From reversible to irreversible computations

Alexander S. Green [1]

Computer Science and IT
The University of Nottingham
Nottingham, UK

Thorsten Altenkirch [2]

Computer Science and IT
The University of Nottingham
Nottingham, UK

Abstract

In this paper we study the relation between reversible and irreversible computation applicable to different models of computation — here we are considering classical and quantum computation. We develop an equational theory of reversible computations and an associated theory of irreversible computations which is obtained by marking some inputs as preinitialised heap and some outputs as garbage to be thrown away at the end of the computation. We present three laws which apply to irreversible classical and quantum computations and show that von Neumann's measurement postulate is derivable from them. We discuss the question whether these laws are complete for irreversible quantum computations.

Key words: Reversible computation, irreversible computation, quantum computation, categorical models.

1 Introduction

Abstract models of computation like λ-calculus, or even more abstractly Cartesian closed categories, are based on irreversible processes; indeed Cartesian products introduce projections which are irreversible. In contrast, in Physics the more fundamental notions describe processes in closed systems where every action is reversible, e.g. Newtonian Mechanics, Maxwellian electrodynamics and quantum mechanics fit into this pattern. Open systems, which allow irreversible processes, are a derived notion — they can be considered as a

[1] Email: asg@cs.nott.ac.uk
[2] Email: txa@cs.nott.ac.uk

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

subsystem of a closed system. Indeed, an irreversible process can be understood in terms of a reversible one with a particular assignment of boundary conditions, e.g. Feynman's and Wheeler's theory of absorbers [11].

Our plan is to follow the physical idea that reversibility is the fundamental notion, and irreversibility is a derived notion to model computation. Reversibility has been investigated by Bennett in his classical paper [3], where he shows that reversible computation has the same power as irreversible computation. It has also since been shown that, in terms of complexity, reversible space is the same as deterministic space [6]. Recently, Abramsky investigated the notion of reversible computation from a structural perspective [1].

This research builds on previous work of the second author with Jonathan Grattage on compiling QML [2,5]. QML's design is based on an analogy between classical and quantum computation. To make this precise we introduce two models of computation: FCC for Finite Classical Computation and FQC for Finite Quantum Computation. Both are based on a notion of reversible computation (bijections vs. unitary operators) and introduce irreversible computations as a derived notion; by marking certain inputs as preinitialised heap, and certain outputs as garbage which is thrown away (i.e. measured, in the quantum case) at the end of the computation. We also introduce the notion of extensional equivalence of two irreversible computations which are given by the associated functions on finite sets in the classical case, and by an embedding into the category of superoperators on finite dimensional Hilbert spaces in the quantum case. While the choice of extensional equality in the two examples is very natural, it is not parametric in the notion of reversible computation. We would like to obtain the notion of irreversible computation as a consequence of our choice of reversible computation.

The goal is approached by introducing three laws which state which algebraic properties a notion of irreversible computation derived from reversible computation must satisfy. Both FCC and FQC satisfy these laws, and it is shown that they are sufficient to derive von Neumann's measurement postulate, which in this setting corresponds to the statement that *measuring twice is the same as measuring once*. A natural question which arises is whether our laws are sufficient to characterise the equivalence of quantum circuits, at least for definable circuits (i.e. classical circuits viewed as quantum circuits).

Our work here is related to other, more sophisticated, categorical models of quantum computing such as Coecke's *Kindergarten Quantum mechanics* [4] and Selinger's dagger-complete categories [9].

Acknowledgements

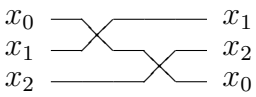
We would like to thank Jonathan Grattage for his help and discussions on this paper, and also the referee who suggested a number of simplifications of our laws and whose comments were very interesting and useful.

2 Reversible computation

We model reversible computations by a groupoid $\mathbf{FxC}^{\simeq}$, that is for every morphism $\psi \in \mathbf{FxC}^{\simeq}(a,b)$ there is an inverse $\psi^{-1} \in \mathbf{FxC}^{\simeq}(b,a)$ such that ψ, ψ^{-1} are an isomorphism. We assume that the groupoid is strict, i.e. that any isomorphic objects are equal. This entails that $\mathbf{FxC}^{\simeq}(a,b)$ is empty, if $a \neq b$, consequently we denote homsets by $\mathbf{FxC}^{\simeq}\, a = \mathbf{FxC}^{\simeq}(a,a)$. We also assume that $\mathbf{FxC}^{\simeq}$ has a strict monoidal structure $I, \otimes$ which corresponds to parallel composition of computations and a special object of Booleans,denoted by $\mathbb{N}_2$. Since we are only interested in objects which can be generated from $I, \mathbb{N}_2, \otimes$ we can use natural numbers $a \in \mathbb{N}$ to denote the object 2^a. Hence we have that $I = 0$, $\mathbb{N}_2 = 1$ and $a \otimes b = a + b$. We write $[a] = \{i \in \mathbb{N} \mid i < a\}$ for the initial segment of $\mathbb{N}$.

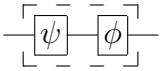
We characterise the morphisms, i.e. circuits, in $\mathbf{FxC}^{\simeq}a$ inductively and also give the inverses:

wires Given a bijection on initial segments $\phi : [a] \simeq [a]$ we write $\mathrm{wires}\,\phi \in \mathbf{FxC}^{\simeq}\, a$ for the associated *rewiring*. For example, the rewiring denoted schematically as

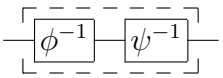


would have $\phi(0) = 2$, $\phi(1) = 0$, and $\phi(2) = 1$. The existence of wires follows from the strict monoidal structure, with the identity (id_a) being a special case of wires.

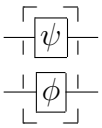
sequential composition combines two circuits of equal size (i.e. with the same number of wires) in sequence. That is, given $\psi, \phi \in \mathbf{FxC}^{\simeq}a$ we construct $\phi \circ \psi \in \mathbf{FxC}^{\simeq}a$.



we can construct the inverse using ϕ^{-1} and ψ^{-1} to give $\psi^{-1} \circ \phi^{-1}$.

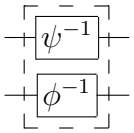


parallel composition combines any two circuits in parallel, and can be thought of as the tensor product. The size of the new circuit constructed is equal to the sum of the sizes of the original two circuits. That is, given $\psi \in \mathbf{FxC}^{\simeq}a$ and $\phi \in \mathbf{FxC}^{\simeq}b$ we can construct $\psi \otimes \phi \in \mathbf{FxC}^{\simeq}(a \otimes b)$.



again we can construct the inverse using ψ^{-1} and ϕ^{-1}, this time to give

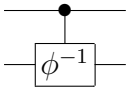
$\psi^{-1} \otimes \phi^{-1}$.



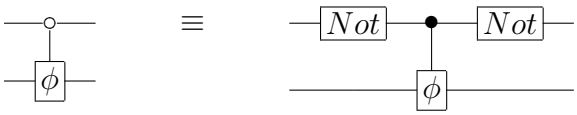
rotations count as any 1 "bit" operations. That is a rotation is any element of $\mathbf{FxC}^{\simeq}1$, and in the case of classical reversible circuits the only rotation available is the Not operation. So we have $\neg \in \mathbf{FxC}^{\simeq}1$ with $\neg^{-1} = \neg$. In the quantum case this would be any single qubit rotation.(i.e. a unitary operation in $U(2)$)

conditionals use a control wire to decide whether a computation should be performed. That is, given $\phi \in \mathbf{FxC}^{\simeq}a$ we can construct $id_a \mid \phi \in \mathbf{FxC}^{\simeq}(\mathbb{N}_2 \otimes a)$.

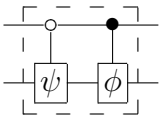
the inverse is again constructed using ϕ^{-1} giving $id_a \mid \phi^{-1}$.



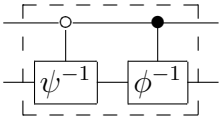
For ease of notation we shall also introduce the conditional that acts when the control wire is set to true. This conditional can be constructed from the conditional already given, and the Not operation (or rotation) as follows:



which for $\phi \in \mathbf{FxC}^{\simeq}a$ can be denoted $\phi \mid id_a \in \mathbf{FxC}^{\simeq}(\mathbb{N}_2 \otimes a)$. This naturally leads us to a choice operator, such that given two computations of the same size, the value of the control wire is used to govern which computation is done. That is, given $\psi, \phi \in \mathbf{FxC}^{\simeq}a$ we can construct $\psi \mid \phi \in \mathbf{FxC}^{\simeq}(\mathbb{N}_2 \otimes a)$, as follow:

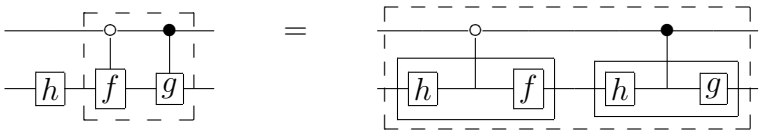


the inverse is once again given by ψ^{-1} and ϕ^{-1}, and constructed as $\psi^{-1} \mid \phi^{-1}$:

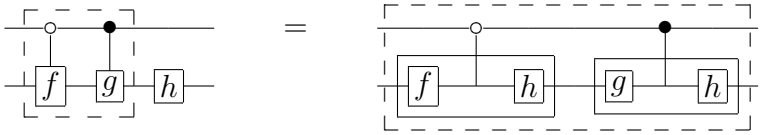


The laws governing wires, sequential composition and parallel composition follow from the categorical infrastructure. Additionally, we assume that the following equalities hold for conditionals:

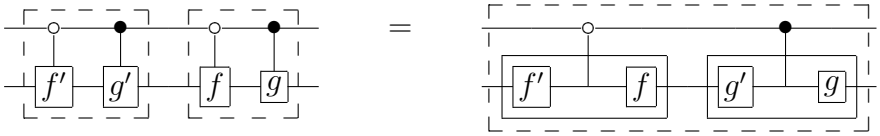
Firstly, we have for $f, g, h \in \mathbf{FxC}^{\simeq}a$ that $(f \mid g) \circ (\mathbb{N}_2 \otimes h) = f \circ h \mid g \circ h$ schematically this can be shown as:



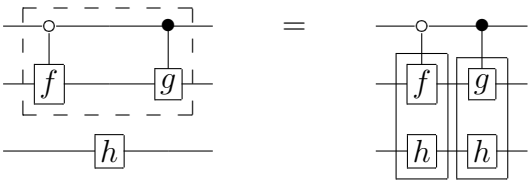
Secondly, we have for $f, g, h \in \mathbf{FxC}^{\simeq}a$ that $(\mathbb{N}_2 \otimes h) \circ (f \mid g) = h \circ f \mid h \circ g$ schematically this can be shown as:



and thirdly, we have that for $f, f', g, g' \in \mathbf{FxC}^{\simeq}a$ that $(f \mid g) \circ (f' \mid g') = (f \circ f') \mid (g \circ g')$ again the schematic representation for this would be:



We also have distributivity over $\otimes$ and $\mid$, such that given $f, g \in \mathbf{FxC}^{\simeq}a$ and $h \in \mathbf{FxC}^{\simeq}b$ we have that $(f \mid g) \otimes h = (f \otimes h) \mid (g \otimes h)$. This can again be given schematically.



using this last axiom it is possible to simplify the first two to just be that $(h \mid h) = (id_1 \otimes h)$ or schematically:

The next axiom that we introduce is that $id_a \mid id_a = id_{\mathbb{N}_2 \otimes a}$, and can be given (in it's most simple form) schematically as:

Moreover, we have for $f, g \in \mathbf{FxC}^{\simeq}a$ that $(\neg \otimes id_a) \circ (f \mid g) = (g \mid$

$f) \circ (\neg \otimes id_a)$, or schematically that would be:

Examples of $\mathbf{FxC}^{\simeq}$ *categories*

There are two obvious computational examples of $\mathbf{FxC}^{\simeq}$ categories: firstly there is the $\mathbf{FCC}^{\simeq}$ category of classical reversible circuits, and secondly there is the $\mathbf{FQC}^{\simeq}$ of quantum circuits. The difference mainly being in the rotations that are available. The extensional equality is given by interpreting circuits as permutations on $[a]$ in the classical case and as unitary operators on a-dimensional Hilbert spaces in the quantum case. Note that $\mathbf{FCC}^{\simeq} \hookrightarrow \mathbf{FQC}^{\simeq}$ and this embedding preserves extensional equality, because the unitary operators which can be obtained from definable circuits contain only 0 and 1 and hence can be obtained by embedding the corresponding permutation.

Bipermutative categories

A symmetric bimonoidal category $(\mathbb{C}, Z, \oplus, I, \otimes)$ is a category with two symmetric monoidal structures $(Z, \oplus)$ and $(I, \otimes)$ and distributivity isomorphisms $d \in A \otimes (B \oplus C) \simeq A \otimes B \oplus A \otimes C$ and $d' \in (A \oplus B) \otimes C) \simeq A \otimes C \oplus B \otimes C$ subject to a number of coherence laws [7]. A bipermutative category is a symmetric bimonoidal category where all isomorphisms apart from $c^{\oplus} \in A \oplus B \simeq B \oplus A$ and $c^{\otimes} \in A \otimes B \simeq B \otimes A$ are identities. There are still a number of coherence laws to be satisfied such as:

$$\begin{array}{ccc} A \otimes (B \oplus C) & = & (A \otimes B) \oplus (A \otimes C) \\ {\scriptstyle A \otimes c^{\oplus}}\downarrow & & \downarrow{\scriptstyle c^{\oplus}} \\ A \otimes (C \oplus B) & = & (A \otimes C) \oplus (A \otimes B) \end{array}$$

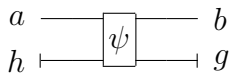
and

$$\begin{array}{ccc} A \otimes (B \oplus C) & = & (A \otimes B) \oplus (A \otimes C) \\ {\scriptstyle c^{\otimes}}\downarrow & & \downarrow{\scriptstyle c^{\otimes} \oplus c^{\otimes}} \\ (B \oplus C) \otimes A & = & (B \otimes A) \oplus (C \otimes A) \end{array}$$

The models for $\mathbf{FCC}^{\simeq}$ and $\mathbf{FQC}^{\simeq}$ give rise to bipermutative categories, where $\mathbb{N}_2 = I \oplus I$ and all the laws stated above hold in all bipermutative categories. Hence, this development could be stated more abstractly in terms of bipermutative categories.

3 Irreversible computation

A notion of irreversible computations is derived from the given notion of reversible computation by defining the category **FxC**, where every morphism of the category represents an irreversible computation, but is in fact of the form $\psi' = (h, g, \psi)$ where h is a set of heap inputs, g is a set of garbage outputs, and ψ is the underlying reversible computation. So a morphism in $\mathbf{FxC}(a, b)$ can be given as a morphism in $\mathbf{FxC}^{\simeq}((a \otimes h), (b \otimes g))$ with the requirement that $(a \otimes h) = (b \otimes g)$. Schematically, an irreversible computation (h, g, ψ) can be represented as the reversible computation ψ, where heap and garbage are marked explicitly:

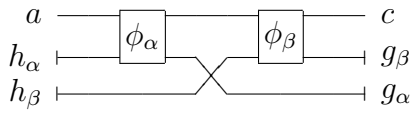


It is also the case that for any $\psi \in \mathbf{FxC}^{\simeq}a$, there is an equivalent circuit $\widehat{\psi} \in \mathbf{FxC}(a, a)$; this precisely is given by the following predicate:

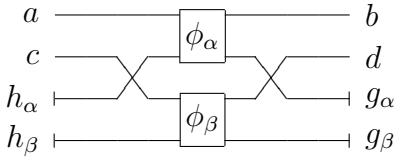
$$\frac{\psi \in \mathbf{FxC}^{\simeq}a}{\widehat{\psi} \in \mathbf{FxC}(a, a)}$$

such that $\widehat{\psi} = (0, 0, \psi)$, i.e. there is no heap or garbage.

Sequential composition for irreversible computations can be defined: given $\alpha = (h_\alpha, g_\alpha, \phi_\alpha) \in \mathbf{FxC}(a, b)$ and $\beta = (h_\beta, g_\beta, \phi_\beta) \in \mathbf{FxC}(b, c)$ we define $\beta \circ \alpha \in \mathbf{FxC}(a, c)$, as



The identity can be obtained by lifting the reversible identity $id_a^{\mathbf{FxC}} = \widehat{id_a^{\mathbf{FxC}^{\simeq}}}$. It is straightforward to verify that **FxC** thus constructed is a category by using the monoidal identities in the underlying category of reversible computations. Moreover, **FxC** inherits the monoidal structure from $\mathbf{FxC}^{\simeq}$, e.g. given $\alpha = (h_\alpha, g_\alpha, \phi_\alpha) \in \mathbf{FxC}(a, b)$ and $\beta = (h_\beta, g_\beta, \phi_\beta) \in \mathbf{FxC}(c, d)$, we obtain $\alpha \otimes \beta \in \mathbf{FxC}(a \otimes c, b \otimes d)$ as:



The neutral element of the tensor, the empty circuit, can be obtained by lifting $I^{\mathbf{FxC}} = \widehat{I^{\mathbf{FxC}^{\simeq}}}$.

Examples of **FxC** *categories*

The two example $\mathbf{FxC}^{\simeq}$ categories can now be extended to **FxC** categories: **FCC**, for the category of finite classical computations; and **FQC**, for finite

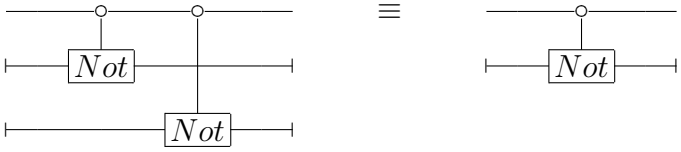
quantum computations. The extensional equality in the classical case is given by interpreting morphisms as functions on finite sets: $(h, g, \phi) \in \mathbf{FCC}(a, b)$ is interpreted as $\pi_g \circ [\![\phi]\!] \circ (0^h, -) \in [a] \to [b]$, where $[\![\phi]\!] \in [a \otimes h] \to [b \otimes g]$ is the associated permutation, $(0^h, -) \in [a] \to [a \otimes h]$ initialises the heap and $\pi_g \in [b \otimes g] \to b$ projects out the garbage.

In the quantum case circuits are interpreted as superoperators (see [8], [10], or [5] for an implementation in Haskell). Superoperators are morphisms on density operators, which are positive operators on the a-dimensional Hilbert space. A superoperator $f \in \mathbf{Super}(a, b)$ is a linear function mapping density operators on a to density operators on b, which preserve the trace and are stable under $\otimes$. Analogously to the classical case, we interpret $(h, g, \phi) \in \mathbf{FQC}(a, b)$ as $\mathrm{tr}_g \circ [\![\phi]\!] \circ 0^h \otimes - \in \mathbf{Super}(a, b)$, where $[\![\phi]\!] \in \mathbf{Super}(h \otimes a, g \otimes b)$ is the superoperator associated to the unitary operator given by interpreting the reversible circuit ϕ. $0^h \otimes - \in \mathbf{Super}(a, a \otimes h)$ initialises the heap and $\mathrm{tr}_g \in \mathbf{Super}(g \otimes b, b)$ is a partial trace which traces out the garbage.

4 Equivalence

In the reversible case the equality of definable circuits is the same in the classical case and in the quantum case, but this doesn't hold for irreversible computations. For example, in the classical case the following two circuits would be equivalent:

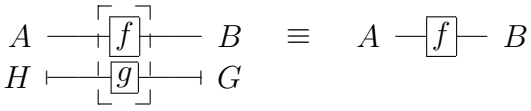
However, this equivalence does not hold when we move into the category of finite quantum computations **FQC**. This is because in quantum computation the control wire (or qubit) can become entangled with the target wire (qubit). However there is another similar equivalence that holds in **FQC**:



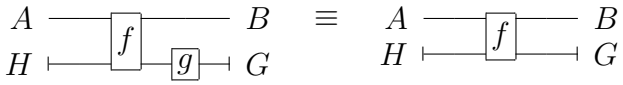
This is akin to von Neumann's measurement postulate. So, how now can we characterise the equivalences which should always hold?

We have developed three laws to try and characterise these equivalences, that hold in both **FCC** and **FQC**. The first law is that of garbage collection. It states that if a circuit can be reduced into two smaller circuits such that one part of the circuit only acts on heap inputs and on garbage outputs, then

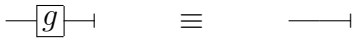
that part of the circuit can be removed.



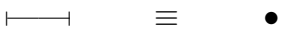
The second law is of the uselessness of garbage processing. This states that if a circuit can be reduced into two smaller circuits such that one part of the circuit only has an effect on garbage outputs, then that part can be removed.



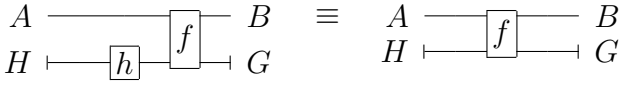
this can be alternately stated as saying that if the only outputs of (part of) a circuit are garbage outputs, then this is equivalent to just having garbage.



and similarly we can now simplify the first law to state that a wire that simply connects the heap to the garbage is equivalent to having nothing.

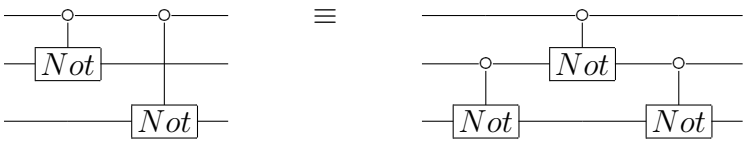


The third law is of the uselessness of heap preprocessing. This states that if a circuit can be reduced into two smaller circuits such that one part of the circuit only has effect on heap inputs, and the effect on the zero vector is the identity, then that part can be removed.
if $h\mathbf{0} = \mathbf{0}$ *then*



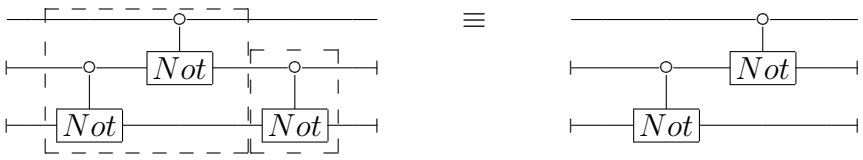
An alternate notation for this would again be to state that if (part of) a circuit only has heap inputs, and its effect on the zero vector is the identity, then this is equivalent to just having a heap.
if $h\mathbf{0} = \mathbf{0}$ *then*

We can already use these laws to give a proof of the measurement postulate. The first step is to show the equivalence of

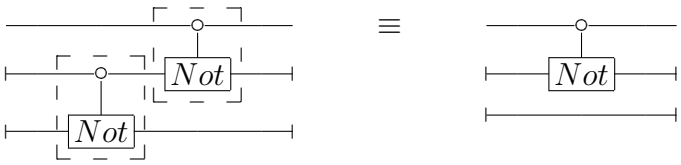


This is simple as you will notice there is no heap or garbage, so we know that the circuits are in $\mathbf{FQC}^{\simeq}$, and in fact only use the elements from $\mathbf{FCC}^{\simeq}$. Thus equivalence can be shown by looking at the truth tables, which are the same.

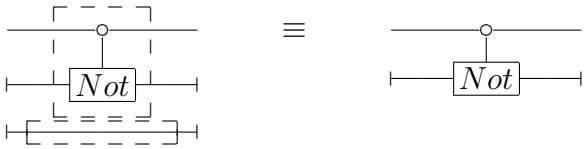
The third controlled not is eliminated using the second law:



The controlled Not operations preserve the zero vector, so we can eliminate the first one using the third law:



Finally the bottom wire can be removed by use of the first law:



5 Conclusions and further work

The first steps toward a theory of irreversible computation based on reversible computation have been outlined, and it has been shown that the laws presented here for irreversible computations are sufficient to derive von Neumann's measurement postulate. Apart from this, there are currently more questions than answers. One question is are there equalities between definable irreversible quantum circuits which are not derivable from our laws? It has been proposed that this question may be answered by translating our formalism into Selinger's dagger-complete categories [9]. Recent work by Coecke shows that this category is not equationally definable in terms of initialisations and measurements, however it is not clear at the moment whether such a counterexample is definable in our sense.

We are investigating whether we could state the whole development more abstractly using only symmetric, strictly bimonoidal, categories as the base for the notion of reversible computations. Currently, it is not clear how to state abstractly the precondition required by the third law; that a circuit is **0**-preserving. An alternative would be to drop this condition and to assume that a computation can be carried out, provided a correct initialisation. Interestingly, our laws would then be symmetric.

Finally, we would like to answer the question whether our laws are complete for quantum computation, that is whether we can characterise the equality of definable quantum circuits just by the three laws presented here.

References

[1] Abramsky, S., *A structural approach to reversible computation.*, Theor. Comput. Sci. **347** (2005), pp. 441–464.

[2] Altenkirch, T. and J. J. Grattage, *A functional quantum programming language*, in: *Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science, LICS 2005*, IEEE Computer Society Press, 2005, pp. 249–258.

[3] Bennett, C. H., *Logical reversibility of computation*, IBM Journal of Research and Development **17** (1973), pp. 525–532.

[4] Coecke, B., *Kindergarten quantum mechanics*, quant-ph/0510032 (2005).

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

[6] Lange, K.-J., P. McKenzie and A. Tapp, *Reversible space equals deterministic space*, in: *IEEE Conference on Computational Complexity*, 1997, pp. 45–50.

[7] Laplaza, M., *Coherence for distributivity*, Lecture Notes in Mathematics **281** (1972), pp. 29–72.

[8] Selinger, P., *Towards a quantum programming language*, Mathematical. Structures in Comp. Sci. **14** (2004), pp. 527–586.

[9] Selinger, P., *Dagger compact closed categories and completely positive maps*, in: P. Selinger, editor, *Proceedings of the 3rd International Workshop on Quantum Programming Languages*, Electronic Notes in Theoretical Computer Science (2005).

[10] Vizzotto, J. K., T. Altenkirch and A. Sabry, *Structuring quantum effects: Superoperators as arrows*, Mathematical Structures in Computer Science, special issue on Quantum Programming Languages (2006), to appear.

[11] Wheeler, J. A. and R. P. Feynman, *Interaction with the absorber as the mechanism of radiation*, Rev. Mod. Phys. **17** (1945), pp. 157–181.