The Structure of Quantum Information and its Ramifications for IT

Case for support by Bob Coecke of Oxford University Computing Laboratory

Part I: Research track record

Research profile and rank

My main recent work consists of applying semantical and logical methods from Computer Science (CS) to Quantum Information and Computation (QIC), which includes recasting the quantum mechanical formalism itself. I also worked on dynamic epistemic logic and information theory, both having applications to protocol security.

During the past 4 years, i.e. my time at Oxford University Computing Laboratory (OUCL), *I gave over 50 invited talks* at corporations (e.g. Google in Silicon Valley), conferences and departments, in the areas of Computer Science, Logic, Mathematics, Physics and even History and Philosophy of Science. I was awarded the *2004 biennial Prize for Meritorious Research in the Field of Quantum Structures* by the International Quantum Structures Association. I have *60 publications* and have been program committee member and organizer of several conferences and workshops in a variety of disciplines. A 2004 joint paper with Abramsky[1] [2] was the first one on QIC to be accepted for the prestigious IEEE conference on Logic in Computer Science (LiCS), and we are currently aware of at least 8 fresh Ph.D. students at other universities who's research comprises elaborations on this paper. EPSRC awarded a grant for the proposal *High-level Methods in Quantum Computation and Information* submitted by Abramsky and myself in 2004 on the topic of the above mentioned paper [3]. The US Office of Naval Research awarded a grant on the basis of the joint work by K. Martin and myself in [16]. I am currently coordinating the creation of a European network entitled *Foundational Structures in Quantum Information and Computation* in which OUCL will have 7 other partner sites including many leading groups in QIC. I run a weekly interdisciplinary seminar at OUCL called the Oxford Advanced Seminar on Informatic Structures (OASIS),[2] and I plan to organize a series of partly coinciding workshops on a variety of disciplines this summer.

I am currently lecturing a newly introduced course at OUCL entitled *Quantum Computer Science* offered within the Computer Science and Mathematics Departments to BA and MSc students.[3]

From Physics to Computer Science. I obtained a Ph.D. in theoretical physics from the Free University of Brussels, on the Foundations of Quantum Mechanics. One of my main concerns was the *low-levelness* and the *redundancies* of the quantum mechanical formalism due to John von Neumann (1932, [29]), but which was also already in 1935 renounced by von Neumann [35]. There were several strands of research motivated by these deficiencies within the mathematical physics community, but non of them were successful, and none sufficiently appealed to me (cf. [17] for a survey). In fact I found myself reading CS papers, fascinated by the advanced and very new mathematical tools Computer Scientists (in particular in Britain) were using, and their potential applicability to recasting the formalism of quantum mechanics. I started to realize that the Computer Science community *does have* something more to offer to Physics than 'the computer'. Indeed, (British) Computer Science is far ahead of many other sciences on the topic of mathematical and logical understanding of fundamental and generally applicable scientific concepts such as concurrency, causality, compositional modeling and reasoning, open systems, qualitative versus quantitative, continuous versus discrete (etc.), and mobile communication, internet and secure e-commerce all deal with distributed, embedded and hybrid systems which require a highly conceptual approach.

After being a PDRA respectively in Mathematics in Brussels, in Theoretical Physics at Imperial College and in Category Theory at McGill-Montreal, I was awarded a research fellowship by the Cambridge node of the European TMR network *Linear Logic in Computer Science*, and became an academic visitor at OUCL. My collaborations at OUCL, with Abramsky in particular, taught me how fundamental research can go hand in hand with applications. After this long journey I now consider myself as a researcher with a very strong but also *quite unique interdisciplinary background*, with an eye both for foundation and application, and I would conceive myself as having the appropriate background and skills to act as a communication channel and bridge builder across different disciplines. Currently there is a growing international community who is investigating the possible cross-breedings between CS and other sciences, resulting in relativity being discussed at bastions of computer science, and computer scientists lecturing at top theoretical physics institutes, even on workshops on the Holy Grail of physics, quantum gravity.[4] And I think that is is fair to say that I have played a pivotal role in establishing this.

Witnesses of multidisciplinarity. below we discuss some cross-disciplinary collaborations relevant for this proposal which contributed to my multidisciplinarity. Here we provide some selected *invited* talks as tokens (links can be found at my webpage):

- Probability = Logic + Partiality + Entropy. Session on *Quantum Logic meets Quantum Information* at *Quantum Theory: Reconsideration of the Foundations 2*. Vaxjo-Sweden, June 2003.
- Processes in Computing and Physics. Special workshop on *Causality in Computer Science and Physics* at the IEEE *Symposium on Logic in Computer Science*. Ottawa, June 2003.
- Probability as Order. *Applications of Lattice Theory and Ordered Sets to Computer Science* at the *Center for Discrete Mathematics and Theoretical Computer Science* (DIMACS), Rutgers-New Jersey, July 2003.
- Categories and Processes. At *Ramifications of Category Theory. Dedicated to F.W. Lawvere.* Florence, November 2003.
- Quantum Information-Flow. At *Perspectives workshop "Quantum Computing". Dagstuhl Seminar 04202*, May 2004.
- Kindergarten Quantum Mechanics. At *Quantum Information, Computation and Logic: Exploring New Connections*. Perimeter Institute for Theoretical Physics, Canada, July 2005.
- Picturing Quantum Informatics. At *Mathematical Theory of Quantum Computation and Quantum Technology*, Texas A&M University, November 2005.
- The Logic of Quantum Information. At *The 2006 Association of Symbolic Logic Annual Meeting*, Montreal, May 2006.

---

[1] OUCL's Christopher Strachey Professor of CS Samson Abramsky chose this joint work for his New Fellow's Lecture as a Fellow of the Royal Society.

[2] `se10.comlab.ox.ac.uk:8080/InformaticPhenomena/index.html`

[3] `web.comlab.ox.ac.uk/oucl/courses/topics05-06/qcs/`

[4] `www.perimeterinstitute.ca/activities/scientific/PI-WORK-3/index.php - rl.cs.mcgill.ca/˜prakash/causality.html - www.dagstuhl.de/04351/ - www.mis.mpg.de/con-ferences/blaubeuren2005/ - rl.cs.mcgill.ca/˜prakash/Bellairs/05/wshop.html - www.dagstuhl.de/06341/`

Relevant past results and collaborations.

We discuss some results relevant for the proposed work, in decreasing order of relevance. At the end of each topic we provide a token of the impact the corresponding work so far has had.

Categorical semantics of quantum protocols. (with Prof. S. Abramsky FRS) This is the content of the above mentioned paper [2] and successful EPSRC proposal [3]. It will be discussed in some detail in Subsections 1.1 and 1.2 of Part II, in particular the intuitive graphical calculus which emerges from it. Here we want to add that this categorical semantics is also more comprehensive than the standard quantum formalism, allowing for a complete purely formal discription of QIC-protocols as compared to the standard literature which involves informal statements such as 'Alice sends her qubit to Bob'. This allowed us to write down the first fully formal descriptions of many QIC-protocols such as quantum teleportation [31], and also to verify their correctness abstractly. We also have genuine types which distinguish quantum, classical and mixed systems (e.g. a qubit together with measurement data) while the standard quantum mechanical formalism is manifestly untyped: mixed states, unitary operations and projective measurements all have type $\mathcal{H} \rightarrow \mathcal{H}$. Also, there are much simpler categories than the one of Hilbert spaces and linear maps with the same categorical structure, which has great potential for qualitative analysis of quantum properties and for the design of protocols (cf. Subsection 2.2 of Part II).

The emerging graphical calculus which I (very recently) made available as lecture notes entitled *Kindergarten quantum mechanics* [14] has caused quite an impressive number excited responses, including from some very eminent senior members of the foundations of physics community: Em. Prof. Basil Hiley (co-author of David Bohm of the Undivided Universe) and Prof. Robert Griffiths (founder of the consistent histories approach to quantum theory).

The logic of entanglement. My 160 page 2003 research report [11] was the essential step-stone for the categorical semantics in [2]. I identified a new geometrical property of the behavior of quantum entanglement, and the categorical semantics of [2] is the axiomatic articulation of this geometric property. This paper also contains results on multipartite entanglement which have not yet been explored axiomatically. The content of [11] has recently become the subject of *experimental investigations* by eminent physicist [28].

Order-theoretic dynamic epistemic logic. (with Dr. A. Baltag and M. Sadrzadeh) While dynamic and epistemic logic are both well-developed fields, combing them was still an open problem. Solutions have been proposed, including an ingenious one by OUCL's A. Baltag, but all were very hard to manipulate towards applications. In [6] we proposed an algebraic semantics for dynamic epistemic logic in terms of order-theoretic objects called *quantales*. As it was the case for Baltag's previous work, notions such as deceit, information hiding, interception (etc.) could all be accommodated in this setting. A referee report on this work mentioned that "this is the first paper in which reasoning about knowledge and epistemic update get a clean mathematical treatment", and this has been acknowledged my many experts in the field. Recently M. Sadrzadeh has successfully applied this work to the analysis of authentication protocols [36], and she is receiving an increasing number of invitations to present this work and is currently elaborating on it with Dr. D. Pavlovic (Kestrel Institute).

Bayesian order and entropy on classical and quantum states. (with Dr. K. Martin) We identified a partial order (even a domain structure) on classical probability distributions and on mixed quantum states [16]. Shannon entropy proved to be a measure of content in Martin's sense [26]. In a subsequent paper I showed that one can factor probability as Probability = Logic + Partiality + Entropy and dubbed this structure *entropic geometry*. This joint work was awarded with a grant by the US Office of Naval Research.

Projective quantum axiomatics. von Neumann's initial concern with the quantum formalism were its redundant global phases, which only get eliminated when passing from vector spaces to projective spaces. Unfortunately, this passage also goes with the loss of the quantitative content. Starting from the 'vectorial categorical semantics' of [2], in [13] we were able to build a 'projective quantum axiomatics' while retaining all quantitative content. One could argue that this solves a more than 70 year old open problem.

From order-theoretic to categorical quantum axiomatics. (with Dr. D.J. Moore and I. Stubbe) I was regularly invited by Em. Prof. C. Piron to Geneva, a leading school in quantum theory (Stuckelberg, Jauch, Piron), but also a bastion of order-theoretic quantum axiomatics. This order-theoretic *quantum logic* endeavor due by Birkhoff and von Neumann [7] failed to axiomatize arguably the most important feature of the quantum mechanics, namely the tensor product (e.g. see [17]). Piron's PDRA D. J. Moore, I. Stubbe and myself 'lifted' the order-theoretic quantum logic to a 'order-concrete' categorical variant [10], using *quantales* and *quantaloids*, in order to introduce compositionality, types, and to give some sense to the tensor product and to the so-called Sasaki hook. Later I renounced this approach, but several researchers are still pursuing this program (e.g. Baltag and Smets at OUCL). During these visits I gained access to Prof. Piron's matchless knowledge both on the experimental and theoretical development on quantum theory.

Relevant ongoing research and new collaborations

Dr. D. E. Browne (Oxford, Materials) and I are working on a high-level model for *measurement based QIC* [4, 33]. I am also in close contact with Ph. Jorrand and S. Perdrix at Grenoble, and with V. Danos who invited me to Laboratoire de Preuves, Programmes et Systèmes in Paris 7 and with whom I am currently organizing a workshop at the Institute H. Poincaré in Paris.[5] Prof. H.-J. Briegel, the inventor of the *one-way quantum computational model*, invited me to Innsbruck (this visit will take place in January).

Dr. D. Pavlovic of Kestrel institute (Silicon Valley),[6] both a specialist in category theory and security protocols, recently invited me and this visit has resulted in several ongoing strands of research, including abstract axiomatics for quantum spectra, connections with domain-theoretic approaches to information theory, and in particular quantum protocol security (cf. Subsection 2.2 and 2.3 in Part II).

Prof. L. H. Kauffman (University of Illinois at Chicago) is renowned both for his work and books on knot theory and application thereof to physics. His recent work has focus on quantum computing, in particular on Topological Quantum Computing which shows remarkable similarities to our work. He visited us last year and has invited both Abramsky and me for further collaborations.

Host Organization

OUCL currently has a substantial group working on QIC.[7] Furthermore, Prof. Tom Melham, Dr. Joel Ouaknine and Dr. James Worrell are experts in Verification, and in particular, Prof. Bill Roscoe and Dr. Gavin Lowe are leading experts in Protocol Security. Next door to OUCL is the Materials Department which includes D. E. Browne and is headed by Prof. Andrew Briggs, Director of the Quantum Information Processing IRC. D. E. Browne currently coordinates the monthly one-day QUOXIC workshops[8] in which our group and Imperial College's Quantum Optics Group both participate.

---

[5] `se10.comlab.ox.ac.uk:8080/FOCS/QdayII_en.html`

[6] `www.kestrel.edu/home/people/pavlovic/`

[7] `se10.comlab.ox.ac.uk:8080/FOCS/PhysicsandCS_en.html`

[8] `www.physics.ox.ac.uk/users/quoxic/`

Part II: Proposed research

1 Background

The development of Quantum Information Technology (QIT) is both a matter of *necessity* and one of many *opportunities*:

a. As the scale of the miniaturization of IT components reaches the quantum domain, taking into account quantum phenomena will become unavoidable. This is not a matter of speculation but a matter of fact, not to be subjected to scepticism.

b. On the other hand, the emerging field of Quantum Information and Computation (QIC) — also sometimes referred to as Quantum Information Processing (QIP) — has exposed new computational potential, some of which endangers current cryptographic encoding schemes, but some of which at the same provides the corresponding remedy in terms of secure quantum cryptographic and communication schemes.

QIC emered from the recognition that quantum phenomena should not be conceived as a *bug* but as a *feature*, contrasting an attitude of defeatism which was addopted by most physicists since the birth of quantum theory. Fruits of this were the BB84 and Ekert 91 public key distribution schemes, the Deutch-Jozsa, Shor and Grover algorithms, the quantum teleportation protocol and many more [31]. But while the attitude has changed, much of the methods remained the same, and it is not totally unfair to compare the 'manipulations of strings of complex numbers and corresponding matrices in bases build from *kets* $|0\rangle$ and $|1\rangle$' with the 'acrobatics with 0's and 1's in the early days of computer programming'. On the other hand, many important questions on QIC remain unanswered and it is unlikely that the current *low-level* methods of QIC will provide the capabilities to answer them. For example, new quantum computational models such as the Briegel et al. measurement-base *one-way-model* [33] challenge the whole conception of what is currently conceived as a quantum computation, and hence what its limits are. In particular, a deep and clear structural understanding of the algorithmic speed-up and the informatic quantum-classical interaction has not yet been achieved. Also, while logic has taken a prominent place in (non-quantum) Computer Science (CS), the quest for a *quantum logic* has (until very recent) been a story of failure. Our (admittedly very ambitious) ultimate intentions are:

1. We want to release QIC research from its banner of being hard and completely inaccessible for the non-initiated ones. This requires an *intuitive*, *very simple* and *easily communicable* formalism for QIC, and hence for quantum mechanics itself.

2. We want to turn QIC research into a *systematic discipline*, hence subject to *automated design and development tools*. This requires a quantum formalism which admits analogues to the currently available *high-level methods* from CS such as types, well-behaving calculi, program logics etc.

3. We want to blend QIC research with the currently available and successful high-level methods for dealing with *distributed*, *hybrid* and *embedded systems*. This requires straightforward compatibility of the above mentioned high-level quantum concepts with their classical counterparts.

Addressing these challenges requires:

- *unveiling the structure of quantum information, of its flow, and of its interaction with other computational resources such as classical information-flow, space, agents, knowledge/belief* etc.

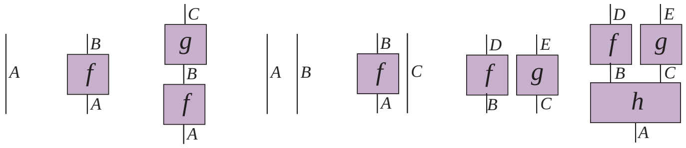
1.1 Concrete pictures from abstract categories

One major step in this direction was made when Abramsky and myself provided an (at least partial) answer to the question:

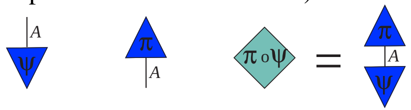
- *What is the structure of quantum mechanics?*

This result was the content of the first paper on QIC to be accepted for the prestigious IEEE conference on Logic in Computer Science [2] and also of a successful EPSRC grant application [3]. We profited from the currently available categorical semantics for Girard's *linear logic* [37], a resource sensitive logic developed in the late eighties. A crucial distinction between classical and quantum computation is indeed the inability to copy and delete unknown quantum states [39], and the ability to take such an inability into account was exactly the conceptual core of linear logic. At a more refined level, we also relied on the study of a particular categorical structure called *compact closed categories* [25] which had initially been introduced 'for purely mathematical reasons'. Surprisingly, after *refining* compact closure to *strong compact closure* [2], at an extremely high level of abstraction we were able to recover the key quantum mechanical notions *scalar, inner-product, unitarity, full and partial trace, Hilbert-Schmidt inner-product and map-state duality, projection, positivity, measurement*, and *Born-rule* (which provides the *probabilities*) [2, 13], and we were able to almost trivially derive the correctness of protocols such as quantum teleportation, entanglement swapping and logic-gate teleportation [31, 23]. Also, while at this level of abstraction there is no underlying field of complex numbers, we could still make sense of *transposition vs. adjoint, global phase and elimination thereof*, *vectorial vs. projective formalism* [13], and recently Selinger recovered *mixed state, complete positivity* and *Jamiolkowski map-state duality* [38]. But this high-level of *abstraction* also comes with an intuitive and simple *graphical calculus/notation* introduced in [2, 12, 38] and surveyed in some detail in [14].[9] This 'strongly compact closed graphical calculus' can be seen as a very substantial 2-dimensional extension of Dirac's *bra-ket* notation [19], and relying on category-theoretic results on free constructions [1, 21, 25, 38] one can show that an equational statement is derivable in the graphical calculus if and only if it is derivable from categorical algebra.

In the graphical calculus we depict physical processes by boxes, and we label the inputs and outputs of these boxes by *types* which tell on which kind of system these boxes act cf. one qubit, n-qubits, classical data etc. Sequential composition (in time) is depicted by connecting matching outputs and inputs by wires, and parallel composition (cf. tensor) by locating entities side by side e.g. $1_A : A \to A$, $f : A \to B$, $g \circ f$, $1_A \otimes 1_B : A \otimes B \to A \otimes B$, $f \otimes 1_C$, $f \otimes g$, $(f \otimes g) \circ h$ for $h : A \to B \otimes C$ respectively depict as:



— i.e. the 'upward' vertical direction represents progress of time. A special role is played by boxes with either no input or no output, respectively called *states* and *costates* (cf. Dirac's kets and bras [19]) which we depict by triangles. Finally, we also need to consider diamonds which arise by post-composing a state with a matching costate (cf. inner-product or Dirac's bra-ket):

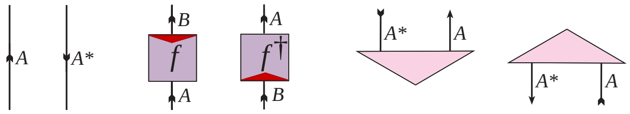


Extra structure is encoded by (i) assigning a direction to the wires, and reversal of this direction is denoted by $A \mapsto A^*$, (ii) allowing

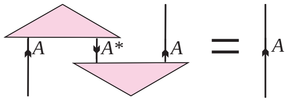
---

[9] While Selinger's notation [38] looks different from ours [14], it is equivalent.

reversal of boxes (cf. the *adjoint* for vector spaces), and, (iii) assuming that for each type A there exists of a special bipartite *Bell-state* and its adjoint *Bell-costate*:

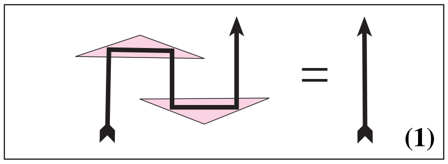


Hence, bra's and ket's are adjoint and the inner-product takes the shape $(-)^\dagger \circ (-)$ on states. The sole *axiom* we impose is:

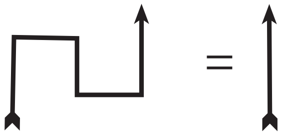


and if we extend the graphical notation of Bell-(co)states to:

we obtain a far more lucid interpretation for the axiom:[10]



which now tells us that we are allowed to *yank* the black line:



— we called this line the *quantum information-flow* [11, 12].

The intuitive graphical calculus is an important benifit of the categorical axiomatics. Other advantages can be found in [2, 12], in the successful EPSRC proposal [3] and also in Part I of this proposal.

1.2 Quantum non-logic vs. quantum hyper-logic

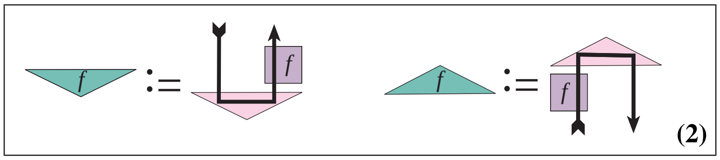
The utterance *quantum logic* is tightly connected with the 1936 Birkhoff-von Neumann proposal to consider the (closed) linear subspaces of a Hilbert space ordered by inclusion as the representative for the logical distinction between quantum and classical physics [7, 17]. While in classical logic we have deduction, the linear subspaces of a Hilbert space constitute a non-distributive lattice and hence there is no obvious notion of implication nor deduction. Therefore quantum logic was always conceived as logically very weak, or even a non-logic, and it has never produced any practically useful results. On the other hand, *compact closed logic* constitutes actually *more* logicality than ordinary logic. Indeed, while in ordinary categorical logic 'logical deduction' implies that *morphisms internalize* as elements (what above we referred to as states) i.e.

$$B \xrightarrow{f} C \quad \overset{\simeq}{\longleftrightarrow} \quad \mathrm{I} \longrightarrow B \Rightarrow C$$

(where I is the multiplicative unit), in *compact closed logic* they internalize both as states and costates i.e.

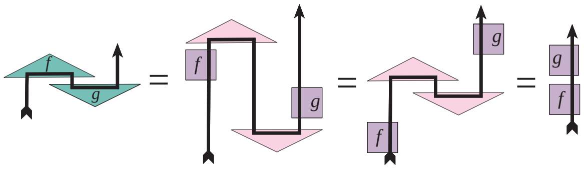
$$B \otimes C^* \longrightarrow \mathrm{I} \quad \overset{\simeq}{\longleftrightarrow} \quad B \xrightarrow{f} C \quad \overset{\simeq}{\longleftrightarrow} \quad \mathrm{I} \longrightarrow B^* \otimes C.$$

It is exactly this 'double logicality' which results in the *yanking axiom* in picture **(1)**. In the graphical calculus this double logicality is witnessed by the fact that we can both define a state and a costate

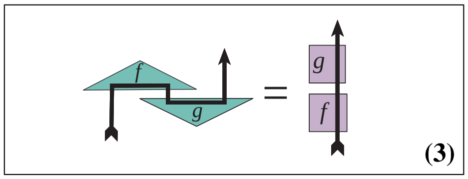


given each operation f — in the physics literature the first of these is known as the Hilbert-Schmidt map-state duality (e.g. [5]).

Two-fold compositionality. The semantics is obviously compositional in an operational sense both with respect to sequential composition of operations and parallel composition of types and operations, allowing to break down problems into smaller components. But we also have something far more compelling. Since we have:

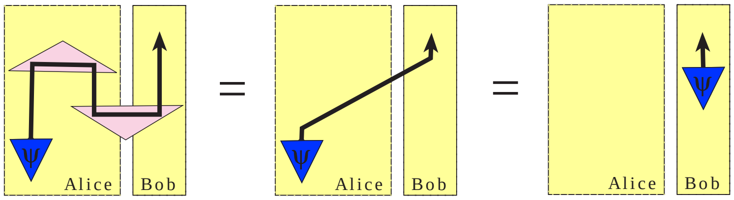


we obtain:

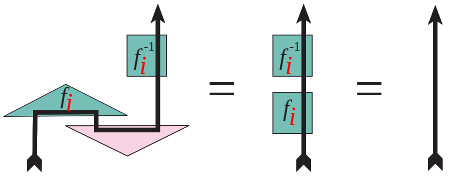


i.e. composition of operations *internalizes* in the behavior of entangled states and costates. Note in particular the interesting phenomenon of 'apparant reversal of the causal order' (cf. [28]).

Derivation of quantum teleportation. This is the most basic application of compositionality in action. Immediately from picture **(1)** we can read the quantum mechanical potential for teleportation:



if it wasn't for the indeterministic nature of measurements. But it suffices to introduce a unitary correction. Using picture **(3)** the full description of teleportation becomes including correctness proof:



where the *classical communication* is now implicit in the fact that the index i is both present in the costate (= measurement-branch) and the correction, and hence needs to be send from Alice to Bob. A purely algebraic version of this story is in [2, 12] (where the 'branching due to measurements' is captured by *biproducts*). A similar derivation of Gottesman-Chuang logic-gate teleportation uses the full power of **(3)** since in this case g will be the teleported gate. Other non-teleportation related (and far more compelling) derivations within the graphical calculus can be found in [13, 14, 38].

2 Programme and Methodology

We intend to proceed along three distinct main strands of activity: **2.1** conceptualization; **2.2** unification; **2.3** application.

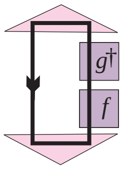
2.1 Conceptualizing quantum information theory

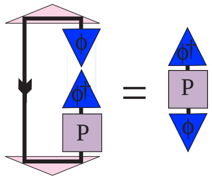
By conceptualizing a formalism we mean reducing it to a minimal set of well-behaving and well-understood primitive ingredients,

---

[10] An explicit proof of the fact that Hilbert spaces satisfy this graphical axiom is in [14]. With this graphical definition we can now provide a definition of a strongly compact closed category: it is a symmetric monoidal category in which there is (i) an involution $A \mapsto A^*$ on objects, (ii) a strict identity-on-objects contravariant monoidal involution $f \mapsto f^\dagger$ on morphisms, (iii) a special morphism $\eta_A : \mathrm{I} \to A^* \otimes A$ for each object A, and which are such that the equivalent diagram to picture **(1)** commutes (which is in [2]). We moreover assume all natural isomorphisms of the structure to be unitary i.e. $U \circ U^\dagger = U^\dagger \circ U = 1$. Examples are in [2].

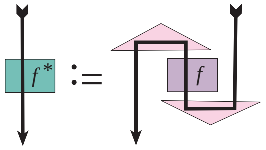
which makes it more intuitive, easier to manipulate, and allows for a wider set of (high-level) methods to be applied. In our graphical calculus there are 4 primitive concepts: sequential composition $-\circ-$, parallel composition $-\otimes-$, adjoint $f\mapsto f^\dagger$ and the Bell-states of type $\mathrm{I}\to A^*\otimes A$. Graphical calculi have recently become the subject of Fields medal awarding research relating C^*-algebras, statistical physics, knot-theory, and various areas of mathematical physics such as quantum groups, topological quantum field theory etc. Some of these calculi preceded their rigorous mathematical treatment e.g. Penrose's tensor calculus [34] (which closely relates to ours), and one couldn't immagine quantum field theory without Feynman diagrams anymore. The impact of a graphical calculus on QIC research could even be greater. As already mentioned, quantitative content survives our abstraction through conceptualization and in particular the passage to pictures. E.g. the *Hilbert-Schmidt inner-product* of operations $f : A\to B$ and $g : A\to B$ (which encompasses both the usual inner-product and a norm for operations), and the *Born-expression* $\mathrm{Tr}(\mathrm{P}\circ\rho)=\phi^\dagger\circ\mathrm{P}\circ\phi$ with $\rho=\phi\circ\phi^\dagger$ for the *probability* of state ϕ and projector P respectively depict as:

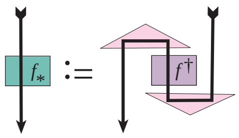




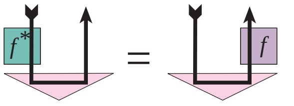
— the equality follows from the trace's *cyclicity* of which a simple proof within the graphical calculus can be found in [13, 14].

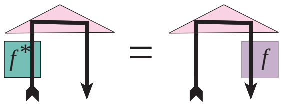
Naturality. Categories were introduced in 1945 to define functors, which themselves were introduced to define naturality. The aim was to nail down what in many cases was referred to by 'canonical', or more specific in the case of vector spaces, 'bases independence'. Naturality tells us how operations have to be *varied* in order to commute with some some special *natural* operation. Unfortunatly, while the crucial notions of *Hilbert-Schmidt* and *Jamiolkowski map-state dualities* do admit a natural isomorphism, in most of the QIC-literature one finds an *unnatural* bijection (cf. [5]), making calculations less manageable and blurry. The same goes for other notions such as *partial transpose* [24] — see below. The kind of naturality which could be very useful for QIC is nicely reflected in the picture calculus where we can easily show that adjoint factors in (see [14]):



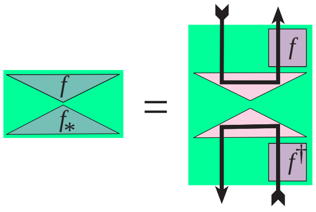


i.e. $f^\dagger=(f_*)^*=(f^*)_*$ with $f^{**}=f_{**}=f$ (for complex matrices we have $(-)^*$:= 'transpose' and $(-)_*$:= 'complex conjugation'). It then trivially follows by picture **(1)** that:



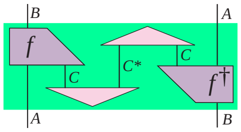


From this follow all the naturalilty requirements for many other notions such as trace, partial transpose, and non-degenerate bipartite projectors which faithfully represent as [2]:

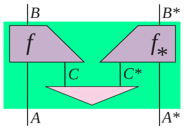


and also for CP maps (which we discuss below). We intend to investigate what the informatic and physical corollaries of the many natural connections between a wide range of QIC-notions are.

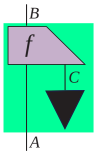
From closed to open systems. Given a strongly compact closed category, or equivalent, a graphical calculus of the above kind, Selinger showed in [38] that one obtains a new strongly compact closed category by 'restricting' to operations of the shape:[11]



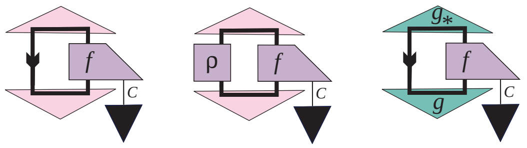
or, equivalently,



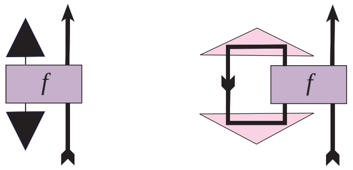
for the type $A\to B$, and that this passage exactly corresponds with the one from pure states and operations to *mixed states* and *completely positive* maps i.e. from closed to open systems. Both pictures cary some sort of redundancy in that they both involve f and a copy of it either subjected to $(-)^\dagger$ or $(-)_*$. We can reduce this notation by introducing a new primitive notion, formally justified in [15], called *maximally mixed state* and depicted as a black triangle:



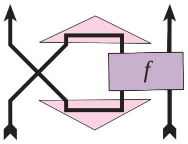
In this representation quantitative notions such as Reimpell-Werner *channel fidelity*, Schumacher's *entanglement fidelity* and Devetak's *entanglement generating capacity* (see [27] and references therein) emerge naturally as (cf. picture **(1)**):



We intend to systematically analyse the important quantitative notions of quantum information theory in this qualitative manner, and cast them within a uniform theory. We expect that new canonical and unifying notions will emerge. What is particularly interesting and should be much better understood is the clear distinction between two alternative canonical trace structures: the maximally mixed state induced *internal* one and the Bell-state induced *external* one:



The notion of *purification*, which due to the Uhlmann-Jozsa theorem [31] is crucial in the understanding of *fidelity*, also plays a key role in the graphical calculus. We discuss its formal counterpart in the following paragraph. We also expect to solve pending problems such as a deep understanding of what *bound entangled states* [24] are all about e.g. by considering the natural variant of partial transpose:



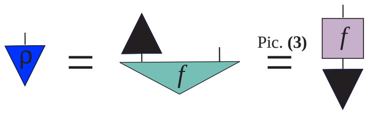
within our highly conceptual setting. Moreover, while much of the study of quantum information theory was guided by analogy with classical information theory, our setting allows quantum information theory to be developed as a theory in its own right, something which also might shed a fresh light on the classical-quantum connection.

Axiomatics for quantum information. De above graphically introduced *maximally mixed state* has a purely formal counterpart which emerged from an analysis of Selinger's construction in [15] with the aim of obtaining an *axiomatic foundation* (as opposed to Selinger's *construction*) for the *quantum theory of open systems*, and

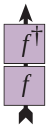
---

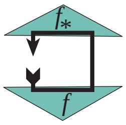
[11] The picture on the left only involves the primitive notions adjoint and Bell-(co)state while the one on the right admits the obvious covariant composition.

hence for quantum information theory. Given a state[12] $\rho : \mathrm{I} \to A$ a *purification* f is defined to be, equivalently (by the strongly compact closed state-map duality), a bipartite states or operation:



and we define the corresponding *squared purifications* respectvely as the positive operation and trace-like construct:





Given these notions, the structure resulting from our analysis is defined as a category in which there is: (α) for each object A a *maximally mixed state* $\perp_A : \mathrm{I} \to A$, and, ($\beta$) an all-objects-including dagger-sub-category of *pure states and operations* which is strongly compact closed, and which are such that *squared purifications of states coincide if and only if the states themselves coincide*. Hence we have recasted a construction in terms of one very simple but operationally significant *congruence*. Roughly spoken, it is equivalent to requiring from a category that: (α) it has no redundant global phases in the sense of [13], and, (β) it is the result of applying Selinger's endoconstruction of [38] to strong compact closure. Starting from this very minimal axiomatic setting we want to investigate further which additional structure, in particular on the commutative monoid of scalars which plays the role of probabilities (cf. Part I and [2, 13]), enables full quantum information theory.

A compositional extension of domain theory. While the above axiomatics is not order-theoretic it does resembles the spirit of Dana Scott's *domain theory*: There is a bottom (for each object), maximal elements (structured as a strongly compact closed category), and other elements which we can reach by *applying operations to the bottom, and which we can conceive as* approximations of the maximal elements. Recall here also that, following Martin [26, 16], domain theory can be considered as a both qualitative and quantitative account on information theory. But as it is the case for categorical proof theory and categorical logic, flattening the compositional structure into a partial order goes with loss of the dynamics of proving/reasoning, and also the operational nature of quantum information theory requires operations as witnesses cf. the above graphical calculus is purely compositionally founded. We wish to investigate how the usual tools of domain theory can be adopted to the categorical setting for QIC — there exists work on applying domain theory to the quantum setting by K. Martin and myself [16] in which we identify a domain-structure on density matrices with pure states as maximal elements and the maximally mixed state as the bottom (see also Part I), and also by A. Edalat [20] on a domain-theoretic variant Gleason's theorem. We expect to collaborate with Abramsky (an expert in Domain theory) on this topic. The scheme:

$$\textbf{value} \rightsquigarrow \textbf{order} \rightsquigarrow \textbf{category} \rightsquigarrow \textbf{picture.}$$

is what we take as general guidance. Also M. Nielsen's work [30] on passing from measures of entanglement to a preorder for bipartite entangled states needs to be extended to the multipartite setting, and we would also seek to embed I. Devetak and A. Winter's *resource inequalities* (used in [18]) within our scheme.

BENCHMARKS FOR THIS TOPIC:

1. A unified highly conceptual compositional and typed axiomatic theory on the quantitative and qualitative notions which are crucial to quantum information theory, with a corresponding intuitive and simple graphical calculus. This will allow quantum information science to become a high-level systematic practice.
2. An extension of domain theory and its applications which meets the demands of quantum information theory (as compared to those of classical information theory) and which intertwines qualitative and quantitative notions.

2.2 Unifying semantic methods

In the previous paragraph we already proposed to unify domain theoretic methods and the use of monoidal categories in semantics. We intend to extend our categorical QIC-setting and in particular the (to be developped) axiomatics for quantum information with a high-level account of classical information and information-flow between systems and agents, knowledge and belief, spatio-temporal causal structure (etc.), and we intend to perform this extensions in a uniform (multi-)monoidal setting — recall that each monoidal category admits a graphical calculus similar to one of the above kind [21].

Multipartite entanglement. Understanding the structure of multipartite entanglement of spatially dislocated systems is still one of the most challenging open problems in QIC. Due to the importance that entanglement plays in the key QIC-protocols [31] it goes without saying that an high-level understanding of the multipartite entanglement would be highly desirable. We think that with our $\otimes$-based categorical axiomatics we have the right tool at hand to take up that challenge. For example most qualitative properties distinguishing states such as the behavioral distinction between *GHZ-state* and *W-state* [31] do not need the full-blown Hilbert space structure but already get exposed in $(\mathbf{Rel}, \times)$, the strongly compact closed category of sets and relations (see also Part I and [2]). Hence $(\mathbf{Rel}, \times)$ constitutes a appropriate starting point for investigation.

Types for axiomatic classicality. In [2] we introduced a biproduct structure to account for alternative measurement outcomes, resulting in *weighted branching*. This structure allowed us to encode classical communication using distributivity, but did come with the redundant global phases which also occur in the Hilbert space formalism (also pointed out in [38]). These redundancies were eliminated in [13] by introducing a weaker notion of additivity (cf. Part I), which was still sufficient to describe quantum measurements and classical communication. We would like to better understand how different possible notions of additivity relate, including enrichment in monoids, and intend to perform this strand of research with Abramsky. On the other hand, the question whether one actually needs any additive structure at all still remains. We intend to tackle this question with Pavlovic, starting from the concept of *classical object* i.e. an object in a strongly compact closed category which admits a natural monoid structure cf. the classically allowed copying and deleting.

Complex multi-agent interaction and spatio-temporal causal structure from quantales. *Quantales*[13] are the *thin* variant of *closed* monoidal categories, and hence also enable deductive reasoning and provide a semantics for linear logic. They have proved to be very useful in a variety of applications such as concurrency, C^*-algebras, ring theory, but we will be in particular interested in their ability to encode complex (classical) communication between multiple agents and corresponding knowledge and belief updating as developed by Baltag, Sadrzadeh and myself in [6] and discussed in Part I, and, as shown by Brown and Engberg-Winskel, quantales also enable to encode spatio-temporal causal structure [9]. We aim to use the quantale *dynamic epistemic logic* setting as a classical control structure for developing sophisticated quantum protocols such as authentication. Also, in many protocols the quantum mechanical

---

[12] In this axiomatics mixed states will indeed have the type $\mathrm{I} \to A$ as opposed to the Hilbert space formalism where they are endomorphisms $\mathcal{H} \to \mathcal{H}$.

[13] While initially quantales were introduced as a quantum version of *locales*, here their use will be purely classical, as a classical control and a causal structure.

spatial observable can be approximated by just considering discrete locations in space, encoded in terms of the tensor structure. There already exists a vast body of work at the insection of Computer Science and Physics such as Lamport's work on the ordering of events in a distributed system and Petri's work on state-transition structures in Physics and Computation in terms of Petri nets, and it has been shown that all this can again be recasted in terms of quantales [9], which will allow us to go for very general monoidal framework. In this context we also wish to consider some new categorical models for modeling space and concurrency recently been developed by R. Milner, G. Winskel and others in Cambridge.

BENCHMARKS FOR THIS TOPIC:

3. A structural understanding of multipartite entanglement.
4. A typed axiomatic formalism capturing both classical and quantum information theoretic notions, and computations.
5. A fully monoidally closed formalism which unifies both classical and quantum types, captures multipartite entangled resources, captures spatio-temporal causal structure, and captures the knowledge and belief update due to complex, not-necessarily trustful interactions between several agents.

2.3 Areas of application

During the progress of the proposal we expect several applications to emerge. We list some immediate straightforward ones.

Information security. It is commonly accepted that information security will be the first practicable application of QIP. Quantum communication devices for experimental setups are available from commercial bodies (MagiQ and ID Quantique) and an actual quantum key distribution protocol has taken place between a Swiss bank and Geneva City Hall [32]. However, while the quantum component of the experiment worked perfectly, the authentication protocol failed to be secure due to flaws in the analysis of its classical component (e.g. [8]). This confirms the importance of correct integration of reliable classical components and quantum components as parts of a hybrid whole. Several authorities in protocol security have acknowledged the potential of the above mentioned quantale approach to dynamic epistemic logic to security (e.g. [36]). With D. Pavlovic, himself an expert in protocol security, we intend to use the categorical semantics with the quantale semantics as classical control structure for the analysis of quantum protocols, study safety properties and ultimately work towards automated verification techniques. Essential for this is of course the great expertise which exist at OUCL in the area of security and verification.

Models for general quantum computation. We will continue current ongoing work with D. E. Browne on a high-level unification of *measurement based QIC* [4, 33], a new and rapidly in popularity growing quantum computational model which is challenging many of the current paradigms of QIC. We also expect to elaborate with L. Kauffman on an abstract approach to topological quantum computing. All this, together with our research on the structure of quantum infor mation, is part of a general foundational endeavor towards an understanding of what could be a model for general quantum computing. Several authorities in QIC have acknowledged this need and we are currently trying to set up an international network (which I am coordinating) with a strong focus on this topic.

High-level semantics for quantum programming. Several languages for quantum (programming) have bee proposed e.g. Selinger, Altenkirch-Grattage and others (see the references in [22]). In collaboration with Pavlovic we are working towards a high-level approach, using ideas from monadic semantics, the categorical theory of fibrations, our own research on abstract notions of quantum spectra, and also the results emerging from the above mentioned research on types for classicality. We would also continue our ongoing work with Abramsky on this topic.

Distributed QIC, quantum relativity and quantum fields. Abramsky and I are currently seeking funding for two students D. Akatov and B. Edwards to work on several extensions of the axiomatics of [2], relevant both to CS and for Physics.

BENCHMARKS FOR THIS TOPIC:

6. A high-level integrated approach secure quantum protocols.
7. Contributions to the understanding of what is a general model of quantum computation, in particular including an axiomatic approach to measurement based quantum computing.
8. A unifying abstract approach to general quantum programing, including distributed, hybrid and embedded programs.
9. Many other applications which we expect to emerge.

3 Relevance to beneficiaries

If the ambitious aims of this proposal would be realized it could substantially change a major part of QIC research, its methods, and its accessibility to and from other sciences. Crucial foundational questions in QIC on its nature and capabilities might be solved. This work is also inherently interdisciplinary: Computer Scientists will find their methods to be highly applicable to Physics, producing a range of novel methods and results. Furthermore this work has a strong British character: British CS is the world leader in the use of semantic methods and logics, and the proposed research would this dominant role to the important emerging field of QIC.

4 Justification for the Fellowship

This research requires expertise in several fields: a strong background in CS semantics and its applications, quantum mechanics, modern logic and category theory. I have been active and have publications in all these fields (cf. also Part I): while my Ph.D. was in foundations of quantum mechanics, as a postdoc I was active in logic and category theory, and during the past five years I was active in CS semantics and its applications at OUCL. After five years of collaboration as a PDRA with Computer Scientists Prof. Abramsky, Dr. Baltag and Dr. Martin at OUCL, involvement in CS teaching, interaction with the speakers of the OASIS seminar which I run at OUCL, and with many colleagues at CS conferences and workshops, I am very confident that I master both the CS and Physics aspects required to independently pursue the proposed work. I attribute the recent rise of success of my research (e.g. resulting 50 invited talks in 4 years) to the high quality of the host institution and its members, so OUCL is the perfect host for the proposed work.

5 Dissemination and exploitation

We will present our work in leading international conferences and journals, reaching out both to the CS and physics communities. We intend to organize conferences and workshops on the topic of this proposal aimed at bringing together researchers of different disciplines concerned, and we intend to pass on our skills and results to students and PDRA's for which we intend to apply for support. We expect to write a monograph on the subject of categorical semantics, graphical calculus for QIC and general high-level methods for QIC.

References

[1] S. Abramsky (2005) Abstract scalars, loops, free traced and strongly compact closed categories. In: *Proceedings of CALCO 2005*, Lecture Notes in Computer Science **3629**.

[2] S. Abramsky and B. Coecke (2004) A categorical semantics of quantum protocols. *Proc. 19th Annual IEEE Symposium on Logic in Computer Science*, IEEE Computer Science Press. `quant-ph/0402130`[14] — (2005) Abstract physical traces. *Theory and Applications of Categories* **14**, 111–124. `www.tac.mta.ca/tac/volumes/14/6/14-06abs.html`

[3] S. Abramsky and B. Coecke (2004) *High-Level Methods in Quantum Computation and Information.* **EP/C500032/1**.

[4] P. Aliferis and D. W. Leung (2004) `quant-ph/0404082`. D. E. Browne and T. Rudolph (2004) `quant-ph/0405157`. P. Jorrand and S. Perdrix (2004) `quant-ph/0404125`. V. Danos, E. Kashefi and P. Panangaden (2004) `quant-ph/0412135`. M. A. Nielsen (2004) `quant-ph/0504097`.

[5] P. Arrighi and C. Patricot (2004) On quantum operations as quantum states. *Annals of Physics* **311**, 26–52. K. Życzkowski and I. Bengtsson (2004) On duality between quantum maps and quantum states. *Open Systems and Information Dynamics* **11**, 3-42. `quant-ph/0401119` (and references therein)

[6] A. Baltag, B. Coecke and M. Sadrzadeh (2005) An algebra and sequent calculus for epistemic actions. In: *Proceedings of the 2nd International Workshop on Logic and Communication in Multi-Agent Systems*, ENTCS **126**;[15] — (2005) Epistemic actions as resources. *Journal of Logic and Computation*. `www.er.uqam.ca/nobel/philmath/LicsWSPub.pdf`

[7] G. Birkhoff and J. von Neumann (1936) The logic of quantum mechanics. *Annals of Mathematics* **37**, 823–843.

[8] Th. Beth, J. Mueller-Quade and R. Steinwandt (2004) Cryptanalysis of a practical quantum key distribution with polarization-entangled photons. *Quantum Information and Computation*. `www.arXiv.org/quant-ph/0407130`

[9] C. Brown (1989) Relating Petri nets to formulae of linear logic. Technical Report ECS LFCS 89-87, University of Edinburgh. — (1989) Petri nets as quantales. ECS LFCS 89-96. U. Engberg and G. Winskel (1993) Linear logic on Petri nets. In: *A Decade of Concurrency, Reflections and perspectives*, pp. 176–229. Lecture Notes in Computer Science **803**.

[10] B. Coecke (2000) Structural characterization of compoundness. *International Journal for Theoretical Physics* **39** 581–590. `quant-ph/0008054` B. Coecke, D. J. Moore and I. Stubbe (2001) Quantaloids describing causation and propagation of physical properties. *Foundations of Physics* **14**, 133–145. `quant-ph/0009100` (and references therein)

[11] B. Coecke (2003) The Logic of entanglement. An invitation. PRG-RR-03-12. `web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html` & `quant-ph/0402014`

[12] B. Coecke (2005) *Quantum information-flow, concretely, and axiomatically. Proc. Quantum Informatics 2004*, Proceedings of SPIE **5833**. `quant-ph/0506132`

[13] B. Coecke (2005) De-linearizing linearity: projective quantum axiomatics from strong compact closure. *Proc. 3rd Int. Workshop on Quantum Programming Languages*, ENTCS. `quant-ph/0506134`

[14] B. Coecke (2005) Kindergarten quantum mechanics — lecture notes. In: *Quantum Theory: Reconsiderations of the Foundations* III, AIP Press. `quant-ph/0510032`

[15] B. Coecke (2005) On a categorical foundation for quantum information. Draft paper OUCL (available upon request).

[16] B. Coecke and K. Martin (2002) A partial order on classical and quantum states. PRG-RR-02-07. `web.comlab.ox.ac.uk/oucl/publications/tr/rr-02-07.html`. B. Coecke (2002) Entropic geometry from logic. In: *Proceedings of Mathematical Foundations of Programming Semantics* XIX. ENTCS **83**. `quant-ph/0212065`

[17] B. Coecke, D.J. Moore and A. Wilce (2000) *Current Research in Operational Quantum Logic: Algebras, Categories, Languages*, Kluwer. Introduction at `quant-ph/0008019`

[18] I. Devetak, A. W. Harrow and A. Winter (2004) A family of quantum protocols. Physical Review Letters **93**, 230504.

[19] P. A. M. Dirac (1947) *The Principles of Quantum Mechanics* (third edition). Oxford University Press.

[20] A. Edalat (2004) An extension of Gleason's theorem for quantum computation. *Int. J. of Theoretical Physics* **43**, 1827–1840.

[21] A. Joyal and R. Street (1991) The geometry of tensor calculus I. *Advances in Mathematics* **88**, 55–112.

[22] S. Gay (2005) Quantum programming languages: survey and sibliography. *Bulletin of the EATCS, June 2005*. `www.dcs.gla.ac.uk/~simon/quantum/`

[23] D. Gottesman and I. L. Chuang (1999) Quantum teleportation is a universal computational primitive. *Nature* **402**, 390–393.

[24] M., P. and R. Horodecki (2001) Mixed state entanglement and quantum communication. In: *Quantum Information: An Introduction to Basic theoretical Concepts and Experiments*. Springer Tracts in Modern Physics. `quant-ph/0109124`

[25] G. M. Kelly (1972) Many-variable functorial calculus. In: *Coherence in Categories*, pp. 66–105, Springer Lecture Notes in Mathematics **281**. G. M. Kelly and M. L. Laplaza (1980) Coherence for compact closed categories. *Journal of Pure and Applied Algebra* **19**, 193–213.

[26] K. Martin (2000) *A Foundation for Computation*. Ph.D. thesis.

[27] D. Kretschmann and R. F. Werner (2004) Tema con variazioni: quantum channel capacity. *New Journal of Physics* **6**, 26.

[28] M. Laforest, R. Laflamme and J. Baugh (2005) Time-reversal formalism applied to maximal bipartite entanglement: Theoretical and experimental exploration. `quant-ph/0510048`

[29] J. von Neumann (1932) *Mathematische Grundlagen der Quantenmechanik*. Springer-Verlag.

[30] M. A. Nielsen (1999) Conditions for a class of entanglement transformations. *Physical Review Letters* **83**, 436–439.

[31] M. A. Nielsen and L. Chuang (2000) *Quantum Computation and Quantum Information*. Cambridge University Press.

[32] Quantum Technologies Group at ARC Seibersdorf research GmbH and the group Quantum Experiments and the Foundations of Physics of the University of Vienna (April 21, 2004) *Quantum Cryptography "live": World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons*. Press release. `www.quantenkryptographie.at/`

[33] R. Raussendorf and H.-J. Briegel (2001) A one-way quantum computer. *Physical Review Letters* **86**, 5188. R. Raussendorf, D.E. Browne and H.-J. Briegel (2003) Measurement-based quantum computation on cluster states. *Physical Review* A **68**, 022312. `quant-ph/0301052`

[34] R. Penrose (1971) Applications of negative dimensional tensors. In: *Combinatorial Mathematics and its Applications*, pp. 221–244, Academic Press. (see also the appendix)

[35] M. Rédei (1997) Why John von Neumann did not like the Hilbert space formalism of quantum mechanics (and what he liked instead). *Studies in History and Philosophy of Modern Physics* **27**, 493–510.

[36] M. Sadrzadeh (2005) A suspicion based quantale model for reasoning about authenticity. Draft paper OUCL.

[37] R. A. G. Seely (1998) Linear logic, $*$-autonomous categories and cofree algebras. *Contemporary Mathematics* **92**, 371–382.

[38] P. Selinger (2005) Dagger compact closed categories and completely positive maps. *Proc. 3rd Int. Workshop on Quantum Programming Languages*, ENTCS. `www.mathstat.dal.ca/~selinger/papers.html#dagger`

[39] W. Wootters and W. Zurek (1982) A single quantum cannot be cloned. *Nature* **299**, 802–803. A. K. Pati and S. L. Braunstein (2000) Impossibility of deleting an unknown quantum state. *Nature* **404**, 164–165.

---

[14] Papers made available at the `arXiv`'s `quant-ph` database are downloadable at the location `www.arXiv.org/quant-ph/xxxxxxx` either as .pdf, .ps or .dvi.

[15] ENTCS := Elsevier's Electronic Notes in Theoretical Computer Science.

Diagramatic workplan

Benchmarks	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
month 01–04 year 1	C	-	C	-	C, A, S1	-	C, B	C, A, P	-
month 05–06 year 1	C	-	C	-	C, A, S1	-	C, B	C, A, P	-
month 07–12 year 1	C	-	C	C, P	C, A, S1	-	C, B	C, A, P	-
month 01–04 year 2	C	C, A	-	C, P	C, A, S1	C, P	C	C, A, P	C, S2
month 05–06 year 2	C	C, A	-	C, P	C, A, S1	C, P	C	C, A, P	C, S2
month 07–12 year 2	C	C, A	-	C, P	C, A, S1	C, P	C	C, A, P	C, S2
month 01–04 year 3	C	C, A	-	C, A	C, A, S1	C, P	C	C, A, P	C, S2
month 05–06 year 3	C	C, A	-	C, A	C, A, S1	C, P	C	C, A, P	C, S2
month 07–12 year 3	C	C, A	-	C, A	C, A, S1	C, P	C	C, A, P	C, S2
month 01–04 year 4	-	C, A	-	C, A	-	C, P	C	C, A, P	C, S2
month 05–06 year 4	-	C, A	-	C, A	-	C, P	C	C, A, P	C, S2
month 07–12 year 4	-	C, A	-	C, A	-	C, P	C	C, A, P	C, S2
month 01–04 year 5	-	-	-	C, A	-	C, P	C	C, A, P	C, S2
month 05–06 year 5	-	-	-	C, A	-	C, P	C	C, A, P	C, S2
month 07–12 year 5	-	-	-	C, A	-	C, P	C	C, A, P	C, S2

Some intended collaborations which are indicated in the schedule (we expect many more collaborations to emerge in due time):

- C := Coecke (the current applicant)
- A := Abramsky
- B := Browne
- P := Pavlovic
- S1 := Students Akatov and Edwards
- S2 := Other students and PDRA's to be recruited