

# Institute for Quantum Information

## Findings – 2004-05

Quantum information science is an exciting emerging field that addresses how fundamental physical laws can be harnessed to dramatically improve the acquisition, transmission, and processing of information. The primary goal of the Institute for Quantum Information (IQI) is to carry out and facilitate research in quantum information science. Our research covers six broad areas: (1) Quantum algorithms that achieve speedups relative to classical algorithms, and limits on such algorithms. (2) Quantum cryptographic protocols, and other types of communication using quantum states. (3) Quantum entanglement and the theory of transformations among quantum states. (4) Protection of quantum information using quantum error correcting codes and fault tolerant protocols for quantum information processing. (5) Theory and practice regarding physical implementations of quantum information processing. (6) Connections between quantum information science and other aspects of fundamental physics.

In the period from 1 June 2004 to 31 August 2005, IQI participants produced 59 publications, which we summarize here.

### Quantum algorithms and quantum complexity

**QMA-completeness of 2-local Hamiltonian problem.** Alexei Kitaev, with Kempe and Regev, showed that the 2-local Hamiltonian problem is QMA-complete [1]. QMA is the quantum analogue of the classical complexity class NP, and the complete problem is finding the ground state energy of a Hamiltonian that can be expressed as a sum of terms where each term acts on a pair of qubits. The proof used a powerful perturbative method for analyzing the sum of two Hamiltonians.

**Efficient quantum circuits for Schur and Clebsch-Gordon transforms.** Dave Bacon, with Chuang and Harrow, found efficient quantum circuits that evaluate the Schur transform [2]. The Schur transform is useful for exploiting symmetry under permutations or collective unitary rotations.

**Quantum cellular automaton for universal quantum computation.** Robert Raussendorf described a quantum cellular automaton capable of performing universal quantum computation [3]. The automaton has an elementary transition function that acts on Margolus cells of  $2 \times 2$  qubits, and both the “quantum input” and the program are encoded in the initial state of the system.

**Optimal measurements for the dihedral hidden subgroup problem.** Dave Bacon and Andrew Childs, with van Dam, showed that the optimal measurement for solving the dihedral hidden subgroup problem is the “pretty good measurement” [4]. They proved that the success probability of this measurement is of order one if the number of hidden subgroup states is  $\nu \log N$  where  $\nu > 1$  and  $2N$  is the order of the hidden subgroup, while the success probability is exponentially small in  $\log N$  for  $\nu < 1$ .

**The symmetric group defies strong Fourier sampling.** Leonard Schulman, with Moore and Russell, showed that the hidden subgroup problem over the symmetric group cannot be efficiently solved by strong Fourier sampling, even if one may perform an arbitrary POVM on a single copy of the coset state [5]. Their results apply in particular to the special case relevant to the Graph Isomorphism problem.

**Efficient quantum computation with probabilistic quantum gates.** Robert Raussendorf, with Duan, showed that efficient quantum computation can be constructed even if all the entangling quantum gates only succeed with an arbitrarily small probability  $p$  [6]. The required computational overhead scales efficiently both with  $1/p$  and  $n$ , where  $n$  is the number of qubits in the computation.

**Efficient quantum algorithms for the hidden subgroup problem over semidirect product groups.** Dave Bacon and Andrew Childs, with van Dam, showed that, for various groups that can be expressed as the semidirect product of an abelian group and a cyclic group, the hidden subgroup problem can be solved using a pretty good measurement [7]. Their results show that entangled measurements across multiple copies of hidden subgroup states can be useful for efficiently solving the nonabelian hidden subgroup problem.

**Quantum computation via translation-invariant operations on a chain of qubits.** Robert Raussendorf described a scheme for universal quantum computation on a chain of qubits that does not require local control [8]. All the required operations, an Ising-type interaction and spatially uniform simultaneous one-qubit gates, are translation-invariant.

**Optimal measurements for state identification.** Carlos Mochon found the optimal measurement for estimating a pure state chosen from an ensemble [9]: it is a “pretty good measurement,” but derived from an ensemble with different a priori probabilities than the ensemble from which the pure state is selected.

**Quantum algorithm for a generalized hidden shift problem.** Andrew Childs, with van Dam, found an efficient quantum algorithm for a family of hidden shift problems [10]. The algorithm is based on the pretty good measurement and uses Lenstra’s classical algorithm for integer programming as a subroutine.

## Quantum communication and quantum cryptography

General security definition and composability for quantum and classical protocols.

Dominic Mayers, with Ben-Or, generalized the theory of universal composability to the quantum world [11]. A composable secure quantum protocol can be safely used as a sub-protocol in a larger protocol that performs a cryptographic task.

**Universal composable security of quantum key distribution.** Debbie Leung and Dominic Mayers, with Ben-Or, Horodecki, and Oppenheim, proved a universal composability theorem for quantum key distribution [12]. This means that the key generated in the protocol can be used in subsequent protocols, for example to authenticate further rounds of key distribution.

**Correcting quantum channels by measuring the environment.** Patrick Hayden, with King, studied the “corrected capacity” of quantum channels — the best one-shot capacity that can be obtained by measuring the environment and using the result to correct the output of the channel [13]. They showed that all qubit channels have corrected capacity  $\log 2$ , and that a product of  $N$  qubit channels has the corrected capacity  $N \log 2$ .

**The number of “refbits” needed to achieve communication tasks.** Steven van Enk defined the “refbit,” which quantifies the resource of sharing a reference frame in quantum communication protocols [14]. Considering both asymptotic and nonasymptotic protocols, he found relations between refbits and other communication resources.

**Tradeoff between forward and backward coherent classical communication.** Debbie Leung, with Harrow, studied the communication capacities of a bipartite unitary interaction [15]. They related the forward-back tradeoff curve for two-way coherent communication to the tradeoffs for two-way classical and quantum communication, and also studied the tradeoff for coherent communication in one direction and quantum communication in the other.

**Capacity theorems for quantum multiple access channels.** Jon Yard, with Devetak and Hayden, studied the capacities of quantum channels with two senders and one receiver [16]. They found multi-letter characterizations of the capacity, and single-letter formulas for some particular channels.

**A large family of quantum weak coin-flipping protocols.** Carlos Mochon found a family of new coin flipping protocols that achieve a bias of  $1/6$ , an improvement over the protocols he had constructed earlier [17]. He obtained tight lower bounds for the bias, proving that  $1/6$  is optimal for all protocols within the family.

**Phase randomization improves the security of quantum key distribution.** John Preskill, with Lo, found that the security of a quantum key distribution protocol that uses weak coherent signal states can be weakened if the adversary knows the phase of the signals [18]. There is a parameter regime in which an eavesdropper who knows the phase can learn every key bit, while a protocol using phase-randomized signals is provably secure.

**Entanglement-assisted one-way capacity of a two-way quantum channel.** Andrew Childs and Debbie Leung, with Lo, studied communication between two parties using a bipartite quantum operation [19]. For the case in which the two parties share unlimited prior entanglement,

they gave inner and outer bounds on the achievable rate region for simultaneous forward and backward classical communication.

**Classical capacity of fermionic product channels.** Sergey Bravyi studied multi-qubit quantum channels that can be represented as a product of one-mode fermionic attenuation channels [20]. He proposed an explicit formula for the classical capacity and for the minimum output entropy of these channels, which he verified numerically.

## Quantum entanglement and quantum information theory

**Efficiently computable multi-partite entanglement measure for stabilizer states.** Bravyi, with Fattal, Cubitt, Yamamoto, and Chuang, formulated a multi-partite entanglement measure for stabilizer states, which can be computed efficiently from a set of generators of the stabilizer group [21]. This measure applies to qubits, qudits and continuous variables.

**Characterization of communication between two systems both coupled to the same system.** Schumacher, with Westmoreland, investigated the situation in which no information can be transferred from a quantum system B to a quantum system A, even though both interact with a common system C [22].

**Analysis of a quantum phase transition in a noisy three-dimensional cluster state.** Robert Raussendorf and Sergey Bravyi, with Harrington, described a phase transition for long-range entanglement in a three-dimensional cluster state affected by noise [23]. They modeled the partially decohered state by the thermal state of a suitable Hamiltonian, and found upper and lower bounds on the (nonzero) transition temperature at which the entanglement length changes from infinite to finite.

**Review of entanglement in random subspaces.** Patrick Hayden reviewed recent developments in the theory of random subspaces [24], including applications to achieving the quantum channel capacity and to elucidating the structure of multipartite entanglement.

**Application of Schubert calculus to quantifying correlations in quantum systems.** Sumit Daftuar and Patrick Hayden surveyed recently developed tools for comparing the eigenvalues of matrices related via a moment map, and explored applications to characterizing the partial trace of a matrix [25].

**Nearest neighbor entanglement for many spins in ring and star geometries.** Sougato Bose, with Hutton, proposed a scheme for optimizing the nearest-neighbor and next-to-nearest neighbor entanglement in a network of interacting spins [26]. Allowing the system to interact through a weighted combination of star and the ring geometries provides the highest entanglement between two chosen spins.

**Limitations of nice mutually unbiased bases.** Andrew Childs and Pawel Wocjan, with Aschbacher, investigated constructions of mutually unbiased bases by partitioning a unitary error

basis [27]. They found that this construction offers no improvement over previous approaches.

**Robustness of two-mode squeezed states.** Steven van Enk, with Hirota, studied how absorption losses degrade the bipartite entanglement of entangled states of light [28]. They determined what state contains the smallest number of photons for a fixed amount of entanglement, and what state is the most robust against photon absorption.

**Localizable entanglement.** Frank Verstraete, 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 [29]. 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.

**Recipe for sequential generation of entangled multi-qubit states.** Frank Verstraete, with Schoen, Solano, Cirac, and Wolf, considered the deterministic generation of entangled multi-qubit states by the sequential coupling of an ancillary system to initially uncorrelated qubits [30]. They characterized all achievable states in terms of classes of matrix product states and gave a recipe for the generation on demand of any multi-qubit state.

**Bounds on the maximal number of real mutually unbiased bases.** Pawel Wocjan, with Boykin, Sitharam, and Tarifi, tabulated bounds on the optimal number of mutually unbiased bases in  $R^d$  [31]. For most dimensions  $d$ , they showed that either there are no real orthonormal bases that are mutually unbiased or the optimal number is at most either 2 or 3.

**Characterization of combinatorially independent permutation separability criteria.** Pawel Wocjan, with Horodecki and with Clarisse, characterized combinatorially independent permutation separability criteria. [32, 33]. Their result implies, in particular, that there are exactly 6 independent criteria for three parties and 22 for four parties.

**Extending the number of observers in a Bell inequality.** Stefano Pironio studied “liftings” of Bell inequalities — extensions to more observers, measurement settings or measurement outcomes [34]. He showed that if the original inequality defines a facet of the polytope of local joint outcome probabilities, then the lifted one also defines a facet of a more complex polytope.

**General monogamy inequality for bipartite qubit entanglement.** Frank Verstraete, with Osborne, considered multipartite states of qubits, and proved that their bipartite quantum entanglement, as quantified by the concurrence, satisfies a monogamy inequality [35]. They related this monogamy inequality to the concept of frustration of correlations in quantum spin systems.

**GHZ extraction yield for multipartite stabilizer states.** Sergey Bravyi, with Fattal and Gottesman, studied conversion via local unitaries of a multi-part stabilizer state into singlets, GHZ states, and local one-qubit states [36]. For an arbitrary number of parties  $m$  they found a formula for the maximal number of  $m$ -partite GHZ states that can be extracted. The numbers of singlets and GHZs are determined by dimensions of certain subgroups of the stabilizer group.

**Emergent classicality of redundantly stored quantum information.** Robin Blume-

Kohout, with Zurek, formulated a comprehensive theory of redundant information storage in decoherence processes [37]. Redundancy has been proposed as a prerequisite for objectivity, the defining property of classical objects.

**Asymptotic entanglement of assistance of a general bipartite mixed state.** Frank Verstraete, with Smolin and Winter, showed that the asymptotic entanglement of assistance of a general bipartite mixed state is equal to the smaller of its two local entropies [38]. They also proposed a protocol that distills GHZ states and an asymptotically optimal number of EPR pairs from a tripartite pure state; under a restricted class of protocols, the GHZ rate is also optimal.

**Relating construction of mutually unbiased bases to orthogonal decompositions of Lie algebras.** Pawel Wocjan, with Boykin, Sitharam, and Tiep established a connection between the problem of constructing maximal collections of mutually unbiased bases and an open problem in the theory of Lie algebras [39]. Their result supports the general belief that a complete collection of mutually unbiased bases can only exist in prime power dimensions.

**Quantifying nonlocality using Popescu-Rohrlich boxes.** Stefano Pironio, with Barrett, showed that a wide class of multipartite correlations can be simulated using local operations on Popescu-Rohrlich nonlocal boxes [40]. They also showed that there are quantum multipartite correlations, arising from measurements on a cluster state, that cannot be simulated with such boxes.

**Evolution of entanglement due to wave packet scattering.** Leonard Schulman, with Lawrence Schulman, showed that the wave packet spread of a particle in a collection of different mass particles, all with Gaussian wave functions, evolves to a value that is inversely proportional to the mass of the particle [41]. They also addressed the question of in-principle measurement of wave packet spread.

## Quantum error correction and fault tolerance

**Proofs of quantum accuracy threshold theorems.** John 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 [42]. 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.

**Proof of fault tolerance in the graph-state model.** Panos Aliferis and Debbie Leung proved an accuracy threshold theorem that applies to simulations of quantum circuits based on general graph states [43]. They obtained lower bounds for the threshold in the graph-state model by invoking the threshold theorem for the circuit model subject to the same noise process.

**Equivalence of decoupling schemes and orthogonal arrays.** Pawel Wocjan, with Roet-

teler, considered the problem of switching off unwanted interactions in a given multi-partite Hamiltonian [44]. They showed that two previously proposed methods, one based on orthogonal arrays, the other on triples of Hadamard matrices closed under pointwise multiplication, actually lead to equivalent decoupling schemes.

**Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays.** Pawel Wocjan constructed decoupling schemes with bounded-strength control Hamiltonians that can be applied to composite quantum systems with few-body Hamiltonians and special couplings to the environment, based on Eulerian orthogonal arrays [45]. He also showed how to construct such arrays with good parameters in order to obtain efficient decoupling schemes.

**Review of nonlinear dynamics of measured quantum systems.** Hideo Mabuchi, Asa Hopkins, and co-authors wrote an introductory review of the nonlinear dynamics of measured quantum systems [46]. They emphasized some of the characteristically nonlinear features, such as chaos, that are especially relevant to controlling quantum systems.

**Introduction to noncommutative quantum filtering theory.** Luc Bouten and Ramon van Handel wrote an introduction to noncommutative quantum filtering theory [47]. They described the construction of Wiener and Poisson processes on the Fock space and the quantum Ito calculus, emphasizing system-observation models from quantum optics.

## Experiment and implementation

**Robust quantum gates on neutral atoms with cavity-assisted photon-scattering.** Jeff Kimble, with Duan and Wang, proposed a scheme to achieve quantum computation with neutral atoms whose interactions are catalyzed by single photons [48]. Conditional quantum gates are obtained in their scheme through cavity-assisted photon scattering, in a manner that is robust to random variation in the atom-photon coupling rate and which does not require localization in the Lamb-Dicke regime.

**Strategies for real-time position control of a single atom in cavity QED.** Theresa Lynn, Kevin Birnbaum, and Jeff Kimble developed feedback algorithms for cooling the radial component of motion of a single atom trapped by strong coupling to single-photon fields in an optical cavity [49]. They studied the performance of their algorithms through simulations of single-atom trajectories, with full dynamical and measurement noise included.

**Theory of photon blockade by an optical cavity with one trapped atom.** Kevin Birnbaum, Andreea Boca, Russell Miller, David Boozar, David Boozar, Tracy Northrup, and Jeff Kimble developed the theory of the photon blockade by an optical cavity with one trapped atom [50], in order to interpret their recent experiments. They described the general condition for photon blockade in terms of the transmission coefficients for photon number states, and explored the effect of different driving mechanisms on the photon statistics.

## Connecting quantum information with the rest of physics

**Classical algorithm for simulating mixed-state dynamics in spin chains.** Mike Zwolak and Guifre Vidal formulated an algorithm to study mixed-state dynamics in one-dimensional quantum lattice systems [51]. The algorithm can be used to construct thermal states or to simulate real time evolution given by a generic master equation, and the computational cost depends only linearly on the system size.

**Efficient evaluation of partition functions of frustrated and inhomogeneous spin systems.** Frank Verstraete, with Murg and Cirac, presented a numerical method to evaluate partition functions and associated correlation functions of inhomogeneous two-dimensional classical spin systems and one-dimensional quantum spin systems [52]. The method is scalable and has a controlled error.

**Variational matrix product state approach to quantum impurity models.** Verstraete, with Weichselbaum, Schollwöck, Cirac, and von Delft, showed how Wilson’s numerical renormalization group method for solving quantum impurity models can be turned into a variational method within the set of matrix product states [53]. This endows it with much more flexibility than before and puts it on the same formal footing as White’s density matrix renormalization group, thereby leading to a unified variational formulation of numerical renormalization group methods.

**Renormalization algorithm for the calculation of spectra of interacting quantum systems.** Verstraete, with Porras and Cirac, presented an algorithm for the calculation of eigenstates with definite linear momentum in quantum lattices [54]. Their method is related to the Density Matrix Renormalization Group, and makes use of the distribution of multipartite entanglement to build variational wave functions with translational symmetry.

**Matrix product states represent ground states faithfully.** 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 in one dimension [55]. Their results justify the use of renormalization group methods even in the case of critical systems.

**Exploiting quantum parallelism to simulate quantum random many-body systems** Verstraete, with Paredes and Cirac, presented an algorithm that exploits quantum parallelism to simulate randomness in a quantum system [56]. In their scheme, all possible realizations of the random parameters are encoded quantum mechanically in a superposition state of an auxiliary system.

**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 [57]. His paper also included a comprehensive review of the theory of anyons, containing many proofs of new results,

including for example a general analysis of the spectral Chern number for a system of free fermions.

**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 [58]. The main idea (adapted from an earlier proposal by Bravyi and Kitaev) is to introduce auxiliary degrees of freedom 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.

**Detecting nonabelian statistics in the  $\nu = 5/2$  fractional quantum Hall state.** Parsa Bonderson, Alexei 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 [59]. 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.

## References Cited

- [1] 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.
- [2] D. Bacon, I. Chuang, A. Harrow, Efficient quantum circuits for Schur and Clebsch-Gordon transforms, arXiv: quant-ph/0407082 (2004).
- [3] R. Raussendorf, A quantum cellular automaton for universal quantum computation, arXiv: quant-ph/0412048 (2004).
- [4] D. Bacon, A. M. Childs, and W. van Dam, Optimal measurements for the dihedral hidden subgroup problem, arXiv: quant-ph/0501044 (2005).
- [5] C. Moore, A. Russell, and L. Schulman, The symmetric group defies strong Fourier sampling: Part I, arXiv: quant-ph/0501056 (2005).
- [6] L. Duan and R. Raussendorf, Efficient quantum computation with probabilistic quantum gates, Phys. Rev. Lett. 95, 080503 (2005), arXiv: quant-ph/0502120.
- [7] 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.

- [8] R. Raussendorf, Quantum computation via translation-invariant operations on a chain of qubits, *Phys. Rev. A* 72, 052301 (2005), arXiv: quant-ph/0505122.
- [9] 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).
- [10] A. Childs and W. van Dam, Quantum algorithm for a generalized hidden shift problem, arXiv: quant-ph/0507190 (2005).
- [11] M. Ben-Or and D. Mayers, General security definition and composability for quantum and classical protocols, arXiv: quant-ph/0409062 (2004)
- [12] 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.
- [13] P. Hayden and C. King, Correcting quantum channels by measuring the environment, arXiv: quant-ph/0409026 (2004).
- [14] S. van Enk, Reference frames and refbits, *Phys. Rev. A* 71, 032339 (2005), arXiv: quant-ph/0410083.
- [15] 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.
- [16] 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).
- [17] C. Mochon, A large family of quantum weak coin-flipping protocols, *Phys. Rev. A* 72, 022341 (2005), arXiv: quant-ph/0502068.
- [18] H.-K. Lo and J. Preskill, Phase randomization improves the security of quantum key distribution, arXiv: quant-ph/0504209 (2005).
- [19] 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.
- [20] S. Bravyi, Classical capacity of fermionic product channels, arXiv: quant-ph/0507282 (2005).
- [21] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, Entanglement in the stabilizer formalism, arXiv: quant-ph/0406168 (2004).

- [22] B. Schumacher and M. Westmoreland, Locality and information transfer in quantum operations arXiv: quant-ph/0406223 (2004).
- [23] 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.
- [24] P. Hayden, Entanglement in random subspaces, arXiv: quant-ph/0409157 (2004).
- [25] S. Daftuar and P. Hayden, Quantum state transformations and the Schubert calculus, *Ann. Phys.* 315, 80-122 (2005), arXiv: quant-ph/0410052.
- [26] A. Hutton and S. Bose, Ground state entanglement in a combination of star and ring geometries of interacting spins, arXiv: quant-ph/0408077 (2004).
- [27] M. Aschbacher, A. Childs, and P. Wocjan, The limitations of nice mutually unbiased bases, arXiv: quant-ph/0412066 (2004).
- [28] Steven van Enk and O. Hirota, The most robust entangled state of light, *Phys. Rev. A* 71, 062322 (2005), arXiv: quant-ph/0412221.
- [29] M. Popp, F. Verstraete, M. A. Martin-Delgado, and J. I. Cirac, Localizable entanglement, *Phys. Rev. A* 71, 042306 (2005), arXiv: quant-ph/0411123.
- [30] 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.
- [31] P. Wocjan, On the maximal number of real mutually unbiased bases, arXiv: quant-ph/0502024 (2005).
- [32] P. Wocjan and M. Horodecki, Characterization of combinatorically independent permutation separability criteria, *Open Syst. Inf. Dyn.* 12, 331 (2005), arXiv: quant-ph/0503129.
- [33] 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.
- [34] S. Pironio, Lifting Bell inequalities, *J. Math. Phys.* 46, 062112 (2005), arXiv: quant-ph/0503179.
- [35] T. J. Osborne and F. Verstraete, General monogamy inequality for bipartite qubit entanglement, arXiv: quant-ph/0502176 (2005).
- [36] S. Bravyi, D. Fattal, and D. Gottesman, GHZ extraction yield for multipartite stabilizer states, arXiv: quant-ph/0504208 (2005).

- [37] 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).
- [38] 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.
- [39] 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).
- [40] J. Barrett and S. Pironio, Popescu-Rohrlich correlations as a unit of nonlocality, Phys. Rev. Lett. 95, 140401 (2005), arXiv: quant-ph/0506180.
- [41] L. Schulman and L. Schulman, Wave packet scattering without kinematic entanglement: Convergence of expectation values, IEEE Transactions on Nanotechnology 4(1):8-13 (2005).
- [42] 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.
- [43] 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.
- [44] M. Roetteler and P. Wocjan, Equivalence of decoupling schemes and orthogonal arrays, arXiv: quant-ph/0409135 (2004).
- [45] P. Wocjan, Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays, arXiv: quant-ph/0410107 (2004).
- [46] 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).
- [47] Luc Bouten and Ramon van Handel, Quantum filtering: a reference probability approach, arXiv: math-ph/0508006 (2005).
- [48] 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.
- [49] 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).
- [50] 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).

- [51] 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.
- [52] 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.
- [53] 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).
- [54] D. Porras, F. Verstraete, and J. I. Cirac, Renormalization algorithm for the calculation of spectra of interacting quantum systems, arXiv: cond-mat/0504717 (2005).
- [55] F. Verstraete and J. I. Cirac, Matrix product states represent ground states faithfully, arXiv: cond-mat/0505140 (2005).
- [56] B. Paredes, F. Verstraete, and J. I. Cirac, Exploiting quantum parallelism to simulate quantum random many-body systems, arXiv: cond-mat/0505288 (2005).
- [57] A. Kitaev, Anyons in an exactly solved model and beyond, *Ann. Phys.* 321, 2-111 (2006), arXiv: cond-mat/0506438.
- [58] F. Verstraete and I. Cirac, Mapping local Hamiltonians of fermions to local Hamiltonians of spins, *J. Stat. Mech.* P09012 (2005), arXiv: cond-mat/0508353.
- [59] 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.