project no 033763

QICS

Foundational Structures for Quantum Information and Computation

Specific Targeted Research Project (STREP)

Thematic priority: Quantum Information Processing and Communications

DELIVERABLE D1

Structures and methods for measurement-based quantum computation

report for first reporting period

Feb. 15th 2008

Chancellor, Masters and Scholars of the University of Oxford

Contents

1 Progress towards objectives and performed tasks for W1.T1. 5
1.1 Computational universality of resource states for measurement-based quantum computation . . . 5
1.2 Computational and algorithmic complexity of quantum computation . . . 5
1.3 Mathematical properties of graph states . . . 6
1.4 General properties for measurement based quantum computing . . . 6
1.5 Quantum machines and measurement based quantum computing . . . 7

2 Progress towards objectives and performed tasks for W1.T2 7
2.1 Resources for measurement-based quantum computing . . . 7
2.2 General properties of graph states . . . 8

3 Progress towards objectives and performed tasks for W1.T3 8
3.1 Calculi for one-way computing . . . 8
3.2 Graphical calculus and categorical semantics for measurement based quantum computing . . . 9
3.3 Automated reasoning tools for measurement based quantum computing . . . 9

A current account of the objectives of W1 and comparison with the state-of-the art. When the project started, measurement-based quantum computation (MQC) was already an established scheme for quantum computation in the sense that a worked-out "manual" e.g. for one-way computation (as well as other schemes of MQC), existed and was well understood. This allowed one to e.g. translate any quantum logic circuit into a measurement pattern and a set of rules how to process the classical measurement outcomes. Furthermore, the fault-tolerance of the scheme had already been proven, even though the threshold has been improved significantly in the meantime. [see e.g. work by Raussendorf et al. PRL 98, 190504 (2007)]. The latter point is, for example, in clear contrast with the current status of quantum adiabatic computation, another hot topic in computational models, where the possible application of quantum error correction has yet to be clarified.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Hans-Jurgen Briegel
Innsbruck, February 10, 2008.

Workpackage objectives :

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

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

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

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

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

Workpackage milestones :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.1.b Phase transition of computational power of measurement-based quantum computer (Objectives: W1.O1, W1.O3; Milestones: W1.M1, W1.M6). In [3], Browne (Ox), Miyake (QICS postdoc at Inn) and their colleagues have tackled a fundamental question on the origin of computational superior power of quantum computer. We considered a simplified model, motivated by the optical lattice implementation of measurement-based quantum computer, and studied how heralded qubit losses during the preparation of a two-dimensional cluster state, a universal resource state for one-way quantum computation, affect its computational power. Above the percolation threshold we present a polynomial-time algorithm that concentrates a universal cluster state, using resources that scale optimally in the size of the original lattice. On the other hand, below the percolation threshold, we show that measurement-based quantum computation on the faulty lattice allows an efficient simulation by classical computers. We observe a phase transition at the threshold when the amount of entanglement in the faulty lattice directly relevant to the computational power changes exponentially.

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

1.2 Computational and algorithmic complexity of quantum computation

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

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

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

1.3 Mathematical properties of graph states

5.1.3.a Graph states as ground states of many-body Hamiltonians (Objective: W1.O3, W1.O4; Milestones: W1.M1). In [9], Van den Nest (Inn), Luttmer (Inn), Duer (Inn), and Briegel (Inn) have analyzed the criteria when graph states are obtained as non-degenerate ground states of interaction Hamiltonians. While we find that many-body interactions are required for any graph state not corresponding to a 1D structure if one considers systems of a fixed size, the usage of auxiliary systems allows for the design of two-body Hamiltonian that have graph states as approximate ground state. This research is of particular interest in the context of the optical lattices, as it provides a potential alternative way of preparing highly entangled resource states (such as graph states) by simply cooling a system with a properly designed interaction Hamiltonian. This might be easier than generating entanglement by performing sequences of gates on some initial prepared product state in a coherent way.

5.1.3.b LU-LC conjecture in graph states (Objectives: W1.O3, W1.O4; Milestones: W1.M1, W1.M6). In [10] Gross and Van den Nest (Inn) report progress on the LU-LC conjecture - an open problem in the context of entanglement in stabilizer states (or graph states). This conjecture states that every two stabilizer states which are related by a local unitary operation, must also be related by a local operation within the Clifford group. The contribution of this paper is a reduction of the LU-LC conjecture to a simpler problem. As the main result, the authors show that, if the LU-LC conjecture could be proved for the restricted case of diagonal local unitary operations, then the conjecture is correct in its totality. Furthermore, the reduced version of the problem, involving such diagonal local operations, is mapped to questions regarding quadratic forms over the finite field GF(2). Finally, the authors prove that correctness of the LU-LC conjecture for stabilizer states implies a similar result for the more general case of stabilizer codes.

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

1.4 General properties for measurement based quantum computing

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

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

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

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

1.5 Quantum machines and measurement based quantum computing

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

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

2 Progress towards objectives and performed tasks for W1.T2

2.1 Resources for measurement-based quantum computing

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

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

In [18] the same authors continue this line of research. The mappings of [VDB07a] are generalized, and existing results about the graph state formalism and quantum computation, namely the universality of the cluster states, are used to gain insights in aspects of statistical mechanics. In particular, the authors prove that the 2D Ising model is complete in the sense that the partition function of any classical q-state spin model (on an arbitrary graph) can be expressed as a special instance of the partition function of a 2D Ising model with complex inhomogeneous couplings and external fields. In the case where the original model is an Ising or Potts-type model, the authors find that the corresponding 2D square lattice requires only polynomially more spins w.r.t the original one, a constructive method to map such models to the 2D Ising model is given. For more general models the overhead in system size may be exponential. The results are established by connecting classical spin models with measurement-based quantum computation and invoking the universality of the 2D cluster states.

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

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

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

2.2 General properties of graph states

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

3 Progress towards objectives and performed tasks for W1.T3

3.1 Calculi for one-way computing

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

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

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

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

3.2 Graphical calculus and categorical semantics for measurement based quantum computing

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

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

3.3 Automated reasoning tools for measurement based quantum computing

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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