QICS Workshop on "Foundational Structures for Quantum Information and Computation"

Monday, 15.9.

8:30 - 8:40: Hans Briegel
Welcome address

8:40 - 9:05: (Tutorial) Robert Raussendorf
Tutorial on measurement-based quantum computation
9:05 - 9:40: Robert Raussendorf
Discrete structures for quantum computation

I describe discrete structures in Hilbert space that give rise to quantum algorithms. The resulting discrete quantum algorithms have the properties that (1) their input and output is digital, and (2) they succeed with unit probability. Both (1) and (2) constrain the capabilities of a quantum computer, but, arguably, not severely so: Discrete Logarithm -- breaking the Diffe-Hellman public key exchange -- is within the considered class [Mosca and Zalka, 2003]. There is a gain, too: the imposed constraints lead to a different method for composition of quantum algorithms.

I will present *very simple* examples of discrete quantum algorithms, both in the circuit model and measurement-based QC, and show how these algorithms can be composed to form new ones. Furthermore, I ask the question of what is genuinely quantum mechanical about these algorithms. This quantum mechanical essence turns out to be contextuality. If a discrete quantum algorithm computes a non-linear function then it cannot be described by a non-contextual hidden-variable model. Any such quantum algorithm implies a proof of the Kochen-Specker theorem.

10:10 - 10:45: Jens Eisert
Too entangled to be useful

It is often argued that entanglement is at the root of the speedup for quantum compared to classical computation, and that one needs sufficient entanglement for this speedup to be manifest. In measurement-based quantum computing (MBQC), the need for a highly entangled initial state is particularly obvious. In this work we show that, remarkably, quantum states can be too entangled to be useful for the purpose of computation. What is more, we can prove that this phenomenon occurs for the dramatic majority of all states: the fraction of pure states on n qubits not subject to the problem is smaller than e^(-n^2). Our results show that computational universality is actually a rare property in quantum states. For the proof we establish a link between the ``quantum probabilistic method" and ideas on quantum many-body systems. This work highlights a new aspect of the question concerning the role entanglement plays for quantum computational speed-ups. We will also present a new classification of primitives that can be used in order to systematically construct new models for measurement-based computation.

10:45 - 11:20: Caterina Mora
Quantum Kolmogorov complexity and its applications

Classical Kolmogorov complexity is one of the fundamental quantities of classical information theory. In this field, its relevance lies in the fact that Kolmogorov complexity is a measure of the information content, and thus the compressibility, of a single classical object. The applications of classical Kolmogorov complexity, though, reach beyond classical information theory, to fields such as economics, logic, and other branches of physics.

In recent years, much effort has been devoted to the definition and the study of quantum Kolmogorov complexity (QKC). In this talk I will review these recent results in the field of QKC theory. I will start by recalling the definitions of QKC that have been proposed, and briefly outlining the differences between them. I will then show how, studying a communication-complexity scenario, it is possible to find a condition that is satisfied by a class of these definitions. Finally, I will illustrate some of the applications that the definitions in this class have in the fields of quantum communication and computation complexity theory.

16:00 - 16:35: Sandu Popescu

TBA

16:35 - 17:10: Robert Spekkens

An information-theoretic application of contextuality

Using a recent generalization of the notion of noncontextuality to arbitrary procedures and to arbitrary operational theories, it is possible to derive noncontextuality inequalities -- constraints on experimental statistics that hold for theories that admit a noncontextual hidden variable model. I describe one such inequality based on an assumption of noncontextuality for preparation procedures; this is the contextual analogue of the CHSH inequality. I demonstrate that a particular kind of two-party secure computation, "parity-oblivious multiplexing", is powered by contextuality in the sense that the degree of violation of the inequality quantifies the degree of success that can be achieved in the task.

17:40 - 18:15: Giacomo Mauro D'Ariano

Quantum mechanics as a fair operational framework

In the last years the new field of Quantum Information has renewed the interest on the problem of deriving Quantum Mechanics (QM) from operational principles, answering to fundamental questions as: Why are the laws of nature quantum? What are the in-principle limitations to information processing? The problem of QM axiomatization has been attacked from a completely new point of view, upon positioning QM within the landscape of general probabilistic theories, including QM, classical theory, and other no-signaling probabilistic theories, e.g. with super-quantum correlations (PR-boxes). In this context Quantum Information has inspired task-oriented axioms to be considered. It has then been shown that certain features (e.g. no cloning, non-unique decomposition of mixed states into pure ones, measurement disturbance related to the possibility of secure key distribution), features that are usually thought of as specifically quantum, are indeed present in all except classical theories.

We are thus left with the big question: Why Quantum?

As a probabilistic theory, QM is very special. What is truly peculiar to QM is that the "effects" make an algebra (precisely a C*-algebra). More precisely, this is true for all hybrid quantum-classical theories, corresponding to QM plus super-selection rules. The oddity of QM is that the notion of "effect" admits a natural interpretation of their "addition", however, the notion itself abhors any kind of "composition".

I will analyze the possibility of deriving QM as the mathematical representation of a "fair" operational framework, i.e. a set of rules which allow one to make predictions on future "events" on the basis of suitable "tests". Two postulates need to be satisfied by any fair operational framework: NSF: no-signaling from future (for the possibility of making prediction based on present tests) FAITH: existence of faithful states (for the possibility of calibrating any test and preparing any state). I will show that all theories satisfying NSF admit a C*-algebra representation of events as linear transformations of effects. Based on another very natural postulate--- AE: atomicity of evolution---along with a purely mathematical postulate---CJ: Choi-Jamiolkowski isomorphism---it is possible to identify effects with atomic events, through which we can then define their composition, thus obtaining the quantum-classical hybrid and excluding the other probabilistic theories.

The presence of a single purely mathematical postulate of the present operational axiomatization of QM is a drawback in common with all previous axiomatization attempts by other authors. I will anyway suggest a possibility, which I'm currently exploring, of deriving the CJ postulate operationally from the new notion of "quantum comb", which seems to be a quantum realization of the "causaloid" of Lucien Hardy.

18:15- 18: 50: Elham Kashefi

Universal blind quantum computation

Joint work with Anne Broadbent and Joseph Fitzsimons
We present the first protocol which allows Alice to have Bob carry out a quantum computation for her such that Alice's inputs, outputs and computation remain perfectly private, and where Alice does not require any quantum computational power or memory. She only needs to be able to prepare single qubits from a finite set and send them to Bob, who has the balance of the required quantum computational resources. Our protocol is interactive: after the initial preparation of quantum states, Alice and Bob use two-way classical communication which enables Alice to drive the computation, giving single-qubit measurement instructions to Bob, depending on previous measurement outcomes. The interaction is polynomial in the size of Alice's underlying quantum circuit. Our protocol works for inputs and outputs that are either classical or quantum. We also discuss the use of authentication in order for Alice to detect an interfering Bob. Furthermore, our construction involves a new, regular universal resource for measurement-based quantum computing called the brickwork state which may also be of independent interest.

Tuesday, 16.9.

8: 30- 8: 55: (Tutorial) Bob Coecke

Category theory for vegetarians: a tutorial

8: 55- 9: 30: Bob Coecke

Categories for the practicing physicist

The content of this talk is a summary of a chapter with the same title that will soon appear in a book series entitled New Structures for Physics. Our focus will mainly be on a direct physical interpretation of symmetric monoidal categories, and some additional structures we can endow these with that have direct physical applications. Example categories include categories of Hilbert spaces with a variety of morphisms, including completely positive maps, as well as categories of relations, cobordisms, and topological quantum field theories. We will point the reader to other chapters in New Structures for Physics for related tutorials.

10:10 - 10:45: Samson Abramsky

No-cloning in categorical quantum mechanics

The No-Cloning theorem is a basic limitative result for quantum mechanics, with particular significance for quantum information. It says that there is no unitary operation which makes perfect copies of an unknown (pure) quantum state. A stronger form of this result is the No-Broadcasting theorem, which applies to mixed states. There is also a No-Deleting theorem.

Recently, the author and Bob Coecke have introduced a categorical formulation of Quantum Mechanics, as a basis for a more structural, high-level approach to quantum information and computation. This has been elaborated by ourselves, our colleagues, and other workers in the field, and has been shown to yield an effective and illuminating treatment of a wide range of topics in quantum information. Diagrammatic calculi for tensor categories, suitably extended to incorporate the various additional structures which have been used to reflect fundamental features of quantum mechanics, play an important role, both as an intuitive and vivid visual presentation of the formalism, and as an effective calculational device.

It is clear that such a novel reformulation of the mathematical formalism of quantum mechanics, a subject more or less set in stone since Von Neumann's classic treatise, has the potential to yield new insights into the foundations of quantum mechanics. In the present paper, we shall use it to open up a novel perspective on No-Cloning. What we shall find, quite unexpectedly, is a link to some fundamental issues in logic, computation, and the foundations of mathematics. A striking feature of our results is that they are visibly in the same genre as a well-known result by Joyal in categorical logic showing that a `Boolean cartesian closed category' trivializes, which provides a major road-block to the computational interpretation of classical logic. In fact, they strengthen Joyal's result, insofar as the assumption of a full categorical product (diagonals *and* projections) in the presence of a classical duality is weakened. This shows a heretofore unsuspected connection between limitative results in proof theory and No-Go theorems in quantum mechanics.

10:45 – 11:20: Ross Duncan

Computing with complementary observables

I present a formalisation of the interaction of complementary quantum observables, and the information flow mediated by them. Using a general categorical formulation, I show that pairs of mutually unbiased quantum observables form bialgebra-like structures. The resulting equations suffice to perform computations with elementary quantum gates, translate between distinct quantum computational models, establish the equivalence of entangled quantum states, and simulate quantum algorithms such as the quantum Fourier transform. All these computations moreover happen within an intuitive diagrammatic calculus.

16:00 – 16:35: Francesco De Martini

Entanglement and nonlocality in microscopic-macroscopic systems

Theoretical and experimental results on the Quantum Injected Optical Parametric Amplification (QI-OPA) of optical qubits in the high gain regime ($g > 6$) are reported.

The entanglement of the related Schroedinger Cat-State (SCS) is demonstrated as well as the establishment of Phase-Covariant quantum cloning for a Macrostate consisting of about 10^6 particles. In addition, the violation of the CHSH inequality is has been realized experimentally. According to the original 1935 definition of the SCS, the overall apparatus establishes for the first time the nonlocal correlations between a microscopic spin (qubit) and a high J angular momentum i.e. a macroscopic multiparticle system close to the classical limit. Applications to Quantum Information will be discussed.

16:35 – 17:10: Philip Walther

Experimental demonstration of quantum algorithms on a photonic one-way quantum computer

In recent years, one-way quantum computing has become an exciting alternative to existing proposals for quantum computers. In this specific model, coherent quantum information processing is accomplished via a sequence of single-qubit measurements applied to an entangled resource known as cluster state. Here we show the experimental realization of various quantum algorithms on a photonic four-qubit cluster state, which is generated by means of parametric down-conversion. We were able to implement simple quantum algorithms, consisting of a few gates. Among them the so-called Deutsch-Josza algorithm, an important quantum algorithm that is capable of distinguishing whether a function is constant or balanced and the implementation of a quantum game known as Prisoner's Dilemma. Playing such a game is essentially the execution of a quantum algorithm in which the players can resolve the "dilemma" that occurs in the classical version of this game. Finally we were able to design decoherence-free subspaces for cluster states which achieve remarkable protection from environmentally induced decoherence, delivering nearly ideal computational outcomes.

17:40 – 18:15: Zhen-Sheng Yuan

Manipulation of photons and cold atoms: towards scalable quantum communication, computation and simulation

Quantum theory predicts a bright future of quantum information processing. In the first part of this talk, a brief survey will be presented on the recent progress of experimental demonstrations of different schemes involving quantum communication, computation and simulation. Some experiments carried out with photonic qubits, in the second part, will be discussed a little more. Then obstacles in front of scalable quantum information processing are analyzed followed by an introduction of quantum memory. In the last part, the proposed solutions to the above obstacles, involving manipulation of photonic and memory qubits will be discussed extensively.

18:15 – 18:50: Pieter Kok

Optical quantum computing with a variety of physical systems

The construction of a quantum computer is a difficult cross-disciplinary problem in physics, computer science, and engineering. Not only do we not know what is the best physical system to implement a quantum computer, we also do not know what is the best computational model for a quantum computer. Moreover, these two questions are related to each other. Optical systems (that is, systems in which the interaction with light plays an essential role) are very attractive in that they potentially allow coupling of a quantum computer to a quantum communication channel using photons. These systems have also been on the forefront in adopting new computational models, such as the one-way model of quantum computation. In this talk, I will give an overview of optical quantum computing using linear optics, hybrid photon--matter-qubit systems, and atomic ensembles coupled to light.

20:30 – 21:05: Simon Benjamin

Robust and efficient QIP with distributed matter-optical systems

We discuss the use of networked optically active matter systems as a practical architecture for full scale QIP. Each matter systems is taken to have a degree of local structure that is greater than one qubit, but only slightly greater! When attempting to create multi-qubit entangled states such as graph states, a single additional qubit at each node can provide insulation from the damage that would arise from failed remote entanglement operations. But by fully exploiting this modest level of complexity one can do more: for example, one can make efficient use of highly imperfect networks where the vast majority of photons 'escape' into the environment. In the light of new techniques to minimise the number of nodes associated with a given task, and recent ideas on parallel entanglement of many nodes, this paradigm may be among the most promising routes to large scale QIP.

Wednesday, 17.9.

8:30 – 9:05: Jonathan Barrett

Non-signalling computation

I show how to define a circuit model for computation in a framework that is broader than classical or quantum theory, but which preserves the no-signalling principle. An interesting question is whether there are non-signalling circuits that are more powerful than a quantum computer, i.e., that solve some problem more efficiently. I don't know how to answer this. But suppose we give our circuits an extra power, the ability to postselect measurement outcomes. It follows from a result of Scott Aaronson that a postselecting quantum computer is just as powerful as any other postselecting (non-signalling) computer.

9:05 – 9:40: Mehdi Mhalla

Finding optimal flows efficiently

Since a One-way QC is based on quantum measurement, which is a fundamentally nondeterministic evolution, a sufficient condition of global determinism has been introduced as the existence of a causal flow in a graph that underlies the computation. Previously, a O(n^3)-algorithm has been introduced for finding such a causal fl,ow when the numbers of output and input vertices in the graph are equal, otherwise no polynomial time algorithm was known for deciding whether a graph has a causal flow or not.
Our main contribution is to introduce a O(m)-algorithm for finding a causal flow (where m is the number of edges of the graph), if any, whatever the numbers of input and output vertices are. This answers the open question stated by Danos and Kashefi and by de Beaudrap . Moreover, we prove that our algorithm produces a flow of minimal depth. Whereas the existence of a causal flow is a sufficient condition for determinism, it is not a necessary condition. A weaker version of the causal flow, called gflow (generalised flow) has been introduced and has been proved to be a necessary and sufficient condition for a family of deterministic computations. Moreover the depth of the quantum computation is upper bounded by the depth of the gflow. We provide here a polynomial time algorithm that outputs an optimal gflow of a given graph and thus finds an optimal correction strategy to the nondeterministic evolution due to measurements.

10:10 – 10:45: Howard Barnum

Information processing in convex operational theories: toward a characterization of quantum mechanics

The rise of quantum information science has been paralleled by the development of a vigorous research program aimed at obtaining an informational characterization or reconstruction of the quantum formalism, in a broad framework for stochastic theories that encompasses quantum and classical theory, but also a wide variety of other theories that can serve as foils to them. Such a reconstruction, at its most ambitious, is envisioned as playing a role in quantum physics similar to Einstein's reconstruction of the dynamics and kinetics of macroscopic bodies, and later of their gravitational interactions, on the basis of simple principles with clear operational meanings and experimental consequences. Short of such an ambitious goal, it could still lead to a principled understanding of the features of quantum mechanics that account for its greater-than-classical information-processing power, an understanding which could help guide the search for new quantum algorithms and protocols.

As part of the project of obtaining such an informational characterization of quantum mechanics, I give a precis of the convex operational framework for possible physical theories, and review work by me and my collaborators, on the information-processing properties of theories in this framework. The main results reviewed are the fact that the only information that can be obtained in the framework without disturbance is inherently classical, no-cloning and no-broadcasting theorems in the generalized framework, the existence of exponentially secure bit commitment in non-classical theories without entanglement, the consequences for theories of the existence of a conclusive teleportation scheme, and sufficient conditions for the existence of a deterministic teleportation scheme. I'll also discuss sufficient conditions for "remote steering" of ensembles using entanglement, rendering insecure bit commitment protocols of the form shown to be secure in the unentangled case.

Joint work with various groups of collaborators including Jonathan Barrett, Matthew Leifer, Alexander Wilce, Oscar Dahlsten, and Ben Toner.

10:45 – 11: 20: Alex Wilce

A recipe for probabilistic theories

After a long hiatus, there has lately been a revival of interest in what we may call *abstract probabilistic models* -- structures characterized by sets of states and observables, with the former assigning probabilities to the outcomes of the latter. Such structures were used Mackey and his successors in their search for a heuristically clear axiomatic foundations for quantum theory, but with a focus on *individual* systems. The new impetus comes from quantum information theory, which suggests focusing rather on *probabilistic theories*: classes of such structures, knit together by some device (or devices) for forming composites. This approach has already proved very fruitful, yielding, for instance, completely general analogues of the no-cloning and no-broadcasting theorems.
In this talk, I outline a method for constructing probabilistic theories that enjoy many of the distinguishing features of quantum mechanics, using group-theoretic data as raw material. I illustrate this method by reconstructing classical and quantum probability theory, and, for contrast, two other theories (in some sense dual to one another) involving doubly-stochastic matrices.

11:20 – 11:55: Antonio Acin

Quantum correlations and device-independent quantum information protocols

Given some correlations among several distant non-communicating parties, can they be obtained by performing local measurements on a quantum state? We introduce a convergent hierarchy of necessary conditions to characterize the set of quantum correlations. We also discuss the application of these concepts to the design of device-independent quantum information protocols.

Thursday, 18.9.

8:30 – 9:05: Richard Jozsa

Simulation complexity of quantum matchgate circuits

Matchgates are a class of 2-qubit gates with remarkable simulation properties and their study reveals a striking perspective on the relationship between classical and quantum computational power. We will outline a proof that uniform families of matchgate circuits can be classically efficiently simulated, if the gates are restricted to act on nearest neighbour (n.n.) qubit lines only. It may be further shown that if the n.n. condition is slightly relaxed, to allowing the same gates to act on n.n. and next-n.n. lines, then the resulting circuits can efficiently perform universal quantum computation. We will also provide evidence that the computational power of n.n. matchgate circuits is strictly weaker than full classical poly-time computation by showing that such circuits can be simulated in quantum log-space computation.

9:05 – 9:40: Maarten Van den Nest

Quantum computation and statistical mechanics

We present simple mappings between classical lattice models and quantum circuits. These mappings provide a systematic formalism to obtain quantum algorithms to approximate partition functions of lattice models in certain complex-parameter regimes. E.g., we present an efficient quantum algorithm for the six-vertex model as well as a 2D Ising-type model. We show that classical simulating of our quantum algorithms is as hard as simulating universal quantum computation (i.e. BQP-complete). Furthermore, our mappings provide a framework to obtain efficiently simulable quantum gate sets from exactly solvable classical models. E.g., we show that the simulability of Valiant's match-gates can be recovered by using the solvability of the free-fermion eight-vertex model.

10:10 – 10:45: Dan Browne

Measurement-based classical computation: classifying the computational power of entangled states

Joint work with Janet Anders, Robin Blume-Kohout, Akimasa Miyake and Debbie Leung. Measurement-based quantum computation has shown us that entangled states can be considered to possess intrinsic computational power. In classical computer science, the notion of computational power has been successfully formalised in the field of computational complexity theory. In this talk, I will describe an approach to the classification of the computational power of families of entangled states in measurement-based quantum computation, based on a consideration of the computational power of the classical computer essential in MBQC to provide the post-porcessing and feed-forward for the adaptive measurements.

This classification leads naturally to the notion of measurement based "classical computation". We shall describe examples of resource states for measurement-based classical computation. Surprisingly, the Greenberger-Horne-Zeilinger and Clauser-Horne-Shimony-Holt problems emerge naturally in this context [1]. We shall also describe some examples [2], where deterministic universal classical computation cannot be attained but classical fault tolerance techniques can be employed. Our work exposes an intriguing relationship between the violation of local realistic models and the computational power of entangled resource states.

References:
[1] J. Anders and D.E. Browne, Measurement-based classical computation, arXiv:0805.1002.
[2] J. Anders, R. Blume-Kohout, D. Leung, A. Miyake, D. E. Browne, in preparation.

10:45 – 11:20: Damian Markham

Entanglement and flow in measurement based QIP

We will discuss conditions for the preservation of quantum coherence in general measurement based quantum information processing, be it in MBQC, error correction or secret sharing. For MBQC using graph states under the standard scheme, a particularly simple and elegant way to write such conditions in terms of flow and generalised flow has been found in previous work. Here we apply these techniques to secret sharing and error correction and interpret them intuitively as simple conditions on the entanglement of the states, linking into several other works on entanglement conditions for MBQC.

16:00 – 16:35: Andreas Winter

New results in quantum identification & approximate randomization

One of the central insights about quantum error correction is that the existence of a decoding operation for a channel is equivalent to the complementary channel (to the environment) being randomising. Here we determine a matching duality for the weaker property of the complementary channel being approximately randomising. It turns out that the main channel then still preserves the pairwise fidelities between input states. This is closely related to the task of identification, where the receiver only wants to simulate measurements for any pure state and its complement. We prove that the entanglement-assisted capacity is an upper bound on the quantum identification capacity of a channel, and show achievability if correctly interpreted.
This is joint work with Patrick Hayden.

16:35 – 17:10: Barbara Kraus

Multipartite entanglement and global information

Joint work with Caroline Kruszynska.
We investigate the entanglement properties of pure quantum states describing *n* qubits. We characterize all multipartite states which can be maximally entangled to local auxiliary systems using controlled operations. A state has this property iff one can construct out of it an orthonormal basis by applying independent local unitary operations. This implies that those states can be used to encode locally the maximum amount of *n* bits. Examples of these states are the so--called stabilizer states, which are used for quantum error correction and one--way quantum computing. We give a simple characterization of these states and construct a complete set of commuting unitary observables which characterize the state uniquely. Furthermore we show how these states can be prepared and discuss their applications.

17:40 – 18:15: Pawel Wocjan

Quantum speed-up of approximate counting of perfect matchings

The Markov Chain Monte Carlo method is at the heart of many fully-polynomial randomized approximation schemes for #P-complete problems such as estimating the permanent or the volume of a polytope. It is therefore very natural and important to determine whether quantum computers can speed-up classical mixing processes based on Markov chains. To this end, we present a new quantum algorithm, making it possible to prepare a quantum sample, i.e., a coherent version of the stationary distribution of a reversible Markov chain. We show that our methods provide a speed-up over a method for preparing quantum samples of Boltzmann-Gibbs distributions of (classical) Hamiltonians that was proposed by Somma et al. We also show that they yield a speed-up of a classical algorithm for approximately counting the number of perfect matchings in dense bipartite graphs.

18:15 – 18:50: Pablo Arrighi

Unitarity plus causality implies locality

Joint work with Vincent Nesme and Reinhard Werner.

We consider a graph having a single quantum system sitting at each node. The entire compound system evolves in discrete time steps by iterating a global evolution G. Moreover we require that this global evolution G be unitary, in accordance with quantum theory, and that this global evolution G 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 G. We show that under these conditions the operator G is local; i.e. it can be put into the form of a quantum circuit made up with more elementary, unitary gates -- each acting solely upon neighbouring nodes.

Friday, 19.9.

8:30 – 9:05: Ignacio Cirac

Quantum computation, quantum state engineering, and quantum phase transitions driven by dissipation

Joint work with Frank Verstraete and Michael M. Wolf.

We investigate the computational power of creating steady-states of quantum dissipative systems whose evolution is governed by time-independent and local couplings to a memoryless environment. We show that such a model allows for efficient universal quantum computation with the result of the computation encoded in the steady state. Due to the purely dissipative nature of the process, this way of doing quantum computation exhibits some inherent robustness and defies some of the DiVincenzo criteria for quantum computation. We show that there is a natural class of problems that can be solved with such a model - the preparation of ground states of frustration free quantum Hamiltonians. This allows for robust and efficient creation of exotic states that exhibit features like topological quantum order and the creation of PEPS and it proves the existence of novel dissipative phase transitions. In particular the latter can in principle be verified experimentally with present day technology such as with optical lattices.

9:05 – 9:40: Reinhard Werner

Structure of quantum cellular automata

Reversible quantum cellular automata are defined as channels on a quantum lattice systems with strictly finite propagation. We show that all such automata can be implemented by local unitary operations, provided local ancillas can used. The class auf 1D automata, for which local ancillas are not needed, is characterized by triviality of an index quantity, which at the same time singles out the automata, which can be continuously connected to the identity. For the implementation of 1D automata the local ancillas can also be replaced by the availability of partial shift operations as elementary building blocks.

10:10 – 10:45: Akimasa Miyake

Ground-code measurement-based quantum computer

I talk about a scheme of measurement-based quantum computation processed inside the degenerate gapped ground state of a two-body Hamiltonian. Every logical quantum wire is encoded in the so-called nonlocal string order parameter of the gapped ground state of a spin-1 chain, that provides built-in robustness against noise on the hardware level. Computation is carried by single-spin measurements along multiple chains dynamically coupled on demand, and the logical information is processed inside the two-fold degenerate ground subspace of each residual chain.

Thus, our architecture may be conceptually phrased as the one-way quantum computational model by the cluster state is enhanced with the tactic taken in other computational models like topological quantum computation and adiabatic quantum computation, such that quantum information is encoded and processed in the gapped ground state. I discuss features of ground-code measurement-based computer, so as to circumvent apparent dilemma that aforementioned two desired properties, processing information by measurements while keeping information in the ground state, are not seemingly compatible. Some new features, for example the progression of the logical time, are in contrast with those of the familiar cluster-state case.
The reference is G.K. Brennen and A. Miyake, Phys. Rev. Lett. 101, 010502 (2008).

10 :45 – 11 :20 : Simon Perdrix

Bases in diagrammatic quantum protocols

Joint work with B. Coecke and E. Paquette.
Categorical axiomatisation of quantum mechanics enables rigorous and abstract design of quantum protocols. This program was initiated by Abramsky and Coecke in their analysis of the quantum teleportation protocol. They showed that dagger compact categories capture essential structures of the quantum mechanical formalism for diagrammatic design of teleportation.

In this paper, we show that the use of base structures, i.e. an axiomatisation of orthonormal bases of Hilbert space within a dagger symmetric monoidal category, leads to a diagrammatic description, among other protocols, of Perdrix' state transfer protocol. State transfer is key to the unification of measurement-only and one-way models of quantum computation. Moreover, state transfer, as a substitute for teleportation, is a key feature for optimizing the resources of measurement-only quantum computation. The diagrammatic analysis of both teleportation and state transfer reveals structural connections between these two measurement-only quantum computational models.

Our notion of basis structure refines the classical objects of Coecke and Pavlovic in an essential manner: it bypasses the conflict between: i.~the necessarily `self-dual' dagger Frobenius comonoids, and, ii.~the compact structures with `non-trivial duals' required to accommodate Selinger's diagrammatic representation of mixed states and operations. One interpretation of our basis structures is that they do not refine, but are complementary to compactness of a dagger symmetric monoidal category. A complementary view is that they do not only refine the compact structures in terms of a comonoid structure, but also require an `un-natural' explicit witness for the passage from a space to its dual, hence reconciling the `natural' compact structures with the `un-natural' dagger Frobenius comonoids.

This refinement also allows us to both accommodate physical flow of information and logical flow of information within one language, hence enriching the currently used diagrammatic languages with an important new feature.

16:00 – 16:35: Peter Selinger

Data types for quantum computing

Data types plays an important role in the theory of classical computing. Particularly the study of lazy types is closely related to the notion of partial information, and is often formalized in terms of Scott domains. In this talk, I will report on recent work with Landry Huet and Yoann Le Montagner on what a theory of lazy quantum data types may look like.

16:35 – 17:10: Peter Hines

Category theory and quantum logic

This talk describes the structure of partial isometries, both in terms of the order-theoretic 'quantum logic' of von Neumann /Birkhoff, and in terms of their categorical structure. The ultimate intention is to consider whether the orthomodular lattices approach to the foundations of quantum mechanics gives rise to categorical structures with nice logical or computational interpretations.

17:40 – 18:15: Chris Heunen

Categorical quantum logic

We abstract properties from the category of Hilbert spaces resembling the axioms of monoidal Abelian categories. We study closed subobjects in such categories, and prove that they form orthomodular lattices. This shows rigorously that quantum logic is just an incarnation of categorical logic. In particular, this provides an existential quantifier for quantum logic.

18:15 – 18:50: Jamie Vicary

The way of the dagger

The inner product is vital for quantum mechanics, and a great way to axiomatise it is with the "dagger-functor". We explore the properties of the dagger-functor in Hilb, the category of Hilbert spaces, and investigate how we can use the dagger-functor to describe orthogonal bases, C*-algebras and measurements, and even to obtain a new understanding of the properties of the complex numbers.