thermal noise in the interferometer’s mirrors that drives fluctuations in the phase of the intracavity field. Kimble, with Lev and Ye, proposed a scheme for reducing this thermally driven phase noise [27]. In their scheme, phase shifts from concomitant strains at the surface and in the bulk of the substrate compensate the phase shift due to the displacement of the surface. Although the position of the physical surface fluctuates, the optical phase upon reflection has reduced sensitivity to this motion.

**The quantum internet.** Kimble reviewed the opportunities and challenges afforded by research on quantum networks, including applications to quantum computation, communication, and metrology [28]. These networks require quantum interconnects that transfer quantum states reversibly from one physical system to another. One way to achieve connectivity is by using optical interactions between single photons and atoms for distribution of entanglement and quantum teleportation between nodes.

**Connecting quantum information with the rest of physics**

**Periodic table for topological insulators and superconductors.** Alexei Kitaev classified gapped phases of noninteracting fermions, with and without charge conservation and/or time-
reversal symmetry, using Bott periodicity [29]. The symmetry and spatial dimension determine a
general universality class, which corresponds to one of the 2 types of complex and 8 types of real
Clifford algebras, and topological properties of finite systems are described in terms of K-homology.
The phases within a given class are further characterized by a topological invariant, an element of
an abelian group that can be 0, \(\mathbb{Z}\), or \(\mathbb{Z}_2\). The interface between two infinite phases with different
topological numbers must carry a gapless mode.

Effects of interactions on the topological classification of free fermion systems. Kitaev and postdoc Łukasz Fidkowski examined the robustness of Kitaev’s classification of free fermion systems, and showed that in some cases distinct free-fermion phases can be smoothly connected without a gap collapse by turning on interactions [30]. In particular, for a one-dimensional chain of Majorana fermions with an unusual T symmetry, the free fermion phases are classified by an integer, but when interactions are allowed this integer invariant is well defined only modulo 8. They described in detail, both in a microscopic theory and in a continuum field theory formalism, how to deform one free-fermion phase to another by passing through a region of the phase diagram with strong interactions.

Entanglement entropy of the disordered golden chain. Gil Refael and Fidkowski, with Bonesteel and Moore, analyzed the ground-state properties of disordered nonabelian anyonic chains [31]. They showed that a disordered chain of Fibonacci anyons exhibits two infinite-randomness phases: a random-singlet phase in which neighboring anyons prefer the trivial fusion channel, and a mixed phase in which anyon pairs preferring the nontrivial fusion channel occur with finite density. The random-singlet phase is unstable and flows to the mixed phase when perturbed. Surprisingly, the mixed phase has a larger value of the effective central charge \(c\) than the random-singlet phase, disproving the conjecture that \(c\) is unable to increase along a renormalization-group trajectory.

New critical phases in disordered nonabelian anyon chains. Extending their work on the disordered Fibonacci chain, Refael, Fidkowski and undergraduate student Han-Hsuan Lin, with Titum, studied the more general class of models classified by \(SU(2)_k\) [32] (where the Fibonacci model is the \(k = 3\) case). They found infinite-randomness critical phases for each odd \(k\), in the same universality class as phases previously constructed by Damle and Huse in a different setting. In contrast to this previous work, however, these critical phases of disordered anyon chains are stable phases rather than multicritical points that are destabilized by generic perturbations.

Dynamics of spinor condensates. Refael and postdoc Ryan Barnett, with Podolsky, studied the dynamics of a spinor Bose-Einstein condensate of cold atoms, another system with potential applications to quantum information processing [33, 34]. They derived a detailed description of the hydrodynamics of spinor condensates, and of their excitation spectrum. One unusual property of spinor-BEC’s is that the spin state exhibits a hidden point-group symmetry. They formulated a mapping between the excitations of spinor-condensates and those of electronic states in crystals with the same point group symmetry.
Ground state entanglement in one-dimensional translationally-invariant quantum systems. Irani showed that ground states of one-dimensional quantum systems with translationally-invariant local Hamiltonians can be highly entangled [35]. She constructed Hamiltonians for an infinite chain such that the entanglement entropy of a region containing \( n \) sites scales linearly with \( n \). A related construction yields translationally-invariant Hamiltonians for finite chains that have unique ground states exhibiting high entanglement. Previously, the best known bounds scaled logarithmically in \( n \).

Exact entanglement renormalization for string-net models. König and former IQI post-doc Ben Reichardt, with Vidal, showed that the ground states of Levin-Wen string-net models are fixed points of an explicit renormalization group transformation [36]. Their construction produces an exact representation of the ground-state wave function in terms of the so-called multi-scale entanglement renormalization ansatz (MERA), and an efficient circuit for preparing topologically ordered states using a quantum computer.

Simplifying quantum-double Hamiltonians using perturbative gadgets. Kitaev showed years ago that a topological phase that supports anyons associated with the quantum double of a finite group can be realized as the ground state of a local Hamiltonian. But Kitaev’s Hamiltonian included complicated four-site interactions, where the system at each site has dimension given by the order of the group. König recently constructed simpler Hamiltonians, with two-site interactions, that realize the same phases [37]. He showed using perturbation theory that Kitaev’s Hamiltonian is well approximated at low energy by the simpler Hamiltonian, which therefore has a similar ground state.

References Cited


