project no 033763

QICS

Foundational Structures for Quantum Information and Computation

Specific Targeted Research Project (STREP)

Thematic priority: Quantum Information Processing and Communications

DELIVERABLE D4

Quantum automata, machines and calculi

report for first reporting period

Feb. 15th 2008

Chancellor, Masters and Scholars of the University of Oxford

Contents

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

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

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

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

Main developments in W4. By studying several forms of abstract models of what quantum information processing devices can or should be, workpackage 4 has produced significant advances in understanding the structure, the mathematical and logical foundations, the operating principles and some of the computational properties of such devices :

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

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

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

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

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

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

The next steps to take. At this early stage, a number of challenging issues remain open questions in workpackage W4: understand all the facets of the classical vs. quantum control issue (objectives W4.O1, W4.O2, W4.03 and W4.O4, milestones W4.M4 and W4.M6), give a satisfactory account of irreversibility and complexity in QCA (objective W4.03, milestone W4.M4), establish theoretical grounds for systematic construction and manipulation of quantum+classical information processing tasks (objectives W4.O1 and W4.O5, milestones W4.M3 and W4.M7), find equivalence and compositional techniques for proofs of distributed quantum systems (objective W4.O6, milestone W4.M8), etc. As stated above, the work accomplished so far in workpackage W4 firmly paves the road toward reaching satisfactory answers to these questions.

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

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

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

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

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

Interactions among sites have been productive:

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

Philippe Jorrand
Grenoble, February 10, 2008.

Workpackage objectives:

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

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

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

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

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

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

Workpackage milestones:

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Progress towards objectives and performed tasks for W4.T1

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

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

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

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

2 Progress towards objectives and performed tasks for W4.T2

8.2.a Universal one-dimensional QCA (Objectives: W4.O3, W4.O4; Milestones: W4.T2, W4.M4). In [5], Arrighi (Gren) and Fargetton (Gren) give a one-dimensional quantum cellular automata (QCA) capable of simulating all others. This means that the initial configuration and the local transition rule of any one-dimensional QCA can be encoded within the initial configuration of the universal QCA. Several steps of the universal QCA will then correspond to one step of the simulated QCA. The simulation preserves the topology in the sense that each cell of the simulated QCA is encoded as a group of adjacent cells in the universal QCA. The encoding is efficient and hence does not carry any of the weight of the computation.

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

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

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

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

3 Progress towards objectives and performed tasks for W4.T3

3.1 Quantum calculi

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

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

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

3.2 Quantum semantics

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

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

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

8.3.2.d Semantics for entanglement (Objectives: W4.O6; Milestones: W4.M5). Entanglement is a non local property of quantum states which has no classical counterpart and plays a decisive role in quantum information theory. The exact role of the entanglement is nevertheless not well understood. Since an exact analysis of entanglement evolution induces an exponential slowdown, Perdrix (Gren & Paris & QICS postdoc at Ox) considers approximative analysis based on the framework of abstract interpretation. A concrete quantum semantics based on super-operators is associated with a simple quantum programming language. The representation of entanglement, i.e. the design of the abstract domain is a key issue. A representation of entanglement as a partition of the memory is chosen. An abstract semantics is introduced, and the soundness of the approximation is proven. These results have been presented at the 2nd QNET workshop in UK.

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

3.3 Quantum languages

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

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

3.4 Logic within quantum computational models

8.3.4.a Undecidable logic and measurement-based quantum computation (Objectives: W1.O1, W1.O4, W4.O1, W4.O6; Milestones: W1.M2, W1.M5, W4.M3). In [16] Van den Nest (Inn) and Briegel (Inn) establish a connection between measurement-based quantum computation with graph states and the field of mathematical logic. They show that the computational power of graph states, representing resources for measurement-based quantum computation, is reflected in the expressive power of (classical) formal logic languages defined on the underlying mathematical graphs. In particular, the authors show that for all graph state resources which yield a computational speed-up with respect to classical computation, the underlying graphs—describing the quantum correlations of the states—are associated with undecidable logic theories. Here undecidability is to be interpreted in a sense similar to Gödel's incompleteness results, meaning that there exist propositions, expressible in the above classical formal logic, which cannot be proven or disproven.

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

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

4 Progress towards objectives and performed tasks for W4.T4

4.1 Quantum process calculi.

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

4.2 Reasoning about knowledge in quantum protocols

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

4.3 Tools for verification

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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