Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

QIP 2010

15th – 22nd January, Zürich, Switzerland

Tutorial and Scientific Programmes

Friday, 15th January

10:00 – 17:10 Jiannis Pachos (Univ. Leeds)

Why should anyone care about computing with anyons?

This is a short course in topological quantum computation. The topics to be covered include:

1. Introduction to anyons and topological models.
2. Quantum Double Models. These are stabilizer codes, that can be described very much like quantum error correcting codes. They include the toric code and various extensions.
3. The Jones polynomials, their relation to anyons and their approximation by quantum algorithms.
4. Overview of current state of topological quantum computation and open questions.

Saturday, 16th January

9:00 – 10:35 Pawel Horodecki (Gdańsk Univ. Tech.)

Additivity of channel capacities

In the introduction of this tutorial review the general additivity problem will be defined in terms of quantum resources. Early illuminative examples of superadditivity of quantum resources in terms of entanglement called activation and superactivation effects will be explained.

Then the additivity problem for channel capacity will be defined. Special examples of channels important in this context will be discussed. Some of the superadditivity results provided recently by numerous authors in the quantum communication field for chosen channel capacities will be explained and discussed.

Some remaining open additivity problems will be discussed.

11:00 – 12:35 Graeme Smith (IBM, Watson)

Regularization and its discontents

The cornerstone of information theory is Shannon's theorem, which shows that the capacity of a channel for noiseless communication is given by a simple optimization problem: it is the maximum mutual information that can be generated between input and output with a single use of the channel. In the quantum setting, such "single-letter" formulas are few and far between. The best expressions we have for quantum capacities involve optimizations of entropic quantities over an asymptotically large number of channel uses. Such "regularized" formulas tell us very little. The purpose of this talk is to give an overview of what we know about this need for regularization, when and why it happens, and what it means. I will focus on the quantum capacity of a quantum channel, which is the case we understand best.

15:00 – 16:55 Daniel Nagaj (Slovak Academy of Sciences)

Local Hamiltonians in quantum computation

This talk is about two Hamiltonian Complexity questions. First, how hard is it to compute the ground state properties of quantum systems with local Hamiltonians? Second, which spin systems with time-independent (and perhaps, translationally-invariant) local interactions could be used for universal computation?

Aiming at a participant without previous understanding of complexity theory, we will discuss two locally-constrained quantum problems: k-local Hamiltonian and quantum k-SAT. Learning the techniques of Kitaev and others along the way, our first goal is the understanding of QMA-completeness of these problems. The second goal is an up-to-date review of results in this field, including QMA-complete problems with restricted geometry of interactions and new universal constructions with a connection to Adiabatic Quantum Computing.

Sunday, 17th January

15:00 – 17:45 Ignacio Cirac (MPQ Garching)

Classical simulation of many-body quantum systems

Many body quantum systems are very hard to describe due to the exponential increase of the number of parameters with the number of particles. During the last years different methods have been envisioned in order to find efficient descriptions of certain many-body quantum states. Those methods are based on families of states which can be expressed in terms of few tensors. The corresponding families include Matrix Product States, Projected Entangled-Pair States, Multi-Scale Renormalization Ansatz, or Tensor-Tree states. In this lecture I will introduce those families of states, describe their properties, and show how they can be used in order to efficiently describe many-body quantum systems; in particular, those occurring in certain condensed matter problems.

Monday, 18th January

9:25 – 10:20 Umesh Vazirani (UC Berkeley)

New bridges between Computer Science and Quantum Computation

Perspective talk.

10:55 – 11:25 Daniel Gottesman (Perimeter Institute)

The quantum and classical complexity of translationally invariant tiling and Hamiltonian problems

(joint work with Sandy Irani)

We study the complexity of a class of problems involving satisfying constraints which remain the same under translations in one or more spatial directions. In this paper, we show hardness of a classical tiling problem on an (N x N) 2-dimensional grid and the problem of finding the ground state energy of a 1-dimensional quantum system of N particles. In both cases, the only input is N, provided in binary. We show that the classical problem is NEXP-complete and the quantum problem is QMAEXP-complete. Thus, an algorithm for these problems that runs in time polynomial in N (exponential in the input size) would imply EXP = NEXP or BQEXP = QMAEXP, respectively. Although tiling in general is already known to be NEXP-complete, to our knowledge, all previous reductions require that either the set of tiles and their constraints or some varying boundary conditions be given as part of the input. In the problem considered here, these are fixed, constant-sized parameters of the problem. Instead, the problem instance is encoded solely in the size of the system.

11:30 – 11:50 Iordanis Kerenidis (CNRS – Univ. Paris-Sud)

On the power of a unique quantum witness

(joint work with Rahul Jain, Greg Kuperberg, Miklos Santha, Or Sattath, and Shengyu Zhang)

In a celebrated paper, Valiant and Vazirani raised the question of whether the difficulty of NP-complete problems was due to the wide variation of the number of witnesses of their instances. They gave a strong negative answer by showing that distinguishing between instances having zero or one witnesses is as hard as recognizing NP, under randomized reductions.

We consider the same question in the quantum setting and investigate the possibility of reducing quantum witnesses in the context of the complexity class QMA, the quantum analogue of NP. The natural way to quantify the number of quantum witnesses is the dimension of the witness subspace W in some appropriate Hilbert space H. We present an efficient deterministic procedure that reduces any problem where the dimension d of W is bounded by a polynomial to a problem with a unique quantum witness. The main idea of our reduction is to consider the Alternating subspace of the d-th tensor power of H. Indeed, the intersection of this subspace with the d-th tensor power of H is one-dimensional, and therefore can play the role of the unique quantum witness.

11:55 – 12:15 Scott Aaronson (MIT)

A full characterization of quantum advice

(joint work with Andrew Drucker)

We prove the following surprising result: given any state rho on n qubits, there exists a local Hamiltonian H on poly(n) qubits (e.g., a sum of two-qubit interactions), such that any ground state of H can be used to simulate rho on all quantum circuits of fixed polynomial size. In complexity terms, this implies that BQP/qpoly is contained in QMA/poly, which supersedes the previous result that BQP/qpoly is contained in PP/poly and refutes a conjecture made by Aaronson in 2004: Indeed, we can exactly characterize quantum advice, as equivalent in power to untrusted quantum advice combined with trusted classical advice.

One implication of our result is that it is possible to send both a quantum state rho and a polynomially-larger classical string x through a one-way communication channel, in such a way that the recipient can use x to verify (in polynomial time) that rho still produces the measurement outcomes that the sender intended on every small circuit. Another implication is a quantum analogue of the famous Karp-Lipton Theorem: if NP-complete problems are efficiently solvable by quantum computers with quantum advice, then Pi2P is contained in QMA^PromiseQMA. Proving our main result requires combining a large number of previous tools and also creating some new ones. In particular, we need a result of Aaronson on the learnability of quantum states, a result of Aharonov and Regev on "QMA_+ super-verifiers," and a result of Alon et al. on fat-shattering dimension of concept classes. The main new tool is a so-called Majority-Certificates Lemma, which has already found some independent applications in complexity theory. In its simplest version, this lemma says the following. Given any set S of Boolean functions on n variables, any function f in S can be expressed as the pointwise majority of m=O(n) other functions in S---f(x)=MAJ(f1(x),...,fm(x))---such that each fi is the unique function in S compatible with O(log|S|) input/output constraints.

14:45 – 15:40 Rahul Jain (NU Singapore)

QIP = PSPACE

(joint work with Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous)

We prove that the complexity class QIP, which consists of all problems having quantum interactive proof systems, is contained in PSPACE, the class of problems that can be solved in polynomial space. This containment is proved by applying a parallelized form of the matrix multiplicative weights update method to a class of semi-definite programs that captures the computational power of quantum interactive proofs. As the containment of PSPACE in QIP follows immediately from the well-known equality IP = PSPACE, the equality QIP = PSPACE follows.

15:45 – 16:05 Stefano Pironio (Univ. Libre Bruxelles)

Random numbers certified by Bell's theorem

(joint work with Antonio Acin, Antoine Boyer de la Giroday, and Serge Massar)

Randomness is difficult to characterize mathematically, and its generation must rely on an unpredictable physical process. Inaccuracies in the theoretical modelling of such processes or failures of the devices, possibly due to adversarial attacks, limit the reliability of random number generators in ways that are difficult to control and detect.

Here, we show that the non-local correlations of entangled quantum particles can be used to produce private randomness without the need for any assumptions on the internal working of the devices used in the generation. This strong form of randomness generation is impossible classically and possible in quantum systems only if certified by a Bell inequality violation.

More spefically, we show that untrusted devices that violate a Bell inequality can be used as "randomness expanders", where a small private random seed of size O($\sqrt{n}$ log$\sqrt{n}$) is expanded into a longer private random string. Although the final output string may not be uniformly random, our analisis guarantees that it contains at least O(n) bits of entropy. With the help of a small initial private random seed, the output string can then be classically processed using a randomness extractor to convert it into a string of size O(n) that is nearly uniform and uncorrelated to the information of an adversary.

16:10 – 16:30 Steve Flammia (Perimeter Institute)

Adiabatic gate teleportation

(joint work with Dave Bacon)

The difficulty in producing precisely timed and controlled quantum gates is a significant source of error in many physical implementations of quantum computers. Here we introduce a simple universal primitive, adiabatic gate teleportation, which is robust to timing errors and many control errors and maintains a constant energy gap throughout the computation above a degenerate ground state space. Notably this construction allows for geometric robustness based upon the control of two independent qubit interactions. Further, our piecewise adiabatic evolution easily relates to the quantum circuit model, enabling the use of standard methods from fault-tolerance theory for establishing thresholds. The method also allows for a detailed analysis of adiabatic braiding of topological quasiparticles as well as a new hybrid model of quantum computing that uses aspects of the adiabatic and measurement-based models. A more detailed presentation of the main results concerning adiabatic gate teleportation can be found in D. Bacon and S. T. Flammia, Phys. Rev. Lett. 103, 120504 (2009).

Tuesday, 19th January

9:15 – 10:10 Ben Reichardt (Univ. Waterloo)

Span programs and quantum algorithms

We show that the general adversary lower bound on quantum query complexity is nearly tight, by giving a matching quantum walk algorithm. The result gives a new semi-definite program for quantum query complexity, and shows an equivalence to the span program model of computation. Span programs compose easily, and this yields a quantum recursion method. Classical algorithms cannot compose in this way. Applying the technique to solve problems defined recursively with independent inputs, i.e., to evaluating formulas, gives an optimal quantum formula-evaluation algorithm. Span programs are a promising model for developing more quantum algorithms.

10:15 – 10:35 David Gross (Univ. Hannover)

Non-commutative compressed sensing: theory and applications for quantum tomography

(joint work with Yi-Kai Liu, Steven Flammia, Stephen Becker, and Jens Eisert)

We establish novel methods for quantum state and process tomography based on compressed sensing. Our protocols require only simple Pauli measurements, and use fast classical post-processing based on convex optimization. Using these techniques, it is possible to reconstruct an unknown density matrix of rank r using $O(r\ d\ log\ d)$ measurement settings, a significant improvement over standard methods that require d^2 settings. The protocols are stable against noise, and extend to states which are approximately low-rank. The acquired data can be used to certify that the state is indeed close to a low-rank one, so no *a priori* assumptions are needed. We present both theoretical bounds and numerical simulations.

At the same time, new mathematical methods for analyzing the problem of low-rank matrix recovery have been obtained. The methods are both considerably simpler, and more general than previous approaches. It is shown that an unknown d x d matrix of rank r can be efficiently reconstructed given knowledge of only $O(d\ r\ v\ log^2 d)$ randomly sampled expansion coefficients with respect to any given matrix basis. The number v quantifies th e "degree of incoherence'' between the unknown matrix and the basis. Existing work concentrated mostly on the problem of "matrix completion'', where one aims to recover a low-rank matrix from randomly selected matrix elements. Our result covers this situation as a special case. The proof consists of a series of relatively elementary steps, which stands in contrast to the highly involved methods previously employed to obtain comparable results. We discuss operator bases which are incoherent to all low-rank matrices simultaneously. For these bases, we show that $O(d\ r\ v\ log\ d)$ randomly sampled expansion coefficients suffice to recover any low-rank matrix with high probability.

11:10 – 11:40 Norbert Schuch (MPI Garching)

An efficient algorithm for finding Matrix Product ground states

(joint work with J. Ignacio Cirac, Dorit Aharonov, Itai Arad, and Sandy Irani)
The Density Matrix Renormalization Group (DMRG) algorithm, a variational method over the class of Matrix Product States (MPS), is the most successful algorithm for finding ground states of one-dimensional Hamiltonians. However, there is no converge proof for DMRG, and in fact hard instances can be constructed. In this talk, we describe an algorithm which efficiently solves the optimization problem encountered in DMRG, in a time which scales polynomially in the accuracy and the length of the chain, and exponentially in the so-called bond dimension. In practice, logarithmic bond dimensions often suffice for a good approximation of ground states, leading to a quasi-polynomial scaling. This scaling is optimal, since the problem is known to be NP-hard for a polynomial bond dimension.

11:45 – 12:05 Dominic W. Berry (Caltech)

The query complexity of Hamiltonian simulation and unitary implementation

(joint work with Andrew M. Childs)
We present a general method for simulating a Hamiltonian given a black box for its matrix elements in a fixed basis. This method improves upon previous simulations of sparse Hamiltonians, but also applies to the non-sparse case. A major application is the implementation of black-box unitary transformations. We show how to implement a general $N \times N$ unitary transformation with bounded error using $\tilde{O}(N^{2/3})$ queries to a black box for its entries (ignoring logarithmic factors). In fact, except in pathological cases, it appears that the implementation can be performed with only $\tilde{O}(N^{1/2})$ queries, which is optimal. In contrast, standard methods use $\tilde{O}(N^2)$ elementary operations.

12:10 – 12:30 Maarten Van den Nest (MPQ Garching)

Simulating quantum computers with probabilistic methods

We investigate the boundary between classical and quantum computational power. This work consists of two parts.
First we develop novel classical simulation techniques that are centered around sampling methods. Using these techniques we generate new classes of simulatable quantum circuits, where standard techniques relying on the exact computation of measurement probabilities fail to provide efficient simulations. For example, we derive a criterion to assess when the concatenation of two simulatable quantum circuits remains simulatable, and use this to show that the concatenation of matchgate, Toffoli, Clifford, bounded-depth circuits, and others, remains simulatable. We also show that sparse quantum circuits can be simulated efficiently classically, as well as circuits composed of CNOT and exp[iθX] gates.
In a second part, we apply our results to the simulation of quantum algorithms. It is shown that a recent quantum algorithm, concerned with the estimation of Potts model partition functions, can be simulated efficiently classically. Finally, we show that the speed-ups of Simon's and Shor's algorithms crucially depend on the very last stage in these algorithms, dealing with the classical postprocessing of the measurement outcomes. Specifically, we prove that both algorithms would become classically simulatable if the function classically computed in this step had a sufficiently peaked Fourier spectrum.

15:00 – 15:55 Philippe Corboz (Univ. Queensland)

Simulation of fermionic lattice models in two dimensions with tensor network algorithms

The numerical simulation of strongly correlated fermionic systems in two dimensions is one of the biggest challenges in computational physics. Borrowing ideas and tools from quantum information and computation, a new generation of simulation techniques for many-body systems, the so-called tensor network algorithms (e.g. PEPS, MERA), have been proposed in the last few years. Given e.g. a 2D lattice system governed by a local Hamiltonian H, a tensor network algorithm attempts to approximate the ground state of H by means of a (in general non-unitary) quantum circuit. The efficiency of simulations depends directly on the amount of entanglement in the ground state of H, with the success of tensor network algorithms being closely related to the so-called "area law" for entanglement entropy. By considering a quantum circuit made of fermions, tensor network algorithms have been recently extended to fermionic systems, thereby offering a new promising way to address long standing problems in condensed matter physics, such as the Hubbard model, which is conjectured to be the key model of high-temperature superconductors. After presenting a general overview on tensor network algorithms, I will discuss the most recent developments involving the simulation of fermions.

16:00 – 16:20 Hari Krovi (NEC Lab.)

Adiabatic quantum optimization fails for random instances of NP-complete problems

(joint work with Boris Altshuler and Jérémie Roland)
Adiabatic quantum optimization has attracted a lot of attention because small scale simulations gave hope that it would allow to solve NP-complete problems efficiently. Later, negative results proved the existence of specifically designed hard instances where adiabatic optimization requires exponential time. In spite of this, there was still hope that this would not happen for random instances of NP-complete problems. This is an important issue since random instances can be considered as a good model for instances typically encountered in practical applications. Here, we will show that because of a phenomenon similar to Anderson localization, an exponentially small eigenvalue gap appears in the spectrum of the

adiabatic Hamiltonian for large random instances, very close to the end of the algorithm. This implies that unfortunately, adiabatic quantum optimization also fails for these instances by getting stuck in a local minimum, unless the computation is exponentially long.

16:55 – 17:25 Kristan Temme (Univ. Vienna)

Quantum metropolis sampling

(joint work with Tobias Osborne, Karl Gerd Vollbrecht, David Poulin, and Frank Verstraete)

Quantum computers have emerged as the natural architecture to study the physics of strongly correlated many-body quantum systems, thus providing a major new impetus to the field of many-body quantum physics. While the method of choice for simulating classical many-body systems has long since been the ubiquitous Monte Carlo method, the formulation of a generalization of this method to the quantum regime has been impeded by the fundamental peculiarities of quantum mechanics, including, interference effects and the no-cloning theorem. In this report, we overcome those difficulties by constructing an efficient quantum algorithm to sample from the Gibbs distribution of an arbitrary quantum Hamiltonian at arbitrary temperatures, both for bosonic and fermionic systems. This validates the quantum computer as a full quantum simulator, with a wealth of possible applications to quantum chemistry, condensed matter physics and high energy physics.

17:30 – 17:50 Sergey Bravyi (IBM)

Tradeoffs for reliable quantum information storage in 2D systems

(joint work with David Poulin, and Barbara Terhal)

We ask whether there are fundamental limits on storing quantum information reliably in a bounded volume of space. To investigate this question, we study quantum error correcting codes specified by geometrically local commuting constraints on a 2D lattice of finite-dimensional quantum particles. For these 2D systems, we derive a tradeoff between the number of encoded qubits k, the distance of the code d, and the number of particles n. It is shown that $kd^2=O(n)$, where the coefficient in $O(n)$ depends only on the locality of the constraints and dimension of the Hilbert spaces describing individual particles. We show that the analogous tradeoff for the classical information storage is $k\, d^{1/2} =O(n)$.

Wednesday, 20th January

9:00 – 9:55 André Chailloux (Univ. Paris-Sud)

Quantum coin flipping

(joint work with Iordanis Kerenidis)

Coin flipping is a fundamental cryptographic primitive that enables two distrustful and far apart parties to create a uniformly random bit. Quantum information allows for protocols in the information theoretic setting where no dishonest party can perfectly cheat. The previously best-known quantum protocol by Ambainis achieved a cheating probability of at most 3/4: On the other hand, Kitaev showed that no quantum protocol can have cheating probability less than 1/sqrt(2). Closing this gap has been one of the important open questions in quantum cryptography.

In this talk, we will present a quantum strong coin flipping protocol with cheating probability arbitrarily close to 1/sqrt(2). More precisely, we will show how to use any weak coin flipping protocol with cheating probability 1/2 + ε in order to achieve a strong coin flipping protocol with cheating probability 1/sqrt(2) + O(ε). The optimal quantum strong coin flipping protocol follows from our construction and the optimal quantum weak coin flipping protocol described by Mochon. In the second part of the talk, we will describe Kitaev's formalism for coin flipping and how it was used by Mochon for the construction of the optimal weak coin flipping protocol.

10:00 – 10:20 Andreas Winter (NU Singapore / Univ. Bristol)

Highly entangled states with almost no secrecy

(joint work with Matthias Christandl and Norbert Schuch)

We illuminate the relation between entanglement and secrecy by providing the first example of a quantum state that is highly entangled, but from which, nevertheless, almost no secrecy can be extracted. More precisely, we provide two bounds on the bipartite entanglement of the totally antisymmetric state in dimension d x d. First, we show that the amount of secrecy that can be extracted from the state is low, to be precise it is bounded by O(1/d). Second, we show that the state is highly entangled in the sense that we need a large amount of singlets to create the state: entanglement cost is larger than a constant, independent of d. Our findings also clarify the relation between the squashed entanglement and the relative entropy of entanglement.

10:25 – 10:45 Thomas Vidick (UC Berkeley)

Improved extractors against bounded quantum storage

(joint work with Anindya De)

We give near-optimal constructions of extractors secure against quantum bounded-storage adversaries. One instantiation gives the first such extractor to achieve an output length Theta(K-b), where K is the source's entropy and b the adversary's storage, depending linearly on the adversary's amount of storage, together with a poly-logarithmic seed length. Another instantiation achieves a logarithmic key length, with a slightly smaller output length Theta((K-b)/K^g) for any g>0. In contrast, the previous best construction [Ta-Shma, STOC'09] could only extract (K/b)^(1/15) bits.

Our construction follows Trevisan's general reconstruction paradigm, and in fact our proof of security shows that essentially all extractors constructed using this paradigm are secure against quantum storage, with optimal parameters. Our argument is based on bounds for a generalization of quantum random access codes, which we call quantum functional access codes. This is crucial as it lets us avoid the local list-decoding algorithm central to the approach in [Ta-Shma, STOC'09] which was the source of the multiplicative overhead. Some of our constructions have the additional advantage that every bit of the output is a function of only a polylogarithmic number of bits from the source, which is crucial for some cryptographic applications.

11:10 – 11:40 Carolin Lunemann (Aarhus Univ.)

Improving the security of quantum protocols via commit-and-open

(joint work with Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner)

We consider two-party quantum protocols starting with a transmission of some random BB84 qubits followed by classical messages. We show a general compiler, improving the security of such protocols: if the original protocol is secure against an "almost honest" adversary, then the compiled protocol is secure against an arbitrary computationally bounded (quantum) adversary. The compilation preserves the number of qubits sent and the number of rounds up to a constant factor. The compiler also preserves security in the bounded-quantum-storage model (BQSM), so if the original protocol was BQSM-secure, the compiled protocol can only be broken by an adversary who has large quantum memory and large computing power. This is in contrast to known BQSM-secure protocols, where security breaks down completely if the adversary has larger quantum memory than expected. We show how our technique can be applied to quantum identification and oblivious transfer protocols.

11:45 – 12:15 Stephanie Wehner (Caltech)

Unconditional security from noisy quantum storage

(joint work with Robert Koenig and Juerg Wullschleger)

We consider the implementation of two-party cryptographic primitives based on the sole assumption that no large-scale reliable quantum storage is available to the cheating party. We construct novel protocols for oblivious transfer and bit commitment, and prove that realistic noise levels provide security even against the most general attack. Such unconditional results were previously only known in the so-called bounded-storage model which is a special case of our setting. Our protocols can be implemented with present-day hardware used for quantum key distribution. In particular, no quantum storage is required for the honest parties.

12:20 – 12:50 Vincent Nesme (Caltech)

Unitarity plus causality implies localizability

(joint work with Pablo Arrighi and Reinhard Werner)

We consider a graph with a single quantum system at each node. The entire compound system evolves in discrete time steps by iterating a global evolution *U*. We require that this global evolution *U* be unitary, in accordance with quantum theory, and that this global evolution *U* be causal, in accordance with special relativity. By causal we mean that information can only ever be transmitted at a bounded speed, the speed bound being quite naturally that of one edge of the underlying graph per iteration of *U*. We show that under these conditions the operator *U* can be implemented locally; i.e. it can be put into the form of a quantum circuit made up with more elementary operators -each acting solely upon neighbouring nodes. We take quantum cellular automata as an example application of this representation theorem: this analysis bridges the gap between the axiomatic and the constructive approaches to defining QCA. Based on arXiv:0711.3975.

Thursday, 21st January

9:15 – 10:10 Aram Harrow (Univ. Bristol)

Quantum algorithms for linear systems of equations

(joint work with Avinatan Hassidim and Seth Lloyd)

Solving linear systems of equations is a common problem that arises both on its own and as a subroutine in more complex problems: given a matrix A and a vector b, find a vector x such that Ax=b. We consider the case where one doesn't need to know the solution x itself, but rather an approximation of the expectation value of some operator associated with x, e.g., x'Mx for some matrix M. In this case, when A is sparse, N by N and has condition number k, classical algorithms can find x and estimate x'Mx in O(N sqrt(k)) time. Here, we exhibit a quantum algorithm for this task that runs in poly(log N, k) time, an exponential improvement over the best classical algorithm. Based on arXiv:0811.3171v3.

10:15 – 10:35 Stefano Chesi (Univ. Basel)

Stability of topological quantum memories in contact with a thermal bath

(joint work with Beat Röthlisberger, Daniel Loss, Sergey Bravyi, and Barbara M. Terhal)

We discuss several aspects related to the thermal stability of quantum memories. These are typically represented by spin lattice Hamiltonians encoding one or several qubits in a degenerate eigenspace. A self-correcting quantum memory has an infinite lifetime in the thermodynamic limit, even if the individual spins of the lattice are short-lived. While several candidate quantum memories were proposed to be self-correcting, many have revealed inadequate or difficult to analyze. In our work: a) We discuss general criteria to establish the stability of a quantum memory and derive a rigorous upper bound to the relaxation rate of a general quantum memory and b) We examine a generalization of the two-dimensional toric code which includes long-range repulsive interactions. By analytical arguments and direct numerical simulations we establish that such long-range interactions lead to stable memories. The lifetime scales polynomially with system size and the exponent is large for a super-ohmic thermal environment. We also show that such long-range interactions are physically relevant.

11:10 – 11:40 Robert Koenig (Caltech)

Quantum computation with Turaev-Viro codes

(joint work with Greg Kuperberg, and Ben Reichardt)

The Turaev-Viro invariant for a closed three-manifold is defined as the contraction of a certain tensor network. The tensors correspond to tetrahedra in a triangulation of the manifold, with values determined by a fixed spherical category. For a manifold with boundary, the tensor network has free indices that can be associated to qudits, and its contraction gives the coefficients of a quantum error-correcting code. The code has local stabilizers determined by Levin and Wen. For example, applied to the genus-one handlebody using the Z2 category, this construction yields the well-known toric code.

For other categories, such as the Fibonacci category, the construction realizes a non-abelian anyon model over a discrete lattice. By studying braid group representations acting on equivalence classes of colored ribbon graphs embedded in a punctured sphere, we identify the anyons, and give a simple recipe for mapping fusion basis states of the doubled category to ribbon graphs (Levin-Wen string nets). We explain how suitable initial states can be prepared efficiently, how to implement braids, by successively changing the triangulation using a fixed five-qudit local unitary gate, and how to measure the topological charge. Combined with known universality results for anyonic systems, this provides a large family of schemes for quantum computation based on local deformations of stabilizer codes. These schemes may serve as a starting point for developing fault-tolerance schemes using continuous stabilizer measurements and active error-correction.

11:45 – 12:05 Mark Howard (UC Santa Barbara)

Tight noise thresholds for quantum computation with perfect stabilizer operations

(joint work with Wim van Dam)

We study how much noise can be tolerated by a universal gate set before it loses its quantum-computational power. Specifically we look at circuits with perfect stabilizer operations in addition to imperfect non-stabilizer gates.

We prove that for all unitary single-qubit gates there exists a tight depolarizing noise threshold that determines whether the gate enables universal quantum computation or if the gate can be simulated by a mixture of Clifford gates. This exact threshold is determined by the Clifford polytope spanned by the 24 single-qubit Clifford gates.

The result is in contrast to the situation wherein non-stabilizer qubit states are used; the thresholds in that case are not currently known to be tight.

12:10 – 12:30 Hui Khoon Ng (Caltech)

A simple approach to approximate quantum error correction

(joint work with Prabha Mandayam)

We demonstrate that there exists a universal, near-optimal recovery map---the transpose channel ---for approximate quantum error-correcting codes, where optimality is defined using the worst-case fidelity. Using the transpose channel, we provide an alternative interpretation of the standard quantum error correction (QEC) conditions, and generalize them to a set of conditions for approximate QEC (AQEC) codes. This forms the basis of a simple algorithm for finding AQEC codes. This analytical result is compared with earlier work that relies on exhaustive numerical search for the optimal recovery map, with optimality defined based on entanglement fidelity. For the practically more relevant case of codes encoding a single qubit of information, our algorithm is particularly easy to implement.

15:00 – 15:30 Roderich Moessner (MPI-PKS Dresden)

Random quantum satisfiability: statistical mechanics of disordered quantum optimization

(joint work with Sergey Bravyi, Cristopher Moore, Alexander Russell, Christopher Laumann, Andreas Läuchli, Antonello Scardicchio, and Shivaji Sondhi)

We report a cluster of results on random quantum k-QSAT formulas with M clauses and N qubits. In this approach, the clause density M/N acts as a control parameter with which to tune one's attention from low density, easily satisfied to high density, highly frustrated instances of QSAT. We characterize the phase diagram of random k-QSAT using several complementary approaches. We examine unentangled (product) satisfying states and discover a geometric criterion for deciding when a QSAT interaction graph is generically product satisfiable. Applied to the random graph ensemble, this criterion provides improved lower bounds on the location of the SAT--UNSAT transition. Coupled with recent work on the quantum Lovasz local lemma, this shows the existence of an entanglement transition in the satisfying space of the random ensemble at large k. For k=3 and k=4, we present numerical results which provide mild evidence for a similar transition at smaller k. Finally, we examine the UNSAT regime and improve the upper bound on the SAT-UNSAT threshold. We show that the threshold for random quantum k-SAT is strictly less than the conjectured classical k-SAT threshold. These bounds work by determining the generic dimension of the satisfying subspace for certain gadgets, and then using differential equations to analyze algorithms that partition the hypergraph of clauses into a collection of these gadgets. The use of differential equation to establish upper bounds on a satisfiability threshold appears to be novel, and our techniques may apply to various classical problems as well.

15:35 – 16:30 Julia Kempe (Tel Aviv Univ.)

A quantum Lovász Local Lemma

(joint work with Andris Ambainis and Or Sattath)

The Lovász Local Lemma (LLL) is a powerful tool in probability theory to show the existence of combinatorial objects meeting a prescribed collection of “weakly dependent” criteria. We show that the LLL extends to a much more general geometric setting, where events are replaced with subspaces and probability is replaced with relative dimension, which allows to lower bound the dimension of the intersection of vector spaces under certain independence conditions.

Our result immediately applies to the k-QSAT problem: For instance we show that any collection of rank 1 projectors with the property that each qubit appears in at most $2^k/(e \cdot k)$ of them, has a joint satisfiable state.

We then apply our results to the recently studied model of random k-QSAT. Recent works have shown that the satisfiable region extends up to a density of 1 in the large k limit, where the density is the ratio of projectors to qubits. Using a hybrid approach building on work by Laumann et al. (also presented at QIP) we greatly extend the known satisfiable region for random k-QSAT to a density of $\Omega(2^k/k^2)$. Since our tool allows us to show the existence of joint satisfying states without the need to construct them, we are able to penetrate into regions where the satisfying states are conjectured to be entangled, avoiding the need to construct them, which has limited previous approaches to product states.

Friday, 22nd January

9:15 – 9:35 Marcin Pawlowski (Univ. Gdańsk)

Information causality

Information Causality [M. Pawłowski et. al. Nature **461**, 1101 (2009)] is a recently discovered physical principle, which can be considered a generalized version of no-signalling. It is satisfied by quantum mechanics and violated by most of the theories that allow for probability distributions not possible to be obtained by the measurements of quantum systems. This fact allows to derive from Information Causality tight bounds on some properties of quantum mechanics (eg. Tsirelson bound) or the efficiency of quantum information protocols (eg. random access codes). In this review we present the results of several papers that are concerned with this principle. We start by presenting Information Causality and discuss its derivation. Then we show its already known applications and comment on the possible future ones. Finally, we study the, so-called, no-signalling polytope to see which part of it is in agreement with Information Causality.

9:40 – 10:00 Sergio Boixo (Caltech)

Local quantum measurement and relativity imply quantum correlations

(joint work with Salman Beigi, Matthew Elliot, and Stephanie Wehner)

We show that, assuming that quantum mechanics holds locally, the finite speed of information is the principle that limits all possible correlations between distant parties to be quantum mechanical as well. Local quantum mechanics means that a Hilbert space is assigned to each party, and then all local POVM measurements are (in principle) available; however, the joint system is not necessarily described by a Hilbert space. In particular, we do not assume the tensor product formalism between the joint systems. Our result shows that if any experiment would give non-local correlations beyond quantum mechanics, quantum theory would be invalidated even locally.

10:05 – 10:25 Markus Mueller (TU Berlin, Univ. Potsdam)

All reversible dynamics in maximally non-local theories are trivial

(joint work with David Gross, Roger Colbeck, and Oscar Dahlsten)

A remarkable feature of quantum theory is non-locality (i.e. the presence of correlations which violate Bell inequalities). However, quantum correlations are not maximally non-local, and it is natural to ask whether there are compelling reasons for rejecting theories in which stronger violations are possible. To shed light on this question, we consider post-quantum theories in which maximally non-local states (non-local boxes) occur. It has previously been conjectured that the set of dynamical transformations possible in such theories is severely limited. We settle the question affirmatively in the case of reversible dynamics, by completely characterizing all such transformations allowed in this setting. We find that the dynamical group is trivial, in the sense that it is generated solely by local operations and permutations of systems. In particular, no correlations can ever be created; non-local boxes cannot be prepared from product states (in other words, no analogues of entangling unitary operations exist), and classical computers can efficiently simulate all such processes.

11:00 – 11:20 Michael Wolf (Niels Bohr Inst. Copenhagen)

Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory

(joint work with David Perez-Garcia, and Carlos Fernandez)

"While [...] the wave function does not provide a complete description of physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible.'' *Einstein, Podolsky and Rosen, 1935.*

More than seventy years after Einstein, Podolsky and Rosen (EPR) raised this puzzle we know, as a consequence of Bell's argument, that a complete theory in the sense of EPR would force us to pay a high price--- such as giving up Einstein locality. Could there, however, be a theory which provides more information than quantum mechanics but still is `incomplete enough' to circumvent such fundamental conflicts? In this work we address a particular instance of this question, in the context of which the answer is clearly negative: observables which are not jointly measurable within quantum mechanics must remain incompatible in every hypothetical refinement of this theory unless one gives up Einstein locality.
More technically speaking we show that the maximal Bell violation is the Lagrangiang dual of the joint measurability problem.

11:25 – 11:55 Toby Cubbit (Univ. Bristol)

Laying the quantum and classical embedding problems to rest

(joint work with Jens Eisert and Michael Wolf)

Quantum channels and master equations are both widely used to describe the dynamics of quantum systems that are subject to noise. Quantum channels, also known as completely-positive maps, are commonly used in quantum information theory, where abstracting away the underlying physics allows one to focus on the information-theoretic aspects of noise. Master equations are frequently used in physics, where the underlying physical processes are the main focus of attention. The connection between these two descriptions is a classic topic in mathematical physics. One direction was solved by the now famous result due to Lindblad, Kossakowski and Gorini, who gave a complete characterisation of master equations that generate completely positive evolutions. However, the other direction has remained open: given a quantum channel, is there a master equation that generates it (and if so, can we deduce it's form)? Physically, this is asking how one can deduce underlying physical processes from experimental observations.

The analogous question can equally well be posed in classical dynamics: given a stochastic map, does there exist a continuous-time Markov chain that generates it? This is known in probability theory as the embedding problem, and it is even older than the quantum version; it was first studied at least as far back as 1937. It too has remained an open problem to this day. In this work, we give complexity theoretic solutions to both the quantum and classical embedding problems: both problems are NP-hard. Moreover, we give an explicit algorithm that reduces the problem to integer semi-definite programming, completing the proof that solving the quantum or classical embedding problem is equivalent to solving P=NP, thus finally laying the embedding problem to rest after more than 70 years.

12:00 – 12:20 Peter Shor (MIT)

Quantum interactive proofs with short messages

(joint work with Salman Beigi and John Watrous)

We consider three variants of quantum interactive proof systems in which short (meaning logarithmic-length) messages are exchanged between the prover and verifier. The first variant is one in which the verifier sends a short message to the prover, and the prover responds with an ordinary, or polynomial-length, message; the second variant is one in which any number of messages can be exchanged, but where the combined length of all the messages is logarithmic; and the third variant is one in which the verifier sends polynomially many random bits to the prover, who responds with a short quantum message. We prove that in all of these cases the short messages can be eliminated without changing the power of the model, so the first variant has the expressive power of QMA and the second and third variants have the expressive power of BQP. These facts are proved through the use of quantum state tomography, along with the finite quantum de Finetti theorem for the first variant.

14:45 – 15:40 Scott Aaronson (MIT)

New evidence that quantum mechanics is hard to simulate on classical computers

(joint work with Alex Arkhipov)

I'll discuss new types of evidence that quantum mechanics is intractable to simulate classically -- evidence that is more complexity-theoretic in character than (say) Shor's factoring algorithm, and that also corresponds to experiments that seem much easier than building a universal quantum computer. Specifically:
(1) I'll discuss recent oracle evidence that BQP has capabilities outside the polynomial hierarchy---namely, that there exists a black-box relational problem in

BQP but not in BPP^PH, and that a *decision* problem separating BQP from PH (that is, an oracle relative to which BQP is not in PH) would follow from the "Generalized Linial-Nisan Conjecture." The original Linial-Nisan Conjecture (about pseudorandomness against constant-depth circuits) was recently proved by Mark Braverman, after being open for 20 years. (Preprint at arXiv:0910.4698)
(2) I'll show that, using only nonadaptive linear optics, one can generate probability distributions that can't be efficiently sampled by a classical computer, unless P^#P = BPP^NP and hence the polynomial hierarchy collapses. I'll also discuss an extension of this result to samplers that only *approximate* the photon distribution in variation distance. The extension relies on an unproved conjecture in classical complexity theory: namely, that approximating the permanent of a matrix of i.i.d. Gaussians is a random-self-reducible #P-complete problem.

15:45 – 16:05 Oded Regey (Tel Aviv Univ.)

No strong parallel repetition with entangled and non-signaling provers

(joint work with Julia Kempe)
We consider one-round games between a classical verifier and two provers. One of the main questions in this area is the *parallel repetition question*: If the game is played l times in parallel, does the maximum winning probability decay exponentially in l? In the classical setting, this question was answered in the affirmative by Raz. More recently the question arose whether the decay is of the form $(1-\Theta(\varepsilon))^l$ where $1-\varepsilon$ is the value of the game and l is the number of repetitions. This question is known as the *strong parallel repetition question* and was motivated by its connections to the unique games conjecture. This question was resolved by Raz by showing that strong parallel repetition does *not* hold, even in the very special case of games known as XOR games.
This opens the question whether strong parallel repetition holds in the case when the provers share entanglement. Evidence for this is provided by the behavior of XOR games, which have strong (in fact *perfect*) parallel repetition, and by the recently proved strong parallel repetition of linear unique games. A similar question was open for games with so-called non-signaling provers. Here the best known parallel repetition theorem is due to Holenstein, and is of the form $(1-\Theta(\varepsilon^2))^l$.
We show that strong parallel repetition holds neither with entangled provers nor with non-signaling provers. In particular we obtain that Holenstein's bound is tight. Along the way we also provide a tight characterization of the asymptotic behavior of the entangled value under parallel repetition of unique games in terms of a semidefinite program.

16:30 – 16:50 William Matthews (IQC Waterloo)

Zero-error channel capacity and simulation assisted by non-local correlations

(joint work with Toby Cubitt, Debbie Leung, and Andreas Winter)
We will show that there are classical channels whose classical (one-shot) zero-error capacity can be increased by making use of a suitable entangled state shared between the sender and receiver. This constitutes a novel use of entanglement to enhance a classical communication task. Our examples are based on proofs of the Bell-Kochen-Specker theorem and the phenomenon is shown to be related to "pseudo-telepathy'' games. These examples pose the question: To what extent can entanglement assist for zero-error communication? To this end we have found upper bounds by considering assistance by general non-signalling (NS) correlations e.g. the 'box' of Popescu and Rohrlich. This vastly simplifies the theory (and sometimes enables zero-error communication even when the available channel has no zero-error capacity). We give an efficiently computable, single-letter formula for both the NS-assisted zero-error capacity and the NS-assisted asymptotic communication cost of exact simulation (similarly for the corresponding single-shot quantities). We even obtain a weak form of asymptotic reversibility between zero-error coding and simulation in the presence of NS correlations (analogous to the reverse Shannon theorem), which we show cannot be made any stronger.

16:55 – 17:15 Tony Cubitt (Univ. Bristol)

Super-duper-activation of the zero-error quantum capacity

(joint work with Jianxin Chen, Aram Harrow, and Graeme Smith)
The zero-error classical capacity of a quantum channel is the asymptotic rate at which it can be used to send classical bits perfectly, so that they can be decoded with zero probability of error. The study of zero-error capacities dates right back to Shannon and the early days of information theory. We show that there exist pairs of quantum channels, neither of which individually have any zero-error capacity whatsoever (even if arbitrarily many uses of the channels are available), but such that access to even a single copy of both channels allows classical information to be sent perfectly reliably. In other words, we prove that the zero-error classical capacity can be superactivated. This result is the first example of superactivation of a classical capacity of a quantum channel.
We further strengthen this result to show that there exist pairs of channels, neither of which have any zero-error classical capacity (as before), yet for which access to one copy of the joint channel even allows far more delicate quantum information to be transmitted perfectly. This subsumes the first result, and also implies that the quantum zero-error capacity can be superactivated. But it is strictly stronger than either of these. Indeed, this is the strongest conceivable form of superactivation, and nothing similar is possible for standard Shannon capacities of quantum channels or for zero-error capacities of classical channels.