Structuring quantum effects: superoperators as arrows

Juliana K. Vizzotto[1]* Thorsten Altenkirch[2] Amr Sabry[1]

[1] Department of Computer Science
Indiana University, USA

[2] School of Computer Science and IT
The University of Nottingham, UK

February 1, 2008

Abstract

We show that the model of quantum computation based on density matrices and superoperators can be decomposed in a pure classical (functional) part and an effectful part modeling probabilities and measurement. The effectful part can be modeled using a generalization of monads called arrows. We express the resulting executable model of quantum computing in the programming language Haskell using its special syntax for arrow computations. The embedding in Haskell is however not perfect: a faithful model of quantum computing requires type capabilities which are not directly expressible in Haskell.

1 Introduction

A newcomer to the field of quantum computing is immediately overwhelmed with many apparent differences with classical computing that suggest that quantum computing might require radically new semantic models and programming languages. In some sense this is true for two reasons: (1) quantum computing is based on a kind of parallelism caused by the non-local wave character of quantum information which is qualitatively different from the classical notion of parallelism, and (2) quantum computing has a peculiar notion of observation in which the observed part of the quantum state and every other part that is entangled with it immediately lose their wave character. Interestingly none of the other differences that are often cited between quantum and classical computing are actually relevant semantically. For example, even though we do not often think of classical computation as "reversible," it is just as reversible as quantum computing. Both can be compiled or explained in terms of reversible circuits [2], but in neither model should the user be required to reason about reversibility.

The two properties of quantum computing discussed above certainly go beyond "pure" classical programming and it has been suspected earlier that they might correspond to some notion of computational effect. Following Moggi's influential paper [9], computational effects like assignments, exceptions, non-determinism, *etc.* could all be modeled using the categorical construction of a *monad*. This construction has been internalized in the programming language Haskell as a tool to elegantly express computational effects within the context of a pure functional language. Since the work of Moggi, several natural notions of computational effects were discovered which could only be expressed as generalizations of monads. Of particular importance to us, is the generalization of monads known as arrows [7] which is also internalized in the programming language Haskell.

In an early paper, Mu and Bird (2001) showed that quantum parallelism is almost a monad. We expand and build on this observation as follows. First the traditional model of quantum computing

*Permanent address: Institute of Informatics, Porto Alegre, Brazil cannot even express measurements, so we use a known more general model using density matrices and superoperators. After expressing this model in Haskell, we establish that the superoperators used to express all quantum computations and measurements are indeed an instance of the concept of arrows (with a small caveat). In particular the construction clarifies the crucial need for some form of linear typing: arrow computations must be required to use every quantum value or else the computations produce results that are inconsistent with quantum mechanics.

In summary, our construction relates "exotic" quantum features to well-understood semantic constructions and programming languages. We hope it will serve as a useful tool to further understand the nature and structure of quantum computation. The remainder of the paper is organized as follows. Section 2 presents the traditional model of quantum computing and its implementation in Haskell, focusing on the possibility of structuring the effects using monads. Section 3 discusses the limitations of the traditional model as a complete model of quantum computation which should include measurement. Section 4 introduces a more general model of quantum based on density matrices and superoperators. Our main result is discussed in Section 5 where we show that general quantum computations including measurement can be structured using the generalization of monads called arrows. Section 6 gives two complete examples implementing a Toffoli circuit and the teleportation experiment: both examples use the arrow notation to express the structure of the computation elegantly. Section 7 discusses the limitations of our model and its connection to the functional quantum programming language QML [2]. Section 8 concludes. Appendix A explains the basics of the Haskell notation used in the paper, and the next two appendices present the proofs that are omitted from the main body of the paper.

2 The Traditional Model of Quantum Computing

We present the traditional model of quantum computing in this section.

2.1 Vectors

A finite set a can be represented in Haskell as an instance of the class *Basis* below. Given such a set a representing observable (classical) values, a pure quantum value is a vector $a \to \mathbb{C}$ which associates each basis element with a complex probability amplitude. The basis elements must be distinguishable from each other which explains the constraint *Eq a* on the type of elements below:

```
class Eq a =>  Basis a where basis :: [a]
type PA = Complex Double
type Vec a = a → PA
```

The type constructor *Vec* is technically not a monad: it corresponds to a *Kleisli structure* [3]. Yet as noted by Mu and Bird (2001), the probabilities introduced by vector spaces constitute a computational effect which can be structured using a slight generalization of monads in Haskell [9]. From a programming perspective, a monad is represented using a type constructor for computations m and two functions: $\mathit{return} :: a \to m\ a$ and $\gg\!= :: m\ a \to (a \to m\ b) \to m\ b$. The operation $\gg\!=$ (pronounced "bind") specifies how to sequence computations and *return* specifies how to terminate computations:

```
return :: Basis a => a → Vec a
return a b = if a≡b then 1 else 0

(>>=) :: Basis a => Vec a → (a → Vec b) → Vec b
va >>= f = λ b → sum [ (va a) * (f a b) | a ∈ basis]
```

Because of the additional constraint that our computations must be over specified bases whose elements must be comparable, the types of our operations are more restricted than strictly desired for a monad. However *return* and ≫= satisfy the three monad laws.

Proposition 2.1 *Vector spaces satisfy the required equations for monads.*

Proof. See Appendix B. □

Vector spaces have additional properties abstracted in the Haskell class *MonadPlus*. Instances of this class support two additional methods: *mzero* and *mplus* which provide a "zero" computation and an operation to "add" computations:

```
mzero :: Vec a
mzero = const 0

mplus :: Vec a → Vec a → Vec a
mplus v_1 v_2 a = v_1 a + v_2 a

mminus :: Vec a → Vec a → Vec a
mminus v_1 v_2 a = v_1 a - v_2 a
```

For convenience, it is also possible to define various kinds of products over vectors: the *scalar* product $\$*$, the *tensor* product $\langle * \rangle$, and the *dot* product $\langle \cdot \rangle$:

```
($*) :: PA → Vec a → Vec  a
pa $* v = λa → pa * v a

(<*>) :: Vec a → Vec b → Vec (a,b)
v1 <*> v2 = λ (a,b) → v1 a * v2 b

(<.>) :: Basis a => Vec a → Vec a → PA
v1 <.> v2 = sum (map (λa → conjugate (v1 a) * (v2 a)) basis)
```

Examples of vectors over the set of booleans may be defined as follows:

```
instance Basis Bool where basis = [False,Bool]
qFalse,qTrue,qFT,qFmT :: Vec Bool
qFalse = return False
qTrue = return True
qFT = (1 / sqrt 2) $* (qFalse ‘mplus‘ qTrue)
qFmT = (1 / sqrt 2) $* (qFalse ‘mminus‘ qTrue)
```

The first two are unit vectors corresponding to basis elements; the last two represent state which are in equal superpositions of *False* and *True*. In the Dirac notation, these vectors would be respectively written as $|\mathit{False}\rangle$, $|\mathit{True}\rangle$, $\frac{1}{\sqrt{2}}(|\mathit{False}\rangle + |\mathit{True}\rangle)$, and $\frac{1}{\sqrt{2}}(|\mathit{False}\rangle - |\mathit{True}\rangle)$.

Vectors over several values can be easily described using the tensor product on vectors or the Cartesian product on the underlying bases:

```
instance (Basis a, Basis b) => Basis(a, b) where
basis = [(a, b) | a ∈ basis, b ∈ basis ]

p1,p2,p3,epr :: Vec (Bool,Bool)
```

```
p1 = qFT <*> qFalse
p2 = qFalse <*> qFT
p3 = qFT <*> qFT

epr (False,False) = 1 / sqrt 2
epr (True,True) = 1 / sqrt 2
```

In contrast to the first three vectors, the last vector describes an *entangled* quantum state which cannot be separated into the product of independent quantum states. The name of the vector "*epr*" refers to the initials of Einstein, Podolsky, and Rosen who used such a vector in a thought experiment to demonstrate some strange consequences of quantum mechanics [5].

2.2 Linear Operators

Given two base sets A and B a linear operator $f \in A \multimap B$ is a function mapping vectors over A to vectors over B. We represent such operators as functions mapping values to vectors which is similar to representation used by Karczmarczuk (2003):

```
type Lin a b = a → Vec b

fun2lin :: (Basis a, Basis b) => (a → b) → Lin a b
fun2lin f a = return (f a)
```

The function *fun2lin* converts a regular function to a linear operator. For example, the quantum version of the boolean negation is:

```
qnot :: Lin Bool Bool
qnot = fun2lin ¬
```

Linear operations can also be defined directly, for example:

```
phase :: Lin Bool Bool
phase False = return False
phase True = (0 :+ 1) $* (return True)

hadamard :: Lin Bool Bool
hadamard False = qFT
hadamard True = qFmT
```

The definition of a linear operation specifies its action on one individual element of the basis. To apply a linear operation f to a vector v, we use the *bind* operation to calculate $v \gg= f$. For example $(\mathit{qFT} \gg= \mathit{hadamard})$ applies the operation *hadamard* to the vector *qFT* which one can calculate produces the vector *qFalse* as a result.

It is possible to write higher-order functions which consume linear operators and produce new linear operators. An important example of such functions produces the so-called *controlled operations*:

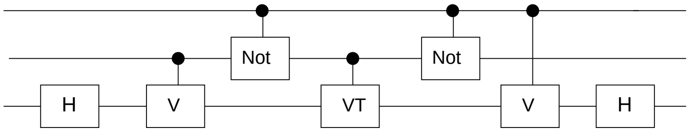
```
controlled :: Basis a => Lin a a → Lin (Bool,a) (Bool,a)
controlled f (b1,b2) = (return b1) <*> (if b1 then f b2 else return b2)
```

The linear operator f is transformed to a new linear operator controlled by a quantum boolean value. The modified operator returns a pair whose first component is the input control value. The second input is passed to f only if the control value is true, and is otherwise left unchanged. For example, $(\mathit{qFT}\ \langle*\rangle\ \mathit{qFalse}) \ggg= (\mathit{controlled\ qnot})$ applies the familiar *controlled-not* gate to a vector over two values: the control value is a superposition of *False* and *True* and the data value is *False*. As one may calculate the result of this application is the *epr* vector.

Linear operations can be combined and transformed in several ways which we list below. The function $\rangle*\langle$ produces the linear operator corresponding to the *outer product* of two vectors. The functions *linplus* and *lintens* are the functions corresponding to the sum and tensor product on vectors. Finally the function *o* composes two linear operators.

```
adjoint :: Lin a b → Lin b a
adjoint f b a = conjugate (f a b)

(>*<) :: Basis a => Vec a → Vec a → Lin a a
(v1 >*< v2) a1 a2 = v1 a1 * conjugate (v2 a2)

linplus :: (Basis a, Basis b) => Lin a b → Lin a b → Lin a b
linplus f g a = f a ‘mplus‘ g a

lintens :: (Basis a, Basis b, Basis c, Basis d) =>
                Lin a b → Lin c d → Lin (a,c) (b,d)
lintens f g (a,c) = f a <*> g c

o :: (Basis a, Basis b, Basis c) => Lin a b → Lin b c → Lin a c
o f g a = (f a >>= g)
```

2.3 Example: A Toffoli Circuit



The circuit diagram uses the de-facto standard notation for specifying quantum computations. Each line carries one quantum bit (*qubit*); we refer to the three qubits in the circuit as *top*, *middle*, and *bottom*. The values flow from left to right in steps corresponding to the alignment of the boxes which represent quantum gates. The gates labeled H, V, VT, and *Not* represent the quantum operations *hadamard*, *phase*, *adjoint phase*, and *qnot* respectively. Gates connected via a bullet to another wire are *controlled* operations.

In general all three qubits in the circuit may be entangled and hence the state vector representing them cannot be separated into individual state vectors. This means that, despite the appearance to the contrary, it is not possible to operate on any of the lines individually. Instead the circuit defines a linear operation on the entire state:

```
toffoli :: Lin (Bool,Bool,Bool) (Bool,Bool,Bool)
toffoli (top,middle,bottom) =
   let cnot = controlled qnot
       cphase = controlled phase
       caphase = controlled (adjoint phase)
   in hadamard bottom >>= λ b1 →
      cphase (middle,b1) >>= λ (m1,b2) →
```

```
cnot (top,m1) >>= λ (t1,m2) →
caphase (m2,b2) >>= λ (m3,b3) →
cnot (t1,m3) >>= λ (t2,m4) →
cphase (t2,b3) >>= λ (t3,b4) →
hadamard b4 >>= λ b5 →
return (t3,m4,b5)
```

3 Measurement

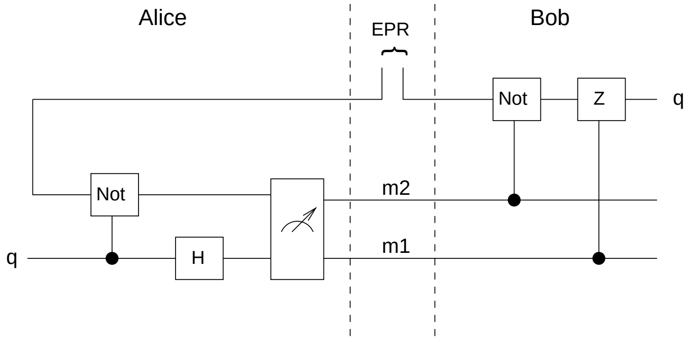
The use of monads to structure the probability effects reveals an elegant underlying structure for quantum computations. This structure can be studied in the context of category theory and exploited in the design of a calculus for quantum computation [14, 15, 13, 2].

Unfortunately in the traditional model of quantum computing we have used so far, is difficult or impossible to deal formally with another class of quantum effects, including measurements, decoherence, or noise. We first give one example where such effects are critical, and then discuss various approaches in the literature on how to deal with such effects.

3.1 Teleportation

The idea of teleportation is to disintegrate an object in one place making a perfect replica of it somewhere else. Indeed quantum teleportation [4] enables the transmission, *using a classical communication channel*, of an unknown quantum state via a previously shared *epr* pair.

In the following diagram, Alice and Bob initially have access to one of the qubits of an entangled *epr* pair, and Alice aims to teleport an unknown qubit q to Bob:



The calculation proceeds as follows. First Alice interacts with the unknown qubit q and her half of the *epr* state. Then Alice performs a measurement collapsing her quantum state and getting two classical bits m_1 and m_2 that she transmits to Bob using a classical channel of communication.

Upon receiving the two classical bits of information, Bob interacts with his half of the *epr* state with gates controlled by the classical bits. The circuit in the figure can be shown to re-create the quantum state q which existed at Alice's site before the experiment.

Our main interest in this circuit is that it is naturally expressed using a sequence of operations on quantum values which include a non-unitary *measurement* in the middle. Using the model developed in the previous section, it is not possible to describe this algorithm as stated. In the next section, we briefly several possible ways to deal with this problem.

3.2 Dealing with Measurement

The literature includes several approaches to the problem of measurement. We characterize such approaches in three broad categories: deferring measurements, using classical control with pointers and side-effects, and using density matrices and superoperators. We discuss the first two approaches in the remainder of this section, and expand on the latter approach in the next section.

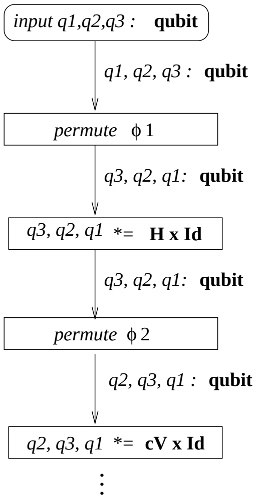
3.2.1 Deferring measurements:

The first approach (used for example by Mu and Bird (2001), Van Tonder (2003; 2004) and Karczmarczuk (2003) relies on the *principle of deferred measurement* [8]. This principle can be used to transform computations to *always* defer measurements to the end. Using this idea one can focus entirely on managing the probability effects and perform the measurements outside the formalism. The drawback of this approach is clear: programs that interleave quantum operations with measurements cannot be expressed naturally. For example, transforming the teleportation circuit above to defer the measurements until after Bob's computation completely changes the character of the experiment, because no *classical* information is transmitted form Alice to Bob.

3.2.2 Classical Control and Side-effects:

In general, this category of models is based on the so-called QRAM (quantum random access machine) model of Knill (1996), which is summarized by the slogan "quantum data, classical control" [12]. In this context, a quantum computer can be seen as a classical computer with a quantum device attached to it. The classical control sends instructions for the quantum machine to execute unitary operations and measurements. A measurement collapses the quantum (probabilistic) computation and forces it to produce a classical (deterministic) result. In fact, the situation is even more complicated: measuring part of a quantum state collapses not only the measured part but any other part of the global state with which it is entangled. The most common approach to computationally realize this hybrid architecture is via manipulating what are effectively *pointers* to a *global shared quantum state* as the following examples show:

- In the flowchart notation for the language introduced by Selinger (2004), the state is represented by a collection of variables that can each be assigned *once*. An operation can only be applied to an initial group of the variables (and is implicitly composed with the identity on the remaining variables). If the variables are not in the desired order, they must be permuted first. Thus the first few steps of the *toffoli* circuit are:



- In the procedural language QCL [10] a *quantum register* is a realized using *pointers* to the complete state. Operations on a register map to operations on the state as follows. If we have an m-qubit register r which points to an n-qubit state, then an operation U on the register is realized using:

  $$U(r) = \Pi_r^\dagger \ (U \times I(n-m)) \ \Pi_r$$

  The operation U is composed with the identity on the remaining number of qubits of the state. The operator Π_r is an arbitrary reordering operator and $\Pi_r^\dagger$ is its inverse. After re-ordering, the lifted U composed with the identity is applied, and the result is permuted back to the original order.

- Jan Skibiński (2001) produced an early Haskell simulator of a quantum computer. The simulator maintains quantum registers and allows operations to act on specific qubits using what is essentially pointers. To apply an operation to the third, fifth, and seventh qubits on a quantum register, some low-level calculations depending on the indices and size of the register are used to produce a lifted operation composed with several identity operations that acts on the entire register.

- Valiron *et. al.* (2004) develop a functional quantum programming language based on the original work of Selinger (2004). The representation of quantum data in their calculus uses an external n-qubit state Q. Programs may contain free variables which are essentially pointers to the quantum state.

- In our previous work [11] we introduced *virtual values* to hide the management of pointers to the global state. Using virtual values the code for the *toffoli* example is essentially identical to the one presented earlier, *except* for the need to manually generate the *adaptors* which mediate between the virtual value and the global state.

The use of pointers and sharing to model the side-effect of measurement is in some sense adequate. However by doing so, we completely lose the monadic structure and the direct connections to categorical semantics.

4 Density Matrices and Superoperators

Fortunately the usual model of quantum computing can be generalized to solve the problem of modeling measurements in a better way. In the generalized model, the state of the computation is represented using a *density matrix* and the operations are represented using *superoperators* [1]. Using these notions, the *projections* necessary to express measurements become expressible within the model. We review this model in this section.

4.1 Density Matrices

Intuitively, density matrices can be understood as a statistical perspective of the state vector. In the density matrix formalism, a quantum state that used to be modeled by a vector v is now modeled by its outer product.

```
type Dens a = Vec (a,a)

pureD :: Basis a => Vec a → Dens a
pureD v = lin2vec (v >*< v)

lin2vec :: (a → Vec b) → Vec (a,b)
lin2vec = uncurry
```

The function *pureD* embeds a state vector in its density matrix representation. For convenience, we uncurry the arguments to the density matrix so that it looks more like a "matrix." For example, the density matrices corresponding to the vectors *qFalse*, *qTrue*, and *qFT* can be visually represented as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

The appeal of density matrices is that they can represent states other than the pure ones above. In particular if we perform a measurement on the state represented by qFT, we should get *False* with probability 1/2 or *True* with probability 1/2. This information which cannot be expressed using vectors, can be represented by the following density matrix:

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Such a density matrix represents a *mixed state* which corresponds to the sum (and then normalization) of the density matrices for the two results of the observation. If we further calculate with the result of measuring qFT by for example, applying the *hadamard* operation, we get one of the two vectors qFT or $qFmT$, each with probability 1/2. Because all operations on vectors are *linear*, we can express this step as follows:

$$H \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = H \begin{pmatrix} 1/2 & 0 \\ 0 & 0 \end{pmatrix} + H \begin{pmatrix} 0 & 0 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

As the calculation shows, the application of *hadamard* has no effect on the density matrix, and indeed there is no observable difference between the two configurations before and after the application of *hadamard*. Indeed, the density matrix representation loses the information in the state vectors that is not observable [12] and hence is a better representation from a semantic perspective.

4.2 Superoperators

Operations mapping density matrices to density matrices are called *superoperators*:

```
type Super a b = (a,a) → Dens b

lin2super :: (Basis a, Basis b) => Lin a b → Super a b
lin2super f (a1,a2) = (f a1) <*> (dual (adjoint f) a2)
     where dual f a b = f b a
```

The function *lin2super* constructs a superoperator from a linear operator on vectors. To understand the basic idea, consider the density matrix resulting from the application of f to $|v\rangle$. This corresponds to the outer product of the vector $f\ |v\rangle$ with itself, which applies f to $|v\rangle$ and the adjoint of f to the "dual vector."

4.3 Tracing and Measurement

In contrast to the situation with the traditional model of quantum computing, it is possible to define a superoperator which "forgets", *projects*, or *traces out* part of a quantum state as well as a superoperator which *measures* part of a quantum state:

```
trL :: (Basis a, Basis b) => Super (a,b) b
trL ((a1,b1),(a2,b2)) =  if a1 ≡ a2 then return (b1,b2) else mzero

meas :: Basis a => Super a (a,a)
meas (a1,a2) = if a1 ≡ a2 then return ((a1,a1),(a1,a1)) else mzero
```

For example, the sequence:

```
pureD qFT >>= meas >>= trL
```

first performs a measurement on the pure density matrix representing the vector qFT. This measurement produces a vector with two components: the first is the resulting collapsed quantum state and the second is the classical observed value. The last operation forgets about the collapsed quantum state and returns the result of the classical measurement. As explained earlier the resulting density matrix is:

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

5 Superoperators as Arrows

By moving to density matrices and superoperators, it becomes possible to express both the original computations as well as measurements in the same formalism. One might hope that the original monadic structure of quantum computations is preserved, but it appears that this is not the case. The best we can do is to prove that the new model of computation fits within a generalization of monads called *arrows*.

5.1 Arrows

The application of a superoperator to a density matrix can still be achieved with the monadic bind operation, instantiated to the following type:

```
>>= :: Dens a → ((a,a) → Dens b) → Dens b
```

This type does not however correspond to the required type as computations now *consume multiple input values*. This observation is reminiscent of Hughes's motivation for generalizing monads to *arrows* [7]. Indeed, in addition to defining a notion of procedure which may perform computational effects, arrows may have a static component independent of the input, or may accept more than one input.

In Haskell, the arrow interface is defined using the following class declaration:

```
class Arrow a where
  arr ::  (b → c) → a b c
  (>>>)  ::  a b c → a c d → a b d
  first  ::  a b c → a (b,d) (c,d)
```

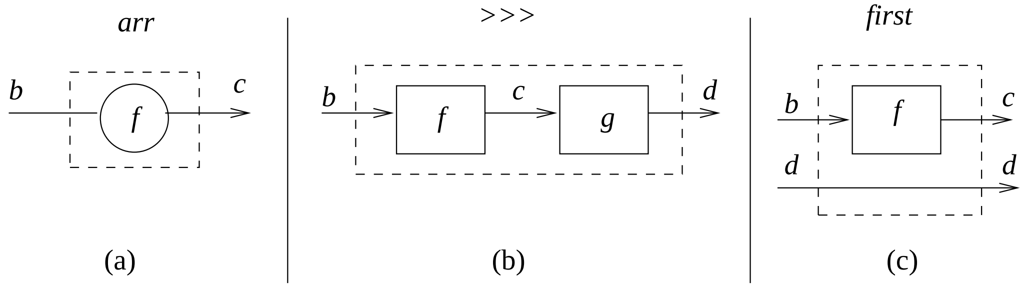
In other words, to be an arrow, a type a must support the three operations arr, $\ggg$, and first with the given types. The operations must satisfy the following equations:

$$\begin{array}{rcl}
arr\ id \ggg f & = & f \\
f \ggg arr\ id & = & f \\
(f \ggg g) \ggg h & = & f \ggg (g \ggg h) \\
arr\ (g\ .\ f) & = & arr\ f \ggg arr\ g \\
\mathit{first}\ (arr\ f) & = & arr\ (f \times id) \\
\mathit{first}\ (f \ggg g) & = & \mathit{first}\ f \ggg \mathit{first}\ g \\
\mathit{first}\ f \ggg arr\ (id \times g) & = & arr\ (id \times g) \ggg \mathit{first}\ f \\
\mathit{first}\ f \ggg arr\ fst & = & arr\ fst \ggg f \\
\mathit{first}\ (\mathit{first}\ f) \ggg arr\ assoc & = & arr\ assoc \ggg \mathit{first}\ f
\end{array}$$

where the functions × and $assoc$ are defined as follows:

$$(f \times g)\ (a,b) = (f\ a, g\ b)$$
$$assoc\ ((a,b),c) = (a,(b,c))$$

Graphically the functions associated with the arrow type are the following:



The function *arr* allows us to introduce "pure" arrows which are simple functions from their inputs to their outputs. The function $\ggg$ is similar to $\gg\!=$: it composes two computations. The function *first* is the critical one for our purposes: it allows us to apply an arrow to a component of the global quantum state. The equations above ensure that these operations are always well-defined even with arbitrary permutations and change of associativity.

5.2 Superoperators are Arrows (with Eq constraint)

Just as the probability effect associated with vectors is not strictly a monad because of the *Basis* constraint, the type *Super* is not strictly an arrow as the following types include the additional constraint requiring the elements to be comparable:

```
arr :: (Basis b, Basis c) => (b → c) → Super b c
arr f = fun2lin (λ (b1,b2) → (f b1, f b2))

(>>>) :: (Basis b, Basis c, Basis d) =>
               Super b c → Super c d → Super b d
(>>>) = o

first :: (Basis b, Basis c, Basis d) => Super b c → Super (b,d) (c,d)
first f ((b1,d1),(b2,d2)) = permute ((f (b1,b2)) <*> (return (d1,d2)))
   where permute v ((b1,b2),(d1,d2)) = v ((b1,d1),(b2,d2))
```

The function *arr* constructs a superoperator from a pure function by applying the function to both the vector and its dual. The composition of arrows is simply the composition of linear operators. The function *first* applies the superoperator f to the first component (and its dual) and leaves the second component unchanged. The definition calculates each part separately and then permutes the results to match the required type.

Proposition 5.1 *Superoperators satisfy the required equations for arrows.*

Proof. See Appendix C. □

The proposition implies that we can use the arrow combinators to structure our computations. For instance, the first few steps of the Toffoli circuit of Section 2.3 would now look like:

```
toffoli :: Super (Bool,Bool,Bool) (Bool,Bool,Bool)
toffoli =
  let hadS = lin2super hadamard
      cphaseS = lin2super (controlled phase)
      cnotS = lin2super (controlled qnot)
  in arr (λ (a0, b0, c0) → (c0, (a0, b0))) >>>
     (first hadS  >>> arr (λ (c1, (a0, b0)) → ((b0, c1), a0))) >>>
     (first cphaseS >>> arr (λ ((b1, c2), a0) → ((a0, b1), c2))) >>>
     (first cnotS >>> arr (λ ((a1, b2), c2) → ((b2, c2), a1))) >>> ...
```

Clearly this notation is awkward as it forces us to explicitly manipulate the entire state and to manually permute the values. However, all the tedious code can be generated automatically as we explain next.

5.3 A Better Notation for Arrows

Following the Haskell's monadic **do**-notation, Paterson (2001) presented an extension to Haskell with an improved syntax for writing computations using arrows. We concentrate only on the explanation of new forms which we use in our examples. Here is a simple example to illustrate the notation:

```
e1 :: Super (Bool,a) (Bool,a)
e1 = proc (a,b) → do
          r ← lin2super hadamard ≺ a
          returnA ≺ (r,b)
```

The **do**-notation simply sequences the actions in its body. The function *returnA* is the equivalent for arrows of the monadic function *return*. The two additional keywords are:

- the *arrow abstraction* **proc** which constructs an arrow instead of a regular function.
- the *arrow application* ≺ which feeds the value of an expression into an arrow.

Paterson (2001) shows that the above notation is general enough to express arrow computations and implemented a preprocessor which translates the new syntax to regular Haskell. In the case of `e1` above, the translation to Haskell produces the following code:

```
e2 :: Super (Bool,a) (Bool,a)
e2 = first (lin2super hadamard)
```

As the example shows, the output of the preprocessor is quite optimized.

5.4 Superoperators are (probably) not monads

Arrows are more general than monads. In particular, they include notions of computation that consume multiple inputs as well as computations with static components, independent of the input. Due to this general aspect of arrows, there are some subclasses of them which turns out to be equivalent to monads. More precisely, arrow types which support the following *app* function are just as expressive as monads.

```
class Arrow => ArrowApply a where
  app :: a (a b c, b) c
```

In other words, for superoperators to be monads, we would have to define a superoperator of type:

```
Super (Super b c, b) c
```

which in our case would require *Super b c* to be an instance of *Basis*. Unfortunately there is no straightforward way to view the space of superoperators as a finite set of observables.

6 Examples Revisited: Toffoli and Teleportation

Using arrows and the notation introduced by Patterson, we can express both of our examples elegantly.

6.1 Toffoli

The code mirrors the structure of the circuit and the structure of the monadic computation expressed earlier:

```
toffoli :: Super (Bool,Bool,Bool) (Bool,Bool,Bool)
toffoli = let hadS = lin2super hadamard
              cnotS = lin2super (controlled qnot)
              cphaseS = lin2super (controlled phase)
              caphaseS = lin2super (controlled (adjoint phase))
          in proc (a0,b0,c0) → do
             c1 ← hadS ≺ c0
             (b1,c2) ← cphaseS ≺ (b0,c1)
             (a1,b2) ← cnotS ≺ (a0,b1)
             (b3,c3) ← caphaseS ≺ (b2,c2)
             (a2,b4) ← cnotS ≺ (a1,b3)
             (a3,c4) ← cphaseS ≺ (a2,c3)
             c5 ← hadS ≺ c4
             returnA ≺ (a3,b4,c5)
```

6.2 Teleportation

We use the machinery we have developed to faithfully express the circuit presented in Section 3.1. We break the algorithm in two individual procedures, *alice* and *bob*. Besides the use of the arrows notation to express the action of superoperators on specific qubits, we incorporate the measurement in Alice's procedure, and trace out the irrelevant qubits from the answer returned by Bob.

```
alice :: Super (Bool,Bool) (Bool,Bool)
alice = proc (eprL,q) → do
             (q1,e1) ← (lin2super (controlled qnot)) ≺ (q,eprL)
             q2 ← (lin2super hadamard) ≺ q1
             ((q3,e2),(m1,m2)) ← meas ≺ (q2,e1)
             (m1',m2') ← trL ((q3,e2),(m1,m2))
             returnA ≺ (m1',m2')

bob :: Super (Bool,Bool,Bool) Bool
bob = proc (eprR,m1,m2) → do
           (m2',e1) ← (lin2super (controlled qnot)) ≺ (m2,eprR)
           (m1',e2) ← (lin2super (controlled z)) ≺ (m1,e1)
           q' ← trL ≺ ((m1',m2'),e2)
           returnA ≺ q'

teleport :: Super (Bool,Bool,Bool) Bool
teleport = proc (eprL,eprR,q) → do
                (m1,m2) ← alice ≺ (eprL,q)
                q' ← bob ≺ (eprR,m1,m2)
                returnA ≺ q'
```

7 Linear Typing: QML

The category of superoperators is considered to be an adequate model of non-reversible quantum computation [12]. Our construction presented so far seems to suggest that this category corresponds to a functional language with arrows, and so that we can accurately express quantum computation in such a framework. But as we explain below, this is not quite the whole story.

First consider the well-known "non-cloning" property of quantum states [8]. The arrow notation allows us to reuse variables more than once, and we are free to define the following operator:

```
copy :: Super Bool (Bool, Bool)
copy = arr (λ x → (x,x))
```

But can this superoperator be used to clone a qubit? The answer, as explained in Section 1.3.5 of the classic book on quantum computing [8], is no. The superoperator *copy* can be used to copy classical information encoded in quantum data, but when applied to an arbitrary quantum state, for example like qFT, the superoperator does not make two copies of the state qFT but rather it produces the *epr* state which is the correct and desired behavior. Thus, in this aspect the semantics of arrows is coherent with quantum computation, *i.e.*, the use of variables more than once models sharing, not cloning.

In contrast, in our model there is nothing to prevent the definition of:

```
weaken :: Super (Bool,Bool) Bool
weaken = arr (λ (x,y) → y)
```

This operator is however not physically realizable. Applying *weaken* to *epr* gives qFT. Physically forgetting about x corresponds to a measurement: if we measure the left qubit of *epr* we should get *qFalse* or *qTrue* or the mixed state of both measurements, but never qFT.

Therefore, our use of Haskell as a vehicle for expressing the ideas finally hits a major obstacle: arrow computations must be required to use every value that is introduced. Instead of attempting to continue working within Haskell, a better approach might be to now consider a functional quantum language like QML whose type system is designed to explicitly control weakening and decoherence, and to express the separation of values and arrow computations in that framework.

In more detail, QML [2] is a functional quantum programming language which addresses this problem by using a type system based on strict linear logic: contraction is permitted and modelled by *copy* while weakening has to be explicit and is translated by a partial trace. QML also features to case operators: a classical case operator which measures a qbit and returns the appropriate branch and a quantum case operator which avoids measurement but requires that the branches return results in orthogonal subspaces.

QML programs can be compiled to quantum circuits, using the category of finite quantum computation FQC — Grattage's QML compiler [6] is based on this semantics. An irreversible computation can be modelled by a reversible circuit, allowing additional heap qubits, which are initialized to a predefined values at the beginning of the computation and disposing, *i.e.* measuring, qbits at the end of the computation. To any FQC morphism we can assign a superoperator and indeed every superoperator can be represented this way.

Alternatively, we can interpret QML programs directly as superoperators, giving rise to a constructive denotational semantics exploiting the library of arrow combinators developed here. We hope to exploit this semantics to further analyze QML and to develop high level reasoning principles for QML programs.

8 Conclusion

We have argued that a realistic model for quantum computations should accommodate both unitary operations and measurements, and we have shown that such *general* quantum computations can be modeled using arrows. This is an extension of the previous-known observation that one can model pure quantum probabilities using monads. Establishing such connections between quantum computations and monads and arrows enables elegant embeddings in current classical languages, and exposes connections to well-understood concepts from the semantics of (classical) programming languages. We have demonstrated the use of arrows to model elegantly two examples in Haskell, including the teleportation experiment which interleaves measurements with unitary operations.

Acknowledgments

We would like to thank Antônio Carlos da Rocha Costa and Jonathan Grattage for extensive discussions and feedback.

A A Haskell Primer

We use Haskell as a precise mathematical (and executable) notation.

It is useful to think of a Haskell type as representing a mathematical set. Haskell includes several built-in types that we use: the type *Boolean* whose only two elements are *False* and *True*; the type *Complex Double* whose elements are complex numbers written $a{:}{+}b$ where both a and b are elements of the type *Double* which approximates the real numbers. Given two types a and b, the type (a, b) is the type of ordered pairs whose elements are of the respective types; the type $a \to b$ is the type of functions mapping elements of a to elements of b; and the type $[a]$ is the type of sequences (lists) whose elements are of type a. For convenience, we often use the keyword **type** to introduce a new type abbreviation. For example:

```
type PA = Complex Double
```

introduces the new type *PA* as an abbreviation of the more verbose *Complex Double*. A family of types that supports related operations can be grouped in a Haskell **class**. Individual types can then be made an **instance** of the class, and arbitrary code can require that a certain type be a member of a given class.

The syntax of Haskell expressions is usually self-explanatory except perhaps for the following points. A function can be written in at least two ways. Both the following definitions define a function which squares its argument:

```
sq n = n * n
sq' = λ n → n * n
```

A function f can be applied to every element of a list using *map* or using *list comprehensions*. If *xs* is the list $[1, 2, 3, 4]$, then both the following:

```
map sq xs
[ sq x | x ← xs ]
```

evaluate to $[1, 4, 9, 16]$.

Usually, a function f is applied to an argument a, by writing $f\ a$. If the function expects two arguments, it can either be applied to both at once $f\ (a, b)$ or one at a time $f\ a\ b$ depending on its type. When convenient the function symbol can be placed between the arguments using back quotes a ‘f‘ b.

B Proof of Monad Laws for Vectors.

Proof of Proposition 2.1: The definitions of *return* and $\gg=$ satisfy the three monad laws:

- First monad law: $(\mathit{return}\ x) \gg= f\ = f\ x$

$$\begin{aligned}
(\mathit{return}\ x) \gg= f\ &= \lambda\, b\,.\, \mathit{sum}\, [\, \mathit{return}\ x\ a\ *\ f\ a\ b \mid a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, b\,.\, \mathit{sum}\, [\, \mathit{if}\ x\ ==\ a\ \mathit{then}\ 1\ \mathit{else}\ 0\ *\ f\ a\ b \mid a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, b\,.\, f\ x\ b \\
&= f\ x
\end{aligned}$$

- Second monad law: $m \gg= \mathit{return}\ =\ m$

$$\begin{aligned}
m \gg= \mathit{return}\ &= \lambda\, b\,.\, \mathit{sum}\, [\, m\ a\ *\ \mathit{return}\ a\ b \mid a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, b\,.\, \mathit{sum}\, [\, m\ a\ *\ \mathit{if}\ a\ ==\ b\ \mathit{then}\ 1\ \mathit{else}\ 0 \mid a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, b\,.\, m\ b \\
&= m
\end{aligned}$$

- Third monad law: $(m \gg= f) \gg= g\ =\ m \gg= (\lambda\, x\,.\, f\ x \gg= g)$

$$\begin{aligned}
(m \gg= f) \gg= g\ &= (\lambda\, b\,.\, \mathit{sum}\, [m\ a\ *\ f\ a\ b \mid a\ \leftarrow\ \mathit{basis}]) \gg= g \\
&= \lambda\, c\,.\, \mathit{sum}[(\mathit{sum}\, [m\ a\ *\ f\ a\ b \mid a\ \leftarrow\ \mathit{basis}])\ *\ g\ b\ c\ \mid \\
&\qquad b\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, c\,.\, \mathit{sum}\, [m\ a\ *\ f\ a\ b\ *\ g\ b\ c \mid a\ \leftarrow\ \mathit{basis},\ b\ \leftarrow\ \mathit{basis}] \\
m \gg= (\lambda\, x\,.\, f\ x \gg= g) &= \lambda\, c\,.\, \mathit{sum}[m\ a\ *\ (f\ a \gg= g)\ c \mid a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, c\,. \mathit{sum}[m\ a\ *\ (\mathit{sum}[f\ a\ b\ *\ g\ b\ c \mid b\ \leftarrow\ \mathit{basis}]) \mid \\
&\qquad a\ \leftarrow\ \mathit{basis}] \\
&= \lambda\, c\,. \mathit{sum}\, [m\ a\ *\ f\ a\ b\ *\ g\ b\ c \mid a\ \leftarrow\ \mathit{basis},\ b\ \leftarrow\ \mathit{basis}]
\end{aligned}$$

C Proof of Arrow Laws for Superoperators

Proof of Proposition 5.1:

- First arrow equation: $\mathit{arr}\ \mathit{id} \ggg f\ =\ f.$

$$\begin{aligned}
\mathit{arr}\ \mathit{id} \ggg f\ &= \mathit{fun2lin}\ (\lambda\, (a1, a2).(\mathit{id}\ a1,\ \mathit{id}\ a2))\ \text{‘}o\text{‘}\ f && (\mathit{by\ arr\ and} \ggg) \\
&= \mathit{fun2lin}\ \mathit{id}\ \text{‘}o\text{‘}\ f && (\mathit{by\ simplification}) \\
&= \mathit{return}\ \text{‘}o\text{‘}\ f && (\mathit{by\ fun2lin}) \\
&= \lambda\, a\,.\, \mathit{return}\ a \gg= f && (\mathit{by}\ \text{‘}o\text{‘}) \\
&= \lambda\, a\,.\, f\ a && (\mathit{by\ monad\ law}\ 1.) \\
&= f
\end{aligned}$$

- Second arrow equation: $f \ggg \mathit{arr}\ \mathit{id}\ =\ f.$

$$\begin{aligned}
f \ggg \mathit{arr}\ \mathit{id}\ &= f\ \text{‘}o\text{‘}\ \mathit{fun2lin}\ (\lambda\, (b1, b2)\,.\,(\mathit{id}\ b1,\ \mathit{id}\ b2)) && (\mathit{by\ arr\ and} \ggg) \\
&= f\ \text{‘}o\text{‘}\ \mathit{fun2lin}\ \mathit{id} && (\mathit{by\ simplification}) \\
&= f\ \text{‘}o\text{‘}\ \mathit{return} && (\mathit{by\ fun2lin}) \\
&= \lambda\, a\,.\, f\ a \gg= \mathit{return} && (\mathit{by}\ o) \\
&= \lambda\, a\,.\, f\ a && (\mathit{by\ monad\ law}\ 2.) \\
&= f
\end{aligned}$$

- Third arrow equation: $(f \ggg g) \ggg h = f \ggg (g \ggg h)$.

$$\begin{aligned}(f \ggg g) \ggg h &= (f\ \lq o\lq\ g)\ \lq o\lq\ h && (\mathit{by}\ \ggg)\\ &= \lambda\, b\,.\,(\lambda\, a\,.\,f\ a \gg= g)\ b \gg= h && (\mathit{by}\ o)\\ &= \lambda\, b\,.\,(f\ b \gg= g) \gg= h && (\mathit{by}\ \beta)\end{aligned}$$

$$\begin{aligned}f \ggg (g \ggg h\,) &= f\ \lq o\lq\ (g\ \lq o\lq\ h) && (\mathit{by}\ \gg=)\\ &= \lambda\, a\,.\,f\ a \gg= (\lambda\, b\,.\,g\ b \gg= h) && (\mathit{by}\ o)\\ &= \lambda\, a\,.\,(f\ a \gg= g) \gg= h && (\mathit{by\ monad\ law}\ 3.)\end{aligned}$$

- Fourth arrow equation: $\mathit{arr}\,(g\,.\,f) = \mathit{arr}\,f \ggg \mathit{arr}\,g$.

$$\begin{aligned}\mathit{arr}\,(g\,.\,f) &= \mathit{fun2lin}\,(\lambda\,(b1,b2)\,.((g\,.\,f)\ b1,\ (g\,.\,f)\ b2)) && (\mathit{by\ arr})\\ &= \mathit{return}\,.(\lambda\,(b1,b2)\,.\,((g\,.\,f)\ b1,\ (g\,.\,f)\ b2)) && (\mathit{by\ fun2lin})\\ &= \lambda\,(b1,b2)\,.\,\mathit{return}\,((g\,.\,f)\ b1,\ (g\,.\,f)\ b2) && (\mathit{simplification})\end{aligned}$$

$$\begin{aligned}\mathit{arr}\,f \ggg \mathit{arr}\,g &= \mathit{fun2lin}\,(\lambda\,(b1,b2)\,.\,(f\ b1,\ f\ b2))\ \lq o\lq\ \mathit{fun2lin}(\lambda\,(b1,b2)\,.\,(g\ b1,\ g\ b2))\\ &\quad (\mathit{by} \gg= \mathit{and\ arr})\\ &= \mathit{return}\,.\,(\lambda\,(b1,b2)\,.\,(f\ b1,\ f\ b2))\ \lq o\lq\ \mathit{return}\,.(\lambda\,(b1,b2)\,.\,(g\ b1,\ g\ b2))\\ &\quad (\mathit{by\ fun2lin})\\ &= \lambda\,(b1,b2)\,.\,\mathit{return}\,(f\ b1,\ f\ b2) \gg= \lambda\,(b1,b2)\,.\,\mathit{return}\,(g\ b1,\ g\ b2))\\ &\quad (\mathit{by}\ o)\\ &= \lambda\,(b1,b2)\,.\,(\lambda\,(b1,b2)\,.\,\mathit{return}\,(g\ b1,\ g\ b2))\ (f\ b1,\ f\ b2)\\ &\quad (\mathit{by\ monad\ law}\ 1.)\\ &= \lambda\,(b1,b2)\,.\,\mathit{return}\,((g\,.\,f)\ b1,\ (g\,.\,f)\ b2) \quad (\mathit{by}\ \beta)\end{aligned}$$

- Fifth arrow equation: $\mathit{first}\,(\mathit{arr}\,f) = \mathit{arr}\,(f \times \mathit{id})$.

$$\begin{aligned}\mathit{first}\,(\mathit{arr}\,f) &= \mathit{first}\,(\mathit{fun2lin}\,(\lambda\,(b1,b2)\,.\,(f\ b1,\ f\ b2))) \quad (\mathit{by\ arr})\\ &= \mathit{first}\,(\mathit{return}\,.\,(\lambda\,(b1,b2)\,.\,(f\ b1,\ f\ b2))) \quad (\mathit{by\ fun2lin})\\ &= \mathit{first}\,(\lambda\,(b1,b2)\,.\,\mathit{return}\,(f\ b1,\ f\ b2)) \quad (\mathit{by\ simplification})\\ &= \lambda\,((b1,d1),(b2,d2))\,.\,\lambda\,((x,y),(w,z))\,.\mathit{return}\,(f\ b1,\ f\ b2)\,(x,w) \ast\\ &\quad \mathit{return}\,(d1,d2)\,(y,z)\ \ (\mathit{by\ first})\\ &= \lambda\,((b1,d1),(b2,d2))\,.\,\lambda\,((x,y),(w,z))\,.\\ &\quad \mathbf{if}\ ((f\ b1, f\ b2),\ (d1,\ d2)) == ((x,w),(y,z))\ \mathbf{then}\ 1\ \mathbf{else}\ 0 \quad (\mathit{by\ return})\end{aligned}$$

$$\begin{aligned}\mathit{arr}\,(f \times \mathit{id}) = &= \mathit{fun2lin}\,(\lambda\,((b1,d1),(b2,d2)).\,((f\ b1,\ d1),(f\ b2,\ d2))) && (\mathit{by\ arr})\\ &= \mathit{return}\,.\,(\lambda\,((b1,d1),(b2,d2)).\,((f\ b1,\ d1),(f\ b2,\ d2))) && (\mathit{by\ fun2lin})\\ &= \lambda\,((b1,d1),(b2,d2))\,.\,\mathit{return}\,((f\ b1,\ d1),(f\ b2,\ d2))\\ &= \lambda\,((b1,d1),(b2,d2))\,.\,\lambda\,((x,y),(w,z))\,.\\ &\quad \mathbf{if}\ ((f\ b1,d1),\ (f\ b2,d2)) == ((x,y),(w,z))\ \mathbf{then}\ 1\ \mathbf{else}\ 0 && (\mathit{by\ return})\end{aligned}$$

- Sixth arrow equation: $\mathit{first}\,(f \ggg g) = \mathit{first}\,f \ggg \mathit{first}\,g$. In the following proofs assume: $ad1\,((b1,d1),(b2,d2)) = (b1,b2)$ and $ad2\,((b1,d1),(b2,d2)) = (d1,d2)$.

$$\begin{aligned}\mathit{first}\,(f\ \lq o\lq\ g) &= \mathit{first}\,(\lambda\, a\,.\,f\ a \gg= g)\\ &\quad (\mathit{by}\ \lq o\lq)\\ &= \lambda\, b\,.\,\lambda\,((x,y),(w,z))\,.\,(f\ (ad1\ b) \gg= g)\,(x,w) \ast \mathit{return}\,(ad2\ b)\,(y,z)\\ &\quad (\mathit{by\ first})\\ &= \lambda\, b\,.\,\lambda\,((x,y),(w,z))\,.\,(\lambda\, c\,.\,\mathit{sum}\,[(f\ (ad1\ b))\ a \ast g\ a\ c \mid a \leftarrow \mathit{basis}])\,(x,w)\\ &\quad \ast\ \mathit{return}\,(ad2\ b)\,(y,z) \quad (\mathit{by} \gg=)\\ &= \lambda\, b\,.\,\lambda\,((x,y),(w,z))\,.\,\mathit{sum}[(f\ (ad1\ b))\ a \ast g\ a\,(x,w) \mid a \leftarrow \mathit{basis}] \ast\\ &\quad \mathit{return}\,(ad2\ b)\,(y,z) \quad (\mathit{by}\ \beta)\end{aligned}$$

$$\begin{aligned}
\mathit{first}\ f\ \text{‘}o\text{‘}\ \mathit{first}\ g\ &=\ \lambda\, a\, .\, \mathit{first}\ f\ a\ \gg\!=\ \lambda\, b\, .\, \mathit{first}\ g\ b\\
&\quad (\mathit{by}\ \text{‘}o\text{‘})\\
&=\ \lambda\, a\, .\, \lambda\, ((x,y),(w,z))\, .\, f\ (\mathit{ad1}\ a)\ (x,w)\ *\ \mathit{return}\ (\mathit{ad2}\ a)\ (y,z)\ \gg\!=\\
&\quad \lambda\, b\, .\, \lambda\, ((x,y),(w,z))\, .\, g\ (\mathit{ad1}\ b)\ (x,w)\ *\ \mathit{return}\ (\mathit{ad2}\ b)\ (y,z)\\
&\quad (\mathit{by}\ \mathit{first})\\
&=\ \lambda\, a\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (\mathit{ad1}\ a)\ (m,o)\ *\ \mathit{return}\ (\mathit{ad2}\ a)\ (n,p)\, *\\
&\quad (\lambda\, ((x,y),(w,z))\, .\, g\ (m,o)\ (x,w)\ *\ \mathit{return}\ (n,p)\ (y,z))((x,y),(w,z))\ |\\
&\quad ((m,n),(o,p)) \leftarrow\ \mathit{basis}] \quad (\mathit{by}\ \gg\!=)\\
&=\ \lambda\, a\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (\mathit{ad1}\ a)\ (m,o)\ *\ \mathit{return}\ (\mathit{ad2}\ a)\ (n,p)\, *\\
&\quad g\ (m,o)\ (x,w)\ *\ \mathit{return}\ (n,p)\ (y,z)\ |((m,n),(o,p)) \leftarrow\ \mathit{basis}]\\
&=\ \lambda\, a\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (\mathit{ad1}\ a)\ a1\ *\ g\ a1\ (x,w)\, *\\
&\quad \mathit{return}\ (\mathit{ad2}\ a)\ a2\ *\ \mathit{return}\ a2\ (y,z)\ |\ a1\ \leftarrow\ \mathit{basis}\ ,\ a2\ \leftarrow\ \mathit{basis}]\\
&\quad (\mathit{by}\ \mathit{simplification})\\
&=\ \lambda\, a\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (\mathit{ad1}\ a)\ a1\ *\ g\ a1\ (x,w)\ |\ a1\ \leftarrow\ \mathit{basis}\ ]\\
&\quad *\ \mathit{return}\ (\mathit{ad2}\ a)\ (y,z) \quad (\mathit{by}\ \mathit{simplification})
\end{aligned}$$

- Seventh arrow equation: $\mathit{first}\, f\ \ggg\ \mathit{arr}\ (\mathit{id}\ \times\ g)\ =\ \mathit{arr}\ (\mathit{id}\ \times\ g)\ \ggg\ \mathit{first}\, f$.

$$lhs = first\ f\ \text{‘}o\text{‘}\ arr\ (id \times g)$$

$$\begin{aligned}
\mathit{lhs} =\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \mathit{first}\, f\ ((a1,b1),(a2,b2))\ \gg\!=\\
&\quad \mathit{fun2lin}\ (\lambda\, ((a,b),(c,d))\, .\, ((a,\ g\ b),(c,\ g\ d)))\quad (\mathit{by}\ \text{‘}o\text{‘}\ \mathit{and}\ \mathit{arr})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \mathit{first}\, f\ ((a1,b1),(a2,b2))\ \gg\!=\\
&\quad \lambda\, ((a,b),(c,d))\, .\, \mathit{return}\ ((a,\ g\ b),(c,\ g\ d))\quad (\mathit{by}\ \mathit{fun2lin})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \lambda\, ((x,y),(w,z))\, .\, f\ (a1,a2)\ (x,w)\ *\ \mathit{return}\ (b1,b2)\ (y,z)\ \gg\!=\\
&\quad \lambda\, ((a,b),(c,d))\, .\, \mathit{return}\ ((a,\ g\ b),(c,\ g\ d))\qquad (\mathit{by}\ \mathit{first})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \lambda\, c\, .\, \mathit{sum}\ [\, f\ (a1,a2)\ (m,o)\ *\ \mathit{return}\ (b1,b2)\ (n,p)\, *\\
&\quad \mathit{return}\ ((m,\ g\ n),(o,\ g\ p))\ c\ |\ ((m,n),(o,p))\ \leftarrow\ \mathit{basis}]\quad (\mathit{by}\ \gg\!=)\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (a1,a2)\ (m,o)\ *\ \mathit{return}\ (b1,b2)\ (n,p)\, *\\
&\quad \mathit{return}\ ((m,\ g\ n),(o,\ g\ p))\ ((x,y),(w,z))|\ ((m,n),(o,p))\ \leftarrow\ \mathit{basis}]\\
&\quad (\mathit{by}\ \mathit{simplification})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \lambda\, ((x,y),(w,z))\, .\, \mathit{sum}\ [\, f\ (a1,a2)\ (m,o)\, *\\
&\quad [\mathbf{if}\ (b1,b2)\ ==\ (n,p)\ \mathbf{then}\ 1\ \mathbf{else}\ 0]\, *\\
&\quad [(\mathbf{if}\ (m,\ g\ n),(o,\ g\ p))\ ==\ ((x,y),(w,z))\ \mathbf{then}\ 1\ \mathbf{else}\ 0]\ |\ ((m,n),(o,p))\ \leftarrow\ \mathit{basis}]\\
&\quad (\mathit{by}\ \mathit{return})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\ .\lambda\, ((x,y),(w,z))\, .\, \mathbf{if}\ (g\ b1,\ g\ b2)\ ==\ (y,z)\\
&\quad \mathbf{then}\ \ f\ (a1,a2)\ (x,w)\ \mathbf{else}\ 0
\end{aligned}$$

$$rhs = arr\ (id \times g)\ \text{‘}o\text{‘}\ first\ f$$

$$\begin{aligned}
\mathit{rhs}\ =\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \mathit{fun2lin}\ (\lambda\, ((a,b),(c,d))\, .\, ((a,\ g\ b),(c,\ g\ d)))\\
&\quad ((a1,b1),(a2,b2))\ \gg\!=\ \mathit{first}\, f\quad (\mathit{by}\ \text{‘}o\text{‘}\ \mathit{and}\ \mathit{arr})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \mathit{return}\ ((a1,\ g\ b1),(a2,\ g\ b2))\ \gg\!=\ \mathit{first}\, f\\
&\quad (\mathit{by}\ \mathit{fun2lin})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\, .\, \mathit{first}\, f\ ((a1,\ g\ b1),(a2,\ g\ b2))\quad (\mathit{by}\ \mathit{monad}\ \mathit{law}\ 1.)\\
=\ &\lambda\, ((a1,b1),(a2,b2))\ .\lambda\, ((x,y),(w,z))\, .\, f\ (a1,a2)\ (x,w)\ *\ \mathit{return}\ (g\ b1,\ g\ b2)\ (y,z)\\
&\quad (\mathit{by}\ \mathit{first})\\
=\ &\lambda\, ((a1,b1),(a2,b2))\ .\lambda\, ((x,y),(w,z))\, .\, f\ (a1,a2)\ (x,w)\, *\\
&\quad [\mathbf{if}\ (g\ b1,\ g\ b2)\ ==\ (y,z)\ \mathbf{then}\ 1\ \mathbf{else}\ 0]\quad (\mathit{by}\ \mathit{return})
\end{aligned}$$

- Eighth arrow equation: $\mathit{first}\,f \ggg \mathit{arr}\,\mathit{fst} \;=\; \mathit{arr}\,\mathit{fst} \ggg f$.

$$lhs = \ first\ f\ `o`\ arr(\lambda(a,b).a)$$

$$\begin{aligned}
\mathit{lhs} \;&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\mathit{first}\,f\;((a1,b1),(a2,b2)) \;\gg\!\!=\; \mathit{arr}\;\lambda\,(a,b)\;.\;a \;\; (\mathit{by}\ o)\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\mathit{first}\,f\;((a1,b1),(a2,b2)) \;\gg\!\!=\; \lambda\,((a,b),(c,d))\;.\;\mathit{return}\;(a,c)\\
&\quad (\mathit{by}\ \mathit{arr}\ )\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\lambda\,((x,y),(w,z))\;.\;f\;(a1,a2)\;(x,w)\,*\\
&\quad \mathit{return}\;(b1,b2)\;(y,z) \;\gg\!\!=\; \lambda\,((a,b),(c,d))\;.\;\mathit{return}\;(a,c) \quad (\mathit{by}\ \mathit{first}\ )\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\lambda\,(c1,c2)\;.\;\mathit{sum}\;[\,f\;(a1,a2)\;(m,o)\;*\;\mathit{return}\;(b1,b2)\;(n,p)*\\
&\quad \mathit{return}\;(m,o)\;(c1,c2)\mid((m,n),(o,p))\;\leftarrow\;\mathit{basis}] \quad (\mathit{by}\ \gg\!\!=)\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\lambda\,(c1,c2)\;.\;\mathit{sum}\;[\,f\;(a1,a2)\;(m,o)\,*\\
&\quad [\mathbf{if}\;(b1,b2)\;==\;(n,p)\;\mathbf{then}\;1\;\mathbf{else}\;0]\,*\\
&\quad [\mathbf{if}\;(m,o)\;==\;(c1,c2)\;\mathbf{then}\;1\;\mathbf{else}\;0]\mid((m,n),(o,p))\;\leftarrow\;\mathit{basis}] \quad (\mathit{by}\ \mathit{return})\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\lambda\,(c1,c2)\;.\;f\;(a1,a2)\;(c1,c2) \;\; (\mathit{by}\ \mathit{simplification})
\end{aligned}$$

$$rhs = arr\ fst\ `o`f$$

$$\begin{aligned}
\mathit{rhs} \;&=\; \lambda\,((a,b),(c,d))\;.\;\mathit{return}\;(a,c)\;`o`\;f \quad (\mathit{by}\ \mathit{arr})\\
&= \lambda\,((a1,b1),(a2,b2))\;.\;(\lambda\,((a,b),(c,d))\;.\;\mathit{return}\;(a,c))\;((a1,b1),(a2,b2)) \;\gg\!\!=\; f\\
&\quad (\mathit{by}\ o)\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;f\;(a1,a2) \quad (\mathit{by}\ \mathit{monad}\ \mathit{law}\ 1.)\\
&=\; \lambda\,((a1,b1),(a2,b2))\;.\;\lambda\,(c1,c2)\;.\;f\;(a1,a2)\;(c1,c2)
\end{aligned}$$

- Ninth arrow equation: $\mathit{first}\;(\mathit{first}\,f) \ggg \mathit{arr}\;\mathit{assoc} \;=\; \mathit{arr}\;\mathit{assoc} \ggg \mathit{first}\,f$

$$\begin{aligned}
lhs = \lambda(((a1,b1),c1),((a2,b2),c2)).first(firstf)(((a1,b1),c1),((a2,b2),c2)) \gg\!\!=\\
arr(\lambda((a,b),c).(a,(b,c)))
\end{aligned}$$

$$
\begin{aligned}
\mathit{lhs} \;=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\mathit{first}\;(\lambda\; b\;.\;\lambda\,((x, y), (w, z))\;.f\;(\mathit{ad1}\;b)\;(x, w) *\\
& \mathit{return}\;(\mathit{ad2}\;b)\;(y, z))\;(((a1, b1), c1), ((a2, b2),\ c2))\;\gg=\\
& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\mathit{return}\;((a1, (b1, c1)), (a2, (b2, c2)))\\
& (\mathit{by\ first})\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((m1, n1), p1)\;((m2, n2),\ p2)\;.\\
& (\lambda\; b\;.\;\lambda\,((x, y), (w, z))\;.\;f\;(\mathit{ad1}\;b)\;(x, w)\;*\;\mathit{return}\;(\mathit{ad2}\;b)\;(y, z))\;((a1, b1), (a2, b2))\\
& ((m1, n1), (m2, n2))\;*\;\mathit{return}\;(c1, c2)\;(p1, p2)\;\gg=\;\lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\\
& \mathit{return}\;((a1, (b1, c1)), (a2, (b2, c2)))\qquad(\mathit{by\ first})\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((m1, n1), p1)\;((m2, n2),\ p2)\;.\\
& f\;(a1, a2)\;(m1, m2)\;*\;\mathit{return}\;(b1, b2)\;(n1, n2)\;*\;\mathit{return}\;(c1, c2)\;(p1, p2)\;\gg=\\
& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\mathit{return}\;((a1, (b1, c1)), (a2, (b2, c2)))\\
& (\mathit{by}\ \beta)\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((x1, (y1, z1)), (x2, (y2, z2)))\;.\\
& \mathit{sum}\;[\,f\;(a1, a2)\;(m1, m2)\;*\;\mathit{return}\;(b1, b2)\;(n1, n2)\;*\;\mathit{return}\;(c1, c2)\;(p1, p2) *\\
& \mathit{return}\;((m1, n1), p1)\;((m2, n2),\ p2)\;((x1, (y1, z1)), (x2, (y2, z2)))\;|\\
& ((m1, n1), p1)\;((m2, n2),\ p2)\;\leftarrow\;\mathit{basis}]\\
& (\mathit{by}\;\gg=)\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((x1, (y1, z1)), (x2, (y2, z2)))\;.\\
& \mathit{sum}\;[\,f\;(a1, a2)\;(m1, m2)\;*[\mathbf{if}\;(b1, b2)\;==\;(n1, n2)\;\mathbf{then}\;1\;\mathbf{else}\;0] *\\
& [\mathbf{if}\;(c1, c2)\;==\;(p1, p2)\mathbf{then}\;1\;\mathbf{else}\;0] *\\
& [\mathbf{if}\;((m1, n1), p1)\;((m2, n2),\ p2)\;==\;((x1, (y1, z1)), (x2, (y2, z2)))\;\mathbf{then}\;1\;\mathbf{else}\;0]|\\
& ((m1, n1), p1)\;((m2, n2),\ p2)\;\leftarrow\;\mathit{basis}]\\
& (\mathit{by\ return})\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((x1, (y1, z1)), (x2, (y2, z2)))\;.\;f\;(a1, a2)\;(x1, x2) *\\
& \mathit{return}\;((b1, c1), (b2, c2))\;((y1, z1), (y2, z2))
\end{aligned}
$$

$$
rhs = \lambda(((a1, b1), c1), ((a2, b2), c2))\;.\;return((a1, (b1, c1)), (a2, (b2, c2)))\;`o`\;first\;f
$$

$$
\begin{aligned}
\mathit{rhs} \;=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\mathit{return}\;((a1, (b1, c1)), (a2, (b2, c2)))\;\gg=\;\mathit{first}\,f\\
& (\mathit{by}\ o)\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\mathit{first}\,f\;((a1, (b1, c1)), (a2, (b2, c2)))\\
& (\mathit{by\ monad\ law}\ 1.)\\
=\;& \lambda\,(((a1, b1), c1), ((a2, b2),\ c2))\;.\;\lambda\,((x1, (y1, z1)), (x2, (y2, z2)))\;.\\
& f\;(a1, a2)\;(x1, x2)\;*\mathit{return}\;((b1, c1), (b2, c2))\;((y1, z1), (y2, z2))\qquad(\mathit{by\ first})
\end{aligned}
$$

References

[1] Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 20–30. ACM Press, 1998.

[2] Thorsten Altenkirch and Jonathan Grattage. A functional quantum programming language. quant-ph/0409065, November 2004.

[3] Thorsten Altenkirch and Bernhard Reus. Monadic presentations of lambda terms using generalized inductive types. In *Computer Science Logic*, 1999.

[4] C Bennett, G Brassard, C Crepeau, R Jozsa, A Peres, and W Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys Rev Lett*, pages 1895–1899, 1993.

[5] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[6] Jonathan Grattage and Thorsten Altenkirch. A compiler for a functional quantum programming language. submitted for publication, January 2005.

[7] John Hughes. Generalising monads to arrows. *Science of Computer Programming*, 37:67–111, May 2000.

[8] Isaac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[9] E. Moggi. Computational lambda-calculus and monads. In *Proceedings of the Fourth Annual Symposium on Logic in computer science*, pages 14–23. IEEE Press, 1989.

[10] Bernhard Ömer. A procedural formalism for quantum computing. Master's thesis, Department of Theoretical Physics, Technical University of Vienna, 1998.

[11] Amr Sabry. Modeling quantum computing in Haskell. In *Proceedings of the ACM SIGPLAN workshop on Haskell*, pages 39–49. ACM Press, 2003.

[12] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[13] Benoit Valiron. Quantum typing. *CoRR*, cs.LO/0404056, 2004.

[14] André van Tonder. Quantum computation, categorical semantics and linear logic. *CoRR*, quant-ph/0312174, 2003.

[15] Andre van Tonder. A lambda calculus for quantum computation. *SIAM Journal on Computing*, 33(5):1109–1135, 2004.