Quantum computing with relations

Dusko Pavlovic

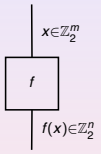
Kestrel Institute
and
Oxford University

QI 2009
Saarbrücken, March 2009

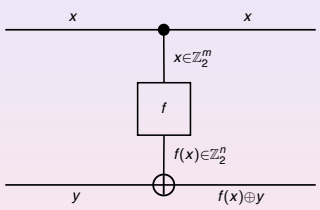
Outline

Outline

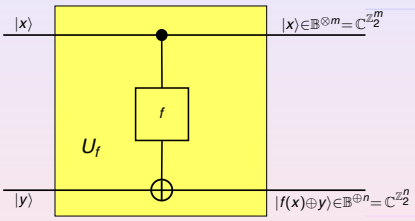
What do quantum programmers do?



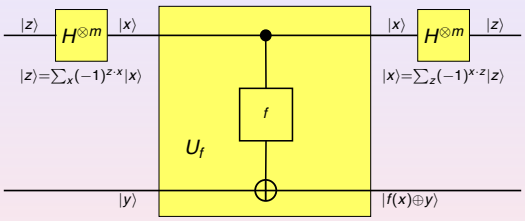
What do quantum programmers do?



What do quantum programmers do?



What do quantum programmers do?



Simon's algorithm

$$f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^n : x \mapsto f(x)$$

$$f' : \mathbb{Z}_2^{m+n} \longrightarrow \mathbb{Z}_2^{m+n} : x, y \mapsto x, f(x) \oplus y$$

$$U_f : \mathbb{C}^{\mathbb{Z}_2^{m+n}} \longrightarrow \mathbb{C}^{\mathbb{Z}_2^{m+n}} : |x, y\rangle \mapsto |x, f(x) \oplus y\rangle$$

$$\begin{aligned} \mathit{Simon} &= (H^{\otimes m} \otimes id) U_f (H^{\otimes m} \otimes id) \, |0, 0\rangle \\ &= \sum_{x,z \in \mathbb{Z}_2^m} (-1)^{x \cdot z} |z, f(x)\rangle \end{aligned}$$

Quantum computing with relations
Dusko Pavlovic
Quantum programs
Quantum categories
Classical interfaces
All that in Rel

Simon's algorithm

$$f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^n : x \mapsto f(x)$$

$$f' : \mathbb{Z}_2^{m+n} \longrightarrow \mathbb{Z}_2^{m+n} : x, y \mapsto x, f(x) \oplus y$$

$$U_f : \mathbb{C}^{\mathbb{Z}_2^{m+n}} \longrightarrow \mathbb{C}^{\mathbb{Z}_2^{m+n}} : |x, y\rangle \mapsto |x, f(x) \oplus y\rangle$$

$$\begin{aligned} \mathit{Simon} &= (H^{\otimes m} \otimes id) U_f (H^{\otimes m} \otimes id) \, |0, 0\rangle \\ &= \sum_{x,z \in \mathbb{Z}_2^m} (-1)^{x \cdot z} |z, f(x)\rangle \end{aligned}$$

. . . to find a hidden subgroup

measurement $\rightsquigarrow$ find c such that $f(x + c) = f(x)$

Quantum computing with relations
Dusko Pavlovic
Quantum programs
Quantum categories
Classical interfaces
All that in Rel

Shor's algorithm

$$f : \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q^n : x \mapsto a^x \mod q$$

$$f' : \mathbb{Z}_q^{m+n} \longrightarrow \mathbb{Z}_q^{m+n} : x, y \mapsto x, a^x + y \mod q$$

$$U_f : \mathbb{C}^{\mathbb{Z}_q^{m+n}} \longrightarrow \mathbb{C}^{\mathbb{Z}_q^{m+n}} : |x, y\rangle \mapsto |x, a^x + y \mod q\rangle$$

$$\begin{aligned} \mathit{Shor} &= (FT_m \otimes id) U_f (FT_m \otimes id) \, |0, 0\rangle \\ &= \sum_{x,z \in \mathbb{Z}_q^m} (-1)^{x \cdot z} |z, f(x)\rangle \end{aligned}$$

. . . to find a hidden subgroup

measurement $\rightsquigarrow$ find c such that $a^{x+c} = a^x \mod q$

Quantum computing with relations
Dusko Pavlovic
Quantum programs
Quantum categories
Classical interfaces
All that in Rel

Hallgren's algorithm

$$h : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n : x \mapsto I_x \text{ (fraction ideal)}$$

$$h' : \mathbb{Z}^{m+n} \longrightarrow \mathbb{Z}^{m+n} : x, y \mapsto x, y - h(x)$$

$$U_h : \mathbb{C}^{\mathbb{Z}^{m+n}} \longrightarrow \mathbb{C}^{\mathbb{Z}^{m+n}} : |x, y\rangle \mapsto |x, y - h(x)\rangle$$

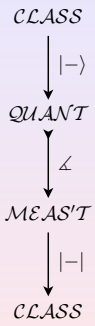
$$\begin{aligned} \mathit{Hallgren} &= (FT_m \otimes id) U_h (FT_m \otimes id) \, |d, \tilde{d}\rangle \\ &= \sum_{x,z \in \mathbb{Z}^m} (-1)^{x \cdot z} |z, h(x)\rangle \end{aligned}$$

. . . to find a hidden subgroup

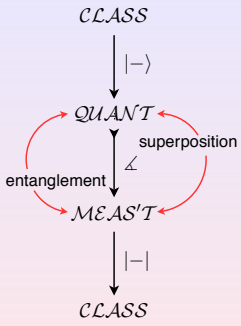
measurement $\rightsquigarrow$ find R such that $h(x + R) = h(x)$

Quantum computing with relations
Dusko Pavlovic
Quantum programs
Quantum categories
Classical interfaces
All that in Rel

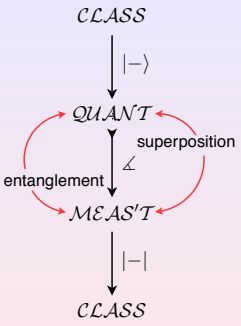
Quantum software engineering ;)



Quantum resources

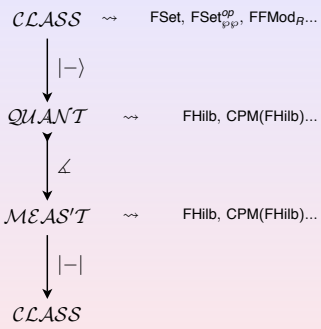


Quantum resources



quantum programming = functional programming
+ superposition + entanglement

Standard universes



Outline

Quantum formalisms

- standard universe: Hilbert spaces

Quantum formalisms

- standard universe: Hilbert spaces
  - von Neumann ('37): "I don't believe in Hilbert spaces"

Quantum formalisms

- standard universe: Hilbert spaces
  - von Neumann ('37): "I don't believe in Hilbert spaces"
- logic of Hilbert spaces: orthonormal lattices

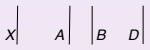
Quantum formalisms

- standard universe: Hilbert spaces
  - von Neumann ('37): "I don't believe in Hilbert spaces"
- logic of Hilbert spaces: orthonormal lattices
  - no compound systems

Quantum formalisms

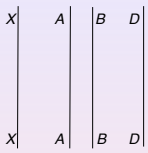
- standard universe: Hilbert spaces
  - von Neumann ('37): "I don't believe in Hilbert spaces"
- logic of Hilbert spaces: orthonormal lattices
  - no compound systems
- structure of Hilbert spaces: ‡**-monoidal categories**

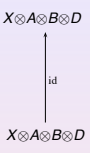
Categories in pictures: Objects



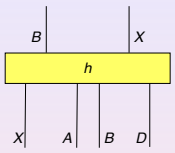
$X \otimes A \otimes B \otimes D$

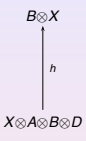
Categories in pictures: Identities



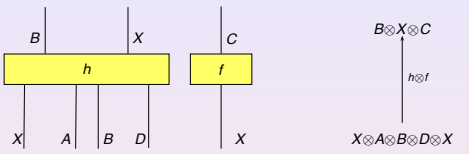


Categories in pictures: Operators

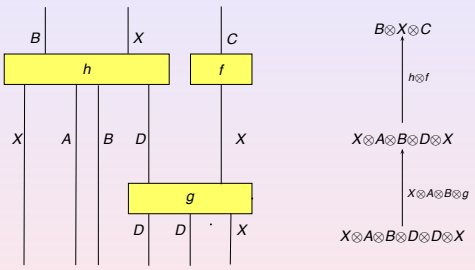




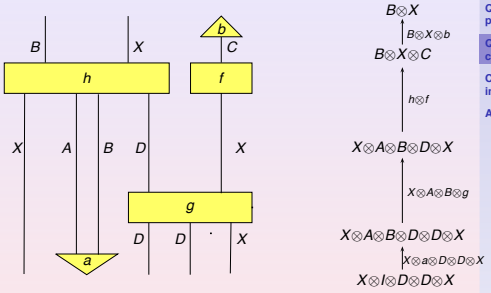
Categories in pictures: Tensors



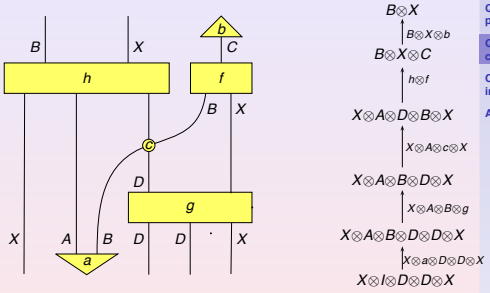
Categories in pictures: Composition



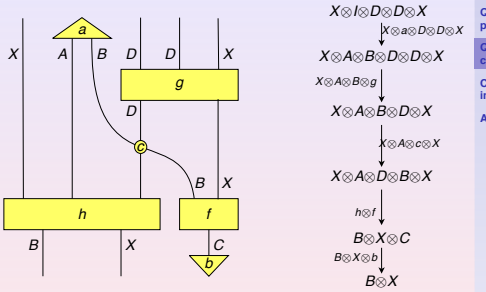
Categories in pictures: vectors and covectors



Categories in pictures: Symmetry



Categories in pictures: Adjoints



Claim

All details of the HSP algorithms can be specified using this structure.

Formal concepts

Universe $\mathcal{S}$

- **spaces:** $|\mathcal{S}| = \{A, B, \ldots\}$
- **operators:** $\mathcal{S}(A, B) = \{f, g, \ldots\}$
- **vectors**: $\mathcal{S}(A) = \mathcal{S}(I, A)$
- **scalars**: $\mathbb{I} = \mathcal{S}(I, I)$

Derived structure

Over formal vectors we define:

- *inner product*

$$\begin{array}{rcl} \langle -|-\rangle_A \ : \ \mathcal{C}(A) \times \mathcal{C}(A) & \longrightarrow & \mathbb{I} \\ (\psi, \varphi : I \longrightarrow A) & \longmapsto & \left(I \xrightarrow{\varphi} A \xrightarrow{\psi^\ddagger} I \right) \end{array}$$

Derived structure

Over formal vectors we define:

- *inner product*

$$\begin{array}{rcl} \langle -|-\rangle_A \ : \ \mathcal{C}(A) \times \mathcal{C}(A) & \longrightarrow & \mathbb{I} \\ (\psi, \varphi : I \longrightarrow A) & \longmapsto & \left(I \xrightarrow{\varphi} A \xrightarrow{\psi^\ddagger} I \right) \end{array}$$

- *partial inner product*

$$\begin{array}{rcl} \langle -|-\rangle_{AB} \ : \ \mathcal{C}(A) \times \mathcal{C}(A \otimes B) & \longrightarrow & \mathcal{C}(B) \\ (\psi : I \to A, \varphi : I \to A \otimes B) & \longmapsto & \left(I \xrightarrow{\varphi} A \otimes B \xrightarrow{\psi^\ddagger \otimes B} B \right) \end{array}$$

Derived structure

Over formal vectors we define:

- *inner product*

$$\begin{array}{rcl} \langle -|-\rangle_A \ : \ \mathcal{C}(A) \times \mathcal{C}(A) & \longrightarrow & \mathbb{I} \\ (\psi, \varphi : I \longrightarrow A) & \longmapsto & \left(I \xrightarrow{\varphi} A \xrightarrow{\psi^\ddagger} I \right) \end{array}$$

- *partial inner product*

$$\begin{array}{rcl} \langle -|-\rangle_{AB} \ : \ \mathcal{C}(A) \times \mathcal{C}(A \otimes B) & \longrightarrow & \mathcal{C}(B) \\ (\psi : I \to A, \varphi : I \to A \otimes B) & \longmapsto & \left(I \xrightarrow{\varphi} A \otimes B \xrightarrow{\psi^\ddagger \otimes B} B \right) \end{array}$$

- *entangled vectors* $\eta \in \mathcal{C}(A \otimes A)$, such that $\forall \varphi \in \mathcal{C}(A)$

$$\langle \eta | \varphi \rangle_{AA} \ = \ \varphi$$

Derived structure

Using

- entangled vectors
  $\eta_A : I \longrightarrow A \otimes A$ and $\eta_B : I \longrightarrow B \otimes B$
- their adjoints
  $\eta_A^\ddagger : A \otimes A \longrightarrow I$ and $\eta_B^\ddagger : B \otimes B \longrightarrow I$

Derived structure

Using

- entangled vectors
  $\eta_A : I \longrightarrow A \otimes A$ and $\eta_B : I \longrightarrow B \otimes B$
- their adjoints
  $\eta_A^\ddagger : A \otimes A \longrightarrow I$ and $\eta_B^\ddagger : B \otimes B \longrightarrow I$

define for every $f : A \longrightarrow B$

- the *dual* $f^* : B \longrightarrow A$

$$f^* \ = \ B \xrightarrow{B\eta} BAA \xrightarrow{BfA} BBA \xrightarrow{\eta^\ddagger A} A$$

Derived structure

Using

- entangled vectors
  $\eta_A : I \longrightarrow A \otimes A$ and $\eta_B : I \longrightarrow B \otimes B$
- their adjoints
  $\eta_A^\ddagger : A \otimes A \longrightarrow I$ and $\eta_B^\ddagger : B \otimes B \longrightarrow I$

define for every $f : A \longrightarrow B$

- the *dual* $f^* : B \longrightarrow A$

$$f^* \quad = \quad B \xrightarrow{B\eta} BAA \xrightarrow{BfA} BBA \xrightarrow{\eta^\ddagger A} A$$

- the *conjugate* $f_* : A \longrightarrow B$

$$f_* \quad = \quad f^{*\ddagger} \quad = \quad f^{\ddagger *}$$

Outline

Classical data

Question

- How do we recognize classical data in a quantum world?

Classical data

Idea

- Classical data can be copied and deleted.
- Quantum data cannot be copied or deleted.

Classical data

Idea

- Classical data can be copied and deleted.
- Quantum data cannot be copied or deleted.

Question

- But how do we really tell them apart in a program?

Classical data

$$f : \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^n : x \mapsto f(x)$$

$$f' : \mathbb{Z}_2^{m+n} \longrightarrow \mathbb{Z}_2^{m+n} : x, y \mapsto x, f(x) \oplus y$$

$$U_f : \mathbb{C}^{\mathbb{Z}_2^{m+n}} \longrightarrow \mathbb{C}^{\mathbb{Z}_2^{m+n}} : |x, y\rangle \mapsto |x, f(x) \oplus y\rangle$$

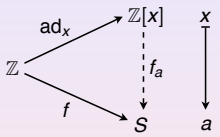
$$\begin{aligned} Simon &= (H^{\otimes m} \otimes id) U_f (H^{\otimes m} \otimes id) \, |0, 0\rangle \\ &= \sum_{x,z \in \mathbb{Z}_2^m} (-1)^{x \cdot z} |z, f(x)\rangle \end{aligned}$$

Classical data

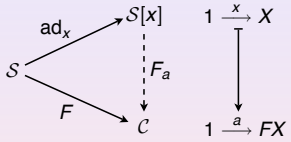
Answer

Classical data are what is denoted by the variables.

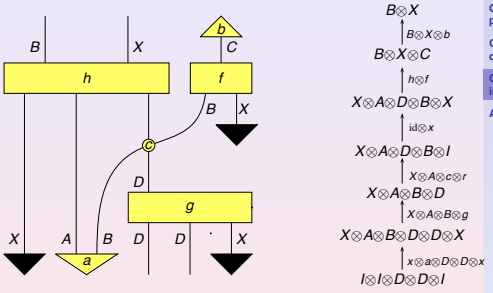
Adjoining variables to algebras



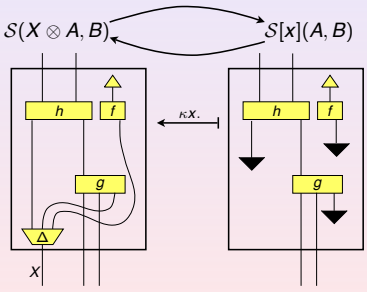
Adjoining variables to categories



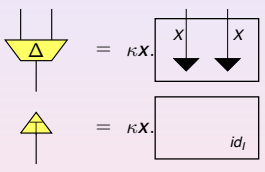
Adjoining variables to categories



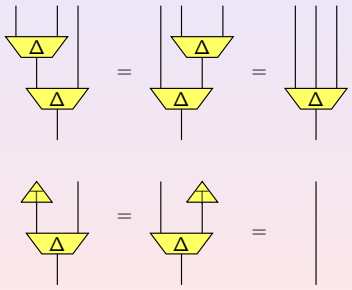
Variable abstraction in categories



Classical structure

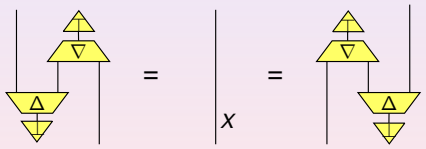


Classical structure: comonoid



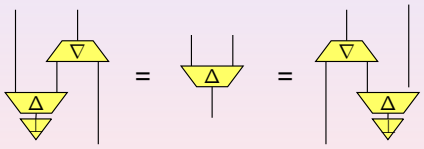
Classical structure: Frobenius algebra

Self-dual



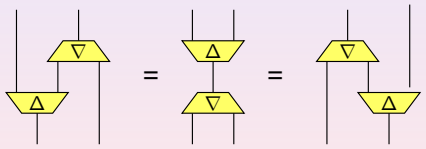
Classical structure: Frobenius algebra

. . . or equivalently



Classical structure: Frobenius algebra

. . . or still equivalently



Classical structures are bases

Theorem (Coecke, DP & Vicary)

Classical structures over Hilbert spaces and linear maps are in a bijective correspondence with the bases.

Classical structures are bases

Theorem

Classical structures over sets and relations are disjoint unions of abelian groups.

Outline

What do quantum programmers do?

Categories for quantum programming

Classical interfaces for categorical quantum programs

All that in the category of relations

What quantum programmers do now?

$$\frac{f(x) = f \circ x \in \mathsf{FSet}_{\wp}[x{:}m](n)}{f'(x,y) = \langle x, y \oplus f(x)\rangle \in \mathsf{FSet}_{\wp}[x,y{:}m+n](m+n)}$$
$$\overline{U_f|x,y\rangle = \mathbb{B}^{\otimes f'(x,y)} \in \mathsf{FHilb}\left[|x,y\rangle{:}\mathbb{B}^{\otimes(m+n)}\right]\left(\mathbb{B}^{\otimes(m+n)}\right)}$$

where $\mathbb{B} = \mathbb{C}^2$ and

$$\mathbb{B}^{\otimes(-)} \;:\; \mathsf{FSet}_{\wp}[x,y{:}m+n] \longrightarrow \mathsf{FHilb}\left[|x,y\rangle{:}\mathbb{B}^{\otimes(m+n)}\right]$$

What can they do in Rel?

The role of $\mathbb{B}$ can be played by $\Xi_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, where

$$\Xi_2 = \{00, 01, 10, 11\}$$
$$\Delta(i0) = \{\langle i0, i0\rangle, \langle i1, i1\rangle\} \quad \Delta(i1) = \{\langle i0, i1\rangle, \langle i1, i0\rangle\}$$
$$\top = \{00, 10\}$$
$$\mathcal{B}(\Xi) = \{\beta_0 = \{00, 01\}, \beta_1 = \{10, 11\}\}$$

What can they do in Rel?

The role of $\mathbb{B}$ can be played by $\Xi_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, where

$$\begin{aligned}
\Xi_n &= \sum_n \mathbb{Z}_n = \{ij \mid 0 \le i, j \le n-1\} \\
\Delta(ij) &= \{\langle ik, i\ell\rangle \mid j = k + \ell\} \\
\top &= \{i0 \mid 0 \le i \le n-1\} \\
\mathcal{B}(\Xi_n) &= \{\beta_i = \{ij\} \mid 0 \le i, j \le n-1\}
\end{aligned}$$

Qubits in Rel

The point is that Ξ_n supports a simple Fourrier transform into the complementary basis

$$\begin{aligned}
FT_n \;:\; \Xi_n &\longrightarrow \Xi_n \\
ij &\longmapsto ji
\end{aligned}$$

Qubits in Rel

The point is that Ξ_n supports a simple Fourrier transform into the complementary basis

$$\begin{aligned}
FT_n \;:\; \Xi_n &\longrightarrow \Xi_n \\
ij &\longmapsto ji
\end{aligned}$$

Use $H = FT_2$ to transform m-bitstrings by $H^{\otimes m} : \Xi^{\otimes m} \longrightarrow \Xi^{\otimes m}$ for Simon's algorithm.