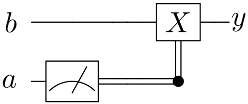
OPERATOR ALGEBRAS IN CATEGORICAL QUANTUM FOUNDATIONS

Mathys Rennela

LIACS (Leiden University)
May 9, 2019

Universiteit Leiden
The Netherlands

Programming quantum circuits



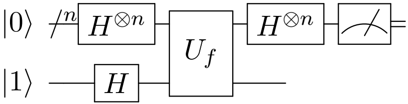
$$
\begin{aligned}
-; a, b : \mathrm{qubit} \vdash C \overset{\mathsf{def}}{=} \; & x \leftarrow \textbf{gate meas } a; \\
& (x, y) \leftarrow \textbf{gate } (\textbf{bit-control } X)\,(x, b); \\
& () \leftarrow \textbf{gate discard } x; \textbf{output } y \qquad : \ \mathrm{qubit}
\end{aligned}
$$

- Problem: not all quantum protocols are that simple...

Concrete model for quantum circuits

- C*-algebras: algebras of physical observables.
- **Intuition:** Measurable quantities of a physical system
- **Example:** 2-by-2 matrices are taken to represent qubits

- Positive maps: arrows which preserve observables
- Completely positive maps: arrows which allows to run the computation on a subsystem of a bigger system
- **Intuition:** Communication channels which transmit quantum information



(Deustch-Jozsa algorithm)

Concrete model for quantum programs

- **Goal:** add recursive types, loops, ...
- **Problem 1:** Finite-dimensional algebras of physical observables aren't enough, semantically.
- **Problem 2:** Complete positivity is at the core of quantum computation.
- **Our solution:** Semantics based on categories of W*-algebras

Infinite-dimensional structures: why should we care?

- **Argument 1**: Benefit from the *full* power of the theory of operator algebras. (e.g. Rennela, Staton, Furber, 2015)
- **Argument 2**: Infinite dimensionality arise naturally in quantum field theory.
- **Argument 3**: The register space in a scalable photonic quantum computer arguably has an infinite dimensional aspect.
- **Argument 4**: Infinite dimensionality comes into play in Quantum PL (e.g. Gielerak, Sawerwain, 2007; Rennela, Staton, 2018).

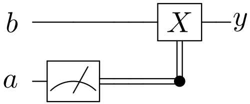
Abstract language for embedded circuits

- Circuit language = first order typed language.
- Wire types, such as a type for bits and qubits, and gates.
- Host language = higher order language (like a proof assistant)
- Special host type $\mathrm{Circ}(W_1, W_2)$

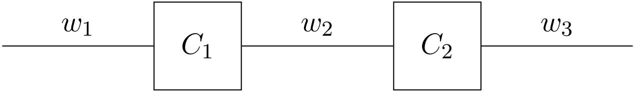
J. Paykin, R. Rand, and S. Zdancewic. QWIRE: a core language for quantum circuits. POPL'17.
J. Egger, R. E. Møgelberg, and A. Simpson. The enriched effect calculus: syntax and semantics. J. of Logic and Computation, 2012.

M. Rennela, S. Staton, Classical Control, Quantum Circuits and Linear Logic in Enriched Category Theory, LMCS, to appear.

Embedding as enrichment

$C \overset{\text{def}}{=}$ 

$$t \overset{\text{def}}{=} \textbf{box}\ (a, b) \Rightarrow C(a, b) : \mathsf{Circ}(\mathsf{qubit} \otimes \mathsf{qubit}, \mathsf{qubit})$$



$$\mathsf{comp} : \mathrm{Circ}(W_1, W_2) \times \mathrm{Circ}(W_2, W_3) \to \mathrm{Circ}(W_1, W_3)$$

(W_i type of the wire w_i for $i \in \{1, 2, 3\}$)

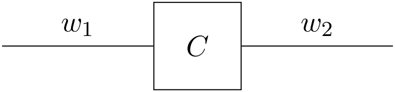
The embedding of the circuit language in the host language is an instance of enriched category theory

What is enriched category theory?

- **Category**: collection of objects and arrows between them.
- **Enriched category**: category whose arrows are objects of another category

Max Kelly. Basic concepts of enriched category theory, volume 64. CUP Archive, 1982.

- **Semantics**: associate (mathematical) meaning to programs.



becomes an arrow $[\![C]\!] : [\![w_1]\!] \to [\![w_2]\!]$

Types as C*-algebras

- A type A is interpreted as a C*-algebra $[\![A]\!]$.
  - C*-algebra $=$ algebra of physical observables (measurable quantities of a physical system).

- Bool: $[\![\text{bool}]\!] = \mathbb{C} \oplus \mathbb{C}$
- Qubit: $[\![\text{qubit}]\!] = M_2 = \mathcal{B}(\mathbb{C}^2)$
- Tensor: $[\![x : A, y : B]\!] = A \otimes B$
- Void: $[\![()]\!] = \mathbb{C}$
- Natural numbers: $[\![\mathrm{nat}]\!] = \oplus_{n \in \mathbb{N}} \mathbb{C}$

Programs as completely positive maps

- $f = [\![x : A \vdash t : B]\!] : [\![B]\!] \to [\![A]\!]$ (predicate transformer)
  - unital: preserves the unit, i.e. $f(1) = 1$
  - sub-unital: $f(1) \leq 1$
  - positive: preserves observables
    - positive element: $a = x^* x$ for some x.
    - observables are determined by positive elements.
  - **completely positive**: allows to run the computation on a subsystem of a bigger system.
    - $M_{2^n}(f) : M_{2^n}(B) \to M_{2^n}(A)$ positive.
      $\mathrm{id}_{[\![\mathsf{qubit}]\!]^{\otimes n}} \otimes f : [\![\mathsf{qubit}]\!]^{\otimes n} \otimes [\![B]\!] \to [\![\mathsf{qubit}]\!]^{\otimes n} \otimes [\![A]\!]$ positive.
- **Complete positivity is at the core of quantum computation**

W*-algebras

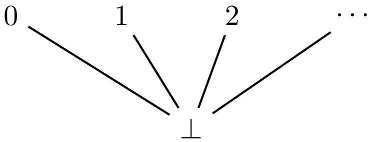
- W*-algebras: C*-algebras with nice domain-theoretic properties.
- *Example:* the poset of positive elements below the unit forms a dcpo.

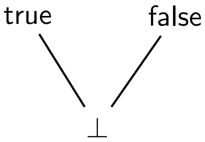
Examples of W*-algebras

- Finite dimensional C*-algebras.
- Algebras of bounded operators $\mathcal{B}(H)$ on any Hilbert space H.
- Function spaces $L^\infty(X)$ for any standard measure space X.
- The space $\ell^\infty(\mathbb{N})$ of bounded sequences.

Recap on domain theory

- Poset $(P, \leq)$ = set P + partial order $\leq$





- $\Delta \subseteq P$ **directed** if every pair in Δ has an upper bound in Δ.
- **least upper bound** (lub) $\bigvee \Delta$ of $\Delta \subseteq P$ (it it exists) is greater than or equal to all the other elements of the set Δ.
- **dcpo** D = poset D where every directed Δ has a lub.
- Example: $[0,1]_A$, subset of positive elements of below the unit of a W*-algebra.
- $f : P \to Q$ **Scott-continuous** if it preserves lubs.

Löwner order

- $\phi : A \to B$ is **normal** if ϕ is a positive between W*-algebras and its restriction $\phi : [0, 1]_A \to [0, 1]_B$ is Scott-continuous.
- $\mathbf{W^*\text{-}Alg}_{\mathrm{CPSU}}$: category of W*-algebras together with normal CPSU-maps
- **Löwner partial order**: For positive maps $f, g : A \to B$ between W*-algebras A and B: $\sqsubseteq$: $f \sqsubseteq g$ if and only if $g - f$ is positive, i.e. $\forall x \in A^+, (g - f)(x) \in B^+$.

Theorem (Rennela, 2013; Rennela, 2018)

For W-algebras A and B, the poset $(\mathbf{W^*\text{-}Alg}_{\mathrm{CPSU}}(A, B), \sqsubseteq)$ is* ***directed-complete****.*

W*-algebras are order-enriched

Recall: a category whose hom-sets are posets is called $\mathbf{Dcpo}_{\perp!}$-**enriched** if:

1. its hom-sets are dcpos with bottom
2. pre-composition and post-composition of morphisms are strict and Scott-continuous.

Theorem (Rennela, 2014)

*The category $\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{PSU}}$ is a $\mathbf{Dcpo}_{\perp!}$-**enriched** category.*

Theorem

$\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}$*, category of W*-algebras together with NCPSU-maps, is $\mathbf{Dcpo}_{\perp!}$-enriched with the following order on maps: $f \sqsubseteq_{cP} g$ if and only if $g - f$ is completely positive.*

Von Neumann functors

Definition

An endofunctor F on a $\mathbf{Dcpo}_{\perp!}$-enriched category $\mathbf{C}$ is **locally continuous** if $F_{X,Y} : \mathbf{C}(X,Y) \to \mathbf{C}(FX,FY)$ is Scott-continuous.

Definition

A **von Neumann functor** is a locally continuous endofunctor on $\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}$ which preserves multiplication-preserving maps.

Theorem

The category $\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}$ *is* **algebraically compact for the class of von Neumann functors**, *i.e. every von Neumann functor* F *admits a canonical fixpoint and there is an isomorphism between the initial F-algebra and the inverse of the final F-coalgebra.*

Recipe: how to construct a fixpoint for such functors

- Consider a sequence of the form $\Delta = D_0 \xrightarrow{\alpha_0} D_1 \xrightarrow{\alpha_1} \cdots$ where $D_0 = 0$, $D_{n+1} = FD_n$, $\alpha_0 =!_{F0}$, $\alpha_{n+1} = F\alpha_n$ $(n \in \mathbb{N})$
- Define a W*-algebra D and turn it into a cocone $\mu : \Delta \to D$, i.e. a sequence of arrows $\mu_n : D_n \to D$ such that the equality $\mu_n = \mu_{n+1} \circ \alpha_n$ holds for every $n \geq 0$. This is a colimit of Δ
- Observe that $F\mu : F\Delta \to FD$ is a colimit for $F\Delta$, obtained by removing the first arrow from Δ.
- Two colimiting cocone with same vertices are isomorphic, which implies that D and FD share the same limit and are isomorphic.
- Dually, consider the sequence $\Delta^{\mathrm{op}} = D_0 \xleftarrow{\beta_0} D_1 \leftarrow \cdots$ and provide a limit for it.
- Conclusion: The functor F admits a fixpoint.

Inductive types for the circuit language

$$A, B, C \ ::= \ X \mid I \mid \textbf{qbit} \mid A + B \mid A \otimes B \mid \mu X.A$$

$$\frac{}{X \vdash X} \qquad \frac{}{\Theta \vdash I} \qquad \frac{}{\Theta \vdash \textbf{qbit}} \qquad \frac{\Theta \vdash A \qquad \Theta \vdash B}{\Theta \vdash A + B}$$

$$\frac{\Theta \vdash A \qquad \Theta \vdash B}{\Theta \vdash A \otimes B} \qquad \frac{X \vdash A \qquad \vdash \Theta}{\Theta \vdash \mu X.A}$$

Example

$\mathsf{nat} \equiv \mu X.\ I + X$ well-formed ✓

$\mu X.I + (\mu Y.\ I + Y \otimes X)$ ill-formed X

Terms for QPL with inductive types

- Based on the language QPL by Peter Selinger
- Partial grammar of terms for QPL with inductive types:

$$
\begin{aligned}
M, N ::= {} & \textbf{new unit } u \mid \textbf{new qbit } q \\
& \textbf{discard } x \mid q_1, \ldots, q_n \mathrel{*}= S \mid \\
& M; N \mid \textbf{skip} \mid b = \textbf{measure } q \mid \textbf{while } b \textbf{ do } M \mid \\
& x = \textbf{left}_{A,B} M \mid x = \textbf{right}_{A,B} M \mid \\
& \textbf{case } y \textbf{ of } \{\textbf{left } x_1 \to M \mid \textbf{right } x_2 \to N\} \mid \\
& x = (x_1, x_2) \mid (x_1, x_2) = x \mid y = \textbf{fold } x \mid y = \textbf{unfold } x \mid \\
& \textbf{proc } f :: \ x : A \to y : B \ \{M\} \textbf{ in } R \mid y = f(x)
\end{aligned}
$$

A categorical model based on W*-algebras for QPL with inductive types

- $\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}$ = category of W*-algebras and normal completely positive subunital maps.
- $\mathbf{C} = \mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}^{\mathbf{op}}$ (opposite category).
- $\mathbf{W}^*\text{-}\mathbf{Alg}_{\mathrm{CPSU}}$ has finite products $\implies$ $\mathbf{C}$ has finite coproducts
- We interpret the entire language in the category $\mathbf{C}$.
- Coproducts distribute over tensor products, i.e. $d_{A,B,C} : A \otimes (B + C) \cong (A \otimes B) + (A \otimes C)$ (Cho, 2016)

Semantics of while-loops

- $d_{A,B,C} : A \otimes (B + C) \cong (A \otimes B) + (A \otimes C)$
- Recall $\mathsf{bit} = I + I$
- Define $d_A = d_{A,I,I} : A \otimes \mathsf{bit} \to A \otimes I + A \otimes I$.
- For any $\mathbf{C}$-morphism $f : A \otimes \mathsf{bit} \to A \otimes \mathsf{bit}$, we define a Scott-continuous endofunction

$$W_f : \mathbf{C}\,(A \otimes \mathsf{bit}, A \otimes \mathsf{bit}) \to \mathbf{C}(A \otimes \mathsf{bit}, A \otimes \mathsf{bit})$$
$$W_f(g) = [\mathrm{id} \otimes \mathsf{newbit}_0,\ g \circ f \circ (\mathrm{id} \otimes \mathsf{newbit}_1)] \circ d_A$$

- $\mathsf{newbit}_0 = \textbf{left}_{I,I} : I \to \mathsf{bit}$
- $\mathsf{newbit}_1 = \textbf{right}_{I,I} : I \to \mathsf{bit}$

Interpreting inductive datatypes

- $[\![\Theta \vdash A]\!] : \mathbf{C}^{|\Theta|} \to \mathbf{C}$ functor defined by induction

$$
\begin{aligned}
[\![X \vdash X]\!] &= \mathsf{Id} \\
[\![\Theta \vdash I]\!] &= K_I \\
[\![\Theta \vdash \textbf{qbit}]\!] &= K_{\textbf{qbit}} \\
[\![\Theta \vdash A + B]\!] &= [\![\Theta \vdash A]\!] + [\![\Theta \vdash B]\!] \\
[\![\Theta \vdash A \otimes B]\!] &= [\![\Theta \vdash A]\!] \otimes [\![\Theta \vdash B]\!]
\end{aligned}
$$

- For inductive types: $[\![\Theta \vdash \mu X.A]\!] = K_{Y([\![X \vdash A]\!])}$
- $Y([\![X \vdash A]\!])$: fixpoint for $[\![X \vdash A]\!]$ given by algebraic compactness.

A categorical view on causality

- Needed: a discarding map $\diamond_A : A \to 1$ which enjoys the property that $\diamond_B \circ f = \diamond_A$ for every morphism $f : A \to B$.

- **Theorem** the interpretation in $\mathbf{C}$ of any *closed type* admits a canonical choice of discarding map by defining the type interpretations on the causal category $\mathbf{C}_c$.
- $\mathbf{C}_c = \mathbf{C}/I$, i.e. objects $= (A, \diamond_A)$, where $A \in \mathsf{Ob}(\mathbf{C})$ and $\diamond_A \in \mathbf{C}(A, I)$. maps $f : (A, \diamond_A) \to (B, \diamond_B)$ in $\mathbf{C}_c =$ maps $f : A \to B$ of $\mathbf{C}$, such that $\diamond_B \circ f = \diamond_A$.

- $\|\Theta \vdash A\| : \mathbf{C}_c^{|\Theta|} \to \mathbf{C}_c$ defined by induction
- Theorem: For any closed type $\cdot \vdash A$, we have $[\![A]\!] = U\|A\|$ and $\|A\| = ([\![A]\!], \diamond_{[\![A]\!]})$

Conclusion

- C*-algebras form a concrete model of quantum circuits
- W*-algebras form a concrete model of quantum programs
- Embedding a quantum PL in a conventional PL is an instance of enriched category theory
- Future work
  - Categorical axiomatization of W*-algebras? (Rennela, Staton, Furber, 2016)
  - Verification tools: abstract interpretation for the analysis of quantum phenomena, e.g. quantum entanglement? (Cousot, Cousot, 1997; Perdrix, 2008)