— Proposal narrative —

Complementary quantum observables and resulting information flows in algorithms and protocols: high-level methods & tool development

Bob Coecke

Oxford University Computing Laboratory
Wolfson Building, Parks Road, OX1 3QD Oxford, UK.
coecke@comlab.ox.ac.uk — +447855298183 (cell) — +441865273839 (fax)

Institution proposal number:

...

BRC topic title:

Quantum information sciences and the future of secure computation

Contents

1 Statement of work (SOW)

Scope of work. The proposed work constitutes the development of high-level descriptions, graphical calculi, discrete models and program logics which capture the flow of information in quantum algorithms, communication protocols and cryptographic schemes. To achieve this goal we will rely on the representation of complementary quantum observables within categorical quantum computational semantics (CQCS), a research program initiated by the PI. CQCS addresses both quantitative aspects and development of supporting software, and both aspects will be exploited in this proposal for the quantitative analysis of algorithms, communication protocols and cryptographic schemes, and the development of software tools to design and verify these.

These complementary observables do not only play a key rule in quantum key distribution (QKD), but are also the 'structural resource' underlying Bell-base measurements, cluster states and other important multi-partite entangled states. They were also recently shown to enable axiomatisation of the quantum Fourier transform (QFT), the quantum mechanical component of Shor's factoring algorithm, which is an important — if not the most important — pillar for the whole quantum informatics endeavour and its funding. Hence the information flows induced by complementary observables are of major importance for any quantum information-processing device intended for secure computation.

The proposed project will lay bare the flows of information, both in terms of a graphical language as well as in terms of a corresponding logical syntax. For the relevant categories there is indeed a Curry-Howard style correspondence: categorical algebra $\leftrightarrow$ graphical calculus $\leftrightarrow$ logic of types. The graphical language enables simple intuitive reasoning about complex situations, and supports knowledge transfer between the distinct scientific communities involved in this type of research. The logic will enable automation of analysis, design and formal verification (= theorem proving) of algorithms and protocols. Discrete models will enable model-checking techniques. The proposed work has the potential to transform research in algorithms, communication protocols and cryptographic schemes — which nowadays still very much relies on a 'bag of tricks' — into a high-level systematic discipline.

Framework within the work takes place. CQCS was initiated by the PI in 2004[1] in the first paper on Quantum Information and Computation (QIC) to ever have been accepted to IEEE-LiCS; this paper has over 100 citations in Google Scholar. The particular fragment of this framework in which we will work is the very recent categorical axiomatisation of complementary observables due to the PI[2], which was described in the paper on QIC to ever have been accepted to ICALP track B. A key result in this paper is an abstract, purely diagrammatic computation of the QFT.

List of objectives / deliverables. The objectives and corresponding deliverables are either of a theoretical nature, hence will be compiled in reports and publications, or are actual software tools.

O1.1 A comprehensive high-level description of various QKD protocols.

O1.2 Insights into the relationship between structural ingredients of this high-level description and various security related properties.

[1] S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols*. Proc. 19th IEEE-LiCS.
[2] B. Coecke and R. Duncan (2008) *Interacting quantum observables*. Proc. 35th ICALP-B.

O1.3 A modular view of various QKD protocols in terms of structural ingredients.

O1.4 Structural conversions between various communication and cryptography protocols; insights into how security-related properties are modified under these conversions.

O1.5 Software tools that help to improve properties of QKD protocols.

O2.1 Rewrite-systems and normal-form related results for the high-level diagrammatic representation of quantum informatic algorithms and protocols.

O2.2 Completeness theorems and discrete models for categorical quantum computational semantics involving complementary quantum observables.

O2.3 Software tools for model-checking and theorem-proving for quantum informatic algorithms and protocols, and QKD in particular.

O3.1 Informatic orderings which allow us to compare important quantum informatic quantities for various systems, algorithms and protocols.

O3.2 A presentation of C*-algebras in terms of information flow and informatic quantities.

O3.3 A compositional theory of quantum informatic resources and quantities.

O4.1 Quantum communication and cryptography as a high-level systematic discipline.

O4.2 Unifying quantum communication and cryptography research and the available high-level accounts of distributed, hybrid and embedded systems, and knowledge acquisition/hiding.

List of milestones.

M1.1 A comprehensive high-level description of (modern versions of) BB84 and Ekert 91.

M1.2 An abstract proof of various security-related properties of BB84 and Ekert 91.

M1.3 An improved QKD protocol.

M2.1 A discrete model involving a variety of SLOCC classes of entangled states.

M2.2 Completeness theorems for basis structure and complementary quantum observable structure, with categorical quantum computational semantics.

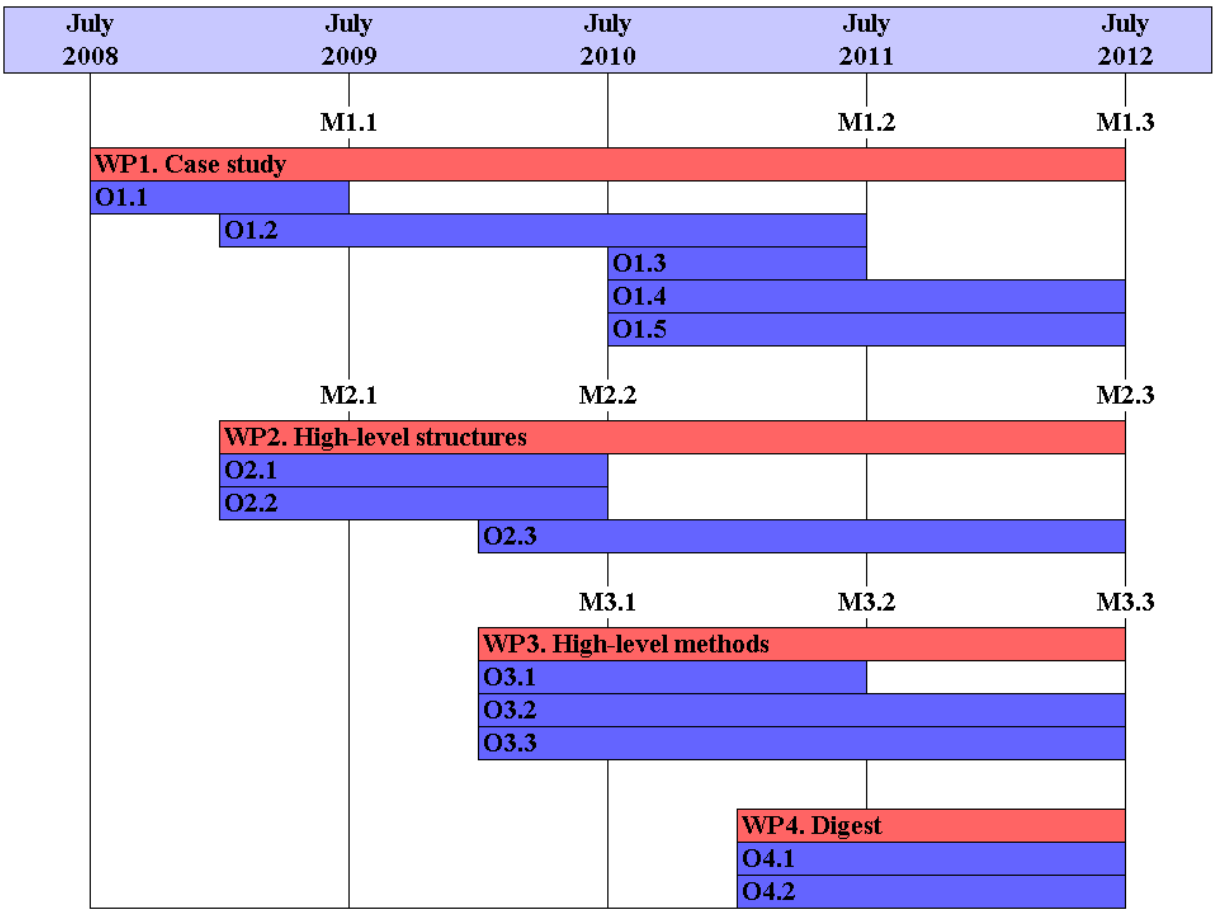
M2.3 Effective software tools.

M3.1 An order-theoretic denotational semantics for the above-discussed operational semantics and corresponding measures of informatic content.

M3.2 A high-level quantitative analysis of the major QKD protocols.

M3.3 A compositional semantics underlying DHW resource calculus.

Schedule for objectives/deliverables/milestones.



Location of the work / contributors. The work will be performed by the PI together with a *multidisciplinary* team of researchers with backgrounds covering logic, category theory, mathematical physics, computer science as well as software development. It will be performed in the Oxford University Computing Laboratory, currently the world-leader in high-level methods for quantum information and computation research, and which also hosts a leading secure computation group. Oxford University pioneered quantum information and computation in the 1980s and is still a world-leader in the area.

2 Background

2.1 Context

The development of Quantum Information Technology (QIT) is not only a matter of *necessity*, but also heralds many *opportunities*:

a. As miniaturization continues and IT components reach the scale of the quantum domain, taking into account quantum phenomena will become unavoidable. This is not a matter of speculation, but a matter of fact.

b. On the other hand, the emerging field of Quantum Information and Computation (QIC) 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 emerged from the recognition that quantum phenomena should not be conceived as a *bug* but as a *feature*, contrasting with the attitude of defeatism that had been adopted by most physicists since the birth of quantum theory. The fruits of this endeavor have been color the Shor and Grover algorithms [35, 56], the quantum teleportation protocol [7] and corresponding measurement-based quantum communication schemes [33, 50, 51], and last but not least, the BB84 and Ekert 91 quantum key distribution (QKD) schemes [6, 31].

But, while *attitudes* changed, most of the *methods* have remained the same. It is interesting to note the similarities between the

- manipulations of strings of complex numbers

which is common practice in the modern-day QIC community, with the

- manipulations of strings of 0s and 1s

which was required to control computers in the early days of computer programming. If we were still using these 0s and 1s, rather than high-level modern computer languages, it is quite obvious that there would be no any user-friendly operating systems, no internet and no mobile phone networks! But QIC is still stuck at the basic stage of manipulating complex numbers, lacking the high-level tools required to realise its full potential. The problem is already present at the level of the quantum mechanical formalism itself, due to the great John von Neumann, but also denounced by him no more than three years after its creation. A solution to the following equation is long overdue:

$$\frac{???}{\textbf{von Neumann quantum formalism}} \simeq \frac{\textbf{high-level language}}{\textbf{low-level language}}$$

A clear sign of the deficiency of this low-level quantum formalism is that it took an incredibly long time for some very simple, but strikingly important, discoveries to be made. For example, it took almost *50 years* to discover the no-cloning theorem [62], which proves the vital fact that quantum data cannot be copied — even though the proof only takes a few lines! Similarly, the capability to teleport continuous data by only relying on finite classical communication was only discovered some 60 years after the birth of the quantum theory, but is sufficiently simple that it can be set as an exam question to undergraduates. The few important results that did come out of the earlier period of quantum logic research, such as Gleason's theorem or Piron's representation theorem, were comparatively more complicated, and lack the same immediate technological relevance. We believe that a minimal requirement for any *high-level* quantum formalism is that simple results should be *easy* to prove, especially results of such crucial importance as the no-cloning and teleportation theorems.

There are still many unanswered questions in QIC, and it is unlikely that the current *low-level* methods will prove able to answer them. For example, what are the limits of QIC, be it in terms of algorithmic speed-up or communication capabilities? New quantum computational models such as the *one-way-model* [50, 51] challenge our entire understanding of the very nature of quantum computation. A clear structural view of the interaction of classical and quantum data cannot be found in any standard account of QIC. Just as an understanding of the flow of classical data — such as the nature of feedback, essential for recursion — is essential to our modern view of classical programming, an understanding the flow of *quantum data* will be essential to answer the foundational questions which are still unsolved in QIC.

2.2 Categorical quantum computational semantics

In 2004 Abramsky and PI Coecke initiated a research program on a *high-level categorical semantics for quantum protocols* [1]. Their pioneering paper was the first on quantum informatics to have ever been accepted to the IEEE-LiCS conference on Logic in Computer Science. This paper has meanwhile over 100 citations on Google Scholar. Other important contributions to this program have been made by Duncan, Edwards, Paquette, Pavlovic, Perdrix, Selinger and proposed RA Vicary [2, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 30, 54, 55, 59, 60, 61]. In particular, in 2008 Duncan and PI Coecke realised a categorical axiomatisation of *complementary observables* in the first paper entirely devoted to quantum informatics to ever have been accepted to the Semantics, Logic and Theory track of ICALP [17]. In the past five years PI Coecke has given approximately 60 invited talks on the topic. He runs a 2M-Euro Specific Targeted Research Project on the development of high-level methods for novel quantum computational architectures such as measurement based quantum computing, topological quantum computing and adiabatic quantum computing. He was awarded an EPSRC Advanced Research Fellowship which relieves him from all faculty duties for a period of five years, specifically for further development of categorical quantum computational semantics. This proposal is an instance of this effort, with the specific focus of exploiting the structure of complementary quantum observables in algorithm and protocol design, towards the development of software tools, an by exploiting the recent results by the PI, his postdocs, students, and other collaborators [16, 17, 18, 19, 22, 24, 30, 52, 55, 60]. Our (admittedly ambitious) ultimate intentions are:

1. We want to release QIC research from its reputation as difficult and completely inaccessible for the uninitiated. This requires an *intuitive*, *very simple* and *easily communicable* formalism for QIC, and hence for quantum theory itself.

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

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 a high-level description of quantum information, of its flow, and of its interaction with other computational resources such as classical information-flow and spatio-temporal causal structure. The main incarnation of quantumness, ever since the early days, is the existence of *complementary observables*. Hence the key challenge is to understand the flows of information that arise from their interaction.

Computer science, logic and mathematics research has produced several important formalisms over the last two decades: 1) linear logic (LL), a resource-sensitive logic; 2) particular kinds of monoidal categories (MCs), which provide semantics for LL-style logics; and 3) diagrammatic calculi, which one the one hand provide *graphical representations* for MCs, and on the other hand give rise to *proof systems* for linear logic and related logical systems.

Linear logic was designed as a *resource-sensitive logic*, in which computational resources are explicitly accounted for. This involved dropping the structural rules of *Contraction* and

Weakening

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta} \quad \text{and} \quad \frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$$

in Gentzen-style logical sequent calculus. Essentially, this restricts the ability to *copy* and *delete* resources. Having in mind the no-cloning (and no-broadcasting) and no-deleting theorems [5, 47, 62], it is clear that linear logic is well-aligned with these fundamental informatic constraints of quantum mechanics. Since its introduction in 1987 [32], linear logic has played an increasingly important rôle in computer science for modelling computational resources. It has also been known from the start that it comes with a diagrammatic calculus (*Proof Nets*) which has no obvious counterpart in classical logic. To understand this connection between linearity at the logical level, and diagrammatic representability of formulae and derivations, we need to pass to the theory of *monoidal categories* which provides an algebraic semantics for linear logic.

On the other hand, categorical semantics has been very successful in computer science because of its generality, finding common structure in many different situations, and because of its support for *compositional modelling*: analyzing complex systems in terms of how they are built up, using a stock of basic operations of wide applicability, from (simpler) sub-systems. This leads to an algebraic view of systems which is both elegant, and extremely effective, in allowing concise descriptions of complex systems, and algebraic manipulation of these descriptions. It is clear that such a compositional structure would also be highly desirable as a foundation for QIC, since many results in quantum information theory show that the same basic components are being combined over and over again to form various protocols.

Another major advantage of categorical algebra is the capability to have "types reflecting kinds", *contra* the Hilbert space formalism, where an operator of type $\mathcal{H} \to \mathcal{H}$ can be a mixed state, a unitary transformation or a measurement. For an *operational theory* such as quantum mechanics, which deals with composable entities such as unitaries, channels and measurements, and in which entanglement is among the most characteristic features, categorical algebra seems to be the natural candidate for an axiomatic framework.

The precise connection between both linear logic and category theory on the one hand, and QIC on the other, has recently been established in terms of *strongly compact closed categories* [1]. It constitutes the basis of categorical quantum semantics.

2.3 Basic setup

2.3.1 General theories: †-SMCs

systems: We represent *types* of systems (or 'kinds' if you prefer), such as physical systems like photons and electrons, or classical data types, or combinations thereof (such as the pair consisting of a quantum system together with observed data), by their names $A, B, C, \ldots$. The trivial system is denoted by I.

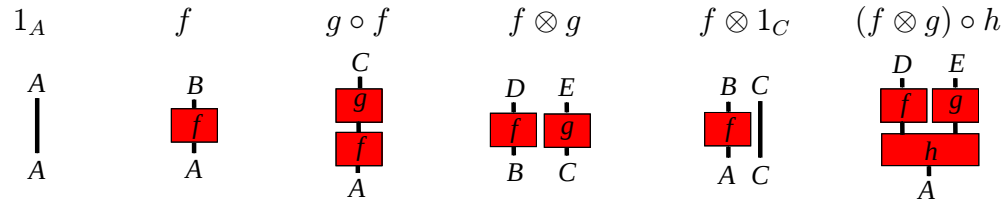
operations and processes: We represent general operations and processes, such as the evolution of a system between time t_1 and time t_2, or the preparation of a system in a certain state, or a computation which takes data of type A as input and produces data of type B, or a measurement that takes a quantum system A as input, destroys it, and produces an outcome of data type B, by arrows $A \to B$ where A is the input type and B is the output type.

sequential composition: We represent the composite of two operations or processes $f : A \to B$ and $g : B \to C$, which are performed or occur one after the other, by $g \circ f : A \to C$.

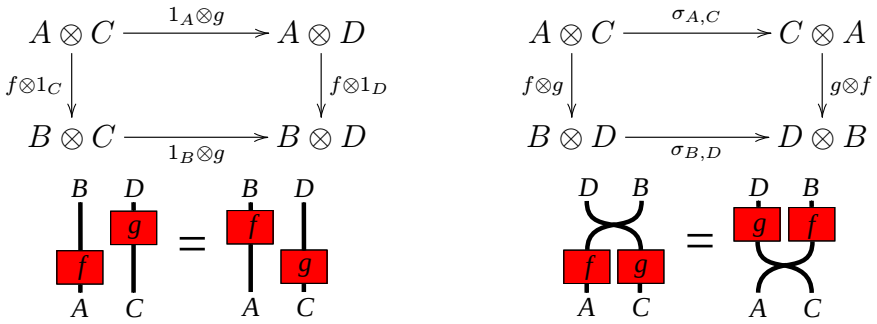
Doing nothing — or if you prefer, nothing occurs — is described for each system by an 'identity' operation $1_A : A \to A$.

compoundness: The joint system formed from A and B is denoted by $A \otimes B$, and the joint performance of operations $f : A \to C$ and $g : B \to D$ is denoted $f \otimes g : A \otimes B \to C \otimes D$. The symbol $\otimes$ is known as the *tensor*.

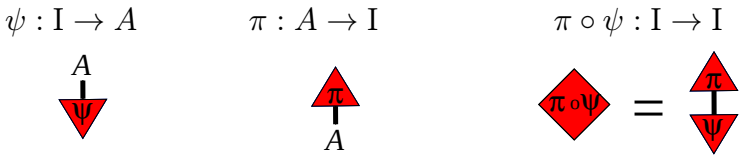
All these pieces of data, together with the obvious structural rules which mainly control how sequential and parallel composition interact, canonically make up a symmetric monoidal category (SMC). But rather than stating these rules we will rely on the fact that SMCs can be equivalently presented as a purely graphical calculus. This calculus can be traced back to Penrose's work in the 1970s [48], but it took a further 20 years for its precise algebraic and topological significance to become settled [38]. Operations are represented by *boxes*, types of systems by *wires*, composition by connecting outputs and inputs by wires, and tensor by locating wires or boxes side by side, as depicted here:



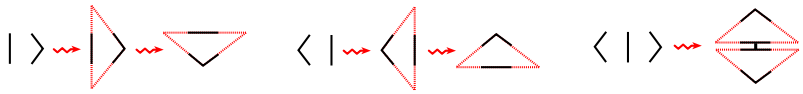
These diagrams should be read from bottom to top, so the second diagram represents the process $f : A \to B$. Typical axioms of the SMC structure are



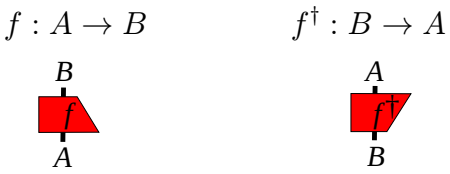
Intuitively, we are allowed to 'slide' boxes along the wires, and also along crossings. The trivial type I is represented by 'no wire':



Note that this indeed precisely captures Dirac's *kets*, *bras* and *bra-kets*:



The adjoint, which exchanges kets and bras, is captured by picture reversal:

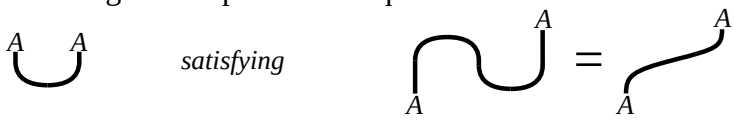


It enables to define the inner product, unitarity and complete positivity [15].

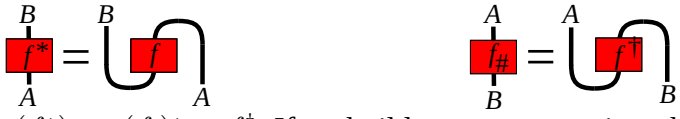
2.3.2 Accommodating Bell states: †-compact categories

We will now adjoin additional structure to this basic setting. Firstly, we assert the existence of Bell states. We require a system A to come with a 'Bell state' $Bell : \mathrm{I} \to A \otimes A$; that is, a 'triangle'

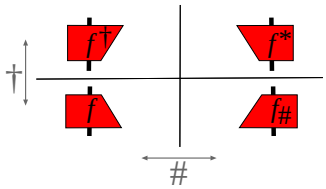
When rather than as a triangle we represent this quantum structure as a wire



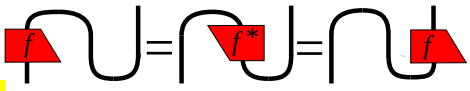
the axiom takes a more lucid form which boils down to 'yanking a piece of rope'. This is a simple structure, but is already enough to abstractly capture *trace* (e.g. [13]), and also transposition and complex conjugation, respectively:



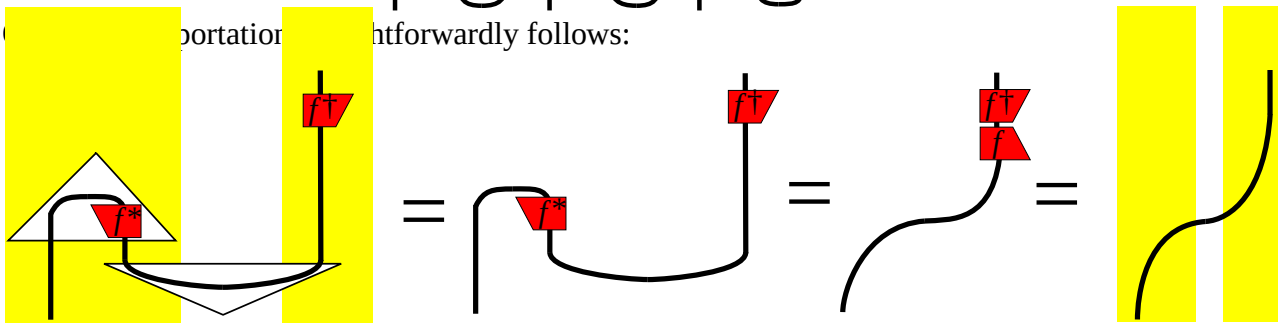
In particular, we have $(f^*)_\sharp = (f_\sharp)^* = f^\dagger$. If we build an asymmetry into the box used to depict a process f, we can depict all of these as follows [54]:



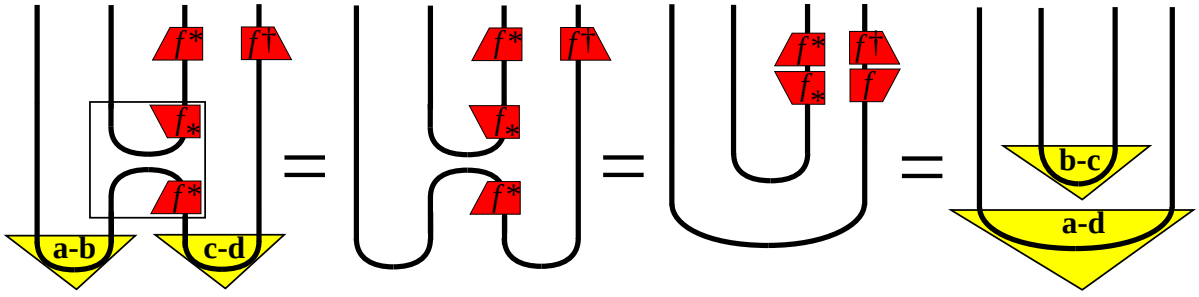
It immediately also follows that we can now 'slide' boxes along wires:[3]



(portation ntforwardly follows:



We require f to be unitary, that is, $f^\dagger \circ f = 1_A$ and $f \circ f^\dagger = 1_B$. The required classical information flow is implicit in the dependency of the correction $f^\dagger$ on the effect $Bell^\dagger \circ (1_A \otimes f^*)$. Entanglement swapping [63] is derived similarly:



[3] To prove this just substitute f^* by its definition, and then apply 'yanking'.

2.3.3 Quantum versus classical: commutative special †-Frobenius algebras

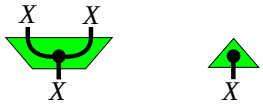
We get traditional logic from linear logic by *adjoining structure which witnesses the ability to copy and delete data*:

classical logic = linear logic + (copying, deleting)

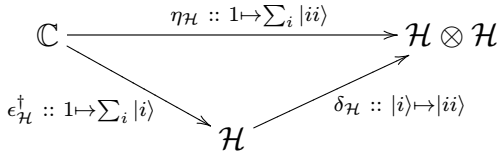
Similarly we set:

pure or mixed classicality = quantumness + (copying or broadcasting, deleting)

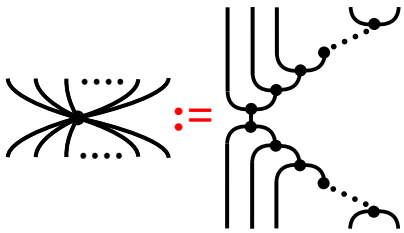
If one has a quantum system represented by a Hilbert space $\mathcal{H}$ then specifying a non-degenerate classical context means choosing an orthogonal basis $\{e_i\}$. Hence the resulting quantum system endowed with a classical context is the pair $(\mathcal{H}, \{e_i\})$, a Hilbert space with additional structure. A *classical context* for a quantum structure consists of two operations, $copy : X \to X \otimes X$ and $del : X \to \mathrm{I}$, respectively depicted as follows [20, 23]:



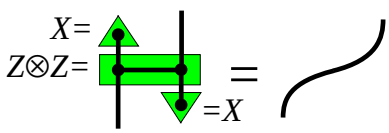
which 'refine' the Bell-states in the sense that for Hilbert spaces we have:



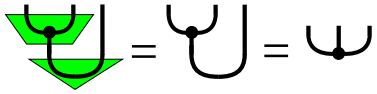
The structural requirements we impose on them are all conceptually very reasonable and translate in mathematical terms as a *commutative special †-Frobenius algebra* [23]. In diagrammatic terms these rules boil down to the assertion that any *connected* network involving copying, deleting, Bell states, and their adjoints is equal to a spider-shape [20], for which the only degrees of freedom are the number of inputs and the number of outputs, justifying the notation:



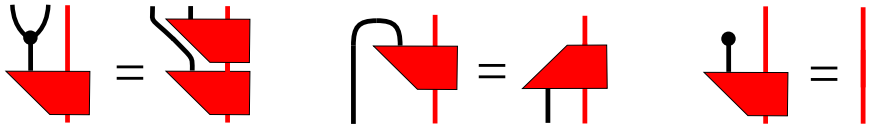
A diagram like this is obtained by 'multiplying' the inputs repeatedly using $copy^\dagger : X \otimes X \to X$ until only a single X remains, then copying this repeatedly using $copy : X \to X \otimes X$ to give the correct number of outputs. The connection between these †-Frobenius algebras and classicality is given by the following theorem [24]: given a finite-dimensional Hilbert space X, there is a bijective correspondence between orthogonal bases for X and commutative special †-Frobenius algebras on X, where the basis corresponding to a particular algebra is given by those elements which can be perfectly copied by the algebra. That is, in the †-SMC $\mathbf{FdHilb}$ of finite-dimensional Hilbert spaces, commutative special †-Frobenius algebras axiomatise orthogonal bases in an algebraic, logical, operational and diagrammatic manner. Perdrix's state transfer protocol [49] immediately follows [21]:



We also capture the very important GHZ-state [34] as:



General non-demolition measurements satisfy [23]:



in the sense that in **FdHilb** these conditions exactly yield the spectra of arbitrary self-adjoint operators. The reader might recognise the first equation to be von Neumann's projection postulate. In the †-symmetric monoidal category of Hilbert spaces, linear maps and the tensor product, this notion of measurement exactly coincides with the usual quantum mechanical one [23]. From a categorical perspective, these measurements are exactly †-Eilenberg-Moore coalgebras for the comonads canonically induced by the †-Frobenius algebra.

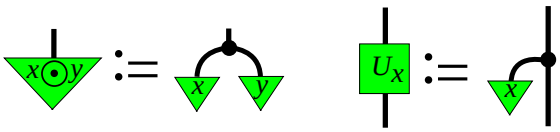
2.4 Interacting quantum observables

2.4.1 Observables separated by a phase

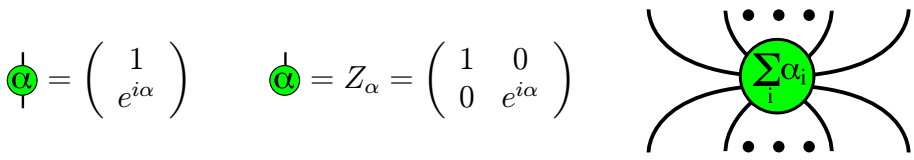
For (X, δ, ϵ) a basis structure in the above sense let $x \odot y := \delta^\dagger \circ (x \otimes y)$ and

$$states_X := \{x : \mathrm{I} \to X\} \qquad actions_X := \{U_x := \delta^\dagger \circ (x \otimes 1_X) \mid x : \mathrm{I} \to X\},$$

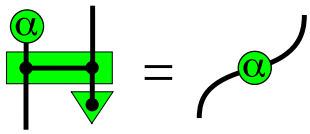
that is, diagrammatically,



Then $(states_X, \odot, \epsilon) \simeq (actions_X, \circ, 1_X)$ are commutative monoids [17]. States $x \in states_X$ are unbiased relative to the basis structure (X, δ, ϵ) if and only if U_x is unitary, in a sense that coincides with the usual one in **FdHilb**; i.e., the absolute value of inner products between the basis vectors of the two bases coincide. For $U\text{-}actions_X$ all unitary actions and $U\text{-}states_X$ all unbiased states, we have that $(U\text{-}states_X, \odot, \epsilon) \simeq (U\text{-}actions_X, \circ, 1_X)$ are abelian groups [17], representing the phase data relative to (X, δ, ϵ). There is a generalisation of the above mentioned 'spider' theorem which involves these phases. In the concrete quantum case we have [17]:



We can use these to show how state transfer can be used to implement a phase gate:



2.4.2 Complementary observables

Complementary observables, such as

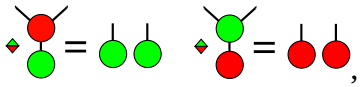
$$\delta_Z :: |i\rangle \mapsto |ii\rangle \qquad \epsilon_Z :: |i\rangle \mapsto 1 \qquad \delta_X :: |\pm\rangle \mapsto |\pm\pm\rangle \qquad \epsilon_X :: |\pm\rangle \mapsto 1,$$

are distinguished in our formalism by *colors*:

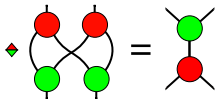
$\delta_Z =$  $\delta_Z^\dagger =$  $\epsilon_Z =$  $\epsilon_Z^\dagger =$ 

$\delta_X =$  $\delta_X^\dagger =$  $\epsilon_X =$  $\epsilon_X^\dagger =$ 

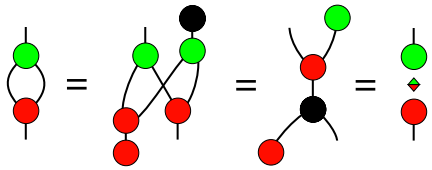
They obey the laws



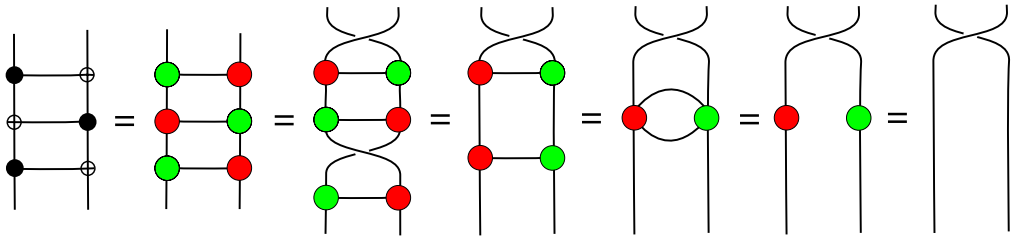
Described in words: up to a scalar, red copies green and green copies red. Under mild assumptions one can use this to show that a scaled bialgebra law holds [17]:



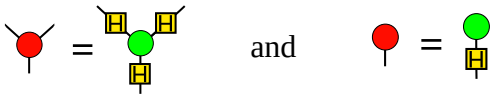
that is, red and green (co-)copying commute. From these two together we can derive a Hopf law:



An example illustrating the power of these rules is the following configuration of three CNOT-gates:



As a final ingredient we assume a 'color changer'

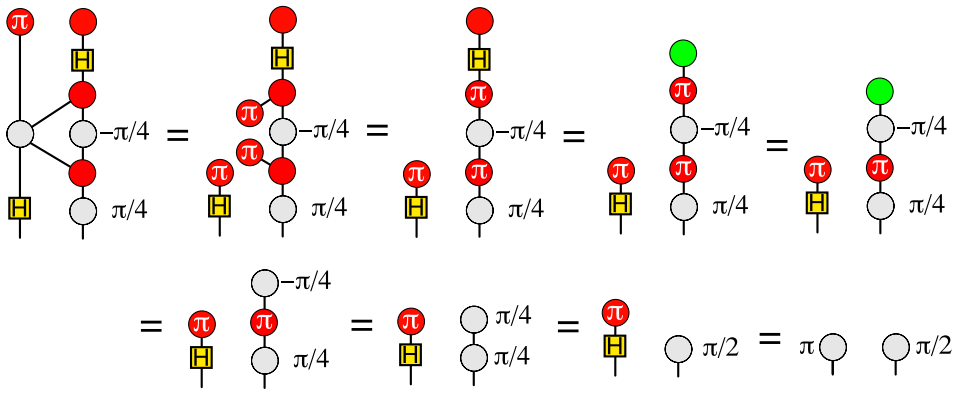


and

which in **FdHilb** represents the Hadamard gate.

2.4.3 Example application: quantum Fourier transform

Following [17] we compute quantum Fourier transform diagrammatically:



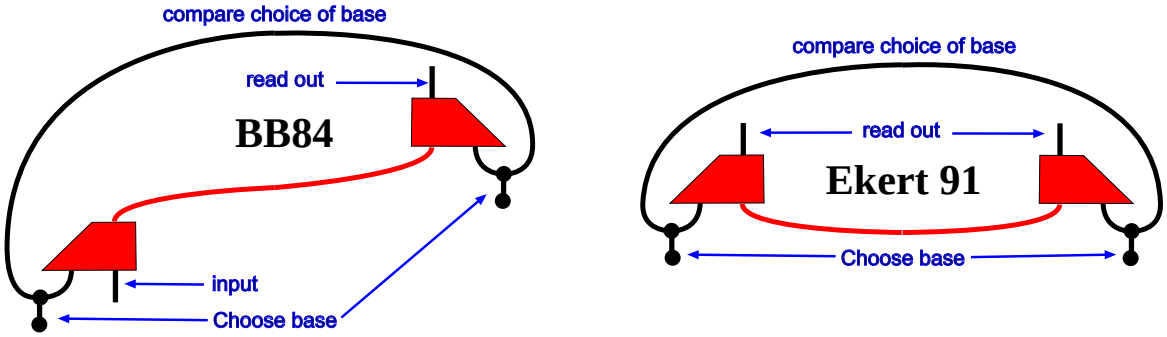
This example is the core of Shor's factoring algorithm [56] which for a long time has been the prime justification of the whole quantum informatic endeavour. Hence it provides proof of concept for our axiomatisation of interacting observables.

3 Research program and methodology

The proposed research has four major work-packages, for each of which we state the objectives and milestones at the end of the technical description. A diagrammatic workplan depicting the envisioned periods of work on each of the objectives, as well as specification of the expected dates we reach the milestones, is in the next section.

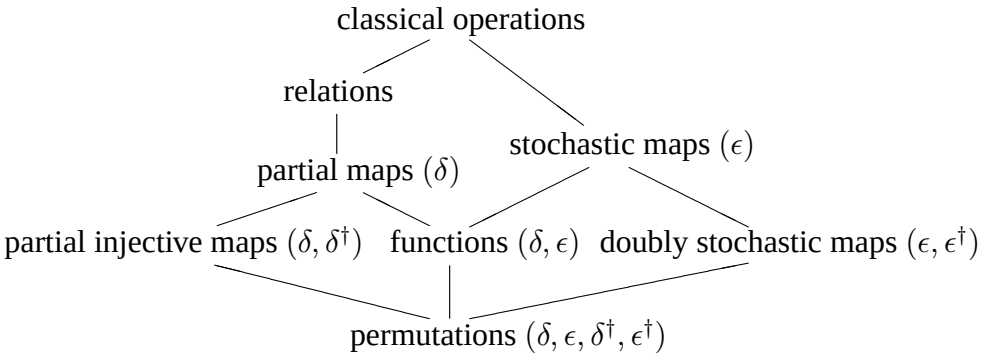
3.1 Case study: quantum communication and cryptography

The main ingredient of quantum key distribution (QKD) protocols are complementary observables. Each of these represent one of the two bases in which Alice and Bob have to choose to measure (or prepare, depending on the protocol) their qubits. However, the full-blown description of QKD involves several other ingredients such classical communication, classical stochastics and a fixed causal structure. The aim of this work-package is to give a comprehensive high-level categorical description of several quantum communication and cryptographic protocols, and to compare the structural resources required for each of these, their resulting dependencies, and ways to convert between them. For example, within our topological diagrams we can easily pass from BB84 QKD to Ekert 91 QKD:

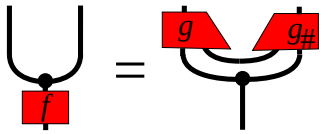


A fixed causal structure would obstruct this passage.

Classical information flows, classical probabilistic data and other classical species. In recent work [22] we showed that an abstract basis structure suffices to extract a substantial number of classical concepts from any †-SMC when fixing a basis structure (X, δ, ϵ) for each object X. Ordered by inclusion these are:

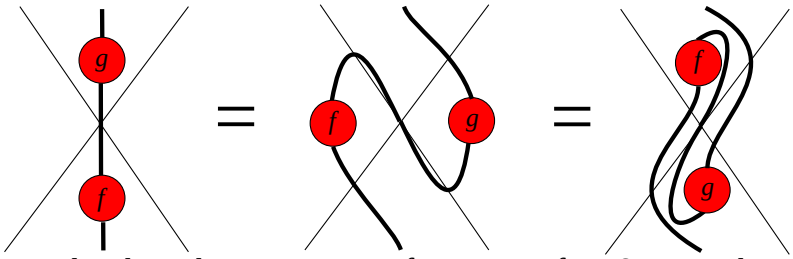


We also specified the operations which they preserve; for example, a function is a comonoid homomorphism (this observation was already made in [8].) Classical operations are those morphisms $f : X \to Y$ for which there exists $g : X \otimes Z \to Y$ such that



and this map is stochastic if we moreover have that $\epsilon_Y \circ f = \epsilon_X$, in the sense that in $\mathbf{FdHilb}$ we indeed exactly obtain all stochastic maps. Doubly-stochastic maps are those for which both f and $f^\dagger$ are stochastic in the above sense. With these stochastic maps at hand, we intend to provide a high-level description of the probabilistic features of a variety of QKD protocols.

Causal structure. There is natural notion of causal structure encoded in any SMC by identifying composition as a temporal separator and the tensor as a space-like separator. However, whenever adjoining the compact identities this causal structure becomes obscured:



We used this also in the above homotopic transformation of BB84 into Ekert 91. This causal structure needs to be re-articulated in a formal manner. A natural manner to do this is the method used in Algebraic Quantum Field Theory (AQFT); that is, by means of a functor from the causal structure into the monoidal category where spatial separation is mapped in pure tensors. In this way we interpret morphisms (i.e. states, operations, etc) relative to a fixed causal structure and the superfluousness vanishes. We wish to obtain a high-level account of the causal structure of a variety of QKD protocols in this manner.

Required structural resources: a comparative study. Having all the above ingredients at hand, in addition to complementary bases, we can provide fully-comprehensive descriptions of various communication and cryptography protocols. The next step would be to provide *abstract* proofs of several security-related properties. These proofs will then point at the *essential structural resources* required for QKD. We intend to investigate how stable these security related properties are under alteration of these resources. All together we will obtain a modular view of QKD, among other protocols, in terms of these structural elements of our abstract framework.

Conversions of QKD schemes and other communication and cryptography protocols. Once high-level descriptions of various quantum communication and cryptography protocols are obtained, as well as the relation of their structural ingredients to various security related properties, we can study conversions between these schemes (such as the conversion between BB84 and Ekert 91 given above) as well as the corresponding changes in various security properties. This will increase the power of our framework, in the same way as categorical proof theory improves on algebraic logic. This will provide the ideal framework to improve on existing protocols in a high-level manner. Since our abstract framework enables automation we intend to build tools which help to improve protocols in terms of improved security properties.

3.1.1 Objectives

O1.1 A comprehensive high-level description of various QKD protocols.

O1.2 Insights into the relationship between structural ingredients of this high-level description and various security related properties.

O1.3 A modular view of various QKD protocols in terms of structural ingredients.

O1.4 Structural conversions between various communication and cryptography protocols; insights into how security-related properties are modified under these conversions.

O1.5 Software tools that help to improve properties of QKD protocols.

3.1.2 Milestones

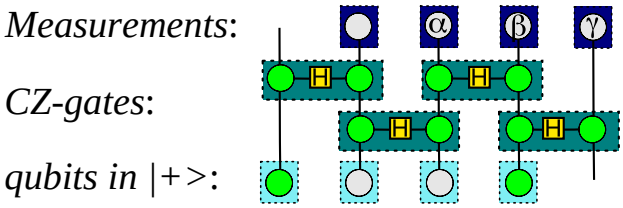
M1.1 A comprehensive high-level description of (modern versions of) BB84 and Ekert 91.

M1.2 An abstract proof of various security-related properties of BB84 and Ekert 91.

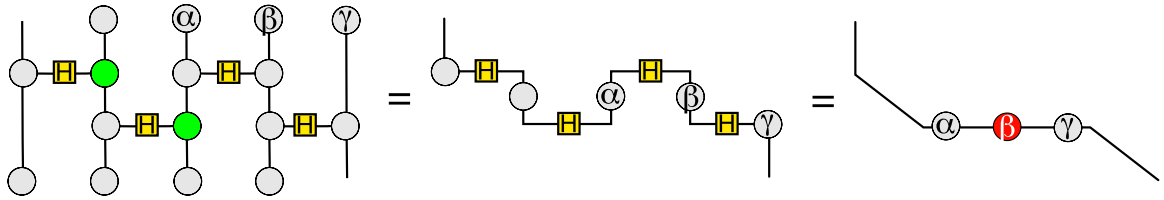
M1.3 An improved QKD protocol.

3.2 Normalisation, models, completeness and automation

Our abstract semantics provides us with enough power to show that the one-way quantum computational model [51] can simulate arbitrary unitary operations on multiple qubits [17]. The network to simulate an arbitrary single-qubit unitary is:



which simulates arbitrary qubit gates in terms of their Euler angles on the Poincaré-sphere:



This example, while quite simple, makes clear how complicated configurations result in a flow of information from input to output under the action of phase gates. The aim of this work-package is to develop high-level methods emerging from the high-level descriptions established in the previous work-package.

Normalisation. We intend to investigate normal-form related properties of reductions of involved diagrammatic networks to simple lines as in the above example. Besides the fact that these clearly expose the information flows in protocols, these normalisation results are of major importance for automation, something which we aim at in this work-package. Initial results in this direction have recently been achieved by Duncan [30], a postdoctoral researcher in the PI's group.

Discrete models. Recent work by PI Coecke, proposed RA Vicary and Edwards, a student of the PI, has exposed a highly unexpected remarkable fact [18]; namely that complementary quantum observables can already be simulated on the two-element set in the †-SMC $\mathbf{Rel}$ of sets, relations, Cartesian product and relational converse. We denote the the two element set as II, and for convenience we set $\mathrm{I} := \{*\}$. The two complementary quantum observables are then

$$\delta_Z : \mathrm{II} \to \mathrm{II} \times \mathrm{II} :: \begin{cases} 0 \sim (0,0) \\ 1 \sim (1,1) \end{cases} \qquad \epsilon_Z : \mathrm{II} \to \mathrm{I} : \begin{cases} 0 \sim * \\ 1 \sim * \end{cases}$$

$$\delta_X : \mathrm{II} \to \mathrm{II} \times \mathrm{II} :: \begin{cases} 0 \sim \{(0,0),(1,1)\} \\ 1 \sim \{(0,1),(1,0)\} \end{cases} \qquad \epsilon_X : \mathrm{II} \to \mathrm{I} : 1 \sim *$$

where the first one canonically arises from the underlying biproduct (= direct sum) structure but the second one is more of a mystery, explicitly involving *entanglement* in its prescription (for example, in $\mathbf{FdHilb}$ the set $\{(0,0),(1,1)\}$ can be interpreted as $|00\rangle + |11\rangle$ and $\{(0,1),(1,0)\}$ can be interpreted as $|01\rangle + |10\rangle$). This model has great potential for important applications. For example, the purely quantum-mechanical component of QKD merely relies on the existence of two complementary observables, and hence can be perfectly simulated by this model.

We also crafted an appropriate category for more involved applications, which exploit all three complementary observables of a qubit. Let $\mathrm{IV} = \{1,2,3,4\}$. The objects of the category **Spek** [19] are I, or of the form $\mathrm{IV} \times \ldots \times \mathrm{IV}$; for convenience we enforce the congruence $\mathrm{IV} \times \mathrm{I} = \mathrm{I} \times \mathrm{IV} = \mathrm{IV}$ and strictness of associativity. The morphisms of **Spek** are all relations generated by composition, cartesian product of relations, and relational converse from:

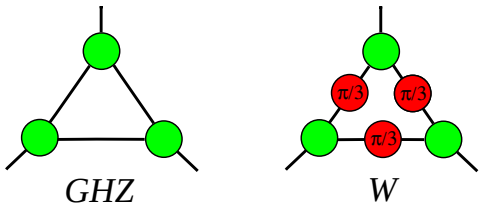
- all permutations $\{\sigma : \mathrm{IV} \to \mathrm{IV}\}$ on four elements;
- a (copying) relation $\delta_Z : \mathrm{IV} \to \mathrm{IV} \otimes \mathrm{IV}$ defined by:

$$1 \sim \{(1,1),(2,2)\} \quad 2 \sim \{(1,2),(2,1)\} \quad 3 \sim \{(3,3),(4,4)\} \quad 4 \sim \{(3,4),(4,3)\};$$

- a (corresponding deleting) relation $\epsilon_Z : \mathrm{IV} \to \mathrm{I} :: \{1,3\} \sim *$.

The category $\mathbf{Spek}$ produces the same ingredients as Spekkens' toy theory [57, 58] which has been receiving a lot of attention in the Foundations of Quantum Mechanics community, as a toy theory which produces many of the typical quantum mechanical features. The above category establishes the fact that all of the quantum-like properties and phenomena Spekkens' toy theory follow for the general reasons articulated in our categorical quantum computational semantics. Also important is the fact that the whole of $\mathbf{Spek}$ is generated from a copying operation, a deleting operation and a symmetry group. Besides the conceptual significance of this in linear

logic terms, this makes it very easy to enrich with other quantum-like features, such as more incomparable modes of multi-party entanglement. **Spek** as it stands only produces as genuine multi-party entangled states those of the GHZ SLOCC class. PI Coecke recently showed that adjoining a $\pi/3$-gate suffices to also interpret the W-state:



This W-state enables protocols such as mediated teleportation and leader election. We intend to develop a hierarchy of discrete models which capture a variety of quantum features, and hence enable us to model a variety of protocols in a discrete — and hence computationally-tractable — manner.

Complete models. Recently it was shown by Selinger [55] that finite-dimensional Hilbert spaces are complete for †-compact categories. This important result shows that if we want to verify an equation expressed in the language of †-compact categories, then it suffices to verify that it holds for Hilbert spaces. We intend to extend this result to the more involved structures outlines above, which enable us to specify and compute important algorithms and general protocols.

Model checking and theorem proving. The above-outlined research supports the development of verification tools, both for model-checking (discrete models) and theorem proving (rewrite systems). We intend to develop these in collaboration with Duncan and Sadrzadeh, two postdoc's of the PI's group who are active in this area [30, 52]. Particularly in the area of verifying security-related properties, these verification techniques have proven extremely useful, such as in Oxford University Computing Laboratory's historical work in which Lowe both broke and fixed the Needham-Schroeder Public-Key Protocol [42, 43].

3.2.1 Objectives

O2.1 Rewrite-systems and normal-form related results for the high-level diagrammatic representation of quantum informatic algorithms and protocols.

O2.2 Completeness theorems and discrete models for categorical quantum computational semantics involving complementary quantum observables.

O2.3 Software tools for model-checking and theorem-proving for quantum informatic algorithms and protocols, and QKD in particular.

3.2.2 Milestones

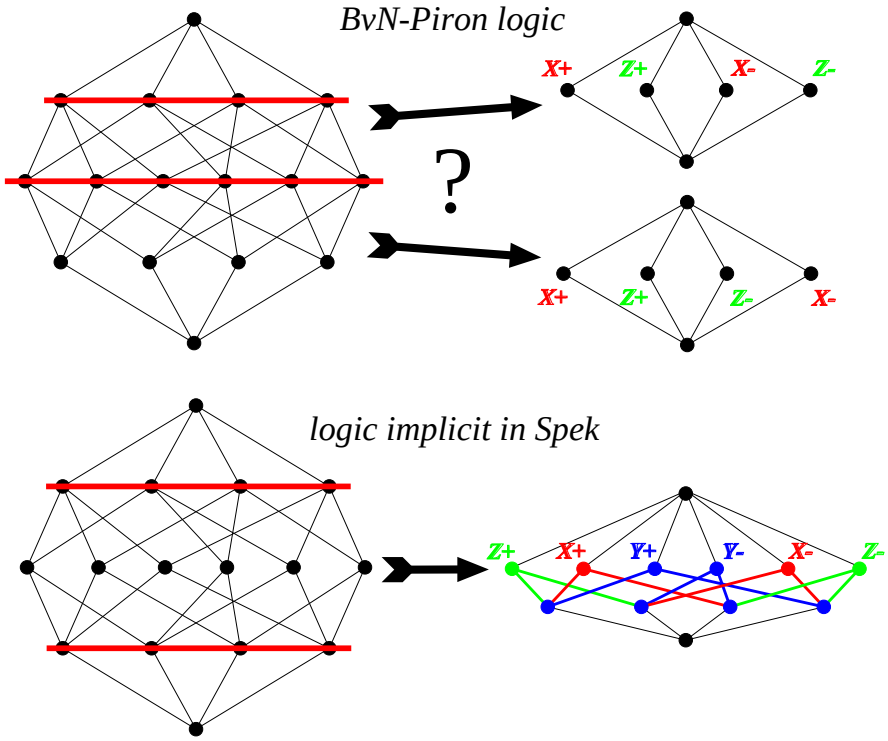
M2.1 A discrete model involving a variety of SLOCC classes of entangled states.

M2.2 Completeness theorems for basis structure and complementary quantum observable structure, with categorical quantum computational semantics.

M2.3 Effective software tools.

3.3 Informatic ordering, C*-algebras and emerging quantities

Informatic ordering. An essential intermediate structure between high-level descriptions of systems and quantitative measures are *informatic orderings* (e.g. [10, 44, 45, 46]). In particular, PI Coecke showed how informatic orderings of classical and quantum states can be extracted from corresponding classical and quantum propositional logics [10]. The discrete model embodied by the above-described category **Spek** has the important feature that, while for ordinary quantum propositional logics the orthocomplementation is an additional piece of structure, here it arises from the underlying set-theoretic complement:



We intend to study how this additional feature enables us to strengthen the concept of informatic ordering. Also, given the above abstract characterisation of doubly-stochastic maps, we can in full generality define a generalised majorization order [3] on states and morphisms by setting that a morphism $f : X_1 \to X_2$ is majorized by morphism $g : Y_1 \to Y_2$ if there exist doubly stochastic maps $h_1 : X_1 \to Y_1$ and $h_2 : X_2 \to Y_2$ such that $g = h_2 \circ f \circ h_1^\dagger$ [22]. All these informatic orderings allow us to compare important informatic quantities without needing to assign specific values. This method allows substantial simplification of various computations. We aim to exploit this fact in applications of our framework to quantum communication, cryptography and algorithms.

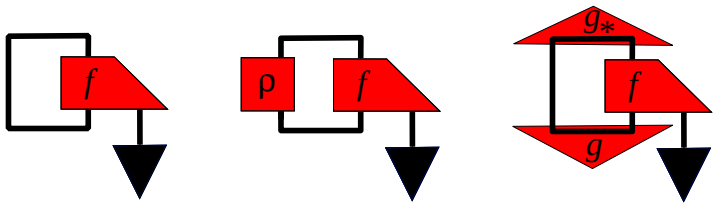
C*-algebra. A recent result by proposed RA Vicary establishes C*-algebras as an intermediate level of abstraction between ordinary quantum theory and †-SMCs with abstract basis structures. He showed that in finite dimensions, C*-algebras are equivalent to a certain class of †-Frobenius algebras [60]. This is significant, as it demonstrates that finite-dimensional C*-algebras can be completely axiomatised within our approach described above. He has also been successful in describing the spectral theorem in a categorical fashion [60]. In [9] the authors identified information-theoretic constraints which single out which C*-algebras correspond to quantum theory. We intend to explore this connection between the C*-algebraic formulation of quantum theory and information theory further now relying on their high-level representation

of [60].

Quantum informatic resources and measures. Ideas from classical Shannon-style information theory have proved influential in understanding quantum information-flow quantitatively; for example, channel-capacity theorems for quantum communication channels are studied intensively. As compared to the classical theory, however, quantum information theory possesses a host of seemingly incomparable resources such as quantum channels, entanglement, classical channels, coherent communication, and so on. Recent work has indicated the exciting possibility of developing a *symbolic calculus* of resource inequalities to describe relations between different mechanisms for information flow, and to systematically organize the many different types of quantum resources [27, 28, 29, 36]. The simplest example is

$$[qq] + 2[c \to c] \geq [q \to q],$$

capturing teleportation and expressing that an entangled pair $[qq]$ and a channel for two classical bits is *at least as powerful as* a channel for quantum bits, and this holds *in compositional contexts*, i.e. in situations where the teleportation protocol is embedded into other more complex protocols. Furthermore the inequality holds not just for sending one qubit; one can actually prove asymptotic bounds on rates of data transmission. This program would greatly benefit from explicit articulation of what it means to compose protocols, to prove equivalences between protocols and to have a general compositional theory of information-flow. In particular, the copying operation of the basis structure provides and abstract counterpart to Harrow's coherent communication scheme [36]. The natural mathematical context to study compositionality and process- or protocol-equivalence is categorical quantum computational semantics. Note that categorical quantum informatic semantics allows explicit representation and computation of key quantum informatic quantities such as channel fidelity [41], entanglement fidelity [53] and entanglement generating capacity [26] emerge naturally as:



where the black triangle represents the maximal mixed state [16].

3.3.1 Objectives

O3.1 Informatic orderings which allow us to compare important quantum informatic quantities for various systems, algorithms and protocols.

O3.2 A presentation of C*-algebras in terms of information flow and informatic quantities.

O3.3 A compositional theory of quantum informatic resources and quantities.

3.3.2 Milestones

M3.1 An order-theoretic denotational semantics for the above-discussed operational semantics and corresponding measures of informatic content.

M3.2 A high-level quantitative analysis of the major QKD protocols.

M3.3 A compositional semantics underlying DHW resource calculus.

3.4 Digest: a high-level and quantitative account of quantum communication and cryptography

All the above elements together together provide a high-level comprehensive account of quantum algorithms and communication protocols. It involves powerful high-level methods which result both in quantitative accounts as well as tools. It turns QIC research into a systematic discipline, not just a bag of clever tricks. We intend to blend this novel form of QIC research with the currently available and successful high-level methods for dealing with distributed, hybrid and embedded systems, and high-level accounts of knowledge acquisition and hiding (e.g. [4]). The graphical language enables knowledge-transfer among all involved disciplines.

3.4.1 Objectives

O4.1 Quantum communication and cryptography as a high-level systematic discipline.

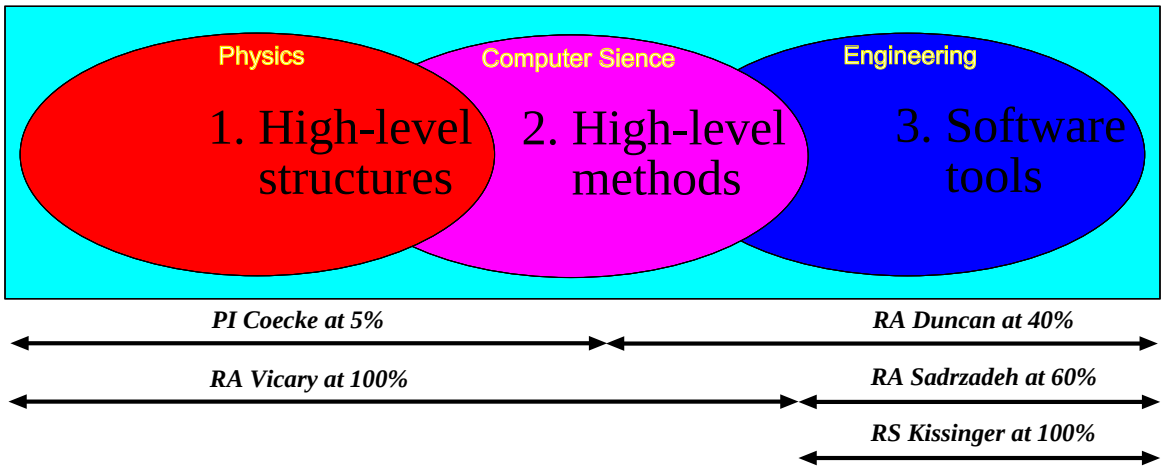
O4.2 Unifying quantum communication and cryptography research and the available high-level accounts of distributed, hybrid and embedded systems, and knowledge acquisition/hiding.

4 Diagrammatic workplan

See SOW.

5 Management approach

The proposed research will involve several researchers with different backgrounds. These distinct backgrounds represent the distinct disciplines involved in the endeavour:



This diagram makes it clear that the proposal is fundamentally multidisciplinary. Several of the proposed collaborators, in particular those active in the software development part of the above diagram, have prestigious personal fellowships and so require no direct allocation of funds. RAs R. Duncan (UK citizen) and M. Sadrzadeh (Canadian) both enjoy prestigious EPSRC-ICT[4] Postdoctoral Research Fellowships while RS A. Kissinger (US citizen) holds a prestigious Clarendon Studentship. All three will mainly work on the software development aspect of the proposal. The theory aspect of the proposal requires both unusual (theoretical physics as well as logic and category theory) and outstanding skills, given the technical difficulty of the problems we intend to solve. We request funding for a brilliant young mathematical physicist J. Vicary (UK citizen) who meanwhile has made pioneering contributions to the categorical quantum computational semantics research program.

5.1 Research track of the PI

Bob Coecke (Belgian) is University Lecturer in Quantum Computer Science at Oxford University Computing Laboratory, and a Governing Body Fellow of Wolfson College. He currently enjoys an EPSRC Advanced Research Fellowship for his work on the structure of quantum information and its ramifications for IT. He obtained his PhD in Theoretical Physics at the Free University of Brussels, and held postdoctoral positions at Imperial College of Science, Technology and Medicine in London, at McGill University in Canada and at Cambridge University.

In 2004 he was awarded the *2004 Biennial Prize for Meritorious Research in the Field of Quantum Structures* by the International Quantum Structures Association. He gave 75 invited talks in a period of 6 years. He coordinates the EC FET Open STREP Foundational Structures for Quantum Information and Computation (QICS), worth 1.625 M EUR, which has the development of high-level methods for unconventional quantum computational models as its main focus, and involves leading European Quantum Informatics and CS groups. This proposal was ranked 2nd out of the 487 proposals that were submitted for this FET Open call within FP6.

Coecke has approximately 75 refereed publications. A joint paper with Abramsky [1] in 2004 was the first paper on quantum computing ever to have been accepted for the prestigious IEEE conference on Logic in Computer Science, and a joint paper with Duncan was the first paper entirely devoted to quantum informatics to ever have been accepted to the Semantics, Logic and Theory track of ICALP [17]. In 2000 Coecke was invited to produce the volume *Current Research in Operational Quantum Logic: Algebras, Categories, Languages* in Springer's *Fundamental Theories of Physics* series. Recently he was invited to produce a number of volumes under the title *New Structures for Physics* in Springer's Lecture Notes in Physics series.

He also organized several events on mathematical formalisms and high-level methods for quantum computing. He was recently invited to organise a special session on Quantum Algorithms and Complexity at this year's Computability in Europe conference, and is currently the PC chair of the Joint International Workshop on Quantum Physics and Logic / Development of Computational Models, a satellite of this year's ICALP conference.

[4]Engineering and Physical Sciences Research Council - Information and Communication Technology.

5.2 Host institution

Oxford University pioneered quantum computation. From David Deutsch's development of the quantum analogue of the Church-Turing Thesis [25] and his invention of the first quantum algorithm, to the discovery of the Ekert 91 QKD protocol [31] and the first experimental implementation of a quantum algorithm [37], Oxford University has remained a leader in the field.

While initially the activity was mainly within the physics department, the Computing Laboratory (OUCL) now hosts one of the largest groups in the area, led by Professor Samson Abramsky FRS and Dr Bob Coecke. By a long way they are the largest group in the world working on high-level methods for QIC, and will next year be over 20 researchers strong. Many of these researchers hold prestigious personal fellowships and studentships. Oxford University Computing Laboratory also hosts a very strong Secure Computation group led by Bill Roscoe, which includes Gavin Lowe (who broke and fixed the Needham-Schroeder protocol) and currently also Dusko Pavlovic as a long-term visitor. It also hosts one of the strongest verification groups (both model checking and theorem proving) in the world, led by Martha Kwiatkowska and Tom Melham. Oxford University Computing Laboratory is a world-leader for computer science semantics, having made pioneering contributions to topics such as computer science logic, categorical semantics and domain theory.

5.3 Research track of the RAs

The requested funding will enable us to hire the exceptionally talented young mathematical physicist Jamie Vicary (UK citizen). He is the only sufficiently gifted and skilled researcher who can perform both the mathematical and the theoretical components of the research outlined above. Despite his young age all of his single-author publications [59, 60, 61] are groundbreaking pieces of work. Two OUCL postdocs and one student have agreed to work on the software development aspect of the proposal, in the event that our bid is successful. Both Duncan and Sadrzadeh obtained their prestigious EPSRC-ICT Postdoctoral Research Fellowships for their PhD work on Computer Science Semantics, and both have recently started active implementation [30, 52]. Kissinger holds a prestigious Clarendon Studentship and will dedicate all of his time to the software development aspects of this project in the event that our bid is successful.

5.4 Other ongoing research projects of the PI

- He currently enjoys a five-year EPSRC Advanced Research Fellowship entitled *The structure of quantum information and its ramifications for IT*, which relieves him from most of his faculty duties.

- He currently coordinates the EC FET Open STREP entitled *Foundational Structures for Quantum Information and Computation* (QICS), worth 1.625 M EUR, aiming at the development of high-level methods for unconventional quantum computational models such as measurement-based quantum computing, topological quantum computing and adiabatic quantum computing. This network involves leading European Quantum Informatics and CS groups, including Jozsa's group in Bristol, Werner's group in Braunschweig, Braunstein's group in York and Briegel's group in Innsbruck. The know-how present in this consortium will be invaluable for the work proposed here.

References

[1] S. Abramsky and B. Coecke (2004) *A categorical semantics of quantum protocols*. In: Proc. 19th IEEE conf. on Logic in Computer Science, pages 415–425. IEEE Press. arXiv:quant-ph/0402130.

[2] S. Abramsky and B. Coecke (2005) *Abstract physical traces*. Theory and Applications of Categories **14**, 111–124. http://www.tac.mta.ca/tac/volumes/14/6/14-06abs.html

[3] P. M. Alberti and A. Uhlmann (1983) *Stochasticity and Partial Order. Doubly Stochastic Maps and Unitary Mixing*. Reidel Publishing Company.

[4] A. Baltag, B. Coecke and M. Sadrzadeh (2007) *Epistemic actions as resources*. Journal of Logic and Computation **17**, 555–585. arXiv:math.LO/0608166.

[5] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher (1996) *Noncommuting mixed states cannot be broadcast*. Physical Review Letters, **76**, 2818–2821. arXiv:quant-ph/9511010

[6] C. H. Bennett and G. Brassard (1984) *Quantum Cryptography: Public Key Distribution and Coin Tossing*. Proceedings IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179. IEEE Press.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wooters (1993) *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*. Physical Review Letters **70**, 1895–1899.

[8] A. Carboni and R. F. C. Walters (1987) *Cartesian bicategories I*. Journal of Pure and Applied Algebra **49**, 11–32.

[9] R. Clifton, J. Bub and H. Halvorson (2003) *Characterizing quantum theory in terms of information-theoretic constraints*. Foundations of Physics **33**, 1561–1591. arXiv:quant-ph/0211089

[10] B. Coecke (2003) *Entropic geometry from logic*. Electronic Notes in Theoretical Computer Science **83**, 2003. arXiv:quant-ph/0212065

[11] B. Coecke (2003) *The logic of entanglement. An invitation*. Oxford University Computing Laboratory Research Report PRG-RR-03-12. arXiv:quant-ph/0402014 (8 page short version) web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html (full 160 page version)

[12] B. Coecke (2005) *Quantum information-flow, concretely, and axiomatically*. In: Proc. Quantum Informatics 2004, Y. Ozhigov (ed), pages 15–29. Proc. SPIE **5833**. arXiv:quant-ph/0506132

[13] B. Coecke (2005) *Kindergarten quantum mechanics — lecture notes*. In: Quantum Theory: Reconsiderations of the Foundations III, pages 81–98. AIP Press. arXiv:quant-ph/0510032

[14] B. Coecke (2006) *Introducing categories to the practicing physicist*. In: What is Category Theory? pages 45–74. Advanced Studies in Mathematics and Logic **30**, Polimetrica Publishing.

[15] B. Coecke (2007) *Complete positivity without positivity and without compactness*. Oxford University Computing Laboratory Research Report PRG-RR-07-05. web.comlab.ox.ac.uk/ oucl/publications/tr/rr-07-05.html

[16] B. Coecke (2008) *Axiomatic description of mixed states from Selinger's CPM-construction*. Electronic Notes in Theoretical Computer Science **210**.

[17] B. Coecke and R. Duncan (2008) *Interacting quantum observables*. In: Proc. 35th Int. Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science, to appear. On arXiv early May.

[18] B. Coecke, B. Edwards and J. Vicary (2008) *Everything you ever thought about relations*. In: New Structures for Physics II: approaches, B. Coecke, Ed, to appear, Springer Lecture Notes in Physics.

[19] B. Coecke and B. Edwards (2008) *Toy quantum categories*. In: Proc. Quantum Physics and Logic/Development of Computational Models (QPL-DCM). Electronic Notes in Theoretical Computer Science, to appear.

[20] B. Coecke and E. O. Paquette (2006) *POVMs and Naimark's theorem without sums*. Electronic Notes in Theoretical Computer Science (To appear). arXiv:quant-ph/0608072

[21] B. Coecke, E. O. Paquette and S. Perdrix (2008) *Bases in diagramatic quantum protocols*. In: Proc. Mathematical Foundations for Programming Semantics XXIV, to appear.

[22] B. Coecke, E. O. Paquette and D. Pavlovic (2008) *Classical structures from tensorial quantum structures*. In: New Structures for Physics II: approaches, B. Coecke, Ed, to appear, Springer Lecture Notes in Physics.

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

[24] B. Coecke, D. Pavlovic, and J. Vicary (2008) *Commutative †-Frobenius algebras in* **FdHilb** *are bases*. In preparation.

[25] D. Deutsch (1985) *Quantum theory, the church-turing principle, and the universal quantum computer*. Proceedings of the Royal Society of London A **400**, 97–117.

[26] I. Devetak (2003) *The private classical information capacity and quantum information capacity of a quantum channel*. arXiv:quant-ph/0304127v3

[27] I. Devetak and A. Winter (2004) *Distilling common randomness from bipartite quantum states*. IEEE Transactions in Information Theory **50**, 3183–3195.

[28] I. Devetak, A. W. Harrow and A. Winter (2005) *A resource framework for quantum Shannon theory*. arXiv:quant-ph/0512015

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

[30] L. Dixon and R. Duncan (2008) *Extending graphical representations for compact closed categories with applications to symbolic quantum computation*.

[31] A. Ekert (1991) *Quantum cryptography based on Bell's theorem*. Physical Review Letters **67**, 661–663.

[32] J.-Y. Girard (1987) *Linear logic*. Theoretical Computer Science **50**, 1–102.

[33] D. Gottesman and I. L. Chuang (1999) *Quantum teleportation is a universal computational primitive*. Nature **402**, 390–393. arXiv:quant-ph/9908010

[34] D. M. Greenberger, M. A. Horne, A. Shimony and A. Zeilinger (1990) *Bell's theorem without inequalities*. American Journal of Physics **58**, 1131–1143.

[35] L. Grover (1997) *Quantum mechanics helps in searching for a needle in a haystack*. Physical Review Letters **79**, 325–328. arXiv:quant-ph/9706033

[36] A. Harrow (2004) *Coherent communication of classical messages*. Physical Review Letters **92**, 097902. arXiv:quant-ph/0307091

[37] J. A. Jones and M. Mosca (1998) *Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer*. Journal of Chemical Physics **109**, 1648–1653

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

[39] L. H. Kauffman (2005) *Teleportation topology*. Optics and Spectroscopy **99**, 227–232. arXiv:quant-ph/0407224

[40] G. M. Kelly and M. L. Laplaza (1980) *Coherence for compact closed categories*. Journal of Pure and Applied Algebra **19**, 193–213.

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

[42] G. Lowe (1995) *An attack on the Needham-Schroeder public-key*. Information Processing Letters **56**, 131–133.

[43] G. Lowe (1996) *Breaking and fixing the Needham-Schroeder public-key protocol using FDR*. Software - Concepts and Tools **17**, 93–102.

[44] K. Martin (2000) *A foundation for computation*. Ph.D. Thesis, Department of Mathematics, Tulane University.

[45] K. Martin, I. S. Moskowitz and G. Allwein (2006) *Algebraic information theory for binary channels*. Electronic Notes in Theoretical Computer Science **158**, 289-306.

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

[47] A. K. Pati and S. L. Braunstein (2000) *Impossibility of deleting an unknown quantum state*. Nature **404**, 164–165.

[48] R. Penrose (1971) *Applications of negative dimensional tensors*. In: Combinatorial Mathematics and its Applications, D.J.A. Welsh, Ed, pages 221–244. Academic Press.

[49] S. Perdrix (2005) *State transfer instead of teleportation in measurement-based quantum computation*. International Journal of Quantum Information **3**, 219–223. arXiv:quant-ph/0402204

[50] R. Raussendorf and H.-J. Briegel (2001) *A one-way quantum computer.* Physical Review Letters **86**, 5188.

[51] R. Raussendorf, D. E. Browne and H.-J. Briegel (2003) *Measurement-based quantum computation on cluster states*. Physical Review A **68**, 022312. arXiv:quant-ph/ 0301052.

[52] S. Richards and M. Sadrzadeh, 'Aximo: Automated Axiomatic Reasoning for Information Update', Proceedings of the 5th workshop on Methods for Modal Logic, Ecole normal superieure de Cachan, Nov 2007, France, to appear in Electronic Notes in Theoretical Computer Science. The actual `Aximo` tool is available at: http://eprints.ecs.soton.ac.uk/14909/

[53] B. Schumacher (1996) *Sending entanglement through noisy quantum channels*. Physical Review A **54**, 2614–2628.

[54] P. Selinger (2007) *Dagger compact categories and completely positive maps*. Electronic Notes in Theoretical Computer Science **170**, 139–163.

[55] P. Selinger (2008) *Finite dimensional Hilbert spaces are complete for dagger compact closed categories*. In: Proc. Quantum Physics and Logic/Development of Computational Models (QPL-DCM). Electronic Notes in Theoretical Computer Science, to appear.

[56] P. W. Shor (1994) *Algorithms for quantum computation: discrete logarithms and factoring*. Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, IEEE Computer Science Press.

[57] R. Spekkens (2007) *Evidence for the epistemic view of quantum states: A toy theory*. Physical Review A **75**, 032110.

[58] R. Spekkens (2007) *Axiomatization through foil theories*. Talk given at the FOILS workshop: Operational probabilistic theories as foils to quantum theory, University of Cambridge, Jul 5.

[59] J. Vicary (2007) *A categorical framework for the quantum harmonic oscillator*. International Journal of Theoretical Physics (To appear). arXiv:0706.0711

[60] J. Vicary (2008) *Categorical formulation of C*-algebras*. In: Proc. Quantum Physics and Logic/Development of Computational Models (QPL-DCM). Electronic Notes in Theoretical Computer Science, to appear.

[61] J. Vicary (2008) *Complex numbers in monoidal categories.* In preparation.

[62] W. Wootters and W. Zurek (1982) *A single quantum cannot be cloned*. Nature **299**, 802–803.

[63] M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert (1993) *'Event-ready-detectors' Bell experiment via entanglement swapping*. Physical Review Letters **71**, 4287–4290.