QICS - PERIODIC ACTIVITY REPORT I

Bob Coecke

Chancellor, Masters and Scholars of the University of Oxford

FP6 FET STREP - project no 033763

Full name: Foundational Structures for Quantum Information and Computation

Thematic priority: Quantum Information Processing and Communications

Period covered: Jan. 1st 2007 – Dec. 31 2007

Date of preparation: Feb. 15th 2008

Start date of project: Jan. 1st 2007

Duration: 36 months

Contents

I Publishable executive summary 3

II Project objectives and major achievements during the reporting peroid 7

1 Objectives, work done, comparison to state-of-the-art and other developments 8
1.1 Objectives of QICS as stated in the initial proposal . . . 8
1.2 Objectives for the workpackages as stated in the initial proposal . . . 10
1.3 Comparison of these objectives to the current state-of-the-art . . . 11
1.4 Progress made on the objectives during the reporting period . . . 11
1.5 Next steps to be taken for reaching the objectives . . . 11

2 Interaction between scientific communities 12
2.1 Interaction between workpackages and sites . . . 12
2.2 Trans-disciplinary efforts . . . 12

3 Recruitment and mobility 13
3.1 Recruitment . . . 13
3.2 Mobility via recruitment . . . 13
3.3 Visits between sites . . . 13

4 QICS events and presentations 14
4.1 QICS events . . . 14
4.2 Major QICS related/suported events . . . 14
4.3 Presentation of QICS output . . . 15

III Workpackage progress reports of the period
***— includes project deliverables —* 17**

5 W1 – *deliverable D1*: Structures and methods for measurement-based quantum computation 19
5.1 Progress towards objectives and performed tasks for W1.T1. . . . 21
5.1.1 Computational universality of resource states for measurement-based quantum computation . . . 21
5.1.2 Computational and algorithmic complexity of quantum computation . . . 22
5.1.3 Mathematical properties of graph states . . . 22
5.1.4 General properties for measurement based quantum computing . . . 22
5.1.5 Quantum machines and measurement based quantum computing . . . 23
5.2 Progress towards objectives and performed tasks for W1.T2 . . . 23
5.2.1 Resources for measurement-based quantum computing . . . 23
5.2.2 General properties of graph states . . . 24
5.3 Progress towards objectives and performed tasks for W1.T3 . . . 24
5.3.1 Calculi for one-way computing . . . 24
5.3.2 Graphical calculus and categorical semantics for measurement based quantum computing . . . 25
5.3.3 Automated reasoning tools for measurement based quantum computing . . . 25

6 W2 – *deliverable D2*: Categorical semantics, logics and diagrammatic methods 28
6.1 Progress towards objectives and performed tasks for W2.T1 . . . 30

6.1.1 Categorical models . . . 32
6.2 Progress towards objectives and performed tasks for W2.T2 . . . 33
6.2.1 Graphical calculus for multipartite entanglement . . . 33
6.2.2 General results on entanglement . . . 33
6.2.3 Distributed quantum computing . . . 33
6.3 Progress towards objectives and performed tasks for W2.T3 . . . 34

7 W3 – *deliverable D3*: Classical-quantum interaction and information flow 36
7.1 Progress towards objectives and performed tasks for W3.T1 . . . 38
7.1.1 Progress on the resource calculus . . . 38
7.1.2 General results on quantum informatic resources . . . 38
7.2 Progress towards objectives and performed tasks for W3.T2 . . . 39
7.2.1 Compositional accounts on information flow . . . 39
7.2.2 Information flow on one-way computing . . . 40
7.2.3 Foundational results on the classical-quantum data (processing) relation . . . 40
7.2.4 Classical limit . . . 40
7.2.5 Coalgebraic structures . . . 40

8 W4 – *deliverable D4*: Quantum automata, machines and calculi 44
8.1 Progress towards objectives and performed tasks for W4.T1 . . . 47
8.2 Progress towards objectives and performed tasks for W4.T2 . . . 48
8.3 Progress towards objectives and performed tasks for W4.T3 . . . 49
8.3.1 Quantum calculi . . . 49
8.3.2 Quantum semantics . . . 49
8.3.3 Quantum languages . . . 50
8.3.4 Logic within quantum computational models . . . 50
8.4 Progress towards objectives and performed tasks for W4.T4 . . . 51
8.4.1 Quantum process calculi. . . . 51
8.4.2 Reasoning about knowledge in quantum protocols . . . 51
8.4.3 Tools for verification . . . 51

IV Consortium management 55

Part I

Publishable executive summary

An exciting and promising first 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 first 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 Paris.

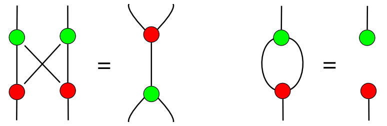
The first round of QICS hiring involved many permutations between these groups, resulting in successful interactions e.g. computer science methods and structures have now been successfully applied to measurement based quantum computational models – we discuss this in more detail below.

The workpackage on *structures and methods for measurement-based quantum computation* [**W1**] addressed fundamental questions, for example, on the relation of the entanglement of the resource state with the computational power of the scheme, which were still largely unanswered. More specifically, which resource states beyond the cluster state would allow universal quantum computation and which entanglement features would be responsible for that? And, which resource states would give no advantages over classical computation at all? This endeavour was highly successful. It has resulted in a much better understanding of graph states, a key resource for measurement based quantum computing, and exposed their scope for application. There is also a number of intriguing new applications and developments of graph state methods in statistical physics: problems involving statistical mechanics of classical spin systems, can be related to problems in quantum physics, relating a large class of classical spin models to quantum stabelizer states. Substantial progress has also been made on the clarification of which features of multi-partite entanglement are responsible for universality of resources in measurement based quantum computing. A detailed discussion of these results is in [**W1**]. We also witnessed the developments of high level calculi for measurement based quantum computing which now makes them subject to the activity in [**W4**]. Finally, adequate categorical structures have been crafted to reason, both diagrammatically and automated, about a variety of schemes and resources for measurement based quantum computing.

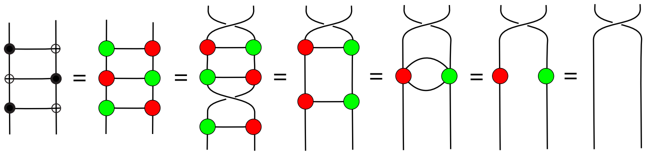
This brings us to the second workpackage, on *categorical semantics, logics and diagrammatic methods* [**W2**]. The main task for this year was to craft the appropriate structures to address problems in workpackage 1 on measurement based quantum computing and workpackage 3 on information flow in quantum informatics. This resulted in a both axiomatic, diagrammatic, and logical (cf. automation) account on:

1. classical vs. quantum data, crucial for the applications in measurement-based quantum computational models which require classically controlled correction operations;

2. complementary observables, which enables abstract simulation of elementary gate computations; the key axioms of this structure are the well-known bialgebra equation and a (degenerated) Hopf law:

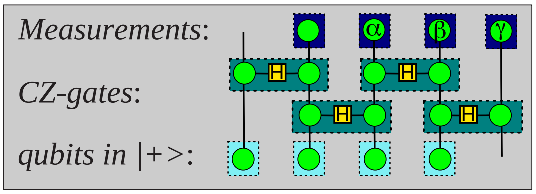


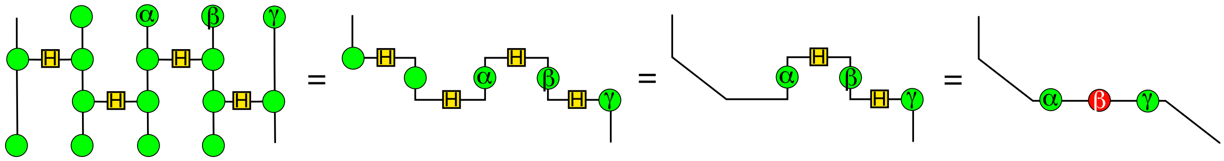
which provides enough structural power for typical circuit computations:



3. all gates and multipartite entangled states of the Hilbert-space formalism in high-level terms, providing us with all the expressive power the full-blown Hilbert space quantum formalism.

Parts **2.** and **3.** together to verify measurement based quantum computational schemes e.g. realisation of arbitrary one-qubit unitaries in no more than three rewrites:





Other notable results in this workpackage are several concrete new categorical models which capture particular features of quantum informatics and important steps toward a categorical axiomatics for topological quantum computing. Details can be found in [**W2**].

The workpackage on *classical-quantum interaction and information flow* [**W3**] has as its main goal to delineate a notion of quantum information flow when quantum and classical systems are interacting. As compared to the purely classical counterpart to this, the situation is of course far more complicated here given that besides the flows between the quantum and the classical there are also the flows within the quantum itself subject to entanglement. In this workpackage we try to approach this involved problem from several angles.

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

- *Quantum data processing*. Here several results were obtained and a key fundamental issue of quantum computation viz. the relationship of classical to quantum computational complexity, and the characterisation of ways in which the latter is an extension of the former.

- *Categorical operational semantics*. Here it was shown that only a tiny bit of structure, namely abstract counterparts to copying and uniform erasing, turns out to be sufficient to extract from an abstract family of quantum processes, a variety of classical processes such as reversible classical processes, deterministic- and non-deterministic processes, stochastic processes and even informatic order in terms of majorisation. We were also able to prove the no-cloning theorem based on purely topological (cf. information flow) principles.

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

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, some of which are:

- a classically-controlled Turing machine which is significantly simpler than Deutsch's quantum Turing machine and which can be specialized into a pure measurement-based quantum Turing machine;
- a universal one-dimensional quantum cellular automata (QCA) capable of simulating all others has been described, and it has been proved that one-dimensional QCA always admit a two layered block representation and that their inverse is also a QCA; this last result came as a major surprise, since such a property does not hold for classical CA; a proof that every QCA can be put in the form of a tiling of more elementary, finite dimensional unitary evolutions, has also led to a most welcome, clear and robust definition of n-dimensional QCA, phrased in the traditional setting of Hilbert spaces;
- a language QML, has the significant advantage of a semantic domain directly built upon quantum objects and operations, but is restricted to first order; a translator from QML to quantum gate networks has recently been implemented;
- a hierarchy of denotational semantics have been defined for a simple quantum imperative language; remarkable progress in the study of semantics for languages giving access to quantum resources has been made by relying upon the abstract setting of dagger compact categories with biproducts.

Several other results on abstract models can be found in [**W4**]. In addition, a connection has been established between measurement-based quantum computations with graph states and the field of mathematical logic, showing that the computational power of graph states is reflected in the expressive power of classical formal logic languages defined on the underlying mathematical graphs, bringing us back to workpackage 1, thus closing the circle.

Bob Coecke, Oxford, February 10, 2008.

`coecke@comlab.ox.ac.uk`

Computing Laboratory
University of Oxford
OX1 3QD Oxford
United Kingdom

References

W1 H.-J. Briegel (2008) Introduction to QICS deliverable D1 for the workpackage *Structures and methods for measurement-based quantum computation*. `Click here here for download.`

W2 S. Abramsky and B. Coecke (2008) Introduction to QICS deliverable D2 for the workpackage *Categorical semantics, logics and diagrammatic methods*. `Click here here for download.`

W3 B. Coecke and R. Jozsa (2008) Introduction to QICS deliverable D3 for the workpackage *Classical-quantum interaction and information flow*. `Click here here for download.`

W4 P. Jorrand (2008) Introduction to QICS deliverable D4 for the workpackage *Quantum automata, machines and calculi*. `Click here here for download.`

Q S. Abramsky, S. L. Braunstein, H.-J. Briegel, B. Coecke, V. Danos, P. Jorrand, R. Jozsa, P. Panangaden and R. F. Werner (2006) *Foundational Structures for Quantum Information and Computation.* Specific Targeted Research Project within the 6th Framework Program of the European Commission, Jan 1st 2007 – Dec 31st 2009, within the Future and Emerging Technologies Open Scheme. `Click here here for download.`

Part II

Project objectives and major achievements during the reporting peroid

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 paragraph entitled **“A current account of the objectives of Wx and comparison with the state-of-the art.”** in the introduction to each of the workpackges i.e. Chapters 5–8.

1.4 Progress made on the objectives during the reporting period

Please see the paragraph entitled **“Main developments in Wx.”** in the introduction to each of the workpackges i.e. Chapters 5–8. Some of the tasks had to be permuted and slightly delayed in time due to the difficulty of finding appropriate postdocs. Meanwhile, at each site, we are happy to report that all necessary current and future appointments are in place for reaching all objectives by the end of the duration of the project. At several sites QICS postdocs are already active *in parallel* to meet our goals. This strategy does require all the funds which were allocated to qics for the whole period. On this issue please also see Chapter 3 called **“Recruitment and mobility.”** and Part IV on **“Consortium management.”**

1.5 Next steps to be taken for reaching the objectives

Please see the paragraph entitled **“The next steps to take.”** in the introduction to each of the workpackges i.e. Chapters 5–8. On the issue of hiring appropriate QICS postdocs see Section 1.4 above, Chapter 3 called **“Recruitment and mobility.”** and Part IV on **“Consortium management.”**

Chapter 2

Interaction between scientific communities

2.1 Interaction between workpackages and sites

For more details please see the paragraph entitled **"Interactions with other workpackages and sites."** in the introduction to each of the workpackges i.e. Chapters 5–8 and the detailed accounts on the activity in those chapters. See also Chapter 3 called **"Recruitment and mobility."** on how several members have been permuted between sites, including the QICS postdocs.

2.2 Trans-disciplinary efforts

To cope with the different backgrounds involved in QICS several initiatives have been taken to bridge the gaps. Firstly, the logicians and computer scientists have compiled several volumes of introductory chapters on the structures and methods we use, mainly aimed at physicist, which will appear this summer. There are two projects of this nature, respectively coordinated by Coecke (Ox), and Gay (Ox affiliated) and Mackie (Ox affiliated). Both will consists of many chapters mostly written by QICS members. These projects are:

- B. Coecke, Ed. (2008) *New Structures for Physics I: tutorials*; *New Structures for Physics II: methods*; *New Structures for Physics III: approaches*. Springer Lecture Notes in Physics.
- S. Gay and I. Mackie (2008) *Semantic Techniques in Quantum Computation*. Cambridge University Press.

Some of the chapters for these volumes can be found in the references to Chapters 5–8. There were also several events which served this more didactical purpose:

- Pre-empting QICS in the summer of 2006, the event `Cats, Kets and Cloisters (click)` included many tutorials by QICS members directed to QICS members. All QICS groups were very well represented and presented the research at their respective sites. The event was attended by approximately 120 researchers. It was unique in terms of the exceptionally broad range of backgrounds of the participants.
- Obviously the QICS events themselves have a strong tutorial component. These QICS events and other QICS related events are in Chapter 4 called **"Academic events and activity."**
- Several visits between sites involved tutorials, for example, Coecke's (Oxford) visit to Braunschweig, a site mainly consisting of physicists, involved a three hour tutorial on categorical axiomatics for quantum physics. Please see also Chapter 3 called **"Recruitment and mobility."** which lists the visits between sites and Chapter 4 called **"Academic events and activity."** which lists events in which QICS members participated, in particular, of course, the **QICS events** themselves.

We intend to continue this educational aspect of QICS. In particular, our first official big event, hosted by the Innsbruck site, will have a very strong tutorial purpose.

Chapter 3

Recruitment and mobility

3.1 Recruitment

As already mentioned above initially we had some difficulties to find available appropriately skilled researchers. This is of course a consequence of the nature of QICS research which is highly specialised; in particular at the logic and computer science end. Meanwhile, also with the growth of the researchers active in the area, all necessary current and future appointments are in place for reaching all objectives by the end of the duration of the project. As already mentioned above, at several sites QICS postdocs are already active *in parallel* to meet our goals. And we repeat again that this strategy does require all the funds which were allocated to QICS for the whole period. On this issue please also see Part IV in **"Consortium management."** One important unexpected recruitment in Oxford is that of a specialist of *adiabatic quantum computing* who became available after leaving D-wave systems (due to his discomfort with the company's PR attitude). Adiabatic quantum computing is a very important quantum computational model, which we mentioned in the QICS abstract, but didn't specify in the objectives since we weren't sure that it would be possible to recruit anyone who would match the QICS requirements.

3.2 Mobility via recruitment

This activity is probably the most compelling token of the interaction between sites in QICS. Many of the QICS postdocs hired at one site have been active in the past in another site. Here are some examples of paths of QICS researchers between sites

- Hines: Oxford ⇝ York; Gratage: Oxford ⇝ Grenoble; Perdrix: Grenoble ⇝ Paris ⇝ Oxford; Nesme: Paris ⇝ Braunschweig; Kashefi: Oxford ⇝ Grenoble; Sadrzadeh: Oxford ⇝ Paris.

Some expected forthcoming ones are:

- Sadrzadeh: Paris ⇝ Oxford; Paquette: McGill ⇝ Ox; Blute: McGill ⇝ Ox.

3.3 Visits between sites

The following list (not complete and in particular excludes QICS events hosted at sites and visits between subsites) clearly witnesses the collaboration between sites:

- Jozsa (Bristol) visited Oxford for two weeks in March'07; Montanaro (Bristol) visted Innsbruck for one week in April'07; Bremner (Bristol) visited Oxford-sub UCL in October'07; Ahlbrecht (Braunschweig) visited Bristol in June'07, Coecke (Ox) Visited Braunschweig in October'07; Abramsky and Coecke (Oxford) visited Paris at several occasions; Coecke (Oxford) visited Bristol in July'07; Coecke (Oxford) visited York in December'06; Blute, Panangaden, Paquette and Scott (McGill) visited Oxford at several occasions; Koslowski (Braunschweig) visited Oxford in July'07; Werner (Braunschweig) visited Innsbruck in March'07; Browne (Oxford) visited Innsbruck at several occasions; Yoran (Bristol) visited Innsbruck in November'07; Popescu (Bristol) visited Innsbruck in January'08; Briegel (Innsbruck) visited Bristol in June'07; Miyake (Innsbruck) visited Bristol in January'088; Miyake (Innsbruck) visited Oxford in January 2008; Arrighi (Grenoble) visited Braunschweig in October'07; Nesme (Braunschweig) visited Grenoble in January'08; Perdrix (Oxford) visited Grenoble at several occasions; Grattage (Oxford) visited Grenoble in June '07; Markham (Paris) visited Grenoble in January'08; Short (Bristol) visited Innsbruck in January'07; Browne (Oxford) visited Innsbruck in January'07; Kashefi (Grenoble) visited Oxford-sub Glasgow in January'08; Sadrzadeh (Paris) visited Oxford at several occasions; Prost (Grenoble) visited Oxford in January'08; . . .

Chapter 4

QICS events and presentations

4.1 QICS events

- 1st QICS workshop, Oxford, March 15-17, 2007 (`click`)
- 2nd QICS workshop, Grenoble, April 5-7, 2008 (`click`)
- The first QICS conference will take place in Obergurgl, Austria, September 14-20, 2008.

4.2 Major QICS related/suported events

The event

- Cats, Kets and Cloisters, Oxford, July 17-23, 2006 (`click`)

and in particular its strongly QICS-related tutorial character is discussed in Section 2.2. The British QICS sites are all part of an EPSRC network called Semantics for Quantum Computing (QNET) which also holds annual events, mainly on the topics of workpackages 2 and 4. These workshops are:

- 1st QNET workshop, Glasgow, December 4-5, 2006 (`click`)
- 2nd QNET workshop, Royal Society, London, December 10-11, 2007 (`click`)

A workshop devoted to workpackage 1 organised by Browne (Oxford) is:

- 1st International Workshop on Measurement Based Quantum Computing, Oxford, March 18-21, 2007 (`click`)

There were also many smaller workshops and seminar series including many QICS members. Some examples are:

- A by now four year running 1-day workshops series QUOXIC addressing topics within the whole of the QICS project; there have been about 25 of these; they were initially organised by Kashefi (then Oxford now Grenoble), then by Browne (then Oxford now Oxford affiliate at UCL), and now by Duncan (QICS postdoc at Oxford). (`click`)
- A 1-day series entitled Categories, Logic and the Foundations of Physics addressing topics in workpackage 2 and workpackage 3 of QICS in the Loxbridge area; the first event of these attracted some 70 participants; it is coordinated by Coecke (Oxford) (`click`)
- Grenoble hosts regular small workshops involving several QICS members (`click`)
- Coecke (Oxford) and Panangaden (McGill) co-chair the Joint 5th Quantum Physics and Logic (QPL) and 4th Development of Computational Models (DCM) Workshops, July 12-13, 2008, Reykjavik, Iceland. (`click`)
- Panangaden (McGill) organises every year a one-week workshop at Bellairs Research Institute in Barbados (which is owned by McGill University) on topics in all QICS workpackages (`click`)
- Most QICS sites have their own weekly seminar(s) which regularly involve speakers of other QICS sites.

4.3 Presentation of QICS output

There are far too many presentations of QICS output by QICS members to be able to give a comprehensive overview; they cover a wide range of venues and disciplines. We do mention some noteworthy ones as a token. QICS members had several contributions to the annual Quantum Information Processing conference:

- At QIP'07 Winter (Bris) gave an invited talk, Harrow (Bris) had an accepted talk, Popescu (Bris) had an accepted talk, and Montanaro (QICS postdoc at Bris) presented an accepted poster. At QIP'08 Hayden (McGi) gave an invited talk, Winter (Bris) had an accepted talk, Browne (Oxford) had two accepted talks of which one jointly with Perdrix (QICS postdoc at Ox, who gave the talk), Kashefi (Grenoble) and Mhalla (Grenoble), and one jointly with Miyake (QICS postdoc at Inns) and Short (Inns), Winter (Bris) and Harrow (Bris) also both had two accepted talks of which one jointly with Montanaro (QICS postdoc at Bris), and Montanaro (QICS postdoc at Bris) presented an accepted poster.

We also list some of the invited talks by some of the QICS members, chosen to indicate the variety of platforms QICS members are able to disseminate the QICS output:

- **Some invited talks** by Abramsky (Ox):
  - Computer Journal Lecture, British Computing Society (BCS), June 2007.
  - Lecture on receipt of Test-of-Time award, IEEE confrence on Logic in Computer Science (LiCS'07), Wroclaw, July 2007.
  - EACSL Conference on Computer Science Logic, Lausanne, September 2007.
- **Invited talks** by Browne (Oxford):
  - The Principles and Applications of Control in Quantum Systems, Sydney, July 2007.
  - Applied Quantum Measurement, Leiden, Netherlands, November 2007.
- **Some invited talks** by Briegel (Inns):
  - Interfaces between Physics and Computer Science (Summer School), Bremen, June 2007.
  - Gordon Research Conference on Quantum Information Science, Il Ciocco, Barga, Italy, April 2007.
  - Workshop in Quantum Algorithms and Applications (QAA07), Sydney, May 2007.
- **Some invited talks** by Coecke (Ox):
  - Category Theory 2007 (CT'07), Carvoeiro, Portugal, June 2007.
  - Deep Beauty: A Conference in Honour of von Neumann's Contributions to the Mathematical Foundations of Physics, Princeton University, October 2007.
  - Structure and Identity, Royal Academy, Brussels, December 2007.
- **Invited talks** by Duer (Inns):
  - Beneasque conference on Quantum Information, Benasque, Spain, June 2007.
  - Workshop on Quantum Information and Many-Body Quantum Systems, Pisa, Italy, March 2007.
- **Invited talk** by Jorrand (Grenoble):
  - Computing Frontiers, Ischia, Italy, May 2007.
- **Some invited talks** by Jozsa (Bris):
  - Workshop on Weak Values and Weak Measurements, Arizona State University, June 2007.
  - Measurement Based Quantum Computing Conference, St John's College, Oxford University, March 2007.
  - Departmental Seminar of the Department of Mathematics of the University of York, June 2007.
- **Invited talk** by Hines (QICS postdoc at York):
  - Mathematical Foundations of Programming Semantics, New Orleans, April 2007.

- **Invited talks** by Miyake (QICS postdoc at Inns):
  - Young Researchers Conference, the Perimeter Institute, Waterloo, Canada, December 2007.
  - Third CREST workshop on quantum information, Okinawa, Japan, August 2007.
- **Invited talks** by Sadrzadeh (QICS postdoc at Paris):
  - Computational Logic seminar, University of St. Andrews, December 2007.
  - Workshop on Logic, Physics and Quantum Information Theory, Barbados, March 2008.

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 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/QICSdeliverable1_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable2_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable3_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable4_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. We also report the results which were obtained before the actual start of the project, that is in the period March 2006 – January 2007, in the case that they contribute to the objectives as stated in the proposal draft which dates from March 2006.

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 5

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. When the project started, measurement-based quantum computation (MQC) was already an established scheme for quantum computation in the sense that a worked-out "manual" e.g. for one-way computation (as well as other schemes of MQC), existed and was well understood. This allowed one to e.g. translate any quantum logic circuit into a measurement pattern and a set of rules how to process the classical measurement outcomes. Furthermore, the fault-tolerance of the scheme had already been proven, even though the threshold has been improved significantly in the meantime. [see e.g. work by Raussendorf et al. PRL 98, 190504 (2007)]. The latter point is, for example, in clear contrast with the current status of quantum adiabatic computation, another hot topic in computational models, where the possible application of quantum error correction has yet to be clarified.

However, fundamental questions, e.g. about the relation of the entanglement of the resource state with the computational power of the scheme, were still largely unanswered. Which resource states beyond the cluster state would be allow universal quantum computation and which entanglement features would be responsible for that? Which resource states would give no advantages over classical computation at all? One of the **milestones** of the first year, W1.M2, was devoted for this question, and W1 has made significant progress on this line and can report very satisfactory outcomes.

Progress in the understanding of MQC has been reported by a number of other international research teams. For example, the possibility of MQC on tensor network states, in particular the matrix product states which were originally developed in condensed matter physics, has been explored and extended in Gross et al. [PRL 98, 220503 (2007), PRA 76, 052315 (2007)] (see also work by Verstraete et al. [PRL 96, 220601 (2006).]). Along with recent progress in classical simulation techniques (to which W1 is also contributing, for instance, through **5.1.2.a** and **5.3.1.c**), these works will stimulate research in condensed matter physics further, providing new perspectives on the computational complexity of (ground or low energy) states available in condensed matter systems and their usage for MQC.

One of research trends that can be observed is to relax conditions required to perform MQC beyond the original model on the cluster state. Such research will be important to facilitate physical implementations, and W1 fertilizes this trend.

Another trend that can be observed is the increasing study of graph states, both in experimental and in theoretical work also beyond their immediate application in MQC. This is also the topic of **milestone** W1.M1. It is quite remarkable that, because of their wide-spread applications in quantum information processing also beyond MQC (e.g. quantum communication and quantum error correction), the graph states seem to have become a standard target in experiments to produce multipartite entanglement, and to test the non-locality of quantum mechanics in terms of Bell inequalities, for instance. In 2007, we have witnessed remarkable experimental progress in creating cluster and graph states with photons and implementing basic one-way quantum computation schemes. We can only mention here the great works by the groups of Zeilinger [Nature 445, 6569 (2007)], De Martini [PRL 98, 180502 (2007); quant-ph/0712.1889], and Pan [PRL 99, 120503 (2007); Nature Physics 3, 9195 (2007)], In the last cited work by Pan et al. a 6-qubit graph state has been produced for the first time.

On the theory side, extending the properties of graph state bases, nonadditive quantum codes, which can provide a better performance compared to the additive (stabilizer) codes, became an emerging hot topic in QIP2008 (cf. Yu et al., arXiv:0704.2122; Cross et al., arXiv:0708.1021). Moreover, the correlation inherited in the graph states turned out to be useful to simulate other quantum systems following the original idea of Feynman. For eample, a graph state with a small number number of qubits was proposed in Han et al. [Phys. Rev. Lett. 98, 150404 (2007)] to simulate the exotic statistics of anyons, which appear originally as quasi-particles in the two-dimensional quantum system. Accordingly, in the year 2007, two experimental groups, the Pan group (arXiv:0710.0278) and the Weinfurter group (arXiv:0710.0895), report observation of anyonic interference for the first time.

These developments clearly demonstrate the ongoing international research activities in the wider context of W1. In the following, we summarize the main developments and results achieved within by the QICS consortium in the year 2007.

Main developments in W1. W1 has so far been a great success, and we have delivered 29 original papers in the first year. Milestones W1.M1 and W1.M2, which were planned to be completed during the first year, have been fully accomplished. Furthermore, we are already witnessing promising developments towards the accomplishment of other milestones, planned to be met during the second and the third year.

The milestone W1.M1 was to establish a deeper understanding of graph states and the scope of their applications, reflecting also the broad interest in these states in the wider community, as mentioned in the general overview. To this end, we can report a variety of exciting developments as listed in **5.1.3**, **5.2.1.a**, **5.2.1.c**, **5.2.2** and explained more detail below. Furthermore, we are quite intrigued by a new application or spin-off of graph state methods in statistical mechanics, as reported in **5.2.1.b**.

The milestone W1.M2 was to clarify the fundamental question which features of multi-partite entanglement are responsible for universality of resources in MQC. We think that we have made full progress here, as well, and milestone W1.M2 has been fully achieved by **5.1.1.a**, **5.1.1.b**, **5.1.4.a**, and **5.2.1.d**.

There has also been ongoing progress that will be relevant for the future milestones, as described e.g. in **5.3**, which should play a key role toward W1.M3 for the year 2008, and in **5.2.1.e** which should pave the road toward W1.M5.

The next steps to take. Encouraged by the success in the first year, we like to carry on our research activities according to our proposal.

Interactions with other workpackages and sites. Even though large parts of the current milestones of W1, have so-far been achieved ”autonomously”, there are a number of fruitful connections with other workpackages. For example, W1 benefits from the categorical semantics of the W2 through **5.3.2**, and from the quantum Turing machine model of the W4 through **5.1.5**. The topic of the W1 is being elaborated into an intuitive diagrammatic form in **6.1.d**, **6.1.e**, and **6.2.1.a** of the W2. An idea of the information flow considered in the one-way model has been quite helpful in studying a rewriting system that translates back and forth between MQC and the circuit model, as seen in **7.2.2** of the W3. Finally, research on classical simulatability of quantum computation, listed in **7.2.3**, is closely connected the objectives of to W1 and will be relevant for W1.M6.

Last but not least, the question of universality of graph state resources is connected to the (un-)decidability of logic theories on the underlying mathematical graphs – both of which seem to express different aspects of the (complexity of the) quantum correlations of the resource. See **8.3.4.a** of W4.

We expect that interactions among different workpackages are going to be further enhanced by an upcoming QICS workshop with international experts working on measurement-based quantum computation, logic and calculi, quantum foundations, and other topics, which is to be held in Obergurgl (near Innsbruck, Austria) in Fall 2008.

Hans-Jurgen Briegel
Innsbruck, February 10, 2008.

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.

5.1 Progress towards objectives and performed tasks for W1.T1.

5.1.1 Computational universality of resource states for measurement-based quantum computation

5.1.1.a Universal entanglement resources for measurement-based quantum computation (Objectives: W1.O1, W1.O3, W1.O4; Milestones: W1.M1, W1.M2). In [1], Van den Nest (Inn), Miyake (QICS postdoc at Inn), Duer (Inn), and Briegel (Inn) have initiated our study of novel resources and schemes for measurement-based quantum computation (MQC). The aim of the work is not only to identify new models and schemes for MQC, but also to better understand the fundamental principles and power of quantum computation. MQC is particularly suited for such studies, as the resource character of entanglement is highlighted. We have analyzed the fundamental requirements for universality, i.e. we have studied the (entanglement) properties resource states need to possess such that that they give rise to a universal resource for MQC in the sense that any quantum state can be prepared by means of local measurements only. This allowed us to derive necessary conditions for universality based on various entanglement measures, and to show that large classes of otherwise highly entangled states (such as GHZ states, W states or 1D cluster states) are not universal for MQC.

In [2], Van den Nest (Inn), Duer (Inn), Miyake (QICS postdoc at Inn), and Briegel (Inn) have extended and deepened these studies, where we also take efficiency of the computation into account. This leads us to the result that entanglement measures need not only obtain their maximum value on universal resource states, but also have to obey a certain scaling law with system size. In addition, there we also consider the possibility of encodings, i.e. of obtaining the desired output state in an encoded form, and analyze the corresponding entanglement-based criteria. Furthermore, we have identified several other lattice structures, e.g. Triangular or Hexagonal lattices, and general families of (encoded) states as being universal resources for MQC. This might also be of practical relevance with respect to experiments, as the generation of certain types of states could be simpler than the generation of the 2D cluster state. Some of these states may also show a higher robustness against noise and decoherence, as is e.g. the case with graph states corresponding to Hexagonal lattices.

5.1.1.b Phase transition of computational power of measurement-based quantum computer (Objectives: W1.O1, W1.O3; Milestones: W1.M1, W1.M6). In [3], Browne (Ox), Miyake (QICS postdoc at Inn) and their colleagues have tackled a fundamental question on the origin of computational superior power of quantum computer. We considered a simplified model, motivated by the optical lattice implementation of measurement-based quantum computer, and studied 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 we 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, we show that measurement-based quantum computation on the faulty lattice allows an efficient simulation by classical computers. We observe a phase transition at the threshold when the amount of entanglement in the faulty lattice directly relevant to the computational power changes exponentially.

5.1.1.c KLM-quantum computing as measurement-based quantum computing (Objectives: W1.O1, W1.O2, W1.O4, W4.O2; Milestones: W1.M1, W1.M5). In [4] Popescu (Bris) shows that the Knill Laflamme Milburn method of quantum computation with linear optics gates can be interpreted as a one-way, measurement based quantum computation of the type introduced by Briegel and Rausendorf. He also shows that the permanent state of n n-dimensional systems is a universal state for quantum computation. In [5] Popescu (Bris) suggests a Knill-Laflamme-Milburn (KLM) type quantum computation with bosonic neutral atoms or bosonic ions. Crucially, as opposite to other quantum computation schemes involving atoms (ions), no controlled interactions between atoms (ions) involving their internal levels are required. Versus photonic KLM computation this scheme has the advantage that single atom (ion) sources are more natural than single photon sources, and single atom (ion) detectors are far more efficient than single photon ones.

5.1.2 Computational and algorithmic complexity of quantum computation

5.1.2.a Classical simulation of measurement-based quantum computation (Objectives: W1.O1, W1.O3, W1.O4; Milestones: W1.M1, W1.M2, W1.M6). In [6], Van den Nest (Inn), Duer (Inn), and Briegel (Inn), in collaboration with Vidal, concentrate more on the possibility of classically simulating certain kinds of quantum computation, and in fact derive entanglement-based criteria when this is possible. For graph states, so-called entanglement-width measures are used, and we provide an explicit classical simulation protocol for any measurement-based computation on graph states with logarithmically bounded width-measure. This includes e.g. all tree graphs such as 1D cluster states as well as GHZ states. This complements the research on universality of states reported above, as we in fact find that in this case the criteria for classical simulatability based on the width-measures coincides with the finding that the states are not universal resources for MQC.

5.1.2.b Noisy quantum simulation for quantum computation (Objectives: W1.O3; Milestones: W1.M1, W1.M6). In [7], Duer (Inn), Bremner(QICS postdoc at Bris), and Briegel (Inn) described in particular the error analysis in the context of quantum simulation, which is also of relevance for the investigation of quantum computational schemes. On the one hand, the methods to generate many-body interaction Hamiltonian we introduce there automatically lead to many-body gates, as these gates simply correspond to an evolution of the system with respect to the generated Hamiltonian for some fixed time. Furthermore, the error analysis also applies to gates generated in this way, and the methods for noise reduction (e.g. entanglement purification) can be applied.

5.1.2.c Quantum Kolmogorov complexity (Objectives: W1.O1, W1.O3; Milestones: W1.M1, W1.M6). In [8], Mora (Inn), Briegel (Inn), and Kraus (Inn) have further investigated the notion of quantum Kolmogorov complexity, a measure of the information required to describe a quantum state, which we introduced in an earlier work. We have shown that, for any definition of a quantum Kolmogorov complexity that measures the number of classical bits required to describe a pure quantum state, there exists a pure n-qubit state whose description requires exponentially many classical bits. Furthermore, we illustrated how the notion of quantum Kolmogorov complexity can be used to prove statements in fields, such as quantum communication, quantum computation and thermodynamics. For instance, we derived conditions under which a quantum algorithm cannot have an exponential speed-up compared to a classical algorithm.

5.1.3 Mathematical properties of graph states

5.1.3.a Graph states as ground states of many-body Hamiltonians (Objective: W1.O3, W1.O4; Milestones: W1.M1). In [9], 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 we 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.

5.1.3.b LU-LC conjecture in graph states (Objectives: W1.O3, W1.O4; Milestones: W1.M1, W1.M6). In [10] Gross and Van den Nest (Inn) 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.

We also note that the theoretical results of [10] were subsequently used by Ji et al. (arXiv:0709.1266) to completely resolve the LU-LC conjecture; these authors use the results of [10] to generate a counter example, showing that the conjecture is false.

5.1.4 General properties for measurement based quantum computing

5.1.4.a Determinism in the one-way model (Objectives: W1.O2, W1.O3; Milestones: W1.M6). In [11], Browne (Ox), Kashefi (Ox & Gren), Mhalla (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox) extend the notion of quantum information flow defined by Danos (Paris) and Kashefi (Ox & Gren) for the one-way model and present a necessary and sufficient condition for the deterministic computation in this model. They apply both measurement calculus and the stabiliser formalism to derive the main theorem which for the first time gives a full characterization of deterministic computation in the one-way model. More importantly they also obtain a better quantum computation depth with this generalized fow. This characterization result is particularly essential for the study of the algorithms and complexity in the one- way model. These remarkable results have also been presented at the 11th Workshop on Quantum Information Processing (**QIP 2008**, December 2007, New Delhi).

5.1.4.b Fault-tolerance in the one-way model (Objectives: W1.O1, W1.O4; Milestones: W1.M1, W1.M2, W1.M5). In [12], Silva, Danos (Paris), Kashefi (Ox & Gren), and Olivier, proposed a simple variant of the one-way quantum computing model where measurements are restricted to be along the eigenbases of the Pauli X and Y operators, while qubits can be initially prepared both in the $|+_{\frac{\pi}{4}}\rangle := 1/\sqrt{2}(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle)$ state and the usual $|+\rangle := 1/\sqrt{2}(|0\rangle + |1\rangle)$ state. They proved the universality of this quantum computation model, and established a standardisation procedure which permits all entanglement and state preparation to be performed at the beginning of computation. Based on this Pauli model they develop a direct approach to fault-tolerance by simple transformations of the entanglement graph and preparation operations, while error correction is performed naturally via syndrome-extracting teleportations.

5.1.4.c Flow in the one-way model (Objectives: W1.O3; Milestones: W1.M1, W1.M4). In [13], Broadbent and Kashefi (Ox & Gren) presented a novel automated technique for parallelizing quantum circuits via forward and backward translation to measurement-based quantum computing patterns and analyze the trade off in terms of depth and space complexity. As a result they distinguished a class of polynomial depth circuits that can be parallelized to logarithmic depth while adding only polynomial many auxiliary qubits. In particular, they provided for the first time a full characterization of patterns with flow of arbitrary depth, based on the notion of influencing paths and a simple rewriting system on the angles of the measurement. Their method led to insightful knowledge for constructing parallel circuits and as applications, they demonstrated several constant and logarithmic depth circuits. Furthermore, they proved a logarithmic separation in terms of quantum depth between the quantum circuit model and the measurement-based model.

5.1.4.d Instantaneous Quantum Computation. (Objectives: W1.O1, W1.O2, W1.O3, W1O4, W2.O2; Milestones: W1.M4, W1.M5, W1.M6). Shepherd (Bris) and Bremner (QICS postdoc at Bris) examine those architectures for quantum computation which, by restriction, allow for essentially no temporal structure within the quantum part of the computation. Such architectures include the 1-way model without adaptive measurement. They investigate the power that this limited form of quantum computing can impart to an otherwise classical player within the context of an interactive proof game. A paper is in preparation.

5.1.5 Quantum machines and measurement based quantum computing

5.1.5.a Measurement based Quantum Turing Machine (Objectives: W1.O1, W1.O4; Milestone: W1.M5). See **8.1.a** [14].

5.1.5.b PhD. thesis Perdrix (Objectives: W1.O1, W1.O4; Milestones: W1.M1, W1.M2, W1.M4, W1.M5). See **8.1.b** [15].

5.2 Progress towards objectives and performed tasks for W1.T2

5.2.1 Resources for measurement-based quantum computing

5.2.1.a Quantification of entanglement and local information access in graph states (Objectives: W1.O3, W1.O4; Milestones: W1.M1, W1.M2). In MMV07, Markham (QICS postdoc at Paris) and Miyake (QICS postdoc at Inn), in collaboration with Virmani, have evaluated exactly a number of multipartite entanglement measures for a class of graph states, including the d-dimensional cluster states (d = 1,2,3), the Greenberger-Horne-Zeilinger states, and some related mixed states. The entanglement measures that we consider are continuous, 'distance from separable states' measures, including the relative entropy, the so-called geometric measure, and robustness of entanglement. Not only did the work suggest an intimate connection between the calculation of entanglement of graph states and widely-studied graph problems such as the maximum independent set problem and the maximum matching problem, but also its result was immediately helpful to construct a necessary criterion for universal quantum computation in terms of the geometric measure in [2].

5.2.1.b Classical spin models (Objectives: W1.O1, W1.O2; Milestones W1.M1). In [17] Van den Nest (Inn), Duer (Inn) and Briegel (Inn) show how problems involving the statistical mechanics of classical spin systems, can be related to problems in quantum physics. In particular, they relate a large class of classical spin models, including the inhomogeneous Ising, Potts, and clock models of q-state spins on arbitrary graphs, to quantum stabilizer states. As the main result, it is shown how to express partition functions as inner products between certain quantum stabilizer states and product states. This connection allows one to use powerful techniques developed in quantum information theory, such as the stabilizer formalism and classical simulation techniques, to gain general insights into these models in a unified way. Conversely, insights in classical spin systems can be used to e.g. identify new simulatable resource states for measurement-based quantum computation.

In [18] the same authors continue this line of research. The mappings of [VDB07a] are generalized, and existing results about the graph state formalism and quantum computation, namely the universality of the cluster states, are used to gain insights in aspects of statistical mechanics. In particular, the authors 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, the authors find that the corresponding 2D square lattice requires only polynomially more spins w.r.t the original one, a constructive method to map such models to the 2D Ising model is given. 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.

5.2.1.c Resources for producing graph states (Objectives: W1.O1, W1.O3, W1.O4; Milestones: W1.M1, W1.M5). In [19], Hoyer, Mhalla (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox) give a rigorous analysis of the resources required for producing graph states. Graph states have become a key class of states within quantum computation. They form a basis for universal quantum computation, capture key properties of entanglement, are related to quantum error correction, establish links to graph theory, violate Bell inequalities, and have elegant and short graph- theoretical descriptions.Using a novel graph-contraction procedure. They show that any graph state can be prepared by a linear-size constant-depth quantum circuit, and establish trade-offs between depth and width. THey show that any minimal-width quantum circuit requires gates that acts on several qubits, regardless of the depth, they relate the complexity of preparing graph states to a new graph-theoretical concept, the local minimum degree, and show that it captures basic properties of graph states.

5.2.1.d Universality of triangular grids (Objectives: W1.O1, W1.O4; Milestones: W1.M1, W1.M2, W1.M5). Mhalla (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox), prove that measurements in the (X, Z)-plane over triangular grids are universal resources for one-way quantum computation. Moreover they prove that any graph is a pivot minor of a triangular grid. This is the first result of classical graph theory derived from the graph state formalism and the measurement based quantum computation. A paper is in preparation. These results have been presented at the Graph and Algorithm National Workshop in Orleans, France, in November 2006.

5.2.1.e Minimal resources for measurement-only quantum computation (Objectives: W1.O1, W1.O4; Milestones: W1.M5). In [20] Perdrix (Gren & Paris & QICS postdoc at Ox) improves the upper bound on the minimal resources required for measurement-only quantum computation: one 2-qubit observable, 2 one-qubit observables and one ancillary qubit are sufficient resources for universal quantum conputation. Minimizing the resources required for measurement-only quantum computation is a key issue for experimental realization of a quantum computer based on projective measurements. Moreover, this new upper bound allows one to reply in the negative to an open question about the existence of a trade-off between observables and ancillary qubits in measurement-only QC.

5.2.2 General properties of graph states

5.2.2.a An algorithm for causal flow (Objectives: W1.O1, W1.O3, W1.O4; Milestones: W1.M1, W1.M5, W1.M6). In [21] Mhalla (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox) introduce two algorithms. The first algorithm decides whether a given open graph has a causal flow. This algorithm improves the algorithm introduced by De Beaudrap since it works whatever the numbers of inputs and outputs are. The second algorithm is for finding a gflow in a given open graph. It proves that the problem of deciding whether a given open graph has a gflow is in P. Moreover the previous algorithms are constructive and produce flows of minimal depth leading to a one-way quantum computation of minimal depth.

5.3 Progress towards objectives and performed tasks for W1.T3

5.3.1 Calculi for one-way computing

5.3.1.a The measurement calculus (Objectives: W1.O1, W1.O2, W1.O3, W1.O5; Milestones: W1.M3, W1.M4, W1.M5). In [22, 23], Danos (Paris), Kashefi (Ox & Gren) and Panangaden (McGi) developed a rigorous mathematical model underlying the one-way quantum computer and presented a concrete syntax and operational semantics for programs, called patterns, and an algebra of these patterns derived from a denotational semantics. More importantly, they presented a calculus for reasoning locally and compositionally about these patterns. They also presented a rewrite theory and proved a general standardization theorem which allows all patterns to be put in a semantically equivalent standard form. Furthermore they formalised several other measurement-based models: Teleportation, Phase and Pauli models and presented compositional embeddings of them into and from the one-way model. This allowed to transfer all the theory developed for the one-way model to these models and showed that the framework they have developed has a general impact on measurement-based computation and is not just particular to the one- way quantum computer.

5.3.1.b Rewriting between computational models (Objectives: W1.O2, W1.O3, W2.O4, W3.O6; Milestones: W1.M1, W1.M6). Duncan (QICS postdoc at Ox) defined a formal rewriting system which is universal for quantum computations. This system provides a unified setting for reasoning about different models of quantum computations. Via a translation from the measurement calculus of **5.3.1.a** he showed that this system has normal forms which are quantum circuits exactly when the corresponding measurement based computation has 'flow'. A paper is in preparation. Ongoing work with (Gren & Paris and QICS postdoc at Ox) to extend this work.

5.3.1.c Quadratic form expansion (Objectives: W1.O2, W1.O3, W2.O4, W3.O6; Milestones: W1.M1, W1.M6). In [24], de Beaudrap, Danos (Paris), Kashefi (Ox & Gren) and Roetteler, introduced techniques to analyze unitary operations in terms of quadratic form expansions, a form similar to a sum over paths in the computational basis when the phase contributed by each path is described by a quadratic form over $\mathbb{R}$. They showed how to relate such a form to an entangled resource akin to that of the one-way measurement model of quantum computing. Using this, they described various conditions under which it is possible to efficiently implement a unitary operation U, either when provided a quadratic form expansion for U as input, or by finding a quadratic form expansion for U from other input data.

5.3.1.c Simulation of networks with matrix product states (Objectives: W1.O1, W1.O2, W1.O3; Milestones: W1.M2, W1.M4). In [25] Jozsa (Bris) considers recent works on the simulation of quantum circuits using the formalism of matrix product states and the formalism of contracting tensor networks. He provides simplified direct proofs of many of these results, extending an explicit class of efficiently simulable circuits.

5.3.2 Graphical calculus and categorical semantics for measurement based quantum computing

5.3.2.a Categorical characterisation and graphical calculus for resources states and one-qubit projections in measurement based quantum computing (Objectives: W1.O1, W1.O2, W1.O5; Milestones: W1.M1, W1.M3, W1.M4). See **6.1.a**, **6.1.c** and in particular **6.1.d** [26, 27, 28].

5.3.2.b Categorical characterisation and graphical calculus for classical-quantum and quantum-classical information flow in measurement based quantum computing (Objectives: W1.O1, W1.O2, W1.O5; Milestones: W1.M4). See **6.1.b** and in particular **6.1.e** [29].

5.3.3 Automated reasoning tools for measurement based quantum computing

See **8.4.2.a**, §**8.4.2** and in particular **8.4.3.b**.

Bibliography

[1] M. Van den Nest, A. Miyake, W. Duer, H. J. Briegel, Universal resources for measurement-based quantum computation, Phys. Rev. Lett. 97, 150504 (2006)

[2] M. Van den Nest, W. Duer, A. Miyake, H. J. Briegel, Fundamentals of universality in one-way quantum computation, New J. Phys. 9, 204 (2007) in the special issue on the measurement-based quantum information processing.

[3] D. E. Browne, M. B. Elliott, S. T. Flammia, S. T. Merkel, A. Miyake, A. J. Short, Phase transition of computational power in the resource states for one-way quantum computation arXiv.org:0709.1729 (2007), to be published in New J. Phys. (2008)

[4] S. Popescu (2006) KLM quantum computation as a measurement based computation. arXiv:quant-ph/0610025

[5] S. Popescu (2007) Knill-Laflamme-Milburn Quantum Computation with Bosonic Atoms. Phys. Rev. Lett. 99, 130503.

[6] M. Van den Nest, W. Duer, G. Vidal, H. J. Briegel, Classical simulation versus universality in measurement based quantum computation, Phys. Rev. A 75, 012337 (2007)

[7] W. Duer, M. Bremner, H. J. Briegel, Quantum simulation of interacting high-dimensional systems: the influence of noise, arXiv.org:0706.0154 (2007)

[8] C.-E. Mora, H. J. Briegel, B. Kraus, Quantum Kolmogorov complexity and its applications, arXiv.org:quant-ph/0610109 (2006)

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

[10] D. Gross, M. Van den Nest, The LU-LC conjecture, diagonal local operations and quadratic forms over GF(2), arXiv.org:0707.4000 (2007), to appear in Quant. Inf. Comp (2008).

[11] D. E. Browne, E. Kashefi, M. Mhalla and S. Perdrix. Generalized Flow and Determinism in Measurement-based Quantum Computation. New Journal of Physics(9) : 250 (2007).

[12] M. Silva, V. Danos, E. Kashefi, and H. Olivier, A direct approach to fault-tolerance in measurement-based quantum computation via teleportation, New Journal of Physics, 2007.

[13] A. Broadbent and E. Kashefi, On parallelising quantum circuit, The international workshop on measurement-based quantum computing, 2007 (Submitted to Journal of Theoretical Computer Science).

[14] S. Perdrix and Ph. Jorrand. Classically-controlled quantum computation. Mathematical Structures in Computer Science, 16:601-620, 2006.

[15] S. Perdrix. Modèles formels du calcul quantique : ressources, machines abstraites et calcul par mesure. Ph.D. thesis, Institut National Polytechnique de Grenoble, Laboratoire Leibniz, Dec. 2006.

[16] D. Markham, A. Miyake, S. Virmani, Entanglement and local information access for graph states, New J. Phys. 9, 194 (2007) in the special issue for measurement-based quantum information processing.

[17] M. Van den Nest, W. Duer, H. J. Briegel Classical spin models and the quantum stabilizer formalism, Phys. Rev. Lett. 98, 117207 (2007).

[18] M. Van den Nest, W. Duer, H. J. Briegel, Completeness of the classical 2D Ising model and universal quantum computation arXiv.org:0708.2275 (2007).

[19] P. Hoyer, M. Mhalla, and S. Perdrix. Resources required for preparing graph states. In Procedings 17th International Symposium on Algorithms and Computation (ISAAC 2006), Lecture Notes in Computer Science, volume 4288, pages 638-649, Dec. 2006.

[20] S. Perdrix. Towards minimal resources of measurement-based quantum computation. New Journal of Physics, 9, 206, 2007.

[21] M. Mhalla and S. Perdrix. Finding Optimal Flows Efficiently. quant-ph/0709.2670.

[22] V. Danos, E. Kashefi, and P. Panangaden, The Measurement Calculus, Journal of ACM, 2007.

[23] V. Danos, E. Kashefi, and P. Panangaden, The One Way to Quantum Computation, Lecture Notes in Computer Science, 4052, Invited Papers to the 33th International Colloquium on Automata, Languages and Programming, July-2006.

[24] N. de Beaudrap, V. Danos, E. Kashefi, and M. Roetteler, Quadratic Form Expansions for Unitaries, The 3rd Workshop on Theory of Quantum Computation, Communication and Cryptography, 2008. Preprint arXiv:0801.2461.

[25] R. Jozsa (2006) On the simulation of quantum circuits. arXiv:quant-ph/0603163.

[26] R. W. Duncan (2006) *Types for Quantum Computing*. D.Phil. thesis. University of Oxford.

[27] B. Coecke and D. Pavlovic (2007) *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 567–604. Taylor and Francis. arXiv:quant-ph/0608035.

[28] B. Coecke and R. Duncan (2008) *Interacting Quantum Observables*. Submitted to ICALP'08.

[29] B. Coecke, E. O. Paquette and D. Pavlovic (2008) *Classical and quantum structures*. To appear in: Semantic Techniques in Quantum Computation, S. Gay and I. Mackie, Eds. Cambridge University Press.

Chapter 6

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. Categorical semantics for quantum mechanics, the corresponding logics and the resulting diagrammatic methods were entirely being carried out by QICS participants at the start of the proposal: the pioneers of this approach are all based at QICS sites or at QICS affiliated sites. This has slightly changed now; several other groups have taken up our approach and in particular several PhD students elsewhere are now being trained in these mathematical methods, which are highly non-standard in quantum information. The interest in this approach has grown substantially since the start of QICS — which is witnessed by the exceptional number of invited talks by its originators. In the light of this growing interest, given the high 'entry cost' of working in this area, a series of volumes is currently being produced by the QICS team, which comprises tutorial chapters on the use of categorical, domain theoretic and other logic tools in quantum informatics [New structures for Physics. Lecture Notes in Physics. Springer-Verlag. (forthcoming, 2008)]. In a separate development, a volume of chapters on computer science methods [Semantic techniques in Quantum computing. Cambridge UP. (forthcoming, 2008)] is also in preparation.

Main developments in W2. Our developments have been specifically focussed on problems and requirements arising from the other workpackages of QICS. This mainly involved refining the axiomatic setting to accommodate all the essential features of the novel quantum computational models and quantum computational paradigms, with a particular focus on measurement-based quantum computing, quantum classical interaction, entanglement as a computational resource, and topology as an (abstract) computational resource. The main objective of this year was to get into sufficiently high gear such that the categorical semantics, the corresponding logics and the resulting diagrammatic methods would provide a powerful vehicle to solve some hard problems of the other workpackages and tasks. The key result obtained are as follows:

CQ We now have a *comprehensive axiomatic account of both quantum and classical data within the diagrammatic language* (**6.1.b**, **6.1.e** in W2.T1). Important insights are starting be gained on the required structural resources which distinguish different measurement-based quantum computational models. E.g. the teleportation model requires less structure than state transfer while it requires more physical qubits to be realised. This seems to point a remarkable trade-off between structure and number of systems. This is crucial for the applications in measurement-based quantum computational models which require classically controlled correction operations. The way this was achieved was by making the ability to copy and uniformly erase classical data (contra quantum data) explicit as a feature.

CO We now have a *axiomatic and diagrammatic account of complementary observables* (**6.1.c** in W2.T1) which enables abstract simulation of elementary gate computations. To put this in some historical perspective, axiomatic approaches to quantum mechanics emphasised *negative* features of quantum theory which followed from the existence of complementary observables: non-distributivity of propositional lattices and non-commutativity of spectral algebras. Categorical axiomatics changed this attitude by making quantum 'features' explicit. The categorical account of mutually unbiassed bases turns the source of the negative quantum structural paradigms now into a posistive and expressive feature. Due to its high-level nature this structure is also promising for automation (**6.1.f** in W2.T1).

Besides the direct developments there were two important strands of study of categorical structures which will be of importance for internal use within this workpackage:

CL We now have a *comprehensive high-level representation for all gates and multipartite entangled states* (**6.1.c**, **6.1.d** in W2.T1 and **6.2.1.a** in W2.T2). this is a further elaboration on **CO**. Interesting results on translations between measurement based quantum computational models (see the picture in **6.1.d**) and a classification of multi-partite entangled states in terms of their informatic capabilities, and which refines SLOCC classification, have started to emerge.

CM *Several new categorical models for particular features of quantum informatics have been produced* (**6.1.1** in W2.T1). Models are very important to guide the development of categorical axiomatics as well as to make computational features such as recursion, cycles, coding-decoding, etc., available within categorical axiomatics.

CL *Steps toward a categorical axiomatics for topological quantum computing have been made* (**6.3.a** and **6.3.b** in W2.T3). This mainly involved the study of functorial and other structural properties of the topologies involved. The connections with Temperley-Lieb algebra in **6.3.a** bring within reach the powerful results from representation theory

The next steps to take. We are very much progressing according to schedule. We reached milestone W2.M1 within the first year of activity for this workpackage and have made substantial progress towards the other milestones. Due to the available postdocs there will be been a trade-off between activity W2.M2 on topological quantum computing (QICS will hire a postdoc on this topic from September 08 on; currently he is finishing his PhD) and W2.M2 on a logical understanding of multipartite behaviour, on which two QICS postdocs have been active, and hence has seen substantially more progress then indicated in the original plan. The next step on the logic of multi-partite entanglement will be the passage from pure to mixed states; this passage is categorically well-understood (see **6.1.g**). So the only change to the original plan is the fact that W2.M2:(12)↦(36) and W2.M6:(36)↦(24). Due to availability of the appropriate postdoc will we also be able to extend our range of quantum computational models with adiabatic quantum computing; something we indicated as a desirable possibility in the QICS abstract. An important activity will also be automated design and analysis of quantum informatic protocols. Tools are currently under development (**6.1.f** in W2.T1).

Interactions with other workpackages and sites. This workpackage is inherently intertwined with the other ones as is clear from our discussion above. It suffices to observe that the results of W2 figure in each of the reports on the work performed in W1, W3 and W4.

Samson Abramsky and Bob Coecke
Oxford, February 10, 2008.

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.

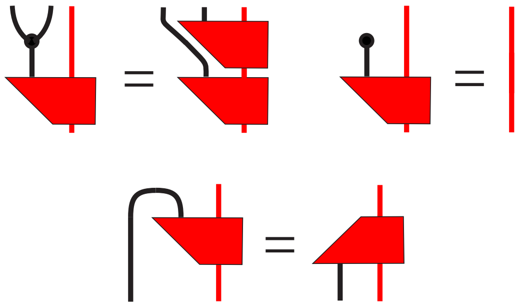
W2.T2 Study the structure of multi-partite entanglement using categorical methods and others; combine quantum structure and spatio-temporal structure.

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.

6.1 Progress towards objectives and performed tasks for W2.T1

6.1.a Ross Duncan's PhD thesis (Objectives: W2.O1, W2.O3, W2.O4; Milestones: W2.M1, W2.M4). In [1] Duncan (QICS postdoc at Ox) developed a general categorical formalism which provides axiomatics for reasoning about entangled systems in the broadest possible generality. Representations of freely constructed abstract quantum theories – precisely, dagger compact categories with certain unitary generators – are constructed. Formal calculi (of an essentially graphical nature) are developed which permit the evolution of quantum systems to be modelled. As an application, the system is used to provide formal rewrites to support reasoning about measurement based quantum computing, and in particular, translations between measurement based and quantum circuit computations.

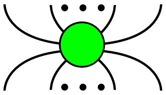
6.1.b A resource-sensitive category theoretic account and diagrammatic calculus for classical data and quantum observables (Objectives: W2.O1, W2.O2; Milestones: W2.M1, W2.M4, W2.M5). In [2] Coecke (Ox) and Pavlovic (Ox) suggest that quantum mechanics can be done without any notion of sum, expressed entirely in terms of the tensor product. The corresponding axioms define classical spaces as objects that allow copying and deleting data. They show that the information exchange between the quantum and the classical worlds is essentially determined by their distinct capabilities to copy and delete data. The sums turn out to be an implicit implementation of this capability. Realizing it through explicit axioms not only dispenses with the unnecessary structural baggage, but also allows a simple and intuitive graphical calculus. In category-theoretic terms, classical data types are dagger-compact Frobenius algebras, of which the data consists of a copying operation $\delta : X \to X \otimes X$ and a deleting operation $\epsilon : X \to \mathrm{I}$, both 'extended by linearity to quantum states'. The algebraic laws for these intuitively capture the nature of copying and deleting. The quantum spectra underlying quantum measurements are exactly dagger Eilenberg-Moore coalgebras induced by these Frobenius algebras. They show that the corresponding three equations, which graphically depict as:



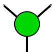
are necessary and sufficient to characterise all projective quantum measurements within the category of $\mathbf{FdHilb}$ of finite dimensional Hilbert spaces, linear maps and tensor product. Moreover, each of these rules admits a clear operational interpretation.

Each base in a Hilbert space canonically induces a dagger-compact Frobenius algebra $(|i\rangle \mapsto |ii\rangle, |i\rangle \mapsto 1)$. Recently, Coecke (Ox), Pavlovic (Ox) and Vicary showed that the coverse is also true: each dagger-compact Frobenius algebra arises in this way. From this one can derive that the dagger-compact Frobenius algebras in the category $\mathbf{FdHilb}$ together with comonoid homomorphisms and inherited monoidal structure, is equivalent to the category of sets, functions and the cartesian product. This procedure establishes a new kind of classical limit: classical process structure is a restriction of the quantum process structure in the sense that classical processes have enhanced capabilities relative to copying and deleting. A paper on this is in preparation.

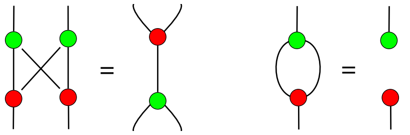
In [3] Coecke (Ox) and Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) build further on the work in [2] by providing an abstract purely compositional characterisation of POVMs. They show that at this highly level Naimark's dilation theorem still holds, and provide a purely graphical proof of this. Also in [3] Coecke (Ox) and Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) prove that all morphism generated from dagger-compact Frobenius algebra structure on an object X and the dagger symmetric monoidal structure, which have the same domain and codomain, and for which the graphical representation is connected, must coincide. Hence, when taking all but the symmetry natural isomorphism of the symmetric monoidal structure to be strict, such a morphism only depends on the object X and it's number of inputs and outputs. This result admits a very convenient diagrammatic interpretation in the sense that each such connected network obtains a 'spider'-normal form



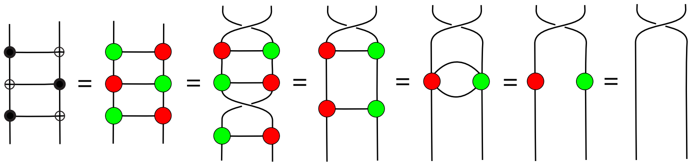
which is obtained by fusing dots which diagrammatically represent δ and ϵ:

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

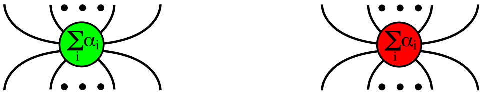
6.1.c Complementary observables as bialgebras (Objectives: W2.O1, W2.O2, W2.O3; Milestones: W2.M1, W2.M4, W2.M6). In [4] Coecke (Ox) and Duncan (QICS postdoc at Ox) formalise the constructive content of an essential feature of quantum mechanics: the interaction of incompatible quantum observables. Axiomatic approaches to quantum mechanics have historically focussed on the failure of various properties: non-commutative algebras, non-distributive lattices, non-Kolmogorovian probabilities, etc. More recent attempts originating in quantum computer science, concentrate mainly on accommodating no-cloning and no-deleting. Coecke (Ox) and Duncan (QICS postdoc at Ox) take a positive attitude: they identify the flow of information between incompatible observables. Using a general categorical formulation, and in particular relying on the structure introduced in [2], they show that a pair mutually unbiassed quantum observables forms a bialgebra-like structure; additional structure enables them to derive all observables and define a computationally universal system. The resulting equations suffice to perform intuitive computations with elementary quantum gates, translate between distinct quantum computational models, establish the equivalence of entangled quantum states, and simulate quantum algorithms such as the quantum Fourier transform. This formalism moreover admits a purely diagrammatic calculus in which the basic laws depict as



which lead to computations such the reduction of three cnot gates to symmetry:

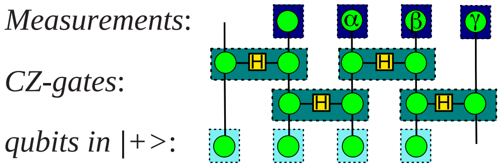


We can also introduce phase data which still obeys a 'generalised spider theorem':

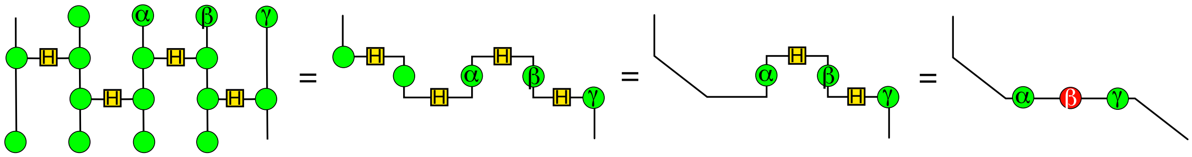


resulting in a language which is rich enough to represent all states, operations and measurements which can be described in the Hilbert space quantum formalism, and diagrammatically reason about them.

6.1.d Diagrammatic accounts on measurement-based quantum computing I: the conditional case (Objectives: W1.O5, W2.O1, W2.O2; Milestones: W1.M4, W2.M1, W2.M4). In [4] Coecke (Ox) and Duncan (QICS postdoc at Ox) provided an elegant diagrammatic schemes to reason about measurement based quantum computational schemes and illustrated this on Perdrix' state transfer and the one-way model. For example, that the network

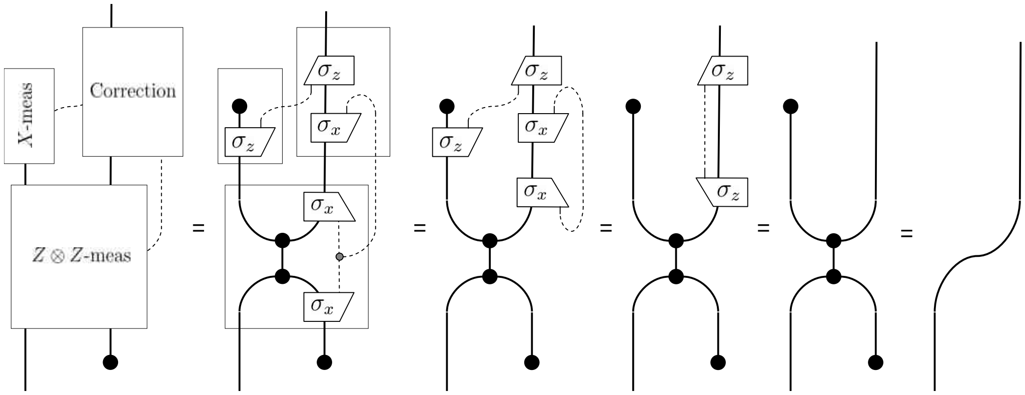


simulate an arbitrary qubit unitary can be proved like this



A paper specifically focussing on the applications of this language to measurement-based quantum computing is in preparation.

6.1.e Diagrammatic accounts on measurement-based quantum computing II: classical control (Objectives: W1.O5, W2.O1, W2.O2, W3.O4, W3.O5; Milestones: W1.M4, W2.M1, W2.M4, W3.M4, W3.M5). In a complementary strand of research Coecke (Ox), Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) and Perdrix (Gren & Paris & QICS postdoc at Ox) focus on the classical-quantum interaction and the minimal (diagrammatic) structural requirements to prove correctness for measurement based quantum computational schemes including classical control. For Perdrix' state transfer we have



A paper is in preparation; some basic cases were already considered in [5] by Coecke (Ox), Pavlovic (Ox) and Paquette (McGi affiliated & forthcoming QICS postdoc at Ox).

6.1.f An automated tool to reason about complementary observables, (Objectives: W2.O4; Milestones: W2.M4). Duncan (QICS postdoc at Ox), Kissinger (Ox) and Dixon (Ox affiliated) have partially implemented an automated tool for reasoning about quantum processes and entangled states. This is a semi-automatic rewriting engine with a GUI based on the graphical formalism of Coecke (Ox) and Duncan (QICS postdoc at Ox). A paper is preparation; development of the tool continues.

6.1.g Axiomatics for complete positivity (Objectives: W2.O2; Milestones: W2.M4, W2.M5). In [7] Coecke (Ox) shows that given any dagger symmetric monoidal category $\mathbf{C}$ we can construct a new category $\mathbf{Mix}(\mathbf{C})$, which, in the case that $\mathbf{C}$ is a †-compact category, is isomorphic to Selinger's $\mathbf{CPM}(\mathbf{C})$. Hence, if $\mathbf{C}$ is the category $\mathbf{FdHilb}$ we exactly obtain completely positive maps as morphisms. This means that mixedness of states and operations is a concept which can exist independently of compactness. Moreover, since our construction does not require †-compactness, it can be applied to categories which have infinite dimensional Hilbert spaces as objects. Finally, in general $\mathbf{Mix}(\mathbf{C})$ is not a †-category, so does not admit a notion of positivity. This means that, in the abstract, the notion of 'complete positivity' can exist independently of a notion of 'positivity', which points at a very unfortunately terminology.

6.1.1 Categorical models

6.2.a A categorical account on Rob Spekkens' toy model (Objectives: W1.O1, W2.O2; Milestones: W2.M5). Coecke (Ox) and Edwards (Ox) provided a very simple category-theoretic presentation of Rob Spekkens' toy model. It suffices to specify the appropriate category, which can be done by specifying only 3 generators, to obtain the model, which is substantially simpler than Spekkens'. All quantum phenomena follow by purely abstract categorical reasons. We expect to get useful insights on the required concrete categories for discrete models of quantum reasoning. A paper is in preparation.

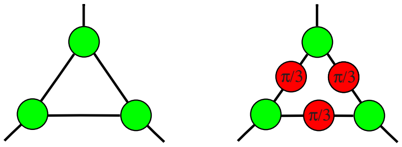
6.2.b Categories and domains of partial isometries (Objectives: W2.O2, W2.O4; Milestones: W2.M4). In [8] Hines (QICS postdoc at York) and Braunstein (York) study of partial isometries in order-theoretic and domain-theoretic terms. In order-theoretic terms, they consider a partial order on partial isometries introduced by Halmos-McLaughlin, and show that this is a natural generalisation of the orthomodular lattice ordering used in Birkhoff - von Neumann quantum logic. From a categorical point of view, it is well-known that the composite of two partial isometries is not itself a partial isometry. However, we introduce an alternative composition (based on Girard's execution formula) that allows us to define a category of partial isometries. We show that this composite is given by a supremum in the Halmos-McLaughlin partial ordering. The resulting category is shown to be an inverse category, and hence has a 'natural partial order' on homsets derived from the inverse structure. This natural partial order is shown to be exactly the Halmos-McLaughlin ordering, making hom-sets are directed-complete partial orders. This category, and the partial ordering on hom-sets, are studied from the point of view of teleportation protocols and compact closure, in order to establish both physical interpretations and connections with the Abramsky-Coecke categorical approach to foundations of quantum mechanics. The logical interpretations of the category theoretic, the orthomodular lattices, approach to quantum logic are contrasted from this point of view.

6.2.c A categorical view on code and data (Objectives: W2.O2, W2.O4; Milestones: W2.M4). In [9] Hines (QICS postdoc at York) considers the differences between quantum and classical information that mean that a quantum computer cannot run the von Neumann architecture, and the implications for quantum information and computation. A case is made that the computational utility of the von Neumann architecture arises from the 'decode a byte and apply the appropriate operation' step in the fetch-execute cycle. The properties of such 'evaluation' operations are considered from the point of view of code / data correspondences (i.e. the categorical property of 'naming arrows'), and the no-cloning and no-deleting theorems. These are studied from the point of view of Nielsen-Chuang's 'Encoding unitary maps on an orthonormal basis', Abramsky-Coecke's categorical foundations program, and the Jamiolkowski-Choi correspondence between density matrices and completely positive maps.

6.2 Progress towards objectives and performed tasks for W2.T2

6.2.1 Graphical calculus for multipartite entanglement

6.2.1a A diagrammatic notation and classification for arbitrary multi-partite entangled states (Objectives: W2.O3; Milestones: W2.M3, W2.M6). The language introduced in [4] is sufficiently expressive to give diagrammatic presentations of multi-partite entangled states: we showed that we can simulate any unitary, hence we can simulate any entangled state as the image of some reference state given the appropriate unitary. For example, the GHZ and W state can be presented as follows



(the three green dots of the GHZ state can in fact be fused into one). Coecke (Ox) and Edwards (Ox) have used this fact to define classes of multipartite states which further refine the SLOCC classes. For example, there are subclasses of the W-SLOCC class which depict differently, and it turns out that they indeed have distinct behavioural properties. A paper is in preparation.

6.2.2 General results on entanglement

6.2.2a (Objectives: W2.O2, W2.O3; Milestones: W2.M3, W2.M6). In [10] Winter (Bris) and co-authors show that genuine multipartite quantum correlations can exist for states which have no genuine multipartite classical correlations, even in macroscopic systems. They construct such states for an arbitrary odd number of qubits. Such possibilities can have important implications in the physics of quantum information and phase transitions.

6.2.2b (Objectives: W1.O1, W2.O2, W2.O3; Milestones: W1.M4, W2.M3, W2.M6). Motivated by the recent discovery of a quantum Chernoff theorem for asymptotic state discrimination, Matthews (Bris) and Winter (Bris) investigate in [11] the distinguishability of two bipartite mixed states under the constraint of local operations and classical communication (LOCC), in the limit of many copies. Surprisingly, the single-copy optimal measurement remains optimal for n copies, in the sense that the best strategy is measuring each copy separately, followed by a simple classical decision rule.

6.2.2c (Objectives: W1.O4, W2.O3; Milestones: W1.M5, W2.M3). In [12] Markham (QICS postdoc at Paris) has developed techniques for calculating entanglement for large classes of states important in many body physics and quantum information, particularly in particular for measurement-based quantum computing (W-states and stabilizer states). Those results imply bounds on local discrimination for these states (important in many quantum information protocols), and the optimality of associated entanglement witnesses (important in the realisable verification of entanglement).

6.2.3 Distributed quantum computing

6.2.3a (Objectives: W1.O1, W1.O4, W3,O2, W4.O2, W4.O4; Milestones: W1.M4, W1.M5). In [13] Linden (Bris), Popescu (Bris), Short (Bris) and Winter (Bris) investigate the problem of "nonlocal" computation, in which separated parties must compute a function with nonlocally encoded inputs and output, such that each party individually learns nothing, yet together they compute the correct function output. They show that the best that can be done classically is a trivial linear approximation. Surprisingly, they also show that quantum entanglement provides no advantage over the classical case. On the other hand, generalized (i.e. super-quantum) nonlocal correlations allow perfect nonlocal computation.

6.3 Progress towards objectives and performed tasks for W2.T3

6.3.a Temperley-Lieb algebra and quantum computing (Objectives: W2.O2, W2.O5; Milestones: W2.M5). In [14, 15] Abramsky (Ox) shows how Abramsky-Coecke categorical quantum axiomatics can be connected in a very direct way with diagram algebras, in particular the Temperley-Lieb algebra, which plays a central rôle in the Jones polynomial and ensuing developments. We find that the Temperley-Lieb algebra is the 'planar' version of our quantum setting; and we find new connections between logic and geometry. For example, we can give a simple, direct (no quotients) description of the Temperley-Lieb algebra, which leads in turn to full completeness results for various non-commutative logics. Moreover, we show that planarity is an invariant of the infomation flow analysis of cut elimination. This leads to a number of interesting new kinds of questions: (i) What is the computational significance of planarity as a constraint on expressiveness or complexity? (ii) Most quantum protocols appear to live on the plane; which do not? (iii) What is the computational or logical significance of braiding? There are obvious direct connections between these notions and topological quantum computing.

6.3.b Modular functors for topological quantum computing (Objectives: W2.O5; Milestones: W2.M5). In [16] Panangaden (McGi) and Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) fill the gap between physics, mathematics and computer science in order to give a simple yet thorough introduction to the cluster of ideas involving category theory, topology, condensed matter physics – specifically anyons – and quantum computation. There is a need for such an introduction as the technical introductions to the subject available are either written for physicists or computer scientists but the categorical ideas are usually not described. For a researcher with a background in category theory the subject can be approached with a simple algebraic language, that is, the language of modular tensor categories and modular functors. The exposition is intended to explain the peculiar physical properties of anyons and two-dimensional physics and to introduce the notion of modular tensor categories and finally to show how such a context is intended to be used in robust quantum computation. Currently ongoing research in the area is: (i) To develop a categorical semantics for topological quantum computation; (ii) Investigate the algorithmic properties of topological computation; (iii) To analyze the various connections with other recent developments in categorical quantum computation i.e., dagger compact categories, classical objects etc.

Bibliography

[1] R. W. Duncan (2007) *Types for Quantum Computing*. D.Phil. thesis. University of Oxford.

[2] B. Coecke and D. Pavlovic (2007) *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 567–604. Taylor and Francis. arXiv:quant-ph/0608035.

[3] B. Coecke and E. O. Paquette (2007) *POVMs and Naimark's theorem without sums*. Electronic Notes in Theoretical Computer Science (To appear). arXiv:quant-ph/0608072

[4] B. Coecke and R. Duncan (2008) *Interacting Quantum Observables*. Submitted to ICALP'08.

[5] B. Coecke, E. O. Paquette and D. Pavlovic (2008) *Classical and quantum structures*. To appear in: Semantic Techniques in Quantum Computation, S. Gay and I. Mackie, Eds. Cambridge University Press.

[6] B. Coecke (2007) De-linearizing linearity: projective quantum axiomatics from strong compact closure. Electronic Notes in Theoretical Computer Science **170**, 47–72. arXiv:quant-ph/0506134

[7] B. Coecke (2007) *Complete positivity without positivity and without compactness*. Oxford University Computing Laboratory Research Report PRG-RR-07-05. web.comlab.ox.ac.uk/oucl/publications/tr/rr-07-05.html

[8] P. Hines and S. Braunstein (2008) The categorical and domain-theoretic structure of partial isometries. To appear in: Semantic Techniques in Quantum Computation, S. Gay and I. Mackie, Eds. Cambridge University Press.

[9] P. Hines (2008) Can a quantum computer run the von Neumann architecture? To appear in: New Structures for Physics, B. Coecke (ed). Springer Lecture Notes in Physics.

[10] D. Kaszlikowski, A. Sen (De), U. Sen, V. Vedral, A. Winter (2007) Quantum Correlation Without Classical Correlations? arXiv:0705.1969

[11] W. Matthews and A. Winter (2007) On the Chernoff distance for asymptotic LOCC discrimination of bipartite quantum states. arXiv:0710.4113

[12] M. Hayashi, D. Markham, M. Murao, M. Owari and S. Virmani (2008) Entanglement of multiparty stabilizer, symmetric, and antisymmetric states. Phys. Rev. A 77, 012104.

[13] N. Linden, S. Popescu, A. J. Short, and A. Winter (2007) Quantum Nonlocality and Beyond: Limits from Nonlocal Computation. Phys. Rev. Lett. 99, 180502.

[14] S. Abramsky (2007) Temperley-Lieb algebra: From knot theory to logic and computation via quantum mechanics. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 515–557. Taylor and Francis.

[15] S. Abramsky and B. Coecke (2007) *Physics from Computer Science: a Position Statement*. International Journal of Unconventional Computing **3**, 179–197.

[16] P. Panangaden and E. O. Paquette (2008) *Introduction to modular tensor categories and topological quantum computation*. To appear in: New Structures for Physics, B. Coecke (ed). Springer Lecture Notes in Physics.

Chapter 7

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. While in traditional computing the notion of information flow is starting to become well-defined, see for example [J. Barwise and J. Seligman (1997) Information Flow: The Logic of Distributed Systems. Cambridge UP.]), the ultimate goal of this workpackage mainly aims at delineating a corresponding notion when quantum and classical systems are interacting. The situation is of course far more complicated here given that besides the flows between the quantum and the classical there are also the flows within the quantum itself subject to entanglement. Moreover, the notion of information, even in a more static sense, is not yet fully understood in the quantum context. To our knowledge a coordinated interdisciplinary joint attempt to work towards a unifying concept of information flow for quantum informatics is unique to QICS. In this workpackage we approach this involved problem from several different angles.

Main developments in W3.

Q I *The quantum information approach* (**7.1** in W3.T1). Quantum information theory is an established area of research which counts several QICS members as its pioneers and important contributors. Important recent developments involve a *modular* account on quantum informatic resources in terms of *resource inequalities*. The discovery by the QICS team of the so-called mother **7.1.1.a** and father **7.1.1.b** protocols in this quantum information resource calculus is a fundamentally significant development – it conceptually unifies a wide variety of previously diverse quantum information processing results, such as characterisation of noisy channel capacities, entanglement distillation, quantum broadcasting and state merging and many more. It is expected to be a powerful tool in many areas such as approximate quantum error correction, the ongoing study of quantum multi-access channels and many further aspects of noisy quantum communication. Correspondingly, further developments of the associated W3 objectives, aimed at increasing our understanding of these fundamental protocols, remain key issues for further research. Further general results by QICS members on quantum information resources cover a wide selection of specific topics indicating the rich fertility of this subject area for further research. Some of these outputs, such as a variety of new results on quantum state discrimination, are expected to have a broader applicability e.g. to issues of cryptographic security in quantum communication.

QD *Quantum data processing* (**7.2.2 and 7.2.3** in W3.T1). A further group of outputs provide new foundational results on the relationship between classical and quantum data processing. From a higher perspective these are significant since they bear directly on the most fundamental issue of quantum computation viz. the relationship of classical to quantum computational complexity, and the characterisation of ways in which the latter is an extension of the former. These results will also relate to cognate developments in W1 on measurement based computation which provides a particular (and to date, the most studied) paradigm of a hybrid system that incorporates both classical and quantum processing, enabling the consideration of their interactions and tradeoff possibilities in a concrete setting.

CT *Categorical operational semantics* (**7.2.2** in W3.T2). The application of category theory in computer science has it roots in the types-as-objects and morphisms-as-processes paradigm, making it an obvious candidate structure to approach information flow from a more abstract perspective. A first result is the paragraph **CQ** discussed in the introduction to W2. The tiny bit of structure required to distinguish classical from quantum in this abstract setting turns out to be sufficient to extract from an abstract family of quantum processes, a variety of classical processes such as reversible classical processes, deterministic- and non-deterministic processes, stochastic processes and even informatic order in terms of majorisation. in the light of the discussion the paragraph **CO** in the introduction to W2, the QICS team was able to prove the no-cloning theorem based on purely topological principles. That is, a negative feature of quantum theory directly follows from imposing a positive one, in this case the existence of correlations (in very abstract terms).

CA *Coalgebraic structures and methods* (**7.2.5** in W3.T2). These have become an important tool in traditional computer science when dealing with non-deterministic and probablistic processes. They are the natural mathematical framework to accomodate *branching*. Therefore one expects them to be very useful in modelling the non-determinism of quantum information dynamics. We were able to recast a range of important quantum informatic concepts coalgebraically, making them subject to a variety of high-level methods.

The next steps to take. Progress towards all milestones has been substantial the most noteworthy being the progress on W3.M1, W3.M5 and W3.M6. We are confident we will realise all the intended objects if the current level of activity is maintained.

Interactions with other workpackages and sites. Obviously, as it follows from the many cross-references in the detailed description of the work, the activity in this workpackage is intertwined with the developments in the other workpackages.

Bob Coecke & Richard Jozsa
Oxford & Bristol, February 10, 2008.

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.

7.1 Progress towards objectives and performed tasks for W3.T1

7.1.1 Progress on the resource calculus

7.1.1.a The mother protocol (Objectives: W3.O1, W3.O2; Milestones: W3.M1, W3.M2, W3.M4). In [1] Hayden (McGi), Winter (Bris) and co-authors give a simple, direct proof of the 'mother' protocol of quantum information theory. The mother protocol described here is easily transformed into the so-called "father" protocol whose children provide the quantum capacity and the entanglement-assisted capacity of a quantum channel, demonstrating that the division of single-sender/single-receiver protocols into two families was unnecessary: all protocols in the family are children of the mother.

7.1.1.b The father protocol (Objectives: W3.O1, W3.O2; Milestones: W3.M1, W3.M2, W3.M3). In [2] Hayden (McGi) and collaborators study a protocol in which many parties use quantum communication to transfer a shared state to a receiver without communicating with each other. This protocol is a multiparty version of the fully quantum Slepian-Wolf protocol for two senders and arises through the repeated application of the two-sender protocol. We describe bounds on the achievable rate region for the distributed compression problem. The inner bound arises by expressing the achievable rate region for our protocol in terms of its vertices and extreme rays and, equivalently, in terms of facet inequalities. We also prove an outer bound on all possible rates for distributed compression based on the multiparty squashed entanglement, a measure of multiparty entanglement.

7.1.1.c A generalised Slepian-Wolf protocol (Objectives: W3.O1, W3.O2; Milestones: W3.M1, W3.M3). In [3] Hayden (McGi) and collaborators present a new protocol for quantum broadcast channels based on the fully quantum Slepian-Wolf protocol is presented. The protocol yields an achievable rate region for entanglement-assisted transmission of quantum information through a quantum broadcast channel that can be considered the quantum analogue of Marton's region for classical broadcast channels. The protocol can be adapted to yield achievable rate regions for unassisted quantum communication and for entanglement-assisted classical communication. Regularized versions of all three rate regions are provably optimal.

7.1.2 General results on quantum informatic resources

7.1.2.a (Objectives: W1.O1, W1.O2, W3.O2; Milestones: W1.M4, W1.M6). Given a collection of states $(\rho_1, ..., \rho_N)$ with pairwise fidelities $F(\rho_i, \rho_j) \leq F < 1$, Harrow (Bris) and Winter (Bris) show in [4] the existence of a POVM that, given $\rho_i^{otimesn}$, will identify i with probability $\leq 1 - \epsilon$, as long as $n \leq 2(logN/\epsilon)/log(1/F)$. This improves on previous results which were either dimension-dependent or required that i be drawn from a known distribution.

7.1.2.b (Objectives: W2.O2, W2.O3, W2.O4, W3.O1, W3.O2; Milestones: W2.M3, W3.M4). In [5] Smith (Bris), Smolin, and Winter (Bris) present an upper bound for the quantum channel capacity that is both additive and convex. Our bound can be interpreted as the capacity of a channel for high-fidelity communication when assisted by the family of all channels mapping symmetrically to their output and environment. They also indicate an analogous notion for distilling entanglement using the same class of (one-way) channels, yielding one of the few genuinely 1-LOCC monotonic entanglement measures.

7.1.2.c (Objectives: W3.O1, W3.O2; Milestones: W3.M4, W3.M4). In [6] Hayden (McGi), Winter (Bris) and co-authors give a proof that the coherent information is an achievable rate for the transmission of quantum information through a noisy quantum channel. Their method is to select coding subspaces according to the unitarily invariant measure and then show that provided those subspaces are sufficiently small, any data contained within them will with high probability be decoupled from the noisy channel's environment.

7.1.2.d (Objectives: W3.O1, W3.O2; Milestones: W3.M4). In [7] Hayden (McGi), Winter (Bris) and co-authors use random Gaussian vectors and an information-uncertainty relation to give a proof that the coherent information is an achievable rate for entanglement transmission through a noisy quantum channel. The present proof is distinguished from other approaches in that it is shown that the classical information in two Fourier-conjugate bases of the code subspace can be recovered at the output. Application of a recent information-uncertainty relation then ensures that the quantum information in the subspace can in fact be decoded.

7.1.2.e (Objectives: W2.O1, W2.O2, W2.O3, W2.O4, W3.O1, W3.O2; Milestones: W2.M1, W2.M3 W3.M5, W3.M4). In [8] Winter (Bris) and co-authors consider a quantum state shared between many distant locations, and define a quantum information processing primitive, state merging, that optimally merges the state into one location. As announced in [Horodecki, Oppenheim, Winter, Nature 436, 673 (2005)], the optimal entanglement cost of this task is the conditional entropy if classical communication is free. Since this quantity can be negative, and the state merging rate measures partial quantum information, they find that quantum information can be negative. The classical communication rate also has a minimum rate: a certain quantum mutual information. State merging enabled one to solve a number of open problems: distributed quantum data compression, quantum coding with side information at the decoder and sender, multi-party entanglement of assistance, and the capacity of the quantum multiple access channel. It also provides an operational proof of strong subadditivity. Here, they give precise definitions and prove these results rigorously.

7.1.2.f (Objectives: W1.O2, W1.O4, W3.O2; Milestones: W1.M4). In [9] Montanaro (QICS postdoc at Bris) gives a lower bound on the probability of error in quantum state discrimination in terms of a weighted sum of the pairwise fidelities of the states to be distinguished.

7.1.2.g (Objectives: W1.O1, W1.O2, W1.O3, W3.O1; Milestones: W1.M4, W1.M6). In [10] Montanaro (QICS postdoc at Bris) and Winter (Bris) prove a general lower bound on the bounded-error entanglement-assisted quantum communication complexity of Boolean functions. The bound is based on the concept that any classical or quantum protocol to evaluate a function on distributed inputs can be turned into a quantum communication protocol. As an application of this bound, we give a very simple proof of the statement that almost all Boolean functions on n+n bits have linear communication complexity, even in the presence of unlimited entanglement.

7.1.2.g (Objectives: W1.O2, W1.O3, W3.O1; Milestones: W1.M4). In [11] Markham (QICS postdoc at Paris) has presented a general geometric approach to state discrimination in QM. It is expected that this approach will be useful for studies of channel capacities, error correction and measurement based quantum computing.

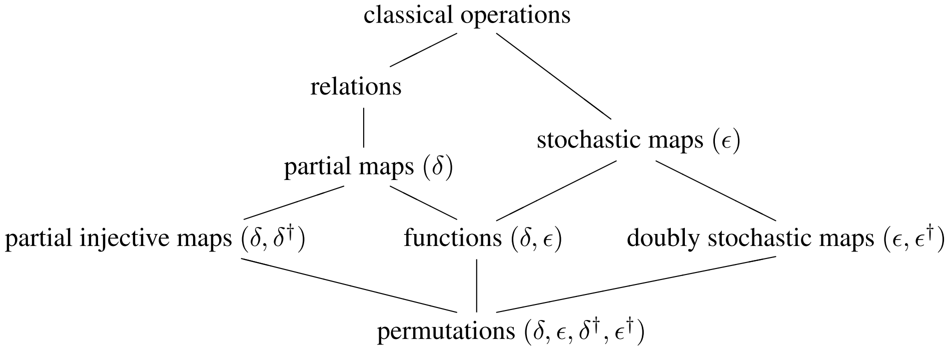
7.2 Progress towards objectives and performed tasks for W3.T2

7.2.1 Compositional accounts on information flow

7.2.1.a Axiomatics for no-cloning and no-deleting (Objectives: W3.O2, W3.O3; Milestones: W3.M5, W3.M6). In [12] Abramsky (Ox) and Coecke (Ox) use the categorical framework to give a new perspective on the axiomatics of No-Cloning. As already mentioned, given a choice of basis, operations for 'copying' and 'deleting' can be defined. However, these operations are basis-dependent; and in fact, it can be shown that *uniform* copying and deleting operations are incompatible with quantum structure (compact closure). Mathematically, a uniform copying operation means a *natural diagonal* $\Delta_A : A \to A \otimes A$, while uniform deleting means a natural transformation $A \to \mathrm{I}$. We have shown that in either case 'the category trivializes'; in other words, that this combination of quantum and classical features is 'inconsistent'. These results are in the same genre as (but proved quite differently to) a well-known result by Joyal in Categorical Logic showing that a "Boolean cartesian closed category" trivializes, which provides a major road-block to the computational interpretation of classical logic. There is an intuitive corresponding purely topological argument to the categorical one.

7.2.1.b Structural resources required to discriminate between classical and quantum structures (Objectives: W3.O1, W3.O4; Milestones: W3.M1, W3.M4, W3.M5, W3.M6). See **6.1.b** [13].

7.2.1.c Classical structures from abstract tensorial structures (Objectives: W3.O1, W3.O4; Milestones: W3.M1, W3.M4, W3.M5, W3.M6). In [14, 15] Coecke (Ox), Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) and Pavlovic (Ox) also build further on the work discussed in **6.1.b** above. They show that from the structure of the dagger-compact Frobenius algebras, in the case of the category **FdHilb**, several familiar classical concepts arise in terms of preservation properties with respect to the copying operation δ and the deleting operation ϵ. These are:


classical operations
relations
stochastic maps (ϵ)
partial maps (δ)
partial injective maps ($\delta, \delta^\dagger$)
functions (δ, ϵ)
doubly stochastic maps ($\epsilon, \epsilon^\dagger$)
permutations ($\delta, \epsilon, \delta^\dagger, \epsilon^\dagger$)

In [16] Coecke (Ox) and Paquette (McGi affiliated & forthcoming QICS postdoc at Ox) provide a tutorial introduction which should provide sufficient background for the physicsists in order to read the more technical papers in this area.

7.2.2 Information flow on one-way computing

7.2.2.a (Objectives: W3.O1, W3.O5; Milestones: W1.M6, W2.M6). In [17], Kashefi (Ox & Gren), studied the question of forward and backward translation between measurement-based computing and quantum circuit computation. It is known that the class of patterns with a particular properties, having flow, is in one-to-one correspondence with quantum circuits. However the paper showed that a more general class of patterns, those having generalised flow, will sometime translate to imaginary circuits, cyclic circuits that are not runable. On the other hand since a pattern with generalised flow implements a well-defined and executable quantum operator one might be able to rewrite the obtained imaginary circuit into an equivalent acyclic circuit. The paper proposed such a complete rewriting system that transforms a particular class of imaginary circuits coming from well-defined MBQC patterns into a runnable equivalent circuit.

7.2.3 Foundational results on the classical-quantum data (processing) relation

7.2.3.a A generalised Gottesman-Knill theorem (Objectives: W1.O1, W1.O2, W1.O3, W3.O2, W1.O4; Milestones: W1.M2, W1.M4, W3.M4). Quantum computations that involve only Clifford operations are classically simulable despite the fact that they generate highly entangled states; this is the content of the Gottesman-Knill theorem. In [19] Clark (Bris), Jozsa (Bris), and Linden (Bris) isolate the ingredients of the theorem and provide generalisations of some of them with the aim of identifying new classes of simulable quantum computations.

7.2.3.b Interpretation of measurement data in weak measurements (Objectives: W1.O1, W3.O2; Milestones: W3.M4). In [20] Jozsa (Bris) derive a physical interpretation of the weak value of any observable in terms of the shift in the measurement pointer's mean position and mean momentum. In particular he demonstrates that the mean position shift contains a term jointly proportional to the imaginary part of the weak value and the rate at which the pointer is spreading in space as it enters the measurement interaction.

7.2.3.c Classical simulation Shor's factoring algorithm (Objectives: W1.O1, W3.O2; Milestones: W1.M4, W1.M5, W1.M6, W3.M4). In [21] Yoran (Bris) and Short (Bris) show that a classical algorithm efficiently simulating the modular exponentiation circuit, for certain product state input and with measurements in a general product state basis at the output, can efficiently simulate Shor's factoring algorithm. This is done by using the notion of the semi-classical Fourier transform due to Griffith and Niu, and further discussed in the context of Shor's algorithm by Browne.

7.2.3.d A classical constant time factoring realisation? (Objectives: W1.O1, W3.O2; Milestones: W3.M4). Factorization is notoriously difficult. Though the problem is not known to be NP-hard, neither efficient, algorithmic solution nor technologically practicable, quantum-computer solution has been found. In [22, 23] Blakey (Ox) presents an analogue factorization system. The systems complexity is prohibitive of its factorizing arbitrary, natural numbers, though the problem is mitigated when factorizing n = pq for primes p and q of similar size. Ultimately, though, we argue that the systems polynomial time and space complexities are testament not to its power, but to the inadequacy of traditional, Turing-machine-based complexity theory; we propose precision complexity [24] as a more relevant measure.

7.2.4 Classical limit

7.2.4.a The classical limit of quantum broadcasting (Objectives: W3.O2, W3.O3; Milestones: W3.M4). In [18] Walker and Braunstein (York) quantify the resolution with which any probability distribution may be distinguished from a displaced copy of itself in terms of a characteristic width. This width, which they call the resolution, is well defined for any normalizable probability distribution. they use this concept to study the broadcasting of classical probability distributions. Ideal classical broadcasting creates two (or more) output random variables each of which has the same distribution as the input random variable. they show that the universal broadcasting of probability distributions may be achieved with arbitrarily high fidelities for any finite resolution. By restricting probability distributions to any finite resolution they have therefore shown that the classical limit of quantum broadcasting is consistent with the actual classical case.

7.2.5 Coalgebraic structures

7.2.5.a Categorical semantics for a call-by-value linear lambda calculus (Objectives: W3.O1, W3.O4, W3.O4; Milestones: W3.M6). In [25] Selinger (McGi affiliated) and Valiron (McGi affiliated) 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 Moggis computational lambda calculus. It is this combination of a monad and a comonad that makes the present paper interesting. They show that our categorical semantics is sound and complete.

7.2.5.b Quantum observables as dagger Eilenberg-Moore coalgebras (Objectives: W3.O5; Milestones: W3.M6). See 6.1.b [13].

7.2.5.c Complementary quantum observables as bialgebras (Objectives: W3.O5; Milestones: W3.M6). See 6.1.c [26].

Bibliography

[1] A. Abeyesinghe, I. Devetak, P. Hayden and A. Winter (2006) The mother of all protocols: Restructuring quantum information's family tree. arXiv:quant-ph/0606225

[2] F. Dupuis and P. Hayden (2006) A father protocol for quantum broadcast channels. arXiv:quant-ph/0612155v2

[3] D. Avis, P. Hayden and I. Savov (2007) Distributed Compression and Multiparty Squashed Entanglement. arXiv:quant-ph/0612155v2

[4] A. W. Harrow and A. Winter (2006) How many copies are needed for state discrimination? arXiv:quant-ph/0606131

[5] G. Smith, J. A. Smolin and A. Winter (2006) The quantum capacity with symmetric side channels. arXiv:quant-ph/0607039

[6] P. Hayden, M. Horodecki, J. Yard and Andreas Winter (2007) A decoupling approach to the quantum capacity. arXiv:quant-ph/0702005

[7] P. Hayden, P. W. Shor and A. Winter (2007) Random quantum codes from Gaussian ensembles and an uncertainty relation. arXiv:0712.0975

[8] M. Horodecki, J. Oppenheim and A. Winter (2007) Quantum State Merging and Negative Information. Communications in Mathematical Physics, 269 pp. 107-136.

[9] A. Montanaro (2007) A lower bound on the probability of error in quantum state discrimination. arXiv:0711.2012

[10] A. Montanaro and A. Winter (2007) A lower bound on entanglement-assisted quantum communication complexity. In Proc. ICALP'07.

[11] D. Markham, J.A. Miszczak, Z. Puchala and K. Zyczkowski (2008) Quantum state discrimination: a geometric approach. quant-ph/0711.4286

[12] S. Abramsky and B. Coecke (2008) A topological proof for no-cloning and no-broadcasting. To be submitted to PRL.

[13] B. Coecke and D. Pavlovic (2007) *Quantum measurements without sums*. In: Mathematics of Quantum Computing and Technology, G. Chen, L. Kauffman and S. Lamonaco (eds), pages 567–604. Taylor and Francis. arXiv:quant-ph/0608035.

[14] B. Coecke, E. O. Paquette and D. Pavlovic (2008) *Classical structures from tensorial quantum structures*. To appear in: New Structures for Physics, B. Coecke (ed). Springer Lecture Notes in Physics.

[15] B. Coecke, E. O. Paquette and D. Pavlovic (2008) *Classical and quantum structures*. To appear in: Semantic Techniques in Quantum Computation, S. Gay and I. Mackie, Eds. Cambridge University Press.

[16] B. Coecke and E. O. Paquette (2008) *Monoidal categories for the practising physicist*. To appear in: New Structures for Physics, B. Coecke (ed). Springer Lecture Notes in Physics.

[17] E. Kashefi, Lost in Translation, To appear in the proceedings of The 3rd International Workshop on Development of Computational Models, 2007.

[18] T.A. Walker and S.L. Braunstein (2007) *Classical Broadcasting is Possible with Arbitrarily High Fidelity and Resolution*. Phys. Rev. Lett. 98, 080501.

[19] S. Clark, R. Jozsa, and N. Linden (2007) Generalized Clifford groups and simulation of associated quantum circuits. QIC 8, pp0106-0126.

[20] R. Jozsa (2007) Complex weak values in quantum measurement. Phys. Rev. A 76, 044103.

[21] N. Yoran, A. J. Short (2007) Classical simulability and the significance of modular exponentiation in Shor's algorithm. arXiv:0706.0872

[22] E. Blakey (2007) An analogue solution to the problem of factorization. Oxford University Computing laboratory research report CS-RR-07-04.

[23] E. Blakey (2008) Factorizing RSA Keys, an Improved Analogue Solution. To appear in the Proceedings of the Second International Workshop on Natural Computing, Nagoya University - Japan.

[24] E. Blakey (2007) On the Computational Complexity of Physical Computing Systems. Unconventional Computing proceedings pp. 95-115.

[25] P. Selinger and B. Valiron (2008) A linear-non-linear model for a computational call-by-value lambda calculus. To appear in Proceedings of the Eleventh International Conference on Foundations of Software Science and Computation Structures (FOSSACS 2008).

[26] B. Coecke and R. Duncan (2008) *Interacting Quantum Observables*. Submitted to ICALP'08.

Chapter 8

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

A current account of the objectives of W4 and comparison with the state-of-the art. Whereas many of the obstacles encountered on the way to a yet hypothetical quantum computer are physical in nature, the picture of what could or should be built still has to be drawn more sharply. The models studied in workpackage 4 focus on several possible organisations of quantum information processing devices, on the interplay of the quantum and classical sides of information and computation, and on the consequences, due to quantum laws, for the architectures and computational properties of these devices.

From the more fundamental point of view adopted in project QICS, the approaches to these questions in workpackage 4 show a potentially fruitful duality. On the one side, a number of approaches follow a path from physics to computer science, considering abstracted models of quantum physical systems, for studying under which conditions these systems can exhibit computationally relevant behaviors. This is the case, for example, with the new results about computational universality of quantum cellular automata in task W4.T2, and with the new links that have been established in task W4.T3 between graphs which specify the entangled states underlying measurement based quantum computations, and undecidable logic theories.

In the other direction, riding from computer science to physics amounts to starting from an abstract model of what computations are, and aiming at understanding how the contraints imposed by the laws of quantum physics can be enforced into the operations and the mathematical semantics of the model. This path is successfully followed in task W4.T1 for the design of classically controlled quantum Turing machines and their instantiation in the form of measurement-based quantum Turing machines. An analogous approach holds in tasks W4.T3 and W4.T4, for the study of quantum lambda calculi and functional quantum languages, for the design of a general quantum calculus, for the definition of mathematical domains for the denotational semantics of quantum programming languages, and for the design of quantum process calculi where, for example, the linearity of quantum mechanics has led to a redefinition of what communications are.

Relevant contributors in this area are QICS-affiliates; hence QICS *is* the moving state-of-the-art for the topics in W4.

Main developments in W4. By studying several forms of abstract models of what quantum information processing devices can or should be, workpackage 4 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 :

- Tasks W4.T1 and W4.T3 have developed new and general models for quantum computations under classical control, i.e. have contributed to objective W4.O1. The design of a classically-controlled Turing machine (CQTM) has been completed in task W4.T1. This model is significantly simpler than Deutsch's quantum Turing machine, it incorporates in a natural way both unitary operations and measurements, and it can be specialized into a pure measurement-based quantum Turing machine, thus establishing a link with the work in workpackage W1. Milestone W4.M1 has yet to be completed for the application of the CQTM to characterizing classical+quantum computational complexity. The general quantum calculus developed in task W4.T3 has been inspired in its form by the measurement calculus of workpackage W1. It incorporates both unitaries and projective measurements and, following Selinger's QPL, it has a clean and well defined denotational semantics based on density matrices. To what extent such a formal system can be put to use for the specification and transformation of quantum programs is still an open issue, to be completed for achieving milestone W4.M3.

- Both the classically-controlled Turing machine and the quantum calculus mentioned above cover situations where quantum computations operate under the control of a classical device. Objective W4.O2 aims at a broader understanding of control structures for QC. This is why purely quantum computations, including control, are considered. In task W4.T1, this is studied in a very broad setting of arbitrary systems with a notion of discrete causality, and generalised to the quantum-mechanical case. In task W4.T3, the study of discrete evolving physical systems with a guaranteed notion of termination gives rise to descriptions of these systems in order-theoretic terms, which are then interpreted computationally, via the Curry-Howard 'proofs as programs' isomorphism. These results constitute significant first steps toward milestone W4.M6.

- With respect to the issues mentioned above related to objective W4.O2, quantum cellular automata (QCA) also implement a purely quantum form of control, in addition to being a natural way to approach the merging of computational and spatio-temporal notions within a single model of QIC, as formulated in objective W4.O4. Task W4.T2 is essentially devoted to studying the computational properties of QCA. A number of results have been obtained that decisively contribute to answering questions of unitarity and universality of QCA as set by objective W4.O3: an algebraic criteria for deciding the unitarity of one-dimensional QCA has been found, a universal one-dimensional QCA capable of simulating all others has been described, and it has been proved that one-dimensional QCA always admit a two layered block representation and that their inverse is also a QCA. This last result came as a major surprise, since such a property does not hold for classical CA. A proof that every QCA can be put in the form of a tiling of more elementary, finite dimensional unitary evolutions, has also led to a most welcome, clear and robust definition of n-dimensional QCA, phrased in the traditional setting of Hilbert spaces.

- Computational models considered in task W4.T3 are inspired by their classical counterparts: lambda calculi, formal systems and languages for specifying computations in imperative and functional styles, with operational and denotational semantics, typing systems and other semantic tools. The main issue is, by far, the design of quantum-adequate semantics, both operational and denotational, while preserving expressive power for the model. For that, at this early stage, the full exploration of several distinct approaches is a methodological necessity. A higher order linear algebraic lambda calculus has been designed, the operational semantics of which comply with the linearity of quantum mechanics by applying a set of simple rewrite rules which have been proved confluent. The language QML, also developed in task W4.T3, has the significant advantage over the previous one of a semantic domain directly built upon quantum objects and operations, but is restricted to first order. A translator from QML to quantum gate networks has recently been implemented. In a first attempt to take into account entanglement as a specific properties of quantum data, a typing system system has been defined for reflecting separability, and an abstract interpretation scheme has been designed for static analysis of the evolution of entanglement along computations. A hierarchy of denotational semantics have been defined for a simple quantum imperative language, and remarkable progress in the study of semantics for languages giving access to quantum resources has been made by relying upon the abstract setting of dagger compact categories with biproducts. All of these are exploratory promising contributions to objective W4.O5. Milestone W4.M2 can be considered as achieved, and milestone W4.M7 still appears as an ambitious goal, since higher order and denotational semantics seem difficult to accomodate together.

- Task W4.T3 also contributes to introducing logics within quantum computational models. An original and very interesting connection, which fits well within both objectives W4.O1 and W4.O6, and is an unexpected addition to milestone W4.M3, has been established between measurement-based quantum computations with graph states and the field of mathematical logic, showing that the computational power of graph states is reflected in the expressive power of classical formal logic languages defined on the underlying mathematical graphs. This also relates to activities in workpackage W1 on one-way quantum computation.

- Theories and techniques for analysis and verification of concurrent classical+quantum systems are studied in task W4.T4 and contribute to objective W4.O6. Here again, like in the study of imperative or functional quantum computational models in task W4.T3, inspiration has come from classical abstract models of concurrency and communication. The goal is the design of tools for the specification and verification of distributed computations and protocols involving both classical and quantum data and operations. The chosen approach has gone through the design of quantum process calculi and the definition of their semantics. This has been completed satisfactorily, mostly with the design of two process calculi, each putting forward a distinct important semantic feature: CQP, which relies upon an elaborate typing system for enforcing no-cloning of quantum states among distinct processes, and QPAlg, for which a semantic equivalence has been defined among processes, thus showing an unexpected but apparently intrinsic difficulty of this enterprise, since no such equivalence has been found yet which is a congruence for the parallel composition operator of the process calculus. This indicates that milestone W4.M8 is still an ambitious goal to reach because of the obstacles facing the definition of a congruence among processes. A model checker for the analysis of quantum protocols is also being implemented and experimented, thus significantly contributing to milestone W4.M5.

The next steps to take. At this early stage, a number of challenging issues remain open questions in workpackage W4: understand all the facets of the classical vs. quantum control issue (objectives W4.O1, W4.O2, W4.03 and W4.O4, milestones W4.M4 and W4.M6), give a satisfactory account of irreversibility and complexity in QCA (objective W4.03, milestone

W4.M4), establish theoretical grounds for systematic construction and manipulation of quantum+classical information processing tasks (objectives W4.O1 and W4.O5, milestones W4.M3 and W4.M7), find equivalence and compositional techniques for proofs of distributed quantum systems (objective W4.O6, milestone W4.M8), etc. As stated above, the work accomplished so far in workpackage W4 firmly paves the road toward reaching satisfactory answers to these questions.

The work accomplished in workpackage W4 also suggests that a motto for the next step is ”unify”. Several notions indeed appear with different shades in various parts of workpackage W4. This is particularly the case for the notion of distributed quantum computation. Computing with QCA is intrinsically a distributed process (task W4.T2), quantum process calculi are abstract models for distributed quantum computations (task W4.T4), and the formal system for reasoning about knowledge views quantum protocols as distributed agents (notice that a tool for actually performing this reasoning has been implemented) (task W4.T4). It is certainly worth looking into the commonalities among these different conceptions of ”distribution”. A similar remark holds for the classical vs. quantum control issue.

In the light of the results already obtained, challenging visions to the future begin to appear. In addition to the circuit model and to measurement-based quantum computation, both present in various ways behind the theories and abstract models developed in workpackage W4, adiabatic quantum computing (AQC) and topological quantum computing (TQC), although computationally equivalent, provide specific approaches to designing new applications and algorithms, introduce new fault-tolerant schemes, suggest different architectures and control structures, require specific means for accommodating classical and quantum computations and call for different measures of complexity. This opens a new territory where theories and abstract models are needed for attacking these issues. The first body of works developed in workpackage W4 give evidence that similar formalisation of the physical schemes of AQC and TQC, will pave the road for wider access to such models and will enrich our techniques in understanding what is quantum computation.

Other major challenges are appearing. For example, the physics to computer science path mentioned in the introduction to workpackage W4 is followed by the work done in task W4.T2 on QCA: how to reach a notion of computational universality from the model of physical quantum systems represented by QCA? Satisfactory answers to this question have been found, in the case of one-dimensional QCA. But the feedback from computer science to physics is now tempting: what does this notion mean, in physics terms? Finally, it is now understood that non-locality and entanglement are distinct notions, that quantum entanglement is a just way to implement non-locality, to some degree. Entanglement has been so far considered as a major quantum computational resource and, as such, it is everywhere present in the models developed in workpackage W4. But wouldn’t it be now more relevant to go one level up, and to explicitly incorporate non-locality, instead of entanglement, in these models?

Interactions with other workpackages and sites. Interactions with other workpackages – most interactions of W4 are with W1 and with W2:

- With W1 - MBQC and the measurement calculus are indeed at the basis of several outcomes of W4: classically-controlled Turing machine with its measurement-based instantiation, used for analysis of minimal resources for MBQC, quantum calculus inspired by measurement calculus, logic associated with the graph states resources of MBQC, formalism for reasoning about knowledge in quantum protocols (extension of measurement calculus).
- With W2 - Both quantum languages developed in W4 have their semantics rooted in the categorical approach to developed in W2. The same holds for the semantics for a call-by value linear lambda calculus developed in W3, which is also closely related with the work done in W4.

Interactions among sites have been productive:

- between the Grenoble and Braunschweig sites, on QCA (co-signed papers published)
- between the Grenoble and Oxford sites, on the quantum calculus, on types for separability and entanglement (co-signed papers in preparation)
- between the Grenoble and Oxford sites, on graph states (co-signed papers published)
- between the Grenoble and Innsbruck sites, on graph states (co-signed paper in preparation)
- between the Grenoble and Oxford/Nottingham sites, on quantum lambda calculus (post-doc in Grenoble)

Philippe Jorrand
Grenoble, February 10, 2008.

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 irrevesible 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 datastructures, 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, irrevesibility 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.

8.1 Progress towards objectives and performed tasks for W4.T1

8.1.a Classically controlled Quantum Turing Machine (Objectives: W4.O1; Milestones: W4.M1). In [1], for modelling a standard situation where quantum computations take place under the control of the classical world, Jorrand (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox) introduce a Classically controlled Quantum Turing Machine (CQTM), which is a Turing machine with a quantum tape for acting on quantum data, and a classical transition function for formalised classical control. In a CQTM, unitary transformations and quantum measurements are allowed. Any classical Turing machine can be simulated by a CQTM without loss of efficiency. Furthermore, any k-tape CQTM can be simulated by a 2-tape CQTM with a quadratic loss of efficiency. In order to compare CQTMs with existing models of quantum computation, it is shown that any uniform family of quantum circuits (Yao 1993) is efficiently approximated by a CQTM. Moreover, any semi-uniform family of quantum circuits (Nishimura and Ozawa 2002), and any measurement calculus pattern (Danos et al. 2004) are efficiently simulated by a CQTM. A Measurement-based Quantum Turing Machine (MQTM) is also introduced, which is a restriction of CQTMs in which only projective measurements are allowed. Any CQTM is efficiently simulated by a MQTM.

8.1.b PhD. thesis Simon Perdrix (Objectives: W4.O1; Milestones: W4.M1, W4.M3). In his doctoral thesis [2], Perdrix (Gren & Paris and QICS postdoc at Ox) studies foundational structures of quantum information processing, considered as a key issue to gain a deeper insight into what quantum computation is in general, its scope and limits. The purpose is to bring theoretical contributions to the physical realisation while minimising the resources of quantum computing. The resources consist of the space and times as well as the size of the operations and the amount of entanglement. This thesis contributes in several ways to minimise resources for recently developed models of quantum computation which open new promising perspectives of physical realisation. These models are the one-way quantum computation and the measurement-only quantum computation. This thesis has also permitted to reduce the resources in time and space necessary for the preparation of some quantum states called graph states. The reduction of the resources requires abstraction and formalisation of quantum computing models which point out the structures of the quantum computing processing. The q-calculus and the classically-controled quantum Turing machines, introduced in this thesis, contribute to this objective. More specific models dedicated to one-way and measurement-only quantum computations are considered as well.

8.1.c Machine semantics (Objectives: W2.O2, W4.O1, W4.O2, W4.O5; Milestones: W2.M4, W4.M1, W4.M6). In [3] Hines (QICS postdoc at York) studies arbitrary systems (computational and physical) with a notion of discrete causality, in domain-theoretic and category-theoretic terms. The set of all descriptions of such a system is studied in detail, using a relation that compares high-level / low-level descriptions. The resulting order theory is shown to be a chain-complete partial order, with a number of additional properties. Using tools based on domain theory, but in a more general setting, a close connection is made with the (particle-style) categorical trace and Girard's resolution formula, which is shown in this setting to be a generalisation of the notion of a supremum in a sublattice. As a sample application, it is shown how the algebraic models of space-bounded Turing machines arise naturally as the suprema of specified sub-lattices, and may be computed in a routine way by the categorical trace. Generalisations of this theory to the quantum-mechanical case are then considered obstacles to a straightforward generalisation are described, and the tools to cope with this are given.

In [4] Hines (QICS postdoc at York) considers the general case, where termination may be partial, or undecidable. The relevant order-theoretic structures corresponding to the intuition of low-level / high-level descriptions of systems with a discrete notion of causality are shown to be, in the general case, Scott domains. A conjecture is presented regarding the class of physical systems that give rise to lambda-models. It is also shown how the configuration set of such physical systems with a notion of causality may be given as the product of 'code' and 'data'. Abstractly this may be considered the construction of labelled transition systems from unlabelled transition systems by means of a quotient. A a particular example, it is shown how the alphabet-state distinction for two-way automata may be recovered in a systematic way. It is also shown how the division of a set of configurations into 'code' and 'data' is not unique rather, the set of all such divisions may also be ordered in a consistent way.

8.2 Progress towards objectives and performed tasks for W4.T2

8.2.a Universal one-dimensional QCA (Objectives: W4.O3, W4.O4; Milestones: W4.T2, W4.M4). In [5], Arrighi (Gren) and Fargetton (Gren) give a one-dimensional quantum cellular automata (QCA) capable of simulating all others. This means 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 efficient and hence does not carry any of the weight of the computation.

8.2.b Unitarity of one-dimensional QCA (Objectives: W4.O3, W4.O4; Milestones: W4.M4). In [6], Arrighi (Gren) provides algebraic criteria for the unitarity of linear quantum cellular automata, i.e. one dimensional quantum cellular automata. These criteria are derived both by direct combinatorial arguments, and by adding constraints into the model which do not change the quantum cellular automata's computational power. The configurations considered have finite but unbounded size.

8.2.c Inverse one-dimensional QCA is a QCA (Objectives: W4.O3, W4.O4; Milestones: W4.M4). In [7], Arrighi (Gren), Nesme (Paris & QICS postdoc Brau) and Werner (Brau) isolate a feature of One-dimensional quantum cellular automata (QCA) which shows a stricking difference with their classical couterparts. One dimensional QCA consist in a line of identical, finite dimensional quantum systems. These evolve in discrete time steps according to a local, shift-invariant unitary evolution. "Local" means that no instantaneous long-range communication can occur. In order to define these over a Hilbert space, the study is restricted to a base of finite, yet unbounded configurations. It is shown that QCA always admit a two-layered block representation, and hence the inverse QCA is again a QCA. This is a striking result since the property does not hold for classical one- dimensional cellular automata as defined over such finite configurations. An example is given of a bijective cellular automata which becomes non-local as a QCA, in a rare case of reversible computation which does not admit a straightforward quantization. It is argued that a whole class of bijective cellular automata should no longer be considered to be reversible in a physical sense. The same two-layered block representation result applies also over infinite configurations, as was previously shown for one-dimensional systems in the more elaborate formalism of operators algebras. The proof given here is simpler and self-contained, and a counterexample QCA in higher dimensions is discussed.

8.2.d Block representation of n-dimensional QCA (Objectives: W4.O3, W4.O4; Milestones: W4.M4). In a submitted work [8], Arrighi (Gren), Nesme (Paris & QICS postdoc Brau) and Werner (Brau) show that every QCA can be put into the form of an infinite tiling of more elementary, finite-dimensional unitary evolutions, i.e. that they can be thought of as a quantum circuit infinitely repeating across space. More precisely they represent an n-dimensional QCA of cell dimension d by an n-dimensional QCA of cell dimension d^2, which admits a $n+1$-layered block representation, thereby generalizing the same result for one- dimensional QCA. Hence this now provides a clear, robust definition of n-dimensional QCA, phrased in the traditional setting of Hilbert spaces.

8.2.e Index theory for one-dimensional QCA (Objectives: W4.O3, W4.O4; Milestones: W2.M3, W4.M4). In work so far disseminated only in the form of invited lectures, Werner (Brau) developed an index theory for 1-dimensional, not necessarily translationally invariant quantum walks and quantum cellular automata. In both cases the index is a number, which can be computed locally anywhere in the system, and classifies walks or automata up to the group of partitioned unitaries. This group is identified at the same time as the connected component of the identity.

8.3 Progress towards objectives and performed tasks for W4.T3

8.3.1 Quantum calculi

8.3.1.a The measurement calculus (Objectives: W4.O1, W4.O2, W4.O6; Milestones: W4.M3). See **5.3.1.a**.

8.3.1.b Confluent linear λ-calculus (Objectives: W4.O2, W4.O5; Milestones: W4.M7). In a submitted work [10], Arrighi (Gren) and Dowek introduce a minimal language combining both higher-order computation and linear algebra. Roughly, this is nothing else than the λ-calculus together with the possibility to make linear combinations of terms $a.t+b.u$. It is shown how to ”execute” this language in terms of a few rewrite rules, and justify these rules through the two fundamental requirements that the language be a language of linear operators, and that it be higher-order. Quantum computation is shown to be easily encoded in this calculus, as well as in other domains such as the interpretation of linear logic. The main result, from a computer science point of view, is the confluence of this calculus.

8.3.1.c Extended λ-calculus (Objectives: W4.O5; Milestones: W4.M2, W4.M3). In [11], Prost (recently joined Gren) proposes an extension to the traditional Lambda-calculus, in which terms are used to control an outside computing device (quantum computer, DNA computer...). Two new binders are introduced: : Nu and Rho. In ”Nu x.M”, x denotes an abstract resource of the outside computing device, whereas in ”Rho x.M”, x denotes a concrete resource. These two binders have properties (in terms of alpha-conversion, scope extrusion, convertibility) that differ from those of the standard Lambda- binder. The potential benefits of this approach is shown by applying it to a quantum computing language in which these new binders prove meaningful. A typing system is defined for this quantum computing framework in which linearity is only required for concrete quantum bits, thus offering greater expressiveness than previous propositions of quantum Lambda calculi.

8.3.2 Quantum semantics

8.3.2.a Domain semantics (Objectives: W1.O1, W4.O1, W4.O5; Milestones: W4.M3). In [9], Jorrand (Gren) and Perdrix (Gren & Paris & QICS postdoc at Ox) introduce a general model of quantum computation, the quantum calculus: both unitary transformations and projective measurements are allowed; furthermore a complete classical control, including conditional structures and loops, is available. Complementary to the operational semantics of this calculus, a pure denotational semantics is defined. Based on probabilistic power domains, this pure denotational semantics associates with any description of a computation in the quantum calculus its action in a mathematical setting. Adequacy between operational and pure denotational semantics is established. Additionally to this pure denotational semantics, an observable denotational semantics is also introduced. Following the work by Selinger, this observable denotational semantics is based on density matrices and super-operators. Finally, an exact abstraction connection is established between these two semantics. These results have been presented at the ICALP workshop on Developments of Computational Models in 2007.

8.3.2.b Semantics for admissible transformations (Objectives: W4.O1, W4.O5; Milestones: W4.M3). Recently Perdrix (Gren & Paris & QICS postdoc at Ox) introduced a semantical domain based on admissible transformations, i.e. multi-sets of linear operators. In order to establish a comparison with existing domains, a simple quantum imperative language (QIL) is introduced, equipped with three different denotational semantics, called pure, observable, and admissible. The pure semantics is a natural extension of probabilistic (classical) semantics and is similar to the semantics proposed by Abramsky. The observable semantics, a la Selinger, associates with any program a superoperator over density matrices. Finally, an admissible semantics which associates with any program an admissible transformation is introduced. These semantics are not equivalent, but exact abstraction or interpretation relations are established between them, leading to a hierarchy of quantum semantics.

8.3.2.c Semantics for admissible transformations (Objectives: W4.O2, W4.O6; Milestones: W4.M2, W4.M5). In [12], as a first step toward a notion of quantum data structures, Perdrix (Gren & Paris & QICS postdoc at Ox) introduces a typing system for reflecting entanglement and separability. This is presented in the context of classically controlled quantum computation where a classical program controls a sequence of quantum operations, i.e. unitary transformations and measurements acting on a quantum memory. This analysis is based on the quantum functional language introduced by Selinger and Valiron.

8.3.2.d Semantics for entanglement (Objectives: W4.O6; Milestones: 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. The exact role of the entanglement is nevertheless not well understood. Since an exact analysis of entanglement evolution induces an exponential slowdown, Perdrix (Gren & Paris & QICS postdoc at Ox) considers approximative analysis based on the framework of abstract interpretation. A concrete quantum semantics based on super-operators 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. These results have been presented at the 2nd QNET workshop in UK.

8.3.2.e Semantics for a call-by-value linear lambda calculus (Objectives: W4.O1, W4.05; Milestones: W4.M2, W4.M7). See **7.2.5.a** [13].

8.3.3 Quantum languages

8.3.3.a PhD. thesis Jon Grattage (Objectives: W4.O1; Milestones: W4.M1, W4.M3). In his doctoral thesis [14], Grattage (Ox affiliated & QICS postdoc at Gren) introduces the language QML, a functional language for quantum computations on finite types. QML exhibits quantum data and control structures, and integrates reversible and irreversible quantum computations. The design of QML is guided by the categorical semantics: QML programs are interpreted by morphisms in the category FQC of finite quantum computations, which provides a constructive operational semantics of irreversible quantum computations, realisable as quantum gates. QML integrates reversible and irreversible quantum computations in one language, using first order strict linear logic to make weakenings, which may lead to decoherence, explicit. Strict programs are free from decoherence and hence preserve superpositions and entanglement. A denotational semantics of QML programs is presented, which maps QML terms into superoperators, via the operational semantics, made precise by the category Q. Extensional equality for QML programs is also presented, via a mapping from FQC morphisms into the category Q.

8.3.3.b Semantics for a simple quantum programming language (Objectives: W4.O1, W4.05; Milestones: W4.M2, W4.M7). In a remarkable M.Sc. dissertation [15] Churchill (Ox) written under Abramsky's (Ox) supervision both operational and denotational semantics for a simple language due to Abramsky was given. He also reworked the whole theory in the abstract setting of dagger compact categories with biproducts, including the computational adequacy results. An account of Quantum Dynamic Logic was also given in this setting, and there were some first steps towards an implementation. This dissertation was awarded a Distinction, and is undoubtedly publishable.

8.3.4 Logic within quantum computational models

8.3.4.a Undecidable logic and measurement-based quantum computation (Objectives: W1.O1, W1.O4, W4.O1, W4.O6; Milestones: W1.M2, W1.M5, W4.M3). In [16] 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.

8.3.4.b A logical approach to engineering ground states in adiabatic quantum computing (Objectives: W1.O1, W2.O1, W2.O2, W4.O1, W4.O2; Milestones: W4.M3, W4.M5). In [17] Jacob D. Biamonte (QICS postdoc at Ox) provided an algebraic and logical approach to engineering the ground states of interacting spin systems. This replaces known methods relying on complicated approximation schemes involving perturbation theory and allows one to reason at a higher level in regards to the construction and development of adiabatic quantum algorithms. We now have a method to capture the ground space of multiple energy level subspaces of the general class of k-body Hamiltonians using only 2-body Hamiltonians. In addition, this work paves the way to help solve several open problems in quantum complexity theory, including a proof of the QMA-completeness of *local Hamiltonian* without the use of perturbation theory (i.e. with constant gap conditions).

8.3.4.c Physical systems as constructive logics (Objectives: W4.O1, W4.O2; Milestones: W4.M3, W4.M6). In [18] Hines (QICS postdoc at York) considers the claim known as Wolfram's 'Principle of Computational Equivalence', that (discrete) systems in the natural world should be thought of as performing computations. He considers discrete evolving physical systems with a guaranteed notion of termination, and axiomatises the notion of low-level / high-level descriptions of such systems in order-theoretic terms. The resulting order theory is special class of Heyting algebras i.e. Lindenbaum-Tarski algebras of intuitionistic logics. This is interpreted computationally, via the Curry-Howard 'proofs as programs' isomorphism.

8.4 Progress towards objectives and performed tasks for W4.T4

8.4.1 Quantum process calculi.

8.4.1.a Process calculus for distributed quantum computing (Objectives: W4.06; Milestones: W4.M2, W4.M8). In her doctoral thesis [19] and in [20], Lalire (member of Gren until end of 2006), has built an abstract model of distributed quantum computations and quantum communication protocols, in the form of a quantum process algebra (QPAlg). QPAlg provides a homogeneous style for formal descriptions of concurrent, distributed and communicating computations involving both quantum and classical resources. Based upon an operational semantics which makes sure that quantum objects, operations and communications operate according to the postulates of quantum mechanics, a semantic equivalence is defined among process configurations (i.e. processes together with the states of their quantum variables and values of their classical variables) considered as having the same behavior. This equivalence is a probabilistic branching bisimulation. From this relation, an equivalence on processes is defined. However, it is found that such relations cannot be congruences for all the operators of the process algebra: it is not preserved for parallel composition, because of entanglement. This is still an open problem: this yet unsolved issue was also encoutered by other, independent approaches to quantum process algebras (e.g. qCCS, by Feng, Duan, Ji and Ying, Information and Computation, 2007).

8.4.2 Reasoning about knowledge in quantum protocols

8.4.2.a Knowledge on quantum states (Objectives: W4.O6; Milestones: W4.M5, W4.M8). Kashefi (Ox & Gren) and Sadrzadeh (Ox affiliated & QICS postdoc at Paris), presented a formal system to reason about knowledge properties of quantum security protocols. The formalism is obtained via a marriage of measurement calculus of Danos-Kashefi-Panangaden with the algebra of epistemic updates of Baltag-Coecke-Sadrzadeh. Reasoning about knowledge of agents after running the protocol is done via unfolding the adjunctions that arise from agent's appearance maps. To present the power of the formalism they encoded and reasoned about sharing and secrecy properties of Ekert'91 and BB'84 key distribution and bit-commitment protocols and showed how to one can derives their corresponding attacks. They presented this work at several conferences, have extended abstracts on it and a journal paper is in preparation. Preliminary results by Sadrzadeh (Ox affiliated & QICS postdoc at Paris) are already available in [21].

8.4.3 Tools for verification

8.4.3.a QMC: A Model Checker for Quantum Systems (Objectives: W4.O6; Milestones: W4.M5, W4.M8). Gay (Ox affiliated), Nagarajan (Ox affiliated) and Papanikolaou (Ox affiliated) introduce a model-checking tool intended specially for the analysis of quantum information protocols. The tool incorporates an efficient representation of a certain class of quantum circuits, namely those expressible in the so-called stabiliser formalism. Models of protocols are described using a simple, imperative style simulation language which includes commands for the unitary operators in the Clifford group as well as classical integer and boolean variables. Formulas for verification are expressed using a subset of exogenous quantum propositional logic

(EQPL). The model-checking procedure treats quantum measurements as the source of non-determinism, leading to multiple protocol runs, one for each outcome. Verification is performed for each run.

8.4.3.b `Aximo`**: A tool to reason about knowledge on quantum states (Objectives: W4.O6; Milestones: W4.M5, W4.M8).** In [23] Sadrzadeh (Ox affiliated & QICS postdoc at Paris) and her MSc student presented an automated reasoner which implements the theory of **8.4.2.a**: a program called Aximo, written in C++, which is now on-line available at [24].

Bibliography

[1] S. Perdrix and Ph. Jorrand. Classically-controlled quantum computation. Mathematical Structures in Computer Science, 16:601-620, 2006.

[2] S. Perdrix. Modèles formels du calcul quantique : ressources, machines abstraites et calcul par mesure. Ph.D. thesis, Institut National Polytechnique de Grenoble, Laboratoire Leibniz, Dec. 2006.

[3] P. Hines (2008) Machine Semantics. To appear in Theoretical Computer Science.

[4] P. Hines (2008) From causality to computational models. International Journal of Unconventional Computation 4(2), 1-26.

[5] P. Arrighi and R. Fargetton. Intrinsically universal one- dimensional quantum cellular automata, DCM'07, Wroclaw 2007. Pre- print arXiv:/0704.3961. Open session of MCU'07, Orlans, July 2007.

[6] P. Arrighi. An algebraic study of unitary linear quantum cellular automata, Proceedings of MFCS 2006, LNCS 4162, 122133, 2006.

[7] P. Arrighi, V. Nesme and R.F. Werner. One-dimensional quantum cellular automata upon finite, unbounded configurations. In Proceedings LATA'08, to appear in LNCS, Springer, 2008. Pre-print arXiv:0711.3517.

[8] P. Arrighi, V. Nesme and R.F. Werner. N-dimensional quantum cellular automata, Sent to STOC'08, Pre-print arXiv:0711.3975.

[9] Ph. Jorrand and S. Perdrix. Towards a quantum calculus. In Proceedings of the 4th International Workshop on Quantum Programming Languages, ENTCS, July 2006.

[10] P. Arrighi and G. Dowek. Linear-algebraic Lambda-calculus: higher-order and confluence. Submitted to RTA'08.

[11] F. Prost. Taming Non-Compositionality Using New Binders. In Proceedings of Unconventional Computation 2007 (UC'07), Lecture Notes in Computer Science, Vol. 4618, Springer, 2007.

[12] S. Perdrix. Quantum patterns and types for entanglement and separability. In Proceedings of the 3rd International Workshop on Quantum Programming Languages (QPL 2005), ENTCS, volume 170, pages 125-138, 2007.

[13] P. Selinger and B. Valiron (2008) A linear-non-linear model for a computational call-by-value lambda calculus. To appear in Proceedings of the Eleventh International Conference on Foundations of Software Science and Computation Structures (FOSSACS 2008).

[14] J. Grattage (2006) QML: A functional quantum programming language. Ph.D. thesis University of Nottingham.

[15] M. Churchill (2007) Abstract semantics for a simple quantum programming language. Dissertation for the M.Sc. in Mathematics and the Foundations of Computer Science, Oxford University.

[16] M. Van den Nest, H. J. Briegel, Measurement-based quantum computation on graph states and undecidable logic theories, arXiv.org:quant-ph/0610040 (2006)

[17] J.D. Biamonte, Non-perturbative k-local to 2-local conversion Hamiltonians and embedding problem instances into Ising spins, submitted to PRA (2008), preprint: http://arxiv.org/abs/0801.3800

[18] P. Hines (2006) Physical systems as constructive logics. Springer LNCS 4135, 101-112.

[19] M. Lalire. Developpement d'une notation algorithmique pour le calcul quantique. Ph.D. thesis, Institut National Polytechnique de Grenoble, Laboratoire Leibniz, Oct. 2006.

[20] M. Lalire. Relations among quantum processes: bisimilarity and congruence. Mathematical Structures in Computer Science, 16:407-428, 2006.

[21] M. Sadrzadeh (2007) High-Level Quantum Structures in Linguistics and Multi-Agent Systems. Proceedings of AAAI Spring Symposium on Quantum Interaction. AAAI Press.

[22] S. J. Gay, N. Papanikolaou and R. Nagarajan (2007) QMC: a model checker for quantum systems. Research Report 432, Department of Computer Science, University of Warwick. arXiv:0704.3705

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

[24] S. Richards and M. Sadrzadeh, The actual `Aximo` tool is available at: http://eprints.ecs.soton.ac.uk/14909/

Part IV

Consortium management

Meetings of the consortium management group

Physical meetings held so far:

- The first meeting of the QICS heads of sites took place at Cats, Kets and Cloisters in July 2006. (see Chapter 4 entitled **"QICS events and presentations."**) Issues discussed included the organisation of QICS events e.g. we decided that the first workshop would be held in March 2007 in Oxford and that the first major QICS event would be organised by Innsbruck. (see Chapter 4 entitled **"QICS events and presentations."**) We also discussed how to improve interaction between communities, resulting in the decisions reported on in Section 2.2 entitled **"Trans-disciplinary efforts."** Explorative discussions took place on which hirings QICS needed to make, resulting in the decisions reported on in Chapter 3 entitled **"Recruitment and mobility."**

- The second meeting of the QICS heads of sites took place at the 1st QICS workshop. Important decisions involved the format of the first set of QICS deliverables (this report), the location of the second QICS workshop, and the format of the first major QICS event. A very important issue was the problem with recruiting appropriately skilled QICS postdocs. As a consequence a joint effort was made to explore which students w ere due to finish PhD's soon and hence would become available for QICS; as mentioned in Section 3.1 entitled **"Recruitment."** these problems have now been successfully dealt with. We also discussed dissemination of reports via webpage: the simplest and most effective solution is just to make the reports publicly available as .pdf files on the QICS website rather than spending amounts of money or time on a sophisticated webpage.

QICS postdocs

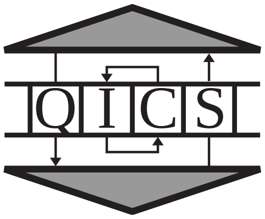
In Section 3.1 entitled **"Recruitment."** we reported on our initial problem of hiring QICS postdocs. Therefore the coordinating site carefully screened the academic job market to obtain a good overview about the people available for hiring. We performed many interviews and communicated the results to our partners. Out of these interviews, several people have meanwhile been hired by QICS sites: Perdrix in Oxford, Nesme in Braunschweig, Grattage in Grenoble, Degorre in Grenoble, Sadrzadeh in Paris, Patra will be hired in York, and Paquette will be hired in Oxford. Now we have the staff required to reach our objectives lined up; this exactly matches the initially requested resources.

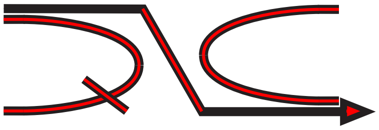
Project timetable and status

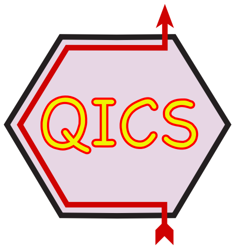
These are reported on in **"The next steps to take."** in the introduction to each of the workpackges i.e. Chapters 5–8.

QICS logo

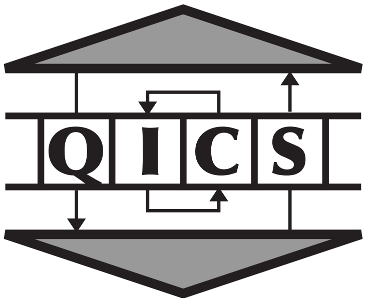
Designing a QICS logo was a joint effort. Several designs were put forward of which those which got backing from more than one site were







respectively designed by Werner's group in Braunschweig, Braunstein in York and the QICS co-ordinator in Oxford. While the York design got strong backing from Grenoble and the Oxford design got backing from Bristol, the Braunschweig design had the majority of the votes; the QICS logo now is:



which elegantly combines the idea of a Turing machine with some key elements of diagrammatic quantum calculus.

Important information on the CNRS Grenoble site with FCF cost model

Person-months as initially planned in 2007, 2008 and 2009:

- 26 p-m in 2007
- 27 p-m in 2008
- 27 p-m in 2009

Person-months actually invested in 2007, planned in 2008 and 2009:

- 19 p-m in 2007 (10 p-m's on W1, 9 p-m's on W4, approx)
- 37 p-m in 2008 (the balance will be strongly in favor of W4, due to the two post-docs)
- 24 p-m in 2009

In spite of the difference of 7 months in 2007 (26 p-m's planned, 19 p-m's actually invested) the total number of p.ms to be invested by CNRS-Grenoble over the 3 years of QICS will remain the same (80). Reasons for the differences in 2007:

- Philippe Jorrand retired on September 1st, 2007
- Elham Kashefi hired on October 8th, 2007
- Jonathan grattage hired as a post-doc on September 1st, 2007 (for 18 months). No post-doc with a scientific profile adequate to the tasks at CNRS-Grenoble was found before Jonathan Grattage got his PhD in Nottingham (in July 2007), and became available as a post-doc on September 1st, 2007.

For the total number of p-ms to remain the same at the Grenoble site, we request that the amount corresponding to 7 post-doc p-ms in 2007, which was actually not spent in 2007, be transfered to 2008, i.e. the total payment to CNRS-Grenoble over the duration of QICS remains as initially planned.

Annex:
Plan for using and disseminating the knowledge

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