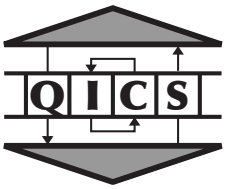


project no 033763

QICS

Foundational Structures for Quantum Information and Computation

Specific Targeted Research Project (STREP)

Thematic priority: Quantum Information Processing and Communications

DELIVERABLE D3

Classical-quantum interaction and information flow

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 W3 and comparison with the state-of-the art. While in traditional computing the notion of information flow is starting to become well-defined, see for example [J. Barwise and J. Seligman (1997) Information Flow: The Logic of Distributed Systems. Cambridge UP.]), the ultimate goal of this workpackage mainly aims at delineating a corresponding notion when quantum and classical systems are interacting. The situation is of course far more complicated here given that besides the flows between the quantum and the classical there are also the flows within the quantum itself subject to entanglement. Moreover, the notion of information, even in a more static sense, is not yet fully understood in the quantum context. To our knowledge a coordinated interdisciplinary joint attempt to work towards a unifying concept of information flow for quantum informatics is unique to QICS. In this workpackage we approach this involved problem from several different angles.

Main developments in W3.

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

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

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

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

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

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

Bob Coecke & Richard Jozsa

Oxford & Bristol, February 10, 2008.

Workpackage objectives: :

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

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

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

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

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

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

Workpackage milestones :

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

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

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

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

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

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

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

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

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

1 Progress towards objectives and performed tasks for W3.T1

1.1 Progress on the resource calculus

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

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

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

1.2 General results on quantum informatic resources

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

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

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

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

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

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

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

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

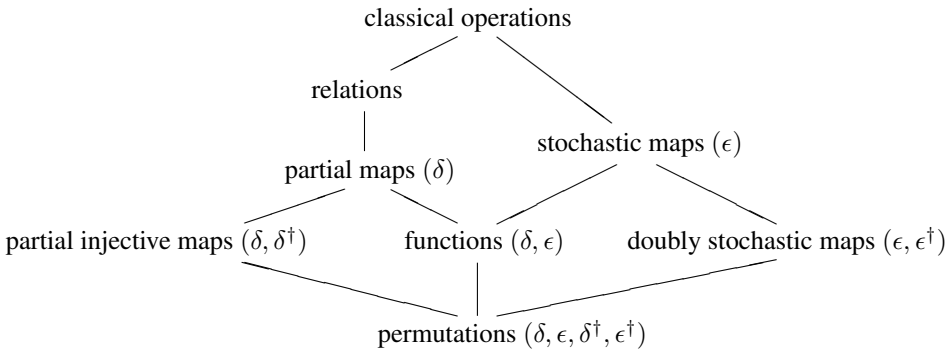
2 Progress towards objectives and performed tasks for W3.T2

2.1 Compositional accounts on information flow

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

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

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



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

2.2 Information flow on one-way computing

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

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

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

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

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

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

2.4 Classical limit

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

2.5 Coalgebraic structures

7.2.5.a Categorical semantics for a call-by-value linear lambda calculus (Objectives: W3.O1, W3.O4, W3.O4; Milestones: W3.M6). In [25] Selinger (McGi affiliated) and Valiron (McGi affiliated) give a categorical semantics for a call-by-value linear lambda calculus. Such a lambda calculus was used by Selinger and Valiron as the backbone of a functional programming language for quantum computation. One feature of this lambda calculus is its linear type system, which includes a duplicability operator ! as in linear logic. Another main feature is its call-by-value reduction strategy, together with a side-effect to model probabilistic measurements. The ! operator gives rise to a comonad, as in the linear logic models of Seely, Bierman, and Benton. The side-effects give rise to a monad, as in Moggis computational lambda calculus. It is this combination of a monad and a comonad that makes the present paper interesting. They show that our categorical semantics is sound and complete.

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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