

Institute for Quantum Information

Findings – 2000-2006

Research themes at the IQI

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 Institute for Quantum Information (IQI) was established on 1 September 2000, funded by a five-year ITR award from NSF. (The award period was later extended by six months.) During the period from 1 September 2000 to 28 February 2006, IQI participants produced over 200 publications. This document is a summary of these contributions.

The IQI, led by a multidisciplinary team of five Caltech professors, is devoted to building the theoretical foundations of quantum information science across a broad front encompassing quantum algorithms, quantum cryptography, fault-tolerant quantum information processing, and physical implementations of quantum computing. We believe that basic advances in all of these areas are needed to bring revolutionary quantum technologies closer to realization.

We emphasize that the IQI is far more than the sum of the research groups it includes. By providing a hub for the widespread research efforts at Caltech in quantum information science, and by facilitating interaction with the broader quantum information science community beyond Caltech, the IQI has created a unique research environment that strongly encourages work straddling the traditional boundaries between academic disciplines. This interdisciplinary attitude has many manifestations reflected in our research accomplishments, which include the discovery of new quantum algorithms, insights into the security of quantum cryptography, new characterizations of quantum separability, new approaches to the realization of topological quantum computing, and new ideas about the simulation of quantum many-body systems.

The primary goal of the IQI is to broaden and deepen the foundations of theoretical quantum information science and quantum computation by fostering fruitful interactions between physicists and computer scientists. Our research covers six broad areas:

- (1) **Quantum algorithms that achieve speedups relative to classical algorithms, and limits on such algorithms.** It is known that quantum computers (if and when we succeed in building them) could solve certain problems far faster than any foreseeable digital computers.

But our current understanding of the power of quantum computing is very limited. For what types of problems are dramatic quantum speedups potentially achievable? Arguably, better characterizing what quantum computers can and cannot do is the most important challenge confronting theoretical QIS.

- (2) **Quantum cryptographic protocols, and other types of communication using quantum states.** Cryptographic protocols that use quantum information rather than classical data can achieve a higher level of security than is possible with classical protocols — the best known example is quantum key exchange, in which a secure shared key is established that can be used for encrypted communication. For what other cryptographic tasks do quantum resources offer distinct advantages? More broadly, in what characteristic ways is communication over a noisy quantum channel different than communication over a noisy classical channel?
- (3) **Quantum entanglement and the theory of transformations among quantum states.** The crucial feature that distinguishes quantum information and classical information is quantum entanglement — the state of a whole quantum system can be more definite than the state of its parts, which is not possible for classical systems. Entanglement can be viewed as a resource that enables certain tasks that cannot be performed without entanglement. How do we characterize and quantify this resource (particularly for systems that are divided into more than two parts)?
- (4) **Protection of quantum information using quantum control, quantum error-correcting codes, and fault-tolerant protocols for quantum information processing.** Reliable large-scale quantum computers and other quantum technologies will never be realized unless quantum states can be suitably protected from damage caused by decoherence and other potential sources of error. How will we control intricate quantum systems? How can we connect the sophisticated theory of quantum error correction to the performance of practical devices?
- (5) **Theory and practice regarding physical implementations of quantum information processing.** Many methods for implementing quantum information processing in the laboratory have been proposed and are being actively pursued, but all are difficult. What new approaches to implementation might bring quantum computers closer to feasibility? What physical systems possess an inherent robustness to imperfections, due to either their fundamental character or their concrete experimental realization? How can entanglement and coherence be exploited to surpass the naive quantum limits on measurement precision?
- (6) **Connections between quantum information science and other aspects of basic physics.** 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. How can insights into the properties of quantum entanglement be exploited in the study of quantum many-body systems and quantum phase transitions? Can progress in quantum information theory illuminate how information is encoded in spacetimes subject to strong quantum fluctuations?

Quantum algorithms and quantum complexity

We have discovered new efficient quantum algorithms, new quantum lower bounds, and new relations among quantum complexity classes. We have also developed the theory of Hamiltonian simulation.

Some research highlights

Efficient quantum algorithm for Pell’s equation. Sean Hallgren formulated an efficient quantum algorithm for the principle ideal problem over real quadratic number fields [1]. An important application of Hallgren’s method is to a problem that has been studied for over 1000 years: finding integer solutions (x, y) to Pell’s equation $x^2 - dy^2 = 1$, where d is an integer that is not a perfect square. This problem is at least as hard as factoring integers, and in fact the best known classical algorithm for solving Pell’s equation is exponentially slower than the best known classical algorithm for factoring.

Quantum algorithms for hidden shift problems. Hallgren, with van Dam and Ip, generalized the hidden subgroup problem to “hidden coset” and “hidden shift” problems that are also solvable efficiently on a quantum computer using the quantum Fourier transform [2]. 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 .

Tight quantum lower bound for the collision problem. Yaoyun Shi found a tight lower bound on the *collision problem*: Given a function f , the problem is to find x and y such that $f(x) = f(y)$, under the promise that such inputs exist. Classically, of order $n^{1/2}$ evaluations of the function are necessary and sufficient, where n is the number of possible values of the input. Shi’s bound establishes that of order $n^{1/3}$ evaluations are necessary and sufficient in the quantum case [3]. Shi’s tight bound improved on a weaker lower bound found earlier by IQI visitor Scott Aaronson [4].

Fourier sampling applied to nonabelian hidden subgroup problems. Leonard Schulman has studied the efficacy of the Fourier sampling method applied to nonabelian hidden subgroup problems. With Grigni, Vazirani, and Vazirani [5], he found that this method works effectively for groups that are “almost abelian,” but that it does not distinguish well between subgroups

that are related by conjugation, or between certain pairs of nonconjugate subgroups. With Moore, Rockmore, and Russell [6], he found that for some groups a carefully chosen measurement performed after execution of the quantum Fourier transform suffices for reconstruction of the hidden subgroup, but that measuring in a randomly chosen basis does not suffice. With Moore and Russell [7], he showed that for the symmetric group, not even a measurement in a cleverly chosen basis is adequate for extracting information about the hidden subgroup from a single copy of a coset state.

Optimal measurements for nonabelian hidden subgroup problems. Dave Bacon and Andrew Childs, with van Dam, found the optimal measurement for distinguishing hidden subgroups that can be performed on k copies of the coset state, for the dihedral group [8] and for other groups [9]. They showed that there is a sharp threshold in k : if the number of copies is above a critical value, the problem can be solved, but if the number of copies is below this value, then the accessible information about the hidden subgroup is negligible. They also studied the quantum complexity of the optimal measurement, relating it to the complexity of solving the subset sum problem.

QMA. Alexei Kitaev, with Shen and Vyalıy, published a book (based on the quantum computing course he has taught at Caltech) that contains many new results concerning quantum algorithms and quantum complexity [10]. For example, Kitaev defined the new computational class QMA (a quantum analog of NP or MA) and gave an example of a QMA-complete problem; this could be regarded as the quantum analog of the Cook-Levin theorem, the fundamental result of classical complexity theory.

Quantum analogue of k -SAT. Sergey Bravyi formulated a quantum analogue of the satisfiability problem (“quantum k -SAT”), and showed that quantum 2-SAT can be solved efficiently by a classical computer [11]. He also showed that for $k \geq 4$ quantum k -SAT is a complete problem for the complexity class QMA with one-sided error.

Other findings

Analysis of one-dimensional quantum random walks [12, 13].

Simulation of Hamiltonian evolution with homogeneous operations [14].

Characterization of when a subgroup of a compact Lie group is dense [15].

Bipartite product Hamiltonians can simulate each other reversibly [16].

Time-optimal two-qubit Hamiltonian simulation [17].

Quantum complexity class QMA is contained in gap-definable classical class A0PP [18].

Approximating the weight enumerator is hard for the polynomial hierarchy [19].

Local search via the Dirac equation matches discrete-time quantum walks [20].

NP problems from quantum stabilizer codes [21].

Power of entanglement in two-prover interactive proof systems [22].

Universality classes for multi-body interactions [23, 24].

Relation of measurement-based quantum computation to one-way quantum computing [25, 26, 27].

Optimal decomposition of two-qubit gates into controlled-not gates and single-qubit gates [28].

The 2-local Hamiltonian problem is QMA-complete [29].

Efficient quantum circuit for the Schur transform [30].

Quantum cellular automaton for universal quantum computation [31].

Efficient quantum computation with probabilistic quantum gates [32].

Quantum computation via translation-invariant operations on a chain of qubits [33].

Optimal measurements for pure state discrimination problems [34].

Quantum algorithm for a generalized hidden shift problem [35].

Quantum hardness of solving isomorphism problems as nonabelian hidden shift problems [36].

Physical limits of heat-bath algorithmic cooling [37].

Quantum algorithms and applications for the Jones polynomial [38].

Quantum communication and quantum cryptography

We have found new security proofs for quantum protocols, and new limitations on security. We have shown that quantum protocols can be composed safely, and have discovered efficient new schemes for encrypting quantum data.

Some research highlights

Security of quantum key distribution. John Preskill, with Gottesman, proved the security of a quantum key distribution system in which squeezed states of light are transmitted [39]. With Koashi, Preskill proved security for a key distribution scheme that uses a badly flawed source [40] (but a perfect detector), and with Gottesman, Lo, and Lütkenhaus he proved security for the case where both the source and the detector have small flaws [41].

Security of quantum coin flipping. Alexei Kitaev showed that any strong quantum coin flipping protocol is susceptible to same-sided bias [42] — by cheating, one player or the other can force the coin to come up heads with probability $1/\sqrt{2} \approx .707$. Carlos Mochon found a weak coin tossing protocol in which the cheater cannot force a win with probability above $2/3$ [43, 44]; he also found improved bounds on the cheat sensitivity of quantum bit commitment protocols [45].

Composability of quantum protocols. Dominic Mayers, with Ben-Or, analyzed how quantum protocols can be composed without compromising security [46], and with Ben-Or, Horodecki, and Oppenheim, Mayers and Debbie Leung showed in particular that classical authentication can

be securely composed with quantum key distribution [47]. Their result means that a key generated in a round of key distribution can be used safely to authenticate further rounds.

Applications of quantum state randomization. Patrick Hayden and Leung, with Shor and Winter, used a probabilistic construction to show that it is possible to encrypt quantum data using half the resources that had previously been thought necessary [48]. Using related ideas, they constructed schemes for bipartite quantum data hiding at a rate of one hidden qubit per pair of physical qubits, and showed the existence of bipartite quantum states such that transmitting a negligibly small classical key can unlock an arbitrarily large amount of classical correlation (an improvement over an earlier observation of Leung and collaborators [49]).

Other findings

One more round of communication can reduce quantum communication complexity exponentially [50].

Almost all bipartite entangled states are useful for catalyzing some entanglement transformation [51].

Tight bound on the probability of error in entanglement-assisted communication [52]

Hiding two classical bits is equivalent to hiding one quantum bit [53].

Using a Heisenberg spin chain as quantum channel [54].

Formula for classical capacity of a unital qudit channels [55, 56].

Proof of security for quantum measurement commitment [57].

Scheme for self-testing of quantum devices [58].

Superdense coding of entangled quantum states [59, 60] as “father” of remote state preparation [61].

Tradeoff of cbits, qubits, and ebits in quantum communication [62].

Compressibility of correlated quantum sources [63]

Multipart quantum data hiding with one hidden qubit per local physical qubit [64].

Tradeoff between forward and backward communication for bidirectional channels [65].

Achieving quantum gates through local interactions in a spin chain [66].

Theory of fermionic Gaussian channels, and the effect of measurement on fermion number [67].

The number of “refbits” needed to achieve communication tasks [68].

Tradeoff between forward and backward coherent classical communication [69].

Capacity theorems for quantum multiple access channels [70].

Improvement in the security of quantum key distribution arising from phase randomization [71].

Entanglement-assisted one-way capacity of a two-way quantum channel [72].

Classical capacity of fermionic product channels [73].

Quantum key distribution based on arbitrarily weak distillable entangled states [74]

Quantum entanglement and quantum information theory

We have found new criteria for bipartite quantum separability, and have shown that bipartite quantum nonlocality can be usefully quantified in terms of classical communication.

Some research highlights

Complete hierarchy of tests that distinguish separable and entangled states. Andrew Doherty, Pablo Parrilo and Federico Spedalieri devised a hierarchy of tests to determine whether a bipartite state is entangled [75, 76, 77, 78]. Each test is a semidefinite program that can be solved efficiently, and constructs an explicit entanglement witness when successful. (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.)

Quantifying quantum nonlocality with classical communication. Dave Bacon and Ben Toner characterized the amount of classical communication needed to simulate quantum correlations [79, 80]. They discovered, for example, that projective measurements on a Bell pair can be simulated with a single bit of communication. One implication of their work is a new bound for the detector inefficiency loophole in certain Bell experiments.

Entanglement of spin-squeezed many-particle states. JM Geremia, Hideo Mabuchi, Doherty, and John Stockton quantified the entanglement of bipartite spin squeezed ensembles of two-level atoms, and investigated the robustness of this entanglement to the loss of atoms from the sample. Such ensembles are promising test-beds for quantum communication experiments [81].

Localizable entanglement. Frank Verstaete, with Popp, Martin-Delgado, and Cirac, formulated the concept of localizable entanglement (and the related concept of entanglement length), applying it to the characterization of quantum phases of matter [82]. They studied the entanglement that can be localized, on average, between two separated spins by performing local measurements on the remaining spins, and related this quantity to connected correlation functions. The entanglement length typically diverges at a quantum critical point, and may diverge even when the correlation length remains finite.

Monogamy of nonlocal quantum correlations. Ben Toner derived upper bounds on the correlations in a bipartite physical system that follow only from the requirement that superluminal signaling is impossible, without assuming the validity of quantum mechanics [83]. He also showed

that in a tripartite system ABC , forcing classical correlations between B and C prevents A and B from violating certain Bell inequalities that are relevant to the security of cryptography.

Other findings

Tradeoff of qubits and bits in visible quantum data compression [84].

Entanglement can be “embezzled” from a catalyst without damaging the catalyst [85].

Quantifying the classical communication needed for entanglement transformations [86, 61].

Entanglement of purification: a measure attaching value to both quantum and classical correlations [87].

Bounds on quantum communication complexity from Renyi entropy [88].

Bell pairs and three-part (GHZ) states are not adequate for reversibly generating all three-part states [89].

A review of quantum entanglement theory [90].

Semidefinite program for constructing local hidden variable theories for quantum states [91]

Necessary and sufficient conditions for a mean field state to be compatible with a pure state [92].

Conditions for equality in strong subadditivity of von Neumann entropy [93].

States with nearly maximal entanglement of formation can have negligible entanglement of distillation [94].

There are three-qubit bound entangled states that are not locally interconvertible [95, 96].

Efficiently computable multi-partite entanglement measure for stabilizer states [97].

Characterization of communication between two systems both coupled to the same system [98].

Analysis of a quantum phase transition in a noisy three-dimensional cluster state [99].

Conditions for the existence of a multi-part mixed state with specified marginal density operators [100].

Review of entanglement in random subspaces [101].

Application of Schubert calculus to quantifying correlations in quantum systems [102].

Limitations of nice mutually unbiased bases [103].

Robustness of two-mode squeezed states [104].

Entropic uncertainty relations for mutually unbiased observables [105].

Recipe for sequential generation of entangled multi-qubit states [106].

Bounds on the maximal number of real mutually unbiased bases [107].

Characterization of combinatorically independent permutation separability criteria [108, 109].

Extending the number of observers in a Bell inequality [110].

General monogamy inequality for bipartite qubit entanglement [111].

GHZ extraction yield for multipartite stabilizer states [112].

Emergent classicality of redundantly stored quantum information [113].

Asymptotic entanglement of assistance of a general bipartite mixed state [114].

Relating construction of mutually unbiased bases to orthogonal decompositions of Lie algebras [115].

Quantifying nonlocality using Popescu-Rohrlich boxes [116].

Evolution of entanglement due to wave packet scattering [117].

Typical entanglement of stabilizer states [118].

Review of entanglement in graph states and applications [119].

Quantum error correction and fault tolerance

We have advanced the theory of topological quantum computation, and have found new connections between quantum fault tolerance and statistical physics.

Some research highlights

Error correction for continuous quantum variables. Kitaev and Preskill, with Gottesman, developed fault-tolerant schemes for processing quantum information encoded in the infinite-dimensional Hilbert space of a system described by continuous quantum variables, such as a mode of the electromagnetic field in a small cavity [120]. The experimental tools needed to perform the computation are plausibly available in the quantum optics laboratory: linear optical elements, squeezers, and photon counters.

Model reduction for concatenated quantum codes. Doherty, Mabuchi, and Ben Rahn have developed new tools for analyzing the performance of concatenated codes [121]. They expressed the effect of adding a level of concatenation as an iterative map acting on an error model for encoded quantum information, and found unstable fixed points of these maps corresponding to the accuracy threshold for quantum storage. They have also adapted the control theory method of balanced truncation to analyze codes with many levels of concatenation.

Phase transition in noisy quantum computers with local gates. Kitaev, Preskill, Eric Dennis, and Andrew Landahl [122] and Chenyang Wang, Jim Harrington, and Preskill [123] discovered intriguing connections between fault-tolerant quantum computation and phase transitions in disordered systems. 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. Their analysis yields improved numerical estimates of the accuracy threshold, and suggests that topological codes provide a promising framework for quantum computing architectures.

Theory of nonabelian anyons. Kitaev constructed an exactly solvable but highly nontrivial quantum spin model in two dimensions, and showed that the spectrum of the model contains nonabelian anyons, whose charges can encode robust quantum information [124]. Mochon showed that the braiding of anyonic magnetic charges with fluxes in a non-solvable finite group suffices for universal quantum computation [125]; in fact it suffices that the group not be nilpotent if electric charges are used as well [126].

Continuous-time quantum error correction using weak measurements. Charlene Ahn, with Doherty and Landahl [127], with Wiseman and Milburn [128], with Wiseman and Jacob [129], and with Sarovar, Jacobs, and Milburn [130], developed schemes for quantum error correction that use weak measurement accompanied by quantum feedback rather than fast projective measurements (which are not always available in realistic laboratory settings).

Universal quantum computation based on distillation of magic states. Kitaev and Sergey Bravyi formulated distillation protocols that extract high-fidelity “quantum software” states from many noisy copies [131]. These protocols can be used to complete the set of universal fault-tolerant gates for a large class of quantum error-correcting codes. Bravyi also used such distillation schemes to show that one rather noisy nontopological gate, together with the topological gates, suffices for universal quantum computation using the anyons of the $\nu = 5/2$ fractional quantum Hall state [132].

Proofs of quantum accuracy threshold theorems. Preskill and Panos Aliferis, with Gottesman, developed new analytic mathematical tools for analyzing the efficacy of fault tolerant protocols that protect quantum states from damage [133]. With these methods, they found a new proof of the quantum accuracy threshold theorem, which is both simpler and more general than previous proofs; it also establishes a rigorous lower bound on the accuracy threshold that is a big improvement over previous estimates. Preskill and Kitaev, with Aharonov, extended these techniques to prove a quantum threshold theorem that applies to non-Markovian noise with algebraically decaying spatial correlations [134]. Aliferis, with Terhal, extended the methods of [133] in a different direction, providing a rigorous analysis of fault-tolerant quantum computation in the presence of local leakage faults [135].

Fault-tolerant one-way quantum computer. Robert Raussendorf and Kovid Goyal, with Harrington, invented a new scheme based on topological codes for performing fault-tolerant quantum computation using cluster states, and proved a quantum accuracy threshold theorem based on their scheme [136]. Using different methods, Aliferis and Debbie Leung also proved an accuracy threshold theorem that applies to simulations of quantum circuits based on general graph states

[137].

Other findings

Achievable rates for the Gaussian quantum channel from lattice coding [138].

Application of model reduction to quantum control [139].

Analysis of fault tolerance of adiabatic quantum computation [140]

Performance of higher-dimensional topological codes [141].

Estimate of the accuracy threshold when all quantum and classical processing is local [142].

Analysis of the “corrected capacity” of a quantum channel, achieved by measuring the environment [143].

Demonstration that two different methods lead to equivalent schemes for decoupling unwanted interactions [144].

Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays [145].

Optimal quantum control depends only on the filter [146].

Review of nonlinear dynamics of measured quantum systems [147].

Introduction to noncommutative quantum filtering theory [148, 149].

Optimal pointers for joint measurement of sigma-x and sigma-z via homodyne detection [150].

Optimal error tracking via quantum coding and continuous syndrome measurement [151].

Physical implementation of quantum information processing

We have proposed scalable schemes for achieving quantum computation with atoms and photons.

Some research highlights

Entangling many atomic ensembles. Luming Duan developed approaches to quantum computation that use macroscopic ensembles of atoms to store and manipulate quantum states, a method with some naturally fault tolerant features. These methods seem to be feasible with current technology, and scalable to systems with many encoded qubits. In particular, Duan has proposed an experimentally feasible scheme to generate multiqubit entangled “cat states” based on simple linear optical operations and single-photon detection [152].

Controlling spin exchange interactions in optical lattices. Duan, with Demler and Lukin, has proposed an efficient way to engineer many-body spin Hamiltonians in optical lattices [153]. In this proposal, the lattice geometry and spin-dependent tunneling interactions between the atoms are specified by controlling interfering laser beams. In particular, Duan et al. have

suggested a way to realize a model proposed by Kitaev [124] that supports both abelian and nonabelian anyons.

Scalable photonic quantum computation through cavity-assisted interaction. Duan and Kimble proposed a scheme for scalable photonic quantum computation based on cavity assisted interactions between single-photon pulses [154]. A quantum controlled phase-flip gate between the single-photon pulses is achieved by successively reflecting the pulses from an optical cavity with a single-trapped atom. They demonstrated that the proposal is robust against practical noise and experimental imperfections in current cavity-QED setups.

Other findings

Analysis of Bell inequality violation exhibited by continuous-variable entangled states [155].

Formalism for sensitivity optimization in continuous quantum measurements [156].

Theory for optical microscopy realized with single atoms trapped in optical resonators [157].

Demonstration of adaptive homodyne measurement of optical phase [158].

Analysis of quantum limits on sensitivity of interferometric gravitational-wave detectors [159].

Three-dimensional theory for interactions of light with atomic ensembles [160].

Algorithm for design of photonic crystals for quantum computation [161].

Proposal for simulation of quantum dynamics using cold atoms or trapped ions [162].

Proposal for engineering of multi-atom entanglement through single-photon detection [163].

Proposal for quantum information processing with “hot” trapped atoms [164].

Protocol for simulating a quantum circuit using a spin chain [165].

Entangled photon pairs generated by collective emission from atomic ensembles [166].

Improved demonstration of quantum teleportation of light beams [167].

Experimental realization and theoretical analysis of a one-atom laser [168, 169].

Generation of single photons on demand using atomic ensembles [170].

Continuous measurement and real-time feedback on symmetric spin ensembles [171].

Analysis of stable quantum state preparation using real-time feedback for a single qubit [172].

Deterministic Dicke state preparation with continuous measurement and control [173].

Robust quantum gates on neutral atoms with cavity-assisted photon-scattering [174].

Strategies for real-time position control of a single atom in cavity QED [175].

Theory of photon blockade by an optical cavity with one trapped atom [176].

Feedback cooling of atomic motion in cavity QED [177].

Measurement-induced entanglement for excitation stored in remote atomic ensembles [178].

Low-lying bifurcations in cavity quantum electrodynamics [179].

Efficient retrieval of a single excitation stored in an atomic ensemble [180].

Connecting quantum information with the rest of physics

Inspired by entanglement theory, we have proposed efficient new methods for simulating quantum many-body systems using classical computers.

Some research highlights

Efficient classical simulation of slightly entangled quantum computers and of quantum many-body systems. Vidal used an iterated Schmidt decomposition to show that a quantum computation can be efficiently simulated by a classical computer provided that the entanglement between any two parts of the computer is bounded above by a constant [181]. He then exploited this observation to formulate efficient classical simulations of the real-time evolution of quantum spin chains [182]. With Daley, Kollath, and Schollwoeck, Vidal clarified the connections between his new algorithm and established density-matrix-renormalization-group (DMRG) methods [183]. Verstraete, with Cirac, showed that matrix product states, which can be succinctly described classically, provide good approximations to ground states of one-dimensional spin chains, explaining the efficacy of renormalization group algorithms for in one dimension [184].

Jordan-Wigner transformations in higher dimensions. Verstraete, with Cirac, showed how to map local fermionic problems onto local spin problems on a lattice in any dimension. The main idea (adapted from an earlier proposal by Bravyi and Kitaev) is to introduce auxiliary degrees and a novel quantum coding scheme. With this method, it should be possible to simulate fermionic systems in two and three dimensions on classical computers with unprecedented efficiency [185].

Entanglement in quantum critical phenomena. Vidal and Kitaev, with Latorre and Rico, quantified the ground-state entanglement in several one-dimensional spin chain models, using both analytic and numeric methods [186, 187], by studying the entropy for a segment of L consecutive spins on the chain. In addition to calculating the critical behavior, they found the leading dependence of the entropy on the deviation from the critical point. Vidal also calculated how the entropy decreases along a renormalization group trajectory in the critical Ising spin chain [188].

Entanglement renormalization. Vidal developed a real-space method for renormalizing entangled quantum states of lattice systems in any number of spatial dimensions [189]. Numerical simulations in one dimension show that the resulting coarse-grained site requires a Hilbert space dimension that does not grow with successive scale transformations. With this method one can analyze the ground state of a critical system comprising tens of thousands of quantum spins with a computational effort that scales logarithmically in the system's size.

Topological entanglement entropy. Kitaev and Preskill discovered a new type of universal “topological quantum entanglement” that arises in topologically ordered gapped two-dimensional media [190]. Using methods borrowed from topological quantum field theory, they found a formula for the entropy that characterizes this topological entanglement, in terms of the properties of the superselection sectors of the medium.

Detecting nonabelian statistics in the $\nu = 5/2$ fractional quantum Hall state. Parsa Bonderson, Kitaev, and Kirill Shtengel proposed an interferometric test of non-Abelian statistics in fractional quantum Hall systems, that would provide the first proof of principle in the lab of one of the primitive elements of a topological quantum computer [191]. This paper (and an independent paper by Halperin and Stern that appeared at the same time) set in motion an intense race to confirm the predicted experimental signal, as is featured in the Search and Discovery section of the October 2005 Physics Today and in the April 2006 Scientific American.

Superselection rules and quantum protocols. Kitaev, Mayers, and Preskill studied the impact of local conservation laws (superselection rules) on the security of quantum games [192]. By explaining how the physics of the invariant world (subject to the conservation law) can be simulated in the unrestricted world and vice versa, they clarified the physical implications of superselection rules, which have a central role in modern quantum field theory.

Other findings

Causal quantum operations need not be localizable [193].

Nondemolition measurement of a spacelike Wilson loop operator is impossible in a relativistic nonabelian gauge theory [194].

There are quantum states that cannot be the ground state of any local Hamiltonian [195].

NP-hard problems can be solved by quantum computers with access to time-traveling qubits [196].

Teleportation with future boundary conditions does not resolve the black hole information paradox [197].

Classical algorithm for simulating mixed-state dynamics in spin chains [198].

Nearest neighbor entanglement for many spins in ring and star geometries [199].

Efficient evaluation of partition functions of frustrated and inhomogeneous spin systems [200].

Variational matrix product state approach to quantum impurity models [201].

Renormalization algorithm for the calculation of spectra of interacting quantum systems [202].

Exploiting quantum parallelism to simulate quantum random many-body systems [203].

Engineered quantum critical points between matrix product states [204].

Theory of simulated emission by black holes [205].

Exactly solvable critical quantum models from classical spin models [206].

Theory of interferometry for nonabelian anyons [207].

Approximating ground states of spin systems with weighted graph states [208].

References Cited

- [1] S. Hallgren, Polynomial-time algorithms for Pell’s equation and the principal ideal problem, Proceedings of the 34th STOC (2002).
- [2] S. Hallgren, W. van Dam, and L. Ip, Quantum algorithms for hidden coset problems, Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA, 2003), arXiv: quant-ph/0211140.
- [3] Y. Shi, Quantum lower bounds for the collision and the element distinctness problems, Proceedings of the 43rd FOCS, pp. 513-519 (2002), arXiv: quant-ph/0112086.
- [4] S. Aaronson, Quantum lower bound for the collision problem, Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing (2002), arXiv: quant-ph/0111102.
- [5] M. Grigni, L. Schulman, M. Vazirani and U. Vazirani, Quantum mechanical algorithms for the nonabelian hidden subgroup problem, *Combinatorica* 24(1) (2004) 137-154, Proceedings of the 33rd STOC (2001).
- [6] C. Moore, D. Rockmore, A. Russell, and L. Schulman, The power of basis selection in Fourier sampling: hidden subgroup problems in affine groups, Proceedings of SODA (2004), arXiv: quant-ph/0211124, quant-ph/0503095.
- [7] C. Moore, A. Russell, and L. Schulman, The symmetric group defies strong Fourier sampling: Part I, arXiv: quant-ph/0501056 (2005).
- [8] D. Bacon, A. M. Childs, and W. van Dam, Optimal measurements for the dihedral hidden subgroup problem, arXiv: quant-ph/0501044 (2005).
- [9] D. Bacon, A. M. Childs, and W. van Dam, From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups, Proc. 46th IEEE Symposium on Foundations of Computer Science (FOCS 2005), pp. 469-478, arXiv: quant-ph/0504083.
- [10] A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics, Volume 47, American Mathematical Society (2002).

- [11] S. Bravyi, Efficient algorithm for a quantum analogue of 2-SAT, arXiv: quant-ph/0602108 (2006).
- [12] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous, One-dimensional quantum walks, Proceedings of the Thirty-Third Annual ACM Symposium on the Theory of Computing (2001).
- [13] A. Nayak and A. Vishwanath, Quantum walk on the line, arXiv: quant-ph/0010117.
- [14] L. Masanes, G. Vidal, and J. I. Latorre, Time-optimal Hamiltonian simulation and gate synthesis using homogeneous local unitaries, Quantum Information and Computation, Vol.2, No.4, 285-296 (2002), arXiv: quant-ph/0202042 (2002).
- [15] M. Freedman, A. Kitaev, and J. Lurie, Diameters of Homogeneous Spaces, Mathematical Research Letters, 10 (1), 11-20 (2003), arXiv: quant-ph/0209113.
- [16] A. M. Childs, D. Leung, and G. Vidal, Reversible simulation of bipartite product Hamiltonians, IEEE Trans. Inf. Theory Vol. 50, No. 6, 1189-1197 (2004), arXiv: quant-ph/0303097.
- [17] H. L. Haselgrove, M. A. Nielsen, and T. J. Osborne, On the practicality of time-optimal two-qubit Hamiltonian simulation, Phys. Rev. A 68, 042303 (2003), arXiv: quant-ph/0303070 (2003).
- [18] M. N. Vyalyi, QMA=PP implies that PP contains PH, Electronic Colloquium on Computational Complexity, TR03-21 (2003).
- [19] M. N. Vyalyi, Hardness of approximating the weight enumerator of a binary linear code, arXiv: cs.CC/0304044 (2003).
- [20] A. Childs and J. Goldstone, Spatial search and the Dirac equation, Phys. Rev. A 70, 042312 (2004), arXiv: quant-ph/0405120.
- [21] S. Bravyi and M. Vyalyi, Commutative version of the k-local Hamiltonian problem and non-triviality check for quantum codes, arXiv: quant-ph/0308021 (2003).
- [22] R. Cleve, P. Høyer, B. Toner, and J. Watrous, Consequences and limits of nonlocal strategies, Proceedings of the 19th IEEE Conference on Computational Complexity (CCC 2004), arXiv: quant-ph/0404076.
- [23] M. J. Bremner, J. L. Dodd, M. A. Nielsen, and D. Bacon, Fungible dynamics: There are only two types of entangling multiple-qubit interactions, Phys. Rev. A, 69, 012313 (2004), arXiv: quant-ph/0307148.

- [24] M. J. Bremner, M. A. Nielsen, and D. Bacon, Simulating Hamiltonian dynamics using many-qudit Hamiltonians and local unitary control, arXiv: quant-ph/0405115 (2004).
- [25] A.M. Childs, D. W. Leung, and M. A. Nielsen, Unified derivations of measurement-based schemes for quantum computation, Phys. Rev. A 71, 032318 (2005), arXiv: quant-ph/0404132.
- [26] D. W. Leung, Quantum computation by measurements, Int. Jour. Quant. Inf. 2, No. 1, 33-43 (2004), arXiv: quant-ph/0310189.
- [27] P. Aliferis and D. W. Leung, Computation by measurements: a unifying picture, Phys. Rev. A 70, 062314 (2004), arXiv: quant-ph/0404082.
- [28] G. Vidal and C. M. Dawson, A universal quantum circuit for two-qubit transformations with three CNOT gates, Phys. Rev. A 69, 010301 (2004), arXiv: quant-ph/0307177.
- [29] J. Kempe, A. Kitaev, and O. Regev, The complexity of the local Hamiltonian problem, SIAM Journal of Computing, Vol. 35(5), 1070-1097 (2006), arXiv: quant-ph/0406180.
- [30] D. Bacon, I. Chuang, A. Harrow, Efficient quantum circuits for Schur and Clebsch-Gordon transforms, arXiv: quant-ph/0407082 (2004).
- [31] R. Raussendorf, A quantum cellular automaton for universal quantum computation, arXiv: quant-ph/0412048 (2004).
- [32] L. Duan and R. Raussendorf, Efficient quantum computation with probabilistic quantum gates, Phys. Rev. Lett. 95, 080503 (2005), arXiv: quant-ph/0502120.
- [33] R. Raussendorf, Quantum computation via translation-invariant operations on a chain of qubits, Phys. Rev. A 72, 052301 (2005), arXiv: quant-ph/0505122.
- [34] C. Mochon, A family of generalized ‘pretty good’ measurements and the minimal-error pure-state discrimination problems for which they are optimal, arXiv: quant-ph/0506061 (2005).
- [35] A. Childs and W. van Dam, Quantum algorithm for a generalized hidden shift problem, arXiv: quant-ph/0507190 (2005).
- [36] A. Childs and P. Wocjan, On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems, arXiv: quant-ph/0510185 (2005).
- [37] L. Schulman, T. Mor, and Y. Weinstein, Physical limits of heat-bath algorithmic cooling, Physical Review Letters 94, 120501 (2005).
- [38] J. Yard and P. Wocjan, The Jones polynomial: quantum algorithms and applications in quantum complexity theory, arXiv: quant-ph/0603069 (2006).

- [39] D. Gottesman and J. Preskill, Secure quantum key distribution using squeezed states, *Phys. Rev. A* 63 (2001) 022309, arXiv: quant-ph/0008046.
- [40] M. Koashi and J. Preskill, Secure quantum key distribution with an uncharacterized source, *Phys. Rev. Lett.* 90 (2003) 057902, arXiv: quant-ph/0208155.
- [41] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, *Quant. Inf. Comp.* 4, 325-360 (2004), arXiv: quant-ph/0212066 (2002).
- [42] A. Kitaev, Any quantum coin tossing protocol is susceptible to same-sided bias, unpublished (2002); see A. Ambainis, H. Buhrman, Y. Dodis, and H. Roehrig, Multiparty quantum coin flipping, arXiv: quant-ph/0304112 (2003).
- [43] C. Mochon, Quantum weak coin-flipping with bias of 0.192, Proceedings of the 45th Symposium on Foundations of Computer Science (FOCS 2004) arXiv: quant-ph/0403193.
- [44] C. Mochon, A large family of quantum weak coin-flipping protocols, *Phys. Rev. A* 72, 022341 (2005), arXiv: quant-ph/0502068.
- [45] C. Mochon, Serial composition of quantum coin-flipping, and bounds on cheat detection for bit-commitment, *Phys. Rev. A* 70, 032312 (2004), arXiv: quant-ph/0311165.
- [46] M. Ben-Or and D. Mayers, General security definition and composability for quantum and classical protocols, arXiv: quant-ph/0409062 (2004)
- [47] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim, The universal composable security of quantum key distribution, *Lecture Notes in Computer Science*, vol 3378, 386-406 (2005), arXiv: quant-ph/0409078.
- [48] P. Hayden, D. Leung, P. Shor and A. Winter, Randomizing quantum states: Constructions and applications, *Commun. Math. Phys.* 250(2):371-391 (2004), arXiv: quant-ph/0307104
- [49] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Locking classical correlation in quantum states, *Phys. Rev. Lett.* 92, 067902 (2004), arXiv: quant-ph/0303088 (2003).
Comm. Math. Phys., accepted (2004), arXiv: quant-ph/030710.
- [50] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman, Interaction in quantum communication and the complexity of Set Disjointness, Proceedings of the Thirty-Third Annual ACM Symposium on the Theory of Computing (2001), arXiv: quant-ph/0005106 and quant-ph/0004100.
- [51] S. Daftuar and M. Klimesh, Mathematical structure of entanglement catalysis, *Phys. Rev. A* 64, 042314 (2001) , arXiv: quant-ph/0104058.

- [52] A. Nayak and J. Salzman, On communication over an entanglement-assisted quantum channel, Proceedings of the Thirty-Fourth Annual ACM Symposium on the Theory of Computing (2002).
- [53] D. P. DiVincenzo, P. Hayden and B. M. Terhal, Hiding quantum data, Found. Phys. 33(11):1629-1647 (2003), arXiv: quant-ph/0207147.
- [54] S. Bose, Quantum communication through an unmodulated spin chain, arXiv: quant-ph/0212041 (2002).
- [55] J. A. Cortese, Relative entropy and single qubit Holevo-Schumacher-Westmoreland channel capacity, arXiv: quant-ph/0207128 (2002).
- [56] J. A. Cortese, The Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels, arXiv: quant-ph/0211093 (2002).
- [57] C. Crépeau, P. Dumais, D. Mayers and L. Salvail, Computational collapse of quantum state with application to oblivious transfer, in Proceedings of First Theory of Cryptography Conference, Lecture Notes in Computer Science 2951, February 2004.
- [58] D. Mayers and A. Yao, Self testing quantum apparatus, Quant. Inf. Comp.4(4), 273-286 (2004), arXiv: quant-ph/0307205 (2003).
- [59] A. Harrow, P. Hayden and D. Leung, Superdense coding of quantum states, Phys. Rev. Lett. 92, 187901 (2004), arXiv: quant-ph/0307221.
- [60] A. Abeyesinghe, P. Hayden, G. Smith, and A. Winter, Optimal superdense coding of entangled states, arXiv: quant-ph/0407061 (2004).
- [61] C. Bennett, P. Hayden, D. Leung, P. Shor and A. Winter, Remote preparation of quantum states, IEEE Trans. Inf. Theory, accepted (2004), arXiv: quant-ph/0307100.
- [62] A. Abeyesinghe and P. Hayden, Generalized remote state preparation: Trading qubits and ebits in quantum communication, Phys. Rev. A 68:062319 (2003), arXiv: quant-ph/0308143.
- [63] Charlene Ahn, Andrew Doherty, Patrick Hayden and Andreas Winter, On the distributed compression of quantum information, arXiv: quant-ph/0403042.
- [64] P. Hayden, D. Leung, and G. Smith, Multiparty data hiding of quantum information, Phys. Rev. A 71, 062339 (2005), arXiv: quant-ph/0407152.
- [65] C. H. Bennett, A. W. Harrow, D. W. Leung, J. A. Smolin, On the capacities of bipartite Hamiltonians and unitary gates, IEEE Trans. Inf. Theory, Vol. 49, No. 8, 1895-1911 (2003), arXiv: quant-ph/0205057.

- [66] M.-H. Yung, D. W. Leung, Sougato Bose, An exact effective two-qubit gate in a chain of three spins, *Quantum Information and Computation* 4, 174 (2004), arXiv: quant-ph/0312105(2003).
- [67] S. Bravyi, Lagrangian representation for fermionic linear optics, *Quantum Inf. and Comp.*, Vol. 5, No. 3, 216-238 (2005), arXiv: quant-ph/0404180.
- [68] S. van Enk, Reference frames and rebits, *Phys. Rev. A* 71, 032339 (2005), arXiv: quant-ph/0410083.
- [69] A. Harrow and D. Leung, Bidirectional coherent classical communication, *Quantum Information and Computation*, vol. 5, no. 4-5, 380-395 (2005), arXiv: quant-ph/0412126.
- [70] J. Yard, I. Devetak, and P. Hayden, Capacity theorems for quantum multiple access channels - Part I: Classical-quantum and quantum-quantum capacity regions, arXiv: quant-ph/0501045 (2005).
- [71] H.-K. Lo and J. Preskill, Phase randomization improves the security of quantum key distribution, arXiv: quant-ph/0504209 (2005).
- [72] A. M. Childs, D. Leung, and H.-K. Lo, Two-way quantum communication channels, *International Journal of Quantum Information*, Vol. 4, No. 1, 63-83 (2006), arXiv: quant-ph/0506039.
- [73] S. Bravyi, Classical capacity of fermionic product channels, arXiv: quant-ph/0507282 (2005).
- [74] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Quantum key distribution based on arbitrarily-weak distillable entangled states, *Phys. Rev. Lett.* 96, 070501 (2006), arXiv: quant-ph/0510067.
- [75] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Distinguishing separable and entangled states, *Phys. Rev. Lett.* 88, 187904 (2002), arXiv: quant-ph/0112007.
- [76] A. Doherty, P. Parrilo, and F. Spedalieri, A complete family of separability criteria, *Phys. Rev. A* 69 (2004) 022308, arXiv: quant-ph/0308032.
- [77] 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).
- [78] F. Spedalieri, Characterizing entanglement in quantum information, Caltech Ph.D. thesis, June 2003, 108 pages.
- [79] D. Bacon and B. F. Toner, Bell inequalities with auxiliary communication, *Phys. Rev. Lett.* 90, 157904 (2003), arXiv: quant-ph/0207147.

- [80] D. Bacon and B. F. Toner, The communication cost of simulating bell correlations, *Phys. Rev. Lett.* 91, 187904 (2003), arXiv: quant-ph/0304076.
- [81] 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), arXiv: quant-ph/0210117.
- [82] M. Popp, F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Localizable entanglement, *Phys. Rev. A* 71, 042306 (2005), arXiv: quant-ph/0411123.
- [83] B. Toner, Monogamy of nonlocal quantum correlations, arXiv: quant-ph/0601172 (2006).
- [84] P. Hayden, R. Jozsa, and A. Winter, Trading quantum for classical resources in quantum data compression, *J. Math. Phys.* 43, 4404-4444 (2002), arXiv: quant-ph/0204038 (2002).
- [85] W. van Dam and P. Hayden, Embezzling entangled quantum states, *Phys. Rev. A* 67, 060302(R) (2003), arXiv: quant-ph/0201041 (2002).
- [86] P. Hayden and A. Winter, On the communication cost of entanglement transformations, *Phys. Rev. A* 67, 012326 (2003), arXiv: quant-ph/0204092 (2002).
- [87] B. M. Terhal, M. Horodecki, D. W. Leung, D. P. DiVincenzo, The entanglement of purification, *J. Math. Phys.* 43, 4286-4298 (2002), arXiv: quant-ph/0202044 (2002).
- [88] W. van Dam and P. Hayden Renyi-entropic bounds on quantum communication, arXiv: quant-ph/0204093 (2002).
- [89] A. Acin, G. Vidal, J. I. Cirac, On the structure of a reversible entanglement generating set for three-partite states, *Quant. Inf. Comp.* 3, 55 (2003), arXiv: quant-ph/0202056 (2002).
- [90] B. M. Terhal, M. M. Wolf and A. C. Doherty, Quantum entanglement: A modern perspective, *Physics Today*, April 2003.
- [91] B. M. Terhal, A. C. Doherty, D. Schwab, Local hidden variable theories for quantum states, *Phys. Rev. Lett.* 90 157903 (2003), arXiv: quant-ph/0210053.
- [92] S. Bravyi, Requirements for compatibility between local and multipartite quantum states, arXiv: quant-ph/0301014 (2003).
- [93] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Structure of states which satisfy strong sub-additivity of quantum entropy with equality, *Commun. Math. Phys.*, 246(2), 359-374 (2004), arXiv: quant-ph/0304007.

- [94] P. Hayden, D. Leung and A. Winter, P. Hayden, Debbie W. Leung, and Andreas Winter, Aspects of generic entanglement, *Comm. Math. Phys.* March 2006, arXiv: quant-ph/0407049.
- [95] S. Bravyi, Requirements for compatibility between local and multipartite quantum states, *Quantum Information Computation*, 4 (1), 12 (2004), arXiv: quant-ph/0301014.
- [96] S. Bravyi, Unextendible product bases and locally unconvertible bound entangled states, arXiv: quant-ph/0310172 (2003).
- [97] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, Entanglement in the stabilizer formalism, arXiv: quant-ph/0406168 (2004).
- [98] B. Schumacher and M. Westmoreland, Locality and information transfer in quantum operations arXiv: quant-ph/0406223 (2004).
- [99] R. Raussendorf, S. Bravyi, and J. Harrington, Long-range quantum entanglement in noisy cluster states, *Phys. Rev. A* 71, 062313 (2005), arXiv: quant-ph/0407255.
- [100] A. Klyachko, Quantum marginal problem and representations of the symmetric group, arXiv: quant-ph/0409113 (2004).
- [101] P. Hayden, Entanglement in random subspaces, arXiv: quant-ph/0409157 (2004).
- [102] S. Daftuar and P. Hayden, Quantum state transformations and the Schubert calculus, *Ann. Phys.* 315, 80-122 (2005), arXiv: quant-ph/0410052.
- [103] M. Aschbacher, A. Childs, and P. Wocjan, The limitations of nice mutually unbiased bases, arXiv: quant-ph/0412066 (2004).
- [104] Steven van Enk and O. Hirota, The most robust entangled state of light, *Phys. Rev. A* 71, 062322 (2005), arXiv: quant-ph/0412221.
- [105] A. Azarchs, Entropic uncertainty relations for incomplete sets of mutually unbiased observables, arXiv: quant-ph/0412083 (2004).
- [106] C. Schoen, E. Solano, F. Verstraete, I. Cirac, and M. Wolf, Sequential generation of entangled multi-qubit states, *Phys. Rev. Lett.* 95, 110503 (2005), arXiv: quant-ph/0501096.
- [107] P. Wocjan, On the maximal number of real mutually unbiased bases, arXiv: quant-ph/0502024 (2005).
- [108] P. Wocjan and M. Horodecki, Characterization of combinatorically independent permutation separability criteria, *Open Syst. Inf. Dyn.* 12, 331 (2005), arXiv: quant-ph/0503129.

- [109] Lieven Clarisse and Pawel Wocjan, Further results on independent permutation separability criteria, *Quantum Information and Computation*, Vol. 6, No. 3, 277-288 (2006), arXiv: quant-ph/0504160.
- [110] S. Pironio, Lifting Bell inequalities, *J. Math. Phys.* 46, 062112 (2005), arXiv: quant-ph/0503179.
- [111] T. J. Osborne and F. Verstraete, General monogamy inequality for bipartite qubit entanglement, arXiv: quant-ph/0502176 (2005).
- [112] S. Bravyi, D. Fattal, and D. Gottesman, GHZ extraction yield for multipartite stabilizer states, arXiv: quant-ph/0504208 (2005).
- [113] R. Blume-Kohout and W. H. Zurek, Quantum Darwinism: Entanglement, branches, and the emergent classicality of redundantly stored quantum information, arXiv: quant-ph/0505031 (2005).
- [114] J. A. Smolin, F. Verstraete, and A. Winter, Entanglement of assistance and multipartite state distillation, *Phys. Rev. A* 72, 052317 (2005), arXiv: quant-ph/0505038.
- [115] P. Oscar Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, arXiv: quant-ph/0506089 (2005).
- [116] J. Barrett and S. Pironio, Popescu-Rohrlich correlations as a unit of nonlocality, *Phys. Rev. Lett.* 95, 140401 (2005), arXiv: quant-ph/0506180.
- [117] L. Schulman and L. Schulman, Wave packet scattering without kinematic entanglement: Convergence of expectation values, *IEEE Transactions on Nanotechnology* 4(1):8-13 (2005).
- [118] G. Smith and D. Leung, Typical entanglement of stabilizer states, arXiv: quant-ph/0510232 (2005).
- [119] M. Hein, W. Dr, Jens Eisert, Robert Raussendorf, M. Van den Nest, and H. Briegel, Entanglement in graph states and its applications, arXiv: quant-ph/0602096 (2006).
- [120] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, *Phys. Rev. A* 64 (2001) 012310, arXiv: quant-ph/0008040.
- [121] B. Rahn, A. C. Doherty, and H. Mabuchi, Exact and approximate performance of concatenated quantum codes, *Phys. Rev. A* 66, 032304 (2002), arXiv: quant-ph/0111003.
- [122] E. Dennis, D. Gottesman, A. Kitaev, and J. Preskill, Topological quantum memory, *J. Math. Phys.*, 43 (2002) 4452-4505, arXiv: quant-ph/0110143.

- [123] 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), arXiv: quant-ph/0207088.
- [124] A. Kitaev, Anyons in an exactly solved model and beyond, *Ann. Phys.* 321, 2-111 (2006), arXiv: cond-mat/0506438.
- [125] C. Mochon, Anyons from non-solvable discrete groups are sufficient for universal quantum computation, *Phys. Rev. A* 67 (2003) 022315, arXiv: quant-ph/0206128.
- [126] C. Mochon, Anyon computers with smaller groups, *Phys. Rev. A* 69, 032306 (2004), arXiv: quant-ph/0306063.
- [127] C. Ahn, A. C. Doherty, A. J. Landahl, Continuous quantum error correction via quantum feedback control, *Phys. Rev. A* 65, 042301 (2002), arXiv: quant-ph/0110111.
- [128] C. Ahn, H. W. Wiseman, and G. J. Milburn, Quantum error correction for continuously detected errors, *Phys. Rev. A* 67, 052310 (2003), arXiv: quant-ph/0302006.
- [129] C. Ahn, H. Wiseman, K. Jacobs, Quantum error correction for continuously detected errors with any number of error channels per qubit, *Phys. Rev. A* 70, 024302 (2004), arXiv: quant-ph/0402067.
- [130] M. Sarovar, C. Ahn, K. Jacobs, G. J. Milburn, Practical scheme for error control using feedback, *Phys. Rev. A* 69, 052324 (2004), arXiv: quant-ph/0402017.
- [131] S. Bravyi and A. Kitaev, Universal quantum computation based on magic states distillation, *Phys. Rev. A* 71, 022316 (2005), arXiv: quant-ph/0403025.
- [132] S. Bravyi, Universal quantum computation with the $\nu=5/2$ Fractional Quantum Hall State, *Phys. Rev. A* 73, 042313 (2006), arXiv: quant-ph/0511178.
- [133] P. Aliferis, D. Gottesman, and J. Preskill, Quantum accuracy threshold for concatenated distance-3 codes, *Quant. Inf. Comput.* 6, 97-165 (2006), arXiv: quant-ph/0504218.
- [134] D. Aharonov, A. Kitaev, and J. Preskill, Fault-tolerant quantum computation with long-range correlated noise, *Phys. Rev. Lett.* 96, 050504 (2006), arXiv: quant-ph/0510231.
- [135] P. Aliferis and B. M. Terhal Fault-tolerant quantum computation for local leakage faults, arXiv: quant-ph/0511065 (2005).
- [136] R. Raussendorf, J. Harrington, and K. Goyal, A fault-tolerant one-way quantum computer, arXiv: quant-ph/0510135 (2005).

- [137] P. Aliferis and D. Leung, Simple proof of fault tolerance in the graph-state model, *Phys. Rev. A* 73, 032308 (2006), arXiv: quant-ph/0503130.
- [138] J. Harrington and J. Preskill, Achievable rates for the Gaussian quantum channel, *Phys. Rev. A* 64, 062301 (2001), arXiv: quant-ph/0105058.
- [139] A. C. Doherty, J. C. Doyle, H. Mabuchi, K. Jacobs, and S. Habib, Robust control in the quantum domain, to appear in Proceedings of the 39th IEEE Conference on Decision and Control (2001), arXiv: quant-ph/0105018.
- [140] A. M. Childs, E. Farhi, and J. Preskill, Robustness of adiabatic quantum computation, *Phys. Rev. A* 65, 012322 (2002), arXiv: quant-ph/0108048.
- [141] C. Ahn, Extending quantum error correction: new continuous measurement protocols and improved fault-tolerant overhead, Caltech Ph.D. thesis (2004).
- [142] J. Harrington, Analysis of quantum error-correcting codes: symplectic lattice codes and toric codes, Caltech Ph.D. thesis (2004).
- [143] P. Hayden and C. King, Correcting quantum channels by measuring the environment, arXiv: quant-ph/0409026 (2004).
- [144] M. Roetteler and P. Wocjan, Equivalence of decoupling schemes and orthogonal arrays, arXiv: quant-ph/0409135 (2004).
- [145] P. Wocjan, Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays, arXiv: quant-ph/0410107 (2004).
- [146] L. Bouten and R. van Handel, On the separation principle of quantum control, arXiv: math-ph/0511021 (2005).
- [147] S. Habib, T. Bhattacharya, A. Doherty, B. Greenbaum, A. Hopkins, K. Jacobs, H. Mabuchi, K. Schwab, K. Shizume, D. Steck, and B. Sundaram, Nonlinear quantum dynamics, arXiv: quant-ph/0505046 (2005).
- [148] Luc Bouten and Ramon van Handel, Quantum filtering: a reference probability approach, arXiv: math-ph/0508006 (2005).
- [149] L. Bouten, R. van Handel, and M. James, An introduction to quantum filtering, arXiv: math.OA/0601741 (2006).
- [150] B. Janssens and L. Bouten, Optimal pointers for joint measurement of sigma-x and sigma-z via homodyne detection, *J. Phys. A: Math. Gen.* 39, 2773-2790 (2006), arXiv: quant-ph/0510086 (2005).

- [151] R. van Handel and H. Mabuchi, Optimal error tracking via quantum coding and continuous syndrome measurement, arXiv: quant-ph/0511221 (2005).
- [152] L.-M. Duan, Entangling many atomic ensembles through laser manipulation, Phys. Rev. Lett. 88, 170402 (2002), arXiv: quant-ph/0201128.
- [153] L.-M. Duan, E. Demler, M. Lukin, Controlling spin exchange interactions of ultracold atoms in optical lattices, Phys. Rev. Lett. 91, 090402 (2003), arXiv: cond-mat/021056 (2002).
- [154] L.-M. Duan and H. J. Kimble, Scalable photonic quantum computation through cavity-assisted interactions, Phys. Rev. Lett. 92, 127902 (2004), arXiv: quant-ph/0309187.
- [155] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, Quantum versus classical domain for teleportation with continuous variables, Phys. Rev. A 64, 022321 (2001), arXiv: quant-ph/0012001.
- [156] F. Verstraete, A. C. Doherty, and H. Mabuchi, Sensitivity optimization in quantum parameter estimation, Phys. Rev. A 64, 032111 (2001), arXiv: quant-ph/0104116.
- [157] A. C. Doherty, T. W. Lynn, C. J. Hood, and H. J. Kimble, Trapping of single atoms with single photons in cavity QED, Phys. Rev. A 63 (2001) 013401, arXiv: quant-ph/0006015.
- [158] M. A. Armen, J. K. Au, J. K. Stockton, A. C. Doherty, H. Mabuchi, Adaptive homodyne measurement of optical phase, arXiv: quant-ph/0204005 (2002).
- [159] V. B. Braginsky, M. L. Gorodetsky, F. Ya. Khalili, A. B. Matsko, K. S. Thorne, and S. P. Vyatchanin, The noise in gravitational-wave detectors and other classical-force measurements is not influenced by test-mass quantization, Phys. Rev. D 67, 082001 (2003), arXiv: gr-qc/0109003.
- [160] L.-M. Duan, J. I. Cirac, and P. Zoller, Three-dimensional theory for interaction between atomic ensembles and free-space light, Phys. Rev. A 66, 023818 (2002), arXiv: quant-ph/0205005 (2002).
- [161] JM Geremia, J. Williams and H. Mabuchi, An inverse problem approach to designing photonic crystals for cavity QED, arXiv: quant-ph/0206094 (2002).
- [162] 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), arXiv: quant-ph/0207011.
- [163] L.-M. Duan, H. J. Kimble, Efficient engineering of multi-atom entanglement through single-photon detections, Phys. Rev. Lett. 90, 253601 (2003), arXiv: quant-ph/0301164.
- [164] 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), arXiv: quant-ph/0208051.

- [165] S. C. Benjamin and S. Bose, Quantum computing in arrays coupled by "always-on" interactions, *Phys. Rev. A* 70, 032314 (2004), arXiv: quant-ph/0210157.
- [166] 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, *Nature*, 3 March (2003), arXiv: quant-ph/0305162.
- [167] 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), arXiv: quant-ph/0207076.
- [168] J. McKeever, A. Boca, A. D. Boozer, J. R. Buck, and H. J. Kimble, A One-atom laser in a regime of strong coupling, *Nature* 425, 268-271 (2003), arXiv: quant-ph/0309199.
- [169] A. D. Boozer, A. Boca, J. R. Buck, J. McKeever, and H. J. Kimble, Comparison of theory and experiment for a one-atom laser in a regime of strong coupling, arXiv: quant-ph/0309133 (2003).
- [170] C. W. Chou, S. V. Polyakov, A. Kuzmich, and H. J. Kimble, Single-photon generation from stored excitation in an atomic ensemble, arXiv: quant-ph/0401147 (2004).
- [171] JM Geremia, J. K. Stockton, and H. Mabuchi, Real-time quantum feedback control of atomic spin-squeezing, *Science* 304, 270 (2004).
- [172] R. van Handel, J. K. Stockton, and H. Mabuchi, Feedback control of quantum state reduction, arXiv: quant-ph/0402136 (2004).
- [173] J. K. Stockton, R. van Handel, and H. Mabuchi, Deterministic Dicke state preparation with continuous measurement and control, arXiv: quant-ph/0402137 (2004).
- [174] L. Duan, B. Wang, and H. J. Kimble, Robust quantum gates on neutral atoms with cavity-assisted photon-scattering, *Phys. Rev. A* 72, 032333 (2005), arXiv: quant-ph/0505054.
- [175] T. Lynn, K. Birnbaum, and H. J. Kimble, Strategies for real-time position control of a single atom in cavity QED, arXiv: quant-ph/0507064 (2005).
- [176] K. Birnbaum, A. Boca, R. Miller, D. Boozer, T. Northup, and H. J. Kimble, Theory of photon blockade by an optical cavity with one trapped atom, arXiv: quant-ph/0507065 (2005).
- [177] D. Steck, K. Jacobs, H. Mabuchi, S. Habib, and T. Bhattacharya, Feedback cooling of atomic motion in cavity QED, arXiv: quant-ph/0509039 (2005).
- [178] C.-W. Chou, H. de Riedmatten, D. Felinto, S. Polyakov, S. J. van Enk, and H. Jeff Kimble, Measurement-induced entanglement for excitation stored in remote atomic ensembles, arXiv: quant-ph/0510055 (2005).

- [179] M. A. Armen, H. Mabuchi, Low-lying bifurcations in cavity quantum electrodynamics. arXiv: quant-ph/0602170 (2006).
- [180] J. Laurat, H. de Riedmatten, D. Felinto, C.-W. Chou, E. Schomburg, H. J. Kimble, Efficient retrieval of a single excitation stored in an atomic ensemble, arXiv:quant-ph/0605122 (2006).
- [181] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, Phys. Rev. Lett. 91, 147902 (2003), arXiv: quant-ph/0301063.
- [182] G. Vidal, Efficient simulation of one-dimensional quantum many-body systems, Phys. Rev. Lett. 93, 040502 (2004), arXiv: quant-ph/0310089 (2003).
- [183] A. J. Daley, C. Kollath, U. Schollwoeck, and G. Vidal, Time-dependent density-matrix renormalization-group using adaptive effective Hilbert spaces, J. Stat. Mech.: Theor. Exp. P04005 (2004), arXiv: cond-mat/0403313.
- [184] F. Verstraete and J. I. Cirac, Matrix product states represent ground states faithfully, arXiv: cond-mat/0505140 (2005).
- [185] F. Verstraete and I. Cirac, Mapping local Hamiltonians of fermions to local Hamiltonians of spins, J. Stat. Mech. P09012 (2005), arXiv: cond-mat/0508353.
- [186] G. Vidal, J.I. Latorre, E. Rico and A. Kitaev, Entanglement in quantum critical phenomena, Phys. Rev. Lett. 90, 227902 (2003), arXiv: quant-ph/0211074.
- [187] J. I. Latorre, E. Rico, and G. Vidal, Ground state entanglement in quantum spin chains, Quant. Inf. and Comp. 4 (1), 048-092 (2004), arXiv: quant-ph/0304098.
- [188] J.I. Latorre, C.A. Lutken, E. Rico, and G. Vidal, Fine-grained entanglement loss along renormalization group flows, Phys.Rev. A71, 034301 (2005), arXiv: quant-ph/0404120.
- [189] G. Vidal, Entanglement renormalization, arXiv: cond-mat/0512165 (2005).
- [190] A. Kitaev and J. Preskill, Topological entanglement entropy, Phys. Rev. Lett. 96, 110404 (2006), arXiv: hep-th/0510092.
- [191] P. Bonderson, A. Kitaev, and K. Shtengel, Detecting non-Abelian statistics in the $\nu=5/2$ Fractional Quantum Hall State, Phys. Rev. Lett. 96, 016803 (2006), arXiv: cond-mat/0508616.
- [192] A. Kitaev, D. Mayers, and J. Preskill, Superselection rules and quantum protocols, Phys. Rev. A 69, 052326 (2004), arXiv: quant-ph/0310088.
- [193] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, Causal and localizable quantum operations, Phys. Rev. A 64, 052309 (2001), arXiv: quant-ph/0102043.

- [194] D. Beckman, D. Gottesman, A. Kitaev, and J. Preskill, Measurability of Wilson loop operators, *Phys. Rev. D* 65, 065022 (2002), arXiv: hep-th/0110205.
- [195] H. L. Haselgrove, M. A. Nielsen, T. J. Osborne, Quantum states far from the energy eigenstates of any local Hamiltonian, *Phys. Rev. Lett.* 91, 210401 (2003), arXiv: quant-ph/0303022 (2003).
- [196] D. Bacon, Quantum Computational Complexity in the Presence of Closed Timelike Curves, arXiv: quant-ph/0309189 (2003).
- [197] D. Gottesman and J. Preskill, Comment on “The black hole final state,” *JHEP* 0403, 026 (2004), arXiv: hep-th/0311269.
- [198] M. Zwolak and G. Vidal, Mixed-state dynamics in one-dimensional quantum lattice systems: a time-dependent superoperator renormalization algorithm, *Phys. Rev. Lett.* 93, 207205 (2004), arXiv: cond-mat/0406440.
- [199] A. Hutton and S. Bose, Ground state entanglement in a combination of star and ring geometries of interacting spins, arXiv: quant-ph/0408077 (2004).
- [200] V. Murg, F. Verstraete, and I. Cirac, Efficient evaluation of partition functions of frustrated and inhomogeneous spin systems, *Phys. Rev. Lett.* 95, 057206 (2005), arXiv: cond-mat/0501493.
- [201] F. Verstraete, A. Weichselbaum, U. Schollwöck, J. I. Cirac, J. von Delft, Variational matrix product state approach to quantum impurity models, arXiv: cond-mat/0504305 (2005).
- [202] D. Porras, F. Verstraete, and J. I. Cirac, Renormalization algorithm for the calculation of spectra of interacting quantum systems, arXiv: cond-mat/0504717 (2005).
- [203] B. Paredes, F. Verstraete, and J. I. Cirac, Exploiting quantum parallelism to simulate quantum random many-body systems, arXiv: cond-mat/0505288 (2005).
- [204] M. Wolf, G. Ortiz, F. Verstraete, and J. I. Cirac, Quantum phase transitions in matrix product systems, arXiv: cond-mat/0512180 (2005).
- [205] C. Adami and G. L. Ver Steeg, Black holes are almost optimal quantum cloners, arXiv: quant-ph/0601065 (2006).
- [206] F. Verstraete, M. Wolf, D. Perez-Garcia, and J. I. Cirac, Criticality, the area law, and the computational power of PEPS, arXiv: quant-ph/0601075 (2006).
- [207] P. Bonderson, K. Shtengel, and J. K. Slingerland, Probing non-Abelian statistics with two-particle interferometry, arXiv: cond-mat/0601242 (2006).

- [208] S. Anders, M. Plenio, W. Dr, F. Verstraete, and H. Briegel, Ground state approximation for strongly interacting systems in arbitrary dimension, arXiv: quant-ph/0602230 (2006).