QICS - PERIODIC ACTIVITY REPORT III

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

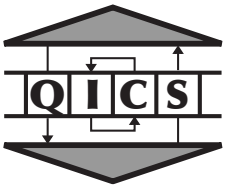
Thematic priority: Quantum Information Processing and Communications

Period covered: Jan. 1st 2009 – Aug. 7th 2010

Date of preparation: Aug. 7th 2010

Start date of project: Jan. 1st 2007

Duration: 42 months



Contents

Part I

Publishable executive summary

Third year of QICS – executive account

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

It is our pleasure to report on an again very successful and exciting 3rd period of QICS research, which due to the extension recommended and granted after the 2nd review, now lasted 18 months. The ultimate goal of QICS, as stated in the initial proposal, is to radically increase our understanding of the foundational structures of quantum informatics, as part of a cross-disciplinary endeavour, involving,

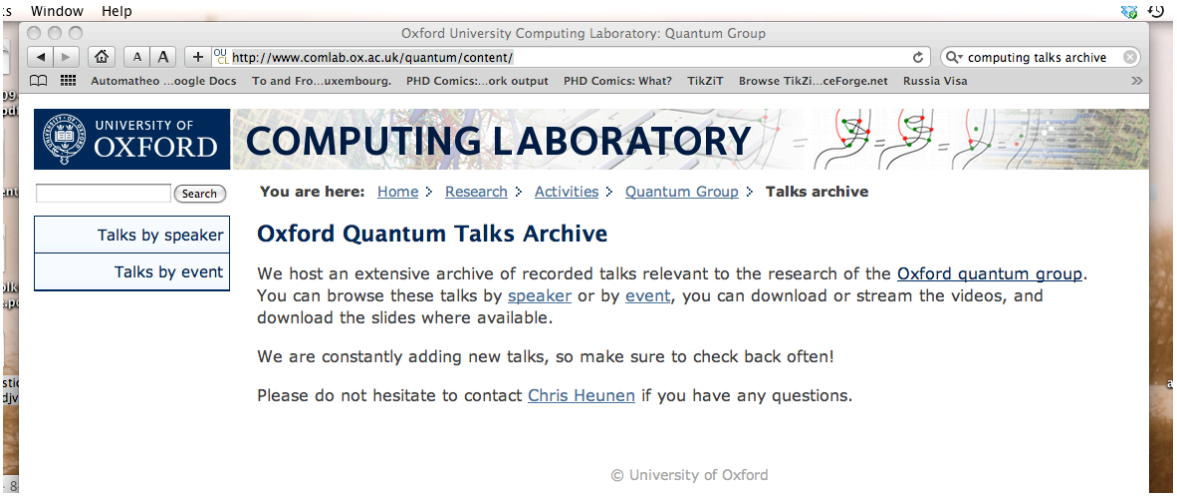
- *physicists* who are challenging the boundaries of nature's capabilities by studying novel quantum computational models such as measurement based quantum computational schemes and quantum cellular automata, mainly in Hannover and Innsbruck,
- *logicians* who adopt novel structural tools such as category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

The goal of this extension was to explore some very exciting new synergies which had emerged during the 2nd period of the QICS project. We report on the results of these efforts below.

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

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

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

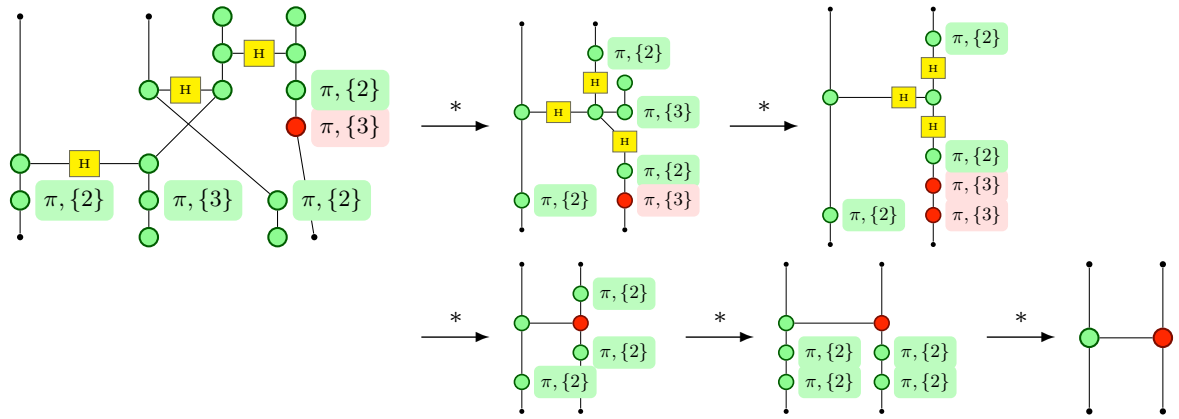


More details are in Section 3 of the 3rd QICS report.

The workpackage on *structures and methods for measurement-based quantum computation* [**W1**] has continued to be a fascinating platform for theoretical and experimental investigations of quantum computation. A concise updated review by QICS members was published in *Nature Physics* in January 2009.

A central question in the field of quantum compution is to what extent a quantum computer is more powerful than a classical computer. One possibility to address this question is to consider the classical simulation of quantum computation and ask: Which classical resources are required for this simulation? Within the QICS W1 activity this question has been addressed and answered for certain types of quantum computations. A central goal of the QICS project is an improved understanding of the structures of MBQC. This will help to devise new algorithms for MBQC, furthermore, it will shed light on the relation between MBQC and the network model of quantum computation. In the last period of QICS a number of relevant results have been obtained. Highlights include the investigation of so-called "universal blind computation", which have resulted in solving an open problem in complexity theory (see also W4 below); the QICS team was in fact awarded prize money for that, by Scott Aaronson. The development of the above protocol for blind quantum computation led to the development of fundamental results for interactive proof systems. It is shown that QMIP=MIP* which means that in the setting of multiple provers with shared entanglement, a quantum verifier is no more powerful than a classical one.

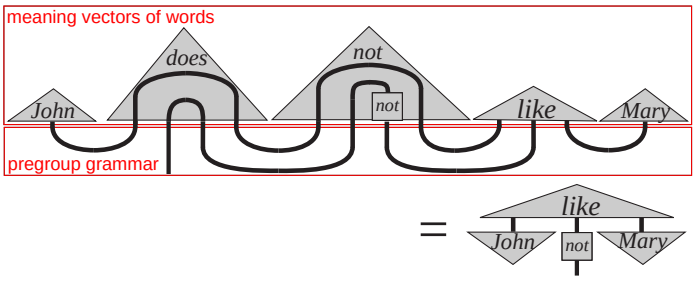
A central aim of the QICS project was the usage of categorial methods to understand MBQC from a new perspective. In the last period, significant success in this direction has been made. For instance, using a diagrammatic formalism some central theorems concerning the entanglement properties of graph states could be formalized and understood.



This brings us to the second workpackage, on *categorical semantics, logics and diagrammatic methods* [**W2**]. At the prestigious ICALP conference which traditionally accepts a number of outstanding papers in the area of quantum computation, this year two out of three accepted quantum computing papers are a result of this workpackage One of these provides an algebraic characterization of three qubit entanglement as well as a compositional account on general multipartite qubit entanglement – multipartite quantum states constitute a (if not the) key resource for quantum computations and protocols. We expect that this work will lead to a generalized graph state paradigm, hence feeding back into W1.

Several survey paper and two books with surveys and tutorials on W2 QICS research were produced, *New Structures for Physics*, and *Semantic Techniques for Quantum Computation*.

W2 has meanwhile led to spin-off in two very actual CS areas, namely compositional linguistics and automated theory exploration, resulting in currently finalized multi-side proposals with world-leading groups. The automated theory exploration activity grew out of the development of the `quantomatic` software. The computational linguistics activity grew out of the realization that quantum information flows can be used to compute how meaning of words in sentences propagates, when representing meaning by the standard vector space-based distributional model.



W3 has been exceptionally successful this term. QICS researchers have introduced modifications to the standard theory of quantum mechanics and studied the computational power of these theories—as well as their mathematical structure—to cast light on the origins and limitations of quantum information processing. These modifications range from simple restrictions on the set of gates allowed in a quantum circuit, to esoteric non-local "post-quantum" theories. Most notably is the notion *information causality*.

QICS researchers have also produced a large body of work dealing with the internal limitations of quantum information processing. These limitations express themselves in terms of the channel capacities obtained when using quantum resources to transmit classical information, to quantum channel capacities and efficiency at carrying computational tasks such as simulating quantum measurements.

As well this theoretical activity, this work package also encompasses a number of more practically oriented investigations. We highlight here the development of new quantum algorithms, novel techniques for establishing private information, and the 'final' graphical calculus for quantum-classical interaction via a formalization of the concept of 'environment'. The latter results in coinciding formal semantics for classical channel and measurement, all in terms of certain Frobenius algebras:

We mention also the involvement of QICS postdocs in a number of experiments to test quantum non-contextuality.

QICS workpackage W4 on *quantum automata, machines and calculi* produced a variety of results that is to broad to summarize. We just pick some. This year has unraveled several fruitful connections between randomness and QIP. For instance it was shown that the knowledge of a probability distribution on the location of an element in an unstructured list can be fruitfully exploited to obtain a significant speed up of the Grover algorithm. More importantly, there is a clear benefit in using quantum algorithms to test properties of probability distributions. This could be an important contribution; in terms of finding new quantum algorithms; but also as a novel way to phrase quantum computation in general.

It was also shown that if one can efficiently simulate on a classical device a quantum computer restricted to commuting gates, then the polynomial hierarchy would collapse to its third level. There were numerous such interesting results on QCAs: e.g. that there exists classical dynamics which transport information faster in the quantum regime than in the classical regime, and that energy transport can be made more efficient by quantum effects.

One outstanding milestone is a denotational semantics accommodating higher order functions in quantum functional languages.

Bob Coecke, Oxford, August 7, 2010.

coecke@comlab.ox.ac.uk

Computing Laboratory
University of Oxford
OX1 3QD Oxford
United Kingdom

Part II

Project objectives and major achievements during the reporting period

Chapter 1

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

The QICS abstract is available from:

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

1.1 Objectives of QICS as stated in the initial proposal

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

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

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

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

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

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

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

Addressing these fundamental questions seriously will require a passage to new high-level methods, which expose the deep structure of quantum information and computations. Indeed, while the fruits of QIC have emerged from the recognition that quantum phenomena should not be seen as a *bug* but as a *feature* — contrasting with the negative attitude to "quantum

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

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

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

Q. What are the precise structural relationships between parallelism, entanglement and mixedness as quantum informatic resources? Or, more generally,

Q. Which features of quantum mechanics account for differences in computational and informatic power as compared to classical computation?

Q. How do quantum and classical information interact with each other, and with a spatio-temporal causal structure?

Q. Which quantum control features (e.g. iteration) are possible and what additional computational power can they provide?

Q. What is the precise logical status and axiomatics of (No-)Cloning and (No-)Deleting, and more generally, of the quantum mechanical formalism as a whole?

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

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

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

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

Strand 1: New MODELS of QIC

Strand 2: Foundational STRUCTURES for QIC

Strand 3: High-level METHODS for QIC

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

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

quantum state machines, which involve only quantum control, and also models which exploit other deep aspects of quantum structure, such as *topological quantum computing*. Furthermore, we are convinced that due to our innovative approach, additional new models will emerge.

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

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

1.2 Objectives for the workpackages as stated in the initial proposal

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Please see the introduction to each of the workpackges.

1.4 Progress made on the objectives during the reporting period

Please see the introduction to each of the workpackges.

1.5 Next steps to be taken for reaching the objectives

Please see the the introduction to each of the workpackges.

Chapter 2

Recruitment, mobility, spin-off

The numerous visits of researchers between QICS sides, on which we reported in great detail in the 1st QICS Periodic Activity Report in §3.3, have of course continued. We won't provide details here. The migration of postdocs between QICS sides reported on in 1st QICS Periodic Activity Report in §3.2 and in the 2nd QICS Periodic Activity Report in §2 has also continued.

Meanwhile, several QICS postdocs have obtained prestigious fellowships permanent positions, even at QICS sites. For example, Elham Kashefi became lecture at Edinburgh and Simon Perdrix obtained a permanent CNRS position at Grenoble. Within the time of the QICS project, the coordinating group at Oxford has grown from 7 members to 30, including two new faculty appointments.

Other funding bodies have meanwhile awarded research grants on the basis of achievements of the QICS team. These bodies for example include the US Office of Naval Research (ONR), The Foundational Questions Institute (FQXi), the British Engineering, Physical Sciences Research Council, the Templeton Foundation and EU-FP7. Currently several multi-site

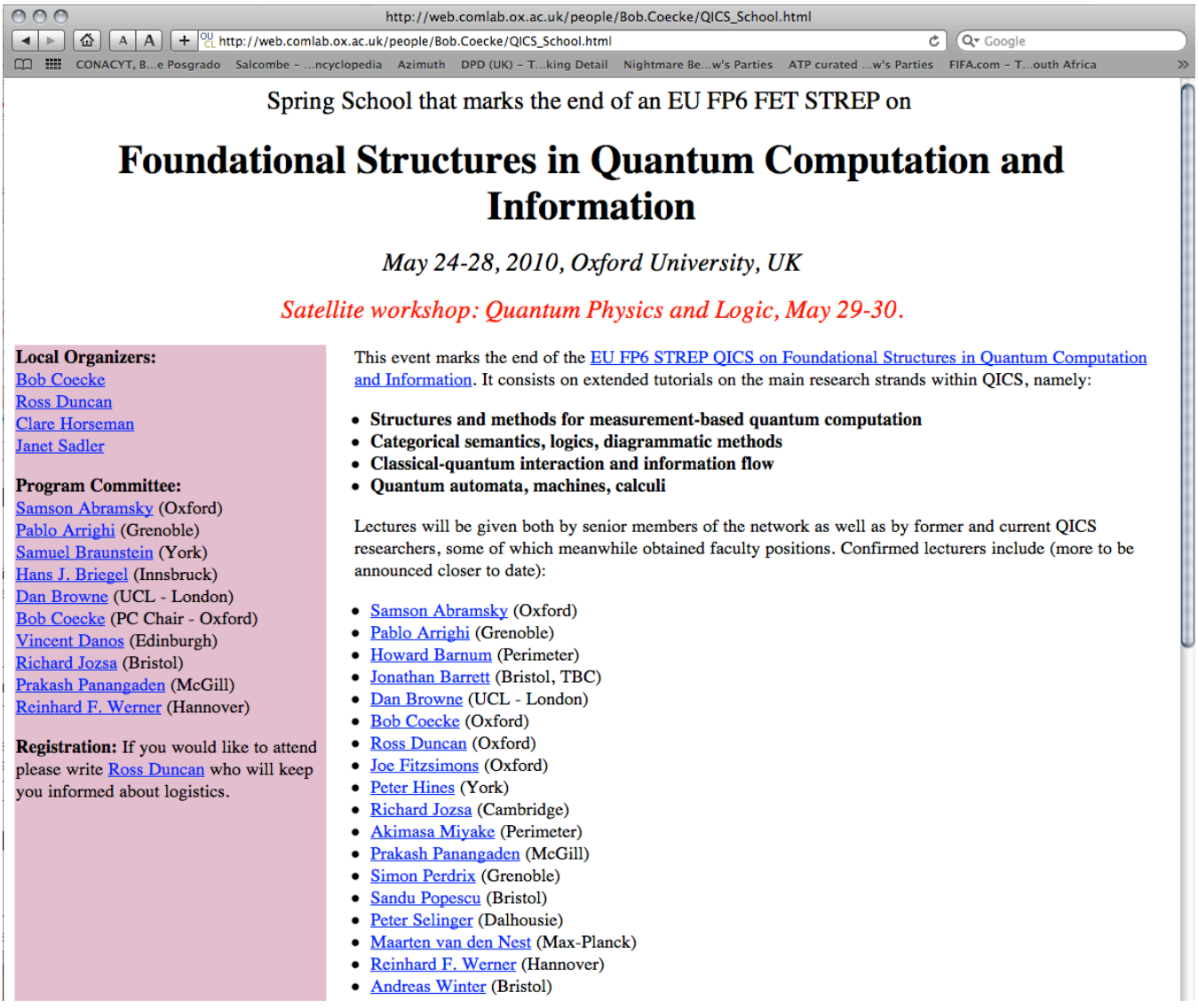
All of these contribute to the consolidation of the QICS activity.

Chapter 3

QICS events and presentations

3.1 The QICS school

The QICS project was concluded with a very successful international school with as its main purpose the dissemination of the major advances made during the QICS project:



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

Spring School that marks the end of an EU FP6 FET STREP on

Foundational Structures in Quantum Computation and Information

May 24-28, 2010, Oxford University, UK

Satellite workshop: Quantum Physics and Logic, May 29-30.

Local Organizers:
Bob Coecke
Ross Duncan
Clare Horseman
Janet Sadler

Program Committee:
Samson Abramsky (Oxford)
Pablo Arrighi (Grenoble)
Samuel Braunstein (York)
Hans J. Briegel (Innsbruck)
Dan Browne (UCL - London)
Bob Coecke (PC Chair - Oxford)
Vincent Danos (Edinburgh)
Richard Jozsa (Bristol)
Prakash Panangaden (McGill)
Reinhard F. Werner (Hannover)

Registration: If you would like to attend please write Ross Duncan who will keep you informed about logistics.

This event marks the end of the EU FP6 STREP QICS on Foundational Structures in Quantum Computation and Information. It consists on extended tutorials on the main research strands within QICS, namely:

- **Structures and methods for measurement-based quantum computation**
- **Categorical semantics, logics, diagrammatic methods**
- **Classical-quantum interaction and information flow**
- **Quantum automata, machines, calculi**

Lectures will be given both by senior members of the network as well as by former and current QICS researchers, some of which meanwhile obtained faculty positions. Confirmed lecturers include (more to be announced closer to date):

- Samson Abramsky (Oxford)
- Pablo Arrighi (Grenoble)
- Howard Barnum (Perimeter)
- Jonathan Barrett (Bristol, TBC)
- Dan Browne (UCL - London)
- Bob Coecke (Oxford)
- Ross Duncan (Oxford)
- Joe Fitzsimons (Oxford)
- Peter Hines (York)
- Richard Jozsa (Cambridge)
- Akimasa Miyake (Perimeter)
- Prakash Panangaden (McGill)
- Simon Perdrix (Grenoble)
- Sandu Popescu (Bristol)
- Peter Selinger (Dalhousie)
- Maarten van den Nest (Max-Planck)
- Reinhard F. Werner (Hannover)
- Andreas Winter (Bristol)

The school was not only attended by many students, but also by world-leading oversees researchers, just to mention some, mathematical physicist, category theoretician and blog-pioneer John Baez who extensively blogged on the School,

The n-Category Café

A group blog on math, physics and philosophy

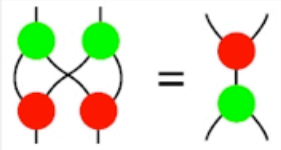
« Boycotting the Nature Publishing Group | Main | Algebraic Model Structures »

June 13, 2010

This Week's Finds in Mathematical Physics (Week 299)

Posted by John Baez

In week299 of This Week's Finds, hear about the school on Quantum Information and Computer Science that was recently held in Oxford, and also the workshop on Quantum Physics and Logic. Watch videos of the talks! Learn how classical structures give Frobenius algebras, and how complementary classical structures almost give bialgebras:



Admire the program called "Quantomatic", which automatically carries out string diagram computations. Hear about Aaron Fenyes' no-cloning theorem for classical mechanics. And finally, learn about "pre-Lie algebras" — algebraic gadgets with deep connections to trees, operads, and the work of Connes and Kreimer on renormalization in quantum field theory.

From Coecke's paper **Quantum picturalism**:

> **Experiment**
>
> Consider ten children of ages between six and ten and consider ten high-school teachers of physics and mathematics. The high-school teachers of physics and mathematics will have all the time they require to refresh their quantum mechanics background, and also to update it with regard to recent developments in quantum information. The children on the other hand will have quantum theory explained in terms of the graphical formalism. Both teams will be given a certain set of questions, for the children formulated in diagrammatic language, and for the teachers in the usual quantum mechanical formalism. Whoever solves the most problems and solves them in the fastest time wins. If the diagrammatic language is much more intuitive, it should in principle be possible for the children to win.

Posted at June 13, 2010 4:34 PM UTC

devoting most of Week 299 of This Week's Finds in Mathematical Physics to the QICS School:

http://math.ucr.edu/home/baez/week299.html

and condensed matter physicist Vladimir Korepin from Stony Brook who was particular interested in the logic and category theory methods developed during the QICS project, and is now organizing a conference "Simons Conference on New Trends in Quantum Computation" at the Simons Center for Geometry and Physics at Stony Brook, with a list of invited speakers that includes a very strong presence of both senior and more junior QICS School Lecturers (e.g. Abramsky (Ox), Coecke (Ox), Gühne (Inns), Miyake (Inns)), complemented pioneers of quantum computation and information such as Edward Farhi (adiabatic quantum computing model), Michael Freedman (topological quantum computing model) Alexander Holevo (Holevo bound) and Peter Shor (Shor's algorithm).

The program of the QICS School was:

Day 1:

- Akimasa Miyake (Perimeter Institute) Introduction to measurement-based quantum computing, with connections to condensed matter physics.
- Bob Coecke, Chris Heunen and Jamie Vicary (Oxford) Introduction to monoidal categories and graphical calculus 1.
- Richard Jozsa (Cambridge) Classical simulation of quantum circuits.
- Peter Selinger (Dalhousie) Higher types in quantum computing.

Day 2:

- Maarten van den Nest (Max Planck Institute) Introduction to graph states and their applications.
- Bob Coecke, Chris Heunen and Jamie Vicary (Oxford) Introduction to monoidal categories and graphical calculus 2.
- Prakash Panagaden (McGill) Modular tensor categories and topological quantum computing.
- Samson Abramsky (Oxford) Coalgebraic methods in quantum computing.

Day 3:

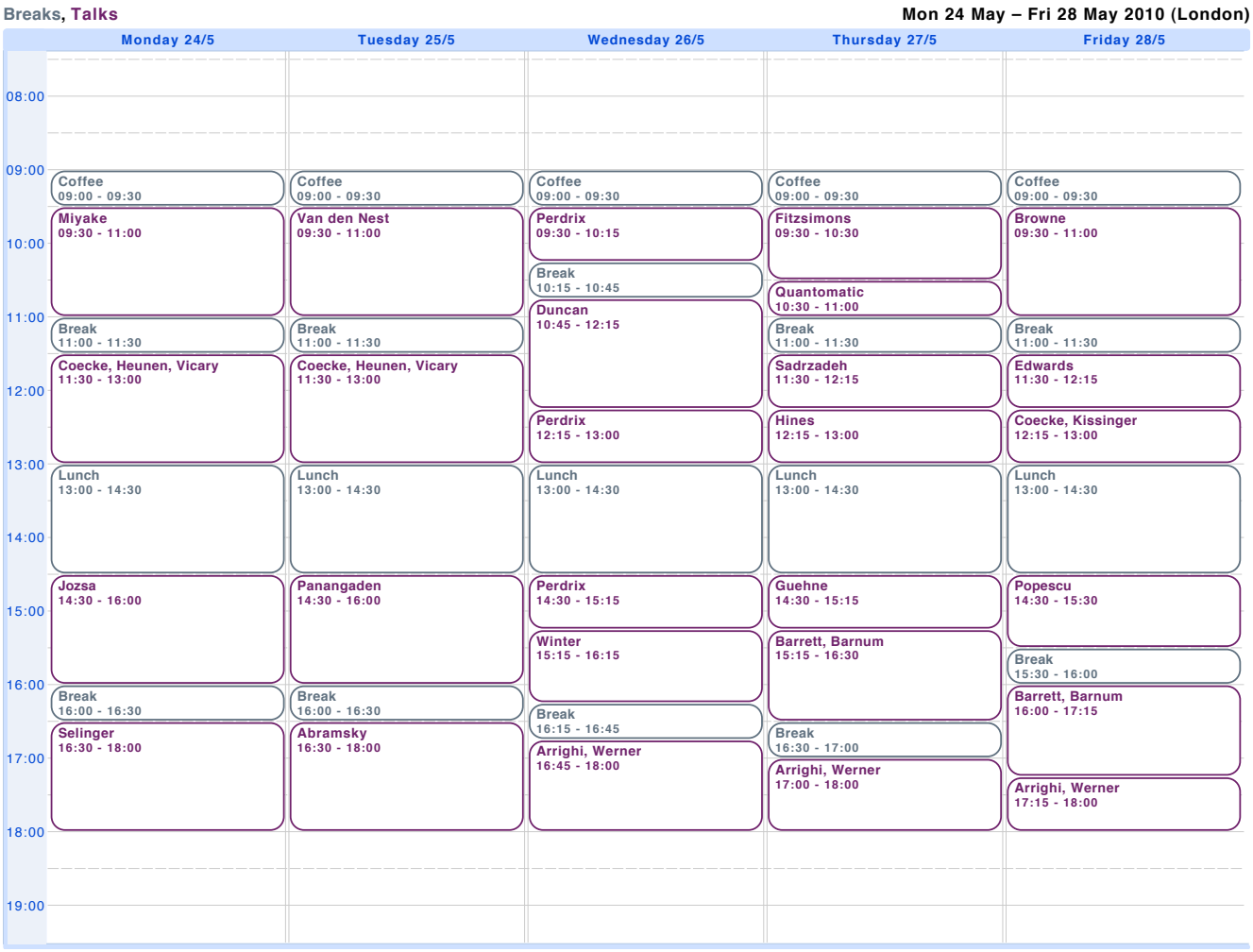
- Simon Perdrix (Grenoble) Flow and depth in measurement-based quantum computing 1.
- Ross Duncan (Oxford) Complementarity, quantum algebra, and applications to measurement-based quantum computing.
- Simon Perdrix (Grenoble) Flow and depth in measurement-based quantum computing 2.
- Simon Perdrix (Grenoble) Classical-quantum graphical calculus.
- Andreas Winter (Bristol) The fidelity alternative and quantum measurement simulation.
- Pablo Arrighi (Grenoble) and Reinhard Werner (Hannover) Quantum cellular automata 1.

Day 4:

- Joe Fitzsimons (Oxford) Blind quantum computing.
- Lucas Dixon (Edinburgh), Ross Duncan and Aleks Kissinger (Oxford) Quantomatic demo.
- Mehrnoosh Sadrzadeh (Oxford) Vector spaces and meaning.
- Peter Hines (York) Is coherence important in quantum computing?
- Ottfried Ghne (Innsbruck) Quantum contextuality.
- Howard Barnum (Perimeter Institute) and Jonathan Barrett (Bristol) Generalized probabilistic theories 1.
- Pablo Arrighi (Grenoble) and Reinhard Werner (Hannover) Quantum cellular automata 2.

Day 5:

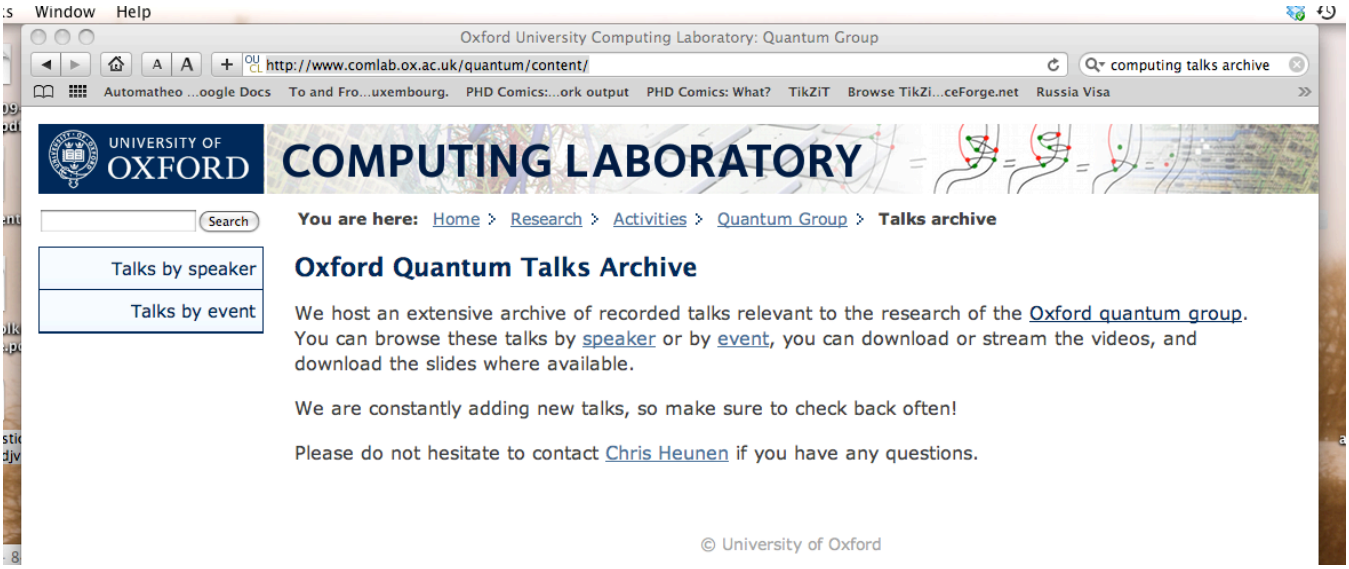
- Dan Browne (UCL) Measurement-based quantum computing, measurement-based classical computing, and non-locality.
- Bill Edwards (Oxford) Phase groups and non-locality.
- Bob Coecke and Aleks Kissinger (Oxford) Compositional multipartite entanglement.
- Sandu Popescu (Bristol) Non-locality.
- Howard Barnum (Perimeter Institute) and Jonathan Barrett (Bristol) Generalized probabilistic theories 2.
- Pablo Arrighi (Grenoble) and Reinhard Werner (Hannover) Quantum cellular automata 3.



All lectures given at the school are available for online viewing and download here:

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

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



3.2 Other QICS events and QICS supported events

Other regular events with partial QICS support have continued:

- Quantum Physics and Logic:

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

  http://web.comlab.ox.ac.uk/people/Bob.Coecke/QPL_10.html

  with as invited speakers:

  - John Baez (Riverside, Singapore)
  - Louis Crane (Kansas State)
  - Mauro D'Ariano (Pavia)
  - Joachim Kock (Barcelona)
  - Benjamin Schumacher (Kenyon College)
  - Reinhard Werner (Hannover)

- There regular workshops Categories, Logic and Foundations of Physics:

  http://categorieslogicphysics.wikidot.com/

3.3 Presentation of QICS output

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

Part III

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

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

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

respectively at:

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable9_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable10_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable11_en.html`

`http://se10.comlab.ox.ac.uk:8080/FOCS/QICSdeliverable12_en.html`

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

Each chapter starts with an introduction which explicitly addresses:

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

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

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

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

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

Chapter 4

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

The research in W1 concerned the mathematical and structural foundations of measurement based quantum computation (MBQC). All in all, the research has been successful, which is also indicated by the fact that more than 30 papers (including one review article in Nature Physics) emerged from the research on the different objectives in W1. Several important developments can be characterized:

Simulation of quantum computation: A central question in the field of quantum compution is to what extent a quantum computer is more powerful than a classical computer. One possibility to address this question is to consider the classical simulation of quantum computation and ask, which classical resources are required for this simulation. Within the QICS part W1 this question has been addressed and answered for certain types of quantum computations [2, 3, 4]. These works and related questions have triggered further work in the quantum information community (see also M.J. Bremner, R. Jozsa, D.J. Shepherd, arXiv:1005.1407), which is discussed in more detail in the introduction to W3.

Structures of MBQC: A central goal of the QICS project is an improved understanding of the structures of MBQC. This will help to devise new algorithms for MBQC, furthermore, it will shed light on the relation between MBQC and the network model of quantum computation. In the last period of QICS a number of relevant results have been obtained. Highlights are the study of the power of classical correlations for measurement based *classical* computation [5] and the investigation of so-called "universal blind computation" [8, 9].

Characterizing resources for MBQC: In the beginning of the QICS project it was not clear at all, which states besides the usual cluster state can be used for MBQC. In the first years of QICS, several fundamental results on this questions have been achieved. In the last two years, the understanding has still significantly improved (see [17, 18]). This, finally, has lead to new areas of research. First, based on the characterization of useful states for MBQC, new experiments have been performed in order to demonstrate some basic elements of MBQC with new resource states (see [19] and [J. Lavoie et al., arXiv:1004.3624]). Second, proposals for MBQC in different physical systems (e.g. ground states of spin models) have been made [24, 23].

Calculi and diagrammatic methods: A central aim of the QICS project was the usage of categorial methods to understand MBQC from a new perspective. In the last period, significant success in this direction has been made. For instance, using a diagrammatic formalism some central theorems concerning the entanglement properties of graph states could be formalized and understood [29]. Moreover, for practical purposes a software package was developed [31], more details are explained in the introduction to W2.

Of course, these points describe only some broad developments, and many more interesting results have been obtained. Details can be found below.

Objectives and milestones. The objectives and milesstones of W1 are given below. Concerning the milestones, the parts W1.M1 (mathematical structure of graph states) and W1.M2 (criteria for graph states to be universal) have already been reached in the first period of QICS. Here, the last period has still given some further insights. Concerning W1.M3 and W1.M4 (high-level languages), these milestones has also been reached with the diagrammatic methods explained above. W1.M5 (characterization of minimal resources for MBQC) has been reached in the last period and the experiments mentioned above show

that these works have a deep impact on the community. The milestone W1.M6 (characterization of quantum computational complexity) has also been reached due to the insights into the simulation of quantum computation.

Interactions with other workpackages and sites. As can be seen from the description of the papers and the publication list below, there has been an intense interaction with other workpackages. These connections became also manifest at the QICS school in Oxford in May 2010, where researchers from different workpackages gave a coherent overview over the topics of QICS.

Impact on research efforts outside of QICS As already mentioned above, the results obtained in W1 had a significant impact on the community outside of QICS, e.g. by stimulating new experiments on MBQC.

Hans J. Briegel and Otfried Gühne
Innsbruck, August 7, 2010.

Workpackage objectives

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

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

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

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

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

Workpackage milestones

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

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

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

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

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

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

Below we discuss the detailed progress for this workpackage which comprises the

Workpackage tasks

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

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

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

4.1 Progress towards objectives and performed tasks for W1.T1

4.1.1 Review article on W1

Measurement-based quantum computation (Paper in Nature Physics by Briegel (Inns), Browne (Ox affiliate) , Dür (Inns), Raussendorf and van den Nest (Former QICS postdoc at Inns)) [1] (Objectives: W1.O1, W1.O2, W1.O3, W1.O4; Milestones: W1.M1, W1.M2, W1.M5; Tasks: W1.T1) QICS researchers from several places presented an overview over the field of measurement based quantum computation. A number of recent developments in measurement-based quantum computation in both fundamental and practical issues were discussed, in particular regarding the power of quantum computation, the protection against noise (fault tolerance) and steps toward experimental realization. Moreover, a number of surprising connections between this field and other branches of physics and mathematics was highlighted.

4.1.2 Study normal forms for quantum algorithms in measurement-based computer models

a. Simulation of quantum computation (Objectives: W1.O3, W1.M1, Milestones: W1.M6, Tasks: W1.T1) In the paper [2] two QICS researchers from Bristol and Innsbruck investigated the classical simulation of quantum circuits consisting only of matchgates. Using a Clifford algebra formalism they showed that arbitrary uniform families of circuits of these gates, restricted to act only on nearest neighbor (n.n.) qubit lines, can be classically efficiently simulated. They further showed that if the n.n. condition is slightly relaxed, to allowing the same gates to act only on n.n. and next-n.n. qubit lines, then the resulting circuits can efficiently perform universal quantum computation.

In [3] the result of [2] was extended, and it was shown that the computational power of circuits of matchgates is equivalent to that of space-bounded quantum computation with unitary gates, with space restricted to being logarithmic in the width of the matchgate circuit. In particular, for the conventional setting of polynomial-sized (logarithmic-space generated) families of matchgate circuits, known to be classically simulatable, we characterise their power as coinciding with polynomial-time and logarithmic-space bounded universal unitary quantum computation.

In [4], Browne (UCL) Kashefi (Gren & Edin) and Perdrix (Gren & OX & Paris) prove that one-way quantum computations have the same computational power as quantum circuits with unbounded fan-out. It demonstrates that the one-way model is not only one of the most promising models of physical realisation, but also a very powerful model of quantum computation. It confirms and completes previous results which have pointed out, for some specific problems, a depth separation between the one-way model and the quantum circuit model. Since one-way model has the same computational power as unbounded quantum fan-out circuits, the quantum Fourier transform can be approximated in constant depth in the one-way model, and thus the factorisation can be done by a polytime probabilistic classical algorithm which has access to a constant-depth one-way quantum computer. The extra power of the one-way model, comparing with the quantum circuit model, comes from its classical-quantum hybrid nature. The authors show that this extra power is reduced to the capability to perform unbounded classical parity gates in constant depth.

b1. Foundational structures of measurement based quantum computation (Objectives: W1.O1, W1.O2, W1.O3, W1.O4; Milestones W1.M1, W1.M6) In [5] Anders and Browne (UCL/Ox) study the intrinsic computational power of correlations exploited in measurement-based quantum computation. They define a general framework in which the meaning of the computational power of correlations can be made precise. This leads to a notion of resource states for measurement-based classical computation. Surprisingly, the Greenberger-Horne-Zeilinger and Clauser-Horne-Shimony-Holt problems emerge as optimal examples. This work exposes an intriguing relationship between the violation of local realistic models and the computational power of entangled resource states.

In [6] Dunjko (Edin) and Kashefi (Edin,Gren) give a complete structural characterisation of the map the positive branch of a one-way pattern implements. They start with the representation of the positive branch in terms of the phase map decomposition, which is then further analysed to obtain the primary structure of the matrix M, representing the phase map decomposition in the computational basis. Using this approach they obtain some preliminary results on the connection between the columns structure of a given unitary and the angles of measurements in a pattern that implements it. It is believed this work is a step forward towards a full characterisation of those unitaries with an efficient one-way model implementation.

In [7] Kashefi (Edin, Gren) et. al. study the power of hypothetical closed time-like curves (CTC's) in quantum computation and show that the one-way model of measurement-based quantum computation encompasses the Bennett/Schumacher/Svetlichny CTC model in a natural way. They identify a class of CTC's in this model that can be simulated deterministically using techniques associated with the stabilizer formalism. They also identify a fundamental limitation of Deutsch's model for quantum time-travel which leads to predictions conflicting with those of the one-way model.

In [8] Kashefi (Edin, Gren) et. al present a protocol which allows a client to have a server carry out a quantum computation for her such that the client's inputs, outputs and computation remain perfectly private, and where she does not require any quantum computational power or memory. The client only needs to be able to prepare single qubits randomly chosen from a finite set and send them to the server, who has the balance of the required quantum computational resources. The protocol is interactive: after the initial preparation of quantum states, the client and server use two-way classical communication which enables the client to drive the computation, giving single-qubit measurement instructions to the server, depending on previous measurement outcomes. Our protocol works for inputs and outputs that are either classical or quantum. They give an authentication protocol that allows the client to detect an interfering server; our scheme can also be made fault-tolerant. They also generalize the result to the setting of a purely classical client who communicates classically with two non-communicating entangled servers, in order to perform a blind quantum computation. By incorporating the authentication protocol, they show that any problem in BQP has an entangled two-prover interactive proof with a purely classical verifier. This work is then connected to MBQC in [9].

In [10] Kashefi (Edin, Gren) et al. construct a family of time-independent Hamiltonians which are able to perform universally programmable quantum computation. The construction is obtained via direct translation of one-way computer assembly language code into a Hamiltonian evolution. They also present how to evolve adiabatically to this Hamiltonian. This approach

contributes further into the study of the structural relationship between measurement-based and adiabatic models of quantum computing.

b2. Foundational structures of measurement based quantum computation bis (Objectives: W1.O1, W2.O3, W3.O2: Tasks: W2.T2, W3.T1 W4.T1 W4.T2; Milestones: W1.M5, W1.M6, W4.M1) Stochastic finite-state generators are compressed descriptions of infinite time series. Alternatively, compressed descriptions are given by quantum finite-state generators [K. Wiesner and J. P. Crutchfield, Physica D 237, 1173 (2008)]. These are based on repeated von Neumann measurements on a quantum dynamical system. In [11], Wiesner (UNIVBRIS) and coauthors generalise the quantum finite-state generators by replacing the von Neumann projections by stochastic quantum operations. In this way they ensure that any time series with a stochastic compressed description has a compressed quantum description. Moreover, they establish a link between these stochastic generators and the sequential readout of many-body states with translationally-invariant matrix product state representations. As an example, they consider the non-adaptive read-out of 1D cluster states. This is shown to be equivalent to a Hidden Quantum Model with two internal states, providing insight on the inherent complexity of the process. Finally, it is proven by example that the quantum description can have a higher degree of compression than the classical stochastic one.

c. Using ancillas in measurement based quantum computation. In [12] Kashefi (Edin, Gren) et. al. propose a method of manipulating a quantum register remotely with the help of a single ancilla that steers the evolution of the register. The fully controlled ancilla qubit is coupled to the computational register solely via a fixed unitary two-qubit interaction, E, and then measured in suitable bases. They characterize all interactions E that induce a unitary, step-wise deterministic measurement back-action on the register sufficient to implement any arbitrary quantum channel. Their scheme offers significant experimental advantages for implementing computations, preparing states and performing generalized measurements as no direct control of the register is required.

In [13] Kashefi (Edin, Gren) et. al introduce a new paradigm for quantum computing called Ancilla-Driven Quantum Computation (ADQC) combines aspects of the quantum circuit and the one-way model to overcome challenging issues in building large-scale quantum computers. By demanding that the ancilla-system qubit interaction should lead to unitary and stepwise deterministic evolution, and that it should be possible to standardise the computation, that is, applying all global operations at the beginning, they are able to place conditions on the interactions that can be used for ADQC which leads to the definition of a new entanglement resource called twisted graph states generated from non-commuting operators. The ADQC model is formalised in an algebraic framework similar to the Measurement Calculus. Furthermore, they present the notion of causal flow for twisted graph states, based on the stabiliser formalism, to characterise the determinism. Finally they demonstrate compositional embedding between ADQC and both the one-way and circuit models which will allow them to transfer the theory and toolkits of measurement-based quantum computing directly into ADQC.

Efficient generation of cluster states is crucial for engineering large-scale measurement-based quantum computers. Hybrid matter-optical systems offer a robust, scalable path to this goal. Such systems have an ancilla which acts as a bus connecting the qubits. In [14], Horsman (UNIVBRIS) and coauthors show that by generating smaller cluster "Lego blocks", reusing one ancilla per block, the cluster can be produced with maximal efficiency, requiring less than half the operations compared with no bus reuse. Their results are general for all ancilla-based computational schemes; they describe it in detail for the qubus system. By reducing the time required to prepare sections of the cluster, bus reuse more than doubles the size of the computational workspace that can be used before decoherence effects dominate. (Objectives: W1.O2, W1.O3, W1.O4; Tasks: W1.T1, W1.T2; Milestones: W1.M1, W1.M2)

d. Magic state distillation (Objectives: W1.O1) Magic state distillation is an important primitive in fault-tolerant quantum computation. The magic states are pure non-stabilizer states which can be distilled from certain mixed non-stabilizer states via Clifford group operations alone. Because of the Gottesman-Knill theorem, mixtures of Pauli eigenstates are not expected to be magic state distillable, but it has been an open question whether all mixed states outside this set may be distilled. In [15] Browne (UXL/Ox) and Campbell show that, when resources are finitely limited, non-distillable states exist outside the stabilizer octahedron. In analogy with the bound entangled states, which arise in entanglement theory, they call such states bound states for magic state distillation.

In [16] Browne (UXL/Ox) and Campbell present a theorem that shows that all useful protocols for magic state distillation output states with a fidelity that is upper-bounded by those generated by a much smaller class of protocols. This reduced class consists of the protocols where multiple copies of a state are projected onto a stabilizer codespace and the logical qubit is then decoded.

4.2 Progress towards objectives and performed tasks for W1.T2

4.2.1 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

a. Universal resources for measurement based quantum computation (Objectives: W1.O2, W1.O3, W1.O4; Milestones: W1.M1, W1.M2, W1.M5, Tasks: W1.T1, W1.T2) In the paper [17] several researchers from Innsbruck gave a detailed discussion of the question, which quantum states can serve as universal resources for approximate and stochastic measurement-based quantum computation, in the sense that any quantum state can be generated from a given resource by means of single-qubit (local) operations assisted by classical communication. It was shown that entanglement-based criteria for universality obtained for the exact, deterministic case can be lifted to the much more general approximate, stochastic case, moving from the idealized situation considered in previous works, to the practically relevant context of non-perfect state preparation.

Several physicists from Innsbruck presented in [18] a comparison between different types of universality for measurement based quantum computation. One type is constructed as "computationally universal" states–i.e. they allow one to efficiently reproduce the classical output of each quantum computation–whereas the cluster states are universal in a stronger sense since they are "universal state preparators". It was shown that the new resources are universal state preparators after all, and must therefore exhibit a whole class of extremal entanglement features, similar to the cluster states.

An interesting question is, whether MBQC with the new resource states for MBQC can demonstrated experimentally. Indeed, in [19] researchers from Innsbruck and Hefei reported an experimental realization of every building block of the model of MBQC in correlation space. In the experiment, they prepared a four-qubit and a six-qubit state, which are proved different from cluster states through two-point correlation functions and the single site entropy of the qubits. With such resources, they have demonstrated a universal set of single-qubit rotations, two-qubit entangling gates and further Deutsch's algorithm. Besides being of fundamental interest, this experiment proves in-principle the feasibility of universal measurement-based quantum computation without cluster states.

In [20] Mhalla (Gren), Murao (Tokyo), Perdrix (Gren & OX & Paris), Someya (Tokyo), and Turner (Tokyo) present a structural characterization of the graph states that can be used for quantum information processing. The existence of a gflow (generalized flow) is known to be a requirement for open graphs (graph, input set and output set) to perform uniformly and strongly deterministic computations. They weaken the gflow conditions to define two new more general types of MBQC: uniform equiprobability and constant probability. These classes can be useful from a cryptographic and information point of view because even though one can not do a deterministic computation in general one can preserve the information and transfer it perfectly from the inputs to the outputs. The authors derive simple graph characterizations for these classes and prove that the deterministic and uniform equiprobability classes collapse when the cardinalities of inputs and outputs are the same. They also prove the reversibility of gflow in that case. The new graphical characterizations allow us to go from open graphs to graphs in general and to consider this question: given a graph with no inputs or outputs fixed, which vertices can be chosen as input and output for quantum information processing? The authors present a characterization of the sets of possible inputs and ouputs for the equiprobability class, which is also valid for deterministic computations with inputs and outputs of the same cardinality.

b. Related results on multipartite states (Objectives: W1.O1, W1.O2, W2.O3, W3.O2; Tasks: W3.T1, W4.T1; Milestones: W1.M1, W1.M2, W1.M4, W1.M6, W2.M3, W2.M6, W4.M1) In [21] Low (UNIVBRIS) presents a technique for derandomising large deviation bounds of functions on the unitary group. He replaces the Haar distribution with a pseudo-random distribution, a k-design. k-designs have the first k moments equal to those of the Haar distribution. The advantage of this is that (approximate) k-designs can be implemented efficiently, whereas Haar random unitaries cannot. Low finds large deviation bounds for unitaries chosen from a k-design and then illustrates this general technique with three applications. He first shows that the von Neumann entropy of a pseudo-random state is almost maximal. Then he shows that, if the dynamics of the universe produces a k-design, then suitably sized subsystems will be in the canonical state, as predicted by statistical mechanics. Finally he shows that pseudo-random states are useless for measurement based quantum computation.

In [22] Browne (UCL/Ox) and Loukopoulos introduce a scheme for secure multiparty computation utilizing the quantum correlations of entangled states. The schemes, each complying with a different definition of security, shed light on which physical assumptions are necessary in order to achieve quantum secure multiparty computation, a task which under the most general security model had been shown to be impossible. This work therefore exposes the physical assumptions necessary for Lo's famous no-go theorem for secure multi-party computation.

c. Novel resources for measurement based quantum computation (Objectives: W1.O2, W1.O4, Milestones: W1.M1, W1.M5; Tasks: W1.T2) In [23] G. Brennen and the QICS postdoc A. Miyake proposed a scheme for a ground-code measurement-based quantum computer, which enjoys two major advantages. First, every logical qubit is encoded in the gapped degenerate ground subspace of a spin-1 chain with nearest-neighbor two-body interactions, so that it equips built-in robustness against noise. Second, computation is processed by single-spin measurements along multiple chains dynamically coupled on

demand, so as to keep teleporting only logical information into a gap-protected ground state of the residual chains after the interactions with spins to be measured are turned off.

In the paper [24] QICS researchers from Innsbruck showed that a local Hamiltonian of spin-3/2 particles with only two-body nearest-neighbor Affleck-Kennedy-Lieb-Tasaki and exchange-type interactions has an unique ground state, which can be used to implement universal quantum computation merely with single-spin measurements. It was proved that the Hamiltonian is gapped, independent of the system size. The results provide a further step towards utilizing systems with condensed matter-type interactions for measurement-based quantum computation.

d. Classical spin models and graph states (Milestones: W1.M1, Tasks: W3.T1) In [25] researchers from Innsbruck showed (using insights from measurement based quantum computation) that the partition function of all classical spin models, including all discrete Standard Statistical Models and all abelian discrete Lattice Gauge Theories (LGTs), can be expressed as a special instance of the partition function of the 4D Z_2 LGT. In this way, all classical spin models with apparently very different features are unified in a single complete model, and a physical relation between all models is established.

In [26] the results of [25] were extended. It was shown how a complete model with real -and, hence, "physical"- couplings can be obtained if the 3D Ising model is considered. We furthermore show how to map general q-state systems with possibly many-body interactions to the 2D Ising model with complex parameters, and give completeness results for these models with real parameters.

In [27] mappings between classical spin systems and quantum physics were investigated from a general perspective. More precisely, it was shown how to express partition functions and correlation functions of arbitrary classical spin models as inner products between quantum stabilizer states and product states. These mappings establish a link between the fields of classical statistical mechanics and quantum information theory, which can be utilized to transfer techniques and methods developed in one field to gain insight into the other.

In the paper [28] QICS researchers from Innsbruck presented a further extension of [25]. The equivalence between the models was illustrated by computing quantities of a specific model as a function of the partition function of the 4D Z_2 LGT.

4.3 Progress towards objectives and performed tasks for W1.T3

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

a. Calculi and diagrammatic methods for general measurement-based quantum computation (Objectives: W1.O1, W1.02, W1.O4, W1.O5, W2.O1, W2.O2, W2.O3, W2.04; Milestones: W1.M1, W1.M3, W2.M1, W2.M3, W2.M4, W2.M6; Tasks: W1.T2, W1.T3 W2.T1, W2.T2, W3.T2) Coecke and Duncan recently introduced a categorical formalisation of the interaction of complementary quantum observables. In the paper [29] we use their diagrammatic language to study graph states, a computationally interesting class of quantum states. We give a graphical proof of the fixpoint property of graph states. We then introduce a new equation, for the Euler decomposition of the Hadamard gate, and demonstrate that Van den Nest's theorem–locally equivalent graphs represent the same entanglement–is equivalent to this new axiom. Finally we prove that the Euler decomposition equation is not derivable from the existing axioms.

Furthermore, in the paper [30] we present a method for verifying measurement-based quantum computations, by producing a quantum circuit equivalent to a given deterministic measurement pattern. We define a diagrammatic presentation of the pattern, and produce a circuit via a rewriting strategy based on the generalised flow of the pattern. Unlike other methods for translating measurement patterns with generalised flow to circuits, this method uses neither ancilla qubits nor acausal loops.

In addition, we developed an automated proof-assistant software, based on diagrammatic / categorical methods [31], a detailed description is discussed in the introduction to W2.

b. Measurement calculus (Objectives: W1.O2; Tasks: W1.T1 W2.T2; Milestones: W1.M1 W1.M3 W1.M4) In [32], Danos, Kashefi, Panangaden and Perdrix revisit the measurement calculus initially developed by the first three authors (see arXiv:quant-ph/0412135 or a preprint), a rigourous mathematical model underlying the measurement-based quantum computing which can be though of as an "assembly language" for this particular type of quantum computation. From this, they: (i). explore whether this model may suggest new techniques for designing quantum algorithms and protocols, (ii). investigate how to transform a projection-based pattern specification to a measurement-based implementation and (iii). demonstrate how the obtained MBQC tools can be used in the traditional quantum circuit model.

Bibliography

[1] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, M. Van den Nest, Measurement-based quantum computation, Nature Physics 5 1, 19-26 (2009); arXiv:0910.1116.

[2] R. Jozsa, A. Miyake, Matchgates and classical simulation of quantum circuits, Proc. R. Soc. A 464, 3089-3106 (2008); arXiv:0804.4050.

[3] R. Jozsa, B. Kraus, A. Miyake, J. Watrous, Matchgate and space-bounded quantum computations are equivalent, Proc. R. Soc. A 466, 809-830 (2010); arXiv:0908.1467.

[4] D. E. Browne, E. Kashefi, S. Perdrix, Computational depth complexity of measurement-based quantum computation, 5th conference on theory of quantum computation, communication and cryptography (TQC'10).

[5] J. Anders, D.E. Browne, Computational power of correlations, Phys. Rev. Lett. 102, 050502 (2009).

[6] V. Dunjko, E. Kashefi, Algebraic characterisation of one-way patterns, Developments in Computational Models, EPTCS 26, (2010).

[7] R. Dias da Silva, E. F. Galvao, E. Kashefi, Closed time-like curves in measurement-based quantum computation, arXiv:1003.4971.

[8] A. Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, (2009).

[9] A. Broadbent, J. Fitzsimons, E. Kashefi, Measurement-based and Universal Blind Quantum Computation, In Formal Methods for Quantitative Aspects of Programming Languages, Edited by Alessandro Aldini, Marco Bernardo, Alessandra Di Pierro, Herbert Wiklicky, LNCS, 2010.

[10] S.Salek, F. Seifan and E. Kashefi, Programmable Hamiltonian for one-way patterns, In Proceeding of the 6th Workshop on Quantum Physics and Logic (2009).

[11] A. Monras, A. Beige and K. Wiesner, Hidden Quantum Markov Models and non-adaptive read-out of many-body states, arXiv:1002.2337.

[12] J. Anders, D. K. L. Oi, E. Kashefi, D.E. Browne, E. Andersson (2009), Ancilla-Driven Universal Quantum Computation, Phys. Rev. A., 2009.

[13] E. Kashefi, D. K. L. Oi, D. E. Browne, J. Anders, E. Andersson, Twisted graph states for ancilla-driven quantum computation, In Proceeding of the 25th Conference on the Mathematical Foundations of Programming Semantics (MFPS 25), ENTCS 249 (2009).

[14] C. Horsman, K.L. Brown, W.J. Munro and V.M. Kendon, Reduce, reuse, recycle, for robust cluster state generation, arXiv:1005.1621.

[15] E. T. Campbell, D. E. Browne, Bound States for Magic State Distillation in Fault-Tolerant Quantum Computation Phys. Rev. Lett. 104, 030503 (2010).

[16] E. T. Campbell, D. E. Browne (2010) On the Structure of Protocols for Magic State Distillation, Lecture Notes in Computer Science 5906 Theory of Quantum Computation, Communication and Cryptography 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13. Page 20.

[17] C. E. Mora, M. Piani, A. Miyake, M. Van den Nest, W. Dür, H. J. Briegel, Universal resources for approximate and stochastic measurement-based quantum computation, Phys. Rev. A 81, 042315 (2010); arXiv:0904.3641.

[18] J.-M. Cai, W. Dür, M. Van den Nest, A. Miyake, H. J. Briegel, Quantum computation in correlation space and extremal entanglement, Phys. Rev. Lett. 103, 050503 (2009); arXiv:0902.1097.

[19] W.-B. Gao, X.-C. Yao, J.-M. Cai, H. L., P. Xu, T. Yang, Y.-A. Chen, Z.-B. Chen, J.-W. Pan, Experimental demonstration of measurement-based quantum computation in correlation space, arXiv:1004.4162.

[20] M. Mhalla, M. Murao, S. Perdrix, M. Someya, P. S. Turner, Quantum Information Processing with Graphs, arXiv:1006.2616.

[21] R. Low, Large Deviation Bounds for k-designs, Proc. R. Soc. A, 465(2111):3289-3308 (2009); arXiv:0903.5236.

[22] K. Loukopoulos, D. E. Browne, Secure Multi-Party Computation with a Dishonest Majority via Quantum Means, Phys. Rev. A 81, 062336 (2010).

[23] G. K. Brennen, A. Miyake, Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian, Phys. Rev. Lett. 101, 010502 (2008); arXiv:0803.1478.

[24] J.M. Cai, A. Miyake, W. Dür, H.J. Briegel, Universal quantum computer from a quantum magnet, arXiv:1004.1907.

[25] G. De las Cuevas, W. Dür, H. J. Briegel, M. A. Martin-Delgado, Unifying all classical spin models in a Lattice Gauge Theory, Phys.Rev.Lett. 102, 230502 (2009); arXiv:0812.3583.

[26] G. De las Cuevas, W. Dür, M. Van den Nest, H.J. Briegel, Completeness of classical spin models and universal quantum computation, J. Stat. Mech. (2009) P07001; arXiv:0812.2368.

[27] R. Hübener, M. Van den Nest, W. Dür, H. J. Briegel, Classical spin systems and the quantum stabilizer formalism: general mappings and applications, J. Math. Phys. 50, 083303 (2009); arXiv:0812.2127.

[28] G. De las Cuevas, W. Dür, H. J. Briegel, M. A. Martin-Delgado, Mapping all classical spin models to a lattice gauge theory, New J. Phys. 12, 043014 (2010); arXiv:0911.2096.

[29] R. Duncan and S. Perdrix, Graph states and the necessity of Euler decomposition. In K. Ambos-Spies, B. Lowe, and W. Merkle (editors): Computability in Europe: Mathematical Theory and Computational Practice (CiEi09), volume 5635 of Lecture Notes in Computer Science, pages 167-177. Springer, 2009.

[30] R. Duncan and S. Perdrix, Rewriting measurement-based quantum computations with generalised flow. In S. Abramsky, C. Gavoille, C Kirchner, F. Meyer auf der Heide, and P. G. Spirakis (editors): Automata, Languages and Programming, 37th International Colloquium, ICALP 2010, Proceedings Part II, volume 6199 of Lecture Notes in Computer Science, pages 285-296. Springer, 2010.

[31] L. Dixon, R. Duncan, and A. Kissinger. Quantomatic. http://dream.inf.ed.ac.uk/projects/quantomatic/

[32] V. Danos, E. Kashefi, P. Panangaden, S. Perdrix, Extended Measurement Calculus in Semantic Techniques for Quantum Computation, In: Simon Gay and Ian Mackie (eds); http://www.cs.mcgill.ca/ prakash/Pubs/DKPP-chap-final.pdf (2009).

Chapter 5

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

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

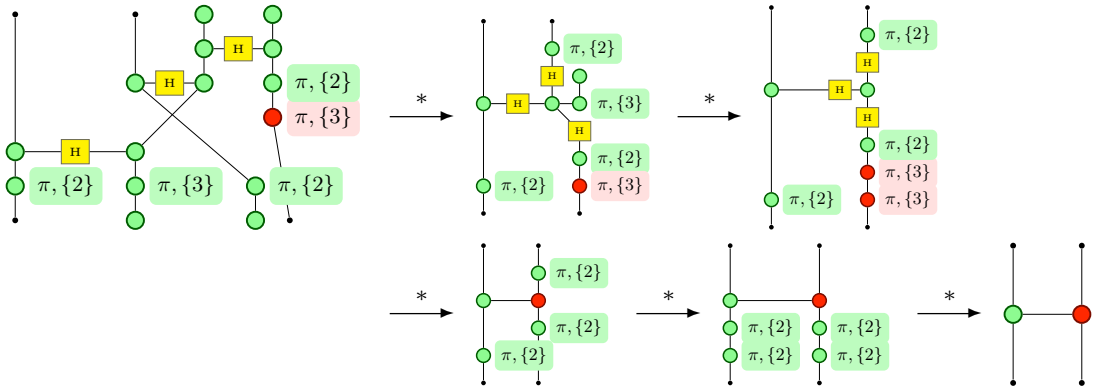
This year was marked by the fact that the categorical approach to quantum computation, the most ambitious and high-risk workpackage of the QICS proposal, has achieved widespread recognition. Hence this endeavor has been a major success.

One token of this is that at the prestigious ICALP conference which traditionally accepts a number of outstanding papers in the area of quantum computation, this year two out of three accepted quantum computing papers are a result of this work-package; we discuss these two results below. Another token is the fact that this work has meanwhile led to spin-off in two very actual CS areas, namely compositional linguistics and automated theory exploration, resulting in currently finalized multi-side proposals with world-leading groups. Most importantly, a number of QICS postdocs working in this area have meanwhile obtained permanent positions, as well as prestigious long-term fellowships, including permanent research positions at CNRS.

Yet another token has been the presence of this activity on leading blogs, e.g. as already mention above in Section 3, in John Baez' current blog, which is the most prominent mathematical physics blog, and in Richard Lipton's "Godel's lost letter and P=NP", which is probably the most prominent computer science and complexity theory blog:

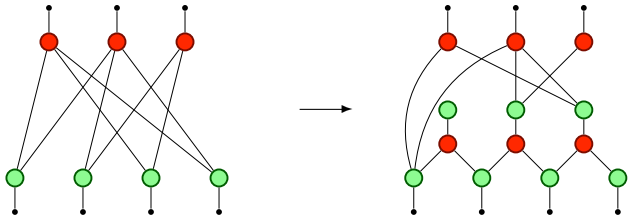
http://rjlipton.wordpress.com/2010/03/21/logic-meets-complexity-theory/

Main developments in W2. The first of the two ICALP accepted papers resulting from QICS research, [24] by Duncan (Ox) and Perdrix (Gren), solves an open problem of WP1, namely, the generation of minimal-width circuits equivalent to a given deterministic measurement-based computation. Recall that the geometry of a graph state dictates whether that state can be used as a resource for a deterministic measurement-based computation, a property known as *generalised flow* (Browne et al, 2007). In [24] it was shown that, when expressed in the graphical language, graph states which have generalised flow correspond locally to simple Hopf algebra expressions. By replacing these expressions with equivalent ones, we can transform measurement-based computations to quantum circuits without introducing any extra qubits, thus minimising the space complexity.



The main technical result is a statement about the equivalence of two expressions in the graphical language: while the result is used to translate from a measurement-based computation to quantum circuit, the intermediate steps do not correspond to any

standard formalism, and are necessarily expressed in the graphical language. In other words, the graphical language developed in WP2 is key to solving this important problem of WP1.



In addition, this work generalises earlier work on determinism in the one-way model by treating the case of non-uniform determinism (i.e. sensitive to choice of parameters), and by analysing concrete programs rather than their resource states, and hence is a key step toward automated verification of measurement-based quantum computation.

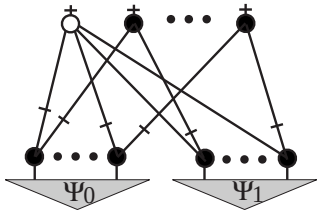
The second paper gives an algebraic characterization of three qubit entanglement as well as a compositional account on general multipartite qubit entanglement. Multipartite quantum states constitute a (if not the) key resource for quantum computations and protocols. However, obtaining a generic structural understanding of entanglement in N-qubit systems is a long-standing open problem in quantum computer science. In [12] Coecke (Ox) and Kissinger (Ox) showed that multipartite quantum entanglement admits a compositional structure, and hence is subject to modern computer science methods. This goes as follows.

Recall that there are only two SLOCC-equivalence classes of genuinely entangled 3-qubit states, the GHZ-class and the W-class. First it was shown that these exactly correspond with two kinds of internal commutative Frobenius algebras on $\mathbb{C}^2$ in the symmetric monoidal category of Hilbert spaces and linear maps, namely 'special' and 'anti-special' ones. In the graphical notation of symmetric monoidal categories speciality and anti-speciality depict as follows:

i.e. 'connected' vs. 'disconnected'. These are (consequently) the only two kinds of Frobenius algebras that exist on a qubit.

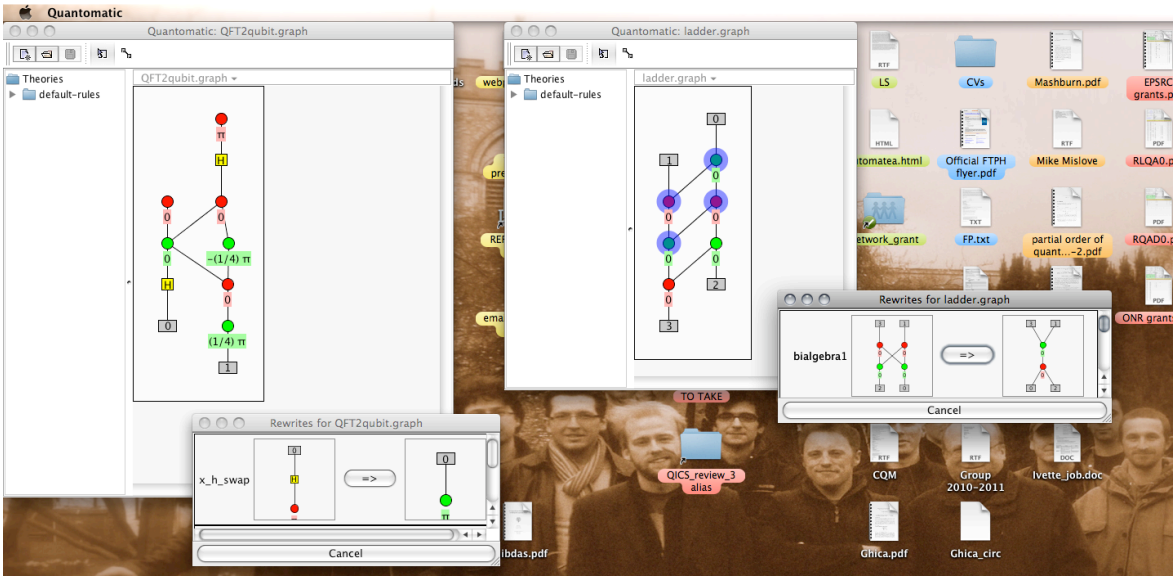
Next it was shown that these GHZ and W Frobenius algebras form the primitives of a graphical calculus which is expressive enough to generate and reason about representatives of arbitrary N-qubit states. Concretely, arbitrary states can be generated inductively –following an approach initiated in Lamata-Leon-Salgado-Solano (2006, 2007)– from W-dots (black) and GHZ-dots (white; the ticks are the corresponding dualizer of the induced compact structure):

$|0\Psi_0\rangle + |1\Psi_1\rangle =$



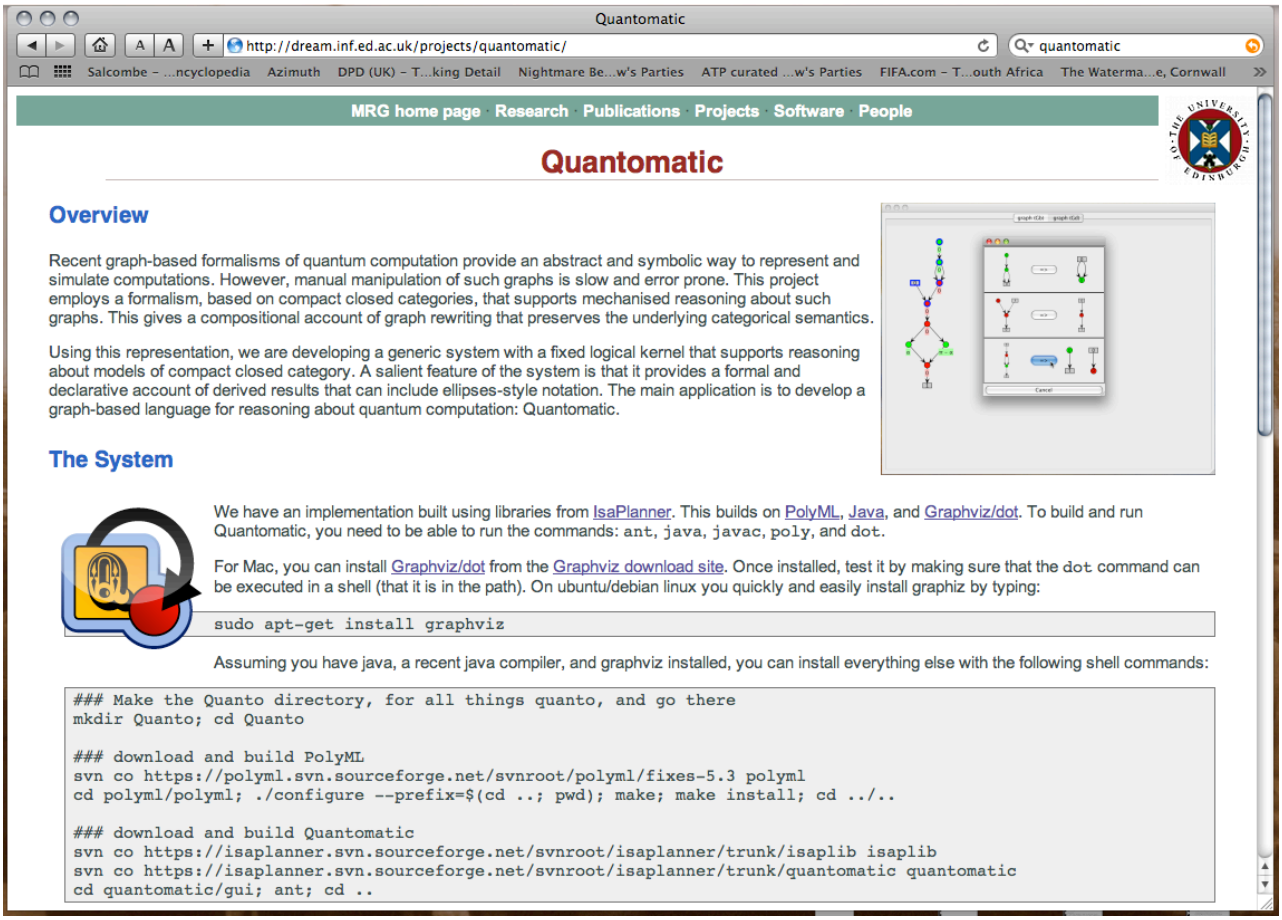
where the tripartite GHZ and W states can be taken to be base cases:

The importance of these results grows with the further development of the `quantomatic` software, on which currently Dixon (Edin/Paris), Duncan (Ox), Kissinger (Ox) and Merry (Ox) are active. This software was initially developed to (semi-)automate exploration of the calculus of complementary observables (also referred to as the 'green/red'- or 'Z/X'-calculus) due to Coecke (Ox) and Duncan (Ox), first presented at ICALP'08 and of which the extended version is the first paper on category theory and physics to appear in the New Journal of Physics [11].



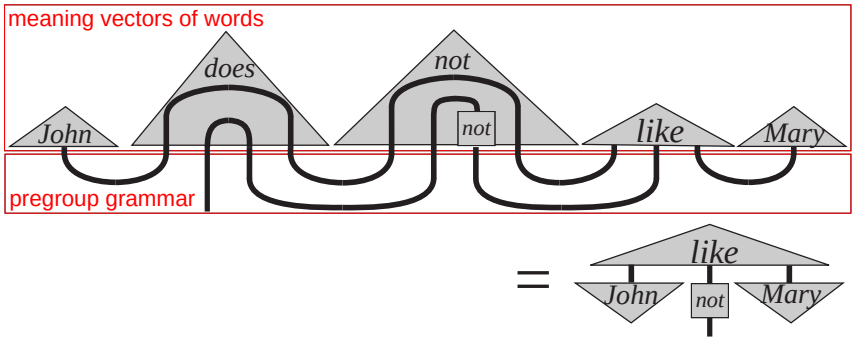
Meanwhile `quantomatic` is flexible enough to also accommodate other graphical rewrite theories, e.g. the GHZ/W-calculus initiated in [12], for which the development of a 'good' rewrite calculus is currently ongoing.

This software can now be run on any platform, unix, Mac and PC, and it is made freely available for download by the automated theorem proving group at Edinburgh:



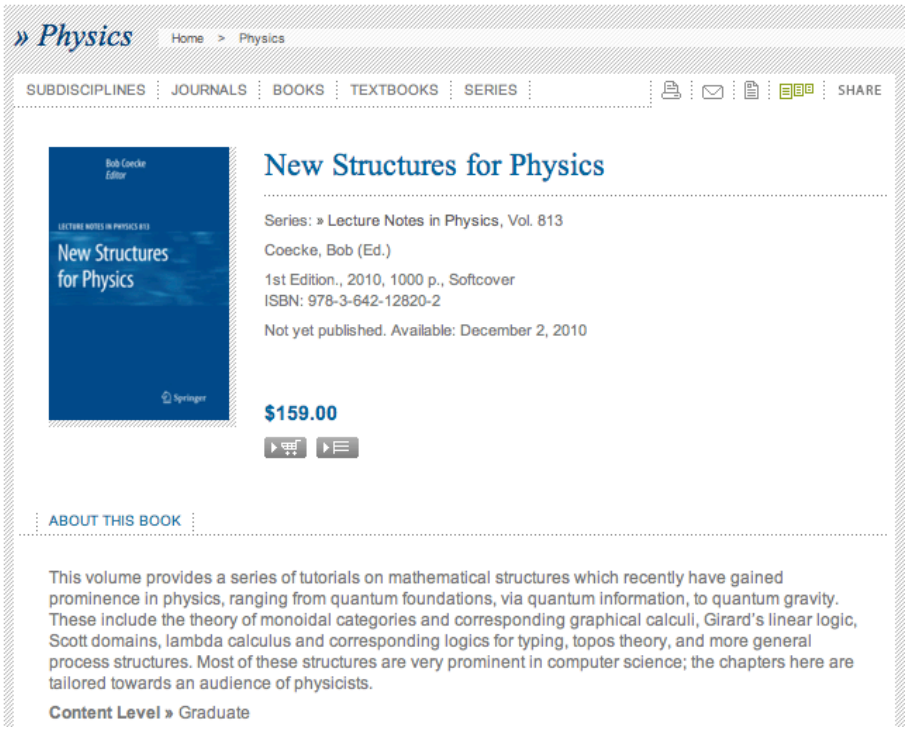
Particularly important about this project is that the team mainly consists of researchers which are involved in the software development [20], in the development of the graphical calculi themselves [11, 12], and in the theory that provides the bridge between the two [22, 21]. The highly ambitious benchmark that has been set for the further development of this tool is that it should produce *the first non-trivial result in physics that is produced by a machine*. Given the hardness of the problem to understand the structure of multipartite entanglement, we expect that it will be in this area that quantomatic has the potential to reach this goal. We expect such a result within two years. Currently, an EU STREP proposal is being put together by Edinburgh, Oxford and some other groups that are world-leaders in automated theory exploration, for which the further development of `quantomatic` in order to achieve this goal is one out of three workpackages.

Besides the work in the direction of automated theory exploration, another spin-off to a 'non-quantum' area of computer science is the use of WP2 methods in computational linguistics [17]. Here, the diagrams for which connectedness represents dependencies of quantum information, now are used to depict the flows of information between words and sentences, and provide a way to compute the meaning of a word from the meaning of its constituents:



Other notable developments in this workpackage include:

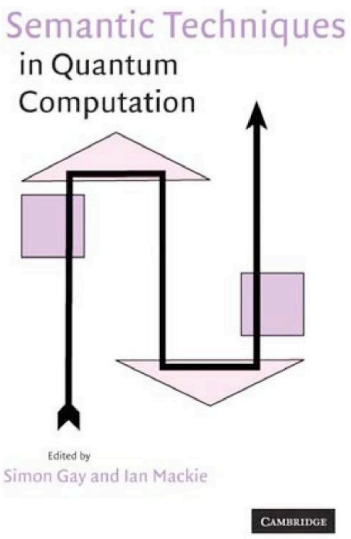
- Publication of *New Structures for Physics* [8], edited by Coecke (Ox), which provides many tutorials, many of which by QICS researchers; Abramsky (Ox), Blute (McGill affiliate) Coecke (Ox), Döring (Ox), Hines (York), Lambek (McGill), Panangaden (McGill), Paquette (McGill), Selinger (McGill affiliate), Scott (McGill affiliate) and Tzevelekos (Ox).[1] This 1000 page volume should enable undergraduates to enter the area of this workpackage.



- Publication of *Semantic Techniques for Quantum Computation* [8], edited by Gay (Ox affiliate) and Mackie (Ox affiliate), which provides many chapters on the subject by QICS researchers; Abramsky (Ox), Altenkirch (Ox affiliate), Coecke

[1] Note in particular the important contribution of the (unfunded) Canadian partner site.

(Ox), Danos (Edinburgh/Paris), Duncan (Ox), Gay (Ox affiliate), Green (Ox affiliate), Hines (York), Jorrand (Grenoble), Kashefi (Edinburgh/Paris), Nagarajan (Ox affiliate), Panangaden (McGill), Papanikolaou (Ox affiliate), Paquette (McGill), Pavlovic (Ox), Perdrix (Grenoble), Selinger (McGill affiliate), Valiron (McGill affiliate),



- Frobenius algebras which play a key role in modeling quantum observables have now also been studied in other categories such as the category of relations [25], and in connection to C*-algebras and certain lattices, which in the past have been used to model complementarity. Also connections between the categorical approach and generalized convex operational theories [4] and quantum generalizations of Bayesian inference [18] have been studied.
- Finally, there are many new structural theorems [29], [38], [39], [40] etc.

Bob Coecke and Ross Duncan
Oxford, August 7, 2010.

Workpackage objectives :

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

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

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

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

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

Workpackage milestones :

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

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

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

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

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

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

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

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

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

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

5.1 Survey's/tutorials/reviews for W2

a. New Structures for Physics (Book, 1000 pages, edited by Coecke (Ox)) [8] Table of contents: 1. Samson Abramsky and Nikos Tzevelekos: Introduction to categories and categorical logic. 2. John Baez and Michael Stay: Physics, topology, logic and computation: A Rosetta Stone. 3. Bob Coecke and Eric Oliver Paquette: Categories for the practising physicist. 4. Peter Selinger: A survey of graphical languages for monoidal categories. 5. Esfandiar Haghverdi and Philip Scott. Geometry of Interaction and the dynamics of proof reduction: a tutorial 6. Richard Blute and Prakash Panangaden. Dagger categories and formal distributions. 7. Richard Blute and Prakash Panangaden. Proof nets as formal Feynman diagrams. 8. Joachim Lambek. Compact monoidal categories from Linguistics to Physics. 9. Keye Martin. Domain theory and measurement. 10. Bob Coecke and Keye Martin. A partial order on classical and quantum states. 11. Keye Martin and Prakash Panangaden. Domain theory and general relativity. 12. B. J. Hiley. Process, distinction, groupoids and Clifford algebras: an alternative view of the quantum formalism. 13. Andreas Doring and Chris Isham. What is a Thing?: Topos theory in the foundations of physics. 14. Peter Hines. Can a quantum computer run the von Neumann architecture? 15. Prakash Panangaden, Eric Oliver Paquette. A categorical presentation of quantum computation with anyons.

b. Semantic Techniques for Quantum Computation (Book, 500 pages, edited by Gay (Ox affiliate) and Mackie (Ox affiliate)) [26] A collection of chapters including many by QICS members. Table of contents: 1. Samson Abramsky: No-cloning in categorical quantum mechanics. 2. Bob Coecke, Eric Oliver Paquette and Dusko Pavlovic: Classical and quantum structuralism. 3. Ross Duncan: Generalized proof-nets for compact categories with biproducts. 4. Peter Hines and Sam Braunstein: The structure of partial isometries . 5. Vincent Danos, Elham Kashefi, Prakash Panangaden and Simon Perdrix: Extended measurement calculus. 6. Philippe Jorrand and Simon Perdrix: Abstract interpretation techniques for quantum computation. 7. Mingsheng Ying, Yuan Feng, Runyao Duan, and Zhengfeng Ji: Predicate transformer semantics of quantum programs. 8. Thorsten Altenkirch and Alexander Green: The quantum io monad. 9. Peter Selinger and Benot Valiron: Quantum lambda calculus. 10. Paulo Mateus, Jaime Ramos, Amlcar Sernadas, and Cristina Sernadas: Temporal logics for reasoning about quantum systems. 11. Simon Gay, Rajagopal Nagarajan, and Nick Papanikolaou: Specification and verification of quantum protocols.

c. Introduction to categories and categorical logic (Chapter of [8] by Abramsky (Ox) and Tzevelekos (Ox)) [3] The aim of these notes is to provide a succinct, accessible introduction to some of the basic ideas of category theory and categorical logic. The notes are based on a lecture course given at Oxford over the past few years. They contain numerous exercises, and hopefully will prove useful for self-study by those seeking a first introduction to the subject, with fairly minimal prerequisites. The coverage is by no means comprehensive, but should provide a good basis for further study; a guide to further reading is included. The main prerequisite is a basic familiarity with the elements of discrete mathematics: sets, relations and functions. An Appendix contains a summary of what we will need, and it may be useful to review this first. In addition, some prior exposure to abstract algebravector spaces and linear maps, or groups and group homomorphismswould be helpful.

d. Categories for the practicing physicist (Chapter of [8] by Coecke (Ox) and Paquette (McGill)) [14] This chapter surveys some particular topics in category theory in a somewhat unconventional manner. The main focus will be on monoidal categories, mostly symmetric ones, for which we propose a physical interpretation. These are particularly relevant for quantum foundations and for quantum informatics. Special attention is given to the category which has finite dimensional Hilbert spaces as objects, linear maps as morphisms, and the tensor product as its monoidal structure (FdHilb). There is a detailed discussion of the category which has sets as objects, relations as morphisms, and the cartesian product as its monoidal structure (Rel), and thirdly, categories with manifolds as objects and cobordisms between these as morphisms (2Cob). While sets, Hilbert spaces and manifolds do not share any non-trivial common structure, these three categories are in fact structurally very similar. Shared features are diagrammatic calculus, compact closed structure and particular kinds of internal comonoids which play an important role in each of them. The categories FdHilb and Rel moreover admit a categorical matrix calculus. Together these features guide us towards topological quantum field theories. One also discusses posetal categories, how group representations are in fact categorical constructs, and what strictification and coherence of monoidal categories is all about.

e. A survey of graphical languages for monoidal categories (Chapter of [8] by Selinger (McGill affiliate) [37] Selinger (Halifax) summarizes the current state of knowledge on various notions of monoidal categories and their associated string diagrams. The author augments this with additional new notions and conjectured soundness and completeness results.

f. Geometry of Interaction and the dynamics of proof reduction: a tutorial (Chapter of [8] by Esfandiar Haghverdi and Philip Scott (McGill affiliate)) [27] Girards Geometry of Interaction (GoI) is a program that aims at giving mathematical models of algorithms independently of any extant languages. In the context of proof theory, where one views algorithms as proofs and computation as cut-elimination, this program translates to providing a mathematical modelling of the dynamics of cut-elimination. The kind of logics we deal with, such as Girards linear logic, are resource sensitive and have their proof-theory intimately related to various monoidal (tensor) categories. The GoI interpretation of dynamics aims to develop an algebraic/geometric theory of invariants for information flow in networks of proofs, via feedback. This chapter gives an introduction to the categorical approach to GoI, including background material on proof theory, categorical logic, traced and partially traced monoidal *-categories, and orthogonalities.

g. Can a quantum computer run the von Neumann architecture? (Chapter of [8] by Hines (York)) [30] The von Neumann architecture is at the heart of almost every modern computer, and at the heart of the von Neumann architecture is the notion that program code may be manipulated in the same way as data. Categorically, this is a form of closure, familiar from a number of settings including logic, quantum mechanics, and theoretical computation. This paper considers the practical utility of the von Neumann architecture in computer science, and whether quantum-mechanical realisations of such categorical closure (in particular, the Choi-Jamiolkowsky correspondence) will exhibit similar utility for quantum computation. It is demonstrated that neither the no-cloning nor the no-deleting theorems prevent such development; however, the Gottesmann-Knill theorem means that any quantum analogue of the von Neumann architecture will be restricted to the Clifford group of operations and thus be efficiently classically simulable. W1.O1 W2.O2 W3.O4 W4.O2 W1.M4

h. A categorical presentation of quantum computation with anyons. (Chapter of [8] by Panangaden (Mcgill) and Paquette (Mcgill)) [35] In nature one observes that in three space dimensions particles are either symmetric under interchange (bosons) or antisymmetric (fermions). These phases give rise to the two possible statistics that one observes. In two dimensions, however, a whole continuum of phases is possible. Anyon is a term coined in by Frank Wilczek to describe particles in 2 dimensions that can acquire any phase when two or more of them are interchanged. The exchange of two such anyons can be expressed via representations of the braid group and hence, it permits one to encode information in topological features of a system composed of many anyons. Kitaev suggested the possibility that such topological excitations would be stable and could thus be used for robust quantum computation. This chapter aims to: 1. give the categorical structure necessary to describe such a computing process; 2. illustrate this structure with a concrete example namely: Fibonacci anyons.

i. Categorical Quantum Mechanics (Invited chapter in the Handbook of Quantum Logic by Abramsky (Ox) and Coecke (Ox)) [2] This chapter is a review and survey of the approach pioneered in Oxford to categorical quantum mechanics, and in particular contains an updated version of the first paper that initiated the area.

j. Quantum Picturalism (Invited paper in Contemporary Physics by Coecke (Ox)) [9] The quantum mechanical formalism doesn't support our intuition, nor does it elucidate the key concepts that govern the behaviour of the entities that are subject to the laws of quantum physics. The arrays of complex numbers are kin to the arrays of 0s and 1s of the early days of computer programming practice. In this review we present steps towards a diagrammatic 'high-level' alternative for the Hilbert space formalism, one which appeals to our intuition. It allows for intuitive reasoning about interacting quantum systems, and trivialises many otherwise involved and tedious computations. It clearly exposes limitations such as the no-cloning theorem, and phenomena such as quantum teleportation. As a logic, it supports 'automation'. It allows for a wider variety of underlying theories, and can be easily modified, having the potential to provide the required step-stone towards a deeper conceptual understanding of quantum theory, as well as its unification with other physical theories. Specific applications discussed here are purely diagrammatic proofs of several quantum computational schemes, as well as an analysis of the structural origin of quantum non-locality. The underlying mathematical foundation of this high-level diagrammatic formalism relies on so-called monoidal categories, a product of a fairly recent development in mathematics. These monoidal categories do not only provide a natural foundation for physical theories, but also for proof theory, logic, programming languages, biology, cooking, ... The challenge is to discover the necessary additional pieces of structure that allow us to predict genuine quantum phenomena.

k. A Universe of Processes and Some of its Guises (Invited chapter in a volume in honor of von Neumann's contributions to Mathematical Physics by Coecke (Ox)) [10] Our starting point is a particular 'canvas' aimed to 'draw' theories of physics, which has symmetric monoidal categories as its mathematical backbone. In this we consider the conceptual foundations

for this canvas, and how these can then be converted into mathematical structure. With very little structural effort (i.e. in very abstract terms) and in a very short time span the categorical quantum mechanics (CQM) research program, initiated by Abramsky and the author, has reproduced a surprisingly large fragment of quantum theory. It also provides new insights both in quantum foundations and in quantum information, for example in, and has even resulted in automated reasoning software called quantomatic which exploits the deductive power of CQM, which is indeed a categorical quantum logic.

5.2 Progress towards objectives and performed tasks for W2.T1

5.2.1 Categorical semantics of complementary quantum observables

a. The axiomatic structure of complementary quantum observables (Objectives/Tasks/Milestones: W1.O1 W2.O1 W2.O2 W2.O4 W3.O2 W3.O4 W1.T3 W2.T1 W3.T2 W2.M1 W2.M4 W3.M5) In [11], Within an intuitive diagrammatic calculus and corresponding high-level category-theoretic algebraic description Coecke (Ox) and Duncan (Ox) axiomatise complementary observables for quantum systems described in finite dimensional Hilbert spaces, and study their interaction. They also axiomatise the phase shifts relative to an observable. The resulting graphical language is expressive enough to denote any quantum physical state of an arbitrary number of qubits, and any processes thereof. The rules for manipulating these result in very concise and straightforward computations with elementary quantum gates, translations between distinct quantum computational models, and simulations of quantum algorithms such as the quantum Fourier transform. They enable the description of the interaction between classical and quantum data in quantum informatic protocols. More specifically, they rely on the previously established fact that in the symmetric monoidal category of Hilbert spaces and linear maps non-degenerate observables correspond to special commutative †-Frobenius algebras. This leads to a generalisation of the notion of observable that extends to arbitrary †-symmetric monoidal categories (†-SMC). We show that any observable in a †-SMC comes with an abelian group of phases. We define complementarity of observables in arbitrary †-SMCs and prove an elegant diagrammatic characterisation thereof. They show that an important class of complementary observables give rise to a Hopf- algebraic structure, and provide equivalent characterisations thereof.

b. Complementary quantum observables in the category of relations (Objectives/Tasks/Milestones: W1.O1 W1.O4 W2.O2) Finding all the mutually unbiased bases in various dimensions is a problem of fundamental interest in quantum information theory and pure mathematics. The general problem formulated in finite-dimensional Hilbert spaces is open. In the categorical approach to quantum mechanics one can find examples of categories which behave "like" the category of finite-dimensional Hilbert spaces in various ways but are subtly different. One such category is the category of sets and relations, **Rel**. One can formulate the concept of mutually unbiased bases here as well. In [25] Evans (McGill), Duncan (Ox), Lang (McGill) and Panangaden (McGill) classify all the mutually unbiased bases in this category by relating it to a standard question in combinatorics.

c. Categorical complementary quantum observables in relation to C*-algebras and lattices (Objectives/Tasks/Milestones: W3.O4, W3.T2, W3.M4) In [28] Heunen (Ox) relates notions of complementarity in three layers of quantum me-chanics: (i) von Neumann algebras, (ii) Hilbert spaces, and (iii) orthomodular lattices. Taking a more general categorical perspective of which the above are instances, we consider dagger monoidal kernel categories for (ii), so that (i) become (sub)endohomsets and (iii) become subobject lattices. By developing a Qpoint-free R definition of copyability we link (i) commutative von Neumann subalgebras, (ii) classical structures, and (iii) Boolean subalgebras.

5.2.2 Categorical semantics for MBQC

a. Categorical axiomatics for van den Nest Thm. [23] See WP1 §4.3.1.a.

b. Rewriting measurement-based quantum computations with generalised flow [24] See WP1 §4.3.1.a.

5.2.3 Automated theory exploration:quantomatic

a. Theory bridging graphical calculi for monoidal categories and actual software implementation. [22, 21] (Objectives/Tasks/Milestones: W1.O2 W2.O4 W2.T1 W2.M4) The theory of monoidal categories has a well-known description via a graphical langauge—frequently exploited in the categorical work described in this work package. However, the notion of "graph" laid out by Joyal and Street (1991) is a topological construction, rather different for the usual combinatorial definition familiar to computer scientists. Indeed, the usual definition is not adequate to represent the kinds of pictorial reasoning used in categorical quantum mechanics, and conversely the topological presentation is not amenable to automated reasoning. The

papers [22, 21] provide alternative notions of graph that capture the necessary properties to support pictorial reasoning, and which can be readily implemented in software. This is extended with a simple pattern language which gives a formal meaning to the informal ellipsis notation frequently used in arguments, permitting its incorporation into the Quantomatic software (see below).

b. Extension and improvement of the quantomatic software. [20] (Objectives/Tasks/Milestones: W1.O2 W2.O4 W2.T1 W2.M4) Quantomatic, already reported on last year, is automated proof-assistant software written by Dixon (Edinburgh/Paris), Duncan (Ox), Kissinger (Ox) and Merry (Ox), based on diagrammatic/categorical methods, currently mainly those developed in [11] by Coecke (Ox) and Duncan (Ox). Quantomatic can verify the correctness of measurement-based quantum computations, translate between different models of quantum computation, and prove equivalences between quantum states. It is highly configurable and can operate either fully automatically, or with a human operator. This software can now be run on any platform, unix, Mac and PC and is made freely available for download.

Currently, an EU STREP proposal is being put together by Edinburgh, Oxford and some other groups that are world-leaders in automated theory exploration, for which the further development of quantomatic will be one out of three workpackages.

5.2.4 Categorical characterization of classicality and environment

a. Categorical axiomatics of classicality relative to quantumness [15] See WP3 §6.2.1.

b. Categorical axiomatics for environment and classical channel [16] See WP3 §6.2.1.

c. Categorical axiomatics for choice of basis with applications to quantum key distribution [19] See WP3 §6.2.1.

5.2.5 Categorical probability and convexity

a. Categories of convex operational models (Objectives/Tasks/Milestones: W1.O4 W2.O2 W2.T2 W2.T1) In [4] Barnum, Duncan (Ox) and Wilce consider symmetric monoidal categories of convex operational models, and adduce necessary and sufficient conditions for these to be compact-closed or dagger-compact. Compact closure amounts to the condition that all processes be implementable by means of a "remote evaluation" protocol (generalizing standard conclusive quantum teleportation protocols), which amounts to a form of classical conditioning. Degenerate dagger compact categories (in which each system is its own dual, not just up to isomorphism, but on the nose) emerge from a further restriction, namely, that a composite of two copies of any systems allowed by the theory admit a symmetric bipartite "isomorphism" state.

b. Classical and quantum Bayesian inference diagrammatically (Objectives/Tasks/Milestones: W2.O1, W2.O4, W2.T1, W2.M1, W2.M3) In [18] Coecke (Ox) and Spekkens introduce a graphical framework for Bayesian inference that is sufficiently general to accommodate not just the standard case but also recent proposals for a theory of quantum Bayesian inference wherein one considers mixed quantum states rather than probability distributions as representative of degrees of belief. The diagrammatic framework is stated in the graphical language of symmetric monoidal categories and of compact structures and Frobenius structures therein, in which Bayesian inversion boils down to transposition with respect to an appropriate compact structure. In the case of quantum-like calculi, the latter will be non-commutative. They identify a graphical property that characterizes classical Bayesian inference. The abstract classical Bayesian graphical calculi also allow to model relations among classical entropies, and reason about these. They generalize conditional independence to this very general setting and also generalize some standard results. Finally, given any dagger compact category, they construct a 'quantum-like' theory of inference. This result is of importance in the light of an existing completeness theorem for dagger compact categories.

c. Dagger categories and formal distributions (Objectives/Tasks/Milestones: W2.O2 W2.T1 W2.M4) Monoidal dagger categories play a central role in the abstract quantum mechanics of Abramsky and Coecke. They show that a great deal of elementary quantum mechanics can be carried out in these categories; for example, the Born rule emerges naturally. In [6] Blute (McGill affiliate) and Panangaden (McGill) construct a category of tame formal distributions with coefficients in a commutative associative algebra and show that it is a dagger category. This gives access to a broad new class of models, with the abstract scalars in the sense of Abramsky being the elements of the algebra. They also consider a subcategory of local formal distributions, based on the ideas of Kac. Locality has been of fundamental significance in various formulations of quantum field theory. Thus this work may provide the possibility of extending the abstract framework to QFT. They also show that these categories of formal distributions are monoidal and contain a nuclear ideal, a weak form of adjunction appropriate for analyzing categories such as the category of Hilbert spaces, where the nuclear maps are the Hilbert-Schmidt maps. By taking

formal distributions with coefficients in the dual of a cocommutative Hopf algebra, they obtain a categorical generalization of the Borcherds' notion of elementary vertex group.

5.2.6 Structural theorems and higher categories

a. An embedding theorem for Hilbert categories (Objectives/Tasks/Milestones: W2.O2, W2.T1, W3.M4) In [29] Heunen (Ox) axiomatically defines (pre-)Hilbert categories. The axioms resemble those for monoidal Abelian categories with the addition of an involutive functor. He then proves embedding theorems: any locally small pre-Hilbert category whose monoidal unit is a simple generator embeds (weakly) monoidally into the category of pre-Hilbert spaces and adjointable maps, preserving adjoint morphisms and all finite (co)limits. An intermediate result that is important in its own right is that the scalars in such a category necessarily form an involutive field. In case of a Hilbert category, the embedding extends to the category of Hilbert spaces and continuous linear maps. The axioms for (pre-)Hilbert categories are weaker than the axioms found in other approaches to axiomatizing 2-Hilbert spaces. Neither enrichment nor a complex base field is presupposed. A comparison to other approaches will be made in the introduction.

b. Coherence theorems for autonomous categories in which A is isomorphic to A* (Objectives/Tasks/Milestones: W2.O1 W2.O2) In [38], Selinger (McGill affiliate) shows what coherence conditions should be required of an autonomous category (e.g. compact closed category) in which the objects are self-dual. The coherence axioms are shown to be sound and complete for a graphical language. This is motivated by the work of Coecke, Pavlovic in [11, 15, 16] and others on classical structures, where self-duality is often assumed, and by recent work of Barnum, Duncan, and Wilce [4], where self-duality appears in the context of convex operational models.

c. Categorical analogues of monoid semirings (Objectives/Tasks/Milestones: W3.O2 W4.M6) In [31] Hines (York) performs a very abstract categorical study of convolution products and their categorical analogues. By extending notions of summation familiar from algebraic program semantics to a more general setting, where both constructive and destructive interference may be modelled, it is demonstrated that the monoid semiring construction may be extended to the case where the monoid is replaced by an arbitrary category, and the semiring is replaced by a summation-enriched category. The ultimate aim of this program is two-fold; a formal setting for the constructions of abstract machines discussed in WP4, and a description of quantum Fourier transforms as components of a natural transformation between two functors, in a similar way to the description of categorical coherence isomorphisms as natural transformations between functors.

d. The structure of partial isometries (Objectives/Tasks/Milestones: W2.O2 W2.O3 W2.T1 W3.T2 W2.M4) In [33], Hines (York) and Braunstein (York) consider the similarities and differences between the competing category-theoretic and order-theoretic approaches to the foundations of quantum information. The (lack of) interaction between orthomodular lattices and tensor products is an obstacle to category-theoretic studies of quantum logic. This paper instead studies the Halmos-McLaughlin partial order on partial isometries, and demonstrates a close connection with both inverse categories and traditional von Neumann - Birkhoff quantum logic. By treating the category of partial isometries as a categorification of quantum logic, a direct comparison of the two competing approaches to foundational questions becomes possible. These are shown to be fundamentally incompatible, with the ultimate reason for this incompatibility being the distinct treatments of post-selection on measurement outcomes in the respective analyses of teleportation.

e. dagger-Frobenius monoids as quantum algebras (Objectives/Tasks/Milestones: W2.O1) In [39] Vicary (Ox) describes how dagger-Frobenius monoids give the correct categorical description of certain kinds of finite-dimensional 'quantum algebras'. He develops the concept of an involution monoid, and use it to construct a correspondence between finite-dimensional C*-algebras and certain types of dagger-Frobenius monoids in the category of Hilbert spaces. Using this technology, he recasts the spectral theorems for commutative C*-algebras and for normal operators into an explicitly categorical language, and he examines the case that the results of measurements do not form finite sets, but rather objects in a finite Boolean topos. He describes the relevance of these results for topological quantum field theory.

f. Completeness of dagger-categories and the complex numbers (Objectives/Tasks/Milestones: W2.O1) The complex numbers are an important part of quantum theory, but are difficult to motivate from a theoretical perspective. In [40] Vicary (Ox) describes a simple formal framework for theories of physics, and shows that if a theory of physics presented in this manner satisfies certain completeness properties, then it necessarily includes the complex numbers as a mathematical ingredient. Central to this approach are the techniques of category theory, and he introduces a new category-theoretical tool, called the dagger-limit, which governs the way in which systems can be combined to form larger systems. These dagger-limits can be

used to characterize the dagger-functor on the category of finite-dimensional Hilbert spaces, and so can be used as an equivalent definition of the inner product. One of the main results is that in a nontrivial monoidal dagger-category with all finite dagger-limits and a simple tensor unit, the semiring of scalars embeds into an involutive field of characteristic 0 and orderable fixed field.

5.2.7 Categorical recursion and algorithms

a. Categorical coherence in quantum algorithms (Objectives/Tasks/Milestones: W1.O1 W2.T1 W2.M4) In [32] Hines (York) studies the utility of categorical coherence conditions and theorems for quantum information and computation. In particular, it is demonstrated that the oracle at the heart of Shor's algorithm (and quantum period-finding generally) is based on the categorical coherence conditions for the distributivity of the tensor product over the direct sum. The coherence theorem for such a form of distributivity implies the equivalence of two quantum circuits – the first being a naive computation of modular exponentials, and the second being the efficient form of modular exponentiation actually presented by P. Shor. The required oracle is observed to be constructed entirely from categorical coherence isomorphisms, and thus such an equivalence holds in any category with two monodical tensors and a suitable notion of distributivity.

b. Categorical traces from single-photon linear optics (Objectives/Tasks/Milestones: W2.T1 W2.M4 W4.T1 W4.M6) Motivated by a single-photon though experiment, based on a modification of the Sagnac interferometer, in [34] Hines (York) and Scott (McGill affiliate) introduce a general construction on linear maps that has a close connection to constructions from algebraic and categorical program semantics. By modelling this thought-experiment in a category of formal power series over linear maps, a partial categorical trace (generalising a particle-style trace on Hilbert spaces found in abstract logical models) is given, with this thought-experiment as the concrete realisation.

5.3 Progress towards objectives and performed tasks for W2.T2

5.3.1 Compositional (categorical) semantics for multipartite entanglement

a. The axiomatic structure of multipartite entanglement (Objectives/Tasks/Milestones: W2.O2 W3.O1 W3.O2 W3.T1 W2.M3) Multipartite quantum states constitute a (if not the) key resource for quantum computations and protocols. However obtaining a generic, structural understanding of entanglement in N-qubit systems is a long-standing open problem in quantum computer science. In [12] Coecke and Kissinger show that multipartite quantum entanglement admits a compositional structure, and hence is subject to modern computer science methods. They consider N-qubit states to be equivalent as computational resources if they can be inter-converted by stochastic local (quantum) operations and classical communication (SLOCC). There are only two SLOCC-classes of genuinely entangled 3-qubit states, the GHZ-class and the W-class, and they show that these exactly correspond with two kinds of internal commutative Frobenius algebras over qubits in the symmetric monoidal category of Hilbert spaces and linear maps, namely 'special' ones and 'anti-special' ones. Within the graphical language of symmetric monoidal categories, the distinction between 'special' and 'anti-special' is purely topological, in terms of 'connected' vs. 'disconnected'. These GHZ and W Frobenius algebras form the primitives of a graphical calculus which is expressive enough to generate and reason about representatives of arbitrary N-qubit states. This calculus refines the graphical calculus of complementary observables due to Duncan and Coecke in [11], which has already shown itself to have many applications and admit automation (cf. quantomatic [20]). Our result also induces a generalised graph state paradigm for measurement-based quantum computing.

b. Improvements on tensor rank estimates (Objectives/Tasks/Milestones: W2.O2 W3.O1 W3.O2 W3.T1 W2.M3 W2.M5 W3.M3) The tensor rank (aka generalized Schmidt rank) of multipartite pure states plays an important role in the study of entanglement classifications and transformations. In [7], Winter (UNIVBRIS) and coauthors employ powerful tools from the theory of homogeneous polynomials to investigate the tensor rank of symmetric states such as the tripartite state W_3 and its N-partite generalization W_N. Previous tensor rank estimates are dramatically improved and they show that (i) three copies of W_3 has rank either 15 or 16, (ii) two copies of W_N has rank 3N-2, and (iii) n copies of W_N has rank O(N). A remarkable consequence of these results is that certain multipartite transformations, impossible even probabilistically, can become possible when performed in multiple copy bunches or when assisted by some catalyzing state. This novel effect is impossible for bipartite pure states.

5.3.2 Categorical quantum relativity

a. Categorical axiomatics of causality (Objectives/Tasks/Milestones: W2.T2) In [13] Coecke (Ox) and Lal (Ox) encode causal space-time structure within categorical process structure, by restricting the tensor to space-like separated entities, i.e. be-

tween which there is no causal flow of information. In such a causal category, a privileged set of morphisms captures the idea of an event horizon. This structure enables us to derive statements independent of specific models and detailed descriptions of processes, for example, that for a teleportation-like configuration from which the classical channel is removed, information flow from Alice to Bob cannot occur. They show that causal categories with compact structures or a dagger collapse, and define a process projector which recovers the full power of categorical quantum mechanics.

b. Categorical algebraic quantum field theory (Objectives/Tasks/Milestones: W2.T2) In an effort to extend the categorical approach to quantum mechanics to include relativistic effects, In [1] Abramsky (Ox), Blute (McGill affiliate), Coecke (Ox), Comeau (McGill affiliate), Porter and Vicary (Ox) introduce the notion of dagger net. Inspired in part by ideas from algebraic quantum field theory, a dagger net is a functor from some poset of regions of spacetime to the category of monoidal dagger categories. One crucial difference with AQFT is that rather than order spacetime regions under subset inclusion, they extend the causal ordering on points to regions. They argue here that, for the purposes of encoding protocols such as quantum teleportation, this is more appropriate. This brings their notion of functorial QFT more in line with the causal set theory of Sorkin. They explore the extent to which the monoidal and dagger structures of the individual categories in the codomain of the functor extend to the dagger net. Such a question makes sense when considering the Grothendieck category associated to the net. They show that there are local versions of the monoidal and dagger structures, and argue that such notions have good physical intuition. In the notion of dagger QFT, they are bringing in higher category theory. This naturally leads to the consideration of ideas from higher-dimensional algebra in conjunction with dagger net structure; in particular we consider (co)stack-like structures. A stack is in essence a sheaf of categories, and the consideration of costacks of dagger categories leads to some potentially interesting physical principles.

5.4 Progress towards objectives and performed tasks for W2.T3

Modular tensor categories as Frobenius pseudoalgebras (Objectives/Tasks/Milestones: W2.O5, W2,T3) In [5] Bartlett and Vicary (Ox) demonstrate that the modular tensor categories used as a setting for topological quantum computation can be formulated abstractly as Frobenius pseudoalgebras in a certain 2-category. These Frobenius pseudoalgebras are 'categorifications' of the classical structures used to model basis structures in the standard approach to categorical quantum mechanics, and as such serve as a bridge between these two paradigms of quantum computation.

5.5 Spin-off to computational linguistics

While not stated in the initial objectives, QICS research has led to an important application in the area of computational linguistics, addressing an open problem to combine probabilistic and logical models of meaning.

Compositional distributional meaning In [17] Coecke (Ox), Sadrzadeh (Ox) and Clark propose a mathematical framework for a unification of the distributional theory of meaning in terms of vector space models, and a compositional theory for grammatical types, for which they rely on the algebra of Pregroups, introduced by Lambek. This mathematical framework enables us to compute the meaning of a well-typed sentence from the meanings of its constituents. Concretely, the type reductions of Pregroups are 'lifted' to morphisms in a category, a procedure that transforms meanings of constituents into a meaning of the (well-typed) whole. Importantly, meanings of whole sentences live in a single space, independent of the grammatical structure of the sentence. Hence the inner-product can be used to compare meanings of arbitrary sentences, as it is for comparing the meanings of words in the distributional model. The mathematical structure we employ admits a purely diagrammatic calculus which exposes how the information flows between the words in a sentence in order to make up the meaning of the whole sentence. A variation of their 'categorical model' which involves constraining the scalars of the vector spaces to the semiring of Booleans results in a Montague-style Boolean-valued semantics.

Bell states and negation In [36] Preller and Sadrzadeh (Ox) use Bell states to provide compositional distributed meaning for negative sentences of English. The lexical meaning of each word of the sentence is a context vector obtained within the distributed model of meaning. The meaning of the sentence lives within the tensor space of the vector spaces of the words. Mathematically speaking, the meaning of a sentence is the image of a quantizing functor from the compact closed category that models the grammatical structure of the sentence (using Lambek Pregroups) to the compact closed category of finite dimensional vector spaces where the lexical meaning of the words are modeled. The meaning is computed via composing eta and epsilon maps that create Bell states and do substitution and as such allow the information to flow among the words within the sentence.

Currently a multi-site EPSRC proposal is being put together by Cambridge, Oxford, Edinburgh, York and Sussex, all leading centers in computational linguistics, to further develop this model.

Bibliography

[1] Samson Abramsky, Rick Blute, Bob Coecke, Marc Comeau, Tim Porter and Jamie Vicary. Compositional Quantum Relativity. Proceedings of the American Mathematical Society, to appear. 2010.

[2] Samson Abramsky and Bob Coecke. Categorical Quantum Mechanics. In: Handbook of Quantum Logic and Quantum Structures: Quantum Logic, ed. K. Engesser, D. Gabbay and D. Lehmann, pages 261–324, Elsevier 2009.

[3] Samson Abramsky and Nikos Tzevelekos. Introduction to categories and categorical logic. In [8]. 2010.

[4] H. Barnum, R Duncan, and Alexander Wilce. Convexity, categorical semantics and the foundations of physics. In B. Coecke, P. Panangaden, and P. Selinger, editors, Proceedings of 7th Workshop on Quantum Physics and Logic (QPL 2010), 2010.

[5] B. Bartlett and J. Vicary (2010) Topological quantum computation with Frobenius pseudoalgebras. Draft paper.

[6] Richard Blute and Prakash Panangaden. Dagger categories and formal distributions. In [8]. 2010.

[7] Lin Chen, Eric Chitambar, Runyao Duan, Zhengfeng Ji and Andreas Winter. Tensor rank and stochastic entanglement catalysis for multipartite pure states. 2010. arXiv:1003.3059.

[8] Bob Coecke (ed) - 1000 pp. New Structures for Physics. Springer Lecture Notes in Physics. Springer-Verlag. 2010.

[9] Bob Coecke. Quantum Picturalism. Contemporary Physics 51, 59-83. 2010. arXiv:0908.1787

[10] Bob Coecke. A Universe of Processes and Some of its Guises. In: Deep Beauty: Understanding the Quantum World through Mathematical Innovation. H. Halvorson (ed). Cambridge University Press. 2010.

[11] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. Accepted for New Journal of Physics. 2010. arXiv:0906.4725

[12] Bob Coecke and Aleks Kissinger. The compositional structure of multipartite quantum entanglement. In: Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP), pp. 297308, Lecture Notes in Computer Science 6199, Springer-Verlag. 2010. arXiv:1002.2540

[13] Bob Coecke and Ray Lal. Causal categories: a backbone for a quantum-relativistic universe of interacting processes. In Proceedings of the 7th International Workshop on Quantum Physics and Logic (QPL 2010), Oxford, 2010.

[14] Bob Coecke and E. O. Paquette. Categories for the practicing physicist. In [8]. 2010. arXiv:0808.1032

[15] Bob Coecke, Eric Oliver Paquette and Dusko Pavlovic. Classical and quantum structuralism. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 2969, Cambridge University Press. 2010. arXiv:0904.1997

[16] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In: Proceedings of the 19th EACSL Annual Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 6247, Springer-Verlag. 2010. arXiv:1004.1598

[17] Bob Coecke, Mehrnoosh Sadrzadeh and Stephen Clark. Mathematical Foundations for a Compositional Distributional Model of Meaning. Linguistic analysis, to appear, 2010. arXiv:1003.4394

[18] Bob Coecke and Robert W. Spekkens. Picturing classical and quantum Bayesian inference. Synthese, to appear. 2010.

[19] Bob Coecke, Quanlong Wang, Baoshan Wang, Yongjun Wang and Qiye Zhang. Graphic calculus for quantum key distribution. Electronic notes in theoretical computer science, to appear. 2010.

[20] Lucas Dixon, Ross Duncan and Aleks Kissinger. Quantomatic. http://dream.inf.ed.ac.uk/projects/quantomatic/

[21] Lucas Dixon, Ross Duncan and Aleks Kissinger. Open graphs and computational reasoning. Proceedings of Developments of Computational Models 2010 (DCM'10). 2010.

[22] Lucas Dixon and Aleks Kissinger. Monoidal categories, graphical reasoning and quantum computation. Proceedings of the Workshop on Computer Algebra Methods and Commutativity of Algebraic Diagrams (CAM-CAD). 2009.

[23] Ross Duncan and Simon Perdrix. Graph states and the necessity of euler decomposition. In K. Ambos-Spies, B. Lowe, and W. Merkle, editors, Computability in Europe: Mathematical Theory and Computational Practice (CiE'09), volume 5635 of Lecture Notes in Computer Science, pages 167-177. Springer, 2009.

[24] R. Duncan and S. Perdrix. Rewriting measurement-based quantum computations with generalised flow. In S. Abramsky, C. Gavoille, C Kirchner, F. Meyer auf der Heide, and P. G. Spirakis, editors, Automata, Languages and Programming, 37th International Colloquium, ICALP 2010, Proceedings Part II, volume 6199 of Lecture Notes in Computer Science, pages 285-296. Springer, 2010.

[25] Julia Evans, Ross Duncan, Alex Lang, and Prakash Panangaden. Classifying all mutually unbiased bases in rel. 2009. arXiv: 0909.4453

[26] S. Gay and I. Mackie (eds) Semantic Techniques for Quantum Computation, Cambridge University Press. 2010.

[27] Esfandiar Haghverdi and Philip Scott. Geometry of Interaction and the dynamics of proof reduction: a tutorial. In [8]. 2010.

[28] Chris Heunen. Complementarity in categorical quantum mechanics. Foundations of Physics, to appear. 2010.

[29] Chris Heunen. An embedding theorem for Hilbert categories. Theory and Applications of Categories 22, 321-344. 2009. arXiv:0811.1448

[30] P. Hines. Can a quantum computer run the von Neumann architecture? In [8]. 2010.

[31] P. Hines. Categorical analogues of monoid semirings, Mathematical Structures in Computer Science, to appear. 2010.

[32] P. Hines. Categorical coherence in quantum algorithms. Submitted.

[33] P. Hines and S. Braunstein. The structure of partial isometries, in Semantic Techniques in Quantum Computation, Cambridge University Press 361-389. 2010.

[34] P. Hines and P. J. Scott. Categorical traces from single-photon linear optics. Submitted.

[35] Prakash Panangaden and E. O. Paquette. A categorical presentation of quantum computation with anyons. In [8]. 2010.

[36] Anne Preller and Mehrnoosh Sadrzadeh. Bell States and Negative Sentences in the Distributed Model of Meaning. Electronic Notes in Theoretical Computer Science, to appear, 2010.

[37] P. Selinger. A survey of graphical languages for monoidal categories. In [8]. 2010. arXiv:0908.3347

[38] P. Selinger. Autonomous categories in which A is isomorphic to A*. Extended abstract. In Proceedings of the 7th International Workshop on Quantum Physics and Logic (QPL 2010), Oxford, 2010.

[39] Jamie Vicary. Categorical formulation of finite-dimensional quantum algebras. To appear in Communications in Mathematical Physics. 2010. arXiv:0805.0432

[40] Jamie Vicary. Completeness of dagger-categories and the complex numbers. To appear in the Journal of Mathematical Physics. 2010. arXiv:0807.2927

Chapter 6

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

A current account of W3 and comparison with the state-of-the-art. A central question in the study of quantum computation is relationship between the power of quantum information processing devices and classical computers. Bluntly stated: does quantum mechanics offer new computational power not available conventional machines? And how much? While a definitive answer remains elusive, the work of W3 has significantly advanced the state of the art on this area, and made an number important contributions toward mapping the frontiers of quantum information processing. We identify two broad themes within this work package.

Firstly, QICS researchers have introduced modifications to the standard theory of quantum mechanics and studied the computational power of these theories—as well as their mathematical structure—to cast light on the origins and limitations of quantum information processing. These modifications range from simple restrictions on the set of gates allowed in a quantum circuit, as seen in the work of Bremner (UNIVBRIS; QICS postdoc) Jozsa (UNIVBRIS) and Shepherd (UNIVBRIS), to esoteric non-local "post-quantum" theories considered by Barrett (UNIVBRIS). The role played by quantum non-locality has been emphasised also in the work of Skrzypczyk (UNIVBRIS) and Brunner (UNIVBRIS), and in the categorical setting by Coecke (Ox) and Edwards (Ox).

Secondly, researchers active on this work package have produced a large body of work dealing with the internal limitations of quantum information processing. These limitations express themselves in terms of the channel capacities obtained when using quantum resources to transmit classical information by Cubitt (UNIVBRIS), Harrow (UNIVBRIS) and Winter (UNIVBRIS), to quantum channel capacities by Hayden (McGill) and efficiency at carrying computational tasks such as simulating quantum measurements by Hayden (McGill) and Winter (UNIVBRIS). Again, non-locality is a key resource, for example in the work of Harrow (UNIVBRIS). We note here the very significant contribution by the McGill group.

As well this theoretical activity, this work package also encompasses a number of more practically oriented investigations. We highlight here the development of new quantum algorithms by Montanaro (UNIVBRIS; QICS postdoc), and Low (UNIVBRIS), the graphical calculus for quantum-classical interaction developed by Coecke (Ox) and Perdrix (Ox), and novel techniques for establishing private information by Bradler (McGill), Hayden (McGill) and Panangaden (McGill), and by Winter (UNIVBRIS) and coauthors. We mention also the involvement of Gühne (Innsbruck; QICS postdoc) in a number of experiments to test quantum non-contextuality.

Some of the main developments in W3

- In [14], Bremmer (UNIVBRIS), Jozsa (UNIVBRIS) and Shepherd (UNIVBRIS) provide important evidence for the power of quantum computation. They consider a restricted class of quantum circuits, called IQC, whose gates are all diagonal in the $|0\rangle \pm |1\rangle$ basis, and therefore all commute. In principle, circuits consisting of these gates are computationally weak since all gates could be applied simultaneously. Indeed the class IQC does not include many problems known to be in P, such as computing elementary arithmetic expressions (since the order of the operations is significant).

  The authors then address the question: how easy is it to simulate this class of quantum circuits on a classical computer? The notion of simulation the authors use is rather weak: given an IQC circuit with n input qubits, they require only the ability to classically *sample* its output distribution, and this sampling can tolerate a multiplicative error up to a 41%.

  The main result of the paper states that if this weak notion of simulation can be carried out efficiently—in time polynomial in n—then an infinite tower of classical complexity classes known as the polynomial hierarchy collapses down to its third level. Without going into the details, classical complexity theorists believe this to be unlikely.

  This result is very striking, especially in the context of the older work [37], as it suggests that even apparently compu-

tationally impoverished quantum classes like IQC contain a surprising amount of computational not found in classical models. Another notable fact is that IQC is actually *stronger* than necessary to cause the collapse, and a variety of weaker circuit models will suffice.

- It is well known that quantum mechanics has many features not found in the world of classical physics: the probabilistic measurement outcomes existence of incompatible observables, the impossibility of copying unknown states, the existence of strong non-local correlations etc. Less well-known is that these features, and indeed many of the distinctive informatic tasks that they allow, can also be performed in a larger class of non-local theories. These theories have been widely studied, partly to address the question: what is special about quantum mechanics among this class? One clue is that in many of these theories—which exhibit non-local correlations stronger than those found in quantum mechanics—make the complexity of various communication tasks trivial (c.f. Brunner (UNIVBRIS) and Skrzypczyk (UNIVBRIS) [16]).

  In [42], M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter (UNIVBRIS) and M. Zukowski introduce a new principle they call *information causality* Simply put this states that if Alice has some data set that is inaccessible to Bob, then despite using all his local resources, Bob can gain no more information than the number of classical bits transmitted to him by Alice. This principle allows is shown to produce Tsirelson's bound on non-local correlations, and hence excludes the stronger correlations found in general non-signalling theories.

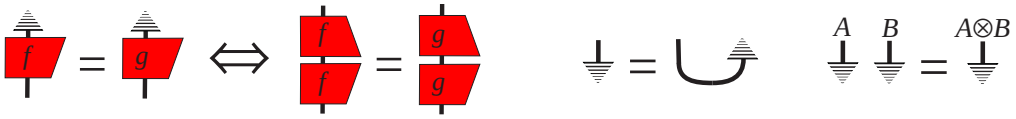
  Tsirelson's bound is however only one point on the boundary between quantum and non-quantum correlations, so information causality does not, *a priori*, exclude all possible non-quantum theories. Allcock (UNIVBRIS), Brunner (UNIVBRIS), Pawlowski and Scarani [5] expand that single point and demonstrate that a 2-dimensional section of the quantum boundary analytically coincides with the information causality criterion, although the their technique is not able to settle the question for the entire boundary.

  Barrett (UNIVBRIS) and a large group of coauthors [9] take another track to study informational causality in generic no-signalling theories by considering the role of two different forms of entropy, called the *mixing entropy* and the *measurement* entropy. Informally, the mixing entropy is the infimun of the Shannon entropies of all possible ways of preparing the system's state as a mixture of pure states; the measurement entropy is the minimum Shannon entropy of any possible measurement. In quantum theory these coincide, but this need not happen in more general theories. Theories where these quantities coincide, dubbed *monoentropic* enjoy strong restrictions on the geometry of the possible state spaces.

  The authors study information causality in the context on monoentropic theories and establish that the key property is not the strength of non-local correlations but rather the strong subadditivity of mutual information in these theories, and go on to establish sufficient conditions for monoentropic theories to have information causality.

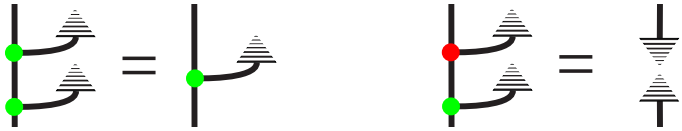
  Information causality is a strikingly simply and appealing principle, whose consequences have begun to be worked out by researchers in QICS project. Of great interest is the the relation between its operational restriction on non-locality and the algebraic characterisations developed by Edwards (Ox) [30].

- The ongoing effort to obtain an elegant representation for classical-quantum interaction in the diagrammatic language reached a milestone with the introduction of the concept of environment, or *ground*, satisfying:



  this gives rise to classical channel/decoherence and destructive and non-destructive measurement:

  which are subject to two simple properties:



  from which many correctness proofs of protocols straightforwardly follow [21].

Bob Coecke and Ross Duncan
Oxford, August 7, 2010.

Workpackage objectives: :

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

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

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

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

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

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

Workpackage milestones :

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

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

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

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

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

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

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

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

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

6.1 Progress towards objectives and performed tasks for W3.T1

6.1.1 Quantum algorithms and complexity

Complexity of quantum multi-prover interactive proof systems (Objectives/Milestones/Tasks: W3.O2, W3.O6, M3.T1) See 7.4.b in WP4 for a discussion.

The complexity of sampling a restricted class of quantum circuits (Objectives/Milestones/Tasks: W1.O1 W1.O3 W1.O4 W2.O2 W4.O2 W3.T1 W4.T1 W1.M5) In [14], Bremner (UNIVBRIS; QICS postdoc), Jozsa (UNIVBRIS) and Shepherd (UNIVBRIS) consider quantum computations comprising only commuting gates, known as IQP computations, and provide compelling evidence that the task of sampling their output probability distributions is unlikely to be achievable by any efficient classical means. More specifically they introduce the class post-IQP of languages decided with bounded error by uniform families of IQP circuits with post-selection, and prove first that post-IQP equals the classical class PP. Using this result they show that if the output distributions of uniform IQP circuit families could be classically efficiently sampled, even up to 41% multiplicative error in the probabilities, then the infinite tower of classical complexity classes known as the polynomial hierarchy, would collapse to its third level. They mention some further results on the classical simulation properties of IQP circuit families, in particular showing that if the output distribution results from measurements on only $O(\log n)$ lines then it may in fact be classically efficiently sampled.

The computational power of match-gate circuits (Objectives/Milestones/Tasks: W1.O1 W1.O2 W1.O4 W3.O2 W1.T1 W3.T1 W4.T1 W1.M5 W1.M6 W4.M1) Match-gates are an especially multiflorous class of two-qubit nearest neighbour quantum gates, defined by a set of algebraic constraints. They occur for example in the theory of perfect matchings of graphs, non-interacting fermions, and one-dimensional spin chains. In [37], Jozsa (UNIVBRIS), Kraus (UIBK), Miyake (UIBK; QICS postdoc) and Watrous show that the computational power of circuits of match-gates is equivalent to that of space-bounded quantum computation with unitary gates, with space restricted to being logarithmic in the width of the match-gate circuit. In particular, for the conventional setting of polynomial-sized (logarithmic-space generated) families of match-gate circuits, known to be classically simulatable, the authors characterise their power as coinciding with polynomial-time and logarithmic-space bounded universal unitary quantum computation.

Unstructured quantum search with probabilistic advice (Objectives/Milestones/Tasks: W1.O1 W4.O1 W3.T1 W3.T2 W3.M4) In [41], Montanaro (UNIVBRIS; QICS postdoc) considers the problem of search of an unstructured list for a marked element, when one is given advice as to where this element might be located, in the form of a probability distribution. The goal is to minimise the expected number of queries to the list made to find the marked element, with respect to this distribution. He presents a quantum algorithm which solves this problem using an optimal number of queries, up to a constant factor. For some distributions on the input, such as certain power law distributions, the algorithm can achieve exponential speed-ups over the best possible classical algorithm. He also gives an efficient quantum algorithm for a variant of this task where the distribution is not known in advance, but must be queried at an additional cost. The algorithms are based on the use of Grover's quantum search algorithm and amplitude amplification as subroutines.

Testing algorithms for the Clifford group (Objectives/Milestones/Tasks: W4.O2 W4.O6 W1.T1 W4.T1 W4.M1) Given oracle access to an unknown unitary C from the Clifford group and its conjugate, in [40] Low (UNIVBRIS) gives an exact algorithm for identifying C with $O(n)$ queries, which he proves is optimal. He then extends this to all levels of the Gottesman-Chuang hierarchy (also known as the C_k hierarchy). Further, for unitaries not in the hierarchy itself but known to be close to an element of the hierarchy, he gives a method of finding this close element. He also presents a Clifford testing algorithm that decides whether a given black-box unitary is close to a Clifford or far from every Clifford.

Mappings between classical spin systems and the stablizer formalism (Objectives/Milestones/Tasks: W1.M1, W3.T1) In [36] mappings between classical spin systems and quantum physics were investigated from a general perspective. More precisely, it was shown how to express partition functions and correlation functions of arbitrary classical spin models as inner products between quantum stabilizer states and product states. These mappings establish a link between the fields of classical statistical mechanics and quantum information theory, which can be utilised to transfer techniques and methods developed in one field to gain insight into the other.

Matroids and quantum probability distributions (Objectives/Milestones/Tasks: W1.O1 W1.O3 W1.O4 W2.O2 W4.O2 W3.T1 W4.T1 W1.M5) In [45], Shepherd (UNIVBRIS) characterises the probability distributions that arise from quantum circuits all of whose gates commute, and shows when these distributions can be classically simulated efficiently. He considers also marginal distributions and the computation of correlation coefficients, and draws connections between the simulation of stabiliser circuits and the combinatorics of representable matroids, as developed in the 1990s.

6.1.2 Resource inequalities

A father protocol for quantum broadcast channels (Objectives/Milestones/Tasks: W3.O2 W3.O4 W3.O5 W3.T1 W3.T2) In [29], Dupuis and Hayden (McGill) present a new protocol for quantum broadcast channels based on the fully quantum Slepian-Wolf protocol. 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.

The mother of all quantum protocols (Objectives/Milestones/Tasks: W3.O2 W3.O4 W3.O5 W3.O6 W3.T1 W3.T2) In [1], Winter (UNIVBRIS) et al give a simple, direct proof of the "mother" protocol of quantum information theory. In this new formulation, it is easy to see that the mother, or rather her generalization to the fully quantum Slepian-Wolf protocol, simultaneously accomplishes two goals: quantum communication-assisted entanglement distillation, and state transfer from the sender to the receiver. As a result, in addition to her other "children," the mother protocol generates the state merging primitive of Horodecki, Oppenheim and Winter, a fully quantum reverse Shannon theorem, and a new class of distributed compression protocols for correlated quantum sources which are optimal for sources described by separable density operators.

Moreover, 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.

The fidelity alternative and quantum measurement simulation (Objectives/Milestones/Tasks: W1.O2 W1.O3 W3.O2 W3.T1 W3.T2 W3.M4) If a quantum system is subject to noise, it is possible to perform quantum error correction reversing the action of the noise if and only if no information about the system's quantum state leaks to the environment. In [34], Hayden (McGill) and Winter (UNIVBRIS) develop an analogous duality in the case that the environment approximately forgets the identity of the quantum state, a weaker condition satisfied by weakly randomizing maps. Specifically, they show that the environment approximately forgets quantum states if and only if the original channel approximately preserves pairwise fidelities of pure inputs, an observation they call the fidelity alternative. Using this tool, they then go on to study the task of using the output of a channel to simulate restricted classes of measurements on a space of input states. The case of simulating measurements that test whether the input state is an arbitrary pure state is known as equality testing or quantum identification. The authors establish that the optimal amortized rate at which quantum states can be identified through a noisy quantum channel is equal to the entanglement-assisted classical capacity of the channel, despite the fact that the task is quantum, not classical, and entanglement-assistance is not allowed. In particular, this rate is strictly positive for every quantum channel, including classical channels, despite the fact that the ability to identify cannot be cloned.

Quantum reverse Shannon theorem (Objectives/Milestones/Tasks: W3.O1 W3.O2 W3.O3 W3.O5 W3.T1 W3.T2 W3.M1) In [10], Bennett, Devetak, Harrow (UNIVBRIS), Shor and Winter (UNIVBRIS) show how to use entanglement and noiseless quantum or classical communication to simulate discrete memoryless quantum channels with unit fidelity and efficiency in the limit of large block size. When the sender and receiver share enough standard ebits and are promised that the input to the channels is a memoryless (or i.i.d.) quantum source, their simulation uses an asymptotic rate of communication equal to the entanglement-assisted capacity of the channel. This communication rate also suffices for general (non-i.i.d.) sources if the ebits are replaced by a stronger entanglement resource, so-called entanglement-embezzling states, or if in addition to a supply of ebits, free backwards communication is allowed. Combined with previous coding theorems for entanglement-assisted classical communication over quantum channels, the results establish the ability of any channels to simulate any other, with an asymptotic efficiency given by the ratio of their entanglement-assisted capacities. This result can be used to prove a strong converse to the coding theorem for entanglement-assisted classical communication.

Conjugate degradability and quantum capacity of cloning channels (Objectives/Milestones/Tasks: W3.O2 W3.O4 W3.T1 W3.T2) A quantum channel is conjugate degradable if the channel's environment can be simulated up to complex conjugation using the channel's output. For all such channels, the quantum capacity can be evaluated using a single-letter formula. In [12], Hayden (McGill) et all introduce conjugate degradability and establish a number of its basic properties. We then use it to calculate the quantum capacity of N to N+1 and 1 to M universal quantum cloning machines as well as the quantum capacity of a channel that arises naturally when data is being transmitted to an accelerating receiver. All the channels considered turn out to have strictly positive quantum capacity, meaning they could be used as part of a communication system to send quantum states reliably.

Trade-off capacities of quantum Hadamard channels (Objectives/Milestones/Tasks: W3.O2 W3.O4 W3.T1 W3.T2 W3.M4) Coding theorems in quantum Shannon theory express the ultimate rates at which a sender can transmit information over a noisy quantum channel. More often than not, the known formulas expressing these transmission rates are intractable, requiring an optimization over an infinite number of uses of the channel. Researchers have rarely found quantum channels with a tractable classical or quantum capacity, but when such a finding occurs, it demonstrates a complete understanding of that channel's capabilities for transmitting classical or quantum information. In [13], Hayden (McGill) et al show that the three-dimensional capacity region for entanglement-assisted transmission of classical and quantum information is tractable for the Hadamard class of channels. Examples of Hadamard channels include generalized dephasing channels, cloning channels, and the Unruh channel. The generalized dephasing channels and the cloning channels are natural processes that occur in quantum systems through the loss of quantum coherence or stimulated emission, respectively. The Unruh channel is a noisy process that occurs in relativistic quantum information theory as a result of the Unruh effect and bears a strong relationship to the cloning channels. They give exact formulas for the entanglement-assisted classical and quantum communication capacity regions of these channels. The coding strategy for each of these examples is superior to a naive time-sharing strategy, and they introduce a measure to determine this improvement.

Improving zero-error classical communication with entanglement (Objectives/Milestones/Tasks: W2.O2 W2.O3 W3.O1 W3.O2 W3.T1 W3.T2 W3.M4) Given one or more uses of a classical channel, only a certain number of messages can be

transmitted with zero probability of error. The study of this number and its asymptotic behaviour constitutes the field of classical zero-error information theory, the quantum generalisation of which has started to develop recently. In [26], Cubitt (UNIVBRIS), Leung, Matthews and Winter (UNIVBRIS) show that, given a single use of certain classical channels, entangled states of a system shared by the sender and receiver can be used to increase the number of (classical) messages which can be sent with no chance of error. In particular, they show how to construct such a channel based on any proof of the Bell-Kochen-Specker theorem. This is a new example of the use of quantum effects to improve the performance of a classical task. The authors investigate the connection between this phenomenon and that of "pseudo-telepathy" games. The use of generalised non-signalling correlations to assist in this task is also considered. In this case, a particularly elegant theory results and, remarkably, it is sometimes possible to transmit information with zero-error using a channel with no unassisted zero-error capacity.

Superactivation of the zero-error classical capacity of a quantum channel (Objectives/Milestones/Tasks: W2.O2 W2.O3 W3.O1 W3.O2 W3.T1 W3.T2 W3.M4) The zero-error classical capacity of a quantum channel is the asymptotic rate at which it can be used to send classical bits perfectly, so that they can be decoded with zero probability of error. In [25], Cubitt (UNIVBRIS), Chen and Harrow (UNIVBRIS) show that there exist pairs of quantum channels, neither of which individually have any zero-error capacity whatsoever (even if arbitrarily many uses of the channels are available), but such that access to even a single copy of both channels allows classical information to be sent perfectly reliably. In other words, they prove that the zero-error classical capacity can be superactivated. This result is the first example of superactivation of a classical capacity of a quantum channel.

Entanglement spread and clean resource inequalities (Objectives/Milestones/Tasks: W2.O2 W3.O1 W3.O2 W3.T1 W2.M3 W2.M5) In [33], Harrow (UNIVBRIS) examines states that superpose different amounts of entanglement and protocols that run in superposition but generate or consume different amounts of entanglement. In both cases he finds a uniquely quantum difficulty: entanglement cannot be conditionally discarded without either using communication or causing decoherence.

The paper first describes the problem of entanglement spread in states and operations, as well as some methods of dealing with it. Then it describes three applications to problems that at first glance appear to be quite different: first, a reinterpretation of the old observation that creating n partially entangled states from singlets requires $\theta(\sqrt{n})$ communication, but cannot itself be used to communicate; second, a new lower bound technique for communication complexity; third, an explanation of how to extend the quantum reverse Shannon theorem from tensor power sources to general sources.

6.1.3 Classicality and quantumness in categorical models

Axiomatics for no-cloning (Objectives/Milestones/Tasks: W3.O2, W3.O3, W3.M4, W3.M6, W3.T2) In [2] Abramsky (Ox) opens up a novel perspective on No-Cloning, by finding a link to some fundamental issues in logic, computation, and the foundations of mathematics. A striking feature of these results is that they are visibly in the same genre as a well-known result by Joyal in categorical logic showing that a 'Boolean cartesian closed category' trivializes, which provides a major road-block to the computational interpretation of classical logic. In fact, they strengthen Joyal's result, insofar as the assumption of a full categorical product (both diagonals and projections) in the presence of a classical duality is weakened. This shows a heretofore unsuspected connection between limitative results in proof theory and No-Go theorems in quantum mechanics.

Categorical formulation of local hidden variable models (Objectives/Milestones/Tasks: W3.O2, W3.O6, W.T1) Coecke (Ox) and Edwards (Ox) [24] provide explicit mathematical definitions of Spekkens's toy qubit theory, in terms of a small set of generators, as well as in terms of an explicit form of all operations, as a subcategory MSpek of the category of finite sets, relations and the cartesian product. States of maximal knowledge form a subcategory Spek. This establishes the consistency of the toy theory, which has previously only been constructed for at most four systems. This formulation also shows that the theory is closed under both parallel and sequential composition of operations (= symmetric monoidal structure), that it obeys map-state duality (= compact closure), and that states and effects are in bijective correspondence (= dagger structure). From the perspective of categorical quantum mechanics, this provides an interesting alternative model which enables us to describe many quantum phenomena in a discrete manner, and to which mathematical concepts such as basis structures, and complementarity thereof, still apply. Hence, the framework of categorical quantum mechanics has delivered on its promise to encompass theories other than quantum theory.

Algebraic charcteristics of non-locality in toy theories (Objectives/Milestones/Tasks: W3.O2, W3.O6, W.T1) Coecke (Ox) , Edwards (Ox) and Spekkens [20] describe a general framework in which we can precisely compare the structures of quantum-like theories which may initially be formulated in quite different mathematical terms. This framework is used to compare two theories: quantum mechanics restricted to qubit stabiliser states and operations, and Spekkens's toy theory. Within

the framework these theories are very similar, but differ in one key aspect - a four element group we term the phase group which emerges naturally within our framework. In the case of the stabiliser theory this group is Z4 while for Spekkens's toy theory the group is Z2 x Z2. The structure of this group is intimately involved in a key physical difference between the theories: whether or not they can be modelled by a local hidden variable theory. This is done by establishing a connection between the phase group, and an abstract notion of GHZ state correlations. The authors formulate precisely how the stabiliser theory and toy theory are 'similar' by defining a notion of 'mutually unbiased qubit theory', noting that all such theories have four element phase groups. Since Z4 and Z2 x Z2 are the only such groups, then the GHZ correlations in this type of theory can only take two forms, exactly those appearing in the stabiliser theory and in Spekkens's toy theory. The results point at a classification of local/non-local behaviours by finite Abelian groups, extending beyond qubits to finitary theories whose observables are all mutually unbiased.

General characterisation of non-locality in categorical quantum mechanics (Objectives/Milestones/Tasks: W3.O2, W3.O6, W.T1) Interest has grown in recent years in the construction of 'quantum-like' theories, toy theories which exhibit some but not all features of quantum mechanics. Such theories are expressed in diverse mathematical terms which may impede comparison of their properties. In his DPhil thesis [30], Edwards (Ox) presents a unifying mathematical framework in which we can compare a variety of 'quantum-like' theories, based on Abramsky and Coecke's work on applying category theory to quantum mechanics. Doing so produces a clearer insight into the precise ways in which these theories differ mathematically, and whether this relates to the differences in phenomena which they predict. As an example of this kind of approach, Edwards expresses Spekkens's toy bit theory within the categorical framework, in the process proving its consistency. The toy bit theory reproduces many features of quantum mechanics, and this is reflected in the fact that within the categorical framework it shares many structural features with quantum mechanics. It differs however, in that it is, by construction, a local hidden variable theory. Edwards develops a categorical treatment of hidden variables, and then demonstrate that the categorical structures which differ between quantum mechanics and the toy theory are exactly those which relate to the question of hidden variables. He extends this to a general result applying to a wider range of theories.

The role of the phase group in Mermin-type no-go theorems (Objectives/Milestones/Tasks: W3.O2, W3.O6, W.T1) Basis structures (commutative isometric dagger Frobenius comonoids) arise in the categories associated with several quantum-like theories, where they provide the abstract counterparts of orthonormal bases, and are thus associated with the measurement of observables. Every basis structure has a corresponding Abelian group, termed its *phase group*. Previous work [24, 20] investigated the categories **Stab** and **Spek** which correspond respectively to qubit stabiliser quantum mechanics, and the toy bit theory proposed by Rob Spekkens (2007). The two categories exhibit different phase groups, Z_4 and $Z_2 \times Z_2$ respectively. It was shown that exactly this difference underlies the fact that while the predictions of the toy theory can be modelled by local hidden variables, those of the stabiliser theory cannot. In [31], Edwards (Ox) attempts to extend this result to more general phase groups. Whilst it does not succeed in encompassing all possible phase groups, it does extend the result to a large class, many of which might be expected to occur in the categories corresponding to theories of interest. The result is essentially a generalisation of Mermin's famous no-go theorem (Mermin, 1990) employing the GHZ state. The main result of the paper is linked to the subject of *group extensions*.

6.1.4 Non-locality and non-contextuality

Relational hidden variables and non-locality (Objectives/Milestones/Tasks: W3.O2, W3.O6, W3.T2) In [3], Abramsky uses a simple relational framework to develop the key notions and results on hidden variables and non-locality. The extensive literature on these topics in the foundations of quantum mechanics is couched in terms of probabilistic models, and properties such as locality and no-signalling are formulated probabilistically. To a remarkable extent, the main structure of the theory, through the major No-Go theorems and beyond, survives intact under the replacement of probability distributions by mere relations.

A new physical principle: Information Causality (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W3.T2 W2.M3 W2.M6) Quantum physics exhibits many remarkable features. For example, it gives probabilistic predictions (non-determinism), does not allow copying of unknown states (no-cloning), its correlations are stronger than any classical correlations but information cannot be transmitted faster than light (no-signaling). However, all the mentioned features do not single out quantum physics. A broad class of theories exist which share all of them with quantum mechanics and allow even stronger than quantum correlations. In [42], Winter (UNIVBRIS) and coauthors introduce the principle of Information Causality, stating that communication of m classical bits causes information gain of at most m bits. They show that this principle is respected both in classical and quantum physics, and that all stronger than quantum correlations violate it. The authors suggest that Information Causality, being a generalization of no-signaling, is one of the foundational properties of nature.

Recovering part of the quantum boundary from information causality (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W2.M3 W2.M6) Recently, the principle of information causality has appeared as a good candidate for an information-theoretic principle that would single out quantum correlations among more general non-signalling models. In [5], Allcock (UNIVBRIS), Brunner (UNIVBRIS), Pawlowski and Scarani present results going in this direction; namely they show that part of the boundary of quantum correlations actually emerges from information causality.

Entropy and Information Causality in General Probabilistic Theories (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W3.T2 W2.M3) In [9], Barrett (UNIVBRIS) and coauthors investigate the concept of entropy in probabilistic theories more general than quantum mechanics, with particular reference to the notion of information causality recently proposed by Pawlowski et. al. (arXiv:0905.2992). They consider two entropic quantities, which they term measurement and mixing entropy. In classical and quantum theory, they are equal, being given by the Shannon and von Neumann entropies respectively; in general, however, they are very different. In particular, while measurement entropy is easily seen to be concave, mixing entropy need not be. In fact, as the authors show, mixing entropy is not concave whenever the state space is a non-simplicial polytope. Thus, the condition that measurement and mixing entropies coincide is a strong constraint on possible theories.

Closure of theories with limited non-locality (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W2.M3 W2.M6) An intensive research effort has recently been devoted to understanding the properties of general non-signaling theories, which can contain more non-locality than quantum mechanics. In [6], Allcock (UNIVBRIS), Brunner (UNIVBRIS), Linden (UNIVBRIS), Popescu (UNIVBRIS), Skrzypczyk (UNIVBRIS) and Vertesi argue that in order to form self-consistent theories, sets of non-signaling correlations with limited non-locality must be closed under a natural class of operations called wirings. After introducing useful concepts and tools to address the issue of closure, they present several case studies. Furthermore they discuss the implications of their findings in the broader context of this line of research, in particular concerning the origin of the boundary between quantum and post-quantum correlations, and towards finding constraints on physical theories beyond quantum mechanics.

A trade-off between states and measurements (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W3.T2 W2.M3 W2.M6) Measurements on entangled quantum states can produce outcomes that are nonlocally correlated. But according to Tsirelson's theorem, there is a quantitative limit on quantum nonlocality. It is interesting to explore what would happen if Tsirelson's bound were violated. To this end, in [46] Short and Barrett (UNIVBRIS) consider a model that allows arbitrary nonlocal correlations, colloquially referred to as "box world". They show that while box world allows more highly entangled states than quantum theory, measurements in box world are rather limited. As a consequence there is no entanglement swapping, teleportation or dense coding.

Non-locality distillation and post-quantum theories with trivial complexity (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W3.T2 W2.M3 W2.M6) In [16], Brunner (UNIVBRIS) and Skrzypczyk (UNIVBRIS) first present a protocol for deterministically distilling non-locality, which is optimal under a general assumption. In particular their protocol works efficiently for a specific class of post-quantum non-local boxes, which they term correlated non-local boxes. In the asymptotic limit, all correlated non-local boxes are distilled to the maximally non-local box, the Popescu-Rohrlich box. Then, taking advantage of a recent result of Brassard et al. [Phys. Rev. Lett. 96, 250401 (2006)] they show that all correlated non-local boxes make communication complexity trivial, and therefore appear very unlikely to exist in nature. Astonishingly, some of these non-local boxes are arbitrarily close to the set of classical correlations. This result therefore gives new insight to the problem of why quantum non-locality is limited.

Couplers for Non-Locality Swapping (Objectives/Milestones/Tasks: W2.O2 W2.O3 W2.T2 W2.M3 W2.M6) In [47] Skrzypczyk (UNIVBRIS) and Brunner (UNIVBRIS) focus on non-locality swapping, the analogue of quantum entanglement swapping. In order to implement such a protocol, one needs a coupler that performs the equivalent of quantum joint measurements on generalized 'box-like' states. Establishing a connection to Bell inequalities, they define consistent couplers for theories containing an arbitrary amount of non-locality, which leads us to introduce the concepts of perfect and minimal couplers. Remarkably, Tsirelson's bound for quantum non-locality naturally appears in their study.

Leggett-Garg inequalities and the geometry of the cut polytope (Objectives/Milestones/Tasks: W3.O2, W3.M3, W3.T2)
The Bell and Leggett-Garg tests offer operational ways to demonstrate that non-classical behavior manifests itself in quantum systems, and experimentalists have implemented these protocols to show that classical worldviews such as local realism and macrorealism are false, respectively. Previous theoretical research has exposed important connections between more general Bell inequalities and polyhedral combinatorics. In [8], Hayden (McGill) and coauthors show that general Leggett-Garg

inequalities are closely related to the cut polytope of the complete graph, a geometric object well-studied in combinatorics. Building on that connection, they offer a family of Leggett-Garg inequalities that are not trivial combinations of the most basic Leggett-Garg inequalities. We then show that violations of macrorealism can occur in surprising ways, by giving an example of a quantum system that violates the new "pentagon" Leggett-Garg inequality but does not violate any of the basic "triangle" Leggett-Garg inequalities.

Entanglement consumption of instantaneous nonlocal quantum measurements (Objectives/Milestones/Tasks: W1.O1 W1.O2 W1.O4 W1.T1 W1.M5 W1.M6) Relativistic causality has dramatic consequences on the measurability of nonlocal variables and poses the fundamental question of whether it is physically meaningful to speak about the value of nonlocal variables at a particular time. Recent work has shown that by weakening the role of the measurement in preparing eigenstates of the variable it is in fact possible to measure all nonlocal observables instantaneously by exploiting entanglement. However, for these measurement schemes to succeed with certainty an infinite amount of entanglement must be distributed initially and all this entanglement is necessarily consumed. In [18], Popescu (UNIVBRIS) and coauthors sharpen the characterisation of instantaneous nonlocal measurements by explicitly devising schemes in which only a finite amount of the initially distributed entanglement is ever utilised. This enables them to determine an upper bound to the average consumption for the most general cases of nonlocal measurements. This includes the tasks of state verification, where the measurement verifies if the system is in a given state, and verification measurements of a general set of eigenstates of an observable. Despite its finiteness the growth of entanglement consumption is found to display an extremely unfavourable exponential of an exponential scaling with either the number of qubits needed to contain the Schmidt rank of the target state or total number of qubits in the system for an operator measurement. This scaling is seen to be a consequence of the combination of the generic exponential scaling of unitary decompositions combined with the highly recursive structure of their scheme required to overcome the no-signalling constraints of relativistic causality.

Zero-error channel capacity and simulation assisted by non-local correlations. (Objectives/Milestones/Tasks: W2.O2 W2.O3 W3.O1 W3.O2 W3.T1 W3.T2 W3.M4) In [27], Shannon's theory of zero-error communication is re-examined by Cubitt (UNIVBRIS), Leung, Matthews and Winter (UNIVBRIS) in the broader setting of using one classical channel to simulate another exactly, and in the presence of various resources that are all classes of non-signalling correlations: Shared randomness, shared entanglement and arbitrary non-signalling correlations. Specifically, when the channel being simulated is noiseless, this reduces to the zero-error capacity of the channel, assisted by the various classes of non-signalling correlations. When the resource channel is noiseless, it results in the "reverse" problem of simulating a noisy channel exactly by a noiseless one, assisted by correlations. In both cases, 'one-shot' separations between the power of the different assisting correlations are exhibited. The most striking result of this kind is that entanglement can assist in zero-error communication, in stark contrast to the standard setting of communicaton with asymptotically vanishing error in which entanglement does not help at all. In the asymptotic case, shared randomness is shown to be just as powerful as arbitrary non-signalling correlations for noisy channel simulation, which is not true for the asymptotic zero-error capacities. For assistance by arbitrary non-signalling correlations, linear programming formulas for capacity and simulation are derived, the former being equal (for channels with non-zero unassisted capacity) to the feedback-assisted zero-error capacity originally derived by Shannon to upper bound the unassisted zero-error capacity. Finally, a kind of reversibility between non-signalling-assisted capacity and simulation is observed, mirroring the famous "reverse Shannon theorem".

A multipartite non-local game with no quantum advantage (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W2.M3 W2.M6) In [7], Almeida, Bancal, Brunner (UNIVBRIS), Acin, Gisin and Pironio present a multipartite nonlocal game in which each player must guess the input received by his neighbour. They show that quantum correlations do not perform better than classical ones at this game, for any prior distribution of the inputs. There exist, however, input distributions for which general no-signalling correlations can outperform classical and quantum correlations. Some of the Bell inequalities associated to their construction correspond to facets of the local polytope. Thus their multipartite game identifies parts of the boundary between quantum and post-quantum correlations of maximal dimension. These results suggest that quantum correlations might obey a generalization of the usual no-signalling conditions in a multipartite setting.

Arbitrarily little knowledge can give a quantum advantage for nonlocal tasks (Objectives/Milestones/Tasks: W1.O1 W2.O2 W2.O3 W3.O2 W2.T2 W2.M3 W2.M6) It has previously been shown that quantum nonlocality offers no benefit over classical correlations for performing a distributed task known as nonlocal computation. This is where separated parties must compute the value of a function without individually learning anything about the inputs. In [4], Allcock (UNIVBRIS), Buhrman and Linden (UNIVBRIS) show that giving the parties some knowledge of the inputs, however small, is sufficient to unlock the power of quantum mechanics to out-perform classical mechanics. This role of information held locally gives new insight into the general question of when quantum nonlocality gives an advantage over classical physics. Their results also reveal a novel feature of the nonlocality embodied in the celebrated task of Clauser, Horne, Shimony and Holt.

Causality and nonlocal games. (Objectives/Milestones/Tasks: W3.O2, W3.O6, W3.T2) Multipartite probability distributions that respect causality form a convex polytope which vertices outside the local polytope are nonlocal boxes. Aiming to improve the understanding of multipartite nonlocal correlations, in [28] Degorre (Gren) and Mhalla (Gren) consider the case where m partners have each one bit of input and one bit of output. With each probability distribution over the inputs and outputs they associate a game defined by a set of forbidden pairs (questions, answers) which are the 0 coordinates of the probability distribution vector. The objective is to take benefit of a new graphical representation of these games to prove new properties about multiplayer games. This understanding of non local correlations directly implies limitations on what the physics laws allow us to do and can be used for example to prove the security of multipartite cryptographic protocols. It will also exhibit quantum correlations that can be used for deriving multipartite protocols that are not achievable classically. They introduce a new graphical representation for probability distributions and multipartite games such that the duality between strategies and probability distributions corresponds to the planar graphs' duality For two players the different sets of inputs and outputs are represented by the vertices of a 4×4 toric grid (weighted grid if the probability distributions are taken into account) in such a way that the dual grid represents the classical strategies. From this representation they derive a combinatorial characterization of causality, and of the set of games that can be won classically. The first step is to take benefit of this representation to have simple combinatorial proofs for some properties in the 2 player case, for example prove that the only nonlocal game is $a + b = xy$ where a and b are the outputs whereas x and y are the inputs.

Closing the detection loophole in Bell experiments using qudits (Objectives/Milestones/Tasks: W1.O1 W3.O2 W4.O1 W4.O6 W2.T2 W3.T1 W1.M5 W2.M3) In [48], Brunner (UNIVBRIS) and coauthors show that the detection efficiencies required for closing the detection loophole in Bell tests can be significantly lowered using quantum systems of dimension larger than two. They introduce a series of asymmetric Bell tests for which an efficiency arbitrarily close to $1/N$ can be tolerated using N-dimensional systems, and a symmetric Bell test for which the efficiency can be lowered down to 61.8% using four-dimensional systems. Experimental perspectives for the schemes look promising considering recent progress in atom-photon entanglement and in photon hyperentanglement.

Quantum experiments with human eyes as detector (Objectives/Milestones/Tasks: W1.O1 W3.O2 W4.O1 W4.O6 W2.T2 W3.T1 W1.M5 W2.M3) In [44], Brunner (UNIVBRIS) and coauthors show theoretically that the multi-photon states obtained by cloning single-photon qubits via stimulated emission can be distinguished with the naked human eye with high efficiency and fidelity. Focusing on the "micro-macro" situation realized in a recent experiment [F. De Martini, F. Sciarrino, and C. Vitelli, Phys. Rev. Lett. 100, 253601 (2008)], where one photon from an original entangled pair is detected directly, whereas the other one is greatly amplified, the authors show that performing a Bell experiment with human-eye detectors for the amplified photon appears realistic, even when losses are taken into account. The great robustness of these results under photon loss leads to an apparent paradox, which they resolve by noting that the Bell violation proves the existence of entanglement before the amplification process. However, they also prove that there is genuine micro-macro entanglement even for high loss.

Experimental testing of contextuality (Objectives/Milestones/Tasks: W3.O2) In [38] the group of R. Blatt in Innsbruck in collaboration with O. Guehne (QICS postdoc) performed the first experimental implementation of a state independent inequality for testing the Kochen Specker theorem using trapped ions. The experiment is not subject to the detection loophole and it was shown that, despite imperfections and possible measurement disturbances, the results cannot be explained in non-contextual terms.

Compatibility and noncontextuality for sequential measurements (Objectives/Milestones/Tasks: W3.O2) In the paper [32] O. Guehne (QICS postdoc) in collaboration with other researchers investigated possible loopholes in Kochen-Specker experiments. Especially the "compatibility loophole" was discussed and several methods to rule out certain hidden variable models which obey a kind of extended noncontextuality were presented. Finally, we applied the analysis to the recent trapped ion experiment of Kirchmair et al.

6.2 Progress towards objectives and performed tasks for W3.T2

6.2.1 Classical control categorically

Categorical axiomatics of classicality relative to quantumness (Objectives/Milestones/Tasks: W3.O2, W3.O5, W3.M4, W3.T2) Symmetric dagger-monoidal (SDM) categories have emerged as a convenient categorical formalization of quantum mechanics. The objects represent physical systems, the morphisms physical operations, whereas the tensors describe composite systems. Classical data turn out to correspond to Frobenius algebras with some additional properties. They express the distinguishing capabilities of classical data: in contrast with quantum data, classical data can be copied and deleted. In [19],

Coecke (Ox), Paquette (McGill) and Pavlovic (Ox) shift the paradigm of "quantization" of a classical theory to "classicization" of a quantum theory. Remarkably, the simple SDM framework suffices not only for this conceptual shift, but even allows us to distinguish the deterministic classical operations (i.e. functions) from the nondeterministic classical operations (i.e. relations), and the probabilistic classical operations (stochastic maps). Moreover, a combination of some basic categorical constructions (due to Kleisli, resp. Grothendieck) with the categorical presentations of quantum states, provides a resource sensitive account of various quantum-classical interactions: of classical control of quantum data, of classical data arising from quantum measurements, as well as of the classical data processing in-between controls and measurements. A salient feature here is the graphical calculus for categorical quantum mechanics, which allows a purely diagrammatic representation of classical-quantum interaction.

Diagrammatic methods for quantum and classical Bayesian reasoning (Objectives/Milestones/Tasks: W3.O2, W3.O4, W3.O5, W3.M4, W3.M5, W3.T1 W3.T2) [23] See WP2

Categorical axiomatics for choice of basis with applications to quantum key distribution (Objectives/Milestones/Tasks: W3.O2, W3.O5, W3.M4, W3.M5, W3.T2) Controlled complementary measurements are key to quantum key distribution protocols, among many other things. In [22] Coecke (Ox) et al axiomatize controlled complementary measurements within symmetric monoidal categories, which provides them with a corresponding graphical calculus. They study the BB84 and Ekert91 protocols within this calculus, including the case where there is an intercept-resend attack.

Diagrammatic calculus for mixed quantum classical protocols (Objectives/Milestones/Tasks: W3.O2, W3.O4, W3.M4, W3.M5, W3.T2) In [21] Coecke (Ox) and Perdrix (Ox) present a both simple and comprehensive graphical calculus for the pure quantum data and mixed classical data fragment of quantum computing, in particular including interaction of quantum and classical information flows. First, within categorical quantum mechanics they axiomatize the concept of an environment. This enables them to formalize classical channels and quantum measurement and classical control. They study the interaction of these notions in the case that the quantum measurements are complementary. They conclude that these concepts provide sufficient structural power for constructive representation and correctness derivation of typical quantum informatic protocols.

6.2.2 Quantum key distribution and quantum cryptography

Private information via the Unruh effect (Objectives/Tasks/Milestones: W3.O2 W3.O4 W3.T2) In a relativistic theory of quantum information, the possible presence of horizons is a complicating feature placing restrictions on the transmission and retrieval of information. In [11] Bradler (McGill), Hayden (McGill) and Panangaden (McGill) consider two inertial participants communicating via a noiseless qubit channel in the presence of a uniformly accelerated eavesdropper. Owing to the Unruh effect, the eavesdropper's view of any encoded information is noisy, a feature the two inertial participants can exploit to achieve perfectly secure quantum communication. They show that the associated private quantum capacity is equal to the entanglement-assisted quantum capacity for the channel to the eavesdropper's environment, which we evaluate for all accelerations.

Highly entangled states with almost no secrecy (Objectives/Milestones/Tasks: W1.01 W2.O2 W3.O1 W3.O2 W3.T1 W2.M3 W2.M5) In [17], Christandl, Schuch and Winter (UNIVBRIS) illuminate the relation between entanglement and secrecy by providing the first example of a quantum state that is highly entangled, but from which, nevertheless, almost no secrecy can be extracted. More precisely, they provide two bounds on the bipartite entanglement of the totally antisymmetric state in dimension d. First, they show that the amount of secrecy that can be extracted from the state is low, to be precise it is bounded by $O(1/d)$. Second, they show that the state is highly entangled in the sense that a large amount of singlets are needed to create the state: entanglement cost is larger than a constant, independent of d. In order to obtain these results the authors use representation theory, linear programming and the entanglement measure known as squashed entanglement.

Quantum mutual independence (Objectives/Milestones/Tasks: W2.O3 W3.O1 W3.O4 W3.O5 W2.T2 W3.T1 W3.M1 W3.M2 W3.M3) In [35], Winter (UNIVBRIS) and coauthors introduce the concept of mutual independence – correlations shared between distant parties which are independent of the environment. This notion is more general than the standard idea of a secret key – it is a fully quantum and more general form of privacy. The states which possess mutual independence also generalize the so called private states – those that possess private key. They then show that the problem of distributed compression of quantum information at distant sources can be solved in terms of mutual independence, if free entanglement between the senders and the receiver is available. Namely, they obtain a formula for the sum of rates of qubits needed to transmit a distributed state between Alice and Bob to a decoder Charlie. The authors also show that mutual independence is bounded from above by the relative entropy modulo a conjecture, saying that if after removal of a single qubit the state becomes product, its initial entanglement is bounded by 1. They suspect that mutual independence is a highly singular quantity, i.e. that

it is positive only on a set of measure zero; furthermore, they believe that its presence is seen on the single copy level. This appears to be borne out in the classical case.

Unconditional security from noisy quantum storage (Objectives/Milestones/Tasks: W2.O2 W3.O1 W3.O2 W3.T1 W2.M3 W2.M5) In [39], Wullschleger (UNIVBRIS) and coauthors consider the implementation of two-party cryptographic primitives based on the sole assumption that no large-scale reliable quantum storage is available to the cheating party. They construct novel protocols for oblivious transfer and bit commitment, and prove that realistic noise levels provide security even against the most general attack. Such unconditional results were previously only known in the so-called bounded-storage model which is a special case of our setting. The protocols can be implemented with present-day hardware used for quantum key distribution. In particular, no quantum storage is required for the honest parties.

Device independent quantum key distribution (Objectives/Milestones/Tasks: W2.O2, W2.O3, W2.O4, W2.T2, W2.M3) Device-independent quantum key distribution (DIQKD) represents a relaxation of the security assumptions made in usual quantum key distribution (QKD). As in usual QKD, the security of DIQKD follows from the laws of quantum physics, but contrary to usual QKD, it does not rely on any assumptions about the internal working of the quantum devices used in the protocol. In [43], Brunner (UNIVBRIS) and coauthors present in detail the security proof for a DIQKD protocol introduced in [Phys. Rev. Lett. 98, 230501 (2008)]. This proof exploits the full structure of quantum theory (as opposed to other proofs that exploit the no-signalling principle only), but only holds again collective attacks, where the eavesdropper is assumed to act on the quantum systems of the honest parties independently and identically at each round of the protocol (although she can act coherently on her systems at any time). The security of any DIQKD protocol necessarily relies on the violation of a Bell inequality. The authors discuss the issue of loopholes in Bell experiments in this context.

Entropic uncertainty relations (Objectives/Milestones/Tasks: W2.O2 W2.O3 W2.O4 W2.T2 W2.M3) Uncertainty relations play a central role in quantum mechanics. Entropic uncertainty relations in particular have gained significant importance within quantum information, providing the foundation for the security of many quantum cryptographic protocols. Yet, rather little is known about entropic uncertainty relations with more than two measurement settings. In [49], Wehner and Winter (UNIVBRIS) review known results and open questions.

Bibliography

[1] Anura Abeyesinghe, Igor Devetak, Patrick Hayden and Andreas Winter (2009) The mother of all protocols: Restructuring quantum information's family tree. Proceedings of the Royal Society A 465(2108):2537-2563, 2009; arXiv:quant-ph/0606225

[2] S. Abramsky No-cloning in categorical quantum mechanics. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 128, Cambridge University Press. 2009. arXiv:0910.2401

[3] Samson Abramsky. Relational Hidden Variables and Non-Locality. arXiv:1007.2754

[4] Jonathan Allcock, Harry Buhrman and Noah Linden (2009) Arbitrarily little knowledge can give a quantum advantage for nonlocal tasks. Phys. Rev. A 80, 032105, arXiv:0903.0586.

[5] Jonathan Allcock, Nicolas Brunner, Marcin Pawlowski and Valerio Scarani (2009) Recovering part of the quantum boundary from information causality. Phys. Rev. A 80, 040103(R), arXiv:0906.3464.

[6] Jonathan Allcock, Nicolas Brunner, Noah Linden, Sandu Popescu, Paul Skrzypczyk and Tamas Vertesi (2009) Closure of theories with limited non-locality. Phys. Rev. A 80, 062107, arXiv:0908.1496.

[7] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acin, N. Gisin and S. Pironio (2010) Guess your neighbour's input: a multipartite non-local game with no quantum advantage. Phys. Rev. Lett. 104, 230404, arXiv:1003.3844.

[8] David Avis, Patrick Hayden and Mark M. Wilde (2010) Leggett-Garg inequalities and the geometry of the cut polytope. arXiv:1004.3818 (submitted to Physical Review A)

[9] Howard Barnum, Jonathan Barrett, Lisa Orloff Clark, Matthew Leifer, Robert Spekkens, Nicolas Stepanik, Alex Wilce and Robin Wilke (2009) Entropy and Information Causality in General Probabilistic Theories. New J. Phys. 12 033024, arXiv:0909.5075.

[10] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor and Andreas Winter (2009) Quantum Reverse Shannon Theorem. arXiv:0912.5537.

[11] Kamil Bradler, Patrick Hayden and Prakash Panangaden. Private information via the Unruh effect. Journal of High Energy Physics 08:074, 2009. arXiv:0807.4536

[12] Kamil Bradler, Nicolas Dutil, Patrick Hayden and Abubakr Muhammad (2010) Conjugate Degradability and the Quantum Capacity of Cloning Channels. Journal of Mathematical Physics 51:072201, 2010; arXiv:0909.3297

[13] Kamil Bradler, Patrick Hayden, Dave Touchette and Mark M. Wilde (2010) Trade-off capacities of the quantum Hadamard channels. Physical Review A 81, 062312, 2010; arXiv:1001.1732

[14] Michael J. Bremner, Richard Jozsa and Dan J. Shepherd (2010) Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. Roy. Soc. A, to appear, arXiv:1005.1407.

[15] Anne Broadbent, Joseph Fitzsimons, Elham Kashefi (2010) QMIP = MIP*, submitted arXiv:1004.1130.

[16] Nicolas Brunner and Paul Skrzypczyk (2009) Non-locality distillation and post-quantum theories with trivial communication complexity. Phys. Rev. Lett. 102, 160403, arXiv:0901.4070.

[17] Matthias Christandl, Norbert Schuch and Andreas Winter (2009) Highly Entangled States With Almost No Secrecy. arXiv:0910.4151.

[18] S.R. Clark, A.J. Connor, D. Jaksch and S. Popescu (2010) Entanglement consumption of instantaneous nonlocal quantum measurements. arXiv:1004.0865.

[19] Bob Coecke, Eric Oliver Paquette and Dusko Pavlovic. Classical and quantum structuralism. In: Semantic Techniques for Quantum Computation, I. Mackie and S. Gay (eds), pages 2969, Cambridge University Press. 2010. arXiv:0904.1997

[20] Bob Coecke, Bill Edwards and Robert W. Spekkens. Phase groups and the origin of non-locality for qubits. Electronic Notes in Theoretical Computer Science, to appear. 2010. arXiv:1003.5005

[21] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. In: Proceedings of the 19th EACSL Annual Conference on Computer Science Logic (CSL), Lecture Notes in Computer Science 6247, Springer-Verlag. 2010. arXiv:1004.1598

[22] Bob Coecke, Quanlong Wang, Baoshan Wang, Yongjun Wang and Qiye Zhang. Graphic calculus for quantum key distribution. Electronic notes in theoretical computer science, to appear. 2010.

[23] Bob Coecke and Robert W. Spekkens. Picturing classical and quantum Bayesian inference. Synthese, to appear. 2010.

[24] Bob Coecke and Bill Edwards. Spekkens's toy theory as a category of processes. Proceedings of the American Mathematical Society, to appear.

[25] Toby S. Cubitt, Jianxin Chen and Aram W. Harrow (2009) Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel. arXiv:0906.2527.

[26] Toby S. Cubitt, Debbie Leung, William Matthews and Andreas Winter (2009) Improving zero-error classical communication with entanglement. arXiv:0911.5300.

[27] Toby S. Cubitt, Debbie Leung, William Matthews and Andreas Winter (2010) Zero-error channel capacity and simulation assisted by non-local correlations. arXiv:1003.3195.

[28] J. Degorre and M. Mhalla. Causality and nonlocal games. Invited talk at International Conference on Quantum Information and Technology, 2009.

[29] Frédéric Dupuis and Patrick Hayden (2010) A father protocol for quantum broadcast channels. IEEE Transactions on Information Theory 56(6):2946-2956, 2010; arXiv:quant-ph/0612155

[30] Bill Edwards. Non-locality in Categorical Quantum Mechanics. DPhil dissertation. University of Oxford. 2010.

[31] Bill Edwards. Phase groups and local hidden variables. Technical Report.

[32] O. Gühne, M. Kleinmann, A. Cabello, J.-A. Larsson, G. Kirchmair, F. Zähringer, R. Gerritsma, C.F. Roos Compatibility and noncontextuality for sequential measurements Phys. Rev. A 81, 022121 (2010) arXiv:0912.4846

[33] Aram W. Harrow (2009) Entanglement spread and clean resource inequalities. arXiv:0909.1557.

[34] Patrick Hayden and Andreas Winter (2010) The Fidelity Alternative and Quantum Measurement Simulation. arXiv:1003.4994 (submitted to IEEE Transactions on Information Theory)

[35] Michal Horodecki, Jonathan Oppenheim and Andreas Winter (2009) Quantum mutual independence. arXiv:0902.0912.

[36] R. Hübener, M. Van den Nest, W. Dür, H. J. Briegel (2009) Classical spin systems and the quantum stabilizer formalism: general mappings and applications J. Math. Phys. 50, 083303 arXiv:0812.2127

[37] Richard Jozsa, Barbara Kraus, Akimasa Miyake, John Watrous (2010) Matchgate and space-bounded quantum computations are equivalent. Proc. R. Soc. A 466, 809-830, arXiv:0908.1467.

[38] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos State-independent experimental test of quantum contextuality Nature 460, 494 (2009) arXiv:0904.1655

[39] Robert Koenig, Stephanie Wehner and Juerg Wullschleger (2009) Unconditional security from noisy quantum storage. arXiv:0906.1030.

[40] Richard Low (2009) Learning and Testing Algorithms for the Clifford Group. Phys. Rev. A Vol 80, 052314, arXiv:0907.2833.

[41] Ashley Montanaro (2010) Quantum search with advice. In Proc. TQC 2010, arXiv:0908.3066.

[42] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter and M. Zukowski (2009) A new physical principle: Information Causality. Nature 461, 1101, arXiv:0905.2292.

[43] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar and Valerio Scarani (2009) Device-independent quantum key distribution secure against collective attacks. New J. Phys. 11, 045021, arXiv:0903.4460.

[44] Pavel Sekatski, Nicolas Brunner, Cyril Branciard, Nicolas Gisin and Christoph Simon (2009) Quantum experiments with human eyes as detectors based on cloning via stimulated emission. Phys. Rev. Lett. 103, 113601, arXiv:0902.2896.

[45] Dan Shepherd (2010) Binary Matroids and Quantum Probability Distributions. arXiv:1005.1744.

[46] Anthony J. Short and Jonathan Barrett (2010) Strong nonlocality: A trade-off between states and measurements. New Journal of Physics 12, 033034, arXiv:0909.2601.

[47] Paul Skrzypczyk and Nicolas Brunner (2009) Couplers for Non-Locality Swapping. New J. Phys. 11 073014, arXiv:0812.0758.

[48] Tamas Vertesi, Stefano Pironio and Nicolas Brunner (2009) Closing the detection loophole in Bell experiments using qudits. Phys. Rev. Lett. 104, 060401, arXiv:0909.3171.

[49] Stephanie Wehner and Andreas Winter (2009) Entropic uncertainty relations - a survey. New J. Phys. 12 025009, arXiv:0907.3704.

Chapter 7

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

A current account of the objectives of W4 and comparison with the state-of-the art.

- Objective W4.O1 is concerned with understanding classically-controlled Quantum Computation in terms of a unified models. There are always many subquestions one can come up with, some of them extremely interesting, but last year already we were noticing that these have become very refined [3][4][5][34][41][40][51]. Therefore we believe that as much as such a wide research objective can be met, this is the case for W4.O1.
- Objective W4.O2 is concerned with understanding quantum control structures for Quantum Computation. Let us remind the reader that models such as Quantum Cellular Automata, or the linear-algebraic lambda-calculus do without the classical control structure that is made explicit in most models of Quantum Computation. Unfortunately, they do not directly address the question of the nature of this elusive notion of quantum control. Earlier in the QICS project, attempts to tackle this question had appeared in [43][55] but the results were still intermediate. This year however has seen the birth of a seminal ideas which are likely to bring contributions on this topic. Indeed, the preliminary work exposed in [35] shows that quantum computation with classical control with black boxes is strictly more expressive that the quantum gates model with black boxes, one of the first model for quantum control. Thus it raises a natural question: is quantum computation with quantum control with black boxes is strictly more expressive than quantum computation with classical control? But programming with quantum control raises some unitarity issues. [36] is an attempt to conciliate the programmable freedom allowed by an algebraic lambda-calculus with the orthogonality constraints of quantum control.
- Objective W4.O3 is concerned with understanding the structure of Quantum Cellular Automata. Last year we pointed that some radical progress had been made [18][19][21][27] towards this task. What we thought remained to be understood was the structure of Open QCA (i.e. when the evolution is a quantum operations, i.e. non-unitary, i.e. irreversible). In particular, we were looking for a robust axiomatisation of them. However, this year's research has lead us to think that no axiomatisation of them is possible; i.e. that their definitions will always remain constructive or trivially derived from the axiomatization of their unitary counterparts [20]. Beyond this difficulty, we got to the point where we can identify minimal, universal instances of Quantum Cellular Automata [22][23]. So we can say that Objective W4.O3 has been met. Witness of this, the change of focus which has happened this year in Quantum Cellular Automata research; towards the study of their dynamical properties [24][25][26][28], some of them very interesting.
- Objective W4.O4 is related to W4.O3 and W4.O6.
- Objective W4.O5 is about finding denotational semantics accommodating higher order functions in quantum functional languages. This point is detailed on page 59.
- Objective W4.O6 is concerned with developing theories and techniques for analysis and verification of concurrent classical plus quantum systems. Contributions on testing quantum properties have been developed this year [1][2]. This is complementary to the previous contributions in this objective, which is still very open.

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

When dealing with a programming language, an important question is to be able to describe the behavior of programs and to characterize the set of programs free from run-time error. A semantics for a programming language serves as a description of properties that valid programs verify. This permits to get insights on the capabilities of the language and the logic behind it through the Curry-Howard isomorphism. Provided that one can encode requirements and particular properties, a semantics can also be used as a tool for designing programs and deciding of the existence of program based on a given set of constraints.

A reasonable property for a logic is modus ponens. It requires the existence of implication in the logic. The corresponding programmatic feature is the notion of function and higher-order computation. A higher order function is a function that inputs or outputs a "blackbox", which is itself a function. Numerous algorithms in quantum computation are expressed in terms of black-box, making higher-order suitable for expressing them [34].

Regarding quantum higher-order, two approaches have been taken. The first one, called classical control, understand a quantum computer as a device attached to a classical computer. Quantum data is then thought of as living in an apparatus with special properties (such as, for example non-duplication of data). The second approach, called quantum control, focuses primarily on quantum operation and consider control (such as tests, loops, ...) encoded within the quantum structure.

In the following, we describe the known results on semantics for the two paradigms in the context of higher-order.

1. Classical control.

The formal study of the semantics of programming language for quantum computation with classical control has been initiated by Selinger in [60]. The language is functional and its semantics is based on the well-known notion of superoperators. The generalization to higher-order has been attacked by Selinger and Valiron [65][66][67][68][34]. The targeted language is a typed lambda-calculus for quantum computation including both classical and quantum data, featuring creations of quantum bits, measurements and unitary operations. For example, in such a language one can build a function that input a boolean and returns a function from quantum bits to quantum bits based on the input bit. The language is powerful enough for encoding all the usual quantum algorithms. It provides a canonical framework for dealing with quantum higher-order in the context of classical control, using a type system based on linear logic. Several papers steam from this seminal research paths. In [67], the authors develop a fully abstract model for the strictly linear fragment of the language. The semantics is based on the category of completely positive maps. Although the equality in the model matches precisely the operational equivalence of programs, the model contains to many morphisms. In [69], the author explore a possible approach for characterizing the precise image of the interpretation by adding a Kripke structure to the semantics. The interaction between duplication, non-duplication and side effects is studied in [68]. Here, the authors develop a categorical interpretation of the language. Based on Moggi's computational lambda-calculus and on Benton's linear-non-linear model, the description adds a probabilistic monad, accounting for the measurement, to a linear category, addressing the juxtaposition of duplicable and non-duplicable elements.

2. Quantum control.

Higher-order quantum control was first conceived [61] as the most natural generalization of a classical lambda-calculus with booleans: lambda-terms are encoded on quantum bits and the reduction is unitary. [61] shows that in order to enforce the orthogonality and norm requirements, terms in superposition need to be equal (up to the place where quantum bits occurs). To bypass this problem, two approaches have been taken so far. [62] consider a functional, first order language with quantum control and manipulating quantum bits, called QML. The language is interpreted through a compilation into quantum circuits. This compilation provides a denotation for the language in term of superoperators in the presence of measurement. If measurements are not considered, the category of isometries is enough [63]. Initiated by [64], a second approach forgets the orthogonality and norm requirements and focuses on the linear combination of lambda-terms. The study consider a generalization of van Tonder's calculus and analyzes precisely the reduction rules that are needed for keeping confluence of an untyped algebraic lambda-calculus called lineal. Various typed versions of the language are considered [38] but do not provide a semantical analysis. In [36], a connection is made between this approach and the approach taken in QML. A typed higher-order language is described, with both a notion of linear superposition of terms and a compilation into quantum circuits. It is a first step towards a denotational model for a lambda-calculus with quantum control. A more general approach is taken in [37], where the author describes a typed extended version of lineal: the linear combination of terms is understood as a computational structure la Moggi, yielding a categorical model in the form of an adjunction between a cartesian closed category and a category enriched over vector spaces (or modules). This approach draw a connection with the algebraic calculi coming from the semantics of linear logic [58, 59], and is related to the work done in [39].

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

- An interesting result had arisen last year, that was concerned with understanding the basic resources that are required for performing Quantum Computation. Actually this was [5] a negative result, expressing the fact that random quantum states are not of much use for Measurement-Based Quantum Computation. → *Understand, in the context of measurement-based quantum computing, what is the computational power of a given family of quantum states.*

- This year however has unraveled several fruitful connections between randomness and QIP. For instance it was shown in [1] that the knowledge of a probability distribution on the location of an element in an unstructured list can be fruitfully exploited to obtain a significant speed up of the Grover algorithm. More importantly, [3] shows that there is a clear benefit in using quantum algorithms to test properties of probability distributions. This could be an important contribution; in terms of finding new quantum algorithms; but also as a novel way to phrase quantum computation in general. → *Investigate how much of quantum computation can be phrased solely in terms of fast testing of properties of probability distributions.*

- In order to have a better understanding of the computational power of a quantum computer, [7] investigate which class of quantum gates are hard to simulate classically. They show that if one can efficiently simulate on a classical device a quantum computer restricted to commuting gates, then the polynomial hierarchy would collapse to its third level. → *Investigate which class of quantum gates are hard to simulate.*

In **Task 2**:

- What could it mean for a physical theory to be universal? Usually a physical theory is something that describes space and time, as well as some objects living upon this background and the way they interact. A sense in which a physical theory could be universal is if its is endowed with an object-to-object interaction which is non-trivial enough, so that any other object-to-object interaction could be built out of this one. Last year we tackled this fascinating question by giving explicit constructions in the simplified context of one-dimensional Quantum Cellular Automata (1DQCA). The n-dimensional case was left to be done, and this is what we have achieved this year [22]. It is interesting to notice that, in the three-dimensional case, this construction can be simplified down to a Partitioned QCA whose cells are qubits: hence we have built a minimal universal 3DQCA [23].

- Again consider in very broad terms a physical theory which describes space, time, as well as some objects living upon this background and the way they interact. Say that this theory is endowed with a well-defined notion of a global evolution, i.e. A forward step operator which acts across the entire space, taking the overall state from t to $t + 1$. Such a global evolution can be said to be causal if there exists a bound to the distance information can travel in one time step. Moreover a global evolution can be said to be locally implementable if it can be decomposed into smaller, elementary local evolutions, which involve only neighbouring sites. Because of entanglement it is far from trivial, in a quantum theoretical setting, to show that causality implies local implementability [18]. We solved this question when the global evolution is unitary and the space is discrete. Transplanted to Quantum Cellular Automata, this entails that the axiomatic definition of Schumacher and Werner admits a block structure, which turns out to be that of the constructive definition of Perez-Delgado and Cheung. This was achieved last year, but there remained several issues. On the one hand there were several other competing definitions of QCA around e.g. that of Watrous. This year we have shown [21] that these are also equivalent to the axiomatic definition. On the other hand, our main challenge was to tackle the axiomatisation of Open QCA (with non-unitary, quantum operations as evolutions). This question was settled negatively; a number of counter-examples discard the natural family of, tighter and tighter candidate axiomatizations [20]. Another, unexpected turn of event is the connection between causality and the validity of the Church-Turing thesis in quantum setting, that has arisen again through the structure theorem of [18] — and which we will discuss in 7.2. → *Axiomatize Quantum Cellular Automata over graphs rather than grids.*

- Classical (reversible) cellular automata research has progressed, about ten years ago, to shift its focus from fundamentals (set theoretical properties such as invertibility etc.) to dynamics (limiting behaviour properties such as periodicity, expansivity etc.). Hence the similar progression that has taken place this year in Quantum Cellular Automata research can only be viewed as a sign of maturity. There were numerous such interesting results this year: showing [24] that there exists classical dynamics which transport information faster in the quantum regime (with superpositions as inputs allowed) than in the classical regime (with only classical input states allowed), showing that [25] energy transport can be made more efficient by quantum effects, studying entanglement generation[31]H6, demonstrating analytically [26][32] the Andersen Localization (whereby a quantum particle stays localized) under an inhomogeneous Quantum Walk (which would never happen in an inhomogeneous classical random walk). → *Many more results are to be expected in looking*

at the dynamical properties of quantum evolutions: in terms of information conservation and transport. For instance we must improve our understanding of Andersen Localization in 3-dimensional inhomogeneous quantum walks.

In **Task 3**:

- Some of the most advanced known techniques are deployed to develop a denotational semantics for quantum programming languages. In [44], the order theory of inverse categories is studied. Contribution [70] addresses the problem of defining a semantics for higher order quantum information. The chosen language features two important properties. The first one, arising from the so-called no-cloning theorem of quantum computation, is the need for a distinction between duplicable and non-duplicable elements. For keeping track of duplicability at higher order, a type system inspired by the resource-sensitive linear logic is used. The second important aspect is the probability inherent to measurement, the only operation for retrieving classical data from quantum data. → *Move on to Quantum Control.*

- Contribution [38][36][37] provide a minimal and general Linear-Algebraic Lambda-Calculus, in which to explore quantum control, as well as potential Quantum Physical Logics that might arise from original type systems for the calculus, via the Curry-Howard Isomorphism. In [39] strong connections are established with the algebraic lambda calculus introduced by Vaux as a fragment of the differential lambda calculus. This contribution points out that the two lambda calculus are equivalent: the former is essentially call-by-value, whereas the latter is call-by-name. → *New semantical models for quantum computation derived from the algebraic lambda calculus. Extension of the call-by-name/call-by-value duality to the algebraic case.*

- In [45] the various developments of quantum programming languages lead to a practical application. Importing methods from abstract interpretation, an algorithm is described which works out the resources consumed by a quantum algorithm, in terms of how many entangled qubits are required for its well-functioning. → *Less coarse-grained analysis?*

In **Task 4**:

- [49] and [50] explores the properties of the quantum proof nets - a graph-theoretic syntax for logic proofs. In [49], they demonstrate how to represent quantum process as proof-nets and show that the dynamic of quantum process is captured by the cut elimination. In [50], proof-nets are inspired from Feynman diagrams.

- The development of a protocol for blind quantum computation [46] led to the development of fundamental results for interactive proof systems. Indeed in [47], it is shown that QMIP=MIP* which means that in the setting of multiple provers with shared entanglement, a quantum verifier is no more powerful than a classical one.

Future works left
These have been indicated in italics next to the above highlights of main developments in W4.

Interactions with other workpackages and sites

As in the previous year it remains the case that most interactions of W4 are with W1 as MBQC and the measurement calculus are indeed at the basis of several outcomes of W4: minimal resources for QC [5], blind quantum computing and interactive proofs [46],[47]. Some contributions are both in W1 and W2 [5],[51],[55], and some others both in W1 and a few make it to W3 [52],[54].

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

- between the Grenoble, Hannover, Oxford, and Paris sites, on QCA, quantum theory and computability, MBQC.

- between Bristol and Innsbruck on matchgates, energy transfer [25].

Pablo Arrighi, Simon Perdrix and Benoit Valiron
Grenoble, August 7, 2010.

Workpackage objectives :

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

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

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

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

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

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

Workpackage milestones :

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

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

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

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

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

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

W4.M7 A quantum functional language incorporating higher-order functions, non-terminating recursion, infinite 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, irreversibility in QCAs, universality and complexity of QCAs.

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

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

7.1 Progress towards objectives and performed tasks for W4.T1

1.a. [1] Quantum algorithms for testing properties of distributions. (Objectives W4.O2, W4.O6, Milestone W4.M1) Suppose one has access to oracles generating samples from two unknown probability distributions P and Q on some N-element set. How many samples does one need to test whether the two distributions are close or far from each other in the L_1-norm? This and related questions have been extensively studied during the last years in the field of property testing. In [1], Bravyi, Harrow (UNIVBRIS) and Hassidim study quantum algorithms for testing properties of distributions. It is shown that the L_1-distance between P and Q can be estimated with a constant precision using approximately $N^{1/2}$ queries in the quantum settings, whereas classical computers need $\Omega(N)$ queries. The authors also describe quantum algorithms for testing Uniformity and Orthogonality with query complexity $O(N^{1/3})$. The classical query complexity of these problems is known to be $\Omega(N^{1/2})$.

1.b. [2] Learning and Testing Algorithms for the Clifford Group. (Objectives W4.O2, W4.O6) Given oracle access to an unknown unitary C from the Clifford group and its conjugate, in [2] Low (UNIVBRIS) gives an exact algorithm for identifying C with $O(n)$ queries, which he proves is optimal. He then extends this to all levels of the Gottesman-Chuang hierarchy (also known as the C_k hierarchy). Further, for unitaries not in the hierarchy itself but known to be close to an element of the hierarchy, he gives a method of finding this close element. He also presents a Clifford testing algorithm that decides whether a given black-box unitary is close to a Clifford or far from every Clifford.

1.c. [3] Quantum search with advice. (Objective W4.O1) In [3], Montanaro (UNIVBRIS; QICS postdoc) considers the problem of search of an unstructured list for a marked element, when one is given advice as to where this element might be located, in the form of a probability distribution. The goal is to minimise the expected number of queries to the list made to find the marked element, with respect to this distribution. He presents a quantum algorithm which solves this problem using an optimal number of queries, up to a constant factor. For some distributions on the input, such as certain power law distributions, the algorithm can achieve exponential speed-ups over the best possible classical algorithm. He also gives an efficient quantum algorithm for a variant of this task where the distribution is not known in advance, but must be queried at an additional cost. The algorithms are based on the use of Grover's quantum search algorithm and amplitude amplification as subroutines.

1.d. [4] Nonadaptive quantum query algorithms for total functions. (Objective W4.O1) In [4], Montanaro (UNIVBRIS; QICS postdoc) shows that any bounded-error quantum query algorithm that computes some total boolean function depending on n variables, and whose queries to the input do not depend on the result of previous queries, must make Omega(n) queries to the input in total. Thus, in this restricted setting, quantum algorithms can achieve at most a constant factor speed-up over classical query algorithms.

1.e. [5] Are random pure states useful for quantum computation? (Objectives W4.O1, W4.O2; Milestones W4.M1, W4.M2) In [5] Bremner (UNIVBRIS; QICS postdoc), Mora and Winter (UNIVBRIS) show the following: a randomly chosen pure state as a resource for measurement-based quantum computation, is - with overwhelming probability - of no greater help to a polynomially bounded classical control computer, than a string of random bits. Thus, unlike the familiar "cluster states", the computing power of a classical control device is not increased from P to BQP, but only to BPP. The same holds if the task is to sample from a distribution rather than to perform a bounded-error computation. Furthermore, they show that their results can be extended to states with significantly less entanglement than random states.

1.f [6] Random Quantum Circuits are Approximate 2-designs. (Milestones W4.M1, W4.M6) Given a universal gate set on two qubits, it is well known that applying random gates from the set to random pairs of qubits will eventually yield an approximately Haar-distributed unitary. However, this requires exponential time. In [6] Harrow (UNIVBRIS) and Low (UNIVBRIS) show that random circuits of only polynomial length will approximate the first and second moments of the Haar distribution, thus forming approximate 1- and 2-designs. Previous constructions required longer circuits and worked only for specific gate sets. As a corollary of their main result, they also improve previous bounds on the convergence rate of random walks on the Clifford group.

1.g. [7] Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. (Objective W4.02) In [7], Bremner (UNIVBRIS; QICS postdoc), Jozsa (UNIVBRIS) and Shepherd (UNIVBRIS) consider quantum computations comprising only commuting gates, known as IQP computations, and provide compelling evidence that the task of sampling their output probability distributions is unlikely to be achievable by any efficient classical means. More specifically they introduce the class post-IQP of languages decided with bounded error by uniform families of IQP circuits with post-selection, and prove first that post-IQP equals the classical class PP. Using this result they show that if the output distributions of uniform IQP circuit families could be classically efficiently sampled, even up to 41

1.h. [8] Binary Matroids and Quantum Probability Distributions. In [8], Shepherd (UNIVBRIS) characterises the probability distributions that arise from quantum circuits all of whose gates commute, and shows when these distributions can be classically simulated efficiently. He considers also marginal distributions and the computation of correlation coefficients, and draws connections between the simulation of stabiliser circuits and the combinatorics of representable matroids, as developed in the 1990s.

1.i. [9] Matchgate and space-bounded quantum computations are equivalent (Milestone W4.M1) Matchgates are an especially multiflorous class of two-qubit nearest neighbour quantum gates, defined by a set of algebraic constraints. They occur for example in the theory of perfect matchings of graphs, non-interacting fermions, and one-dimensional spin chains. In [9], Jozsa (UNIVBRIS), Kraus (UIBK), Miyake (UIBK; QICS postdoc) and Watrous show that the computational power of circuits of matchgates is equivalent to that of space-bounded quantum computation with unitary gates, with space restricted to being logarithmic in the width of the matchgate circuit. In particular, for the conventional setting of polynomial-sized (logarithmic-space generated) families of matchgate circuits, known to be classically simulatable, the authors characterise their power as coinciding with polynomial-time and logarithmic-space bounded universal unitary quantum computation.

1.j. [10] Samson Abramsky. Big Toy Models: Representing Physical Systems As Chu Spaces. Synthese, to appear. 2010. arXiv:0910.2393 In [10] Abramsky pursues a model-oriented rather than axiomatic approach to the foundations of Quantum

Mechanics, with the idea that new models can often suggest new axioms. This approach has often been fruitful in Logic and Theoretical Computer Science. Rather than seeking to construct a simplified toy model, the author aims for a 'big toy model', in which both quantum and classical systems can be faithfully represented - as well as, possibly, more exotic kinds of systems. To this end, the author shows how Chu spaces can be used to represent physical systems of various kinds. In particular, the author shows how quantum systems can be represented as Chu spaces over the unit interval in such a way that the Chu morphisms correspond exactly to the physically meaningful symmetries of the systems - the unitaries and antiunitaries. In this way the author obtains a full and faithful functor from the groupoid of Hilbert spaces and their symmetries to Chu spaces. The authors also consider whether it is possible to use a finite value set rather than the unit interval; the author shows that three values suffice, while the two standard possibilistic reductions to two values both fail to preserve fullness.

1.k. [11] Samson Abramsky. Coalgebras, Chu Spaces, and Representations of Physical Systems. In: Proceedings of 25th IEEE conference on Logic in Computer Science. IEEE Press. 2010. arXiv:0910.3959 In [11], Abramsky revisits his earlier work on the representation of quantum systems as Chu spaces, and investigate the use of coalgebra as an alternative framework. On the one hand, coalgebras allow the dynamics of repeated measurement to be captured, and provide mathematical tools such as final coalgebras, bisimulation and coalgebraic logic. However, the standard coalgebraic framework does not accommodate contravariance, and is too rigid to allow physical symmetries to be represented. The author introduces a fibrational structure on coalgebras in which contravariance is represented by indexing. The author uses this structure to give a universal semantics for quantum systems based on a final coalgebra construction. The author characterizes equality in this semantics as projective equivalence. The author also defines an analogous indexed structure for Chu spaces, and use this to obtain a novel categorical description of the category of Chu spaces. The author uses the indexed structures of Chu spaces and coalgebras over a common base to define a truncation functor from coalgebras to Chu spaces. This truncation functor is used to lift the full and faithful representation of the groupoid of physical symmetries on Hilbert spaces into Chu spaces, obtained in our previous work, to the coalgebraic semantics.

1.l. [12] Quantum circuits giving oracles for abstract machine computations (Objective W4.O2) In [12] Hines (York) gives a concrete application, in the quantum circuit model, of the abstract categorical and domain-theoretic tools developed by the same author. Using a very general model of computation by conditional iteration, it is demonstrated how the underlying category theory allows one to not only characterise those computations which may be implemented reversibly, but to give concrete quantum circuits that provide oracles for such computations. This provides a systematic method of translating high-level classical computations based on conditional iteration into quantum oracles, given explicitly as quantum circuits. An immediate application is the ability to provide quantum circuits for computations performed by space-bounded Turing machines

1.m. [13] Categorical analogues of monoid semirings (Milestone W4.M6) In [13] Hines (York) proceeds to a very abstract categorical study of convolution products and their categorical analogues. By extending notions of summation familiar from algebraic program semantics to a more general setting, where both constructive and destructive interference may be modelled, it is demonstrated that the monoid semiring construction may be extended to the case where the monoid is replaced by an arbitrary category, and the semiring is replaced by a summation-enriched category. The ultimate aim of this program is two-fold; a formal setting for the constructions of [12] and a description of quantum Fourier transforms as components of a natural transformation between two functors, in a similar way to the description of categorical coherence isomorphisms as natural transformations between functors.

1.n. [14] Categorical traces from single-photon linear optics (Milestone W4.M6). In [14] Motivated by a single-photon though experiment, based on a modification of the Sagnac interferometer, Hines (York) and Scott introduces a general construction on linear maps that has a close connection to constructions from algebraic and categorical program semantics. By modelling this thought-experiment in a category of formal power series over linear maps, a partial categorical trace (generalising a particle-style trace on Hilbert spaces found in abstract logical models) is given, with this thought-experiment as the concrete realisation.

1.o. [15] Closing the detection loophole in Bell experiments using qudits. (Objectives W4.O1, W4.O6.) In [15], Brunner (UNIVBRIS) and coauthors show that the detection efficiencies required for closing the detection loophole in Bell tests can be significantly lowered using quantum systems of dimension larger than two. They introduce a series of asymmetric Bell tests for which an efficiency arbitrarily close to $1/N$ can be tolerated using N-dimensional systems, and a symmetric Bell test for which the efficiency can be lowered down to 61.8 using four-dimensional systems. Experimental perspectives for the schemes look promising considering recent progress in atom-photon entanglement and in photon hyperentanglement.

1.p. [16] Quantum experiments with human eyes as detectors based on cloning via stimulated emission. (Objectives W4.01, W4.06.) In [16], Brunner (UNIVBRIS) and coauthors show theoretically that the multi-photon states obtained by cloning single-photon qubits via stimulated emission can be distinguished with the naked human eye with high efficiency and fidelity. Focusing on the "micro-macro" situation realized in a recent experiment (See F. De Martini, F. Sciarrino, and C. Vitelli, Phys. Rev. Lett. 100, 253601) , where one photon from an original entangled pair is detected directly, whereas the other one is greatly amplified, the authors show that performing a Bell experiment with human-eye detectors for the amplified photon appears realistic, even when losses are taken into account. The great robustness of these results under photon loss leads to an apparent paradox, which they resolve by noting that the Bell violation proves the existence of entanglement before the amplification process. However, they also prove that there is genuine micro-macro entanglement even for high loss.

7.2 Progress towards objectives and performed tasks for W4.T2

2.a [17] Quantum Cellular Automata. (Objectives W4.O2, W4.O3, W4.O4; Milestone W4.M4, W4.M6) In [17] Wiesner (UNIVBRIS) reviews Quantum cellular automata (QCA), including early and more recent proposals. QCA are a generalization of (classical) cellular automata (CA) and in particular of reversible CA. The latter are reviewed shortly. An overview is given over early attempts by various authors to define one-dimensional QCA. These turned out to have serious shortcomings which are discussed as well. Various proposals subsequently put forward by a number of authors for a general definition of one- and higher-dimensional QCA are reviewed and their properties such as universality and reversibility are discussed.

2.b [18] Unitarity plus causality implies locality (Objectives W4.O2, W4.O3) In [18] Arrighi (Gren), Nesme (Brau, QICS post-doc) and Werner (Brau) consider a graph with a single quantum system at each node. The entire compound system evolves in discrete time steps by iterating a global evolution U. The authors require that this global evolution U be unitary, in accordance with quantum theory, and that this global evolution U be causal, in accordance with special relativity. By causal it is meant that information can only ever be transmitted at a bounded speed, the speed bound being quite naturally that of one edge of the underlying graph per iteration of U. They show that under these conditions the operator U can be implemented locally; i.e. it can be put into the form of a quantum circuit made up with more elementary operators – each acting solely upon neighbouring nodes. They apply this representation theorem to n-dimensional quantum cellular automata and show that they can be put into the form of an infinite tiling of more elementary, finite-dimensional unitary evolutions.

2.c [19] A quantum extension of Gandy's theorem (Objectives W4.O2, W4.O3, W4.M4) In [19] Arrighi (Gren) and Dowek (Paris, LIX) tackle the question of the interplay between computability and quantum theory, in a way that is inspired by Gandy. Gandy postulates properties of nature, such as homogeneity of space and time, bounded density and velocity of information, and proves that the physical Church thesis is a consequence of these postulates. The authors provide a quantum extension of Gandy's theorem.

2.d [20] On axiomatizations of Probabilistic Cellular Automata (Objectives W4.O2, W4.O3, W4.M4) In [20] Arrighi, Fargetton (Gren) and Nesme (Hanno) tackle the question of axiomatizations of Probabilistic Cellular Automata. Indeed, the celebrated Hendlund's theorem axiomatizes classical Cellular Automata as being shift-invariant continuous functions. In a similar vein, Schumacher and Werner, and then [18] axiomatize Quantum Cellular Automata as shift-invariant causal unitary operators. Both these axiomatizations come with characterisation, structure theorems: the axioms can be shown to lead to a more constructive, hands-on definition of (Quantum) Cellular Automata. Can the same be done for non-unitary QCA? Since quantum operations include probabilistic classical evolutions, this means we first have to see whether the same can be done with classical Probabilistic Cellular Automata. In this research report, the authors show through a series of counter-examples that Probabilistic Cellular Automata cannot be axiomatized. This discussion is reminiscent of prior works on Stochastic Einstein Locality and the Principle of common cause.

2.e. [21] Partitioned Quantum Cellular Automata are intrinsically universal (Objectives W4.O2, W4.O3) In [21] Arrighi and Grattage (Gren & Lyon) start by recalling the fact that there have been several different non-axiomatic approaches put forward to define Quantum Cellular Automata (QCA). A subclass of QCA, which is the most canonical of these non-axiomatic definitions, is the Partitioned QCA (PQCA). At the same time as PQCA were proposed, an axiomatisation of QCA emerged, which consists solely of an enumeration of the properties which the global evolution of the QCA should have. The question of whether these general QCA can be brought, without loss of generality, to the more concrete, operational forms is apparent. It was shown in [18] that any QCA can be put into a certain form given in Perez-Cheung, thus showing they are equivalent, in that one can be simulated by the other. The authors show that any QCA can be put into the form of a PQCA. Our proof reconciles all the non-axiomatic definitions of QCA, showing that they can all simulate one another, and that they are all equivalent to

the axiomatic definition. This is achieved by defining generalised n-dimensional intrinsic simulation, which brings the computer science based concepts of simulation and universality closer to theoretical physics. The result is not only an important simplification of the QCA model, but also a key step in the search for a minimal n-dimensional intrinsically universal QCA.

2.f. [22] A Simple n-Dimensional Intrinsically Universal Quantum Cellular Automaton (Objectives W4.O2, W4.O3, W4.M4) In [22] Arrighi and Grattage (Gren & Lyon) describe a simple n-dimensional quantum cellular automaton (QCA) capable of simulating all others, in that the initial configuration and the forward evolution of any n-dimensional QCA can be encoded within the initial configuration of the intrinsically universal QCA. Several steps of the intrinsically universal QCA 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.

2.g. [23] Quantum Game of Life (Objectives W4.O2, W4.O3, W4.M4) In [23] Arrighi and Grattage (Gren & Lyon) describe a 3-dimensional quantum cellular automaton (QCA) capable of simulating all others, in the sense that the initial configuration and the forward evolution of any other 3-dimensional QCA can be encoded within the initial configuration of this QCA. This powerful property has been referred to as intrinsic universality. The simplest way to describe a QCA is as a Partitioned QCA, la Watrous and [21]. As a Partitioned QCA of block size 2 and cell dimension 2, our intrinsically universal QCA is therefore minimal.

2.h. [24] Faster quantum signalling (Objectives W4.O2 W4.O3, Milestones W4.M4) In [24] Arrighi (Gren), Nesme (Hanno, QICS postdoc) and Werner (Hanno) show that there exists some dynamics such that information travels faster in the quantum regime than in the classical regime. Indeed consider some global, discrete, classical dynamics f, such that the state of each output physical system depends only on the state of a subset of the input physical systems — this determines the causal structure of f, which is captured by a dependency graph. When f is bijective, we can quantize this global dynamics just by linear extension, so that it turns into a unitary operator Qf acting upon this set of, now quantum, physical systems. The questions the authors address are: what becomes, then, of the dependency graph? How does this carry through asymptotically? The authors provide characterizations, optimal bounds and examples answering these questions.

2.i. [25] Motional effects on the efficiency of excitation transfer. (Objective W4.O6.) Energy transfer plays a vital role in many natural and technological processes. In [25], Asadian (UIBK), Tiersch (UIBK), Guerreschi (UIBK), Cai (UIBK), Popsecu (UNIVBRIS) and Briegel (UIBK) study the effects of mechanical motion on the excitation transfer through a chain of interacting molecules with application to the biological scenario of energy transfer in alpha-helices. Their investigation demonstrates that, for various types of mechanical oscillations, the transfer efficiency is significantly enhanced over that of comparable static configurations. This enhancement is a genuine quantum signature, and requires the collaborative interplay between the quantum-coherent evolution of the excitation and the mechanical motion of the molecules via their distance-dependent coupling; it has no analogue in the classical incoherent energy transfer. This effect may not only occur naturally, but it could be exploited in artificially designed systems to optimize transport processes. As an application, the authors discuss simple and hence robust control techniques.

2.j. [26] Inhomogeneous Quantum Walks. (Objective W4.O1, Milestone W4.M1.) In [26], Linden (UNIVBRIS) and Sharam (UNIVBRIS) study a natural construction of a general class of inhomogeneous quantum walks (namely walks whose transition probabilities depend on position). Within the class they analyze walks that are periodic in position and show that, depending on the period, such walks can be bounded or unbounded in time; in the latter case they analyze the asymptotic speed. The authors compare the construction to others in the existing literature. As an example they give a quantum version of a non-irreducible classical walk: the Polya Urn.

2.k. [27] Index Theory for One-dimensional Reversible Quantum Walks and Quantum Cellular Automata. (Objectives W4.O2, W4.O3, Milestone W4.M4) In [27] Gross, Nesme, Vogts and Werner (Hanno) define indexes for one-dimensional reversible QW and QCA. This is a very robust definition (you do not even have to assume shift invariance, not even in the cell structure) having many nice properties. For the composition of walks or automata, it is a group homomorphism. When considering the tensor product of walks or automata, it is a monoid homomorphism. The index is a continuous function, and takes different values on different connected components of the set of walks/automata. The index theory, together with other published articles on the structure of one-dimensional reversible cellular automata, pretty much closes the subject of the classification of these objects. Let us go into more details. If a one-dimensional quantum lattice system is subject to one step of a reversible discrete-time dynamics, it is intuitive that as much "quantum information" as moves into any given block of cells from the left, has to exit that block to the right. For two types of such systems - namely quantum walks and cellular automata - the authors make this intuition precise by defining an index, a quantity that measures the "net flow of quantum information"

through the system. The index supplies a complete characterization of two properties of the discrete dynamics. First, two systems S_1, S_2 can be pieced together, in the sense that there is a system S which locally acts like S_1 in one region and like S_2 in some other region, if and only if S_1 and S_2 have the same index. Second, the index labels connected components of such systems: equality of the index is necessary and sufficient for the existence of a continuous deformation of S_1 into S_2. In the case of quantum walks, the index is integer-valued, whereas for cellular automata, it takes values in the group of positive rationals. In both cases, the map $S \to indS$ is a group homomorphism if composition of the discrete dynamics is taken as the group law of the quantum systems. Systems with trivial index are precisely those which can be realized by partitioned unitaries, and the prototypes of systems with non-trivial index are shifts.

2.l. [28] The fractal structure of the space-time diagrams of Clifford Cellular Automata (Milestone W4.M4) In [28] Gütschow (Hanno) and Nesme (Hanno; QICS postdoc) explain the fractal structure of the space-time diagrams of Clifford Cellular Automata. When running QCA on some particular observables, one can often see a fractal structure emerge. They explain why this happens and how to "predict" this structure and find some of its properties, like its fractal dimension.

2.m. [29] Implementation of Clifford gates in the Ising-anyon topological quantum computer. (Objectives W4.O2, W4.O3, Milestone W4.M4) In [28] Andre Ahlbrecht, Lachezar S. Georgiev, Reinhard F. Werner (2009) a general proof for the existence and realizability of Clifford gates in the Ising topological quantum computer. The authors show that all quantum gates that can be implemented by braiding of Ising anyons are Clifford gates. The authors find that the braiding gates for two qubits exhaust the entire two-qubit Clifford group. Analyzing the structure of the Clifford group for n $\geq$ 3 qubits the authors prove that the the image of the braid group is a non-trivial subgroup of the Clifford group so that not all Clifford gates could be implemented by braiding in the Ising topological quantum computation scheme. The authors also point out which Clifford gates cannot in general be realized by braiding.

2.n. [30] Time Asymptotics and Entanglement Generation of Clifford Quantum Cellular Automata. (Objective W4.O2, Milestone W4.M4) In [30], Johannes Gtschow (Hanno), Sonja Uphoff, Reinhard F. Werner (Hanno), Zoltn Zimbors consider Clifford Quantum Cellular Automata (CQCAs) and their time evolution. CQCAs are an especially simple type of Quantum Cellular Automata, yet they show complex asymptotics and can even be a basic ingredient for universal quantum computation. In this work the authors study the time evolution of different classes of CQCAs. The authors distinguish between periodic CQCAs, fractal CQCAs and CQCAs with gliders. The authors then identify invariant states and study convergence properties of classes of states, like quasifree and stabilizer states. Finally the authors consider the generation of entanglement analytically and numerically for stabilizer and quasifree states.

2.o. [31] Entanglement Generation of Clifford Quantum Cellular Automata (Objective W4.O2, Milestone W4.M4) In [31] Johannes Gtschow (Hanno) recalls that Clifford quantum cellular automata (CQCAs) are a special kind of quantum cellular automata (QCAs) that incorporate Clifford group operations for the time evolution. Despite being classically simulable, they can be used as basic building blocks for universal quantum computation. This is due to the connection to translation-invariant stabilizer states and their entanglement properties. He gives a self-contained introduction to CQCAs and investigate the generation of entanglement under CQCA action. Furthermore, he discusses finite configurations and applications of CQCAs.

2.p. [32] Andre Ahlbrecht, Albert Werner, Volkher Scholz, Reinhard Werner, (2010) Andersen Localization in Disordered Quantum Walks, Draft paper. (Objective W4.O2, Milestone W4.M4) In [32] Andre Ahlbrecht, Albert Werner, Volkher Scholz and Reinhard Werner (Hanno), study a Spin-$\frac{1}{2}$-particle moving in a one dimensional lattice subjected to disorder induced by a random space dependent coin. The discrete time evolution is given by a family of random unitary quantum walk operators, where the shift operation is assumed to be non-random. Each coin is an independent identically distributed random variable with values in the group of two dimensional unitary matrices. They find that if the probability distribution of the coins is absolutely continuous with respect to the Haar measure, then the system exhibits localization. That is, every initially localized particle remains on average and up to exponential corrections in a finite region of space for all times.

2.q. [33] Hidden Quantum Markov Models and non-adaptive read-out of many-body states. (Milestone W4.M1) Stochastic finite-state generators are compressed descriptions of infinite time series. Alternatively, compressed descriptions are given by quantum finite-state generators (see K. Wiesner and J. P. Crutchfield, Physica D 237, 1173 (2008)). These are based on repeated von Neumann measurements on a quantum dynamical system. In [33], Wiesner (UNIVBRIS) and coauthors generalise the quantum finite-state generators by replacing the von Neumann projections by stochastic quantum operations. In this way they ensure that any time series with a stochastic compressed description has a compressed quantum description. Moreover, they establish a link between these stochastic generators and the sequential readout of many-body states with translationally-invariant matrix product state representations. As an example, they consider the non-adaptive read-out of 1D

cluster states. This is shown to be equivalent to a Hidden Quantum Model with two internal states, providing insight on the inherent complexity of the process. Finally, it is proven by example that the quantum description can have a higher degree of compression than the classical stochastic one.

7.3 Progress towards objectives and performed tasks for W4.T3

3.a. [34] Quantum lambda calculus (Objectives W4.O1, W4.O5, Milestone W4.M7) In [34], Selinger (Halifax) and Valiron (Grenoble) give an exposition of their design of the quantum lambda calculus, a typed higher-order programming language for quantum computation.

3.b. [35] Beyond Quantum Computers In [35] Valiron (Gre) et al. show that quantum higher order with classical control is potentially much more powerful than the usual quantum processing. There exists a program such that, although feasible, it cannot be realized by a usual quantum circuit. In order to implement this new kind of computation one needs to change the rules of quantum circuits, also considering circuits with the geometry of the connections that can be itself in a quantum superposition.

3.c. [36] Orthogonality and Algebraic Lambda-Calculus (Extended Abstract) Directly encoding lambda-terms on quantum strings while keeping a quantum interpretation is a hard task. As shown by van Tonder (2004), requiring a unitary reduction forces the lambda-terms in superposition to be mostly equivalent. In [36] Valiron (Gre) follows instead Arrighi and Diaz-Caro (2009) and shows how one can conceive a lambda-calculus with algebraic features and that admits a general notion of orthogonality amongst lambda-terms, by providing a compiler of the system into unitary maps.

3.d. [37] Semantics of a Typed Algebraic Lambda-Calculus In [37], Valiron (Gre) proposes a semantic analysis of a general simply-typed lambda-calculus endowed with a structure of vector space. He sketches the relation with two established vectorial lambda-calculi. Then he studies the problems arising from the addition of a fixed point combinator and how to modify the equational theory to solve them. He then sketches an algebraic vectorial PCF and its possible denotational interpretations.

3.e. [38] Scalar System F for Linear-Algebraic Lambda-Calculus: Towards a Quantum Physical Logic? (Objectives W4.O2, W4.O5) The aim of this work [38] by Arrighi and Diaz-Caro (Gren) is to set up a System F type system la Curry for the Linear-Algebraic lambda-Calculus (Lineal) [64] able to handle scalars within the types, and hence in some way characterise the amount of a type, following the idea of superposition in the sense of how much a term belongs to a type. The reason why the authors use Lineal is because it has the advantage of not being bound to a particular type system (being untyped), and it is general enough to describe any quantum computation in terms of vectors. This scalar type system is a the first step of a research program which seeks for a form quantum physical logic obtained via the Curry-Howard isomorphism; it is also interesting in itself because of its relations with probabilistic systems, Linear Logic (LL), cloning, etc.

3.f. [39] Equivalence of Algebraic Lambda-Calculi - work in progress. (Objective W4.O1, Milestones W4. M3) In [39], Diaz-Caro (Gren), Perdrix (Gren), Tasson and Valiron (Gren) examine the relationship between the algebraic lambda-calculus Lalg, a fragment of the differential lambda-calculus, and the linear-algebraic lambda-calculus Llin, a candidate lambda-calculus for quantum computation. Both calculi are algebraic: each one is equipped with an additive and a scalar-multiplicative structure, and the set of terms is closed under linear combinations. The authors answer the conjectured question of the simulation of Lalg by Llin and the reverse simulation of Llin by Lalg. Our proof relies on the observation that Llin is essentially call-by-value, while Lalg is call-by-name. The former simulation uses the standard notion of thunks, while the latter is based on an algebraic extension of the continuation passing style. This result is a step towards an extension of call-by-value / call-by-name duality to algebraic lambda-calculi.

3.g. [40] On the completeness of quantum computation models (Objectives W4.O1, W4.O5) The notion of computability is stable (i.e. independent of the choice of an indexing) over infinite-dimensional vector spaces provided they have a finite "tensorial dimension". In [40] Arrighi (Gre) and Dowek show that such vector spaces with a finite tensorial dimension permit to define an absolute notion of completeness for quantum computation models and give a precise meaning to the Church-Turing thesis in the framework of quantum theory. (Extra keywords: quantum programming languages, denotational semantics, universality.)

3.h. [41] Measurements and confluence in quantum lambda calculi with explicit qubits (Objective W4.O1) In [41] Diaz-Caro (Gren) et al. demonstrate how to add a measurement operator to quantum lambda-calculi. A proof of the consistency of the semantics is given through a proof of confluence presented in a sufficiently general way to allow this technique to be used for other languages. The method described here may be applied to probabilistic rewrite systems in general, and to add measurement to more complex languages such as QML or Lineal, which is the subject of further research.

3.i. [42] The structure of partial isometries This paper [42] studies both Neumann-Birkhoff quantum logic, and Abramsky-Coecke categorical quantum semantics using partial isometries - in particular, a partial order on partial isometries introduced by Halmos & McLaughlin. This partial order is shown to be a natural generalisation of the usual subspace ordering used in (lattice-theoretic) quantum logic. Using standard techniques from the field of inverse categories, a composition based on this partial order is given, allowing us to define a category of partial isometries that may reasonably be considered a categorification of Birkhoff-von Neumann quantum logic. This thus enables a comparison to be made with Abramsky-Coecke style categorical approaches to quantum mechanics. Explicit calculations are given, relating to the treatment of teleportation in both systems, that demonstrate a fundamental incompatibility between the two approaches. This is based on the differing treatment of post-selection by the two systems.

3.j. [43] Can a quantum computer run the von Neumann architecture? (Objective W4.O2) The von Neumann architecture is at the heart of almost every modern computer, and at the heart of the von Neumann architecture is the notion that program code may be manipulated in the same way as data. Categorically, this is a form of closure, familiar from a number of settings including logic, quantum mechanics, and theoretical computation. In [43], Hines (York) considers the practical utility of the von Neumann architecture in computer science, and whether quantum-mechanical realisations of such categorical closure (in particular, the Choi-Jamiolkowsky correspondence) will exhibit similar utility for quantum computation. It is demonstrated that neither the no-cloning nor the no-deleting theorems prevent such development; however, the Gottesmann-Knill theorem means that any quantum analogue of the von Neumann architecture will be restricted to the Clifford group of operations and thus be efficiently classically simulable.

3.k. [44] On the order theory of inverse categories (Objective W4.O5) In [44] Hines (York) studies the abstract properties of the natural partial ordering on inverse categories, with a concrete example being the Halmos-McLaughlin partial ordering on partial isometries he studied before. A particular result is that within a certain class of inverse categories (including partial isometries), the natural partial order on hom-sets is always a directed-complete partial order. Thus the partial isometries between two spaces form a Complete Partial Order (satisfying the appropriate continuity properties), where the down-closure of each maximal element is an orthomodular lattice.

7.4 Progress towards objectives and performed tasks for W4.T4

4.a. [46] Universal blind quantum computation In [46] Kashefi (Edin, Gren) et. al present a protocol which allows a client to have a server carry out a quantum computation for her such that the client's inputs, outputs and computation remain perfectly private, and where she does not require any quantum computational power or memory. The client only needs to be able to prepare single qubits randomly chosen from a finite set and send them to the server, who has the balance of the required quantum computational resources. The protocol is interactive: after the initial preparation of quantum states, the client and server use two-way classical communication which enables the client to drive the computation, giving single-qubit measurement instructions to the server, depending on previous measurement outcomes. Our protocol works for inputs and outputs that are either classical or quantum. They give an authentication protocol that allows the client to detect an interfering server; our scheme can also be made fault-tolerant. They also generalize the result to the setting of a purely classical client who communicates classically with two non-communicating entangled servers, in order to perform a blind quantum computation. By incorporating the authentication protocol, they show that any problem in BQP has an entangled two-prover interactive proof with a purely classical verifier.

4.b. [47] QMIP =MIP* In [47] Kashefi (Edin, Gren) et. al. study the long-standing open question of the way entanglement influences the power of quantum and classical multi-prover interactive proof systems. They show that the class of languages recognized by quantum multi-prover interactive proof systems, QMIP, is equal to MIP*, the class of languages recognized by classical multi-prover interactive proof systems where the provers share entanglement. After the recent result by Jain, Ji, Upadhyay and Watrous showing that QIP=IP, this work completes the picture from the verifier's perspective by showing that also in the setting of multiple provers with shared entanglement, a quantum verifier is no more powerful than a classical one: QMIP=MIP*. The central technique of the paper is based on the adaptation of universal blind quantum computation to the context of interactive proof systems. They show that in the multi-prover scenario, shared entanglement has a positive effect in

removing the need for a quantum verifier. As a consequence, their results show that the entire power of quantum information in multi-prover interactive proof systems is captured by the shared entanglement and not by the quantum communication.

4.c. [48] A logical analysis of entanglement and separability in quantum higher-order functions (Objective W4.O6; Milestone W4.M5) In this paper [48], Prost et al. (Gren) present a logical separability analysis for a functional quantum computation language. This logic is inspired by previous works on logical analysis of aliasing for imperative functional programs. Both analyses share similarities notably because they are highly non-compositional. Quantum setting is harder to deal with since it introduces non determinism and thus considerably modifies semantics and validity of logical assertions. This logic is the first proposal of entanglement/separability analysis dealing with a functional quantum programming language with higher-order functions.

4.d. [49] Generalised proof-nets for compact categories with biproducts Just as conventional functional programs may be understood as proofs in an intuitionistic logic, so quantum processes can also be viewed as proofs in a suitable logic. In [49] Duncan (Oxford QICS Post-doc) describes such a logic, the logic of compact closed categories and biproducts, presented both as a sequent calculus and as a system of proof-nets. This logic captures much of the necessary structure needed to represent quantum processes under classical control, while remaining agnostic to the fine details. The author demonstrates how to represent quantum processes as proof-nets, and show that the dynamic behaviour of a quantum process is captured by the cut-elimination procedure for the logic. The author shows that the cut elimination procedure is strongly normalising: that is, that every legal way of simplifying a proof-net leads to the same, unique, normal form. Finally, taking some initial set of operations as non-logical axioms, the author shows that that the resulting category of proof-nets is a representation of the free compact closed category with biproducts generated by those operations.

4.e. [50] Proof nets as formal Feynman diagrams The introduction of linear logic and its associated proof theory has revolutionized many semantical investigations, for example, the search for fully-abstract models of PCF and the analysis of optimal reduction strategies for lambda calculi. In [50] Blute and Panangaden (McGill) show how proof nets, a graph-theoretic syntax for linear logic proofs, can be interpreted as operators in a simple calculus. This calculus was inspired by Feynman diagrams in quantum field theory and is accordingly called the phi-calculus. The ingredients are formal integrals, formal power series, a derivative-like construct and analogues of the Dirac delta function. Many of the manipulations of proof nets can be understood as manipulations of formulas reminiscent of a beginning calculus course. In particular, a certain box construct behaves like an exponential and the nesting of boxes phenomenon is the analogue of an exponentiated derivative formula. The authors show that the equations for the multiplicative-exponential fragment of linear logic hold.

4.e [51] Temporally Unstructured Quantum Computation. (Objectives W4.O1, W4.O6; Milestones W4.M1, W4.M6, W4.M8) In [51] Shepherd (UNIVBRIS) and Bremner (UNIVBRIS; QICS postdoc) examine theoretic architectures and an abstract model for a restricted class of quantum computation, called here instantaneous quantum computation because it allows for essentially no temporal structure within the quantum dynamics. Using the theory of binary matroids, they argue that the paradigm is rich enough to enable sampling from probability distributions that cannot, classically, be sampled from efficiently and accurately. This paradigm also admits simple interactive proof games that may convince a skeptic of the existence of truly quantum effects. Furthermore, these effects can be created using significantly fewer qubits than are required for running Shor's Algorithm.

4.g. [52] Low Efficient Quantum Tensor Product Expanders and k-designs Harrow (UNIVBRIS) and Low (UNIVBRIS) in [52] give an efficient construction of constant-degree, constant-gap quantum k-tensor product expanders. The key ingredients are an efficient classical tensor product expander and the quantum Fourier transform. Their construction works whenever k=O(n/log n), where n is the number of qubits. An immediate corollary of this result is an efficient construction of approximate unitary k-designs on n qubits for any $k = O(\frac{n}{\log n})$.

4.h. [53] Large Deviation Bounds for k-designs. (Milestone W4.M1.) In [53], Low (UNIVBRIS) presents a technique for derandomising large deviation bounds of functions on the unitary group. He replaces the Haar distribution with a pseudo-random distribution, a k-design. k-designs have the first k moments equal to those of the Haar distribution. The advantage of this is that (approximate) k-designs can be implemented efficiently, whereas Haar random unitaries cannot. Low finds large deviation bounds for unitaries chosen from a k-design and then illustrates this general technique with three applications. He first shows that the von Neumann entropy of a pseudo-random state is almost maximal. Then he shows that, if the dynamics of the universe produces a k-design, then suitably sized subsystems will be in the canonical state, as predicted by statistical mechanics. Finally he shows that pseudo-random states are useless for measurement based quantum computation.

4.i. [54] Classical and Quantum Tensor Product Expanders. In [54], Hastings and Harrow (UNIVBRIS) introduce the concept of quantum tensor product expanders. These are expanders that act on several copies of a given system, where the Kraus operators are tensor products of the Kraus operator on a single system. They begin with the classical case, and show that a classical two-copy expander can be used to produce a quantum expander. They then discuss the quantum case and give applications to the Solovay-Kitaev problem. They give probabilistic constructions in both classical and quantum cases, giving tight bounds on the expectation value of the largest nontrivial eigenvalue in the quantum case.

4.j. [55] Quantum boolean functions (Objectives W4.O2, W4.O3) In [55], Montanaro (UNIVBRIS; QICS postdoc) and Osborne introduce the study of quantum boolean functions, which are unitary operators f whose square is the identity: f2= I. They describe several generalisations of well-known results in the theory of boolean functions, including quantum property testing; a quantum version of the Goldreich-Levin algorithm for finding the large Fourier coefficients of boolean functions; and two quantum versions of a theorem of Friedgut, Kalai and Naor on the Fourier spectra of boolean functions. In order to obtain one of these generalisations, they prove a quantum extension of the hypercontractive inequality of Bonami, Gross and Beckner.

4.k. [45] Abstract Interpretation Techniques for Quantum Computation (Objectives W4.O6) In [45], Jorrand and Perdrix (Gre) present two applications of abstract interpretation techniques in quantum computing. Quantum computing is a now well established domain of computer science, and the recent developments of semantic techniques attest of the vitality of this rapidly growing area. On the other hand, the proof has been made that abstract interpretation is a powerful theory (of classical computer science) for comparing more or less precise semantics of the same programming language. In a more general picture, abstract interpretation can be seen as a framework for comparing the precision of several representations of the same dynamic system evolution. In this paper, abstract interpretation is fruitfully used in quantum computing: (i) for establishing a hierarchy of quantum semantics and (ii) for analysing entanglement evolution.

4.l. [56] A short impossibility proof of Quantum Bit Commitment (Milestone W4.M8, Objective W4.O6) In [56] Chiribella, D'Ariano, Perinotti, Schlingemann (Hanno) and R. F. Werner (Hanno) study Bit commitment protocols, whose security is based on the laws of quantum mechanics alone, are generally held to be impossible on the basis of a concealment-bindingness tradeoff. A strengthened and explicit impossibility proof has been given in: G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A 76, 032328 (2007), in the Heisenberg picture and in a C*-algebraic framework, considering all conceivable protocols in which both classical and quantum information are exchanged. In the present paper the authors provide a new impossibility proof in the Schrodinger picture, greatly simplifying the classification of protocols and strategies using the mathematical formulation in terms of quantum combs, with each single-party strategy represented by a conditional comb. The authors prove that assuming a stronger notion of concealment–worst-case over the classical information histories–allows Alice's cheat to pass also the worst-case Bob's test. The present approach allows us to restate the concealment-bindingness tradeoff in terms of the continuity of dilations of probabilistic quantum combs with respect to the comb-discriminability distance.

4.m. [57] Quantum cryptography as a retrodiction problem (Milestone W4.M8, Objective W4.O6) In [57] A. H. Werner, T. Franz, R. F. Werner (Hanno) propose a quantum key distribution protocol based on a quantum retrodiction protocol, known as the Mean King problem. The protocol uses a two way quantum channel. The authors show security against coherent attacks in a transmission error free scenario, even if Eve is allowed to attack both transmissions. This establishes a connection between retrodiction and key distribution.

Bibliography

[1] Sergey Bravyi, Aram W. Harrow and Avinatan Hassidim (2009) Quantum algorithms for testing properties of distributions. In Proc. STACS'10, arXiv:0907.3920.

[2] Richard Low (2009) Learning and Testing Algorithms for the Clifford Group. Phys. Rev. A Vol 80, 052314, arXiv:0907.2833.

[3] Ashley Montanaro (2010) Quantum search with advice. In Proc. TQC 2010, arXiv:0908.3066.

[4] Ashley Montanaro (2010) Nonadaptive quantum query algorithms for total functions. arXiv:1001.0018.

[5] Michael J. Bremner, Caterina Mora, Andreas Winter (2009) Are random pure states useful for quantum computation? ArXiv: 0812.3001, Phys. Rev. Lett. 102, 190502.

[6] Aram Harrow and Richard Low (2009) Random Quantum Circuits are Approximate 2-designs, arXiv:0802.1919, Comm. Math. Phys. ,Volume 291, Number 1.

[7] Michael J. Bremner, Richard Jozsa and Dan J. Shepherd (2010) Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. Roy. Soc. A, to appear, arXiv:1005.1407.

[8] Dan Shepherd (2010) Binary Matroids and Quantum Probability Distributions. arXiv:1005.1744.

[9] Richard Jozsa, Barbara Kraus, Akimasa Miyake, John Watrous (2010) Matchgate and space-bounded quantum computations are equivalent. Proc. R. Soc. A 466, 809-830, arXiv:0908.1467.

[10] Samson Abramsky, (2010), Big Toy Models: Representing Physical Systems As Chu Spaces. Synthese, to appear, arXiv:0910.2393.

[11] Samson Abramsky. Coalgebras, Chu Spaces, and Representations of Physical Systems (2010). In: Proceedings of 25th IEEE conference on Logic in Computer Science. IEEE Press. arXiv:0910.3959.

[12] P. Hines (2010), Quantum circuits giving oracles for abstract machine computations, Theoretical Computer Science, Volume 411, Issues 11-13, Pages 1501-1520.

[13] P. Hines (2010), Categorical analogues of monoid semirings, invited subm. to Proc. Physics, Computation & Information, MFPS 2007, Mathematical Structures in Computer Science 1-36.

[14] P. Hines, P. Scott (2010, submitted) Categorical traces from single-photon linear optics Proc. Symp. App. Math.

[15] Tamas Vertesi, Stefano Pironio and Nicolas Brunner (2009) Closing the detection loophole in Bell experiments using qudits. Phys. Rev. Lett. 104, 060401, arXiv:0909.3171.

[16] Pavel Sekatski, Nicolas Brunner, Cyril Branciard, Nicolas Gisin and Christoph Simon (2009) Quantum experiments with human eyes as detectors based on cloning via stimulated emission. Phys. Rev. Lett. 103, 113601, arXiv:0902.2896.

[17] K. Wiesner (2008) Quantum Cellular Automata, ArXiv:0808.0679, Springer Encyclopedia of Complexity and Systems Science (2009).

[18] Pablo Arrighi, Vincent Nesme, Reinhard Werner, Unitarity plus causality implies locality, Pre-print arXiv:0711.3975, QIP 2010 long talk, accepted in JCSS.

[19] Pablo Arrighi, Gilles Dowek (2010), A quantum extension of Gandy's theorem, Draft paper.

[20] Pablo Arrighi, Renan Fargetton, Vincent Nesme (2010), On axiomatizations of Probabilistic Cellular Automata, Draft paper.

[21] Pablo Arrighi, Jonathan Grattage(2010), Partitioned Quantum Cellular Automata are intrinsically universal, Invited subm. to Proceedings of Physics and Computation 2009.

[22] Pablo Arrighi, Jonathan Grattage (2010), A Simple n-Dimensional Intrinsically Universal Quantum Cellular Automaton, Proceedings of the 4th International Conference on Language and Automata Theory and Applications (LATA 2010), Lecture Notes in Computer Science (LNCS). Journal version submitted to JCSS.

[23] Pablo Arrighi, Jonathan Grattage (2010), Quantum Game of Life, Draft paper.

[24] Pablo Arrighi, Vincent Nesme, Reinhard Werner (2010), Faster quantum signalling, arXiv:0910.4461.

[25] Ali Asadian, Markus Tiersch, Gian Giacomo Guerreschi, Jianming Cai, Sandu Popescu and Hans J. Briegel (2010) Motional effects on the efficiency of excitation transfer. arXiv:1002.0346.

[26] Noah Linden and James Sharam (2009) Inhomogeneous Quantum Walks. Phys. Rev. A 80, 052327, arXiv:0906.3692.

[27] D. Gross, V. Nesme, H. Vogts, R.F. Werner (2009) Index Theory for One-dimensional Reversible Quantum Walks and Quantum Cellular Automata. arXiv:0910.3675.

[28] J. G ”utschow and V. Nesme (2009). Draft paper.

[29] Andre Ahlbrecht, Lachezar S. Georgiev, Reinhard F. Werner (2009) Implementation of Clifford gates in the Ising-anyon topological quantum computer. Phys. Rev. A 79, 032311, arXiv:0812.2338.

[30] Johannes Gtschow, Sonja Uphoff, Reinhard F. Werner, Zoltn Zimbors, (2010) Time Asymptotics and Entanglement Generation of Clifford Quantum Cellular Automata, J. Math. Phys. 51, 015203.

[31] Johannes Gtschow, Entanglement Generation of Clifford Quantum Cellular Automata, (2009), to appear in the ”DPG spring meeting 2009” special issue of Applied Physics B, arXiv:1001.1062.

[32] Andre Ahlbrecht, Albert Werner, Volkher Scholz, Reinhard Werner, (2010) Andersen Localization in Disordered Quantum Walks, Draft paper.

[33] Alex Monras, Almut Beige and Karoline Wiesner (2010) Hidden Quantum Markov Models and non-adaptive read-out of many-body states. arXiv:1002.2337.

[34] P. Selinger, B. Valiron. (2009) Quantum lambda calculus. Book chapter. In Simon Gay and Ian Mackie, editors, Semantic Techniques in Quantum Computation, Cambridge University Press, pp. 135-172.

[35] G. Chiribella, G. M. D’Ariano, P. Perinotti, B. Valiron. Beyond Quantum Computers. Draft, 2009.

[36] B. Valiron. Orthogonality and Algebraic Lambda-Calculus (Extended Abstract). Proceedings of QPL’10, Oxford, May 29-30 2010.

[37] B. Valiron. Semantics of a Typed Algebraic Lambda-Calculus. Proceedings of the 6th workshop on Developments in Computational Models, Edinburgh, 9 10 July 2010.

[38] Pablo Arrighi, Alejandro Diaz-Caro, Scalar System F for Linear-Algebraic lambda-Calculus: Towards a Quantum Physical Logic? QPL’09, J. version submitted to TCS.

[39] A. Diaz-Caro, S. Perdrix, C. Tasson, and B. Valiron. Equivalence of Algebraic Lambda-Calculi - work in progress -. International Workshop on Higher-Order Rewriting (HOR’10, FLoC workshop). ArXiv:1005.2897.

[40] Pablo Arrighi, Gilles Dowek, On the completeness of quantum computation models, 6th conference on Computability in Europe, CiE 2010, Proceedings in LNCS

[41] Pablo Arrighi, Alejandro Diaz-Caro, Manuel Gadella, Jonathan Grattage, Measurements and confluence in quantum lambda calculi with explicit qubits, QPL’08, Pre-print arXiv:0806.2447

[42] Hines, Braunstein: The structure of partial isometries, Semantic Techniques in Quantum Computation, edited by Gay, S. and Mackie, I. (Cambridge University Press, Cambridge) 361-388 (2009).

[43] Hines: Can a quantum computer run the von Neumann architecture? in New Structures for Physics, Springer Lecture notes in Physics 1-43 (2010).

[44] P. Hines (in preparation) On the order theory of inverse categories.

[45] Jorrand, Perdrix. Abstract Interpretation Techniques for Quantum Computation. In Semantic Techniques in Quantum Computation. Cambridge University Press, 2010.

[46] Anne Broadbent, Joseph Fitzsimons, Elham Kashefi (2009), Universal blind quantum computation, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, and Measurement-based and Universal Blind Quantum Computation, Anne Broadbent, Joseph Fitzsimons, Elham Kashefi, In Formal Methods for Quantitative Aspects of Programming Languages, Edited by Alessandro Aldini, Marco Bernardo, Alessandra Di Pierro, Herbert Wiklicky, LNCS, 2010.

[47] Anne Broadbent, Joseph Fitzsimons, Elham Kashefi (2010) QMIP =MIP*, submitted arXiv:1004.1130.

[48] Frédéric. Prost, C. Zerrari, A logical analysis of entanglement and separability in quantum higher-order functions, UC 2009, LNCS pp 219-235, (2009).

[49] Ross Duncan. Generalised proof-nets for compact categories with biproducts. In Semantic Techniques in Quantum Computation, chapter 3, pages 70-134. Cambridge University Press, 2010.

[50] Richard Blute and Prakash Panangaden (McGill) (2010) Proof nets as formal Feynman diagrams in New structures in physics, B. Coecke Ed. Springer Lecture Notes in Physics. http://www.cs.mcgill.ca/ prakash/Pubs/phi_calc.pdf

[51] Dan Shepherd and Michael J. Bremner (2009) Temporally Unstructured Quantum Computation. Proc. Roy. Soc. A 465(2105) pp. 1413-1439, arXiv:0809.0847.

[52] Aram W. Harrow and Richard A. Low Efficient Quantum Tensor Product Expanders and k-designs. arXiv:0811.2597. In Proc. Of APPROX-RANDOM, volume 5687 of LNCS, pages 548–561. Springer, 2009.

[53] Richard Low (2009) Large Deviation Bounds for k-designs. Proc. R. Soc. A, 465(2111):3289-3308, arXiv:0903.5236.

[54] M. B. Hastings and A. W. Harrow (2009) Classical and Quantum Tensor Product Expanders. ArXiv:0804.0011, Q. Inf. Comp., 9(3&4):336 360.

[55] Ashley Montanaro and Tobias J. Osborne (2008) Quantum boolean functions. ArXiv:0810.2435, CJTCS, Vol 2010, Art. 1.

[56] G. Chiribella, G. M. D'Ariano, P. Perinotti, D. M. Schlingemann, R. F. Werner (2009) A short impossibility proof of Quantum Bit Commitment, arXiv:0905.3801

[57] A. H. Werner, T. Franz, R. F. Werner (2009) Quantum cryptography as a retrodiction problem, Phys. Rev. Lett. 103, 220504.

The following are not QICS production, or at least not of the recent years, but were cited:

[58] T. Ehrhard, L. Regnier, The differential lambda-calculus, Theoretical Computer Science, 309, 1-41, (2003).

[59] L. Vaux, On linear combinations of lambda-terms, Proceedings of RTA 2007, LNCS 4533, (2007).

[60] P. Selinger. Towards a quantum programming language, Mathematical Structures in Computer Science 14(4):527-586, 2004.

[61] A. van Tonder. A Lambda Calculus for Quantum Computation. Siam Journal on Computing 33 (5) pp. 1109-1135 (2004).

[62] J. Grattage. QML: A functional quantum programming language. Ph.D. Thesis.

[63] T. Altenkirch, J. Grattage, J. K. Vizzotto, and A. Sabry. An Algebra of Pure Quantum Programming. 3rd International Workshop on Quantum Programming Languages (QPL 2005).

[64] P. Arrighi and G. Dowek, Linear-algebraic lambda-calculus: higher-order, encodings and confluence in A. Voronkov, Rewriting techniques and applications, Lecture Notes in Computer Science, Springer-Verlag, 2008.

[65] B. Valiron. A functional programming language for quantum computation with classical control. M.Sc. Thesis, University of Ottawa, 2004.

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

[67] P. Selinger, B. Valiron. On a fully abstract model for a quantum linear functional language. roceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006), Oxford, July 17-19, 2006. ENTCS Volume 210, pp. 123-137, 2008.

[68] P. Selinger, B. Valiron. A linear-non-linear model for a computational call-by-value lambda calculus. Proceedings of the 11th International Conference on Foundation of Software Science and Computation Structures (FOSSACS'08), Budapest, March 29 - April 6, 2008. Springer LNCS 4962, pp. 81-96, 2008.

[69] B. Valiron. On Quantum and probabilistic linear lambda-calculi. roceedings of the joint 5th QPL and 4th DCM: Quantum Physics and Logic and Development of Computational Models (QPL/DCM 2008), Reykjavik, 2008.

[70] B. Valiron. Semantics for a Higher Order Functional Programming Language for Quantum Computation. Ph.D. Thesis, University of Ottawa, 2008.

Part IV

Consortium management

Consortium management

- QICS was extended for six months which enabled to develop research in new areas that combined ideas from several workpackages, and the school to take place in May 2010.
- Three consortium management meetings took place:
  - Two via Skype on the future of QICS;
  - One at the school on the overall success of QICS.
- With the move of Reinhard Werner from Brauschweig to Hannover the QICS side move with him.
- With the move of Richard Jozsa from Bristol to Cambridge, local coordination was takes over by Noah Linden, and W3 coordination was taken over by Oxford, by Coecke and Duncan.
- With the move of Simon Perdrix to Grenoble, he assisted in the coordination of W4.

Project timetable and status

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

Annex:
Plan for using and disseminating the knowledge

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