

QICS - PUBLISHABLE FINAL ACTIVITY REPORT

Bob Coecke

Chancellor, Masters and Scholars of the University of Oxford

FP6 FET STREP - project no 033763

Full name: Foundational Structures for Quantum Information and Computation

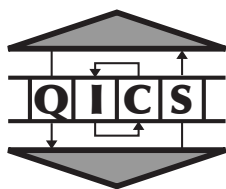
Thematic priority: Quantum Information Processing and Communications

Period covered: Jan. 1st 2007 – Jun. 31 2010

Date of preparation: Sept. 7th 2010

Start date of project: Jan. 1st 2007

Duration: 42 months



It is our pleasure to report on a very successful QICS project, which due to the extension recommended and granted after the 2nd review, lasted 42 months in total. The ultimate goal of QICS, as stated in the initial proposal, was to radically increase our understanding of the foundational structures of quantum informatics, as part of a cross-disciplinary endeavour, involving,

- *physicists* who are challenging the boundaries of nature’s capabilities by studying novel quantum computational models such as measurement based quantum computational schemes and quantum cellular automata, mainly in Hannover and Innsbruck,
- *logicians* who adopt novel structural tools such as category theory, type systems and formal calculi to cast quantum behaviour, mainly in McGill et al, Oxford and York,
- *mathematicians* trying to achieve an understanding of quantum information by providing both qualitative and quantitative accounts on it, mainly in Bristol, McGill et al, Oxford and York, and,
- *computer scientists* who bring in their know-how on high-level methods to cope with complex interactive and distributed situations, mainly in Grenoble, McGill et al, Oxford and Edinburgh/Paris.

Project background

The background to the QICS project is the fact that in the not too distant future, Information Technology will have to confront the challenge of the fundamentally quantum nature of physically embodied computing systems. This passage to Quantum Information Technology is both a matter of *necessity* and one which offers many new *opportunities*:

- As the scale of the miniaturization of IT components reaches the quantum domain, taking quantum phenomena into account will become unavoidable.
- On the other hand, the emerging field of Quantum Information and Computation (QIC) has exposed new computational potential, including several quantum algorithms, some of which endanger currently used cryptographic encoding schemes, while at the same time QIC provides the corresponding remedy in the form of secure quantum cryptographic and communication schemes, which have no classical counterparts.

Much of the quantum informatics research to date has focussed on a quest for new quantum algorithms and new kinds of quantum protocols, and great advances have been made. However, many important basic questions which are fundamental to the whole quantum informatics endeavor still remain to be answered, such as:

- “What are the true origins of quantum computational algorithmic speed-up?”
- “How do quantum and classical information interact?”
- “What are the limits of quantum computation?”

Generally speaking, these are all questions which explore the *axiomatic structure and boundaries* of QIC.

But the gaps in our deeper understanding of the phenomena of QIC and its structural properties already exist at a very basic level. While at first, it seemed that the notions of Quantum Turing Machine and the quantum circuit model could supply canonical analogues of the classical computational models, new very different models for quantum computation have emerged, e.g. Raussendorf and Briegel’s *one-way quantum computing* model and *measurement based quantum computing* in general, *adiabatic quantum computing*, *topological quantum computing* etc. These new models have features which are both theoretically and experimentally of great interest, and the methods developed to date for the circuit model of quantum computation do not carry over straightforwardly to them. In this situation, we can have no confidence that a comprehensive paradigm has yet been found. It is more than likely that we have overlooked many new ways of letting a quantum system compute. So the whole issue of the scope and limits of quantum computation remains a topic of fundamental interest and importance, the ultimate question which still needs to be addressed being:

- “What actually *are* general quantum computations, and what is a convincing model thereof?”

Addressing these fundamental questions seriously will require a passage to new high-level methods, which expose the deep structure of quantum information and computations. Indeed, while the fruits of QIC have emerged from the recognition that quantum phenomena should not be seen as a *bug* but as a *feature* — contrasting with the negative attitude to “quantum weirdness” which was adopted by many scientists since the birth of quantum theory — this change of attitude came without a change of methods, and it is not totally unfair to compare the “manipulations of complex vectors and matrices in bases built from *kets* $|0\rangle$ and $|1\rangle$ ” with the “acrobatics with 0’s and 1’s” in the early days of low-level computer programming. These still essentially *low-level* methods are in strong contrast to the modern methods in classical distributed computing, security, protocol verification etc., which involve type systems, logics and calculi based on well-understood semantic structures. It is obvious that a passage to such high-level methods will be essential as quantum computational architectures start to become more elaborate, combining classical and quantum components, and involving non-trivial concurrency. But on the other hand, we also recognize the opportunity to use these semantic methods and structures to explore and expose the fundamental structure of quantum informatics itself, which may lead to answers to the questions posed above, and provide key insights in the quest for a general model of quantum computation.

Our overall objectives address a range of key *structural issues* in QIC.

We want to answer *fundamental questions on the nature of QIC* which should provide a deeper understanding of the quantum informatics endeavor as a whole, and guide further developments. Examples are:

- Q. What are the precise structural relationships between parallelism, entanglement and mixedness as quantum informatic resources? Or, more generally,
- Q. Which features of quantum mechanics account for differences in computational and informatic power as compared to classical computation?
- Q. How do quantum and classical information interact with each other, and with a spatio-temporal causal structure?
- Q. Which quantum control features (e.g. iteration) are possible and what additional computational power can they provide?
- Q. What is the precise logical status and axiomatics of (No-)Cloning and (No-)Deleting, and more generally, of the quantum mechanical formalism as a whole?

We want to design structures and develop methods and tools which apply to *non-standard quantum computational models* where most of the current methods fail, in particular the *one-way quantum computing* model and *measurement based quantum computing* in general. We will also address the question of how the various models compare — can they be interpreted in each other, and which computational and physical properties are preserved by such interpretations? In the light of the recent emergence of *many* alternatives to the circuit model, ultimately we want to provide an answer to:

- Q. What is a convincing *model for general quantum computation*?

We want to establish QIC as a systematic discipline with powerful design methods and structuring concepts, based on deep structural and foundational insights, rather than as a bag of tricks, however ingenious. This step towards high-level and systematic methods has proved – and continues to prove – essential to the successful development of classical computation and information. We believe that the quantum case will, if anything, pose greater challenges, and hence rely all the more on the development of such concepts and methods. Since this involves insights and techniques coming both from Computer Science and from Quantum Physics, our consortium comprises an *interdisciplinary team* of leading Computer Scientists and Physicists, including several of the pioneers of QIC.

To tackle these challenges, the research will involve three main intertwined strands of activity. Our consortium has great expertise in each of these:

Strand 1: New MODELS of QIC

Strand 2: Foundational STRUCTURES for QIC

Strand 3: High-level METHODS for QIC

The inter-disciplinary interplay between the different communities and individuals involved in drawing these strands and approaches together is a key feature of this project. We believe that it can play a major rôle in developing a common framework for the currently disparate research communities, and in encouraging synergies between them.

New MODELS. This strand stretches from current leading-edge experimental activity to perhaps the most momentous pending question for quantum informatics. New experimental developments have indeed indicated that the likely candidates for a QC-device might end up being very different than what one had in mind in most QIC-activity so far. We want to study these challenging architectures, hopefully gaining insight towards the ultimate quest for a general model. We intend to intensively investigate models which rely on classical control, such as *measurement based quantum computational models*, with the *one-way quantum computational model* and *teleportation-based computational models* as special cases. But we will also study models which live at the other end of the spectrum such as *quantum cellular automata* and *quantum state machines*, which involve only quantum control, and also models which exploit other deep aspects of quantum structure, such as *topological quantum computing*. Furthermore, we are convinced that due to our innovative approach, additional new models will emerge.

Foundational STRUCTURES. A deeper analysis of the fundamental concepts of QIC must go hand-in-hand with a sharper elucidation of its logical and axiomatic structure. But the deep structure of QIC has yet to be unveiled. Much of the work in QIC has developed in a rather piecemeal and ad hoc fashion. There is great potential for future developments to be guided by structural insights, and hence to proceed more systematically. Here we aim to develop the appropriate mathematical and logical tools to address the key foundational issues in QIC with which we are concerned. The lack of grasp of QIC in structural terms also results in a wide range of unanswered questions on the *axiomatic boundaries of QIC*. Some recently introduced mathematical structures seem very well suited to provide a basis for a deep but also practical and effectively exploitable structural understanding of QIC. These new structures come with intuitive *graphical calculi*, which not only greatly facilitate human design, but at the same time provide a basis, due to their connection with logics, for *automated design methods*. Furthermore, exposing the semantic structure of QIC is also essential as the necessary bridge between the different computational models and well-tailored sophisticated design and analysis methods which apply to each of them.

High-level METHODS. The aim of developing high-level methods for QIC is in fact inextricably intertwined with our objective of gaining deeper insight into what QIC is in general. Moreover, the development of powerful formalisms for the specification, description and analysis of quantum information processing systems will be essential for the successful development of such systems — just as has proved and is increasingly proving to be the case for classical computing systems. For example, the development of secure distributed quantum communication schemes will involve an interplay between classical and quantum components, distributed agents, and all the subtle concepts pertaining to information security. It will be *harder* to specify and reason about quantum information security than classical information security, which is already a major topic of current research. We intend to apply and adapt the high-level methods developed for classical computing, such as type systems, logics, semantics-based calculi and verification tools, to the quantum domain, and also to develop

new ones specifically tailored for quantum informatics, guided by our development of foundational semantic structures.

Project execution

Workpackage 1: Structures and methods for measurement-based quantum computation

This workpackage addressed several fundamental questions, for example, on the relation of the entanglement of the resource state with the computational power of the scheme, which were still largely unanswered. More specifically, which resource states beyond the cluster state would allow universal quantum computation and which entanglement features would be responsible for that? And, which resource states would give no advantages over classical computation at all? This endeavour was highly successful.

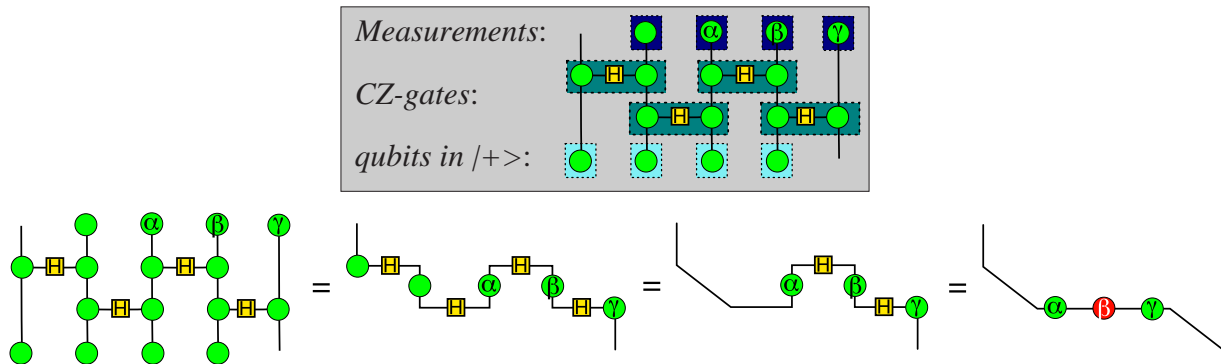
It has resulted in a much better understanding of graph states, a key resource for measurement based quantum computing, and exposed their scope for application. There is also a number of intriguing new applications and developments of graph state methods in statistical physics: problems involving statistical mechanics of classical spin systems, can be related to problems in quantum physics, relating a large class of classical spin models to quantum stabilizer states. Substantial progress has also been made on the clarification of which features of multi-partite entanglement are responsible for universality of resources in measurement based quantum computing.

Some other persistent central issues in this workpackage included: (i) good applications, e.g., the search for new quantum algorithms in the paradigm of MBQC as well as complementarily the search for efficient classical simulation techniques, and (ii) investigations for a robust, feasible implementation of MBQC that facilitates fault-tolerance by quantum error correction.

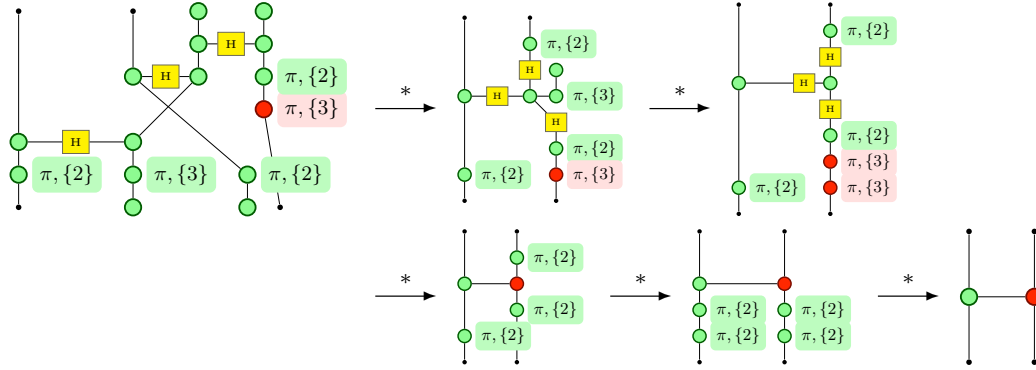
A very fascinating development is that concepts and methods which were originally developed to study condensed matter physics, have been getting more relevant to the goal of this workpackage than used to be in the beginning of the project. The converse is also true, methods resulting from MBQC research are now applied to long-standing problems in condensed matter physics. Some of the results in this context opened up an appealing possibility to prepare the resource state as the (preferably gapped) ground state in engineering an associated parent Hamiltonian, in addition to a conventional resource preparation by the controlled unitary operations as is supposed to be the case for the cluster state.

A central goal of the QICS project is an improved understanding of the structures of MBQC. This will help to devise new algorithms for MBQC, furthermore, it will shed light on the relation between MBQC and the network model of quantum computation. In the last period of QICS a number of relevant results have been obtained. A highlight here is the investigation of so-called “universal blind computation”, which has resulted in solving an open problem in complexity theory; it led to fundamental results for interactive proof systems: it is shown that $\text{QMIP} = \text{MIP}^*$ which means that in the setting of multiple provers with shared entanglement, a quantum verifier is no more powerful than a classical one.

A cross-workpackage result was the usage of categorical methods to understand MBQC. Significant success in this direction has been made. Diagrammatic calculi were crafted that enabled to verify MBQC schemes e.g. realisation of arbitrary one-qubit unitaries in no more than three rewrites:



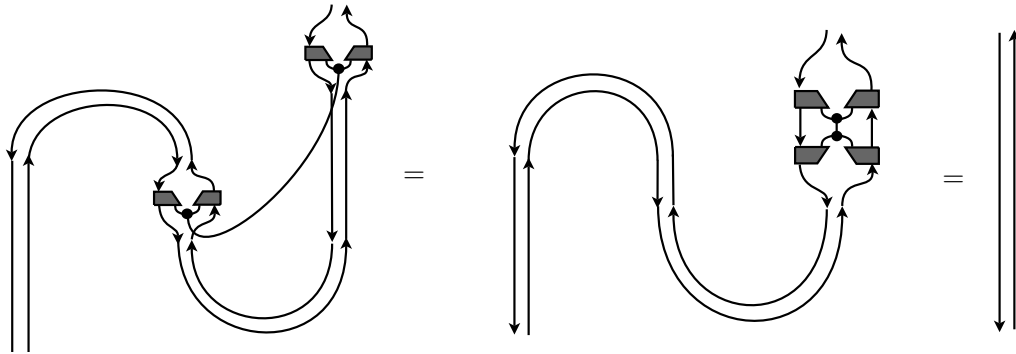
Novel results in the area of MBQC have emerged from this, which showed how to transform MBQ computations to quantum circuits without introducing any extra qubits, thus minimising the space complexity:



Workpackage 2: Categorical semantics, logics and diagrammatic methods

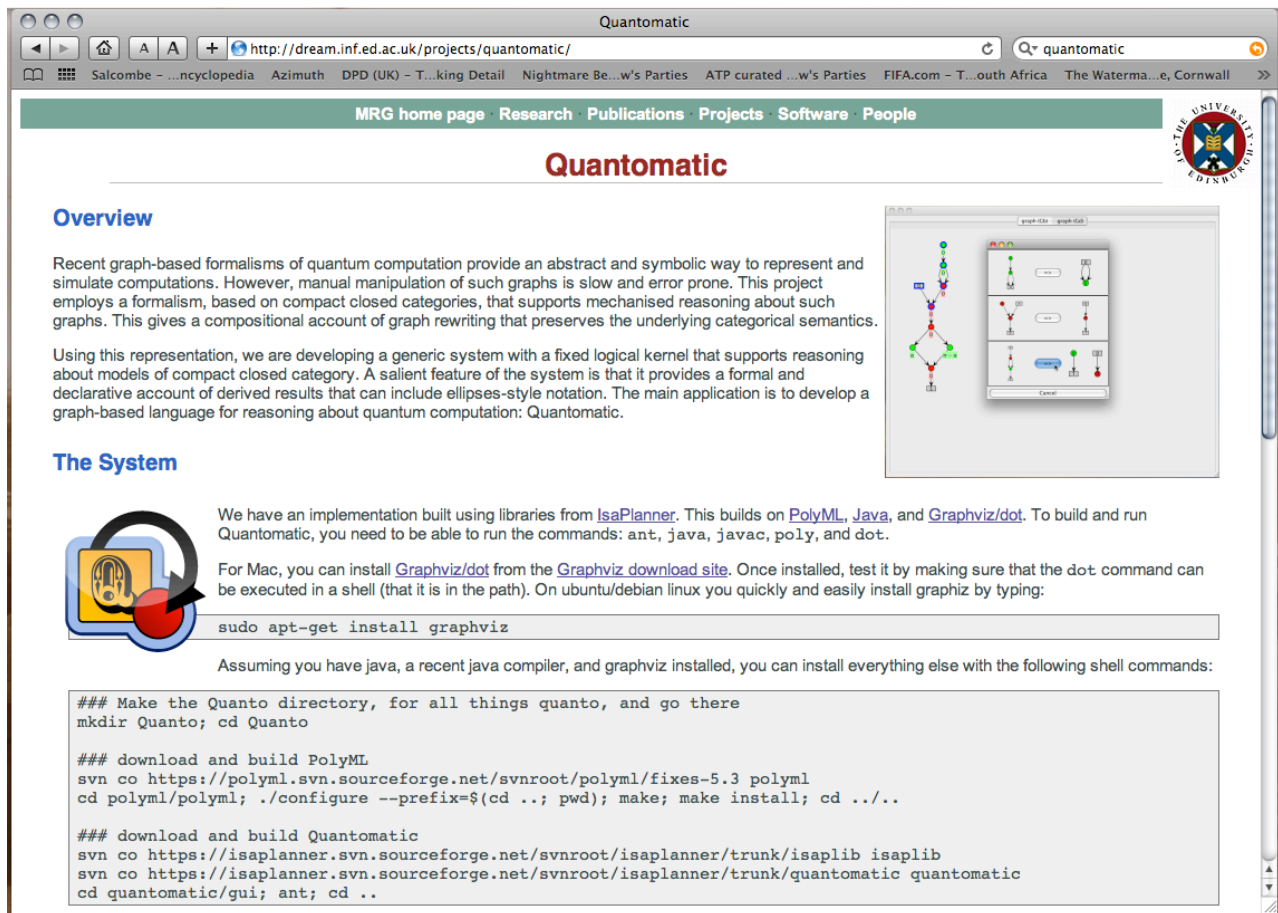
A key task of this workpackage was to craft the appropriate structures to address problems in workpackage 1 on measurement based quantum computing and workpackage 3 on information flow in quantum informatics. This resulted in a both axiomatic, diagrammatic, and logical (cf. automation) account on:

1. classical vs. quantum data, crucial for the applications in measurement-based quantum computational models which require classically controlled correction operations (see pictures above); e.g. a correctness proof of quantum teleportation looks as follows:



2. complementary observables, which enables abstract simulation of elementary gate computations; the key axioms of this structure are the well-known bialgebra equation, which provides enough structural power for typical circuit computations.
3. an algebraic characterization of three qubit entanglement as well as a compositional account on general multipartite qubit entanglement – multipartite quantum states constitute a (if not the) key resource for quantum computations and protocols. We expect that this work will lead to a generalized graph state paradigm, hence feeding back into the previously discussed workpackage.

Another important result which is a first of its kind is a completeness result for dagger compact categories and finite dimensional Hilbert spaces: any formal statement that can be expressed in the language of dagger compact categories holds if and only if it holds in the category of Hilbert spaces and linear maps. In turns this tells us what the graphical calculus is able to prove, and consequently which proofs can be automated by on graphical calculus based software. Substantial progress has indeed been made on “quantomatic”, a software tool for quantum reasoning based on the diagrammatic calculus.



Quantomatic

Overview

Recent graph-based formalisms of quantum computation provide an abstract and symbolic way to represent and simulate computations. However, manual manipulation of such graphs is slow and error prone. This project employs a formalism, based on compact closed categories, that supports mechanised reasoning about such graphs. This gives a compositional account of graph rewriting that preserves the underlying categorical semantics.

Using this representation, we are developing a generic system with a fixed logical kernel that supports reasoning about models of compact closed category. A salient feature of the system is that it provides a formal and declarative account of derived results that can include ellipses-style notation. The main application is to develop a graph-based language for reasoning about quantum computation: Quantomatic.

The System

We have an implementation built using libraries from [IsaPlanner](#). This builds on [PolyML](#), [Java](#), and [Graphviz/dot](#). To build and run Quantomatic, you need to be able to run the commands: `ant`, `java`, `javac`, `poly`, and `dot`.

For Mac, you can install [Graphviz/dot](#) from the [Graphviz download site](#). Once installed, test it by making sure that the `dot` command can be executed in a shell (that it is in the path). On ubuntu/debian linux you quickly and easily install graphviz by typing:

```
sudo apt-get install graphviz
```

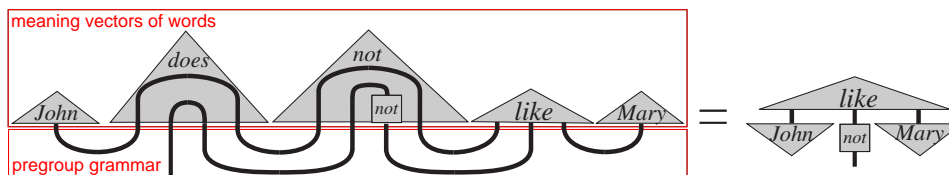
Assuming you have java, a recent java compiler, and graphviz installed, you can install everything else with the following shell commands:

```
### Make the Quantomatic directory, for all things quantomatic, and go there
mkdir Quantomatic; cd Quantomatic

### download and build PolyML
svn co https://polymml.svn.sourceforge.net/svnroot/polymml/fixes-5.3 polymml
cd polymml/polymml; ./configure --prefix=$(cd ..; pwd); make; make install; cd ../..

### download and build Quantomatic
svn co https://isaplanner.svn.sourceforge.net/svnroot/isaplanner/trunk/isaplib isaplib
svn co https://isaplanner.svn.sourceforge.net/svnroot/isaplanner/trunk/quantomatic quantomatic
cd quantomatic/gui; ant; cd ..
```

Besides automated theory exploration by means of quantomatic, this workpackage has also led to another spin-off in two very actual CS areas, namely compositional linguistics; both of these spin-off resulted in currently finalized multi-side proposals with world-leading groups, applied for to FP7 and EPSRC respectively. The computational linguistics activity grew out of the realization that quantum information flows can be used to compute how meaning of words in sentences propagates, when representing meaning by the standard vector space-based distributional model.



Workpackage 3: Classical-quantum interaction and information flow

This workpackage had as its main goal to delineate a notion of quantum information flow when quantum and classical systems are interacting. As compared to the purely classical counterpart to this, the situation is of course far more complicated here given that besides the flows between the quantum and the classical there are also the flows within the quantum itself subject to entanglement. We approached this involved problem from several angles.

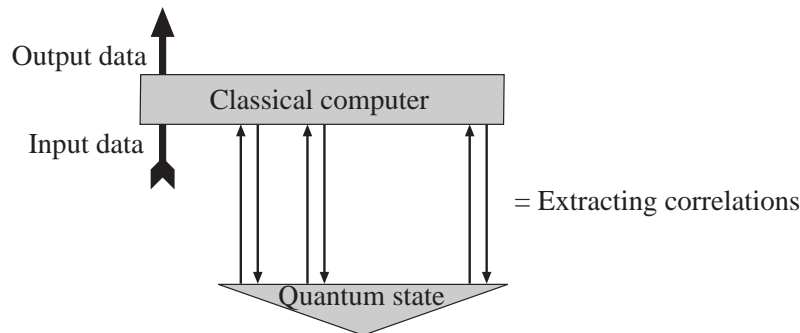
- *Resource inequalities.* The discovery by the QICS team of the so-called mother and father protocols in this quantum information resource calculus is a fundamentally significant development – it conceptually unifies a wide variety of previously diverse quantum information processing results, such as characterisation of noisy channel capacities, entanglement distillation, quantum broadcasting and state merging and many more.

- *Quantum data processing.* Here several results were obtained and a key fundamental issue of quantum computation viz. the relationship of classical to quantum computational complexity, and the characterisation of ways in which the latter is an extension of the former.
- *Categorical operational semantics.* Here it was shown that only a tiny bit of structure, namely abstract counterparts to copying and uniform erasing, turns out to be sufficient to extract from an abstract family of quantum processes, a variety of classical processes such as reversible classical processes, deterministic- and non-deterministic processes, stochastic processes and even informatic order in terms of majorisation. We were also able to prove the no-cloning theorem based on purely topological (cf. information flow) principles. The ‘final’ graphical calculus for quantum-classical interaction involved axiomatization of the concept of ‘environment’. The latter results in coinciding formal semantics for classical channel and measurement, all in terms of certain Frobenius algebras:



- *Coalgebraic structures and methods.* They are the natural mathematical framework to accommodate non-deterministic branching. We were able to recast a range of important quantum informatic concepts coalgebraically, making them subject to a variety of high-level methods.

A particularly original perspective bridging different workpackages is embodied by the following question: Can quantum correlations increase the capability to perform certain tasks for a classical computer? The main inspiration for this question comes from MQC since there we indeed have a classical control computer which turns quantum correlations, namely those of a cluster state, into a (polynomial) universal quantum computer.



Surprising results on the trade-off between classical computational power and the availability of physical resources resulted from this e.g. the $\oplus P$ complexity class can be boosted up to the **BQP** complexity class in the availability of either large cluster states, or three qubit GHZ correlations, or two-partite PR-box correlations. Another key results is the observation that for an important class of classically simulatable quantum circuits the threshold between Classical Computation and Quantum Computation is not related to entanglement, but rather just to the possibility to have far-away wires interacting with one another. Related to this turned out to be the fact that non-locality can be traced back to certain properties of small finite groups: while theories with phases that have $Z_2 \times Z_2$ as a subgroup allow local hidden variable representations, those with phases that have Z_4 as a subgroup are necessarily non-local theories.

QICS researchers have also introduced modifications to the standard theory of quantum mechanics and studied the computational power of these theories—as well as their mathematical structure—to cast light on the origins and limitations of quantum information processing. These modifications range from simple restrictions on the set of gates allowed in a quantum circuit, to esoteric non-local “post-quantum” theories. Most notably is the notion *information causality*.

QICS postdocs have also been involved in a number of experiments to test quantum non-contextuality.

Workpackage 4: Quantum automata, machines and calculi

This QICS workpackage is defining the state-of-the-art in this area. By studying several forms of abstract models of what quantum information processing devices can or should be, this workpackage has produced significant advances in understanding the structure, the mathematical and logical foundations, the operating principles and some of the computational properties of such devices. Here are some examples:

- What could it mean for a physical theory to be universal? A way to define a universal physical theory is to say that it is endowed with an object-to-object interaction which is non-trivial enough, so that any other object-to-object interaction could be built out of this one. In other words, this is not just a matter of being able to simulate a single (Quantum) Turing Machine, but being able to simulate a whole network of them in parallel, respecting the topology of the network and the way they interact. Explicit constructions in the simplified context of one-dimensional Quantum Cellular Automata have been made. A universal one-dimensional quantum cellular automata (QCA) capable of simulating all others has been described, and it has been proved that one-dimensional QCA always admit a two layered block representation and that their inverse is also a QCA; this last result came as a major surprise, since such a property does not hold for classical CA; a proof that every QCA can be put in the form of a tiling of more elementary, finite dimensional unitary evolutions, has also led to a clear and robust definition of n-dimensional QCA, phrased in the traditional setting of Hilbert spaces.
- Some of the the hard question on a denotational semantics for quantum programming languages have also been addressed. The most advanced known techniques are deployed to this end, including approaches via Game Theory and Category Theory. The outcome of this is that various important fragments of Quantum Programming Languages for Classically-Controlled Quantum Computation now possess a such a model, and that these models come in various flavours. One outstanding milestone obtained at the end of the project is a denotational semantics accommodating higher order functions in quantum functional languages.
- General methods have been introduced which serve the goal of proving the security of quantum cryptographic protocols. An example is an automated method which is based upon the operational semantics of a distributed quantum computation model, itself related to MBQC.
- A classically-controlled Turing machine which is significantly simpler than Deutsch's quantum Turing machine and which can be specialized into a pure measurement-based quantum Turing machine has been crafted.
- A language QML, has the significant advantage of a semantic domain directly built upon quantum objects and operations, but is restricted to first order; a translator from QML to quantum gate networks has recently been implemented.
- A connection between measurement-based quantum computations with graph states and the field of mathematical logic was established, showing that the computational power of graph states is reflected in the expressive power of classical formal logic languages defined on the underlying graphs.

Major events

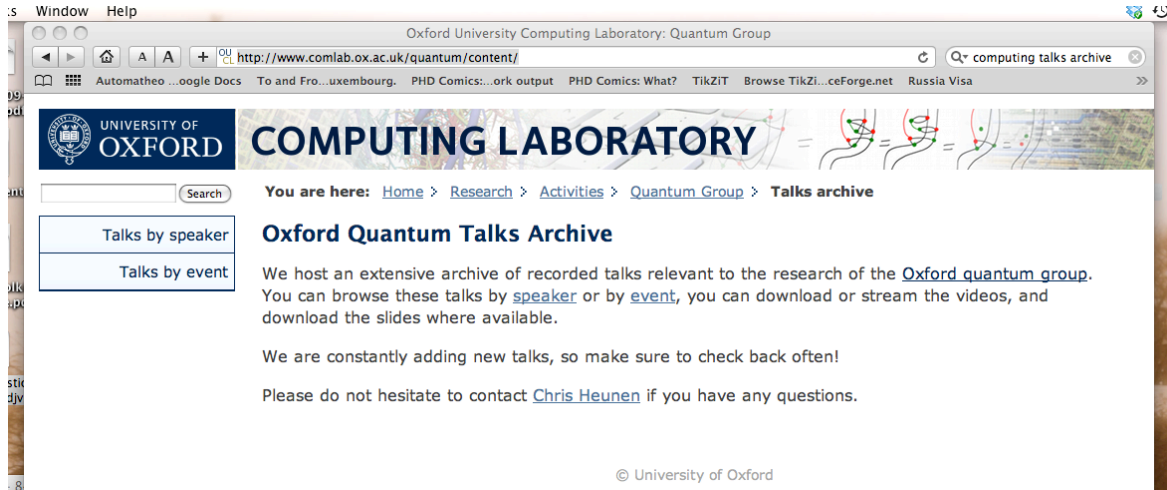
The major QICS conference took place in Obergurgl, Austria, September 14-20, 2008, hosted by Hans.-J. Briegel and the Innsbruck group, which was considered a major event in foundational Quantum Information and Computation research, also beyond the QICS network:

<http://www.uibk.ac.at/th-physik/qics-obergurgl2008/>

The QICS project was concluded with a very successful international school with as its main purpose the dissemination of the major advances made during the QICS project. All lectures given at the school are available for online viewing and download here:

<http://www.comlab.ox.ac.uk/quantum/events.html>

at the video archive maintained by the Quantum Group of the Oxford University Computing Laboratory:



Tutorial and survey publications

Two books with surveys and tutorials on research were produced, entitled *New Structures for Physics*, published by Springer, and *Semantic Techniques for Quantum Computation*, published by Cambridge University Press, mainly on W2–W4. A survey on W1 appeared in *Nature Physics*.

Consolidation of the community

Many QICS postdocs obtained faculty positions during the project.

Dissemination and use

Does not apply given the theoretical nature of the research.

Project webpage

http://se10.comlab.ox.ac.uk:8080/FOCS/FP6STREPQICS_en.html