

## **Good quantum codes with low-weight stabilizers**

Sergey Bravyi, IBM Watson Research Center

Tuesday, January 21, 2014, \*\* 2:00 pm, this week only \*\* 107 Annenberg

Quantum codes with low-weight stabilizers known as LDPC codes have been actively studied recently due to their potential applications in fault-tolerant quantum computing. However, all families of quantum LDPC codes known to this date suffer from a poor distance scaling limited by the square-root of the code length. This is in a sharp contrast with the classical case where good families of LDPC codes are known that combine constant encoding rate and linear distance.

In this talk I will describe the first family of good quantum codes with low-weight stabilizers. The new codes have a constant encoding rate, linear distance, and stabilizers acting on at most square root of  $n$  qubits, where  $n$  is the code length. For comparison, all previously known families of good quantum codes have stabilizers of linear weight. The proof combines two techniques: randomized constructions of good quantum codes and the homological product operation from algebraic topology. We conjecture that similar methods can produce good stabilizer codes with stabilizer weight  $n^a$  for any  $a > 0$ . Finally, we apply the homological product to construct new small codes with low-weight stabilizers.

This is a joint work with Matthew Hastings

Preprint: arXiv:1311.0885

## **Quantum Information, Entanglement, and Many-body Physics**

Fernando Brandao, University College London

Tuesday, January 28, 2014, 4:00 p.m. 114 East Bridge

Quantum information science has been developed in the past twenty years with an eye on future technologies, such as quantum computers and quantum cryptography. In this talk I will argue that the theory is also very useful as a tool for studying other areas of physics.

I will exemplify this feature mainly focusing on the problem of describing low-temperature states of quantum many-body models. I will show how both non-critical states in one-dimension and low-energy states in very large dimensions have a simple entanglement structure, thus being well describable by classical means. Both results will follow from the theory of entanglement originally developed for understanding the capabilities of quantum systems for information processing (in particular we will employ optimal protocols for entanglement distillation and an information-theoretic characterization of the so-called monogamy of entanglement).

Time permitting I will also briefly mention applications of quantum information theory to the study of the quantum-to-classical transition (in particular to the proposal termed quantum Darwinism) and to thermodynamics on the nanoscale. The talk will be geared at a general physics audience and no background on quantum information will be assumed.

## **Delegating Private Quantum Computations**

Anne Broadbent, University of Ottawa

Tuesday, February 11, 2014, 3:00 p.m. 107 Annenberg

Given the technological challenge in building quantum computers, it is likely that their initial availability will be in a client-server configuration. We address the question of privacy in this scenario, by showing that an almost-classical client can delegate the execution of any quantum computation, where the data uploaded to the server is encrypted via the one-time pad. In order to do this, the quantum power required of the client is limited to being able to prepare random BB84 states. We give a simulation-based security definition and a rigorous proof of security using a transformation to an entanglement-based protocol.

## **Physical Randomness Extractors**

Xiaodi Wu, MIT

Tuesday, February 18, 2014, 3:00 p.m. 107 Annenberg

How can one be certain that the output of an alleged random number generator is indeed random? This question is important not only for the security and the efficiency of modern day information processing, but also for understanding how fundamentally unpredictable events are possible in the physical world. The mathematical theory of randomness extraction from weak randomness sources shows that such certainty is possible only when two or more *\*independent\** sources are available. However, the independence requirement seems hard to enforce or even just to verify.

To circumvent this fundamental and hard-to-enforce limit, we propose a framework of extracting randomness from physical systems, and base the security on the validity of physical theories --we envision a scenario in which in addition to a weak random source, we have access to (multiple, spatially separated, untrusted) physical devices that may have been prepared by the adversary but are nevertheless constrained by quantum mechanics and special relativity. We require that, when the extraction procedure succeeds, the output randomness is close to uniform against any quantum adversary. We call such extraction procedure a *\*physical randomness extractor\**.

We construct the first physical randomness extractor for arbitrary min-entropy sources. Additionally, our extractor enjoys the desirable properties of being efficient and robustness. Specifically, to produce  $n$ -bits of certified randomness, our extractor takes a  $d = \text{poly}(\log(n))$  bits source with  $d^{\{0.1\}}$  bits of min-entropy (measured against the devices) and  $\text{poly}(n)$  devices and runs in  $\text{poly}(n)$  time. Our extractor is robust in the sense that it tolerates a constant level of implementation imprecision of the devices.

Our result enables practical and provably secure randomness generation with a minimal assumption on the randomness source and the generating devices. It also implies that unless the world is deterministic, we can experimentally create inherently random events and be confident of its unpredictability.

This is joint work with Kai-Min Chung and Yaoyun Shi.

## **On the Informational Completeness of Local Observables**

Isaac Kim, Perimeter Institute

Tuesday, March 11, 2014, 3:00 p.m. 107 Annenberg

For a general multipartite quantum state, we formulate a locally checkable constraint, under which the expectation values of certain nonlocal observables are completely determined by the expectation values of some local observables. The constraint is satisfied for ground states of gapped quantum many-body systems in one and two spatial dimensions, assuming a generic entanglement entropy scaling law holds. Its implications on quantum state tomography and quantum error correcting codes are discussed. On the quantum state tomography side, we establish nontrivial upper bound on the sample/measurement complexities. On the quantum error correcting code side, we provide an upper bound on the code distance, which is shown to be tight for a large class of known models.

## **Ultimate Communication Capacity of Quantum Optical Channels**

Raul Garcia-Patron, Universite Libre de Bruxelles

Tuesday, April 1, 2014, 3:00 p.m. 107 Annenberg

Optical channels, such as fibers or free-space links, are ubiquitous in today's telecommunication networks. A complete physical model of these channels must necessarily take quantum effects into account in order to determine their ultimate performances. Specifically, Gaussian bosonic quantum channels have been extensively studied over the past decades given their importance for practical purposes. In spite of this, a longstanding conjecture on the optimality of Gaussian encodings has yet prevented finding their communication capacity. In this talk we will present a recent result that solves this conjecture and establishes the ultimate achievable bit rate under an energy constraint. We will conclude discussing further implications of our result.

Joint work with V. Giovannetti, N. J. Cerf and A. S. Holevo

Reference: <http://arxiv.org/abs/1312.6225>

## **How "Quantum" is the D-Wave Machine?**

Seung Woo Shin, UC Berkeley

Tuesday, April 15, 2014, 3:00 p.m. 107 Annenberg

Recently there has been intense public interest in research surrounding the D-Wave "quantum computer". While claims about speedups over classical computers have been largely refuted, studies also claim that D-Wave machines exhibit signatures of "quantum behavior." In this talk, I will outline a very simple classical model which explains the published large scale input-output behavior of the D-Wave One machine. While raising serious questions about "how quantum" the D-Wave machine is, the new model also provides insights into the native problem solved by the D-Wave machine.

Joint work with Graeme Smith, John Smolin, and Umesh Vazirani

Reference: <http://arxiv.org/abs/1401.7087>

## **Harnessing Quantum Systems with Long-Range Interactions**

Alexey Gorshkov, Joint Quantum Institute

Tuesday, April 22, 2014, 3:00 p.m. 107 Annenberg

AMO (atomic, molecular, and optical) systems with long-range interactions, such as Rydberg atoms, polar molecules, and ions, are arguably the most controllable, tunable, and strongly interacting quantum systems. In this talk, we will first review how precise control over such systems has recently opened a new paradigm for quantum computing and communication, entanglement generation, and engineering of new phases of matter. Motivated by recent experiments, we will then focus on lattice systems with interactions featuring power-law decay with distance. In particular, we will derive a new bound on the propagation of information in such systems and exhibit a simple model that partially saturates the new bound [1]. The new bound is expected to provide crucial insights into numerous equilibrium and non-equilibrium phenomena in long-range-interacting systems and is on the verge of being verified experimentally by the trapped ion community [2,3].

[1] Z.-X. Gong, M. Foss-Feig, S. Michalakis, AVG, arXiv:1401.6174.

[2] P. Richerme, Z.-X. Gong, A. Lee, C. Senko, J. Smith, M. Foss-Feig, S. Michalakis, AVG, C. Monroe, arXiv:1401.5088 (Nature in press).

[3] P. Jurcevic, B. P. Lanyon, P. Hauke, C. Hempel, P. Zoller, R. Blatt, C. F. Roos, arXiv:1401.5387 (Nature in press).

## **Local tests of global entanglement and a counterexample to the generalized area law**

Daniel Nagaj, Simons Institute, UC Berkeley

Tuesday, May 6, 2014, 3:00 p.m. 107 Annenberg

We introduce a technique for applying quantum expanders in a distributed fashion, and use it to solve two basic questions: testing whether a bipartite quantum state shared by two parties is the maximally entangled state and disproving a generalized area law. In the process these two questions which appear completely unrelated turn out to be two sides of the same coin. Strikingly in both cases a constant amount of resources are used to verify a global property.

Joint work with Dorit Aharonov, Aram Harrow, Zeph Landau, Daniel Nagaj, Mario Szegedy, and Umesh Vazirani

### **Gauge Color Codes**

Hector Bombin, Perimeter Institute

Tuesday, May 13, 2014, 3:00 p.m. 107 Annenberg

Color codes are topological stabilizer codes with unusual transversality properties. I will show that their group of transversal gates only depends on the spatial dimension, not the local geometry. I will also introduce a generalized, gauge version of color codes. In 3D they allow the effectively transversal implementation of a universal set of gates by gauge fixing, while error-detecting measurements involve only 4 or 6 qubits. Furthermore, they do not require multiple rounds of error detection to achieve fault-tolerance.

### **Symmetry-Protected Topological Entanglement**

Iman Marvian, USC

Tuesday, May 20, 2014, 3:00 p.m. 107 Annenberg

We propose an order parameter for the Symmetry-Protected Topological (SPT) phases which are protected by Abelian on-site symmetries. This order parameter, called the "SPT entanglement", is defined as the entanglement between A and B, two distant regions of the system, given that the total charge (associated with the symmetry) in a third region C is measured and known, where C is a connected region surrounded by A and B and the boundaries of the system. In the case of 1-dimensional systems we prove that at the limit where A and B are large and far from each other compared to the correlation length, the SPT entanglement remains constant throughout a SPT phase, and furthermore, it is zero for the trivial phase while it is nonzero for all the non-trivial phases. Moreover, we show that the SPT entanglement is invariant under the low-depth quantum circuits which respect the symmetry, and hence it remains constant throughout a SPT phase in the higher dimensions as well. Finally, we show that the concept of SPT entanglement leads us to a new interpretation of the string order parameters, and based on this interpretation we propose an algorithm for extracting the relevant information about the SPT phase of the system from the string order parameters.

Reference: <http://arxiv.org/abs/1307.6617>

### **Rapid Mixing of Quantum Local Dissipative Systems**

Angelo Lucia, Universidad Complutense de Madrid

Tuesday, May 27, 2014, 3:00 p.m. 107 Annenberg

Open quantum systems weakly coupled to the environment are modelled by completely positive, trace preserving semigroups of linear maps. The generators of such evolutions are called Liouvillians, and similarly to the Hamiltonian in the case of coherent evolution, they encode the physical properties of the system. In the setting of quantum many-body systems on a lattice it is natural to consider local or exponentially decaying interactions. We will focus on the case of maps with a unique fixed point, and

consider the scaling of the mixing time with respect to the system size. In particular, if such scaling is sub-linear, a number of good properties of the evolution can be obtained: local observables are stable against perturbations, the fixed point has a finite correlation length, and in the case of frustration-free systems, satisfies an area law.

### **Quantum-proof extractors via operator space theory**

Omar Fawzi, ETH, Zurich

Randomness extractors are an important building block for classical and quantum cryptography. They are used for privacy amplification which is an essential step in quantum key distribution but also in many other protocols such as device independent randomness amplification and expansion. For most of these applications, it is important that the extractor be quantum-proof, i.e., be secure against quantum adversaries. It is known that some extractor constructions are quantum-proof whereas others are provably not. We argue that the theory of operator spaces offers a natural framework for studying to what extent extractors are secure in the presence of quantum adversaries.

In this talk, I will start by formulating the definition of extractors as a condition on the norm of an associated operator. Then, after introducing the basics of the theory of operator spaces, I will show that the definition of quantum-proof extractors can be formulated as a condition on the completely bounded norm of the same operator. As an application, we use Grothendieck's inequality to show that very high min-entropy extractors are always approximately quantum-proof.

This is joint work with Mario Berta and Volkher Scholz.

### **de Finetti Theorems: Quantum and Beyond**

Rotem Arnon-Friedman, ETH, Zurich

When analysing quantum information processing protocols one has to deal with large entangled systems, each consisting of many subsystems. It is therefore necessary to find some additional structure of the relevant state space, which can allow us to simplify the analysis. de Finetti theorems enable a substantially simplified analysis of information-processing tasks by giving us a way to relate states, which are symmetric under permutation of the subsystems, to states in which the subsystems are independent of each other. This relation plays an important role in various areas, e.g., in quantum cryptography or state tomography, where permutation invariant systems are ubiquitous. The known de Finetti theorems usually refer to the internal quantum state of a system and depend on its dimension. In this talk a different de Finetti theorem will be presented, where systems are modelled in terms of their statistics under measurements. This is necessary for a large class of applications widely considered today, such as device independent protocols, where the underlying systems and the dimensions are unknown.

In the talk I will explain the concept of de Finetti theorems, motivate the need for a device independent de Finetti theorem and present the new results.

Joint work with Renato Renner

Reference: <http://arxiv.org/abs/1308.0312>

### **A Non-commuting Stabilizer Formalism**

Oliver Buerschaper, Perimeter Institute

Tuesday, June 24, 2014, 3:00 p.m. 107 Annenberg

We propose a non-commutative extension of the Pauli stabilizer formalism. The aim is to describe a class of many-body quantum states which is richer than the standard Pauli stabilizer states. In our framework, stabilizer operators are tensor products of single-qubit operators drawn from the group  $\{\alpha I, X, S\}$ , where  $\alpha = \exp(i\pi/4)$  and  $S = \text{diag}(1, i)$ . We provide techniques to efficiently compute various properties related to bipartite entanglement, expectation values of local observables, preparation by means of quantum circuits, parent Hamiltonians etc. We also highlight significant differences compared to the Pauli stabilizer formalism. In particular, we give examples of states in our formalism which cannot arise in the Pauli stabilizer formalism, such as topological models that support non-Abelian anyons.

### **Strong converse bounds for quantum communication**

Mark Wilde, Louisiana State University

Tuesday, July 8, 2014, 3:00 p.m. 107 Annenberg

One of the main goals in quantum information theory is to establish the capacity of a quantum channel for communicating various kinds of information, whether it be bits or qubits. While several communication capacities of quantum channels are now known, the characterization of capacity in many of these cases is often limited to it being a threshold that determines the rates at which reliable communication is or is not possible. This characterization might be satisfactory for some purposes, but it leaves open the possibility for a trade-off between communication rate and error probability (that is, one might think that it would be possible to send data at a higher rate by allowing for errors to occur some of the time). However, we now know that such a trade-off is not possible for many quantum channels and capacities of interest. The seminar will focus on quantum communication capacity and a recent result establishing the Rains information of a quantum channel as a strong converse bound for quantum communication when using the channel many independent times. We also settle an open question posed by Rains, namely, to show that the Rains bound for entanglement distillation represents a strong converse rate for this task. The main application of our first result is to settle the strong converse question for the quantum capacity of all generalized dephasing channels.

This is joint work with Marco Tomamichel and Andreas Winter (arXiv:1406.2946).

## **Robust Quantum Random Number Generation**

Carl Miller, University of Michigan

Tuesday, July 22, 2014, 3:00 p.m. 107 Annenberg

Random numbers have countless applications, and so the kind of randomness postulated in quantum physics--"true randomness"--may be a vital resource. A line of research has developed whose goal is to harness this resource. The central goal is simple: construct a protocol which uses quantum devices to generate bits, and at the same time, certify that the bits are truly random. Crucially, the certification procedure must not depend on any prior trust in the accuracy of the devices.

Colbeck's thesis (2006) proposed a scheme for quantum random number generation. While the scheme is simple, its security proof was very challenging--the first (and only) previous full proof was given by Vazirani and Vidick in 2012.

In our work we have taken several steps forward from Vazirani-Vidick 2012 and brought quantum RNG close to the point of practical implementation. We have constructed a security proof that is robust (error-tolerant), that provides cryptographic security, and that is implementable with constant quantum memory. The proof invents multiple new techniques which we are hopeful will find applications elsewhere.

Joint work with Yaoyun Shi.

Reference: <http://arxiv.org/abs/1402.0489>

## **Infinite dimensional Adaptive Control for Quantum Systems**

Mark Balas, UWY, College of Engineering and Applied Science

Tuesday, July 29, 2014, 3:00 p.m. 107 Annenberg

Many control systems are inherently infinite dimensional when they are described by partial differential equations or have internal transport delays. Currently there is renewed interest in the control of these kinds of systems especially in flexible aerospace structures, smart electric power grids, and the quantum information and computing field. Since the dynamics of these systems will not be perfectly known, it is especially of interest to control these systems adaptively via low-order finite-dimensional controllers in the presence of persistent disturbances.

In our work, we have developed direct model reference adaptive control and disturbance rejection with very low-order adaptive gain laws for both large-scale finite dimensional systems and infinite dimensional systems whose states reside in a Hilbert Space. In this presentation I want to first give an introduction to some basic ideas in control theory, and then talk about some of our recent work in infinite dimensional control systems, and finally talk about how these ideas can be used in control of quantum systems to improve the transmission of quantum information. I think this will certainly be fun and how much profit, beyond intellectual capital, remains to be seen.

## **Plasmons, chirality, and electron energy-gain spectroscopy**

Ana Asenjo García, ICFO

Tuesday, August 12, 2014, 3:00 p.m. 107 Annenberg

In the first part of this talk, I will present some recent work on the interaction of plasmonic chiral matter with both circularly polarized light and vortex electron beams. For light, we compare the calculations based upon multiple scattering theory with recent observations of circular dichroism in plasmonic nanoparticles assembled using DNA origami. For electrons, we predict strong dichroism in the electron energy-loss spectroscopy (EELS) signal by using vortex beams. These electrons carry orbital angular momentum that can be exchanged in the interaction with chiral plasmons. We also predict a dichroic response when probing chiral biomolecules, which suggests the use of these vortex for resolving different enantiomers.

In the second part of the talk, I will address the phenomenon of plasmon-mediated electron energy gain, in which the interaction of swift electrons with strong evanescent light fields scattered by a nanostructure (e.g., by excitation of a plasmon by an external laser beam) can produce energy gains in the electrons and stimulated photon emission. This electron-light interaction can provide detailed information on the optical properties of the sampled nanostructures in the time and frequency domains. I will show that, taking advantage of plasmonic resonances, spectroscopy can be performed by varying the illumination frequency at remarkably low light intensities.

## **Entanglement in one-dimensional quantum systems**

Yichen Huang, UC Berkeley

Tuesday, October 14, 2014, 3:00 p.m. 107 Annenberg

Quantum entanglement, a concept from quantum information theory, has been widely used in condensed matter physics to characterize quantum correlations that are difficult to study using conventional methods. It provides unique insights into the physics of critical states and topological order. It is also quantitatively related to the difficulty of describing ground states using matrix-product-state representations in numerical approximations. In this talk, I will discuss some recent examples in these directions in the context of 1D quantum systems. I will focus on conceptual messages rather than technical perspectives.

Area law: Starting with a review of known rigorous results on the relation between gapped states, correlation decay, area law, and efficient matrix-product-state representations, I will discuss area law for Renyi entropy and possible generalizations in the presence of ground-state degeneracy.

Entanglement and topological order: It is argued that topological order is essentially a pattern of long-range entanglement. I will discuss a quantitative characterization of long-range entanglement using local quantum circuits. In particular, I will show that to generate a topologically ordered state from a product state a local quantum circuit of linear (in system size) depth is necessary and (up to small errors) sufficient.

Entanglement in critical disordered systems: Many-body localization studies how disorder leads to localized states in strongly correlated systems. It is a property associated with all eigenstates (not just the ground state) of disordered systems. I will show how to use entanglement for probing the

singularities of all eigenstates.

References:

<http://arxiv.org/abs/1403.0327>

<http://arxiv.org/abs/1401.3820>

<http://arxiv.org/abs/1405.1817>

### **Information Causality, Szemerédi-Trotter, and algebraic variants of CHSH**

Mohammad Bavarian, MIT

Tuesday, November 18, 2014, 3:00 p.m. 107 Annenberg

In this work, we consider the following family of two prover one-round games. In the  $\text{CHSH}_q$  game, two parties are given  $x, y$  in  $F_q$  uniformly at random, and each must produce an output  $a, b$  in  $F_q$  without communicating with the other. The players' objective is to maximize the probability that their outputs satisfy  $a + b = xy$  in  $F_q$ . This game was introduced by Buhrman and Massar (PRA 2005) as a large alphabet generalization of the celebrated CHSH game---which is one of the most well-studied two-prover games in quantum information theory, and which has a large number of applications to quantum cryptography and quantum complexity. Our main contributions in this paper are the first asymptotic and explicit bounds on the entangled and classical values of  $\text{CHSH}_q$ , and the realization of a rather surprising connection between  $\text{CHSH}_q$  and geometric incidence theory. On the way to these results, we also resolve a problem of Pawłowski and Winter about pairwise independent Information Causality, which, beside being interesting on its own, gives as an application a short proof of our upper bound for the entangled value of  $\text{CHSH}_q$ .

Joint work with Peter W. Shor.