

Towards a High Level Quantum Programming Language

Thorsten Altenkirch

University of Nottingham

based on joint work with Jonathan Grattage
and discussions with V.P. Belavkin

Background

Background

- Simulation of quantum systems is expensive:
PSPACE complexity for polynomial circuits.

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.
- Grover: Blind search in $O(\sqrt{n})$

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.
- Grover: Blind search in $O(\sqrt{n})$
- Can we build a quantum computer?

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.
- Grover: Blind search in $O(\sqrt{n})$
- Can we build a quantum computer?
yes We can run quantum algorithms.

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.
- Grover: Blind search in $O(\sqrt{n})$
- Can we build a quantum computer?

yes We can run quantum algorithms.

no Nature is classical after all!

Background

- Simulation of quantum systems is expensive: PSPACE complexity for polynomial circuits.
- Feynman: *Can we exploit this fact to perform computations more efficiently?*
- Shor: Factorisation in quantum polynomial time.
- Grover: Blind search in $O(\sqrt{n})$
- Can we build a quantum computer?

yes We can run quantum algorithms.

no Nature is classical after all!

Assumption: Nature is fair...

The quantum software crisis

The quantum software crisis

- Quantum algorithms are usually presented using the circuit model.

The quantum software crisis

- Quantum algorithms are usually presented using the circuit model.
- Nielsen and Chuang, p.7, *Coming up with good quantum algorithms is hard.*

The quantum software crisis

- Quantum algorithms are usually presented using the circuit model.
- Nielsen and Chuang, p.7, *Coming up with good quantum algorithms is hard.*
- Richard Josza, QPL 2004: *We need to develop quantum thinking!*



QML

QML

- QML: a functional language for quantum computations on finite types.

QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.

QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.
- Design guided by semantics

QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.
- Design guided by semantics
- Analogy with classical computation
 - FCC Finite classical computations
 - FQC Finite quantum computations


QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.
- Design guided by semantics
- Analogy with classical computation
 - FCC Finite classical computations
 - FQC Finite quantum computations
- Important issue: **control of decoherence**

QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.
- Design guided by semantics
- Analogy with classical computation
 - FCC Finite classical computations
 - FQC Finite quantum computations
- Important issue: **control of decoherence**
- Draft paper available
(Google:Thorsten,functional,quantum)

QML

- QML: a functional language for quantum computations on finite types.
- Quantum control **and** quantum data.
- Design guided by semantics
- Analogy with classical computation
 - FCC Finite classical computations
 - FQC Finite quantum computations
- Important issue: **control of decoherence**
- Draft paper available
(Google:Thorsten,functional,quantum)
-  Compiler under construction (Jonathan)

Example: Hadamard operation

Example: Hadamard operation

Matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Example: Hadamard operation

Matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

QML

had : $Q_2 \multimap Q_2$

had $x = \mathbf{if}^\circ x$

then { *qfalse* | (-1) *qtrue* }

else { *qfalse* | *qtrue* }

Overview

1. Semantics of finite classical and quantum computation
2. QML basics
3. Compiling QML
4. Conclusions and further work

1. Semantics

1. Semantics of finite classical and quantum computation
2. QML basics
3. Compiling QML
4. Conclusions and further work

Something we know well ...

Something we know well ...

- Start with classical computations on finite types.

Something we know well ...

- Start with classical computations on finite types.
- Quantum mechanics is time-reversible...

Something we know well ...

- Start with classical computations on finite types.
- Quantum mechanics is time-reversible...
- ... hence quantum computation is based on reversible operations.

Something we know well ...

- Start with classical computations on finite types.
- Quantum mechanics is time-reversible...
- ... hence quantum computation is based on reversible operations.
- **However:** Newtonian mechanics, Maxwellian electrodynamics are also time-reversible...

Something we know well ...

- Start with classical computations on finite types.
- Quantum mechanics is time-reversible...
- ... hence quantum computation is based on reversible operations.
- **However:** Newtonian mechanics, Maxwellian electrodynamics are also time-reversible...
- ... hence classical computation **should be** based on reversible operations.

Classical computation (FCC)

Classical computation (FCC)

Given finite sets A (input) and B (output):



Classical computation (FCC)

Given finite sets A (input) and B (output):



- a finite set of initial heaps H ,

Classical computation (FCC)

Given finite sets A (input) and B (output):



- a finite set of initial heaps H ,
- an initial heap $h \in H$,

Classical computation (FCC)

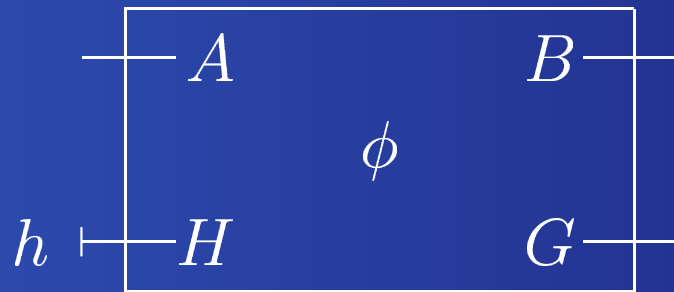
Given finite sets A (input) and B (output):



- a finite set of initial heaps H ,
- an initial heap $h \in H$,
- a finite set of garbage states G ,

Classical computation (FCC)

Given finite sets A (input) and B (output):



- a finite set of initial heaps H ,
- an initial heap $h \in H$,
- a finite set of garbage states G ,
- a bijection $\phi \in A \times H \simeq B \times G$,

Semantics

Semantics

- A classical computation $\alpha = (A, B, H, h \in H, G, \phi \in A \times H \simeq B \times G)$ induces a function $U\alpha \in A \rightarrow B$ by

$$U\alpha a = \pi_1 \phi (h, a)$$

Semantics

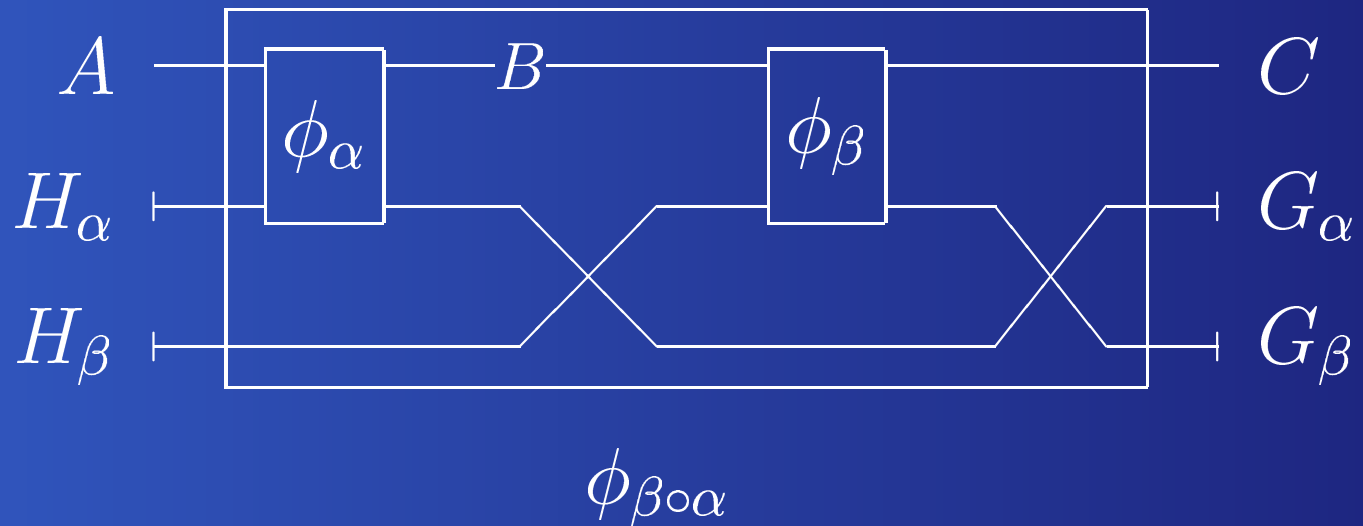
- A classical computation $\alpha = (A, B, H, h \in H, G, \phi \in A \times H \simeq B \times G)$ induces a function $\cup\alpha \in A \rightarrow B$ by

$$\cup\alpha a = \pi_1 \phi(h, a)$$

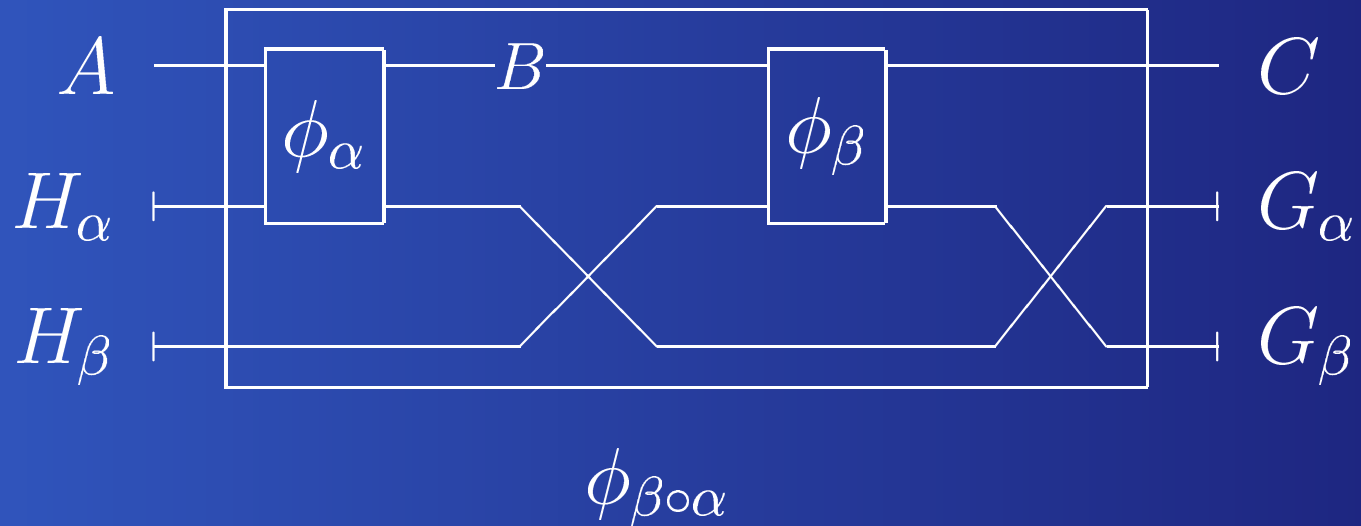
- **Theorem** Any function $f \in A \rightarrow B$ (on finite sets A, B) can be realized by a quantum computation.

Composing classical computations

Composing classical computations



Composing classical computations



Theorem:

$$\mathbf{U}(\beta \circ \alpha) = (\mathbf{U}\beta) \circ (\mathbf{U}\alpha)$$

Coming next: Quantum computations

Develop FQC analogously to FCC...

Linear algebra revision

Linear algebra revision

Given a finite set A (the base)
 $\mathbb{C}^A = \mathbb{C}^{|A|} \rightarrow \mathbb{C}^A$ is a **Hilbert space**.

Linear algebra revision

Given a finite set A (the base)

$\mathbb{C}A = A \rightarrow \mathbb{C}$ is a **Hilbert space**.

Linear operators:

$f \in A \rightarrow B \rightarrow \mathbb{C}$ induces $\hat{f} \in \mathbb{C}A \rightarrow \mathbb{C}B$.

we write $f \in A \multimap B$

Linear algebra revision

Given a finite set A (the base)

$\mathbb{C}A = A \rightarrow \mathbb{C}$ is a **Hilbert space**.

Linear operators:

$f \in A \rightarrow B \rightarrow \mathbb{C}$ induces $\hat{f} \in \mathbb{C}A \rightarrow \mathbb{C}B$.

we write $f \in A \multimap B$

Norm of a vector:

$$\|v\| = \sum_{a \in A} (va)^* (va) \in \mathbb{R}^+,$$

Linear algebra revision

Given a finite set A (the base)
 $\mathbb{C}A = A \rightarrow \mathbb{C}$ is a **Hilbert space**.

Linear operators:

$f \in A \rightarrow B \rightarrow \mathbb{C}$ induces $\hat{f} \in \mathbb{C}A \rightarrow \mathbb{C}B$.

we write $f \in A \multimap B$

Norm of a vector:

$$\|v\| = \sum_{a \in A} (va)^* (va) \in \mathbb{R}^+,$$

Unitary operators:

A unitary operator $\phi \in A \multimap_{\text{unitary}} B$ is a linear isomorphism that preserves the norm.

Basics of quantum computation

Basics of quantum computation

- A **pure state** over A is a vector $v \in \mathbb{C}A$ with unit norm $\|v\| = 1$.

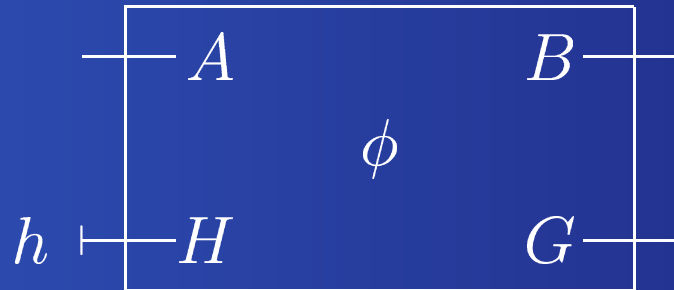
Basics of quantum computation

- A **pure state** over A is a vector $v \in \mathbb{C}A$ with unit norm $\|v\| = 1$.
- A **reversible computation** is given by a unitary operator $\phi \in A \multimap_{\text{unitary}} B$.

Quantum computations (FQC)

Quantum computations (FQC)

Given finite sets A (input) and B (output):



Quantum computations (FQC)

Given finite sets A (input) and B (output):



- a finite set H , the base of the space of initial heaps,

Quantum computations (FQC)

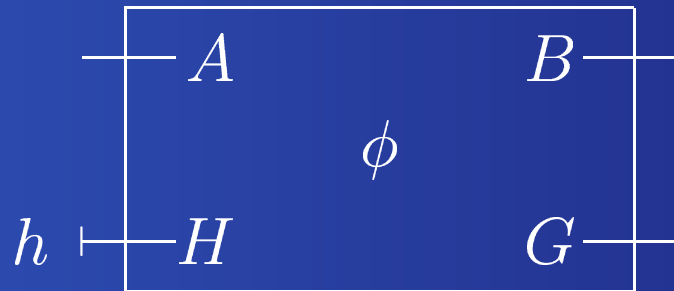
Given finite sets A (input) and B (output):



- a finite set H , the base of the space of initial heaps,
- a heap initialisation vector $h \in \mathbb{C}H$,

Quantum computations (FQC)

Given finite sets A (input) and B (output):



- a finite set H , the base of the space of initial heaps,
- a heap initialisation vector $h \in \mathbb{C}H$,
- a finite set G , the base of the space of garbage states,

Quantum computations (FQC)

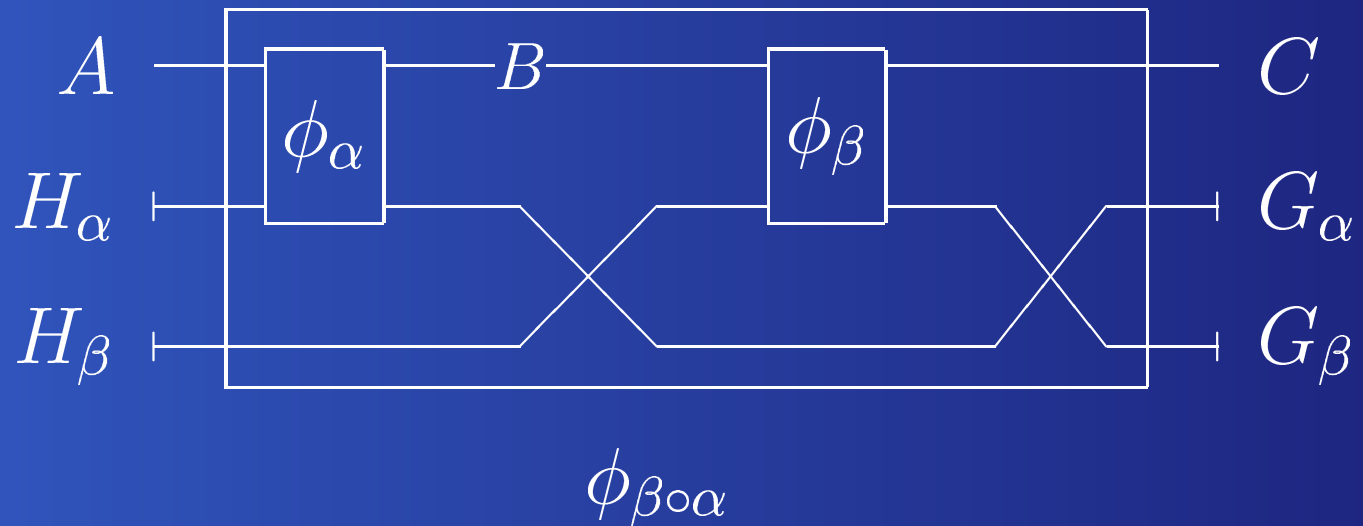
Given finite sets A (input) and B (output):



- a finite set H , the base of the space of initial heaps,
- a heap initialisation vector $h \in \mathbb{C}H$,
- a finite set G , the base of the space of garbage states,
- a unitary operator $\phi \in A \otimes H \xrightarrow{\text{unitary}} B \otimes G$.

Composing quantum computations

Composing quantum computations



Semantics of quantum computations.

Semantics of quantum computations.

- ... is a bit more subtle.

Semantics of quantum computations.

- ... is a bit more subtle.
- There is no (sensible) operator on vector spaces, replacing $\pi_1 \in B \times G \rightarrow B$.

Semantics of quantum computations...

- ... is a bit more subtle.
- There is no (sensible) operator on vector spaces, replacing $\pi_1 \in B \times G \rightarrow B$.
- **Indeed:** Forgetting part of a **pure state** results in a **mixed state**.

Density matrices and superoperators

Density matrices and superoperators

- Mixed states are represented by *density matrices*.

Density matrices and superoperators

- Mixed states are represented by *density matrices*.
- Operations on mixed states (i.e. density matrices) are represented by superoperators.

Density matrices and superoperators

- Mixed states are represented by *density matrices*.
- Operations on mixed states (i.e. density matrices) are represented by superoperators.
- Every unitary operator ϕ gives rise to a superoperator $\hat{\phi}$.

Density matrices and superoperators

- Mixed states are represented by *density matrices*.
- Operations on mixed states (i.e. density matrices) are represented by superoperators.
- Every unitary operator ϕ gives rise to a superoperator $\hat{\phi}$.
- There is an operator

$$\text{tr}_{B,G} \in B \otimes G \xrightarrow{\circ}_{\text{super}} B$$

called *partial trace*.

Semantics

Semantics

Every quantum computation α gives rise to a superoperator $U\alpha \in A \multimap_{\text{super}} B$

$$\begin{array}{ccc} A \otimes H & \xrightarrow{\hat{\phi}} & B \otimes G \\ \uparrow - \otimes \tilde{h} & & \downarrow \text{tr}_G \\ A & \xrightarrow{U\alpha} & B \end{array}$$

Semantics

Every quantum computation α gives rise to a superoperator $U\alpha \in A \multimap_{\text{super}} B$

$$\begin{array}{ccc} A \otimes H & \xrightarrow{\hat{\phi}} & B \otimes G \\ \uparrow -\otimes \tilde{h} & & \downarrow \text{tr}_G \\ A & \xrightarrow{U\alpha} & B \end{array}$$

Theorem: Every superoperator $F \in A \multimap_{\text{super}} B$ (on finite Hilbert spaces) comes from a quantum computation.

Classical vs quantum

Classical vs quantum

classical

quantum

Classical vs quantum

classical	quantum
finite sets	

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	tensor product (\otimes)

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	tensor product (\otimes)
functions	

Classical vs quantum

classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	tensor product (\otimes)
functions	superoperators

Classical vs quantum

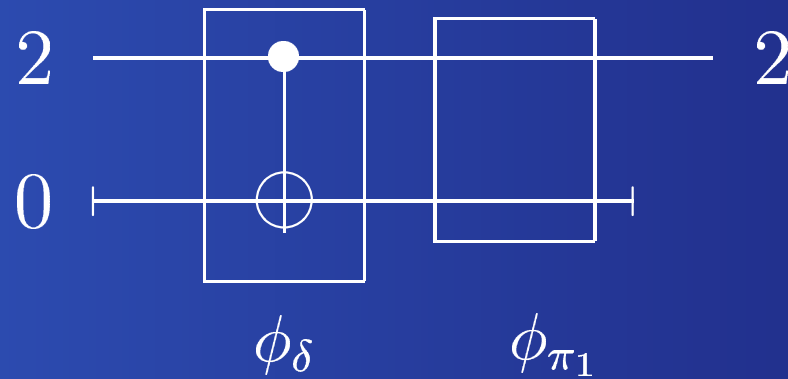
classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	tensor product (\otimes)
functions	superoperators
projections	

Classical vs quantum

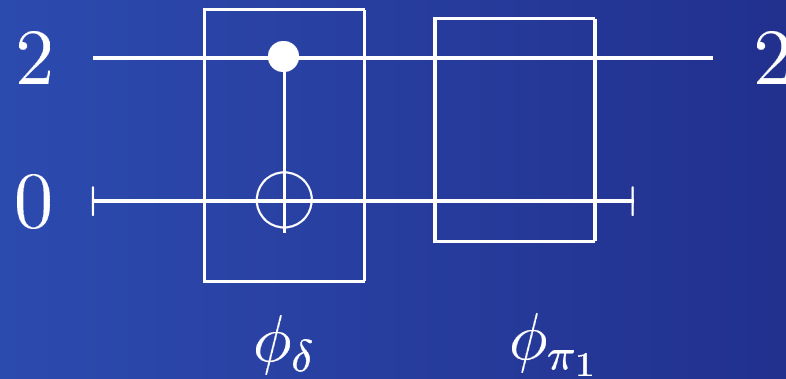
classical	quantum
finite sets	finite dimensional Hilbert spaces
bijections	unitary operators
cartesian product (\times)	tensor product (\otimes)
functions	superoperators
projections	partial trace

Decoherence

Decoherence



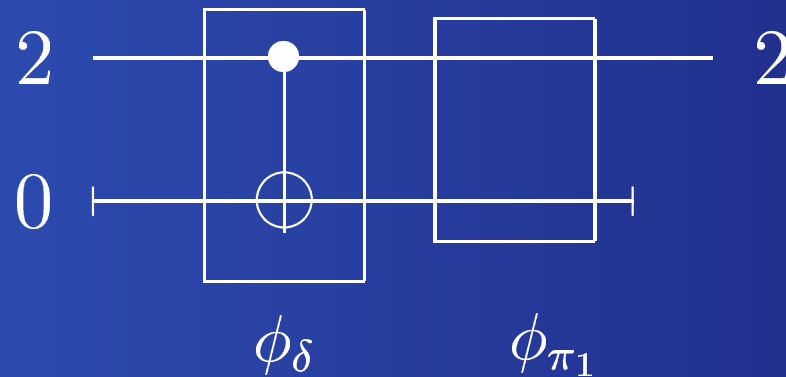
Decoherence



Classically

$$\pi_1 \circ \delta = I$$

Decoherence

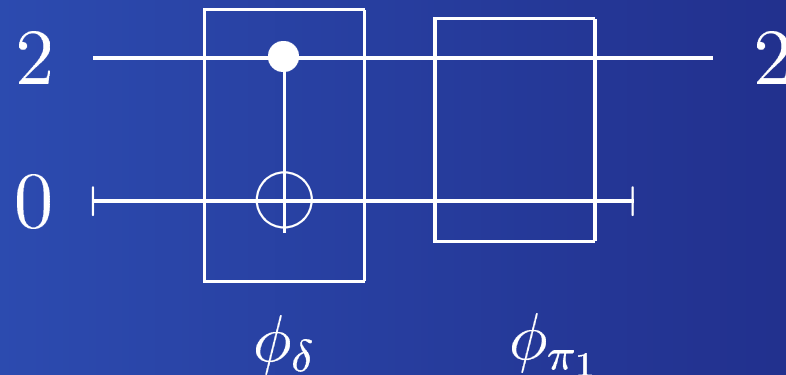


Classically

$$\pi_1 \circ \delta = I$$

Quantum

Decoherence



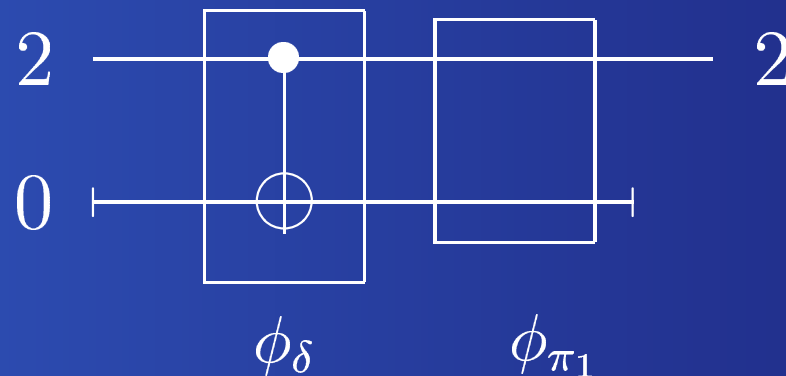
Classically

$$\pi_1 \circ \delta = I$$

Quantum

input: $\left\{ \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |0\rangle \right\}$

Decoherence



Classically

$$\pi_1 \circ \delta = I$$

Quantum

input: $\left\{ \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |0\rangle \right\}$

output: $\frac{1}{2} \{ |0\rangle \} + \frac{1}{2} \{ |1\rangle \}$

2. QML basics

1. Semantics of finite classical and quantum computation
2. QML basics
3. Compiling QML
4. Conclusions and further work

QML basics

QML basics

- QML is a first order functional languages, i.e. programs are well-typed expressions.

QML basics

- QML is a first order functional languages, i.e. programs are well-typed expressions.
- QML types are $1, \sigma \otimes \tau, \sigma \oplus \tau$

QML basics

- QML is a first order functional languages, i.e. programs are well-typed expressions.
- QML types are $1, \sigma \otimes \tau, \sigma \oplus \tau$
- Qbits $Q_2 = 1 \oplus 1$

QML basics

- QML is a first order functional languages, i.e. programs are well-typed expressions.
- QML types are $1, \sigma \otimes \tau, \sigma \oplus \tau$
- Qbits $Q_2 = 1 \oplus 1$
- Qbytes
 $Q_2^8 = Q_2 \otimes Q_2 \otimes Q_2 \otimes Q_2 \otimes Q_2 \otimes Q_2 \otimes Q_2 \otimes Q_2.$

QML basics ...

- A QML program is an expression in a context of typed variables, e.g.

$$qnot : Q_2 \multimap Q_2$$
$$qnot\ x = \mathbf{if}^\circ\ x$$
$$\quad \mathbf{then}\ qfalse$$
$$\quad \mathbf{else}\ qtrue$$

QML basics ...

- A QML program is an expression in a context of typed variables, e.g.

$$qnot : Q_2 \rightarrow Q_2$$
$$qnot\ x = \mathbf{if}^\circ\ x$$
$$\quad \mathbf{then}\ qfalse$$
$$\quad \mathbf{else}\ qtrue$$

- We can compile QML programs into quantum computations (i.e. quantum circuits).

QML basics ...

- Forgetting variables has to be explicit.

QML basics ...

- Forgetting variables has to be explicit.

E.g.

$$qfst : Q_2 \otimes Q_2 \multimap Q_2$$

$$qfst (x, y) = x$$

is illegal,

QML basics ...

- Forgetting variables has to be explicit.

E.g.

$$qfst : Q_2 \otimes Q_2 \multimap Q_2$$

$$qfst (x, y) = x$$

is illegal,

but

$$qfst : Q_2 \otimes Q_2 \multimap Q_2$$

$$qfst (x, y) = x \uparrow \{y\}$$

is ok.

QML basics ...

- There are two different if-then-else (or more generally case) constructs.

QML basics ...

- There are two different if-then-else (or more generally case) constructs.

$$id : Q_2 \multimap Q_2$$

$$id\ x = \mathbf{if}^\circ\ x$$

then *qtrue*

else *qfalse*

is just the identity,

QML basics ...

- There are two different if-then-else (or more generally case) constructs.

$$id : Q_2 \multimap Q_2$$

$$id\ x = \mathbf{if}^\circ\ x$$

then $qtrue$

else $qfalse$

is just the identity, but

$$meas : Q_2 \multimap Q_2$$

$$meas\ x = \mathbf{if}\ x$$

then $qtrue$

else $qfalse$

introduces a measurement (and hence decoherence).

QML basics ...

- Using `ifo` is only allowed, if the branches are orthogonal, i.e. observable different.

QML basics ...

- Using `ifo` is only allowed, if the branches are orthogonal, i.e. observable different.

$$cswap : Q_2 \otimes Q_2 \dashv\circ Q_2 \dashv\circ Q_2 \otimes Q_2$$

$$cswap(x, y) \ c = \mathbf{if}^o \ c$$

then (y, x)

else (x, y)

is illegal,

QML basics ...

- Using `ifo` is only allowed, if the branches are orthogonal, i.e. observable different.

$$cswap : Q_2 \otimes Q_2 \multimap Q_2 \multimap Q_2 \otimes Q_2$$

$$cswap(x, y) c = \mathbf{if}^o c$$

$$\mathbf{then} (y, x)$$

$$\mathbf{else} (x, y)$$

is illegal, but

$$cswap : Q_2 \otimes Q_2 \multimap Q_2 \multimap Q_2 \otimes (Q_2 \otimes Q_2)$$

$$cswap(x, y) c = \mathbf{if}^o c$$

$$\mathbf{then} (qtrue, (y, x))$$

$$\mathbf{else} (qfalse, (x, y))$$

is ok.

QML basics ...

- We can introduce superpositions, e.g.

$$had : Q_2 \multimap Q_2$$

$$had\ x = \mathbf{if}^\circ\ x$$

$$\mathbf{then}\ \{ qfalse \mid (-1)\ qtrue \}$$

$$\mathbf{else}\ \{ qfalse \mid qtrue \}$$

QML basics ...

- We can introduce superpositions, e.g.

$$had : Q_2 \multimap Q_2$$

$$had\ x = \mathbf{if}^\circ\ x$$

$$\mathbf{then}\ \{ q_{false} \mid (-1)\ q_{true} \}$$

$$\mathbf{else}\ \{ q_{false} \mid q_{true} \}$$

However, the terms in the superposition have to be orthogonal.

3. Compiling QML

1. Semantics of finite classical and quantum computation
2. QML basics
3. Compiling QML
4. Conclusions and further work

Compilation

Compilation

- Correct QML programs are defined by typing rules, e.g.

$$\frac{\Gamma \vdash t : \sigma \otimes \tau \quad \Delta, x : \sigma, y : \tau \vdash u : C}{\Gamma \otimes \Delta \vdash \mathbf{let} (x, y) = t \mathbf{in} u : C} \otimes \text{elim}$$

Compilation

- Correct QML programs are defined by typing rules, e.g.

$$\frac{\Gamma \vdash t : \sigma \otimes \tau \quad \Delta, x : \sigma, y : \tau \vdash u : C}{\Gamma \otimes \Delta \vdash \mathbf{let} (x, y) = t \mathbf{in} u : C} \otimes \text{elim}$$

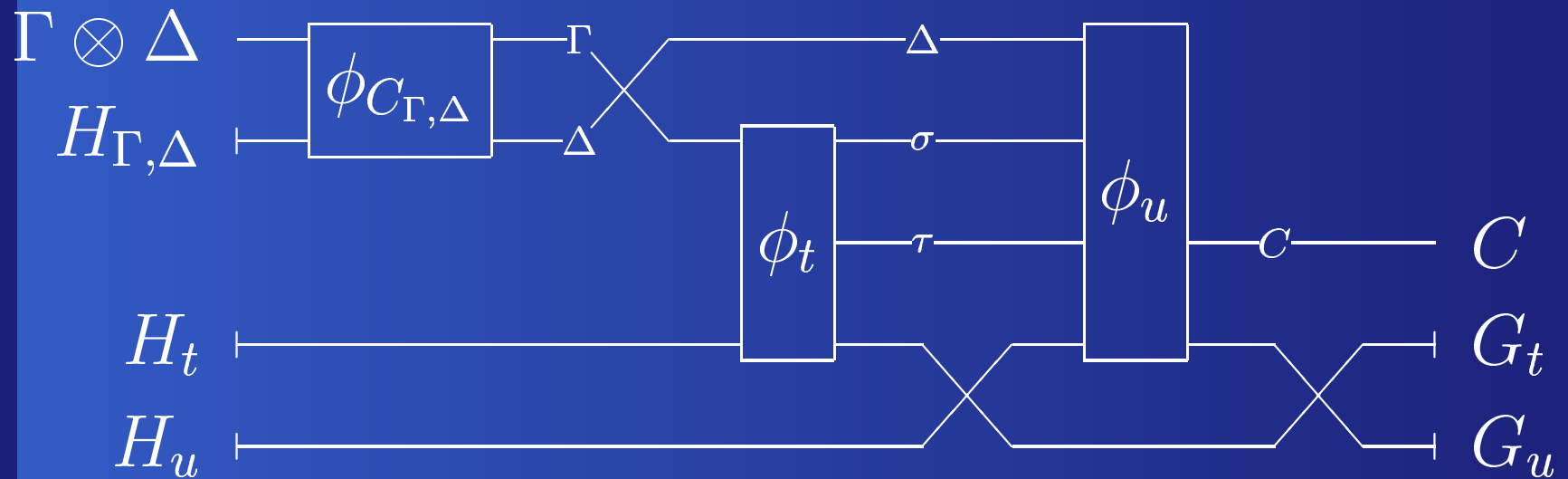
For each rule we can construct a quantum computation, i.e. a circuit.

\otimes -elim

$$\frac{\Gamma \vdash t : \sigma \otimes \tau \quad \Delta, x : \sigma, y : \tau \vdash u : C}{\Gamma \otimes \Delta \vdash \text{let } (x, y) = t \text{ in } u : C} \otimes \text{elim}$$

⊗-elim

$$\frac{\Gamma \vdash t : \sigma \otimes \tau \quad \Delta, x : \sigma, y : \tau \vdash u : C}{\Gamma \otimes \Delta \vdash \text{let } (x, y) = t \text{ in } u : C} \otimes \text{elim}$$



Compiler

Compiler

- A compiler is currently being implemented by my student Jonathan Grattage (in Haskell).

Compiler

- A compiler is currently being implemented by my student Jonathan Grattage (in Haskell).
- The output of the compiler are quantum circuits which can be simulated by a quantum circuit simulator.

Compiler

- A compiler is currently being implemented by my student Jonathan Grattage (in Haskell).
- The output of the compiler are quantum circuits which can be simulated by a quantum circuit simulator.
- Amr Sabry and Juliana Vizotti (Indiana University) embarked on an independent implementation of QML based on our paper.

4. Conclusions

1. Semantics of finite classical and quantum computation
2. QML basics
3. Compiling QML
4. Conclusions and further work

Conclusions

Conclusions

- Our semantic ideas proved useful when designing a quantum programming language, analogous concepts are modelled by the same syntactic constructs.

Conclusions

- Our semantic ideas proved useful when designing a quantum programming language, analogous concepts are modelled by the same syntactic constructs.
- Our analysis also highlights the differences between classical and quantum programming.

Conclusions

- Our semantic ideas proved useful when designing a quantum programming language, analogous concepts are modelled by the same syntactic constructs.
- Our analysis also highlights the differences between classical and quantum programming.
- Quantum programming introduces the problem of *control of decoherence*, which we address by making forgetting variables explicit and by having different if-then-else constructs.

Further work

Further work

- We have to analyze more quantum programs to evaluate the practical usefulness of our approach.

Further work

- We have to analyze more quantum programs to evaluate the practical usefulness of our approach.
- Are we able to come up with completely new algorithms using QML?

Further work

- We have to analyze more quantum programs to evaluate the practical usefulness of our approach.
- Are we able to come up with completely new algorithms using QML?
- How to deal with higher order programs?

Further work

- We have to analyze more quantum programs to evaluate the practical usefulness of our approach.
- Are we able to come up with completely new algorithms using QML?
- How to deal with higher order programs?
- How to deal with infinite datatypes?

Further work

- We have to analyze more quantum programs to evaluate the practical usefulness of our approach.
- Are we able to come up with completely new algorithms using QML?
- How to deal with higher order programs?
- How to deal with infinite datatypes?
- Investigate the similarities/differences between FCC and FQC from a categorical point of view.

The end

Thank you for your attention.