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 five broad areas: (1) Quantum algorithms that achieve speedups relative to classical algorithms, and limits on such algorithms. (2) Quantum protocols and quantum entanglement (3) Protection of quantum information using quantum error correcting codes, fault-tolerant protocols for quantum information processing, and control of quantum systems. (4) Theory and practice regarding physical implementations of quantum information processing. (5) Connections between quantum information science and other aspects of fundamental physics.

Since our last annual report in May 2010, IQI participants have produced 45 publications, which we summarize here.

Quantum algorithms and quantum complexity

Preparing thermal states of quantum systems with a quantum computer. Student Ersen Bilgin and postdoc Sergio Boixo proposed a new method for preparing thermal states of quantum many-body systems on a quantum computer [1]. By exploiting the underlying geometry of the systems of interest, their method obtains an exponential speedup over previously known alternatives. In particular, for one-dimensional systems, the running time of their quantum algorithm is dominated by the quantity $N \|h\|/T$, where $N$ is the size of the system, $\|h\|$ is a bound on the operator norm of the local terms of the Hamiltonian (the coupling energy), and $T$ is the temperature; hence the time complexity is polynomial in system size for any constant nonzero temperature.

Separating quantum computation from the polynomial hierarchy. Student Bill Fefferman, with Caltech computer science professor Chris Umans, studied the problem of finding a relativized separation of BQP, the class of problems with efficient quantum algorithms, from the Polynomial Hierarchy, a generalization of nondeterministic time believed to be strictly more powerful than NP. In [2] they proved that such a separation would follow from a previously studied conjecture on the capacity of the Nisan-Wigderson pseudorandom generator (with Majority as its
hard function) to fool polynomial size, constant depth classical circuits composed of AND, OR, and NOT gates of unbounded fan-in. In [3], Fefferman and Umans, with Shaltiel and Viola, and proved a simplification of this conjecture.

**Quantum algorithm for approximating Turaev-Viro invariants of mapping tori.** Postdoc Stephen Jordan, with Alagic, extended earlier work on quantum algorithms for computing topological invariants of three-dimensional manifolds. In 2010, with Koenig and Reichardt, they had shown that estimating the Turaev-Viro invariant for an arbitrary three-manifold presented by a Heegaard splitting is a BQP-complete problem. In 2011 they showed that for a restricted class of three-manifolds called mapping tori, the Turaev-Viro invariant can be estimated efficiently by a weaker model of quantum computation called the one-clean-qubit model, in which all but one of the qubits are initially maximally mixed [4]. Furthermore, this problem is complete for the one-clean-qubit complexity class.

**Complexity of commuting Hamiltonians on a square lattice of qubits.** Postdoc Norbert Schuch considered the computational complexity of Hamiltonians which are sums of commuting terms acting on plaquettes in a square lattice of qubits, and showed that deciding whether the ground state minimizes the energy of each local term individually is in the complexity class NP [5]. This is, if the ground states has this property, this can be proven using a classical certificate which can be efficiently verified on a classical computer. In contrast to previous results on commuting Hamiltonians, the certificate proves the existence of such a state without giving instructions on how to prepare it.

**Quantum property testing for bounded-degree graphs.** Postdoc Yi-Kai Liu, with Ambainis and Childs, found quantum algorithms for testing bipartiteness and expansion of bounded-degree graphs, which achieve a polynomial speed-up compared to the best possible classical algorithms [6]. These algorithms apply to the property testing setting, in which the graph either has the property $P$ or is far from having $P$. The quantum algorithm runs in time $\tilde{O}(N^{1/3})$, beating the $\Omega(\sqrt{N})$ classical lower bound. These results were obtained by combining the existing classical algorithms with the previously known quantum algorithm for element distinctness and a derandomization using $k$-wise independent bits.

**Quantum protocols, quantum entanglement, and quantum information theory**

**Direct fidelity estimation from few Pauli measurements** Postdoc Steve Flammia and Liu showed that the fidelity between an ideal quantum state or process and an actual one in a lab can be estimated by measuring only a constant number of Pauli expectation values, independent of the size of the system [7]. This scheme substantially reduces the experimental effort required to verify that large quantum computations are functioning as advertised. Their method is faster than full
tomography by a factor of $d$, the dimension of the state space, and extends easily and naturally to quantum channels.

**Achieving the physical limits of the bounded-storage model.** Student Prabha Mandayam and postdoc Stephanie Wehner studied the security of two-party quantum cryptography in the bounded-storage model, where the adversary can store only a fraction of the qubits transmitted during the protocol. Previously it was known that security is achievable if the fraction is less than one half, but they showed that the fraction can be close to one [9]. Their analysis relies on entropic uncertainty relations for encodings using higher-dimensional states; whether the same result can be obtained using BB84-encoded qubits is still open.

**Simplified instantaneous non-local quantum computation.** Postdoc Salman Beigi and Robert König studied the amount of entanglement required to implement non-local unitaries and measurements under communication constraints [10]. They found simple protocols reducing the entanglement consumption by an exponential amount compared to previously known methods. They also established a linear lower bound on the entanglement required for the implementation of certain measurements. These results relate to position-based cryptography: an amount of entanglement scaling exponentially in the number of communicated qubits is sufficient to render any such scheme insecure.

**Long distance two-party quantum cryptography.** Wehner, with Kerenidis, studied two-party quantum cryptography in a network setting [11]. It is known that any two-party primitive can be implemented securely using quantum communication under the assumption that it is difficult to store a large number of quantum states perfectly. Wehner and Kerenidis showed that such secure protocols can be achieved even when the parties are arbitrarily far apart. Specifically, they showed that oblivious transfer can be achieved in a network if and only if there exists a path in the network between the sender and the receiver along which all nodes are honest, assuming that neighbors in the network can achieve secure oblivious transfer. Their results are based on techniques from classical cryptography and do not resort to technologically difficult procedures like entanglement swapping.

**Operational interpretations of quantum discord.** Quantum discord quantifies non-classical correlations, going beyond the standard classification of quantum states into entangled and unentangled ones. Boixo, with Cavalcanti, Aolita, Modi, Piani, and Winter, gave quantum discord an operational meaning by relating it to entanglement consumption in an extended quantum state merging protocol [12]. They also found a connection between quantum discord and the performance imbalance in quantum state merging and dense coding.
Quantum error correction, fault tolerance, and control

Topological quantum computing in one-dimensional wire networks. Gil Refael, with Alicea, Oreg, von Oppen, and Fisher, proposed a realization of topological quantum computing using Majorana fermions in a network of quantum wires [13]. Building on work done last year, in which Refael and collaborators showed that Majorana fermions can arise in a semiconductor wire with strong spin-orbit coupling in proximity to a superconductor, they pointed out that these particles can be steered using a keyboard of voltage gates and exchanged when steered through wires with T-junctions; furthermore, they obey non-abelian exchange statistics suited for quantum information processing. Several experimental groups are now striving to build devices based on this proposal.

Self-correcting quantum memory in three dimensions. Student Jeongwan Haah proposed a mathematical model of self-correcting quantum memory in three dimensions [14]. While all previous three-dimensional models that are exactly solvable had string-like logical operators which made the models non-self-correcting, Haah proved that his model has no such string-like operators. The construction involves an exhaustive but systematic search over a large number of quantum codes. In later work with Bravyi, Haah studied the energy landscape of models without string operators, proving that for any such model there is an energy barrier protecting against logical errors that grows at last logarithmically with the system size [15].

Logical operator tradeoff for local quantum codes. John Preskill and Haah found limits on self-correcting quantum memory based on certain quantum codes in two dimensions [16]. They showed that a topologically ordered system realized by a stabilizer code can store neither quantum nor classical information reliably at any finite temperature. Their proof of this no-go result makes use of a succinct treatment of the Pauli group as a vector space over a finite field.

Interface between topological and superconducting qubits. Preskill and postdoc Liang Jiang, with Charlie Kane, proposed and analyzed an interface between a topological qubit and a superconducting flux qubit [17]. In this new scheme, the interaction between Majorana fermions in a topological insulator can be coherently controlled by a superconducting phase that depends on the quantum state of the flux qubit. A controlled-phase gate, achieved by pulsing this interaction on and off, can transfer quantum information between the topological qubit and the superconducting qubit.

Majorana fermions in equilibrium and driven cold atom quantum wires. Refael and Jiang, with collaborators, introduced a new approach to create and detect Majorana fermions using optically trapped 1D fermionic atoms [18]. In their proposed setup, two internal states of the atoms couple via an optical Raman transition simultaneously inducing an effective spin-orbit interaction and magnetic field, while a background molecular BEC cloud generates s-wave pairing for the atoms. The resulting cold atom quantum wire supports Majorana fermions at phase boundaries.
between topologically trivial and nontrivial regions, as well as “Floquet Majorana fermions” when the system is periodically driven. They also analyzed experimental parameters, detection schemes, and various imperfections.

**Universal dynamical decoupling of multi-qubit states from environment.** Jiang, with Imambekov, studied the dynamical decoupling of multi-qubit states from the environment [19]. For a system of $m$ qubits, the nested Uhrig dynamical decoupling (NUDD) sequence can efficiently suppress generic decoherence induced by system-environment interaction to $N$th order using a number of pulses polynomial in $N$. They proved that the NUDD sequence is universal, i.e., that it can restore the coherence of an $m$-qubit quantum system for any form of the system-environment interaction. They also constructed a general mapping between dynamical decoupling problems and discrete quantum walks in certain functional spaces.

**Toric codes and quantum doubles from two-body Hamiltonians.** Flammia, with Brell, Bartlett, and Doherty, showed that the complicated ground states in the topologically ordered phases of the Kitaev quantum double models can be realized using only two-body couplings [20]. The models require perturbative couplings, but unlike previous constructions which achieve similar results, the couplings retain an extensive number of symmetries of the original models, making them much more natural for potential implementations.

**Exactly solvable 3D quantum model with finite temperature topological order.** Student Isaac Kim found the first exactly solvable topologically ordered three-dimensional quantum many-body system that undergoes a finite temperature phase transition and has a ground state that cannot be described by a Calderbank-Shor-Steane code [21]. This system is a robust classical memory, but it cannot store quantum information at finite temperature.

**Experiment and implementation**

**Entanglement of spin waves among four quantum memories.** The Kimble group, with IQI Faculty Associate Steven van Enk, demonstrated high-fidelity measurement-induced entanglement stored in four atomic ensembles [23]. They showed that this atomic entanglement can be coherently transferred to four photonic quantum channels, and they fully characterized the four-part quantum entanglement using quantum uncertainty relations.

**Quantum opto-mechanics with weakly tethered membranes.** Kimble and postdoc Darrick Chang, with Ni and Painter, proposed and analyzed a new class of opto-mechanical systems that should be able to reach unprecedented values of the figure of merit $Q_m f_m$, where $Q_m$ is the quality factor of a mechanical oscillator and $f_m$ is its frequency [24]. Their technique uses optical forces to “trap” and stiffen the motion of a tethered mechanical structure, thereby freeing the resultant mechanical frequencies and decoherence rates from underlying material properties.

**Slow and stopped light in an opto-mechanical crystal array.** Chang, with Oskar
Painter’s group, proposed a technique to slow and stop an optical pulse by mapping that pulse into mechanical excitations in an opto-mechanical crystal array [25]. This scheme enables long storage times, large bandwidths, and ease of tuning on a compact, on-chip platform. The ability to implement a controllable pulse delay using a single opto-mechanical system was recently demonstrated experimentally by the Painter group [26].

Robust quantum state transfer in random unpolarized spin chains. Postdocs Liang Jiang and Alexey Gorshkov, with Yao, Gong, Zhai, Lukin, and Duan, proposed a new approach for transferring quantum states between remote spin qubits via certain classes of random, unpolarized spin chains [27]. They showed that the method is robust to coupling strength disorder and does not require control over individual spins. They also demonstrated the method’s applicability in solid-state quantum information processors, such as those based on Nitrogen-Vacancy color centers in diamond.

Scalable architecture for a room temperature solid-state quantum information processor. Jiang and Gorshkov, with Yao, Maurer, Giedke, Cirac, and Lukin, proposed an architecture for a scalable, solid-state quantum information processor capable of operating at or near room temperature [28]. They showed that the architecture, based on Nitrogen-Vacancy color centers in diamond, is applicable to realistic conditions, which include disorder and relevant decoherence mechanisms. The proposed architecture may greatly alleviate the stringent constraints currently limiting the realization of scalable quantum processors.

Photon-photon interactions via Rydberg blockade. Gorshkov, with Otterbach, Fleischhauer, Pohl, and Lukin, developed the theory of light propagation under the conditions of electromagnetically induced transparency in systems involving strongly interacting Rydberg states [29]. They demonstrated that this system can be used for the generation of nonclassical states of light including trains of single photons, for implementing photon-photon quantum gates, as well as for studying many-body phenomena with strongly correlated photons.

Resolved atomic interaction sidebands in an optical clock transition. Gorshkov, with Bishof, Lin, Swallows, Ye, and Rey, reported on the experimental observation of resolved atomic interaction sidebands in the $^{87}$Sr optical clock transition when ultracold Sr atoms are confined in a two-dimensional optical lattice [30]. They predict that the interaction sidebands will function as powerful spectroscopic tools in optical clocks, quantum simulators, and quantum information processors based on strongly interacting alkaline-earth gases.

Light storage in an optically thick atomic ensemble under conditions of electromagnetically induced transparency and four-wave mixing. Gorshkov, with Phillips and Novikova, presented a detailed theoretical and experimental study of the effects of four-wave mixing on light storage in A-type atomic media [31]. Specifically, they showed that the two weak coherent fields involved in the four-wave mixing cannot be stored independently of each other. These findings shed light on limitations of photonic quantum memories operated in the presence of...
four-wave mixing.

**Graphene plasmonics.** Chang, with Koppens and de Abajo, proposed that surface plasmon excitations in graphene can be used to confine electromagnetic fields to volumes that are approximately $10^6$ times smaller than allowed by the diffraction limit in free space [32]. The associated enhancement in the per-photon electric field in turn allows for extremely strong quantum light-matter interactions, and makes graphene an attractive alternative to cavity quantum electrodynamics. They showed theoretically that vacuum Rabi splittings between a single quantum emitter and a single plasmon in graphene should be experimentally observable.

**The dark exciton as a bright qubit.** Postdoc Netanel Lindner, with the Gershoni group, studied the optical accessibility and coherence properties of an excited electron in a quantum dot which is prohibited from relaxing to its ground state, known as a “dark exciton” [33]. Their theoretical and experimental results indicate that the dark excitation can be accessed optically and has a long coherence time, making it a promising candidate for a qubit.

**Nonlinear interferometry with Bose-Einstein condensates.** Boixo, with Tacla, Datta, Shaji, and Caves further developed their earlier proposal to achieve a sensitivity scaling better than $1/N$ in a nonlinear Ramsey interferometer that uses a two-mode Bose-Einstein condensate (BEC) of $N$ atoms [34]. Their numerical simulations confirm analytical predictions concerning how the spreading of the BEC ground-state wave function affects the ideal $N^{-3/2}$ scaling. They conclude that the two modes share the same spatial wave function for a length of time that is sufficient to run the metrology scheme.

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

**Topological phases of fermions in one dimension.** Alexei Kitaev and postdoc Lukasz Fidkowski classified the topologically distinct phases of one-dimensional gapped systems with a given symmetry [35]. Specifically, they considered Majorana chains with a nonstandard time-reversal operation (which squares to 1 rather than -1). While the band classification yields an integer topological index, they had previously demonstrated that phases characterized by integers in the same congruence class modulo 8 can be adiabatically transformed one to another by adding suitable interaction terms. Their more recent results show that these eight quantum phases really are distinct, and that there are no other phases. They used matrix-product state methods to prove these results.

**Models for gapped boundaries and domain walls.** Kitaev and former IQI postdoc Liang Kong defined a class of lattice models for two-dimensional topological phases with boundary such that both the bulk and the boundary excitations are gapped [36]. The bulk part is constructed using a unitary tensor category $\mathcal{C}$ as in the Levin-Wen quantum code, whereas the boundary is associated with a module category over $\mathcal{C}$. They also considered domain walls (or defect lines)
between different bulk phases, showing that a domain wall is transparent to bulk excitations if the corresponding unitary tensor categories are Morita equivalent.

**Condensation and symmetries in quantum double models.** Postdoc Salman Beigi, with Shor and Whalen, studied boundaries of bulk phases described by quantum double models [37]. Their framework can be used to study equivalences between two anyonic systems, or symmetries of a single system. In particular they showed that for a class of groups, where $\mathbb{Z}_2$ and $S_3$ are two examples, transposition of a certain pair of chargeon and fluxon together with charge conjugation of all particles gives a symmetry of the anyonic system.

**Anyonic entanglement renormalization.** Postdoc Robert König and student Ersen Bilgin proposed a new variational ansatz for states arising in topological quantum field theories [38]. Their method generalizes the multi-scale entanglement renormalization ansatz for spins and fermions, optimally exploiting the structure of the anyonic Hilbert space. To test the accuracy of the ansatz, they numerically reproduced ground state energies and correlations function for the so-called golden chain and its variations, matching conformal field theory predictions in the thermodynamic limit.

**Classifying quantum phases using matrix-product states.** Postdoc Norbert Schuch, with Perez-Garcia and Cirac, used the framework of matrix-product states (MPS) and their associated parent Hamiltonians to give a classification of gapped quantum phases of one-dimensional systems, both without and with symmetries [39]. To this end, they introduced a new normal form – the isometric form – which allows for an easy classification of phases. In the absence of symmetries, they found that the classification depends on the ground state degeneracy, while imposing symmetries leads to a classification based on projective representations of the symmetry group and its subgroups.

**Complexity of computing the density of states.** Flammia and Schuch, with Brown, studied the computational complexity of computing the density of states for local Hamiltonians, as well as the problem of computing ground state degeneracies [40]. They introduced a quantum counting class $\#\text{BQP}$, and showed that both problems are complete for this class. They also showed that $\#\text{BQP}$ is no harder than its classical counterpart $\#\text{P}$ (counting satisfying inputs to a Boolean function); thus computing these numbers for quantum Hamiltonians is just as hard as for classical Hamiltonians.

**Information propagation for bosonic systems.** Lieb-Robinson-bounds limit the speed at which information can propagate in systems with bounded interaction strength. Schuch, with Harrison, Osborne, and Eisert, studied the propagation of information in systems of interacting bosons, and showed that, despite the unboundedness of the interactions, bosons always propagate at a finite speed into initially empty regions, thus limiting the speed at which information can propagate in those systems [41].

**Entanglement spectra and boundary theories.** Schuch, with Cirac, Poilblanc, and Verstraete, used Projected Entangled Pair States (PEPS) to define a rigorous holographic mapping
between bulk and boundary theories [42]. In particular, this mapping associates to any bulk region a Hamiltonian on its boundary such that the spectrum of the bulk region’s reduced density operator corresponds to the excitation spectrum of the boundary theory; furthermore, bulk properties such as criticality or topological order are reflected in the interaction structure of the boundary model.

**Power-law spin correlations in a perturbed honeycomb spin model.** Kitaev, with Tikhonov and Feigel’man, studied Kitaev’s honeycomb lattice model in the presence of a weak magnetic field, which destroys the model’s exact integrability in terms of gapless fermions and static $Z_2$ fluxes [43]. They showed that the perturbed model has a long-range tail in the irreducible dynamic spin correlation function, decaying as the minimum of $r^{-4}$ and $t^{-4}$, where $r$ is distance and $t$ is time.

**Definition of quantum phases.** Postdoc Spyridon Michalakis, with Bachmann, Nachtergaele, and Sims, formulated a rigorous definition of quantum phases [44]. Their work formalizes the notion that two states are in the same phase if one can be transformed to the other with quasi-locally generated unitaries over a gapped path of Hamiltonians. The ultimate goal is to identify a minimal set of conditions under which general gapped systems are stable against perturbations, an important step toward classifying the quantum phases of interacting systems.

**Floquet topological insulator.** Phase transitions between conventional and topological insulators have been proposed and observed in mercury telluride/cadmium telluride quantum wells. Lindner and Refael, with Galitski, proposed that a topological state can be induced in such a device by shining microwave radiation on the conventional insulator, without closing the gap and crossing the phase transition [45]. They showed that the quasi-energy spectrum exhibits a single pair of helical edge states, and that the velocity of the edge states can be tuned by adjusting the intensity of the microwave radiation. Their work launch a new subject: non-equilibrium topological phases of matter.

**References Cited**


