QICS - PERIODIC ACTIVITY REPORT II

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 2008 – Dec. 31 2008

Date of preparation: Feb. 21st 2009

Start date of project: Jan. 1st 2007

Duration: 36 months

Contents

Part I

Publishable executive summary

Second year of QICS – executive account

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

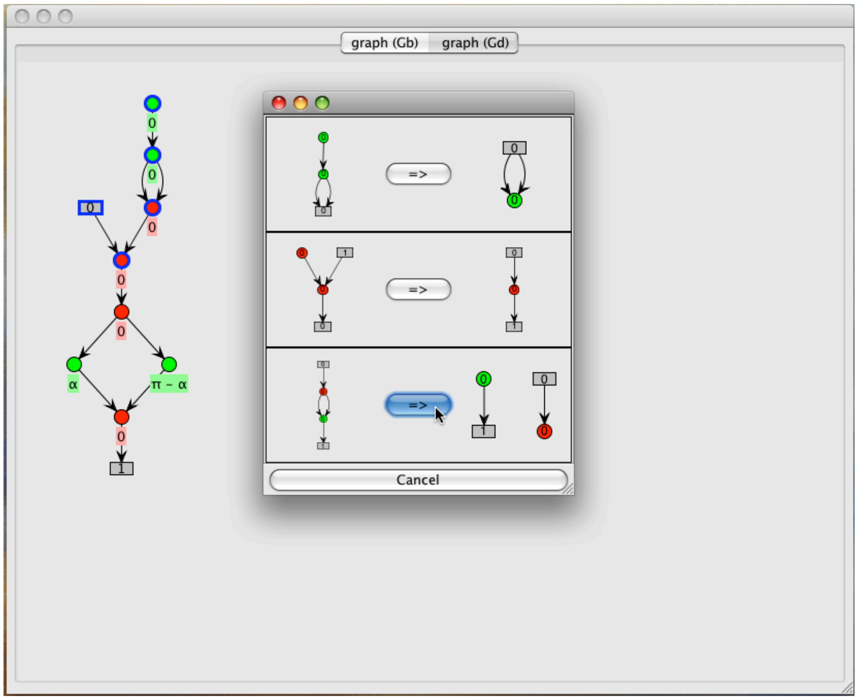
It is our pleasure to report on a very successful and exciting second year of QICS research. The ultimate goal of QICS, as stated in the initial proposal, is to radically increase our understanding of the foundational structures of quantum informatics. The *method* is a cross-disciplinary endeavour, 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 Braunschweig and Innsbruck,
- *logicians* who adopt novel structural tools such as category theory, type systems and formal calculi to cast quantum behaviour, mainly in McGill, 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 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, Oxford and Edinburgh/Paris.

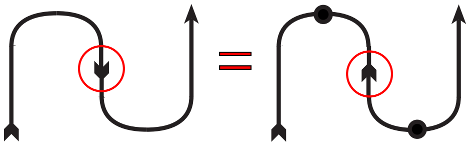
As it was the case during the first year, there were again many permutations of staff between the different QICS partners sites. We also held our first main conference, a very successful event with more than 100 participants which took place in the Austrian Alps:

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

The workpackage on *structures and methods for measurement-based quantum computation* [**W1**] has continued to be a fascinating platform for theoretical and experimental investigations of quantum computation.. A concise updated review by QICS members has been published in *Nature Physics* in January 2009. There are a couple of persistent central issues, which include: (i) fundamental questions on universality and the role of entanglement, (ii) good applications, e.g., the search for new quantum algorithms in the paradigm of MQC as well as complementarily the search for efficient classical simulation techniques, and (iii) investigations for a robust, feasible implementation of MQC 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 W1 than used to be in the beginning of the project. The converse is also true, methods resulting from MQC 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. To name one more result, regarding the computational power of quantum states, a new surprise is the observation that a randomly chosen generic pure state, in other words the majority of all states, is no more useful as a resource of measurement-based quantum computation than a string of random classical bits, regardless of the fact that the former is known to be highly entangled in some sense. This shows that much still remains to be discovered about the foundational nature of resource states for MQC, This brings us to the second workpackage, on *categorical semantics, logics and diagrammatic methods* [**W2**]. The research of this workpackage has reached unpreceded heights. A token of the quality of the work performed in this workpackage is that results by QICS researchers on complementary quantum observables became the first paper on Quantum Computation and Information to ever have been accepted by the Logic, Semantic, and Theory of Programming track (Track B) of the prestigious International Colloquium on Automata, Languages and Programming (ICALP). Another important result which is a first of its kind is Selinger's (McGill) 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.

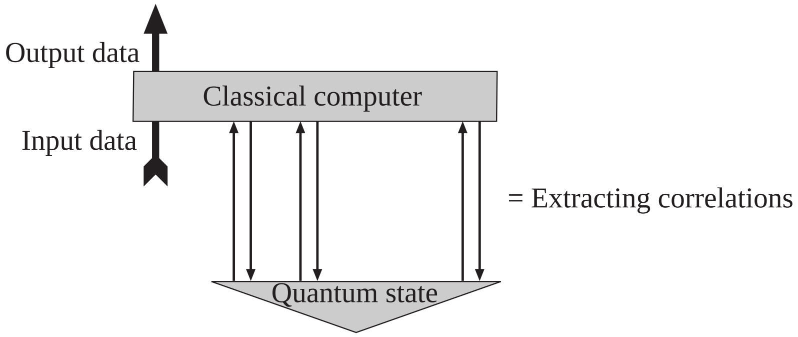


The tool as it currently stands will be demonstrated at the review meeting. There was also substantial progress on the understanding and applications of commutative special dagger Frobenius comonoids, on which we reported last year. A finer notion was introduced which enabled passing from logical reading to physical reading in teleportation-like protocols:



and representations of the interaction of the classical and the quantum information flows in MQC.

Workpackage [**W3**] has as its main goal to delineate a notion of quantum information flow when quantum and classical systems are interacting. A particularly original perspective on this 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. The origin of non-locality was also 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.

The QICS workpackage on *quantum automata, machines and calculi* [**W4**] 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.

- 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.

- 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 MQC.

Bob Coecke, Oxford, February 10, 2009.

`coecke@comlab.ox.ac.uk`

Computing Laboratory
University of Oxford
OX1 3QD Oxford
United Kingdom

Part II

Project objectives and major achievements during the reporting period

Chapter 1

Objectives, work done, comparison to state-of-the-art and other developments

The QICS abstract is available from:

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

1.1 Objectives of QICS as stated in the initial proposal

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.

Innovation and methodology. 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, utimately 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 piece-meal 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 inter-twined 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 comunication 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.

1.2 Objectives for the workpackages as stated in the initial proposal

Objectives as listed in the initial proposal for workpackage I are:

W1.O1 Gain a deeper understanding of the essential features of a quantum computation.

W1.O2 Develop a platform for formulating new measurement-based quantum algorithms.

W1.O3 Establish the basis for measurement-based computational complexity.

W1.O4 Identify the key resources for universal measurement-based quantum computation.

W1.O5 Design high-level calculi and diagrammatics for general measurement-based quantum computation.

Objectives as listed in the initial proposal for workpackage II are:

W2.O1 Find simple intuitive graphical calculi and more conceptually motivated constructions and proofs to replace the highly non-intuitive definitions and manipulations in terms of matrices.

W2.O2 Expose the foundational structure and axiomatic boundaries of QIC.

W2.O3 Study the structure of multipartite entanglement and distributed quantum systems.

W2.O4 Exploit the above for automated design and verification for algorithms and protocols.

W2.O5 Contribute to the quest of a general model for QIC by studying the topological QC model.

Objectives as listed in the initial proposal for workpackage III are:

W3.O1 Obtain a modular and compositional understanding on quantum informatic resources, extending the resource inequality calculus of Devetak/Harrow/Winter et al..

W3.O2 Expose the foundational structure and axiomatic boundaries of QIC.

W3.O3 Obtain a resource-sensitive logical understanding of No-cloning and No-deleting.

W3.O4 Develop a formalism in which quantum and classical data are treated at the same level, and in which the distinct abilities (cloning, deleting) to manipulate them are first-class citizens.

W3.O5 Use this formalism for qualitative and quantitative analysis of information flow in general QIC-models.

W3.O6 Use this formalism for the design of protocols and algorithms for non-standard QIC-models.

Objectives as listed in the initial proposal for workpackage IV are:

W4.O1 Develop a unified and fully general model for quantum computations under classical control.

W4.O2 Obtain a deeper and more logical understanding of possible quantum control structures for QIC.

W4.O3 Give satisfactory accounts of unitarity, irreversibility, universality and complexity in QCAs.

W4.O4 Merge computational and spatio-temporal notions within a single model of QIC.

W4.O5 Find a denotational semantics accommodating higher order functions in quantum functional languages.

W4.O6 Develop theories and techniques for analysis and verification of concurrent classical+quantum systems.

1.3 Comparison of these objectives to the current state-of-the-art

Please see the introduction to each of the workpackges.

1.4 Progress made on the objectives during the reporting period

Please see the introduction to each of the workpackges.

1.5 Next steps to be taken for reaching the objectives

Please see the the introduction to each of the workpackges.

Chapter 2

Recruitment, mobility, spin-off

The numerous visits of researchers between QICS sides, on which we reported in great detail in the 1st QICS Periodic Activity Report in §3.3, have of course continued. We won't provide details here.

The migration of postdocs between QICS sides reported on in 1st QICS Periodic Activity Report in §3.2 has also continued. To give some examples, Simon Perdrix who started his work on the QICS project in Grenoble, first became QICS postdoc in Paris, then became QICS postdoc in Grenoble, and now is QICS postdoc in Edinburgh, a new satellite from Paris. Elham Kashefi started her work on the QICS project in Oxford, then moved to Grenoble, and now has a lectureship in the new QICS satellite in Edinburgh. Eric Paquette started his work on the QICS project in McGill, and is now QICS postdoc in Oxford. Mehrnoosh Sadrzadeh worked both in Oxford and Montreal, then became a QICS postdoc in Paris, went back to Oxford, and will now go for a three month visit back to McGill.

Many QICS postdocs meanwhile also obtained prestigious postdoctoral fellowships at QICS sides which enables them to continue their QICS related research. As an example we mention the dynamics around the coordinating site Oxford. Ross Duncan, who was the first QICS postdoc at Oxford, obtained an EPSRC Postoctoral Fellowship at Oxford. Mehrnoosh Sadrzadeh, who was a QICS postdoc at Paris, recently also became an EPSRC Postoctoral Fellowship at Oxford. Simon Perdrix who was QICS postdoc in Paris, Oxford and Edinburgh, is now shortlisted for an interview for the same fellowship.

Other funding bodies have meanwhile awarded research grants on the basis of achievements of the QICS team. These bodies for example include the US Office of Naval Research (ONR), The Foundational Questions Institute (FQXi) and the British Engineering and Physical Sciences Research Council.

Chapter 3

QICS events and presentations

3.1 QICS events and QICS supported events

- The first major QICS even was the "QICS International Workshop on Foundational Structures for Quantum Information and Computation", Obergurgl, Austria, September 14-20, 2008, 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/`

  It was hosted by the Innsbruck QICS site headed by Briegel. It exposed the QICS activity to a broader community of researchers. Over 100 people attended the event. The speakers were Samson Abramsky (Oxford), Antonio Acin (ICFO Barcelona), Pablo Arrighi (QCG Grenoble), Howard Barnum (Los Alamos), Jonathan Barrett (Perimeter), Simon Benjamin (Oxford), Daniel Browne (UCL London), Ignacio Cirac (MPQ Garching), Bob Coecke (Oxford), Mauro D'Ariano (Pavia), Francesco De Martini (La Sapienza, Rome), Ross Duncan (Oxford), Jens Eisert (Imperial College), Chris Heunen (Nijmegen), Peter Hines (York), Richard Jozsa (Bristol), Elham Kashefi (QCG Grenoble), Pieter Kok (Sheffield), Barbara Kraus (Innsbruck), Damian Markham (Paris), Medhi Mhalla (QCG Grenoble), Akimasa Miyake (Innsbruck), Caterina Mora (IQC, Waterloo), Simon Perdrix (Oxford), Sandu Popescu (Bristol), Robert Raussendorf (UBC Vancouver), Peter Selinger (Dalhousie), Robert Spekkens (Cambridge), Maarten Van den Nest (MPQ Garching), Jamie Vicary (Imperial College), Philip Walther (Vienna), Reinhard Werner (Braunschweig), Alex Wilce (Selinsgrove), Andreas Winter (Bristol/Singapore), Pawel Wocjan (UCF, Orlando) and Zhen-Sheng Yuan (Heidelberg). There were also many contribute posters which had to be presented in two separate sessions. Besides the talks most of the afternoons were left open for discussions and work sessions.

- This large event was preceded by a smaller QICS workshop in Grenoble, April 4-6, 2008:

  `http://capp.imag.fr/qcg/qics2008/`

- Quantum Physics and Logic:

  `http://web.comlab.ox.ac.uk/people/Bob.Coecke/DCM_QPL_08.html`

  `http://web.comlab.ox.ac.uk/people/Bob.Coecke/QPL_09.html`

- There regular workshop series Categories, Logic and Foundations of Physics:

  `http://categorieslogicphysics.wikidot.com/`

- The QNET/QICS workshop on Semantics of Quantum Computation:

  `http://www.informatics.sussex.ac.uk/users/im74/QNET/QNWS3/`

3.2 Presentation of QICS output

As there are far too many presentations of QICS output by QICS members for a comprehensive overview we refer the reader to the evidence in the 1st QICS Periodic Activity Report in §4.3 of the range of events at which QICS papers have been presented and at which QICS members give invited talks. More details are available from the websites of QICS members.

Part III

Workpackage progress reports of the period *— includes project deliverables —*

This part consists of four chapters each of which represent a workpackage; these chapters are also separately available as a deliverable. They will be made available online, subject to some access restrictions, on the QICS webpage

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

respectively at:

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable5_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable6_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable7_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable8_en.html`

Each chapter is in turns divided in the tasks outlined in the original proposal, which, in terms of the focus of the performed work, are further divided. The basic units of research typically correspond with one or more papers, or a paper in preparation. Each such unit is labelled with the objects and milestones it addresses, as outlined in the initial proposal.

Each chapter starts with an introduction which explicitly addresses:

a. A general view on how the objectives for this workpackage relate to the current state-of-the-art of the topic of this workpackage — e.g. in the light of developments that might have taken place elsewhere by other teams or in other areas of science. What is their current importance as compared to their importance at the time of the draft phase of QICS; do they need to be adjusted, and in case of yes, how?

b. Which have been the main developments by the QICS team and main surprises for this workpackage, relative to the stated the objectives. This is cast within a *visionary* perspective on the activity within this workpackage.

c. How the work needs to evolve further i.e. what are the most important next steps for the QICS team to take within this workpackage, relative to the stated the objectives.

d. An appreciation on how this workpackage has interacted with other workpackage and an appreciation on how this workpackage involves interaction from different sites.

Then we list the worpackage's objectives, milestones and tasks as stated in the initial proposal.

Chapter 4

W1 – *deliverable D1*: Structures and methods for measurement-based quantum computation

A current account of the objectives of W1 and comparison with the state-of-the art.

Main developments in W1.

The next steps to take.

Interactions with other workpackages and sites.

Hans-Jurgen Briegel and Akimasa Miyake
Innsbruck, February 10, 2009.

Workpackage objectives :

W1.O1 Gain a deeper understanding of the essential features of a quantum computation.

W1.O2 Develop a platform for formulating new measurement-based quantum algorithms.

W1.O3 Establish the basis for measurement-based computational complexity.

W1.O4 Identify the key resources for universal measurement-based quantum computation.

W1.O5 Design high-level calculi and diagrammatics for general measurement-based quantum computation.

Workpackage milestones :

W1.M1 Results relating the mathematical structure of graph states to applications. (12)

W1.M2 Necessary and sufficient criteria for graph states to be universal in the one-way model. (12)

W1.M3 High-level languages following from the mathematical structure of graph states. (24)

W1.M4 New high-level methods to be used for solving the other challenges of this workpackage. (24)

W1.M5 Characterization of minimal resources sufficient for measurement based computation. (36)

W1.M6 Characterization of quantum computational complexity within measurement based models. (36)

Below we discuss the detailed progress for this workpackage which comprises the *workpackage tasks* :

W1.T1 Study normal forms for quantum algorithms in measurement-based computer models.

W1.T2 Study graph-theoretical characterizations of resources for measurement based quantum computation; develop necessary criteria for a graph state to be universal in the one-way model.

W1.T3 Develop calculi and diagrammatic methods for general measurement-based quantum computation, by using the structures and methods developed in W2, W3 and W4.

4.1 W1.T1: Normal forms for quantum algorithms in MQC

4.1.1 Computational universality of the resource states for measurement-based quantum computation

Progress report for measurement-based quantum computation (Objective: W1.O1, W1.O2, W1.O4; Milestones: W1.M1, W1.M2, W1.M5)

In [3], Briegel (Inn), Browne (UCL), Duer (Inn), and Van den Nest (Inn), in collaboration with Raussendorf, review recent developments in measurement-based quantum computation with regards to both fundamental and practical issues, in particular the power of quantum computation, the protection against noise (fault tolerance) and steps towards experimental realization. This article also highlights emerging connections between the field of measurement-based computation and other branches of physics and mathematics.

Phase transition of computational power of measurement-based quantum computer (Objective: W1.O1, W1.O3; Milestones: W1.M1, W1.M6)

In [4], Browne (Ox), Miyake (QICS postdoc at Inn) and their colleagues have tackled a fundamental question on the origin of the superior computational power of a quantum computer. They consider a simplified model, motivated by the optical lattice implementation of measurement-based quantum computer, and study how heralded qubit losses during the preparation of a two-dimensional cluster state, a universal resource state for one-way quantum computation, affect its computational power. Above the percolation threshold they present a polynomial-time algorithm that concentrates a universal cluster state, using resources that scale optimally in the size of the original lattice. On the other hand, below the percolation threshold, they show that single qubit measurements on the faulty (randomly filled) lattice can be efficiently simulated classically. They observe a phase transition at the threshold when the amount of entanglement in the faulty lattice, directly relevant to the computational power, changes exponentially.

Measurement-based quantum computational scheme in the gapped ground state of a two-body Hamiltonian (Objective: W1.O2, W1.O4; Milestones: W1.M4, W1.M5)

In [2], Miyake (QICS postdoc at Inn) and Brennen propose a scheme for a ground-code measurement-based quantum computer, which enjoys two major advantages. First, every logical qubit is encoded in the gapped degenerate ground subspace of a spin-1 chain with nearest-neighbor two-body interactions, which provides built-in robustness against noise. Second, the computation is processed by single-spin measurements along multiple chains dynamically coupled on demand. In this way, one keeps teleporting logical information into a gap-protected ground state of the residual chains, only after the interactions with the to-be-measured spins are turned off. Implementations are described using trapped atoms or polar molecules in an optical lattice, where the gap is expected to be as large as 0.2 kHz or 4.8 kHz respectively.

Quantum computation in correlation space and extremal entanglement (Objective: W1.O1, W1.O3, W1.O4; Milestones: W1.M2, W1.M4, W1.M5)

Recently, a framework was established to systematically construct novel universal resource states for measurement-based quantum computation using techniques involving finitely correlated states. With these methods, universal states were found which are in certain ways much less entangled than the original cluster state model, and it was hence believed that with this approach many of the extremal entanglement features of the cluster states could be relaxed. The new resources were constructed as “computationally universal” states–i.e. they allow one to efficiently reproduce the classical output of each quantum computation–whereas the cluster states are universal in a stronger sense since they are “universal state preparators”. In [6], Cai (Inn, QICS postdoc), Duer (Inn), Van den Nest (Inn), Miyake (Inn, QICS postdoc), and Briegel (Inn) show that the new resources are universal state preparators after all, and must therefore exhibit a whole class of extremal entanglement features, similar to the cluster states.

Are random pure states useful for quantum computation? (Objective: W1.O1, W1.O3, W1.O4, W2.O2, W2.O3, W4.O1, W4.O2; Milestones: W1.M2, W1.M4, W1.M6, W2.M3, W4.M1, W4.M2)

In [1] Bremner (Bris; QICS postdoc), Mora and Winter (Bris) show the following: a randomly chosen pure state as a resource for measurement-based quantum computation, is - with overwhelming probability - of no greater help to a polynomially bounded classical control computer, than a string of random bits. Thus, unlike the familiar cluster states, the computing power of a classical control device is not increased from P to BQP, but only to BPP. The same holds if the task is to sample from a distribution rather than to perform a bounded-error computation. Furthermore, they show that their results can be extended to states with significantly less entanglement than random states.

4.1.2 Computational and algorithmic complexity of quantum computation

Noisy quantum simulation for quantum computation (Objective: W1.O2, W1.O3; Milestones: W1.M1, W1.M6)

In [10], Duer(Inn), Bremner(QICS postdoc at Bris), and Briegel(Inn) investigate the influence of noise in quantum simulation. They consider errors in the interaction Hamiltonians for different noise models, including e.g. timing errors in pairwise interactions. They analyze and compare the effect of noise for the different simulation methods and propose methods to significantly reduce the influence of noise by making use of entanglement purification together with a teleportation-based protocol, using graph-state resources. These investigations are also of relevance for the investigation of quantum computational scheme, since the methods to generate many-body interaction Hamiltonians automatically lead to quantum many-body gates. The error analysis also applies to gates generated in this way, and the methods for noise reduction (e.g. entanglement purification) can be applied.

Renormalization algorithm with graph enhancement (Objective: W1.O2, W1.O3; Milestones: W1.M1, W1.M4)

In [15], Huebener (Inn), Kruszynska (Inn), Hartmann (Inn), and Duer (Inn) in collaboration with Verstraete, Eisert, and Plenio, find a way to improve the density-matrix renormalization method, a standard algorithm in condensed matter physics, with the help of graph state related techniques. They introduce a class of variational states to describe quantum many-body systems. This class generalizes matrix product states which underlie the density-matrix renormalization group approach by combining them with weighted graph states. States within this class may (i) possess arbitrarily long-ranged two-point correlations, (ii) exhibit an arbitrary degree of block entanglement entropy up to a volume law, (iii) may be taken translationally invariant, while at the same time (iv) local properties and two-point correlations can be computed efficiently. This new variational class of states can be thought of as being prepared from matrix product states, followed by commuting unitaries on arbitrary constituents, hence truly generalizing both matrix product and weighted graph states. They use this class of states to formulate a renormalization algorithm with graph enhancement (RAGE) and present numerical examples demonstrating that improvements over density-matrix renormalization group simulations can be achieved in the simulation of ground states and quantum algorithms. Further generalizations, e.g., to higher spatial dimensions, are outlined.

Link to W3.T2: Classical simulation of quantum computation etc.

Matchgate circuits: a gap between universal quantum computation and classically simulatable computation (Objective: W1.O1, W1.O2, W3.O2, W3.O4; Milestones: W1.M4, W1.M6, W3.M4). See 6.2.4.b [17].

Quantum algorithms for spin models and classically simulable gate sets (Objective: W1.O1, W1.O2, W3.O2, W3.O4; Milestones: W1.M4, W1.M6, W3.M4)

In [27], Van den Nest (Inn), Duer (Inn), and Briegel (Inn) together with Raussendorf present elementary mappings between classical lattice models and quantum circuits. These mappings provide a general framework to obtain efficiently simulatable quantum gate sets from exactly solvable classical models. For example, they recover and generalize the simulability of Valiant's match-gates by invoking the solvability of the free-fermion eight-vertex model. Our mappings furthermore provide a systematic formalism to obtain simple quantum algorithms to approximate partition functions of lattice models in certain complex-parameter regimes. For example, they present an efficient quantum algorithm for the six-vertex model as well as a 2D Ising-type model. They finally show that simulating our quantum algorithms on a classical computer is as hard as simulating universal quantum computation (i.e. BQP-complete).

Efficiently contractable quantum circuits cannot produce much entanglement (Objective: W1.O1, W1.O4, W3.O2, W3.O4; Milestones: W1.M4, W1.M6, W3.M4)

In [24] Yoran (Bris) shows a similarity between two different classical simulation methods for measurement-based quantum computation – one relying on a low entanglement (tree tensor network) representation of the computer's state, and the other a tensor contraction method based on the topology of the graph state. He uses this similarity to show that any quantum circuit that can be efficiently simulated via tensor contraction cannot produce much entanglement.

4.1.3 General properties for measurement-based quantum computation

Link to W4.T3: Logic within quantum computational models

Undecidable logic and measurement-based quantum computation (Objective: W1.O1, W1.O4, W4.O1, W4.O6; Milestones: W1.M2, W1.M5, W4.M3)

In [25], Van den Nest (Inn) and Briegel (Inn) establish a connection between measurement-based quantum computation with graph states and the field of mathematical logic. They show that the computational power of graph states, representing resources for measurement-based quantum computation, is reflected in the expressive power of (classical) formal logic languages defined on the underlying mathematical graphs. In particular, the authors show that for all graph state resources which yield a computational speed-up with respect to classical computation, the underlying graphs—describing the quantum correlations of the states—are associated with undecidable logic theories. Here undecidability is to be interpreted in a sense similar to Gödel's incompleteness results, meaning that there exist propositions, expressible in the above classical formal logic, which cannot be proven or disproven.

4.2 W1.T2: Graph-theoretical characterization of resources for MQC

4.2.1 Resources for measurement-based quantum computing

Quantum stabilizer formalism and classical spin systems (Objective: W1.O1, W1.O2; Milestones: W1.M1, W1.M3)

In [16], Huebener (Inn), Van den Nest (Inn), Duer (Inn), and Briegel (Inn) further explore general mappings between classical spin systems and quantum physics, continuing earlier work from the previous reporting period. They show how to express partition functions and correlation functions of arbitrary classical spin models as inner products between quantum stabilizer states and product states, thereby generalizing mappings for some specific models established in the previous paper by some of the same authors [Phys. Rev. Lett. 98, 117207 (2007)]. These mappings establish a link between the fields of classical statistical mechanics and quantum information theory, which can be used to transfer techniques between the fields. They allow one, for example, to recover well-known duality relations and local symmetries of classical models in a simple way, but also to provide new classical simulation methods to simulate types of classical spin models. It is shown that in this way all inhomogeneous models of q-dimensional spins with pairwise interaction pattern specified by a graph of bounded tree-width can be simulated efficiently.

Completeness of classical spin models and simple lattice gauge theories and its relation to universal quantum computation (Objective: W1.O1, W1.O2; Milestones: W1.M1, W1.M3)

Van den Nest (Inn), Duer (Inn), De las Cuevas (Inn) and Briegel (Inn), partly in collaboration with Martin-Delgado, found that that results and techniques from the theory of graph states and quantum computation, in particular the universality of cluster states, can be used to gain new insight in statistical mechanics and simple lattice gauge theories.

In [26], they prove that the 2D Ising model is complete in the sense that the partition function of any classical q-state spin model (on an arbitrary graph) can be expressed as a special instance of the partition function of a 2D Ising model with complex inhomogeneous couplings and external fields. In the case where the original model is an Ising or Potts-type model, they find that the corresponding 2D square lattice requires only polynomially more spins w.r.t the original one, and they give a constructive method to map such models to the 2D Ising model. For more general models the overhead in system size may be exponential. The results are established by connecting classical spin models with measurement-based quantum computation and invoking the universality of the 2D cluster states.

In [9], these studies are extended and deepened. In order to obtain the completeness result in [26], one had to assume complex values for the coupling strengths on the 2D lattice, with no obvious physical interpretation. In [9] it is however shown that a complete model with only real -and, hence, “physical”- couplings can be obtained if one goes to the 3D Ising model. It is furthermore shown how to map general q-state systems with possibly many-body interactions to the 2D Ising model with complex parameters, and how to obtain completeness results for these models with real parameters. It is also demonstrated that the computational overhead in these constructions is in all relevant cases polynomial.

In [8], it is shown that the partition function of all classical spin models, including all discrete Standard Statistical Models and all Abelian discrete Lattice Gauge Theories (LGTs), can be expressed as a special instance of the partition function of the 4D Z_2 LGT. In this way, all classical spin models with apparently very different features are unified in a single complete model, and a physical relation between those models is established. As applications of this result, a new method is presented how to do mean field theory for Abelian discrete LGTs with d¿3, and it is shown that the computation of the partition function of the 4D Z_2 LGT is a computationally hard (#P-hard) problem. These results can be extended to Abelian continuous models, for which the approximate completeness of the 4D Z_2 LGT can be proven.

Dissipative preparation of multipartite entangled states (Objective: W1.O2, W1.O4; Milestones: W1.M1, W1.M4)

In [18], Kraus (Inn) and collaborators investigate the possibility of using a dissipative process to prepare a quantum system in a desired state, including the resources for measurement-based quantum computation. They derive for any multipartite pure state a dissipative process for which this state is the unique stationary state and solve the corresponding master equation analytically. For certain states, such as the cluster states, they use this process to show that the jump operators can be chosen quasilocally, i.e. they act nontrivially only on a few, neighboring qubits. Furthermore, the relaxation time of this dissipative process is independent of the number of subsystems. They demonstrate the general formalism by considering arbitrary matrix-product states or projected entangled pair states. In particular, they show that the ground state of the Affleck-Kennedy-Lieb-Tasaki model can be prepared employing a quasi-local dissipative process.

Multipartite entanglement and global information (Objective: W1.O4; Milestones: W1.M1, W1.M5)

In [19], Kruszynska (Inn) and Kraus (Inn) investigate the entanglement properties of pure quantum states describing n qubits. They 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. They give a simple characterization of these states and construct a complete set of commuting unitary observables which characterize the state uniquely. Furthermore they show how these states can be prepared and discuss their applications.

Scheme for directly measuring entanglement (Objective: W1.O2; Milestones: W1.M3, W1.M4)

In [7], Cai (QICS postdoc at Inn) and Song reveal an intrinsic connection between maximally entangled states and certain entanglement measures, and propose novel schemes for measuring entanglement of general states without state prior reconstruction. Our schemes are parametrically efficient and feasible in various kinds of physical systems. In particular, they demonstrate that for two-qubit entangled states, local factorizable projective measurements performed on a small number of copies are sufficient without extra requirement for state generation.

4.2.2 General and mathematical properties of graph states

Non-locality for graph states (Objective: W1.O1, W1.O4; Milestones: W1.M1, W1.M3)

Guehne (QICS postdoc at Inn) and his colleagues work on a fundamental aspects of graph states, such as their non-locality, methods for an efficient detection of such state in the photon experiments, and on applications for quantum simulation.

In [5], it is shown that any n-qubit state with n independent perfect correlations is equivalent to a graph state. They present the optimal Bell inequalities for perfect correlations and maximal violation for all classes of graph states with $n < 7$ qubits. Twelve of these inequalities were previously unknown and four give the same violation as the Greenberger-Horne-Zeilinger state, although the corresponding states are more resistant to decoherence.

In [12], the authors derive Bell inequalities for graph states by generalizing the approach proposed by Ardehali [Phys. Rev. A 46, 5375 (1992)] for Greenberger-Horne-Zeilinger (GHZ) states. Using this method, they demonstrate that Bell inequalities with non-stabilizer observables are often superior to the optimal GHZ-Mermin-type (or stabilizer-type) Bell inequalities.

Hyper-entangled ten-qubit Schrödinger cat states (Objective: W1.O4; Milestones: W1.M1, W1.M3)

In collaboration with the experimental group of J.W. Pan in Hefei, Guehne (QICS postdoc at Inn) contributed to the experimental creation of a ten-qubit GHZ state using hyper-entanglement of five photons [11]. One the one hand, this constitutes the largest entangled multi-qubit state so far, on the other hand, the experimental techniques employed here enable the generation of different graph states of up to ten qubits, which will lead to many new experiments and proof of principle demonstrations of measurement based quantum computation. Guehne et al. provided the theoretical methods to analyze this experiment (for a review see [14]), and these methods have also be used for a variety of other experiments in which graph states have been observed.

Simulating anyonic fractional statistics with a six-qubit graph state (Objective: W1.O4; Milestones: W1.M1, W1.M3)

Anyons are exotic quasiparticles living in two dimensions that do not fit into the usual categories of fermions and bosons, but obey a new form of fractional statistics. In [20] and following a recent proposal, Guehne (QICS postdoc at Inn) in collaboration with J.-W. Pan's group contributes to an experimental demonstration of the fractional statistics of anyons in the Kitaev spin lattice model using a photonic quantum simulator. They dynamically create the ground state and excited states (which are six-qubit graph states) of the Kitaev model Hamiltonian, and implement the anyonic braiding and fusion operations by single-qubit rotations. A phase shift of π related to the anyon braiding is observed, confirming the prediction of the fractional statistics of Abelian 1/2-anyons.

Optical network for deterministic preparation of two-dimensional cluster states (Objective: W1.O4; Milestones: W1.M1, W1.M4)

The optical quantum computer is one of the few experimental systems to have demonstrated small scale quantum information processing. Making use of cavity quantum electrodynamics approaches to operator measurements, in [23] O'Brien (Bris) and co-authors detail an optical network for the deterministic preparation of arbitrarily large two-dimensional cluster states. They show that this network can form the basis of a large scale deterministic optical quantum computer that can be fabricated entirely on chip.

LU-LC conjecture in graph states (Objective: W1.O3, W1.O4; Milestones: W1.M1, W1.M6)

In [13], Van den Nest (Inn) and Gross report progress on the LU-LC conjecture - an open problem in the context of entanglement in stabilizer states (or graph states). This conjecture states that every two stabilizer states which are related by a local unitary operation, must also be related by a local operation within the Clifford group. The contribution of this paper is a reduction of the LU-LC conjecture to a simpler problem. As the main result, the authors show that, if the LU-LC conjecture could be proved for the restricted case of diagonal local unitary operations, then the conjecture is correct in its totality. Furthermore, the reduced version of the problem, involving such diagonal local operations, is mapped to questions regarding quadratic forms over the finite field GF(2). Finally, the authors prove that correctness of the LU-LC conjecture for stabilizer states implies a similar result for the more general case of stabilizer codes.

They also note that the theoretical results of [13] were subsequently used by Ji et al. (arXiv:0709.1266) to completely resolve the LU-LC conjecture; these authors use the results of [13] to generate a counter example, showing that the conjecture is false.

Graph states as ground states of many-body Hamiltonians (Objective: W1.O3, W1.O4; Milestones: W1.M1, W1.M5)

In [28], Van den Nest (Inn), Luttmer (Inn), Duer (Inn), and Briegel (Inn) have analyzed the criteria when graph states are obtained as non-degenerate ground states of interaction Hamiltonians. While they find that many-body interactions are required for any graph state not corresponding to a 1D structure if one considers systems of a fixed size, the usage of auxiliary systems allows for the design of two-body Hamiltonian that have graph states as approximate ground state. This research is of particular interest in the context of the optical lattices, as it provides a potential alternative way of preparing highly entangled resource states (such as graph states) by simply cooling a system with a properly designed interaction Hamiltonian. This might be easier than generating entanglement by performing sequences of gates on some initial prepared product state in a coherent way.

Graph states for quantum secret sharing (Objective: W1.O6; Milestones: W1.M1)

In [21] D. Markham (Paris, QICS postdoc), in collaboration with B. Sanders, developed a set of secret sharing schemes on graph states. This approach has several advantages. First, it generalizes and unites previous schemes to offer a more complete picture of quantum secret sharing. Second, as graph states are the most studied and almost the only multiparty states in the laboratory these schemes have most chance of implementation. Finally, the graphical understanding of these schemes has allowed us to integrate understanding of measurement based quantum computing via the measurement calculus and express the schemes with respect to flow. This leads to an extension of the ideas of Danos (Paris) and Kashefi (Gre) flow beyond MBQC to more general schemes and the prospect of integrated quantum information networks consisting of computation and secret sharing amongst other tasks, all described in the same framework of flow.

4.3 W1.T3: Calculi and diagrammatic methods for general MQC, using W2, W3 W4

Finding optimal flows of deterministic one-way computation (Objective: W1.O1, W1.O3, W1.O4, W1.O5; Milestones: W1.M1, W1.M5, W1.M6)

In [22], Mhalla (Gre) and Perdrix (Gre & OX & Paris; QICS Postdoc) introduce an efficient classical algorithm for finding generalised flow of minimal depth in a given graph. Generalised flow has been proved earlier by Browne, Kashefi, Mhalla and Perdrix to be a full characterisation of deterministic computation in the one-way model. As a consequence, this algorithm for finding flow efficiently can be used for deciding whether a deterministic computation can be driven on a given resource (described by a graph). Moreover, since the flow produced by the algorithm is of minimal depth, it provides an automatic method for optimising the depth of deterministic one-way computations.

Bibliography

[1] M. J. Bremner, C. Mora and A. Winter (2008) *Are random pure states useful for quantum computation?*, arXiv:0812.3001.

[2] G. K. Brennen and A. Miyake (2008) *Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian*, Phys. Rev. Lett. 101, 010502.

[3] H. J. Briegel, D. E. Browne, W. Duer, R. Raussendorf and M. Van den Nest (2009) *Measurement-based quantum computation*, Nature Physics 5 1, pp. 19–26.

[4] D. E. Browne, M. B. Elliott, S. T. Flammia, S. T. Merkel, A. Miyake and A. J. Short (2008) *Phase transition of computational power in the resource states for one-way quantum computation*, New. J. Phys. 10, 023010.

[5] A. Cabello, O. Guehne and D. Rodriguez (2008) *Mermin inequalities for perfect correlations*, Phys. Rev. A 77, 062106.

[6] J. M. Cai, W. Duer, M. Van den Nest, A. Miyake and H. J. Briegel (2009) *Quantum computation in correlation space and extremal entanglement*, arXiv:0902.1097.

[7] J. Cai and W. Song, *Novel schemes for directly measuring entanglement of general states*, Phys. Rev. Lett. 101, 190503.

[8] G. De las Cuevas, W. Duer, H. J. Briegel and M. A. Martin-Delgado (2008) *Unifying all classical spin models in a Lattice Gauge Theory*, arXiv:0812.3583.

[9] G. De las Cuevas, W. Duer, M. Van den Nest and H. J. Briegel (2008) *Completeness of classical spin models and universal quantum computation*, arXiv:0812.2368.

[10] W. Duer, M. Bremner and H. J. Briegel (2008) *Quantum simulation of interacting high-dimensional systems: the influence of noise*, Phys. Rev. A 78, 052325.

[11] W.-B. Gao, C.-Y Lu, X.-C. Yao, P. Xu, O. Guehne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen and J.-W. Pan (2008) *Experimental demonstration of a hyper-entangled ten-qubit 'Schro"dinger cat' state*, arXiv:0809.4277.

[12] O. Guehne and A. Cabello (2008) *Generalized Ardehali-Bell inequalities for graph states*, Phys. Rev. A 77, 032108.

[13] D. Gross and M. Van den Nest (2008) *The LU-LC conjecture, diagonal local operations and quadratic forms over $GF(2)$*, Quantum Information and Computation 8, 263.

[14] O. Guehne and G. Toth (2008) *Entanglement detection*, arXiv:0811.2803.

[15] R. Huebener, C. Kruszynska, L. Hartmann, W. Duer, F. Verstraete, J. Eisert and M. B. Plenio (2008) *Renormalization algorithm with graph enhancement*, arXiv:0802.1211.

[16] R. Huebener, M. Van den Nest, W. Duer and H. J. Briegel (2008) *Classical spin systems and the quantum stabilizer formalism: general mappings and applications*, arXiv:0812.2127

[17] R. Jozsa and A. Miyake (2008) *Matchgates and classical simulation of quantum circuits*, Proc. R. Soc. A 464, pp. 3089–3106.

[18] B. Kraus, H. P. Buechler, S. Diehl, A. Kantian, A. Micheli and P. Zoller (2008) *Preparation of Entangled States by Quantum Markov Processes*, Phys. Rev. A 78, 042307.

[19] C. Kruszynska and B. Kraus (2008) *Multipartite entanglement and global information*, arXiv:0808.3862.

[20] C.-Y. Lu, W.-B. Gao, O. Guehne, X.-Q. Zhou, Z.-B. Chen, and J.-W. Pan (2009) *Demonstrating anyonic fractional statistics with a six-qubit quantum simulator*, Phys. Rev. Lett. 102, 030502.

[21] D. Markham and B. Sanders (2008) *Graph States for Quantum Secret Sharing*. Phys. Rev. A 78, 042309.

[22] M. Mhalla and S. Perdrix (2008) *Finding optimal flow efficiently*. 35th International Colloquium on Automata, Languages and Programming, Track A (ICALP'08). Lecture Notes in Computer Science (LNCS) vol. 5125, pp. 857–868.

[23] A. M. Stephens, Z. W. E. Evans, S. J. Devitt, A. D. Greentree, A. G. Fowler, W. J. Munro, J. L. O'Brien, Kae Nemoto and L. C. L. Hollenberg (2008) *A deterministic optical quantum computer using photonic modules*. Phys. Rev. A 78, 032318 (2008). arXiv:0805.3592.

[24] N. Yoran (2008) *Efficiently contractable quantum circuits cannot produce much entanglement*. arXiv:0802.1156.

[25] M. Van den Nest and H. J. Briegel (2008) *Measurement-based quantum computation on graph states and undecidable logic theories*, Foundations of Physics 38 5, pp. 448–457.

[26] M. Van den Nest, W. Duer and H. J. Briegel (2008) *Completeness of the classical 2D Ising model and universal quantum computation*, Phys. Rev. Lett. 100, 110501.

[27] M. Van den Nest, W. Duer, R. Raussendorf and H. J. Briegel (2008) *Quantum algorithms for spin models and simulable gate sets for quantum computation*, arXiv:0805.1214.

[28] M. Van den Nest, K. Luttmer, W. Duer and H. J. Briegel (2008) *Graph states as ground states of many-body spin-1/2 Hamiltonians*, Phys. Rev. A 77, 012301.

Chapter 5

W2 – *deliverable D2*: Categorical semantics, logics and diagrammatic methods

A current account on the objectives of W2 and comparison with the state-of-the art. The work in QICS on this subject is the state-of-the art. The area was pioneered and is further developed mainly by QICS members.

The research of this workpackage has reached unpreceded heights. A token of the quality of the work performed in this workpackage is that results by Coecke (Ox) and Duncan (Ox; QICS Postdoc at the time that these results were obtained) in complementary quantum observables[1] [6] became the first paper on Quantum Computation and Information to ever have been accepted by the Logic, Semantic, and Theory of Programming track (Track B) of the prestigious International Colloquium on Automata, Languages and Programming (ICALP).

Another important result which is a first of its kind is Selinger's (McGill) 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 been made on "quantomatic", a software tool for quantum reasoning based on the diagrammatic calculus. The tool as it currently stands will be demonstrated at the review meeting.

Main developments in W2. The most important results obtained are the following:

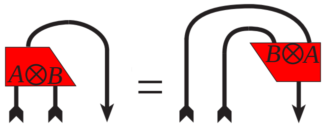
Complementary quantum observables. We reported on this last year; see above.

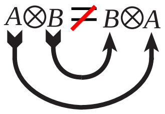
Completeness of finite dimensional Hilbert spaces for dagger compact categories. See above.

Further development of the theory of basis structures. Last year, both in the research reviews of W1 and W3, we extensively reported on the use of special commutative dagger Frobenius comonoids and how they can be used to represent bases, observables and classical data flow. Work on this topic has continued with several successful outcomes.

- In [9] it was shown that special commutative dagger Frobenius comonoids do not only allow to faithfully encode bases but that they are exactly the same thing as bases in the category of finite dimensional Hilbert spaces and linear maps. This is an important new mathematical theorem which will yield many important applications in a variety of areas. In [25] it was moreover shown that if we drop commutativity, we obtain all finitary C*-algebras, an important mathematical result on operator algebras which was recently accepted for publication in Communications in Mathematical Physics.

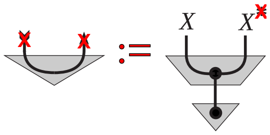
- In [12], an annoying dilemma was resolved. Compact structures involve an object X and its dual X^* and these need to be different for a planar graphical calculus since we need to be able to set $(A \otimes B)^* = B^* \otimes A^*$ as the following pictures indicate:



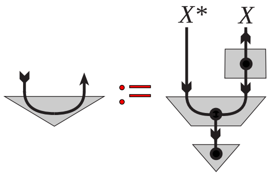


On the other hand, each special commutative dagger Frobenius comonoid, or in short, basis structure, induces a self-dual compact structure:

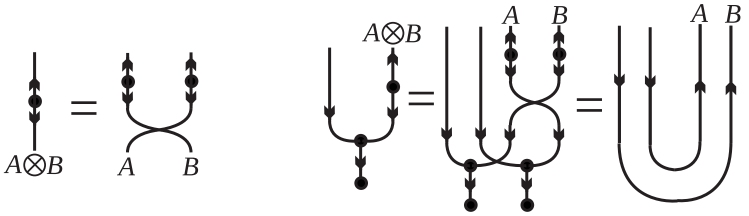
[1] We reported on these results in the previous QICS progress report.



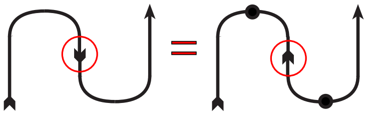
The solution is to introduce a unitary comonoid homomorphism, the ‘dualiser’ $A \simeq A^*$ which allows to set:



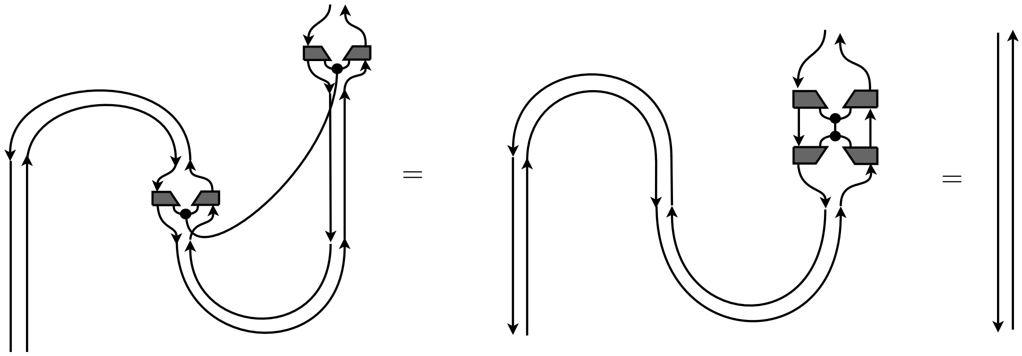
Now we have:



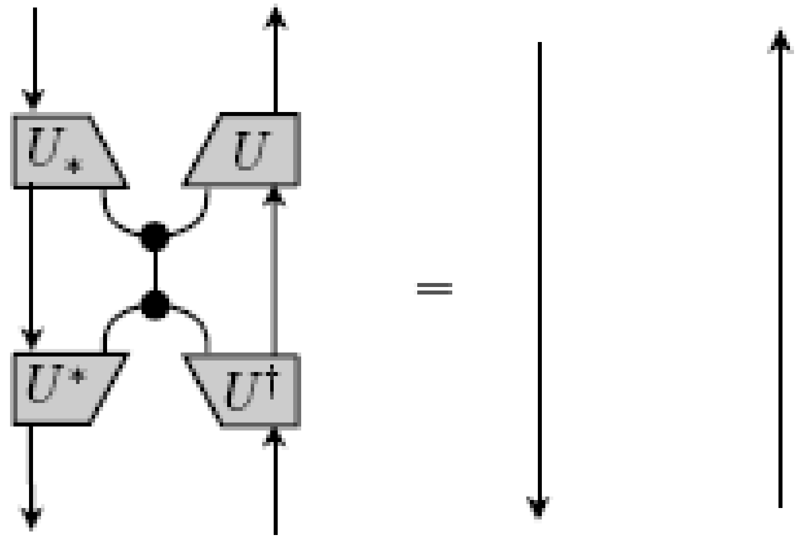
This in particular also allows to pass from logical reading to physical reading in teleportation-like protocols:



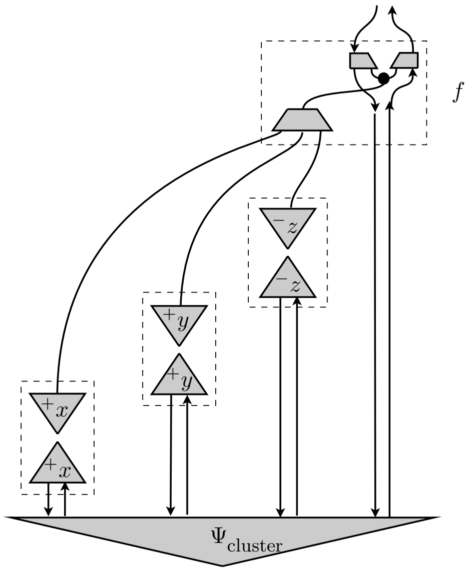
- In [11] the capability of basis structures to describe classical data was fully exploited. It enables in arbitrary symmetric monoidal categories to define functions, relations, permutations, stochastic maps, doubly stochastic maps, majorisation ordering and other concepts. A high-level description of the interaction of quantum and classical data operations make use of Kleisli construction and Grothendieck construction was introduced and studied. This results in a correctness proof of quantum teleportation looks as follows:



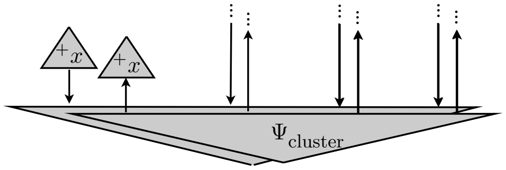
where single wires represent classical data and double wires represent quantum data, and where the equality:



is an 'indexed' version of unitarity. Post-selected cluster state computation with unitary corrections looks as follows:



where the bra's and $\Psi_{cluster}$ each in fact correspond to two triangles:

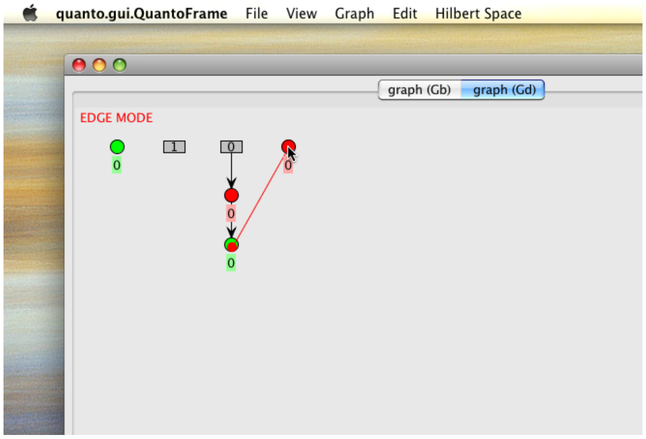


where we can use the categorical semantics for complementary observables to describe the internal structure of the cluster state, and its behaviour under under single-qubit measurements.

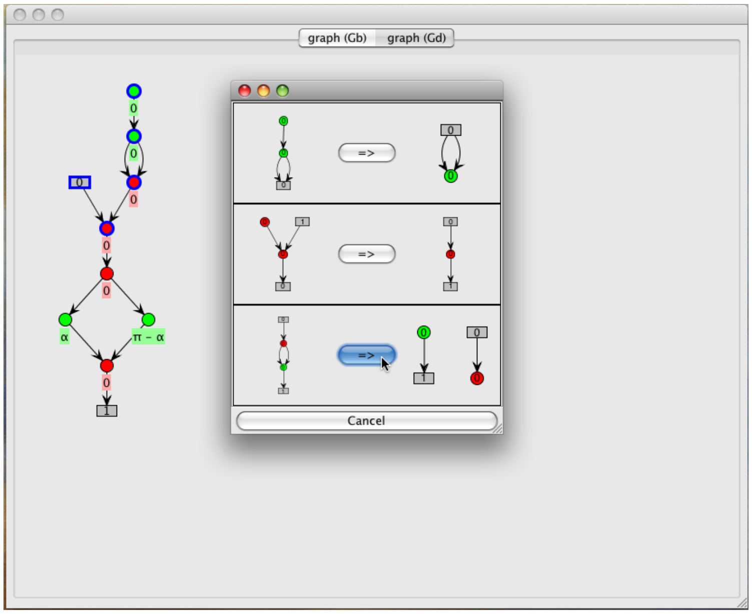
- In [18] the previous two were blended together.

Automation based on graphical calculus: quantomatic. Compact categories admit a faithful diagrammatic notation such that the structural equations of the theory are precisely captured by homotopy: if one diagram can be continuously deformed to another, then the terms they represent are equal. To represent quantum computations we consider a class of diagrams built up from certain basic operations, modulo some equations. By redrawing the diagrams according to the equations we show that different processes are equivalent – for example to simulate the execution of a quantum algorithm. However, these diagrams quickly become large and complicated, and their manual manipulation is slow and error-prone. For this reason we have developed *quantomatic*, a semi-automatic proof assistant based on graph rewriting.

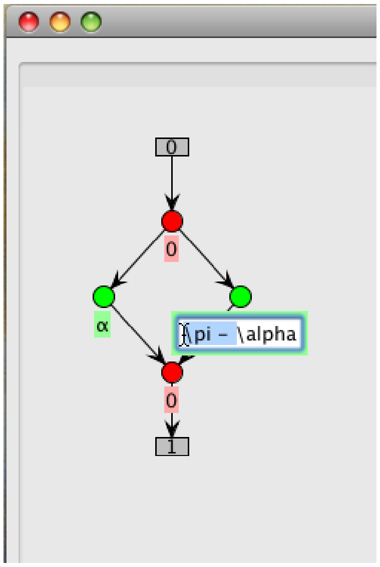
Quantomatic represents diagrams as graphs whose vertices have certain prescribed types; the equations are given as graph rewrites.



Using its graphical front end, the user can define graphs corresponding to quantum systems, and manipulate them according to the rewrite rules of the theory. A rewrite sequence from one graph to another is a proof that the two graphs represent equivalent quantum systems. These rewrites can be chosen from a list of possibilities,



or the program can run in automatic mode, taking advantage of strong normalisation results for certain subtheories. Quantomatic moreover incorporates a syntactic feature called a !-box; this permits infinite families of graphs to be represented by a single diagram. (This is used, for example to formalise “the spider rule” discussed below.) The theory of rewriting over such infinite families has been elaborated by Dixon (Edinburgh) and the tool is capable of working with these. Quantomatic therefore provides a powerful tool for proving the correctness of protocols, simulating algorithms, and exploring the structure of entangled quantum states.



In a sense we can view the graphs of quantomatic as a primitive quantum programming language, and the tool itself is a simulator to which can execute these programs. But there is more.

The categorical formalism of quantum mechanics is a live research topic and so the inference rules and term language of the tool must be easily modified. Quantomatic achieves this by implementing a generic rewriting system where the rewrite rules can be modified at runtime. Further, the categorical formulation of quantum mechanics is incomplete, in the sense that certain equations true in the Hilbert space model are not provable. Quantomatic addresses this problem in two ways:

- Firstly, it has the ability to find results combinatorially by exhaustively searching a finite input space. For graphs of quantum states, we can often deduce results by plugging a certain combination of so-called "classical points" (concretely: basis vectors) into the boundaries of the graph. If our vector space is finite-dimensional, we can search the whole space of classical inputs to see which induce a (machine-recognisable) change to the graph topology, such as the disconnection of components or reduction of cycle count. Such explorations can offer insight into various measures and descriptions of the entanglement of particles.

- Secondly, quantomatic can convert graphs into concrete matrices and test equalities using a computer algebra system. For a candidate identity $G = H$, we can often generate matrix terms for G and H and use a computer algebra system to attempt to unify the these two matrices via free variables and/or a scaling factor. Since these matrices are exponential in size with respect to the complexity of the graph, this method is limited to small identities, but this limit can be relaxed by optimising how terms are generated from graphs.

New equations discovered using these techniques can be added to the rule set, and used in subsequent proofs. Quantomatic therefore supports not just the use of graphical notation in quantum mechanics but also the development of the theory itself.

Compositional distributional models of meaning for search. Search applications, since the discovery of Grover's search algorithm, have played an important role in quantum information science. It enables substantial speedup of unstructured search when run on a quantum computer. An unforeseen application of the work previously performed in this workpackage is a completely different application, which does not involve a quantum computer, but any ordinary computer. It turns out that the categorical semantics for quantum computing which have been developed and studied in this workpackage provides a compositional distributional model for meaning for natural languages [4]. This is very important for further improvement of search engines. Currently they consider sentences as a 'bag of words'. This new work allows the meaning of a sentence to be computed from the meaning of the words that make it up. While slightly out of the scope of QICS, this result shows that the high-level structures developed here are very versatile in their potential for future applications.

The next steps to take. We need to move on from pairs of two complementarity observables to maximal sets of complementary observables to capture in an even tighter manner the quantum mechanical structure. The dualiser was an essential missing piece of structure to realise this. Indeed, in the case of a qubit there are three complementary observables:

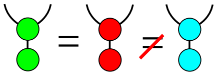
$\delta_Z :: |i\rangle \mapsto |ii\rangle$ $\qquad \epsilon_Z :: |i\rangle \mapsto 1$ $\qquad \delta_Z =$ $\quad \epsilon_Z =$

$\delta_X :: |\pm\rangle \mapsto |\pm\pm\rangle$ $\qquad \epsilon_X :: |\pm\rangle \mapsto 1$ $\qquad \delta_X =$ $\quad \epsilon_X =$

$\delta_Y :: |\pm i\rangle \mapsto |\pm i \pm i\rangle$ $\epsilon_Y :: |\pm i\rangle \mapsto 1$ $\delta_Y =$ $\epsilon_Y =$

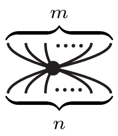
but the corresponding induced compact structures do not match:

$$\delta_Z \circ \epsilon_Z^\dagger = \delta_X \circ \epsilon_X^\dagger :: 1 \mapsto |00\rangle + |11\rangle \qquad \delta_Y \circ \epsilon_Y^\dagger :: 1 \mapsto |00\rangle - |11\rangle$$

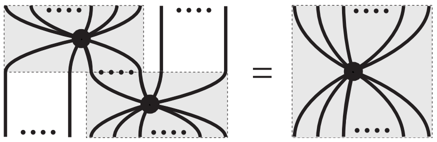


When using dualisers, then the induced compact structures do coincide since we can define these dualisers in terms of a fixed compact structure which will then the induced one for all three observables. Key in realising an axiomatic description of n interacting complementary observables is a theorem proved in [8]: In all dagger symmetric monoidal categories, observables and 'generalised' GHZ-states are in a canonical bijective correspondence. Moreover, if for a certain object all states are either eigenstates or unbiased relative to an observable, then the 'generalised' phase group of that observable completely determines the GHZ-correlations for the corresponding GHZ-states.

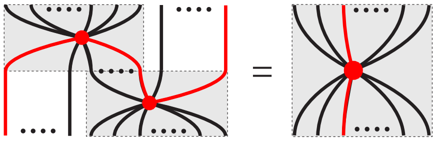
Related to this is the desire for a better understanding of the graphical properties of complementary observables. For example, basis structures have a very intuitive graphical reasoning mechanisms with normal form results. This is best seen in the following 'equivalent' definition of a special commutative dagger Frobenius comonoid [5]. A basis structure on an object A in a dagger symmetric monoidal category is a family of *spiders* with n front and m back legs, one for each $n, m \in \mathbb{N}$, depicted



and denoted by $A^{\otimes n} \xrightarrow{\delta_n^m} A^{\otimes m}$. The composition axiom which governs these spiders is:



In words, whenever we have two spiders such that at least one leg of spider 1 is connected to a leg of spider 2 then we can *fuse* them into a single spider. We also require δ_1^1 to be the identity, and that the set of spiders in invariant under upside-down flipping and leg-swapping. Note that is rule is a direct generalisation of the 'yanking' rule which defines compactness:



We would like to have a similarly well-behaved graphical principle for the interaction of different colours. All this should lead to unified and standardised graphical calculus involving all the ingredients we need for graphical quantum reasoning.

We discuss some future work on quantomatic. Quantomatic is under continuous development to extend its capabilities. We list here some of the objectives of current work.

Since quantomatic is based on rewriting, questions of confluence and termination of rewrite rules are of prime importance. This problem is more difficult for graphical systems than for conventional term rewriting systems because of the large number of ways that two rules may overlap. Up till now such analysis has been performed by hand but we aim to be able to automate key parts of this process: for example the enumeration of critical pairs. This will allow quantomatic to perform meta-analysis on its own rewrite system which is very important when we can add rules to the system in an ad-hoc fashion.

The !-box notation used in quantomatic has the virtue of simplicity, but it is not very expressive. Further development of this language would allow parametric families of graphs – for example certain classes of entangled states – to be analysed automatically. This would be aided by enhancing the connection between quantomatic and the Isabelle theorem prover [20], allowing inductive reasoning to formally verify properties of these states.

Finally we would like to enhance the semantic analysis component of quantomatic. For example, to test whether certain identities are dependent on the dimension of the underlying space, or to evaluate equations in non-vector based models, such as **Rel**, which may be more computationally feasible. Semantic analysis could be extended with a model checking element which would actually produce counter examples to failed equations.

Work has also been initiated to study processes embedded in space-time. We identified a monoidal structure on space-time regions which emerges from an underlying poset via the Egli-Milner ordering. This will be key, not only for distributed quantum information processing but also for relativistic quantum information processing.

Maybe the most important challenge for the following year is to use the automation discussed above to tackle one of the long-standing open problems of quantum information and computation: understanding multipartite entanglement.

Bob Coecke, Ross Duncan, Aleks Kissinger and Eric Oliver Paquette
Oxford, February 10, 2009.

Workpackage objectives :

W2.O1 Find simple intuitive graphical calculi and more conceptually motivated constructions and proofs to replace the highly non-intuitive definitions and manipulations in terms of matrices.

W2.O2 Expose the foundational structure and axiomatic boundaries of QIC.

W2.O3 Study the structure of multipartite entanglement and distributed quantum systems.

W2.O4 Exploit the above for automated design and verification for algorithms and protocols.

W2.O5 Contribute to the quest of a general model for QIC by studying the topological QC model.

Workpackage milestones :

W2.M1 A comprehensive graphical calculus which captures a substantial fragment of QIC. (12)

W2.M2 Structural insights in the topological quantum computational model. (12)

W2.M3 A logical understanding of distributed quantum systems. (24)

W2.M4 Powerful methods arising from a category-theoretic axiomatic framework. (24)

W2.M5 A simple axiomatic framework which captures the different quantitative quantum-informatic concepts. (36)

W2.M6 A logical understanding of multipartite behavior, including graph states. (36)

Below we discuss the detailed progress for this workpackage which comprises the *workpackage tasks* :

W2.T1 Develop categorical semantics, logics and diagrammatic methods for general QIC; apply these to the problems posed in other workpackages.

W2.T2 Study the structure of multipartite entanglement using categorical methods and others; combine quantum structure and spatio-temporal structure.

W2.T3 Study the structure of the topological quantum computational model from the point of view of categorical semantics; build categorical semantics for the knot-theoretic models.

5.1 Progress towards objectives and performed tasks for W2.T1

5.1.1 Categorical semantics of complementary quantum observables

Interacting Quantum Observables (Objectives: W1.O1 W1.O2 W1.O5 W2.O1 W2.O2 W3.O2 W3.O3 W3.O4, W4.O1, Milestones: W1.M4 W2.M1 W2.M4 W2.M5 W3.M5 W3.M6 W4.M5 W4.M8) In [6] Coecke (Ox) and Duncan (Ox) provide a categorical axiomatisation of the complementary quantum observables, and provide “positive” structural results about their algebraic structure, revealing for the first time that such observables induce a Hopf algebra-like structure. They give an abstract account of phase data and interference phenomena. All this is done in an intuitive graphical language, and the proofs can be done purely by rewriting diagrams. We show that these axioms suffice to simulate quantum algorithms such as the quantum Fourier transform, and to separate different classes of entangled states. This became the first paper on Quantum Computation and Information to ever have been accepted by the Logic, Semantic, and Theory of Programming track (Track B) of the prestigious International Colloquium on Automata, Languages and Programming (ICALP).

5.1.2 Automation based on categorical semantics

a. Extending Graphical Representations for Compact Closed Categories with Applications to Symbolic Quantum Computation (Objectives: W1.O2 W1O5 W2.O1 W2.O4 W3.O4 W4.O6; Milestones: W1.M3 W1.M4 W2.M4 W4.M5 W4.M8) In [14], Dixon (Ed) and Duncan (Ox) present 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, they describe 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. They illustrate the framework by instantiating it for a graphical language of quantum computation described in [6] and show how this can be used to perform symbolic computation.

b. Graphical Reasoning in Compact Closed Categories for Quantum Computation (Objectives:W1.O2 W1.O5 W2.O1 W2.O4 W3.O4 W4.O6; Milestones: W1.M3 W1.M4 W2.M4 W4.M5 W4.M8) This paper is an extension of [14] above. Dixon (Ed) and Duncan (Ox) augment the formal graphical reasoning described previously [14] with various notions of composition for graphs and graph patterns, and define more precise control mechanisms for matching.

c. Quantomatic Prototype software (W1.O2 W1.O5 W2.O1 W2.O4 W3.O4 W4.O6; Milestones: W1.M3 W1.M4 W2.M4 W4.M5 W4.M8) Dixon (Ed), Duncan (Ox) and Kissinger (Ox) implement the formal graphical reasoning system described in [14] [15] in a graphical software tool. The tool provides a user-friendly way to enter graphs corresponding to quantum states or processes and automatically finds the possible rewrites allowed by the equational theory. The tool functions as a semi-automatic theorem prover for graphical theories such as [6]. Diverse other capabilities are implemented, and many extensions are possible.

d. Finite dimensional Hilbert spaces are complete for dagger compact closed categories (Objectives: W2.O2; Milestones: W2.M4) In [23], P. Selinger (McGill) shows that an equation follows from the axioms of dagger compact closed categories if and only if it holds in finite dimensional Hilbert spaces.

5.1.3 Categorical axiomatisation of bases and classicity

a. A new description of orthogonal bases (Objectives: W1.O1, W2.O1, W2.O2) In [9], B. Coecke (Ox), D. Pavlovic (Ox) and J. Vicary (Ox) show that an orthogonal basis for a finite-dimensional Hilbert space can be equivalently characterised as a commutative dagger-Frobenius monoid in the category **FdHilb**, which has finite-dimensional Hilbert spaces as objects, continuous linear maps as morphisms and tensor product for the monoidal structure. The basis is normalised exactly when the corresponding commutative dagger-Frobenius monoid is special. Hence orthogonal and orthonormal bases can be axiomatised in terms of composition of operations and tensor product only, without any explicit reference to the underlying vector spaces. This axiomatisation moreover admits an operational interpretation, as the comultiplication copies the basis vectors and the counit uniformly deletes them. That is, we rely on the distinct ability to clone and delete classical data as compared to quantum data to capture basis vectors. For this reason our result has important implications for categorical quantum mechanics.

b. Bases in diagrammatic quantum protocols (Objectives: W1.O5 W2.O2; Milestones: W2.M1 W2.M4) In [12], Coecke (Ox), Paquette (Ox; QICS Postdoc) and Perdrix (Gre & OX & Paris; QICS Postdoc) amend the notion of abstract basis in a dagger symmetric monoidal category, as well as its corresponding graphical representation, in order to accommodate non-self-dual dagger compact structures; this is crucial for obtaining a 'planar' diagrammatic representation of the induced dagger compact structure as well as for representing many complementary bases within one diagrammatic calculus. Moreover, the authors crucially rely on these basis structures in a purely diagrammatic derivation of the 'quantum state transfer protocol'; this derivation provides interesting insights in the distinct structural resources required for state-transfer and teleportation as models of quantum computing.

c. Classical and quantum structuralism (Objective: W2.O1 W2.02; Milestones: W2.M1 W2.M2 W2.M4) In [11], Coecke (Ox), Paquette (Ox; QICS Postdoc) and Pavlovic (Ox) provide categorical semantics and diagrammatic representations of deterministic, non-deterministic and probabilistic operations over classical data represented by special commutative dagger Frobenius algebras. In addition, the authors provide a specific categorical presentations of pure and mixed quantum states which provides a resource sensitive categorical account of classical control of quantum data, of classical data resulting from quantum measurements, as well as of the classical data processing that may happen in between measurements and controls.

d. Éric Paquette's Ph. D. thesis (Objectives: W2.O2, W3.O4; Milestones: W2.M1 W2.M4 W2.M5 W3.M4 W3.M5) In [18], É. O. Paquette (Ox; QICS Postdoc) introduces a categorical semantics for quantum computation which includes both the classical and the quantum fragments of the theory. In order to do so, he introduces the notion of classical-quantum interface, which is sufficiently general to include the two fragments of the theory. Moreover, the classical fragment is axiomatised exclusively with respect to the tensorial structure, i.e. without using biproducts. The axiomatisation of basis structures – from which is derived the notion of classical transformation – also enables de definition of many families of classical transformations such as relations, functions, bijections, stochastic and bistochastic transformations; the later three being especially suitable in the context of quantum computation. Some quantum protocols are presented along with some results concerning these. The works presented in this thesis incorporate those of [11] and [12].

e. Categorical formulation of quantum algebras (Objectives: W1.O1, W2.O1, W2.O2) In [25], J. Vicary (Ox) describe how dagger-Frobenius monoids give the correct categorical description of two kinds of finite-dimensional 'quantum algebras'. He develops the concept of an involution monoid, and use it to show that finite-dimensional C*-algebras are the same as special unitary dagger-Frobenius monoids in the category of finite-dimensional complex Hilbert spaces. The spectral theorems for commutative C*-algebras and for normal operators are discussed from this perspective, and we formulate them in an explicitly categorical way. He examine the case that the results of measurements do not form finite sets, but rather objects in a finite Boolean topos, and are motivated to define the term 'finite quantum Boolean topos'. The paper ends with a study of the 2-categorical generalisation, and show that 2-H*-algebras are the same as dagger-Frobenius pseudomonoids in the bicategory of 2-Hilbert spaces.

f. Quantum and classical structures in nondeterministic computation (Objective: W2.O2; Milestones: M2.M4) In categorical quantum mechanics, classical structures characterize the classical interfaces of quantum resources on one hand, while on the other hand giving rise to some quantum phenomena. In the standard Hilbert space model of quantum theories, classical structures over a space correspond to its orthonormal bases. In [23], D. Pavlovic (Ox) show that classical structures in the category of relations correspond to biproducts of Abelian groups. Although relations are, of course, not an interesting model of quantum computation, this result has some interesting computational interpretations. If relations are viewed as denotations of nondeterministic programs, it uncovers a wide variety of non-standard quantum structures in this familiar area of classical computation. Ironically, it also opens up a version of what in philosophy of quantum mechanics would be called an ontic-epistemic gap, as it provides no direct interface to these nonstandard quantum structures.

g. A survey of categorical semantics and diagrammatic quantum calculus (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). In [5] Coecke (Ox) argues that the quantum mechanical formalism doesn't support our intuition, nor does it elucidate the key concepts that govern the behaviour of the entities that are subject to the laws of quantum physics. The arrays of complex numbers are kin to the arrays of 0s and 1s of the early days of computer programming practice. Using a technical term from computer science, the quantum mechanical formalism is 'low-level'. This review presents steps towards a diagrammatic 'high-level' alternative for the Hilbert space formalism, one which appeals to our intuition. The diagrammatic language as it currently stands allows for intuitive reasoning about interacting quantum systems, and trivialises many otherwise involved and tedious computations. It clearly exposes limitations such as the no-cloning theorem, and phenomena such as quantum teleportation. As a logic, it supports 'automation': it enables a (classical) computer to reason about interacting quantum systems, prove theorems, and design protocols. It allows for a wider variety of underlying theories, and can be easily modified, having the potential to provide the required step-stone towards a deeper conceptual understanding of quantum theory, as well as its unification with other physical theories. Specific applications discussed here are purely diagrammatic proofs of several quantum computational schemes, as well as an analysis of the structural origin of quantum non-locality. The underlying mathematical foundation of this high-level diagrammatic formalism relies on so-called *monoidal categories*, a product of a fairly recent development in mathematics, and its logical underpinning is *linear logic*, an even more recent product of research in logic and computer science. These monoidal categories do not only provide a natural foundation for physical theories, but also for proof theory, logic, programming languages, biology, cooking, ... So the challenge is to discover the required additional pieces of structure that allow us to predict genuine quantum phenomena. These pieces of structure, in turns, represent the capabilities nature has provided us with in order to manipulate entities subject to the laws of quantum theory.

5.1.4 Non-locality as a structure via categorical toy theories

a. Spekkens' toy theory as a category (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). In [7] Coecke (Ox) and Edwards (Ox) showed that Rob Spekkens' toy quantum theory arises as an instance of categorical approach quantum axiomatics, as a (proper) subcategory of the dagger compact category $\mathbf{FRel}$ of finite sets and relations with the cartesian product as tensor, where observables correspond to dagger Frobenius algebras. This in particular implies that the quantum-like properties of the toy model are in fact very general category-theoretic properties.

b. Modeling complementary observables with relations (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). Also in [8] Coecke (Ox) and Edwards (Ox) showed that the two-element set in $\mathbf{FRel}$ has two complementary basis structures. From this follows the remarkable fact that we can already interpret complementary quantum observables on the two-element set $\mathbf{FRel}$. In [23] Pavlovic (Ox) characterised all basis structures in $\mathbf{FRel}$.

c. The group-theoretic origin of quantum non-locality (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). In [8] Coecke (Ox), Edwrads (Ox) and Spekkens studied the difference between quantum mechanics restricted to qubit stabiliser states and operations, and a toy theory proposed by Spekkens. They showed that viewed within categorical quantum axiomatics these theories are very similar, but differ in one key aspect - a four element group we term the *phase group* which emerges naturally within our framework. In the case of the stabiliser theory this group is Z_4 while for Spekkens' theory the group is $Z_2 \times Z_2$. They also show that the structure of this group is intimately involved in a key physical difference between the theories: whether or not they can be modelled by a local hidden variable theory. This is done by establishing a connection between the phase group, and an abstract notion of GHZ state correlations. They formulate precisely how the stabiliser theory and toy theory are 'similar' by defining a notion of 'mutually unbiased qubit theory', noting that all such theories have four element phase groups. Since Z_4 and $Z_2 \times Z_2$ are the only such groups we conclude that the GHZ correlations in this type of theory can only take two forms, exactly those appearing in the stabiliser theory and those appearing in Spekkens' theory. The results point at a classification of local/non-local behaviours by finite Abelian groups, extending beyond qubits to any finitary theory whose observables are all mutually unbiased.

5.1.5 Categories, logic and QIP

a. Proof Nets as Formal Feynman Diagrams (Objectives: W2.O2; Milestones: W2.M4) The introduction of linear logic and its associated proof theory has revolutionized many semantical investigations, for example, the search for fully-abstract models of PCF and the analysis of optimal reduction strategies for lambda calculi. In [2], R. Blute (McGill) and P. Panangaden (McGill) show how proof nets, a graph-theoretic syntax for linear logic proofs, can be interpreted as operators in a simple calculus. This calculus was inspired by Feynman diagrams in quantum field theory and his accordingly called the ϕ-calculus. The ingredients are formal integrals, formal power series, a derivative-like construct and analogues of the Dirac delta function. Many of the manipulations of proof nets can be understood as manipulations of formulas reminiscent of a beginning calculus course. In particular, the "box" construct behaves like an exponential and the nesting of boxes phenomenon is the analogue of an exponentiated derivative formula. Blute and Panangaden show that the equations for the multiplicative-exponential fragment of linear logic hold.

b. Dagger categories and formal distributions (Objectives: W2.O2; Milestones: W2.M4, W2.M5) Monoidal dagger categories play a central role in the abstract quantum mechanics of Abramsky and Coecke [1]; indeed, a deal of elementary quantum mechanics can be carried out in these categories; for example, the Born rule emerges naturally. In [3], R. Blute (McGill) and P. Panangaden (McGill) construct a category of tame formal distributions with coefficients in a commutative associative algebra and show that it is a dagger category. This gives access to a broad new class of models, with the abstract scalars in the sense of Abramsky being the elements of the algebra. They also consider a subcategory of local formal distributions, based on the ideas of Kac. Locality has been of fundamental significance in various formulations of quantum field theory. Their work may provide the possibility of extending the abstract framework to QFT. They also show that these categories of formal distributions are monoidal and contain a nuclear ideal, a weak form of adjunction appropriate for analyzing categories such as the category of Hilbert spaces, where the nuclear maps are the Hilbert-Schmidt maps. By taking formal distributions with coefficients in the dual of a cocommutative Hopf algebra, they obtain a categorical generalization of the Borcherds' notion of elementary vertex group.

c. A survey of graphical languages for monoidal categories (Objectives: W2.01; Milestones: W2.M1) In [22], P. Selinger (McGill) presents an intended reference guide to various notions of monoidal categories and their associated string diagrams. It is hoped that this will be useful not just to mathematicians, but also to physicists, computer scientists, and others who use diagrammatic reasoning. The treatment of the topological notions are somewhat informal, and most proofs are omitted. Nevertheless, the exposition is sufficiently detailed to make it clear what is presently known, and to serve as a starting place for more in-depth study. Where possible, pointers are provided to more rigorous treatments in the literature.

d. Categorical properties of the complex numbers (Objectives: W2.02; Milestones: W2.M5) In [26], J. Vicary (Ox) studies the categorical properties of the complex numbers by describing the natural categorical conditions under which the scalars of a monoidal dagger-category gain many of the features of the complex numbers. Central to the approach is the requirement that the dagger-functor is compatible with the construction of particular limits in the category; this implies nondegeneracy of the dagger-functor, as well as cancellable hom-set addition. The main theorem is that in a nontrivial monoidal dagger-category with finite dagger-biproducts and finite dagger-equalisers, for which the monoidal unit has no proper dagger-subobjects, the scalars have an involution-preserving embedding into an involutive field with characteristic 0 and orderable fixed field, and therefore embed into the complex numbers if they are at most of continuum cardinality.

e. A categorical framework for the quantum harmonic oscillator (Objectives: W2.02; Milestones: W2.M5) In [27], J. Vicary (Ox) describes how the structure of the state space of the quantum harmonic oscillator can be described by an adjunction of categories, that encodes the raising and lowering operators into a commutative comonoid. The formulation is an entirely general one in which Hilbert spaces play no special role. Generalised coherent states arise through the hom-set isomorphisms defining the adjunction, and we prove that they are eigenstates of the lowering operators. Surprisingly, generalised exponentials also emerge naturally in this setting, and it is demonstrated that coherent states are produced by the exponential of a raising morphism acting on the zero-particle state. Finally, all of these constructions are examined in a suitable category of Hilbert spaces, and it is shown that they reproduce the conventional mathematical structures.

f. Idempotents in dagger categories (Objectives: W2.O2 W3.O2 W3.O4; Milestones: W2.M4 W3.M4) A technical detail of the $\mathbf{CPM}(\mathbf{C})$ construction – The category of Completely Positive Maps of a dagger-compact category – is that it does not preserve biproducts. Therefore, to obtain an interpretation of classical types such as **bit** $= I \oplus I$, one must work in the free biproduct completion $\mathbf{CPM}(\mathbf{C})^{\oplus}$. In [24], P. Selinger (McGill) shows that there is another view of classical types, namely as splittings of self-adjoint idempotents on quantum types; it is shown that all the objects of $\mathbf{CPM}(\mathbf{C})^{\oplus}$ arise as such splittings.

5.1.6 A compositional distributional model of meaning for natural languages.

In [4] Clark (Ox), Coecke (Ox) and Sadrzadeh (Paris and Oxford; QICS Postdoc) propose a mathematical framework for a unification of the distributional theory of meaning in terms of vector space models, and a compositional theory for grammatical types, namely Lambek's pregroup semantics. A key observation is that the monoidal category of (finite dimensional) vector spaces, linear maps and the tensor product, as well as any pregroup, are examples of compact closed categories. Since, by definition, a pregroup is a compact closed category with trivial morphisms, its compositional content is reflected within the compositional structure of any non-degenerate compact closed category. The (slightly refined) category of vector spaces enables to compute the meaning of a compound well-typed sentence from the meaning of its constituents, by 'lifting' the type reduction mechanisms of pregroup semantics to the whole category. These sentence meanings live in a single space, independent of the grammatical structure of the sentence. Hence one can use the inner-product to compare meanings of arbitrary sentences. A variation of this procedure which involves constraining the scalars of the vector spaces to the semiring of Booleans results in the well-known Montague semantics.

5.2 Progress towards objectives and performed tasks for W2.T2

a. Graphs States and the necessity of Euler Decomposition (Objectives: W1.O1 W1.O2, W2.O1 W2.O2, Milestones: W1.M4 W2.M1 In [13] Duncan (Ox) and Perdrix (Gre & OX & Paris; QICS Postdoc) use Coecke (Ox) and Duncan's (Ox) results to study graph states, a computationally interesting class of quantum states. They give a graphical proof of the fixpoint property of graph states. They then introduce a new equation, for the Euler decomposition of the Hadamard gate, and demonstrate that Van den Nest's theorem–locally equivalent graphs represent the same entanglement–is equivalent to this new axiom. Finally they prove that the Euler decomposition equation is not derivable from the existing axioms.

b. Thermal robustness of multipartite entanglement of the 1-D spin 1/2 XY model (Objective: W2.O3) In [17] D. Markham (Paris) and co-authors study the structure of multipartite entanglement in the XY model using the thermal robustness of entanglement. We see that this approach witnesses the full phase diagram whereas until recently only part was seen in terms of the entanglement properties.

5.3 Progress towards objectives and performed tasks for W2.T3

A categorical presentation of quantum computation with anyons (Objectives: W2.O1 W2.O5; Milestones: W2.M2) The well known spin-statistics theorem states that elementary particles are either symmetric under interchange (bosons) or antisymmetric (fermions). This theorem holds for 3 dimensions but not in two dimensions. "Anyon" is a term coined in by Frank Wilczek to describe particles in 2 dimensions that can acquire "any" phase when two or more of them are interchanged.

The exchange of two such anyons can be expressed via representations of the braid group and hence, it permits us to encode information in topological features of a system composed of many anyons. Kitaev suggested the possibility that such topological excitations would be stable and could thus be used for robust quantum computation. In [19], a survey paper, É. O. Paquette (Ox; QICS Postdoc) and P. Panangaden (McGill) aim to:

1. give the categorical structure necessary to describe such a computing process;
2. illustrate this structure with a concrete example namely: Fibonacci anyons.

Bibliography

[1] S. Abramsky and B. Coecke (2008) *Categorical Quantum Mechanics*. Chapter in: The Handbook of Quantum logic and Quantum Structures. Elsevier. arXiv:0808.1023

[2] R. Blute and P. Panangaden (2008) *Proof Nets as Formal Feynman Diagrams*. To appear in New structures in physics. B. Coecke Ed. Springer Lecture Notes in Physics. http://www.cs.mcgill.ca/∼prakash/accepted.html

[3] R. Blute and P. Panangaden (2008) *Dagger categories and formal distributions*. To appear in New structures in physics. B. Coecke Ed. Springer Lecture Notes in Physics. http://www.cs.mcgill.ca/∼prakash/accepted.html

[4] S. Clark, B. Coecke and M. Sadrzadeh (2008) *A compositional distributional model of Meaning*. In: Proceedings of the Second Quantum Interaction Symposium, pp. 133–141. College Publications.

[5] B. Coecke (2009) *Quantum picturalism*. Contemporary physics, to appear.

[6] B. Coecke and R Duncan (2008) *Interacting Quantum Observables*. Proceedings of ICALP 2008, Springer LNCS vol. 5126. http://www.springerlink.com/content/y443214116h76122/

[7] B. Coecke and B. Edwards (2008) *Toy quantum categories*. Electronic Notes in Theoretical Computer Science, to appear. arXiv:0808.1037

[8] B. Coecke, B. Edwards and R. Spekkens (2008) *The group theoretic origin of non-locality for qubits*. Draft paper.

[9] B. Coecke, D. Pavlovic and Jamie Vicary (2008) *A new description of orthogonal bases*. arXiv:0810.0812

[10] B. Coecke and É. Paquette (2008) *Categories for the practising physicists*. To appear in: *New structures in physics*. B. Coecke Ed. Springer Lecture Notes in Physics.

[11] B. Coecke, É. Paquette and D. Pavlovic (2008) *Classical and quantum structuralism*. To appear in: *Semantic techniques in Quantum Computation*. S. Gay and I. Mackie, Eds. Cambridge University Press.

[12] B. Coecke, É. Paquette, S. Perdrix (2008). *Bases in diagrammatic quantum protocols*. 24th Conference on Mathematical Foundations of Programming Semantics (MFPS XXIV). Electronic Notes in Theoretical Computer Science (ENTCS) vol. 218, pp. 131–152, 2008.

[13] R. Duncan and S. Perdrix (2009) *Graphs States and the necessity of Euler Decomposition*. arXiv:0902.0500

[14] L. Dixon and R. Duncan (2008) *Extending Graphical Representations for Compact Closed Categories with Applications to Symbolic Quantum Computation*. Proceedings of AISC 2008, Springer LNCS vol. 5144.

[15] L. Dixon and R. Duncan (2008) *Graphical Reasoning in Compact Closed Categories for Quantum Computation*. Submitted to AMAI. arXiv:0902.0514

[16] L. Dixon, R. Duncan and A. Kissinger (2008) *Quantomatic Prototype Software*, tool of which the source code is made available at http://dream.inf.ed.ac.uk/projects/quantomatic/

[17] Y. Nakata, D. Markham, M. Murao (2008). Thermal robustness of multipartite entanglement of the 1-D spin 1/2 XY model. arxiv:0806.3644

[18] É. O. Paquette (2008) *Categorical Quantum Computation*. Ph. D. Thesis, Université de Montréal.

[19] É. O. Paquette and P. Panangaden (2008) *A categorical presentation of quantum computation with anyons*. To appear in: *New structures in physics*. B. Coecke Ed. Springer Lecture Notes in Physics. http://www.cs.mcgill.ca/∼prakash/accepted.html

[20] L. C. Paulson (1994) *Isabelle: a generic theorem prover*. Lecture Notes in Computer Science **828**, Springer-Verlag.

[21] D. Pavlovic (2008) *Quantum and classical structures in nondeterministic computation*. Preprint. `arXiv:0812.2266`

[22] P. Selinger (2008) *A survey of graphical languages for monoidal categories*. To appear in: *New structures in physics*. B. Coecke Ed. Springer Lecture Notes in Physics. `http://www.mscs.dal.ca/∼selinger/papers.html`

[23] P. Selinger (2008) *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. Extended Abstract. To appear in Proceedings of the 5th International Workshop on Quantum Physics and Logic (QPL 2008), Reykjavik, 2008. `http://www.mscs.dal.ca/∼selinger/papers.html`

[24] P. Selinger (2008) *Idempotents in dagger categories*. Extended Abstract. In Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006), Oxford. ENTCS 210, pp. 107–122.`http://www.mscs.dal.ca/ selinger/papers.html`

[25] Jamie Vicary, *Categorical formulation of quantum algebras* (2008). Communications in Mathematical Physics, to appear. `arXiv:0805.0432`

[26] Jamie Vicary, *Categorical properties of the complex numbers* (2008). Submitted for publication, accepted for CT08. `http://arxiv.org/abs/0807.2927`

[27] Jamie Vicary, *A categorical framework for the quantum harmonic oscillator* (2008). International Journal of Theoretical Physics, vol. 47, 12, pp. 3408–3447.

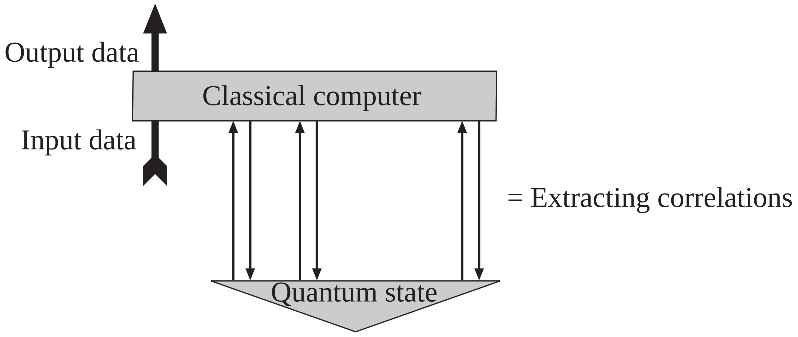
Chapter 6

W3 – *deliverable D3*: Classical-quantum interaction and information flow

A current account of the objectives of W3 and comparison with the state-of-the art. Some of the work performed in W3 constitutes the cutting edge on an understanding of what separates quantum information processing from classical information processing, as well as on an understanding of what the limitations of quantum information processing. Examples of this are the work by Browne (UCL; Ox affiliate) and Anders (UCL; Ox affiliate) on classical computing with quantum correlations, and in particular on the trade-off between classical computational power and the availability of physical resources. Interesting results in a similar spirit where also produced by Popescu and collaborators on post-quantum correlations and entanglement swapping, by Jozsa (UNIVBRIS) and Miyake (QICS postdoc Innsbruck) on matchgates and classical simulation of quantum circuits, and by Coecke (Ox) and Edwards (Ox) in collaboration with Robert Spekkens of the perimeter Institute.

Some of the main developments in W3. A major aspect of the research in W3 is tightly intertwined with the work in W2. In particular, the work on basis structures supports logical description of classical and quantum information flows. However, more unexpected links between 'mainstream' research and categorical axiomatics have emerged at the following two fronts:

- In [10, 11] Miyake and Jozsa investigate a whole class of classically simulatable quantum circuits (matchgate circuits). Quite surprisingly the threshold between Classical Computation and Quantum Computation is not related to entanglement in their setting, but rather just by the possibility to have far-away wires interacting with one another (e.g. to have a Swap gate, say). In category-theoretic terms this seems to tell us that the symmetry of a monoidal category is a key component which enables a classical to quantum transition. This also seems to indicate that there is something fundamentally non-planar to genuine quantum circuits.
- In [1, 3] posed the following interesting question: can quantum correlations increase the capability to perform certain tasks for a classical computer? The main inspiration for this question comes from measurement based quantum computing 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.



However, this does not require full-blown classical computational power, but merely cnot and not gates. Complexity class of problems that can be solved with cnot and not in polynomial time is usually denoted by $\oplus P$. So we can write:

$$\text{cluster state correlations} + \oplus\mathbf{P} \Rightarrow \mathbf{BQP}$$

This of course requires a large two-dimensional cluster state. So are there smaller resources that also realise this goal? It was shown that a tree-party resources suffices:

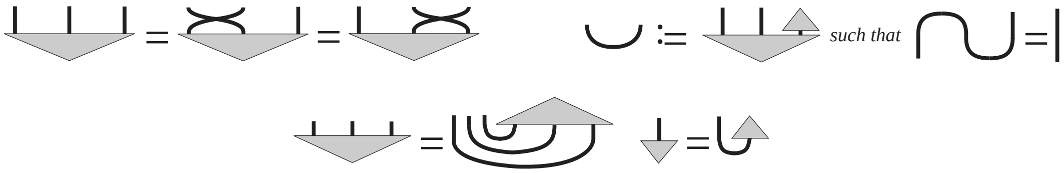
$$\text{GHZ stabiliser correlations} + \oplus\mathbf{P} \Rightarrow \mathbf{BQP}$$

For two-party resources we need to rely on super-quantum correlations:

$$\text{PR-box correlations} + \oplus\mathbf{P} \Rightarrow \mathbf{BQP}$$

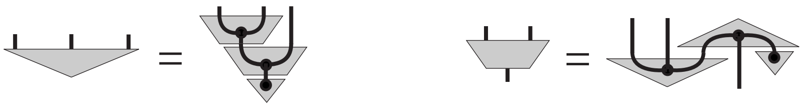
- Spekkens proposed a *toy theory* which looked remarkably similar to quantum theory. More precisely, there is an important restriction of quantum theory, its *stabiliser* fragment, in which for a qubit we only consider the eigenstates of the Z-, X- and Y-observables, but which already carries an important fragment of quantum theory. In particular, it is *non-local*. It is this fragment of quantum theory which Spekkens' toy theory aims to mimic, and at first sight it does this on-the-nose. However, there is a crucial difference: Spekkens' toy theory happens to be *local*. Given that these two theories seem so similar, what makes one local and the other one non-local?

  In [6] Spekkens' toy theory was succinctly recast as a dagger symmetric monoidal category, called $\mathbf{Spek}$. The same can easily be done for the stabiliser fragment of quantum theory, to which we refer as $\mathbf{Stab}$. One can show that the observables for a qubit, now of course in our more generalised sense, exactly match in these theories. In particular, in both a qubit has three mutually complementary observables (in our generalised sense). There are many other correspondences between these, namely in both cases all qubit states are either an unbiased state or an eigenstate for any qubit observables. There is a notion of GHZ-state and GHZ-correlations that applies to arbitrary dagger symmetric monoidal categories. GHZ-state are defined by:

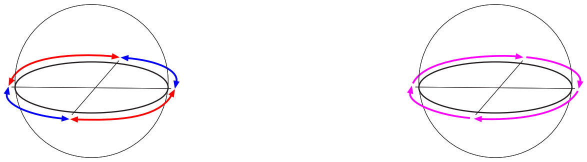


  For three qubits there are tripartite GHZ-states both in $\mathbf{Spek}$ and in $\mathbf{Stab}$. Hence we can speak of *GHZ-correlations* in both theories, that is, which outcomes one can simultaneously obtain in measurements of each of the qubits in a GHZ-state.

  It is here that things become interesting. In the discussion of future work for W2 we already pointed to the fact that in all dagger symmetric monoidal categories, observables and GHZ-states are in a canonical bijective correspond:



  and that, if for a certain object all states are either eigenstates or unbiased relative to an observable, then the phase group of that observable completely determines the GHZ-correlations for the corresponding GHZ-states.



  We also know that phase groups are commutative groups. Both for the qubits in $\mathbf{Spek}$ and $\mathbf{Stab}$ these contain four elements, and in fact, there are exactly two four element groups, namely Z_4 and $Z_2 \times Z_2$. For observables on qubits in $\mathbf{Spek}$ the phase group happens to be $Z_2 \times Z_2$, while for observables on qubits in $\mathbf{Stab}$ the phase group is Z_4.

  One can moreover show that having Z_4 as a phase group is enough for a theory to be non-local. This result (at least to some extend) unveils which 'piece' of the Hilbert space puzzle causes non-locality.

The next steps to take. There are some striking similarities between this work and the work by Browne and Anders discussed above which we intend to explore further. There is a clear challenge to lift the results of Miyake and Jozsa and Anders and Browne to a logical level. The language required to state their results can be expressed in elegant purely category-theoretic terms so one expects that the intermediate computations can also be axiomatised. Would it be possible to craft a categorical framework in which one can establish all of the above results, as well as those reported on last year on Devetak-Harrow-Hayden-Winter resource calculus? We think so.

Bob Coecke and Eric Oliver Paquette
Oxford, February 10, 2009.

Workpackage objectives: :

W3.O1 Obtain a modular and compositional understanding on quantum informatic resources, extending the resource inequality calculus of Devetak/Harrow/Winter et al..

W3.O2 Expose the foundational structure and axiomatic boundaries of QIC.

W3.O3 Obtain a resource-sensitive logical understanding of No-cloning and No-deleting.

W3.O4 Develop a formalism in which quantum and classical data are treated at the same level, and in which the distinct abilities (cloning, deleting) to manipulate them are first-class citizens.

W3.O5 Use this formalism for qualitative and quantitative analysis of information flow in general QIC-models.

W3.O6 Use this formalism for the design of protocols and algorithms for non-standard QIC-models.

Workpackage milestones :

W3.M1 A compositional representation of the resource inequality calculus of Devetak/Harrow/Winter et al. (12)

W3.M2 A diagrammatic calculus for the resource inequality calculus. (12)

W3.M3 An extension of the resource inequalities calculus to multiple parties. (24)

W3.M4 A general theory on mixed quantum-classical information flow in QIC. (24)

W3.M5 A diagrammatic theory for general quantum protocols and resources. (36)

W3.M6 A resource-sensitive logic on mixed quantum-classical information flow in QIC. (36)

Below we discuss the detailed progress for this workpackage which comprises the *workpackage tasks* :

W3.T1 Study resources in quantum information theory: resource inequalities, compositional understanding, multiple agents, simple and intuitive formalism.

W3.T2 Study the logic of information flow in QIC-protocols: theory for quantum-quantum flow, quantum-classical flow, classical-quantum flow, classical-classical flow, and their interaction; coalgebraic methods.

6.1 Progress towards objectives and performed tasks for W3.T1

6.1.1 Quantum vs. Non-Local corrections

a. Bit Commitment from Non-Local Correlations (Objectives: W3.O1, W3.O2, W3.O6; Milestones: W3.M5) S. Winkler, S. Wolf and J. Wullschleger (UNIVBRIS) in [21] consider general two-party input-output systems that do not allow for message transmission, and show that they can be used for realizing unconditionally secure bit commitment as soon as they are non-trivial, i.e., cannot be realized from distributed randomness only. In particular, their result implies that any two-qubit state without hidden-variable model has an input-output behavior allowing for unconditional bit commitment.

b. Emergence of Quantum Mechanics from Non-Locality Swapping (Objectives: W3.O2, W3.O3; Milestones: W3.M6) In [18] P. Skrzypczyk (UNIVBRIS), N. Brunner (UNIVBRIS) and S. Popescu (UNIVBRIS) revisit the paradigmatic model of non-signalling boxes and introduce the concept of a genuine box. This allows them to present the first generalized non-signalling model featuring quantum-like dynamics. In particular, they present the coupler, a device enabling non-locality swapping, the analogue of quantum entanglement swapping, as well as teleportation. Remarkably, a clear boundary between quantum and post-quantum correlations naturally emerges in their study.

c. Simulation of partial entanglement with no-signaling resources (Objectives: W1.O1, W2.O2, W2.O3; Milestones: W2.M3, W2.M6) With the goal of gaining a deeper understanding of quantum non-locality, S. Popescu (UNIVBRIS) and co-authors in [5] decompose quantum correlations into more elementary non-local correlations. In particular they present two models for simulating the correlations of partially entangled states of two qubits without communication, hence using only non-signaling resources. The crucial role of the quantum marginals is discussed.

d. Error-correcting Bell inequalities In [19] T. S. Walker (York), T. W. F. A. C. Polack (York) and S. Braunstein (York) construct a family of Bell inequalities with intrinsic error correcting capabilities. These inequalities exhibit a violation of local realism, without any quantum information processing (except for the creation of an entangled state). This family shows no reduction in the size of the violation of local realism for arbitrary errors on a limited number of qubits.

e. Continuous-variable quantum cryptography using two-way quantum communication In [16], S. Pirandola, S. Mancini, S. Lloyd and S. Braunstein (York) show how to enhance the security thresholds of quantum cryptography protocols based on continuous degrees of freedom. This is achieved by extending these protocols to two-way quantum communication schemes where subsequent uses of the quantum channel are suitably combined. In the resulting two-way schemes, one of the honest parties assists the secret encoding of the other, with the chance of a non-trivial superadditive enhancement of the security thresholds. These results should enable the extension of quantum cryptography to more complex quantum communications.

f. A Maximal Entropy Analysis of Degrees of Information in Quantum Protocols (Objectives: W2.O1. W2.O4; Milestones: W2.M5, W4.M5) In [17], M. Sadrzadeh (Paris and Oxford; QICS Postdoc) shows how the above algebra can be enriched with uniform quantitative measures to not only verify epistemic properties of the principals involved in a quantum protocol, but also to verify the degree of information each principal has acquired as a result of running the protocol and based on his role in the protocol (e.g. honest, dishonest, intruder, attacker). The algebra is applied to a Quantum Key Distribution protocol (Ekert'91) and the degrees of the information of principals and intruders are analyzed at each step of the protocol, including the security amplification part. It is shown how these degree decrease for the honest principals and increase for the intruders in the classical version of the protocol, illustrating that this analysis provides a quantitative way of comparing a quantum protocol with its classical counterparts.

6.1.2 Sequential composition of protocols

Composable Security in the Bounded-Quantum-Storage Model (Objectives: W3.O2, W3.O6 Milestone: W3.M4) In [20] S. Wehner and J. Wullschleger (UNIVBRIS) present a simplified framework for proving sequential composability in the quantum setting. In particular, they give a new, simulation-based, definition for security in the bounded-quantum-storage model, and show that this definition allows for sequential composition of protocols.

6.1.3 Results on quantum informatic resources

a. An exponential separation between the entanglement and communication capacities of a bipartite unitary interaction (Objectives: W2.O2, W2.O3, W3.O1, W3.O2, W3.O5, W3.O6, Milestones: W3.M4, W3.M6) A. W. Harrow (UNIVBRIS) and D. W. Leung consider in [8] asymptotic capacities of bipartite unitary gates. They present a gate with exponentially larger entanglement capacity than the total communication capacity. The key tool in their proof, which may be of independent interest, is a communication-efficient protocol for testing whether a bipartite quantum state belongs to a short list of candidate states.

b. Computational Complexity in Non-Turing Models of Computation; The What, the Why and the How (Objective: W1.O3; Milestone: W1.M6) In [2], E. Blakey (Ox) argue that traditional complexity theory does not adequately capture the true complexity of certain non-Turing computers, and, hence, that an extension of the theory is needed in order to accommodate such machines. He propose a framework of complexity that is not computation-model-dependent–that, rather, is extensible so as to accommodate diverse computational models–, and that allows meaningful comparison of computers' respective complexities, whether or not the comparison be with respect to different resources, and whether or not the computers be instances of different models of computation. Whilst, he suggest, complexity theory is–without some modification–of limited applicability to certain non-standard models, we hope that the ideas described here go some way to showing how such modification can be made, and that members of the non-Turing-computation community–not least participants of Quantum Physics and Logic/Development of Computational Models 2008–find these ideas both useful and interesting.

6.2 Progress towards objectives and performed tasks for W3.T2

A technique for verifying measurements (Objective: W3.O2; Milestone: W3.M4) In [12], K. Martin and P. Panangaden (McGill) give a technique that can be used to prove that a given function is a measurement. They demonstrate its applicability by using it to resolve three notoriously difficult cases: capacity in information theory, entropy in quantum mechanics and global time in general relativity. Finally, they show that this technique provides a new and surprising characterization of measurement. Thus, in principle, it can always be used.

6.2.1 Computational power of correlations

a. Computational Power of Correlations (Objectives: W1.O1 W1.O3 W1.O4 W2.O2 W2.O3 W4.O2; Milestones: W1.M6 W1.M1 W2.M6) In [1], D. Browne (UCL) and J. Anders (UCL) study the intrinsic computational power of the correlated outputs of quantum measurements as is exploited in measurement-based quantum computation (MBQC). Exploiting computational complexity theory, they provide a classification of the Bell inequalities and the Greenberger-Horne-Zeilinger effect, two of the most well-studied examples of quantum Physics' incompatibility with a local realistic model of nature.

This research will lead in a number of new directions, for example, providing tools for the systematic study of quantum non-locality in the general multipartite setting, which will give insight into the mechanisms responsible (and necessary) for measurement-based quantum computation.

b. The Role of Classical Computation in Measurement-Based Quantum Computation (Objectives: W1.O3 W1.O4; Milestone: W1.M5) In [3], D. Browne (UCL) and J. Anders (UCL) describe and classify the classical computational resources required for measurement-based quantum computation. These results formed an important preliminary study to [1].

6.2.2 Non-locality as a structure via categorical toy theories

a. Spekkens' toy theory as a category (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). See 5.1.4.a [6].

b. Modeling complementary observables with relations (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). See 5.1.4.b [6, 14].

c. The group-theoretic origin of quantum non-locality (Objectives: W2.O2, W2.O3, W3.O1, W3.O2; Milestones: W2.M2, W2.M5). See 5.1.4.c [7].

6.2.3 Results one one-way computing

a. Phase transition of computational power in the resource (Objectives: W1.O1 W1.O4 Milestones: W1.M2 W1.M5) In [4], D. Browne (UCL) and co-authors study how heralded qubit losses during the preparation of a two-dimensional cluster state, a universal resource state for one-way quantum computation, affect its computational power. Above the percolation threshold they present a polynomial-time algorithm that concentrates a universal cluster state, using resources that scale optimally in the size of the original lattice. They thus identify a new class of disordered universal resource state for measurement-based quantum computation. Below the percolation threshold, they show that single qubit measurements on the faulty lattice can be efficiently simulated classically. They observe a phase transition at the threshold when the amount of entanglement in the faulty lattice directly relevant to the computational power changes exponentially.

b. Characterisation of collective Gaussian attacks and security of coherent-state quantum cryptography (Objectives: W1.O1) In [15], S. Pirandola, S. Braunstein and S. Lloyd provide a simple description of the most general collective Gaussian attack in continuous-variable quantum cryptography. In the scenario of such general attacks, we analyze the asymptotic secret-key rates which are achievable with coherent states, joint measurements of the quadratures and one-way classical communication.

6.2.4 Foundational results on the classical-quantum data relation

a. Embedding classical into quantum computation (Objectives: W1.O1 W1.O2 W4.02; Milestones: W1.M4 W1.M6 W4.M1) In [10], R. Jozsa (UNIVBRIS) describes a simple formalism for generating classes of quantum circuits that are classically efficiently simulatable and shows that the efficient simulation of Clifford circuits (Gottesman-Knill theorem) and of matchgate circuits (Valiant's theorem) appear as two special cases. Viewing these simulatable classes as subsets of the space of all quantum computations, we may consider minimal extensions that suffice to regain full quantum computational power, which provides an approach to exploring the efficacy of quantum over classical computation.

b. Matchgates and classical simulation of quantum circuits (Objectives: W1.O1, W1.O2, W1.O3, W1.O5, W4.O2; Milestones: W1.M4, W1.M5, W1.M6, W4.M1) Let $G(A, B)$ denote the 2-qubit gate which acts as the 1-qubit $SU(2)$ gates A and B in the even and odd parity subspaces respectively, of two qubits. Using a Clifford algebra formalism in [11] R. Jozsa (UNIVBRIS) and A. Miyake (UIBK) show that arbitrary uniform families of circuits of these gates, restricted to act only on nearest neighbour (n.n.) qubit lines, can be classically efficiently simulated. This reproduces a result originally proved by Valiant using his matchgate formalism, and subsequently related by others to free fermionic physics. They further show that if the n.n. condition is slightly relaxed, to allowing the same gates to act only on n.n. and next-n.n. qubit lines, then the resulting circuits can efficiently perform universal quantum computation. From this point of view, the gap between efficient classical and quantum computational power is bridged by a very modest use of a seemingly innocuous resource (qubit swapping). They also extend the simulation result above in various ways. In particular, by exploiting properties of Clifford operations in conjunction with the Jordan-Wigner representation of a Clifford algebra, they show how one may generalise the simulation result above to provide further classes of classically efficiently simulatable quantum circuits, which we call Gaussian quantum circuits.

Bibliography

[1] J. Anders and D. E. Browne (2008) *Computational Power of Correlations*. Phys. Rev. Lett. 102, 050502.

[2] E. Blakey (2008) *Computational Complexity in Non-Turing Models of Computation; The What, the Why and the How.* Proceedings of Quantum Physics and Logic/Development of Computational Models 2008, to appear in the series Electronic Notes in Theoretical Computer Science, M. Mislove (managing editor), B. Coecke, P. Panangaden (guest editors).

[3] D. E. Browne and J. Anders (2008) *The Role of Classical Computation in Measurement-Based Quantum Computation*. Lecture Notes in Computer Science 5028, 94 (2008) - Presented at Computability in Europe 2008, Athens.

[4] D. E. Browne, M. B. Elliott, S. T. Flammia, S. T. Merkel, A. Miyake and A. J. Short (2008) *Phase transition of computational power in the resource states for one-way quantum computation* New J. Phys. 10, 023010.

[5] N. Brunner, N. Gisin, S. Popescu, V. Scarani (2008) *Simulation of partial entanglement with no-signaling resources*. Phys. Rev. A 78, 052111 (2008). `arXiv:0803.2359`.

[6] B. Coecke and B. Edwards (2008) Toy quantum categories. Electronic Notes in Theoretical Computer Science, to appear. `arXiv:0808.1037`

[7] B. Coecke, B. Edwards and R. Spekkens (2008) The group theoretic origin of non-locality for qubits. Draft paper.

[8] A. W. Harrow and D. W. Leung (2008) *An exponential separation between the entanglement and communication capacities of a bipartite unitary interaction*. arXiv:0803.3066.

[9] M. B. Hastings and A. W. Harrow (2008) *Classical and Quantum Tensor Product Expanders*. `arXiv:0804.0011`.

[10] R. Jozsa (2008) *Embedding classical into quantum computation*. LNCS 5393 Beth Festschrift, J Calmet, W. Geiselmann, J. Mueller-Quade (Eds.), pp 43–49. `arXiv:08124511`.

[11] R. Jozsa and A. Miyake (2008) *Matchgates and classical simulation of quantum circuits*. Proc. Roy. Soc. (Lond.) A 464, p3089-3106 (Dec 2008). `arXiv:0804.4050`.

[12] K. Martin and P. Panangaden (2008) *A technique for verifying measurements*. To appear in the proceedings of the XXIV Symposium on Mathematical Foundations of Programming Semantics. `http://www.cs.mcgill.ca/ prakash/accepted.html`

[13] A. Montanaro and T. J. Osborne (2008) *Quantum boolean functions*. `arXiv:0810.2435`.

[14] D. Pavlovic (2008) *Quantum and classical structures in nondeterministic computation*. Preprint. `arxiv:0812.2266`

[15] S. Pirandola, S. Braunstein and S. Lloyd (2008) *Characterisation of collective Gaussian attacks and security of coherent-state quantum cryptography*. Physical Review Letters 101, 200504-1/4.

[16] S. Pirandola, S. Mancini, S. Lloyd and S. Braunstein (2008) *Continuous-variable quantum cryptography using two-way quantum communication*. Nature Physics 4, pp. 726–730.

[17] M. Sadrzadeh (poster at Obergurgl) *Maximal Entropy Analysis of Degrees of Information in Quantum Protocols*, QICS European Project Workshop on Foundational Structures for Quantum Information and Computation, Austria, Sept 2008.

[18] P. Skrzypczyk, N. Brunner and S. Popescu (2008) *Emergence of Quantum Mechanics from Non-Locality Swapping*. `arXiv:0811.2937`.

[19] Walker, Polack and Braunstein (2008) *Error-correcting Bell inequalities*. Physical Review Letters 101 220501-1/4.

[20] S. Wehner and J. Wullschleger (2008) *Composable Security in the Bounded-Quantum-Storage Model*. Proceedings of ICALP 2008, pp. 604–615. `arXiv:0709.0492`.

[21] S. Winkler, S. Wolf and J. Wullschleger (2008) *Bit Commitment from Non-Local Correlations*. `arXiv:0811.3589`.

Chapter 7

W4 – *deliverable D4*: Quantum automata, machines and calculi

A current account of the objectives of W4 and comparison with the state-of-the art. Objective W4.O1 is concerned with understanding classically-controlled Quantum Computation in terms of a unified and fully general model. There are many interesting questions one can come up with in this context and they have become very refined. We can consider that this research objective has been met – as much as it can possibly be – [7, 10, 13, 20, 24, 30, 32, 33].

Objective W4.O2 is concerned with understanding quantum control structures for Quantum Computation. Quantum Cellular Automata are a good example of architecture which gets rid of the necessity for classical control [4, 5, 6, 7, 25, 36]; however, we should mention that their purpose is not give a meaning to this elusive notion of quantum control. On the other hand, the linear-algebraic lambda-calculus [2, 3] does that to some extent even if it does not address the question directly : this language is minimal an yet, it clearly encompasses such a notion. Attempts to tackle the question directly are found in [17, 22] but the results are still intermediate.

Objective W4.O3 is concerned with understanding the structure of Quantum Cellular Automata (QCA). Some radical progress has been made [4, 5, 6, 35, 36]. What remains to be understood is the structure of Open QCA (i.e. QCA with quantum operations as evolutions); we can find some preliminary results about these in [5].

Objective W4.O4 is related to W4.O3 and W4.O6.

Objective W4.O5 is about finding denotational semantics accommodating higher order functions in quantum functional languages. Many progresses have been accomplished along that aim [9, 10, 30, 31, 33]. It seems that for classically-controlled Quantum Computation the question is solved though it lacks a unifying view. For quantum-controlled Quantum Computation the question is only now being attacked.

Objective W4.O6 is concerned with developing theories and techniques for analysis and verification of concurrent classical plus quantum systems. We can no doubt say that it has taken a lot of momentum in contributions [11, 25, 27, 32] with some automated tools for entanglement or security analysis. This objective is, of course, very open-ended.

Main developments in W4. Here are some non-exhaustive highlights of the contributions brought to W4. In Task 1:

- A number of interesting results have arisen that are concerned with understanding the basic resources that are required for performing Quantum Computation. A first negative result [7] states that random quantum states are not of much use for Measurement-Based Quantum Computation. A second positive result [13] states that one qubit gate plus any entangling two qubit gate form a universal set. Taken together, both contributions provide formal evidence and a quantified sense in which one could say that "Quantum Computation arises as soon as usable entanglement becomes available".

- The papers [20, 24] are further developments in terms of classically-controlled models of Quantum Computation which enable to solve the problem linked with iteration and halting i.e., "how to observe that some condition is satisfied, without spoiling the computation via this observation?". → *get a Universal QTM from this picture*.

In Task 2:

- What could it mean for a physical theory to be universal? Usually a physical theory is something that describes space, time, objects living in this background and the way they interact. 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 rather like being able to simulate a whole network of them in parallel, respecting the topology of the network and the way they interact. Paper [4] illustrates this fascinating question by giving explicit constructions in the simplified context of one-dimensional Quantum Cellular Automata (1DQCA). → *The n-dimensional case?*

- Again consider in very broad terms a physical theory which describes space, time, some objects living upon this background and the way they interact. Say that this theory is endowed with a well-defined notion of a global evolution i.e., a forward step operator which acts across the entire space, taking the overall state from t to $t+1$. We can say that a global evolution is causal if there exists a bound to the distance information that can travel in one time step. Moreover, a global evolution can be said to be locally implementable if it can be decomposed into smaller, elementary local evolutions which involve only neighbouring sites. Because of entanglement, it is far from trivial in a quantum theoretical setting, to show that causality implies local implementability. Such a question is solved when the global evolution is unitary and space is discrete. In the context of Quantum Cellular Automata, this entails that the definition of Schumacher and Werner [28] admits a block structure, which turns out to be that of Perez-Delgado and Cheung. Hence we have a unifying picture for n-dimensional QCA. → *Open QCA, i.e. non-unitary case.*

In Task 3:

- Contributions [9, 10, 30, 31, 33] address the hard question of a denotational semantics for quantum programming languages. Some of 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 this models come in various flavours. → *Unify these views and fragments. Move on to Quantum Control.*

- Contributions [2] and [3] provide a minimal and general Linear-Algebraic Lambda-Calculus, in which to explore quantum control, as well as potential Quantum Physical Logics that might arise from original type systems for the calculus, via the Curry-Howard Isomorphism. → *Denotational semantics? More fancy types and hence logics.*

- Contribution [12] further develops the functional quantum language QML, introducing a new syntax, examples, and judgements, and an implementation of a compiler and simulator for the language in Haskell. Orthogonality and the problems with coproducts are also discussed.

- In [25] the various developments of quantum programming languages lead to a practical application. Importing methods from abstract interpretation, an algorithm is described which works out the resources consumed by a quantum algorithm, in terms of how many entangled qubits are required for its well-functioning. → *Less coarse-grained analysis? Check for other properties?*

In Task 4 :

- In [11, 27] some general methods are described which serve the goal of proving the security of quantum cryptographic protocols. The first two contributions deal with an automated method which is based upon the operational semantics of a distributed quantum computation model, itself related to Measurement-Based Quantum Computation (MBQC). This is a particularly interesting idea as Measurement-Based Quantum Computation is a particularly good theoretical framework for dealing with all sorts of measurements ... and hence all sorts of attackers. → *Understand exactly how much MBQC gives us as a model for Secure Multi-party quantum cryptographic problems, as illustrated in the Universal Blind Quantum Computation of Broadbent, Fitzsimons and Kashefi [8].*

The next steps to take. These have been indicated in italics next to the above highlights of main developments in W4.

Interactions with other workpackages and sites. As in the previous year it remains the case that most interactions of W4 are with W1 as MBQC and the measurement calculus are indeed at the basis of several outcomes of W4: classically-controlled Turing machine [24], minimal resources for QC [7, 24], formalism for reasoning about knowledge in quantum protocols (extension of measurement calculus) [11, 27]. Some contributions are both in W1 and W2 [7, 22, 32], and some others both in W1 and a few make it to W3 [11, 15, 16, 27].

Interactions among sites have been productive. There have been many co-signed papers for instance:

- between the Grenoble and Braunschweig, Oxford and Paris sites, on QCA quantum calculi, types for separability and entanglement.

- between Bristol and Innsbruck on Matchgates.

Pablo Arrighi and Medhi Mahlla
Grenoble, February 10, 2009.

Workpackage objectives:

W4.O1 Develop a unified and fully general model for quantum computations under classical control.

W4.O2 Obtain a deeper and more logical understanding of possible quantum control structures for QIC.

W4.O3 Give satisfactory accounts of unitarity, irreversibility, universality and complexity in QCAs.

W4.O4 Merge computational and spatio-temporal notions within a single model of QIC.

W4.O5 Find a denotational semantics accommodating higher order functions in quantum functional languages.

W4.O6 Develop theories and techniques for analysis and verification of concurrent classical+quantum systems.

Workpackage milestones:

W4.M1 Classically-controlled quantum Turing machines, and their use for characterizing classical+quantum computational complexity. (12)

W4.M2 A functional type system taking into account entanglement and separability of quantum data; an abstract domain for static analysis of entanglement by means of abstract interpretation. (12)

W4.M3 A fully general classical+quantum calculus, its formal properties, and its applications to quantum program specification and transformation. (24)

W4.M4 Characterization of physically and computationally relevant QCAs, and of the computational power of irreversible and measurement-based QCAs; definition of universal QCAs. (24)

W4.M5 Type systems and model-checking techniques for analysis and verification of quantum protocols (24)

W4.M6 Categorical interpretation of iteration, feedback, and control structures in state machine-like models of quantum computation. (36)

W4.M7 A quantum functional language incorporating higher-order functions, non-terminating recursion, infinite data structures, with its denotational semantics. (36)

W4.M8 Equivalences and compositional techniques for component-wise correctness proofs of concurrent quantum systems. (36)

Below we discuss the detailed progress for this workpackage which comprises the *workpackage tasks*:

W4.T1 Study quantum machines: classically controlled quantum computation, quantum state machines, quantum-mechanical control structures.

W4.T2 Study quantum cellular automata: unitarity and compositionality of QCAs, irreversibility in QCAs, universality and complexity of QCAs.

W4.T3 Develop and exploit quantum calculi, types, and semantics: quantum lambda-calculi, higher-order quantum programs, type systems, logics and semantics for functional quantum languages, quantum types for entanglement.

W4.T4 Develop and exploit quantum process-calculi, and models of quantum concurrency: types for certification of quantum systems, model-checking, equivalences and compositional techniques for analysis and verification of quantum processes.

7.1 Progress towards objectives and performed tasks for W4.T1

8.1.a Are random pure states useful for quantum computation? (Objectives: W4.O1, W4.O2; Milestones: W4.M1, W4.M2) In [7] Bremner (UNIVBRIS; QICS postdoc), Mora and Winter (UNIVBRIS) show the following: a randomly chosen pure state as a resource for measurement-based quantum computation, is - with overwhelming probability - of no greater help to a polynomially bounded classical control computer, than a string of random bits. Thus, unlike the familiar "cluster states", the computing power of a classical control device is not increased from P to BQP, but only to BPP. The same holds if the task is to sample from a distribution rather than to perform a bounded-error computation. Furthermore, they show that their results can be extended to states with significantly less entanglement than random states.

8.1.b Exact universality from any entangling gate without inverses. (Objectives: W4.O1, W4.O3) In [13] Harrow (UNIVBRIS) proves that arbitrary local gates together with any entangling bipartite gate V are universal. Previously this was known only when access to both V and V-1was given, or when approximate universality was demanded.

8.1.c Partial observation of quantum Turing machine and weaker well-formedness condition (Objective: W4.O1; Milestone: W4.M1) In [24], Perdrix (Gre & OX & Paris; QICS Postdoc) introduces a weakening of the well-formedness conditions for quantum Turing machines introduced by Deutsch, leading to a new class of Turing machines, the Observed Quantum Turing Machines (OQTM). The introduction of such abstract machines allowing classical and quantum computations is motivated by the emergence of models of quantum computation like the one-way model. More generally, the OQTM aims to be an abstract framework for the pragmatic paradigm of quantum computing: 'quantum data, classical control'. This model allows a formal treatment of problems requiring classical interactions, like the halting of quantum Turing machines and opens new perspectives for the construction of a universal quantum Turing machine.

8.1.d Quantum circuits giving oracles for abstract machine computations (Objective: W4.O1) In [20], P. Hines tackles a single precisely defined problem. An Abstract machine (as defined in D2), with specified starting and halting subsets, defines a computation based on conditional iteration. The problem solved is the following: given a quantum oracle for the 'primitive evolution' (i.e. the operational semantics) of an abstract machine, how may we construct a quantum oracle for the computation? Explicit circuits are given to do this. For a computation with worst-case running time T, the solution has complexity $O(3T)$, and requires an ancilla of $2.\log(T)$ qubits that start and finish in the constant state $|0\rangle$.

8.1.e Hybrid quantum computation in quantum optics In this paper [34] Van Look et al. propose a hybrid quantum computing scheme where qubit degrees of freedom for computation are combined with quantum continuous variables for communication. In particular, universal two-qubit gates can be implemented deterministically through qubit-qubit communication, mediated by a continuous-variable bus mode ("qubus"), without direct interaction between the qubits and without any measurement of the qubus.

8.1.f Random Quantum Circuits are Approximate 2-designs (Milestones: W4.M1, W4.M6) Given a universal gate set on two qubits, it is well known that applying random gates from the set to random pairs of qubits will eventually yield an approximately Haar-distributed unitary. However, this requires exponential time. In [14] Harrow (UNIVBRIS) and Low (UNIVBRIS) show that random circuits of only polynomial length will approximate the first and second moments of the Haar distribution, thus forming approximate 1- and 2-designs. Previous constructions required longer circuits and worked only for specific gate sets. As a corollary of their main result, they also improve previous bounds on the convergence rate of random walks on the Clifford group.

8.1.g Categorical analogues of monoid semirings (Milestone: W4.M6) This paper [18] (P. Hines) is a strongly category-theoretic approach to one of the fundamental building blocks of quantum algorithms. Using the algebraic characterisation of the Discrete Fourier Transform as an isomorphism between a group ring and a direct sum (categorically, product) of rings, this paper aims to reproduce this theory in a more general categorical setting. By replacing both groups and rings by categories in the usual definition of a group ring, a general categorical construction is given. This reduces to the usual group-ring construction in the one-object case. Following this, the conditions required to emulate the isomorphism provided by the discrete Fourier transform (that is, the existence of analogues of character groups) are considered.

7.2 Progress towards objectives and performed tasks for W4.T2

8.2.a Quantum Cellular Automata. (Objectives W4.O2, W4.O3, W4.O4; Milestone W4.M4, W4.M6) In [36] Wiesner (UNIVBRIS) reviews Quantum cellular automata (QCA), including early and more recent proposals. QCA are a generalization of (classical) cellular automata (CA) and in particular of reversible CA. The latter are reviewed shortly. An overview is given over early attempts by various authors to define one-dimensional QCA. These turned out to have serious shortcomings which are discussed as well. Various proposals subsequently put forward by a number of authors for a general definition of one- and higher-dimensional QCA are reviewed and their properties such as universality and reversibility are discussed.

8.2.b Intrinsically universal one-dimensional quantum cellular automata in two flavours (Objectives: W4.O2, W4.O3, W4.M4) In [4] Arrighi, Fargetton and Wang (Gre) a one-dimensional quantum cellular automaton (QCA) capable of simulating all others. By this we mean that the initial configuration and the local transition rule of any one-dimensional QCA can be encoded within the initial configuration of the universal QCA. Several steps of the universal QCA will then correspond to one step of the simulated QCA. The simulation preserves the topology in the sense that each cell of the simulated QCA is encoded as a group of adjacent cells in the universal QCA. The encoding is linear and hence does not carry any of the cost of the computation. We do this in two flavours: a weak one which requires an infinite but periodic initial configuration and a strong one which needs only a finite initial configuration.

8.2.c Unitarity plus causality implies locality (Objectives: W4.O2, W4.O3) In [6] Arrighi (Gre), Nesme (Brau, QICS postdoc) and Werner (Brau) 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. They 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. They apply this representation theorem to n-dimensional quantum cellular automata and show that they can be put into the form of an infinite tiling of more elementary, finite-dimensional unitary evolutions.

8.2.d Quantization of Cellular Automata (Objectives: W4.O2, W4.O3; Milestone: W4.M4). In [5] Arrighi (Gren) and Nesme (Brau; QICS postdoc) tackle the problem of quantizing classical CA. They show that the linearization of a classical CA satisfies causality if and only if the CA is reversible. So, while a robust definition of nonreversible QCA is still not available, they exclude a whole category of objects from this class: linearizations of nonreversible classical CA can never be acceptable nonreversible QCA.

8.2.e Index Theory for One-dimensional Reversible Quantum Walks and Quantum Cellular Automata. (Objectives: W4.O2, W4.O3; Milestone W4.M4). In [35] Vogts (Brau) and Werner (Brau) define indexes for one-dimensional reversible QW and QCA. This is a very robust definition (you don't even have to assume shift invariance, not even in the cell structure) having many nice properties. For the composition of walks or automata, it is a group homomorphism. When considering the tensor product of walks or automata, it is a monoid homomorphism. The index is a continuous function, and takes different values on different connected components of the set of walks/automata. The index theory, together with other published articles on the structure of one-dimensional reversible cellular automata, pretty much closes the subject of the classification of these objects.

8.2.f The fractal structure of the space-time diagrams of Clifford Cellular Automata (Milestone: W4.M4). Gutschow (Brau) and Nesme (Brau; QICS postdoc) explain the fractal structure of the space-time diagrams of Clifford Cellular Automata. When running QCA on some particular observables, one can often see a fractal structure emerge. They explain why this happens and how to "predict" this structure and find some of its properties, like its fractal dimension.

7.3 Progress towards objectives and performed tasks for W4.T3

8.3.a Quantum games as quantum types (Objectives: W4.05; Milestones: W4.M3, W4.M7) In [9], Y. Delbecque (McGi) presents a new model for higher-order quantum programming languages. The proposed model is an adaptation of the probabilistic game semantics developed by Danos and Harmer expanded with quantum strategies which enable one to represent quantum states and quantum operations. Some of the basic properties of these strategies are established and then used to construct denotational semantics for three quantum programming languages. The first of these languages is a formalisation of the measurement calculus proposed by Danos et al. The other two are new: they are higher-order quantum programming languages. Previous attempts to define a denotational semantics for higher-order quantum programming languages have failed. Some of the key reasons for this are identified and the design of the higher-order languages are based on these observations. The game semantics proposed in the thesis is the first denotational semantics for a lambda-calculi equipped with quantum types and with extra operations which allow one to program quantum algorithms. The quantum strategies presented in this thesis allow one to understand the constraints that must be imposed on quantum type systems with higher-order types. Quantum strategies are a new mathematical model which describes the interaction between classical and quantum data using system-environment dialogues. The interactions between the different parts of a quantum system are described using the rich structure generated by composition of strategies. This approach has enough generality to be put in relation with other work in quantum computing. Quantum strategies could thus be useful for other purposes than the study of quantum programming languages.

8.3.b Game semantics for quantum stores (Objectives: W4.O1, W4.O5; Milestones: W4.M3, W4.M7) In [10], Y. Delbecque and P. Panangaden present a game semantics for a simply-typed -calculus equipped with quantum stores. The quantum stores are equipped with quantum operations as commands which give the language enough expressiveness to encode any quantum circuits. The language uses a notion of extended variable, similar to that seen in functional languages with pattern matching, but adapted to the needs of dealing with tensor products. These tensored variables are used to refer to quantum stores and to keep track of the size of the states which they contain. The game semantics is constructed from classical game semantics using intervention operators to encode the effects of the commands. A soundness result for the semantics is given.

8.3.c On a fully abstract model for a quantum linear functional language (Objectives: W4.O1, W4.O5; Milestones: W4.M3, W4.M7) In [31], P. Selinger (McGi) and B. Valiron (McGi) study the linear fragment of the programming language for quantum computation with classical control previously introduced. They sketch the language, and discuss equivalence of terms. In addition, they also describe a fully abstract denotational semantics based on completely positive maps.

8.3.d A linear-non-linear model for a computational call-by-value lambda calculus (Objectives W4.O1, W4.O5; Milestones W4.M3, W4.M7) In [30], P. Selinger and B. Valiron give a categorical semantics for a call-by-value linear lambda calculus. Such a lambda calculus was used by Selinger and Valiron as the backbone of a functional programming language for quantum computation. One feature of this lambda calculus is its linear type system, which includes a duplicability operator "!" as in linear logic. Another main feature is its call-by-value reduction strategy, together with a side-effect to model probabilistic measurements. The "!" operator gives rise to a comonad, as in the linear logic models of Seely, Bierman, and Benton. The side-effects give rise to a monad, as in Moggi's computational lambda calculus. It is this combination of a monad and a comonad that makes the present paper interesting. We show that our categorical semantics is sound and complete.

8.3.e Semantics for a Higher Order Functional Programming Language for Quantum Computation (Objectives: W4.O1, W4.O5; Milestones: W4.M3, W4.M7) In [33], B. Valiron (McGi) develops a semantics for higher order quantum information. Following the work done in [29], the author studies a lambda calculus for quantum computation with classical control. The language features two important properties:

> (i) The first one, arising from the so-called no-cloning theorem of quantum computation, is the need for a distinction between duplicable and non-duplicable elements. For keeping track of duplicability at higher order, we use a type system inspired by the resource-sensitive linear logic.
>
> (ii) The second important aspect is the probability inherent to measurement, the only operation for retrieving classical data from quantum data. This forces us into choosing a reduction strategy for being able to define an operational semantics.

He also address the question of a denotational semantics. First, he restricts the study to the strictly linear aspect to build a fully abstract denotational model of the strictly linear fragment of the language. Further, the studies the full language results in a model called a linear category for duplication. Finally, he only focus on the fragment of the language that contains the aforementioned elements, and remove the classical Boolean and quantum Boolean features to get a generic computational linear lambda-calculus. In this idealized setting, he shows that such a language have a full and complete interpretation in a linear category for duplication.

8.3.f Linear-algebraic Lambda-calculus: higher-order, encodings and confluence (Objectives: W4.O2, W4.O5) In [3] Arrighi (Gre) and Dowek (Lix) introduce a minimal language combining both higher-order computation and linear algebra. Roughly, this is nothing else than the Lambda-calculus together with the possibility to make linear combinations of terms $a.t + b.u$. They describe how to "execute" this language in terms of a few rewrite rules, and justify them through the two fundamental requirements that the language be a language of linear operators, and that it be higher-order. They mention the perspectives of this work in field of quantum computation, whose circuits we show can be easily encoded in the calculus. Finally we prove the confluence of the calculus, this is our main result.

8.3.g Measurements and confluence in quantum lambda calculi with explicit qubits (Objective: W4.O1) In [1] Daz-Caro (Gren) et al. demonstrate how to add a measurement operator to quantum lambda-calculi. A proof of the consistency of the semantics is given through a proof of confluence presented in a sufficiently general way to allow this technique to be used for other languages. The method described here may be applied to probabilistic rewrite systems in general, and to add measurement to more complex languages such as QML or Lineal, which is the subject of further research.

8.3.h Scalar System F for Linear-Algebraic Lambda-Calculus: Towards a Quantum Physical Logic? (Objectives: W4.O2, W4.O5) The aim of this work [2] by Arrighi and Diaz-Caro (Gre) is to set up a System F type system à la Curry for the Linear-Algebraic lambda-Calculus (Lineal) [3] able to handle scalars within the types, and hence in some way characterise the amount of a type, following the idea of superposition in the sense of how much a term belongs to a type. The reason why we use Lineal is because it has the advantage of not being bound to a particular type system (being untyped), and it is general enough to describe any quantum computation in terms of vectors. This scalar type system is at the first step of a research program which seeks for a form quantum physical logic obtained via the Curry-Howard isomorphism; it is also interesting in itself because of its relations with probabilistic systems, Linear Logic (LL), cloning, etc.

8.3.i An overview of QML with a concrete implementation in Haskell (Objectives W4.O2, W4.O5) This paper [12] by Grattage (Gren; QICS Postdoc) gives an introduction to and overview of the functional quantum programming language QML. The syntax of this language is defined and explained, along with a new QML definition of the quantum teleport algorithm. The categorical operational semantics of QML is also briefly introduced, in the form of annotated quantum circuits. This definition leads to a denotational semantics, given in terms of superoperators. Finally, an implementation in Haskell of the semantics for QML is presented as a compiler. The compiler takes QML programs as input, which are parsed into a Haskell datatype. The output from the compiler is either a quantum circuit (operational), an isometry (pure denotational) or a superoperator (impure denotational). Orthogonality judgements and problems with coproducts in QML are also discussed.

8.3.j A logical analysis of entanglement and separability in quantum higher-order functions (Objective W4.O6; Milestone W4.M5) In this paper [26], Prost et al. (Gren) present a logical separability analysis for a functional quantum computation language. This logic is inspired by previous works on logical analysis of aliasing for imperative functional programs. Both analyses share similarities notably because they are highly non-compositional. Quantum setting is harder to deal with since it introduces non determinism and thus considerably modifies semantics and validity of logical assertions. This logic is the first proposal of entanglement/separability analysis dealing with a functional quantum programming language with higher-order functions.

8.3.k Quantum Entanglement Analysis based on Abstract Interpretation (Objective: W4.O6; Milestone: W4.M5) Entanglement is a non local property of quantum states which has no classical counterpart and plays a decisive role in quantum information theory. Several protocols, like the teleportation, are based on quantum entangled states. Quantum algorithms which do not create entanglement can be efficiently simulated on a classical computer. The exact role of the entanglement is nevertheless not well understood. Since an exact analysis of entanglement evolution induces an exponential slowdown, Perdrix (Gre & OX & Paris; QICS Postdoc) considers an approximate analysis based on the framework of abstract interpretation. In [25], a concrete quantum semantics based on superoperators is associated with a simple quantum programming language. The representation of entanglement, i.e. the design of the abstract domain is a key issue. A representation of entanglement as a partition of the memory is chosen. An abstract semantics is introduced, and the soundness of the approximation is proven.

8.3.l The structure of partial isometries This paper [21] studies both Neumann-Birkhoff quantum logic, and Abramsky-Coecke categorical quantum semantics using partial isometries - in particular, a partial order on partial isometries introduced by Halmos & McLaughlin. This partial order is shown to be a natural generalisation of the usual subspace ordering used in (lattice-theoretic) quantum logic. Using standard techniques from the field of inverse categories, a composition based on this partial order is given, allowing us to define a category of partial isometries that may reasonably be considered a categorification of Birkhoff-von Neumann quantum logic. This thus enables a comparison to be made with Abramsky-Coecke style categorical approaches to quantum mechanics. Explicit calculations are given, relating to the treatment of teleportation in both systems, that demonstrate a fundamental incompatibility between the two approaches. This is based on the differing treatment of post-selection by the two systems.

8.3.m Machine Semantics (Milestone: W4.M6) In [19] we combine categorical models of iteration with domain-theoretic techniques to give a very general treatment of conditional iteration and causality in physical and computational systems (Abstract Machines). This provides concrete tools for reasoning about and manipulating a range of computational devices, from the von Neumann architecture to space-bounded Turing machines. The tools presented are designed to be equally applicable in the quantum-mechanical setting, and specifically quantum-mechanical applications are given, and extended in [20] and [25].

8.3.n Can a quantum computer run the von Neumann architecture? (Objective: W4.O2) This paper [17] (P. HineS) is a study of the program code / data distinction in the context of quantum computation. Starting from the stored-code programming paradigm introduced by von Neumann, it identifies the core of this architecture as the notion of 'evaluation' or the interchangeability of data and code. This is based on the notion of 'abstraction' in the logical systems, and the closely related evaluation operation within monoidal closed categories. Various candidates for such operations are considered within the quantum-mechanical setting (including Nielsen/Chuang orthonomal basis encoding, Abramsky-Coecke compact closure, the Brassard-Braunstein-Cleve protocol, and the Choi-Jamiolkowsky correspondence). An ultimate obstacle to such an operation is shown to be the Gottesmann-Knill theorem: any 'stored-code quantum computer' must be restricted to Clifford group operations, and thus may be efficiently simulated by a classical computer.

7.4 Progress towards objectives and performed tasks for W4.T4

8.4.a Classical Knowledge for Quantum Security (Milestone: W4.M5) In [11] M. Sadrzadeh (Paris and Oxford; QICS Postdoc) proposes a decision procedure for analysing security of quantum cryptographic protocols. It combines a classical algebraic rewrite system for knowledge with an operational semantics for quantum distributed computing (developed with other QICS members: E. Kashefi V. Danos, and P. Panangaden). As a test case the procedure is used to reason about security properties of a recent quantum secret sharing protocol proposed by D. Markham (Paris, QICS post-doc) published in Physical Review A'08). Three different scenarios based on the safety assumptions of the classical and quantum channels are analysed. The novelty of our approach lies in the simplicity of the algebraic semantics and thus the decision procedure based on it; in particular the epistemic analysis used to discover the paths of attacks is purely based on a simple intuitive classical notion of knowledge.

8.4.b Aximo: Automated Axiomatic Reasoning for Information Update (Milestone: W4.M5) In [27] S. Richards and M. Sadrzadeh (Paris and Oxford; QICS Postdoc) discuss the implementation of the algebra and decision procedure mentioned above. The implemented program is a re-write engine which interacts with the user to input the description of the protocol, then given an epistemic property outputs a yes-no answer, together with the full path of the analysis that led to that answer. A yes answer means that the protocol, as described by the user, satisfies the epistemic property; more precisely, that a principal acquires a certain piece of information in all the end states resulting from running the protocol. Previous work of M. Sadrzadeh (Paris and Oxford; QICS Postdoc) has shown how the addition of a simple axiom set (formalizing the measurement effects of agents sharing Bell pairs) to this decision procedure makes the method applicable to the verification of quantum protocols.

8.4.c Temporally Unstructured Quantum Computation. (Objectives: W4.O1, W4.O6; Milestones: W4.M1, W4.M6, W4.M8) In [32] Shepherd (UNIVBRIS) and Bremner (UNIVBRIS; QICS postdoc) examine theoretic architectures and an abstract model for a restricted class of quantum computation, called here instantaneous quantum computation because it allows for essentially no temporal structure within the quantum dynamics. Using the theory of binary matroids, they argue that the paradigm is rich enough to enable sampling from probability distributions that cannot, classically, be sampled from efficiently and accurately. This paradigm also admits simple interactive proof games that may convince a skeptic of the existence of truly quantum effects. Furthermore, these effects can be created using significantly fewer qubits than are required for running Shor's Algorithm.

8.4.d Quantum boolean functions (Objectives: W4.O2, W4.O3) In [22] Montanaro (UNIVBRIS; QICS postdoc) and Osborne introduce the study of quantum boolean functions, which are unitary operators f whose square is the identity: $f^2 = I$. They describe several generalisations of well-known results in the theory of boolean functions, including quantum property testing; a quantum version of the Goldreich-Levin algorithm for finding the large Fourier coefficients of boolean functions; and two quantum versions of a theorem of Friedgut, Kalai and Naor on the Fourier spectra of boolean functions. In order to obtain one of these generalisations, they prove a quantum extension of the hypercontractive inequality of Bonami, Gross and Beckner.

8.4.e Low Efficient Quantum Tensor Product Expanders and k-designs. Harrow (UNIVBRIS) and Low (UNIVBRIS) in [15] give an efficient construction of constant-degree, constant-gap quantum k-tensor product expanders. The key ingredients are an efficient classical tensor product expander and the quantum Fourier transform. Their construction works whenever $k = O(n/\log n)$, where n is the number of qubits. An immediate corollary of this result is an efficient construction of approximate unitary k-designs on n qubits for any $k = O(n/\log n)$.

8.4.f Classical and Quantum Tensor Product Expanders. In [16] Hastings and Harrow (UNIVBRIS) introduce the concept of quantum tensor product expanders. These are expanders that act on several copies of a given system, where the Kraus operators are tensor products of the Kraus operator on a single system. They begin with the classical case, and show that a classical two-copy expander can be used to produce a quantum expander. They then discuss the quantum case and give applications to the Solovay-Kitaev problem. They give probabilistic constructions in both classical and quantum cases, giving tight bounds on the expectation value of the largest nontrivial eigenvalue in the quantum case.

Bibliography

[1] P. Arrighi, A. Diaz-Caro (2008) *Measurements and confluence in quantum lambda calculi with explicit qubits*, QPL'08, Pre-print arXiv:0806.2447

[2] P. Arrighi, A. Diaz-Caro, M. Gadella, J. Grattage (2008) *Scalar System F for Linear-Algebraic lambda-Calculus: Towards a Quantum Physical Logic?* Submitted to QPL'09.

[3] P. Arrighi, G. Dowek (2008) *Linear-algebraic lambda-calculus: higher-order, encodings and confluence*, RTA'08, LNCS 5117, Pre-print arXiv:quant-ph/0612199.

[4] P. Arrighi, R. Fargetton and Z. Wang (2008)*Intrinsically universal one-dimensional quantum cellular automata in two flavours*. Fundam. Informaticae, Pre-print arXiv:/0704.3961.

[5] P. Arrighi and V. Nesme (2008) *Quantization of Cellular Automata*. Presented in Journées Automates Cellulaires 2008. Proceedings in HAL.

[6] P. Arrighi, V. Nesme and R. Werner (2008) *Unitarity plus causality implies locality*, Pre-print arXiv:0711.3975, invited talk by Pablo Arrighi in "Foundational Structures for Quantum Information and Computation", Obergurgl, Austria, September 2008 and in the final meeting of the GdR Information et communication quantiques, Paris, October 2008.

[7] M. J. Bremner, C. Mora and A. Winter (2008) *Are random pure states useful for quantum computation?* arXiv: 0812.3001

[8] A. Broadbent, J. Firzsimons and E. Kashefi (2008) *Universal Blind Quantum Computation*. arXiv:0807.4154

[9] Y. Delbecque's Ph.D. Thesis. Advisor: Prakash Panangaden (McGi) (2008) *Quantum games as quantum types*. McGill University.

[10] Y. Delbecque and P. Panangaden (2008) Game semantics for quantum stores. To appear in the proceedings of the XXIV Symposium on Mathematical Foundations of Programming Semantics. http://www.cs.mcgill.ca/∼prakash/accepted.html

[11] E. D'Hondt and M. Sadrzadeh (2008). *Classical Knowledge for Quantum Security*. To appear in Electronic Notes in Theoretical Computer Science, Proceedings of Joint workshop on Quantum Physics and Logic and Development of Computational Models, International Colloquium on Automata, Languages and Programming (ICALP), July 2008. arXiv:0808.3574

[12] J. Grattage (2008) *An overview of QML with a concrete implementation in Haskell*, QPL '08, Pre-print arXiv:0806.2735.

[13] A. W. Harrow (2008) *Exact universality from any entangling gate without inverses*. arXiv:0806.0631

[14] A. W. Harrow and R. Low (2008) *Random Quantum Circuits are Approximate 2-designs*. To appear in Comm. Math. Phys. arXiv:0802.1919

[15] A. W. Harrow and A. Richard (2008) *Low Efficient Quantum Tensor Product Expanders and k-designs*. arXiv:0811.2597.

[16] M. B. Hastings and A. W. Harrow (2008) *Classical and Quantum Tensor Product Expanders*. arXiv:0804.0011.

[17] P. Hines (2008) *Can a quantum computer run the von Neumann architecture?* New structures in Physics, submitted.

[18] P. Hines (2008) *Categorical analogues of monoid semirings* . Mathematical Structures in Computer Science, submitted.

[19] P. Hines (2008) *Machine Semantics*. Theoretical Computer Science **409**.

[20] P. Hines (2008) *Quantum circuits giving oracles for abstract machine computations* (Theoretical Computer Science, submitted)

[21] P. Hines and S. Braunstein (2008) *The structure of partial isometries*. Semantic Structures in Quantum Computation, to appear.

[22] A. Montanaro and T. J. Osborne (2008) *Quantum boolean functions*. `arXiv:0810.2435`.

[23] D. Pavlovic (2008) *Quantum and classical structures in nondeterministic computation*. Preprint. `arxiv:0812.2266`

[24] S. Perdrix (2008) *Partial observation of quantum Turing machine and weaker well-formedness condition.* In proceedings of Joint Quantum Physics and Logic & Development of Computational Models (Joint 5th QPL and 4th DCM).

[25] S. Perdrix (2008). *Quantum Entanglement Analysis based on Abstract Interpretation*. 15th International Static Analysis Symposium (SAS'08). Lecture Notes in Computer Science (LNCS) volume 5079, pp. 270–282.

[26] F. Prost and C. Zerrari (2008) *A logical analysis of entanglement and separability in quantum higher-order functions*, Submitted to QPL'09, Pre-print `arXiv:0801.0649`

[27] S. Richards and M. Sadrzadeh (2008). *Aximo: Automated Axiomatic Reasoning for Information Update*. To appear in Electronic Notes in Theoretical Computer Science, in the Proceedings of the 5th workshop on Methods for Modal Logic, Ecole normal superieure de Cachan, Nov 2007.

[28] B. Schumacher and R.F. Werner (2004) *Reversible quantum cellular automata*. `quant-ph/0405174` to appear in New Journal of Physics

[29] P. Selinger and B. Valiron (2006) *A lambda calculus for quantum computation with classical control*. Mathematical Structures in Computer Science 16(3):527–552.

[30] P. Selinger and B. Valiron (2008) *A linear-non-linear model for a computational call-by-value lambda calculus*. Extended Abstract. In Proceedings of the Eleventh International Conference on Foundations of Software Science and Computation Structures (FOSSACS 2008), Budapest, Springer LNCS 4962, pp. 81–96. `http://www.mscs.dal.ca/∼selinger/papers.html`

[31] P. Selinger and B. Valiron (2008) *On a fully abstract model for a quantum linear functional language*. Extended Abstract, with Benoit Valiron. In Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006), Oxford. ENTCS 210:123–137.

[32] D. Shepherd and M. J. Bremner (2008) *Temporally Unstructured Quantum Computation*. To appear in Proc. Roy. Soc. (Lond.) A. `arXiv:0809.0847`.

[33] B. Valiron's Ph.D. Thesis. Advisor: Peter Selinger (McGi) (2008) *Semantics for a Higher Order Functional Programming Language for Quantum Computation*. University of Ottawa.

[34] P. Van Loock, W. J. Munro, K. Nemoto, T. P. Spiller, T. D. Ladd, S. L. Braunstein and G. J. Milburn (2008) *Hybrid quantum computation in quantum optics*, Physical Review A 78, 022303-1/5.

[35] H. Vogts and R. Werner (2006) *Index Theory for One-dimensional Reversible Quantum Walks and Quantum Cellular Automata*. Draft paper.

[36] K. Wiesner (2008) *Quantum Cellular Automata*. To appear in Springer Encyclopedia of Complexity and Systems Science. `arXiv:0808.0679`

Part IV

Consortium management

Meetings of the consortium management group

'Physical' meetings held in 2008:

- Paris, France, March 3, 2008, after the first QICS review meeting. We considered the very positive feedback by the reviewers and were obviously very happy with that. We studies the research reported on and discussed together what the next step to take are. We discussed the Obsergurgl conference that was going to take place in September, what the format should be, who the invited speakers should be, etc.
- Grenoble, France, April 5, 2008, at the 2nd QICS workshop. An issues which we discussed was the retirement of Philippe Jorrand, who headed W4. It was decided that W4 would still be based in Grenoble, now headed jointly by Mehdi Mhalla and Pablo Arrighi. Directions of research where also discussed. We also discussed the future of the Paris site after Vincent Danos obtained a Chair at Edinburgh. Since he still retains his CNRS position we opted to retain the Paris site and adjoin Edinburgh as an affiliated site to it.
- Obergurgl, Innsbruck, September 18, 2009, at the first QICS confrence. A first issue we discussed was the faith of the Braunschweig site given that Reinhard Werner and his group will move to Hannover. The plan is to move the QICS site with him. We also discussed: "What after QICS?" Due to the success of the QICS endeavour many partners are of the opinion that this interdisciplinary effort should continue after the QICS STREP ends.

'Conference call' meetings held in 2008:

- The discussion on "What after QICS?" has continued in terms of conference calls and is still ongoing.

Project timetable and status

These are reported on in the introduction to each of the workpackges i.e. Chapters 5–8.

Annex:
Plan for using and disseminating the knowledge

Does not apply to us given the purely theoretical nature of our research.