QUANTUM INFORMATION PROCESSING

TWELFTH ANNUAL WORKSHOP

SANTA FE, NEW MEXICO
JANUARY 12, 2009 – JANUARY 16, 2009

WITH SUPPORT FROM:

Institute for Advanced Studies at Los Alamos National Laboratory • Los Alamos National Laboratory: Center for Nonlinear Sciences • Los Alamos National Laboratory: Information Science & Technology Institute • Sandia National Laboratories • University of New Mexico: Center for Advanced Studies • National University of Singapore: Centre for Quantum Technologies • NEC

TABLE OF CONTENTS

ORGANIZING COMMITTEES

LOCAL ORGANIZING COMMITTEE

Andrew Landahl (University of New Mexico) (Chair)
Howard Barnum (Los Alamos National Laboratory)
Jim Harrington (Los Alamos National Laboratory)
Cris Moore (University of New Mexico/Santa Fe Institute)
Jon Yard (Los Alamos National Laboratory)

STEERING COMMITTEE

Cris Moore (UNM/SFI) (Chair)
Dorit Aharonov (Hebrew University)
John Preskill (Caltech)
Jaikumar Radhakrishnan (TIFR, Mumbai)
Renato Renner (ETH Zurich)
Peter Shor (MIT)
John Watrous (Waterloo)
Andreas Winter (Bristol)
Ronald de Wolf (CWI, Amsterdam)

PROGRAM COMMITTEE

Richard Jozsa (Bristol) (Chair)
Hans Briegel (Innsbruck)
Harry Buhrman (CWI, Amsterdam)
Wim van Dam (UCSB)
Daniel Gottesman (Perimeter)
Aram Harrow (Bristol)
Patrick Hayden (McGill)
Julia Kempe (Tel Aviv)
Manny Knill (NIST)
Andrew Landahl (New Mexico)
Debbie Leung (Waterloo)
Keiji Matsumoto (NII Tokyo)
Ben Reichardt (Caltech)
Alex Russell (Connecticut)
Barbara Terhal (IBM)
Frank Verstraete (Vienna)

QIP 2009 PROGRAM

SUNDAY, JANUARY 11, 2009

7:00-10:00 p.m. Early Registration (La Fonda Hotel – Main lobby)

MONDAY, JANUARY 12, 2009

7:30-8:45 a.m. Registration at the Santa Fe Convention Center

8:45-9:00 a.m. Andrew Landahl, Opening Remarks

9:00-9:55 a.m. Matt Hastings, Invited Speaker
A counterexample to additivity

10:00-10:30 a.m. Patrick Hayden and Andreas Winter
The fidelity alternative and quantum measurement simulation

10:30-11:05 Break

11:05-11:35 a.m. Sergey Bravyi and Barbara Terhal
A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes

11:40-12:00 p.m. Dmitry Gavinsky
Predictive quantum learning

12:00-2:00 Lunch

2:00-2:55 p.m. Graeme Smith, Invited Speaker
Quantum communication with zero-capacity channels

3:00-3:20 p.m. John Smolin and Graeme Smith
Can non-private channels transmit quantum information?

3:20-3:50 Break

3:50-4:10 p.m. Ashley Montanaro and Tobias Osbourne
Quantum Boolean functions

4:15-4:35 p.m. Yi-Kai Liu
Quantum algorithms using the curvelet transform

4:40-5:00 p.m. Dave Bacon, Wim van Dam, and Alexander Russell
Analyzing quantum circuits using the least action principle

TUESDAY, JANUARY 13, 2009

8:30-9:00 a.m. Registration at the Santa Fe Convention Center

9:00-9:55 a.m. Avinatan Hassidim, Invited Speaker
Multi-prover interactive proofs with communicating provers

10:00-10:30 a.m. Andris Ambainis
Quantum algorithms are at most polynomially faster than classical for any symmetric function

10:30-11:05 Break

11:05-11:35 a.m. Jean-Pierre Tillich
Quantum tornado codes

11:40-12:00 p.m. Norbert Schuch and Frank Verstraete
Interacting electrons, density functional theory, and quantum Merlin-Arthur

Tuesday afternoon: Free. (Explore! Collaborate! Enjoy!)

[This space is reserved for creative doodling.]

WEDNESDAY, JANUARY 14, 2009

8:30-9:00 a.m. Registration at the Santa Fe Convention Center

9:00-9:55 a.m. Andrew Childs, Invited Speaker
Universal computation by quantum walk

10:00-10:30 a.m. Dmitry Gavinsky
Classical interaction cannot replace quantum nonlocality

10:30-11:05 Break

11:05-11:35 a.m. Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando Somma, and David Yonge-Mallo
Efficient discrete-time simulations of continuous-time quantum query algorithms

11:40-12:00 p.m. Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto
Oracularization and two-prover one-round interactive proofs against nonlocal strategies

12:00-2:00 Lunch

2:00-2:20 p.m. Panos Aliferis and John Preskill
Fault-tolerant quantum computing against highly biased noise

2:25-2:45 p.m. Bryan Eastin and Emanuel Knill
Restrictions on transversal encoded quantum gate sets

2:50-3:10 p.m. Avraham Ben-Aroya and Amnon Ta-Shma
Approximate quantum error correction for correlated noise

3:15-3:20 p.m. Dmitry Maslov (Program Director, AF/CCF/CISE at NSF)
Quantum information funding at the National Science Foundation

3:20-3:30 Break

3:30-6:00 p.m. Poster Session

THURSDAY, JANUARY 15, 2009

8:30-9:00 a.m. Registration at the Santa Fe Convention Center

9:00-9:55 a.m. Charles Marcus, Invited Speaker
Holding quantum information in electron spins

10:00-10:30 a.m. Sandy Irani
Ground states entanglement in one-dimensional translationally-invariant quantum systems

10:30-11:05 Break

11:05-11:35 a.m. Fernando Brandao and Martin Plenio
Quantum Stein's lemma for correlated states and asymptotic entanglement transformations

11:40-12:00 p.m. Steve Flammia, David Gross, Jens Eisert, Michael Bremner, Andreas Winter, and Caterina Mora
Most quantum states are useless for measurement-based quantum computation

12:00-2:00 Lunch

2:00-2:55 p.m. Matt Hastings, Invited Speaker
Area laws for quantum many-body systems: Gapped one-dimensional systems are in NP

3:00-3:20 p.m. Norbert Schuch, J. Ignacio Cirac, and Frank Verstraete
The computational difficulty of finding MPS ground states

3:20-3:50 Break

3:50-4:10 p.m. Dan Shepherd and Michael Bremner
Instantaneous quantum computation

4:15-4:35 p.m. Jens Eisert and David Gross
Lieb-Robinson bounds and "supersonic quantum communication"

4:40-5:00 p.m. Scott Aaronson and John Watrous
Closed timelike curves make quantum and classical computing equivalent

5:00-6:00 Free

6:00-7:00 p.m. Cocktail hour at La Fonda (cash bar)

7:00-10:00 p.m. Banquet at La Fonda (Informal talk by Michael Nielsen)

FRIDAY, JANUARY 16, 2009

8:30-9:00 a.m. Registration at the Santa Fe Convention Center

9:00-9:55 a.m. Lluis Masanes, Invited Speaker
Towards device-independent security in QKD

10:00-10:30 a.m. Amnon Ta-Shma
Short seed extractors against quantum storage

10:30-11:05 Break

11:05-11:35 a.m. Jop Briet, Harry Buhrman, and Ben Toner
A generalized Grothendieck inequality and entanglement in XOR games

11:40-12:00 p.m. Dejan Dukaric, Manuel Forster, Severin Winkler, and Stefan Wolf
On non-locality distillation

12:00-2:00 Lunch

2:00-2:20 p.m. Gilles Brassard, Louis Salvail, and Alain Tapp
Key distribution and oblivious transfer à la Merkle

2:25-2:45 p.m. Robert König, Renato Renner, and Christian Schaffner
The operational meaning of min- and max-entropy

2:50-3:10 p.m. Matthias Christandl, Dejan Dukaric, Robert König, and Renato Renner
Postselection-technique with applications to quantum cryptography and the parallel repetition problem

3:10-3:50 Break

3:50-4:10 p.m. Robert König, Ben Reichardt, and Guifre Vidal
Exact entanglement renormalization for string-net models

4:15-4:35 p.m. Aram Harrow and Richard Low
Efficient quantum tensor product expanders and k-designs

4:40-5:00 p.m. Bill Rosgen
Distinguishability of random unitary channels

ORAL PRESENTATIONS

INVITED TALKS
(IN CHRONOLOGICAL ORDER)

Matt Hastings (LANL). *A counterexample to additivity*

There are four different additivity conjectures in quantum information theory, all of which were shown to be equivalent by Shor in 2004. These include the additivity of the Holevo capacity for sending classical information over a quantum channel, and the additivity of the minimum output entropy of a quantum channel. These conjectures relate to whether or not entanglement between different inputs to a quantum channel is useful to increase classical capacity or reduce output entropy. I will present a counter-example to the minimum output entropy conjecture, which implies that all of these additivity conjectures are false. The counter-example is based on a random construction of a channel with a large environment dimension and an even larger system dimension. I will relate this channel to recent work on quantum expanders, and I will propose a slightly weaker additivity conjecture which would give us a two-letter formula for capacity of channels invariant under complex conjugation.

Graeme Smith (IBM, TJ Watson). *Quantum communication with zero-capacity channels*

Communication over a noisy quantum channel introduces errors in the transmission that must be corrected. A fundamental bound on quantum error correction is the quantum capacity, which quantifies the amount of quantum data that can be sent. I will show how two quantum channels, each with a transmission capacity of zero, can have a nonzero capacity when used together. This unveils a rich structure in the theory of quantum communications, and points towards several new questions about communication and information in the physical world.

This is work done jointly with Jon Yard.

Avinatan Hassidim (Jerusalem). *Multi-prover interactive proofs with communicating provers*

We introduce a variant of Quantum Multi Prover Interactive Proofs (QMIP), where the provers do not share entanglement, the communication between the verifier and the provers is quantum, but the provers are unlimited in the classical communication between them. At first, this model may seem very weak, as provers who exchange information seem to be equivalent in power to a single prover. This in fact is not the case - we show that any language in NEXP can be recognized in this model efficiently, with just two provers and two rounds of communication, with a constant completeness-soundness gap.

The main idea is not to bound the information the provers exchange with each other, as in the classical case, but rather to prove that any "cheating" strategy employed by the provers has constant probability to diminish the entanglement between the verifier and the provers by a constant amount. Detecting such reduction gives us the soundness proof. Similar ideas and techniques may help help with other models of Quantum MIP, including the dual question, of non communicating provers with unlimited entanglement.

Joint work with Michael Ben-Or and Haran Pilpel.

Andrew Childs (Waterloo). *Universal computation by quantum walk*

In some of the earliest work on quantum mechanical computers, Feynman showed how to implement universal quantum computation by the dynamics of a time-independent Hamiltonian. I show that this remains possible even if the Hamiltonian is restricted to be a sparse matrix with all entries equal to 0 or 1, i.e., the adjacency matrix of a low-degree graph. Thus quantum walk can be regarded as a universal computational primitive, with any desired quantum computation encoded entirely in some underlying graph. The main idea of the construction is to implement quantum gates by scattering processes.

Charles Marcus (Harvard). *Holding quantum information in electron spins*

This talk will review recent progress in the control of single electron spins in quantum dots. In GaAs, progress has been rapid, but may ultimately be limited by hyperfine coupling of electrons to nuclear spins of the host lattice. It appears, though, that a variant on dynamic nuclear polarization can help reduce the hyperfine field fluctuations. An alternative is to move out of GaAs, and consider materials with zero nuclear spin, where obviously hyperfine coupling is absent. Work along both of these directions will be discussed.

Research Supported by ARO/IARPA, the Department of Defense, and the NSF.

Matt Hastings (LANL). *Area laws for quantum many-body systems: Gapped one-dimensional systems are in NP*

One of the basic problems in physics is approximating the ground state energy of a quantum many-body system. For arbitrary choice of local interactions, this problem is extremely difficult, even in one dimension where Aharonov, Gottesman, and Kempe and Irani showed that this problem is QMA-complete. However, many of the quantum ground states encountered in practice have a limited amount of entanglement. As I will explain, this makes it possible to efficiently represent the ground state of these systems on a classical computer. In the important case that the Hamiltonian has a spectral gap, I will explain a recent proof of an "area law" which bounds the entanglement entropy. This result implies that a certain promise problem for approximating the ground state energy of gapped one-dimensional Hamiltonians is in NP, while a similar problem for approximating the adiabatic evolution of such systems is in P.

Lluis Masanes (Barcelona). *Device-independent security in QKD*

This talk is about secret key distribution from correlations that violate Bell inequalities. A security proof can be obtained from the assumption that arbitrarily-fast signaling between different subsystems is impossible. This assumption is imposed at the level of the outcome probabilities given the choice of observables, therefore, the scheme remains secure in situations where the honest parties distrust their quantum apparatuses.

CONTRIBUTED TALKS
(IN CHRONOLOGICAL ORDER)

Patrick Hayden and Andreas Winter. *The Fidelity Alternative and quantum measurement simulation*

> If a quantum system is subject to noise, it is possible to perform quantum error correction and reverse the action of the noise if and only if no information about the system's quantum state leaks to the environment. In this article, we develop an analogous duality in the case that the environment approximately forgets the identity of the quantum state, a weaker condition satisfied, for example, by approximately randomizing maps. Specifically, we show that the environment approximately forgets quantum states if and only if the original channel approximately preserves pairwise fidelities of pure inputs, an observation we call the Fidelity Alternative. Using this tool, we then go on to study the task of simulating restricted classes of measurements on a space of input states using the output of a noisy channel. The case of simulating measurements that test whether the input state is an arbitrary pure state is essentially equality testing and known as quantum identification. We establish that the optimal (amortized) rate at which quantum states can be "identified" through a noisy quantum channel is equal to the entanglement-assisted classical capacity of the channel, despite the fact that the task is quantum, not classical, and entanglement-assistance is not allowed.

Sergey Bravyi and Barbara Terhal. *A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes*

> We study properties of stabilizer codes that permit a local description on a regular D-dimensional lattice. Specifically, we assume that the stabilizer group of a code (the gauge group for subsystem codes) can be generated by local Pauli operators such that the support of any generator is bounded by a hypercube of constant size. Our first result concerns the optimal scaling of the distance d with the linear size of the lattice L. We prove an upper bound $d = O(L^{D-1})$ which is tight for D=1, 2. This bound applies to both subspace and subsystem stabilizer codes. Secondly, we analyze the suitability of stabilizer codes for building a self-correcting quantum memory. Any stabilizer code with geometrically local generators can be naturally transformed to a local Hamiltonian penalizing states that violate the stabilizer condition. A degenerate ground-state of this Hamiltonian corresponds to the logical subspace of the code. We prove that for D=1, 2 the height of the energy barrier separating different logical states is upper bounded by a constant independent of the lattice size L. It demonstrates that a self-correcting quantum memory cannot be built using stabilizer codes in dimensions D=1, 2. This result is in sharp contrast with the existence of a classical self-correcting memory in the form of a two-dimensional ferromagnet. Our results leave open the possibility for a self-correcting quantum memory based on 2D subsystem codes or on 3D subspace or subsystem codes.

Dmitry Gavinsky. *Predictive quantum learning*

> We give an example of a relational concept class that is efficiently learnable in certain quantum analogue of the PAC model, while in any classical model exponential number of examples would be required. We show that our separation is the best possible in several ways; in particular, there is no analogous result for a functional class, as well as for some weaker versions of quantum PAC. This is the first (unconditional) separation of quantum and classical learning models.

John Smolin and Graeme Smith. *Can non-private channels transmit quantum information?*

> We study the power of quantum channels with little or no capacity for private communication. Because privacy is a necessary condition for quantum communication, one might expect that such channels would be of little use for transmitting quantum states. Nevertheless, we find strong evidence that there are pairs of such channels that, when used together, can transmit far more quantum information than the sum of their individual private capacities. Specifically, we present channels with $O(\log d)$ input qubits which display either (1) joint quantum capacity $O(\log d)$ but vanishing individual private capacities or (2) $O(\log d)$ classical capacity with vanishingly small one-shot Holevo information.

Ashley Montanaro and Tobias Osborne. *Quantum Boolean functions*

> In this paper we introduce the study of quantum Boolean functions, which are unitary operators f whose square is the identity: $f^2 = 1$. We describe several generalisations of well-known results in the theory of Boolean functions, including quantum property testing; a quantum version of the Goldreich-Levin algorithm for finding the large Fourier coefficients of Boolean functions; and two quantum versions of a theorem of Friedgut, Kalai and Naor on the Fourier spectra of Boolean functions. In order to obtain one of these generalisations, we prove a quantum extension of the hypercontractive inequality of Bonami, Gross and Beckner.

Yi-Kai Liu. *Quantum Algorithms using the Curvelet Transform*

> The curvelet transform is a directional wavelet transform over R^n, originally due to Candes and Donoho (2002). It is used to analyze functions that have singularities along smooth surfaces. I demonstrate how this can lead to new quantum algorithms. I give an efficient implementation of a quantum curvelet transform, together with two applications: a single-shot measurement procedure for approximately finding the center of a ball in R^n, given quantum-samples over the ball; and, a quantum algorithm for finding the center of a radial function over R^n, given oracle access to the function. I conjecture that these algorithms only require a constant number of quantum-samples or oracle queries, independent of the dimension n --- this can be interpreted as a quantum speed-up. Finally, I prove some rigorous bounds on the distribution of probability mass for the continuous curvelet transform. This almost proves my conjecture, except for issues of discretization.

Dave Bacon, Wim van Dam and Alexander Russell. *Analyzing quantum circuits using the least action principle*

> We introduce and analyze circuits that are the quantum mechanical generalization of (classical) algebraic circuits. Using the algebraic operations of addition and multiplication, as well as the quantum Fourier transform, such circuits are well-defined for rings Z/mZ and finite fields GF(q). The acceptance probabilities of algebraic quantum circuits can be expressed as exponential sums $\sum_x e^{2\pi i f(x)/m}$ where the multivariate polynomial f is determined by the circuit, while it is independent of the ring or field over which we interpret the circuit. Dawson *et al.* [Quantum Information & Computation, **5**(2), pp. 102-112 (2004)] introduced this "sum over paths" description as a discrete version of the path integral approach to standard quantum mechanics. From this perspective, the polynomial f should be interpreted as the "action" of a specific (classical) computational path between the input and output of the circuit. Here we show that, despite the fact that the polynomial f is defined only over the integers, we can indeed apply the least action principle to derive which computational paths are relevant for the calculation of the acceptance amplitude, and which are not.

Andris Ambainis. *Quantum algorithms are at most polynomially faster than classical for any symmetric function*

> We show that, for any symmetric function $f(x_1, \ldots, x_N)$ of variables $x_1, \ldots, x_N$ taking values in an arbitrary finite set $\{1, \ldots, M\}$, its quantum query complexity is polynomially related to its classical (probabilistic) query complexity. This generalizes the quantum lower bounds on the collision problem and related problems.

Jean-Pierre Tillich. *Quantum tornado codes*

> There are quantum analogues for LDPC codes, however due to the orthogonality constraints which appear in the quantum setting they seem to be much harder to construct than classical LDPC codes. For instance, it is still unknown whether or not there exist families of such quantum codes with nonvanishing rate and unbounded minimum distance. Moreover, the Tanner graph associated to a quantum LDPC code necessarily contains many 4-cycles which are well known for their negative effect on the performance of iterative decoding and make rigorous analysis of iterative decoding quite delicate. We present here a way to get around these difficulties by presenting a modification of quantum LDPC codes with unbounded minimum distance and for which it can be proved that they attain the capacity of the quantum erasure channel under iterative decoding.

Norbert Schuch and Frank Verstraete. *Interacting electrons, density functional theory, and quantum Merlin-Arthur*

> One of the central problems in quantum mechanics is to find the ground state energy of a system of electrons interacting via the Coulomb potential. Density Functional Theory (DFT), the most widely used and successful method for dealing with such systems, uses a universal functional to reduce the difficulty of the problem. Here, we show that the field of computational complexity imposes fundamental limitations on DFT, as an efficient description of the associated functional would lead to the unlikely collapse of the complexity class QMA to NP, i.e., quantum proofs would be no more powerful than classical proofs. We do so by showing QMA-completeness of the 2D Hubbard model and proving that it could be solved in NP if the universal functional could be computed efficiently. This provides a clear illustration of how thinking about quantum computers can be useful even if they would never be built.

Richard Cleve, Daniel Gottesman, Michele Mosca, Rolando Somma and David Yonge-Mallo. *Efficient discrete-time simulations of continuous-time quantum query algorithms*

> The continuous-time query model is a variant of the discrete query model in which queries can be interleaved with known operations continuously in time. We show that any quantum algorithm in the continuous-time query model whose total query time is T can be simulated by an algorithm in the discrete query model that makes $O(T \log T)$ queries. This bound is independent of known operations (i.e., the norm of the driving Hamiltonian). One consequence of this result is that any lower bound of T in the discrete-time query model immediately carries over to a lower bound of order $T/\log T$ for the continuous-time query model. Although our simulation uses $O(T^2 \log T)$ unitary gates (in addition to the queries), it could serve as inspiration for more efficient conversions.

Dmitry Gavinsky. *Classical interaction cannot replace quantum nonlocality*

> We present a 2-player communication task that can be solved efficiently in the simultaneous message passing model with classical communication, where the players share entanglement. On the other hand, the task requires exponentially more communication in the classical interactive (two-way) model. Our second result is a two-player nonlocality game with input length n and output of polylogarithmic length, that can be won with probability $1 - o(1)$ by entangled players.

On the other hand, the game is lost with constant probability by players without entanglement, even if they are allowed to exchange $o(n^{1/4})$ bits in interactive communication before producing their output.

Tsuyoshi Ito, Hirotada Kobayashi and Keiji Matsumoto. *Oracularization and two-prover one-round interactive proofs against nonlocal strategies*

A central problem in quantum computational complexity is how to prevent entanglement-assisted cheating in multi-prover interactive proof systems. It is well-known that the standard oracularization technique completely fails in some proof systems under the existence of prior entanglement. This paper studies two constructions of two-prover one-round interactive proof systems based on oracularization. First, it is proved that the two-prover one-round interactive proof system for PSPACE by Cai, Condon, and Lipton still achieves exponentially small soundness error in the existence of prior entanglement between dishonest provers (and more strongly, even if dishonest provers are allowed to use arbitrary no-signaling strategies). It follows that, unless the polynomial-time hierarchy collapses to the second level, two-prover systems are still advantageous to single-prover systems even when only malicious provers can use quantum information. Second, it is proved that the two-prover one-round interactive proof system obtained by oracularizing a three-query probabilistically checkable proof system becomes sound in a weak sense even against dishonest entangled provers with the help of a dummy question. As a consequence, every language in NEXP has a two-prover one-round interactive proof system of perfect completeness, albeit with exponentially small gap between completeness and soundness, in which each prover responds with only two bits. In other words, it is NP-hard to approximate within an inverse-polynomial the value of a classical two-prover one-round game, even when provers are entangled and each sends a two-bit answer to a verifier.

Panos Aliferis and John Preskill. *Fault-tolerant quantum computing against highly biased noise*

Experimentalists in quantum computing observe that in many of their systems noise is biased --- that is, loss of phase coherence in the computational basis occurs faster than relaxation to the lowest energy eigenstate or leakage outside the computational subspace. We will discuss a scheme for fault-tolerant quantum computation that is especially designed to protect against biased noise. The scheme is particularly effective when the noise bias is very high, with dephasing dominating other types of noise by three orders of magnitude or more. To illustrate how this scheme could be relevant for future experiments, we will discuss how to design a universal set of biased-noise operations for the superconducting flux qubit investigated at the IBM labs.

Bryan Eastin and Emanuel Knill. *Restrictions on transversal encoded quantum gate sets*

We show that the ability of a quantum code to detect an arbitrary error on any single physical subsystem is incompatible with the existence of a universal, transversal encoded gate set for the code.

Avraham Ben-Aroya and Amnon Ta-Shma. *Approximate quantum error correction for correlated noise*

Quantum error correcting codes cannot deal even with limited correlated noise. For example, no non-trivial quantum error correcting code can correct controlled-X errors, when the control depends on all the qubits. In this note we ask whether correction is possible if we allow approximate decoding. We show both positive and negative results. On the one hand, we show controlled-X errors can be corrected with sub-constant approximation error. On the other hand, we show no non-trivial quantum error-correcting code can correct controlled phase error with sub-constant approximation error.

Sandy Irani. *Ground states entanglement in one-dimensional translationally-invariant quantum systems*

We examine one dimensional quantum systems and ask what is the minimal set of properties a system must have in order to exhibit a high degree of ground state entanglement. In particular, do symmetries such as translational invariance limit entanglement? We present a Hamiltonian H for a chain of n 21-state particles, where n is assumed to besodd. H is a sum of identical terms acting on each pair of neighboring particles in the chain. We show that H has a unique ground state and a spectral gap of $1/\mathrm{poly}(n)$. We quantify the entanglement of this system by determining the entropy of the ground state when the system is traced down to a linear number of particles on either end of the chain and show that the entropy scales linearly with n.

Fernando Brandao and Martin Plenio. *Quantum Stein's lemma for correlated states and asymptotic entanglement transformations*

We present a generalization of quantum Stein's Lemma to the situation in which the alternative hypothesis is formed by a *family* of states, which can moreover be *non-i.i.d.* We consider sets of states which satisfy a few natural properties, the most important being the closedness under permutations of the copies, and determine the rate function of the probability of the error in a very similar fashion to quantum Stein's Lemma, in terms of the quantum relative entropy. This result has interesting applications to entanglement theory. First it gives an *operational meaning* to the entanglement measure known as regularized relative entropy of entanglement. Second, it shows that this measure is faithful, being strictly positive on every entangled state. This implies, in particular, that whenever a multipartite state can be asymptotically converted into another entangled state by local operations and classical communication, the rate of conversion must be non-zero. Therefore, the *operational* definition of multipartite entanglement is equivalent to its *mathematical* definition.

Steve Flammia, David Gross, Jens Eisert, Michael Bremner, Andreas Winter and Caterina Mora. *Most quantum states are useless for measurement-based quantum computation*

It is often argued that entanglement is at the root of the speedup for quantum compared to classical computation, and that one needs a sufficient amount of entanglement for this speedup to be manifest. In measurement-based quantum computing (MBQC), the need for a highly entangled initial state is particularly obvious. Defying this intuition, we show that quantum states can be too entangled to be useful for the purpose of computation. We prove that this phenomenon occurs for a dramatic majority of all states: the fraction of useful n-qubit pure states is less than $\exp(-n^2)$, using concentration of measure ideas. Computational universality is hence a rare property in quantum states. This work highlights a new aspect of the question concerning the role entanglement plays for quantum computational speed-ups. The statements remain true if one allows for certain forms of post-selection and also cover the notion of CQ-universality. We identify scale-invariant states resulting from a MERA constructrion as likely candidates for physically relevant states subject to this effect.

Norbert Schuch, J. Ignacio Cirac and Frank Verstraete. *The computational difficulty of finding MPS ground states*

We determine the computational difficulty of finding ground states of one-dimensional (1D) Hamiltonians which are known to be Matrix Product States (MPS). To this end, we construct a class of 1D frustration free Hamiltonians with unique MPS ground states and a polynomial gap above, for which finding the ground state is at least as hard as factoring. By lifting the requirement of a unique ground state, we obtain a class for which finding the ground state solves an NP-complete problem. Therefore, for these Hamiltonians it is not even possible to certify that the ground state has been found. Our results thus imply that in order to prove

convergence of variational methods over MPS, as the Density Matrix Renormalization Group, one has to put more requirements than just MPS ground states and a polynomial spectral gap.

Dan Shepherd and Michael Bremner. *Instantaneous quantum computation*

We examine theoretic architectures and an abstract model for a restricted class of quantum computation, called here instantaneous quantum computation because it allows for essentially no temporal structure within the quantum dynamics. Using the theory of binary matroids, we argue that the paradigm is rich enough to enable sampling from probability distributions that cannot, classically, be sampled from efficiently and accurately. This paradigm also admits simple interactive proof games that may convince a skeptic of the existence of truly quantum effects. Furthermore, these effects can be created using significantly fewer qubits than are required for running Shor's Algorithm. The full version of this paper is available on the eprint arXiv (arXiv:0809.0847).

Jens Eisert and David Gross. *Lieb Robinson bounds and "supersonic quantum communication"*

When locally exciting a quantum lattice model, the excitation will propagate through the lattice. The effect is responsible for a wealth of non-equilibrium phenomena, and has been exploited to transmit quantum information through spin chains. It is a commonly expressed belief that for local Hamiltonians, any such propagation happens at a finite "speed of sound." Indeed, the Lieb-Robinson theorem states that in spin models, all effects caused by a perturbation are limited to a causal cone defined by a constant speed (up to exponentially small corrections). In this work we show that for meaningful translationally-invariant bosonic models with nearest-neighbor interactions, this belief is incorrect: We prove---using ideas of convex optimization---that one can encounter excitations which accelerate under the natural dynamics of the lattice and allow for reliable transmission of information faster than any finite speed of sound. The effect is only limited by the model's range of validity. The result shows that non-equilibrium dynamics in bosonic models may involve far-away regions interacting with each other, even on short time scales and when the total energy in the system is bounded. It further suggests that chains of bosonic systems may possibly serve as fast channels for quantum communication.

Scott Aaronson and John Watrous. *Closed timelike curves make quantum and classical computing equivalent*

While closed timelike curves (CTCs) are not known to exist, studying their consequences has led to nontrivial insights in general relativity, quantum information, and other areas. Here we show that if CTCs existed, then quantum computers would be no more powerful than classical computers: both would have the (extremely large) power of the complexity class PSPACE, consisting of all problems solvable by a conventional computer using a polynomial amount of memory. This solves an open problem proposed by one of us in 2005, and gives an essentially complete understanding of computational complexity in the presence of CTCs. Following the work of Deutsch, we treat a CTC as simply a region of spacetime where a "causal consistency" condition is imposed, meaning that Nature has to produce a (probabilistic or quantum) fixed-point of some evolution operator. Our conclusion is then a consequence of the following theorem: given any quantum circuit (not necessarily unitary), a fixed-point of the circuit can be (implicitly) computed in polynomial space. This theorem might have independent applications in quantum information. For the full version of this paper, please see http://arxiv.org/abs/0808.2669

Amnon Ta-Shma. *Short seed extractors against quantum storage*

Some, but not all, extractors resist adversaries with limited quantum storage. In this paper we show that Trevisan's extractor has this property, thereby showing an extractor against quantum storage with logarithmic seed length.

Jop Briet, Harry Buhrman and Ben Toner. *A generalized Grothendieck inequality and entanglement in XOR games*

> Suppose Alice and Bob make local two-outcome measurements on a shared entangled state. For any d, we show that there are correlations that can only be reproduced if the local dimension is at least d. This resolves a conjecture of Brunner et al. [Phys. Rev. Lett. **100**, 210503 (2008)] and establishes that the amount of entanglement required to maximally violate a Bell inequality must depend on the number of measurement settings, not just the number of measurement outcomes. We prove this result by establishing the first lower bounds on a new generalization of Grothendieck's constant.

Dejan Dukaric, Manuel Forster, Severin Winkler and Stefan Wolf. *On non-locality distillation*

> Under measurements, two (possibly physically distant) parts of certain quantum states can behave non-locally, meaning that they show a correlation unexplainable by shared (classical) information only. Such correlations are not only fascinating, but have turned out to be an interesting resource for information processing, *e.g.*, in communication complexity or cryptography. Since stronger non-locality leads to better results in this context, it is a natural question whether it is distillable: Can strong non-locality be obtained from (a larger quantity of) weaker? In this note, we give a three-fold answer: First, certain types of non-locality can substantially be amplified. More precisely, a stronger violation of a CHSH Bell inequality can be obtained. Second, for the most natural type of CHSH non-locality, namely its symmetric version, we prove that the possibility of distillation is at most very limited --- a strong indication that it might actually be zero. Finally, this latter result is based on the fact that a certain family of entangled (mixed) states cannot be distilled at all by any non-interactive protocol. The best previous such result was limited distillability of Werner states.

Gilles Brassard, Louis Salvail and Alain Tapp. *Key distribution and oblivious transfer à la Merkle*

> Ralph Merkle's seminal 1974 protocol for (classical) public key distribution is extended in two directions: In the quantum setting and for achieving oblivious transfer. First we show that Merkle's original protocol is totally insecure against a quantum adversary; but then we prove that it can be repaired by allowing the legitimate parties to use quantum computation as well. Second, we give a novel classical protocol for oblivious transfer, based on Merkle's original construction for key distribution, and we prove its polynomial security against all classical attacks in the black-box model. However, we also show that our classical oblivious transfer protocol melts down against a quantum attack: it's easier to cheat it than to use it legitimately! Finally, we propose a fully quantum protocol for oblivious transfer and we conjecture that it is polynomially secure against quantum attacks.

Robert König, Renato Renner and Christian Schaffner. *The operational meaning of min- and max-entropy*

> We show that the conditional min-entropy $H_{min}(A|B)$ of a bipartite state is directly related to the maximum achievable overlap with a maximally entangled state if only local actions on the B-part of ρ_{AB} are allowed. In the special case where A is classical, this overlap corresponds to the probability of guessing A given B. In a similar vein, we connect the conditional max-entropy $H_{max}(A|B)$ to the maximum fidelity of ρ_{AB} with a product state that is completely mixed on A. In the case where A is classical, this corresponds to the security of A when used as a secret key in the presence of an adversary holding B. Because min- and max-entropies are known to characterize information-processing tasks such as randomness extraction and state merging, our results establish a direct connection between these tasks and basic operational problems. For example, they imply that the (logarithm of the) probability of guessing A given B is a lower bound on the number of uniform secret bits that can be extracted from A relative to an adversary holding B.

Matthias Christandl, Dejan Dukaric, Robert König, and Renato Renner. *Postselection-technique with applications to quantum cryptography and the parallel repetition problem*

We propose a general method for studying properties of quantum channels acting on an n-partite system, whose action is invariant under permutations of the subsystems. Our main result is that, in order to prove that a certain property holds for any arbitrary input, it is sufficient to consider the special case where the input is a particular de Finetti-type state, *i.e.,* a state which consists of n identical and independent copies of an (unknown) state on a single subsystem. Our technique can be applied to the analysis of information-theoretic problems. For example, we present a new (quantum) proof for the classical Parallel Repetition Theorem and we get a new proof for the fact that security of a discrete-variable quantum key distribution protocol against collective attacks implies security of the protocol against the most general attacks. Compared to previous proofs (based on the exponential de Finetti theorem) the argument is tighter and simpler.

Robert König, Ben Reichardt and Guifre Vidal. *Exact entanglement renormalization for string-net models*

We construct an explicit renormalization group (RG) transformation for Levin and Wen's string-net models on a hexagonal lattice. The transformation leaves invariant the ground-state "fixed-point" wave function of the string-net condensed phase. Our construction also produces an exact representation of the wave function in terms of the multi-scale entanglement renormalization *Ansatz* (MERA). This sets the stage for efficient numerical simulations of string-net models using MERA algorithms. It also provides an explicit quantum circuit to prepare the string-net ground-state wave function using a quantum computer.

Aram Harrow and Richard Low. *Efficient quantum tensor product expanders and k-designs*

We give an efficient construction of constant-degree, constant-gap quantum k-tensor product expanders. The key ingredients are an efficient classical tensor product expander and the quantum Fourier transform. Our construction works whenever $k = O(n/\log n)$, where n is the number of qubits. An immediate corollary of this result is an efficient construction of unitary k-designs on n qubits for any $k=O(n/\log n)$. Previously, efficient constructions of approximate k-designs were known only for $k=2$.

Bill Rosgen. *Distinguishability of random unitary channels*

A random unitary channel is one that is given by a convex combination of unitary channels. It is shown that the computational problem of distinguishing mixed-state quantum circuits, which is complete for the class of problems with quantum interactive proof systems, remains equivalent when restricted to circuits implementing random unitary operations. This is done by constructing a random unitary approximation to a general quantum channel, from which the result on distinguishability follows. The approximation can also be applied to the problem of the additivity of the minimum output entropy, and it is hoped that it will also have other applications.

POSTERS

POSTERS

1. Dibwe Pierrot Musumbu and Francesco Petruccione. *Quantum walks and the dispersion relation in one-dimensional many-particle system on lattice*

2. Arturo Fernandez, Andrei Klimov, Carlos Muñoz and Carlos Saavedra. *Optimal quantum state reconstruction for cold trapped ions*

3. Sevag Gharibian. *Strong NP-hardness of the quantum separability problem*

4. Yong Zhang. *Quantum error correction codes via Jones unitary braid representations at q=i*

5. Berihu Gebrehiwot, Stefano Olivares and Matteo G A Paris. *Bayesian estimation of qubit gates*

6. Hang Dinh and Alexander Russell. *Quantum and randomized lower bounds for local search on vertex-transitive graphs*

7. Hui Khoon Ng and Lorenza Viola. *Generalized entanglement as a unifying framework for fermionic entanglement*

8. Masahito Hayashi. *Universal coding for classical-quantum channel*

9. Masahito Hayashi. *Universal approximation of multi-copy states and universal quantum loss less data compression*

10. Masahito Hayashi. *Optimal ratio between phase basis and bit basis in QKD*

11. Koji Azuma, Masato Koashi and Nobuyuki Imoto. *Accessing genuinely quantum information without causing disturbance*

12. Soojoon Lee, Jinhyoung Lee and Jaewan Kim. *Any multipartite entangled state violating Bell inequality can be distilled for almost all bipartite splits*

13. Jim Harrington, Mark Wilde and Todd Brun. *Closed timelike curves enable perfect state distinguishability*

14. Christopher Portmann and Akinori Kawachi. *On the power of quantum encryption keys*

15. Debbie Leung and Graeme Smith. *Continuity of a quantum channel's capacities*

16. Wim van Dam and Qingqing Yuan. *Quantum online memory checking*

17. Masahito Hayashi. *Discretization of group-symmetric LOCC detection*

18. Masahito Hayashi. *Group-theoretical study of LOCC detection of maximally entangled state using hypothesis testing*

19. Dong Pyo Chi, Jeong Woon Choi, Kabgyun Jeong, Jeong San Kim, Taewan Kim and Soojoon Lee. *Monogamy equality in 2 × 2 × d quantum systems*

20. Dong Pyo Chi, Jeong Woon Choi, Jeong San Kim, Taewan Kim and Soojoon Lee. *Quantum states for perfectly secure secret sharing*

21. Go Kato. *Quantum cloning of qubits with orthogonal states as hints*

22. Hari Krovi and Martin Roetteler. *An efficient quantum algorithm for the hidden subgroup problem over Weyl-Heisenberg groups*

23. Min-Hsiu Hsieh and Mark Wilde. *The classically-enhanced father protocol*

24. Marco Tomamichel, Renato Renner and Roger Colbeck. *A quantum asymptotic equipartition property*

25. Koji Nuida, Gen Kimura, Takayuki Miyadera and Hideki Imai. *On minimum-error state discrimination problems in generic probability models*

26. Anne Broadbent, Joseph Fitzsimons and Elham Kashefi. *Universal blind quantum computation*

27. Daniel Nagaj. *Railroad switch: from circuits to Hamiltonians*

28. Andris Ambainis, Kazuo Iwama, Masaki Nakanishi, Harumichi Nishimura, Rudy Raymond, Seiichiro Tani and Shigeru Yamashita. *Average/worst-case gap of quantum query complexities*

29. Sebastien Gambs. *Quantum classification*

30. Vlad Gheorghiu, Shiang Yong Looi and Robert B. Griffiths. *Location of quantum information in additive quantum codes*

31. Jeong San Kim, Anirban Das and Barry Sanders. *Entanglement monogamy of multipartite higher-dimensional quantum systems using convex-roof extended negativity*

32. Yingkai Ouyang, Debbie Leung and Man Hong Yung. *A more accurate measurement model for fault tolerant quantum computing*

33. Ivan Kassal, Stephen Jordan, Peter Love, Masoud Mosheni and Alan Aspuru-Guzik. *Quantum simulation of chemical dynamics.*

34. Salman Beigi. NP *vs.* QMA log(2)

35. Hiroshi Imai and Masahito Hayashi. *Fourier analytic approach to phase estimation*

36. Retracted.

37. Anil Shaji, Alexandre Tacla, Animesh Datta, Sergio Boixo, Steve Flammia, Carlton Caves and Matthew Davis. *Quantum metrology from an information theory perspective*

38. Cedric Beny, Achim Kempf and David Kribs. *Quantum error correction for infinite-dimensional Hilbert spaces*

39. Peng Xue. *Quantum computing with dangling bonds on a silicon surface*

40. Nicolas Menicucci, Steve Flammia and Olivier Pfister. *One-way quantum computing in the optical frequency comb*

41. Andris Ambainis, Debbie Leung, Laura Mancinska and Maris Ozols. *Quantum random access codes with shared randomness*

42. Andrew Childs, Debbie Leung, Laura Mancinska and Maris Ozols. *Characterization of universal 2-qubit Hamiltonians*

43. Frédéric Dupuis. *The capacity of quantum channels with side information at the transmitter*

44. Marco Piani, Matthias Christandl, Pawel Horodecki and Caterina-Eloisa Mora. *Broadcast copies reveal quantumness of bipartite correlations*

45. Geza Toth and Juan Jose Garcia-Ripoll. *Efficient algorithm for multi-qudit twirling for ensemble quantum computation*

46. Elad Eban, Dorit Aharonov and Michael Ben-Or. *Interactive proofs for quantum computations*

47. Joseph Fitzsimons. *Quantum repetition encodings*

48. Or Sattath, Dorit Aharonov, Michael Ben-Or and Fernando Brandao. *The pursuit for uniqueness: extending Valiant-Vazirani theorem to the probabilistic and quantum settings*

49. David Menzies and Sarah Croke. *Approximating quantum operations using weak values*

50. Rolando Somma, Sergio Boixo, Howard Barnum and Emanuel Knill. *Quantum computing through decoherence and quantum simulated annealing*

51. William Matthews, Stephanie Wehner and Andreas Winter. *Distinguishability of quantum states under restricted families of measurements*

52. Elham Kashefi, Daniel Oi, Dan Browne, Erika Andersson and Janet Anders. *Twisted Graph states for ancilla-driven universal quantum computation*

53. Peter Shor, Graeme Smith, John Smolin and Bei Zeng. *Quantum error correction via codes over GF(3)*

54. Raisa Karasik, Karl-Peter Marzlin, Barry Sanders and Birgitta Whaley. *Avoiding irreversible dynamics in quantum Markovian systems*

55. Steve Flammia, Stephen Bartlett, David Gross and Rolando Somma. *Heralded polynomial-time quantum state tomography*

56. Retracted.

57. Retracted.

58. Jing Shu, Xu-Bo Zou, Yun-Feng Xiao and Guangcan Guo. *Quantum phase gate of photonic qubits in cavity QED system*

59. Lin Chen and Yi-Xin Chen. *Rank three bipartite entangled states are distillable*

60. Milos Drezgic, Andrew Hines, Mohan Sarovar and Shankar Sastry. *Complete characterization of mixing time for the continuous quantum walk on the hypercube with subspace projection decoherence model*

61. Seth Merkel, Gavin Brennen, Poul Jessen and Ivan Deutsch. *Quantum control of hyperfine spins with coherent electromagnetic fields*

62. Eric Chitambar and Runyao Duan. *Nonlocal entanglement transformations achievable by separable operations*

63. Gregory Crosswhite and Dave Bacon. *The great hunt for small subsystem codes*

64. Brian Mischuck, Ivan Deutsch and Poul Jessen. *Control of atomic wave functions in optical lattices*

65. Alina Vasilieva and Ruben Agadzanyan. *Quantum query algorithms for AND, OR and MAJORITY Boolean functions*

66. Paul Skrzypczyk, Nicolas Brunner and Sandu Popescu. *Emergence of quantum correlations from non-locality swapping*

67. Ligong Wang and Renato Renner. *One-shot classical capacities of quantum channels*

68. Michael Frey. *Quantum Fisher information associated with the qudit depolarizing channel*

69. Loïck Magnin, Nicolas J. Cerf and Frédéric Magniez. *Quantum bit-commitment with continuous-variables*

70. Yasuhito Kawano and Hiroshi Sekegawa. *Producing quantum circuits of the extended Clifford group*

71. Prabha Mandayam Doddamane and David Poulin. *Approximate quantum error correction*

72. Mayer Landau. *Convex roof calculations of the entanglement of harmonic oscillators interacting only via a reservoir*

73. Yoritoshi Adachi, Takashi Yamamoto, Masato Koashi and Nobuyuki Imoto. *Passive-decoy quantum key distribution with pseudo-single-photon sources*

74. Michael Frey and Michael Steiner. *Stern-Gerlach measurement with external coupling*

75. Toshiki Ide. *Violation of a local uncertainty relation in a photon telecloning*

76. Hugue Blier and Alain Tapp. *A quantum characterization of NP*

77. Olivier Landon-Cardinal and Richard MacKenzie. *Decoherence of a quantum reference frame*

78. Michael Zwolak. *Representing continuum environments*

79. Gabriela Lemos and Fabricio Toscano. *Can a chaotic environment with few degrees of freedom produce decoherence?*

80. Vincent Nesme, Holger Vogts, David Gross and Reinhard Werner. *Index theory for one-dimensional quantum walks and cellular automata*