Towards a Curry-Howard Correspondence for Quantum Computation

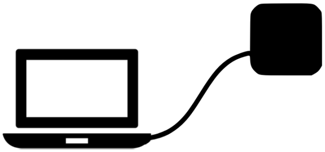
Kostia Chardonnet

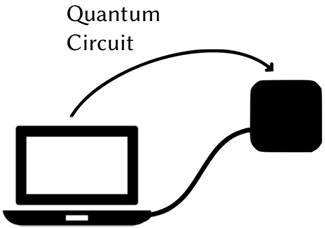
Univ. Paris Saclay, LMF, Quacs
Univ. Paris Centre, IRIF

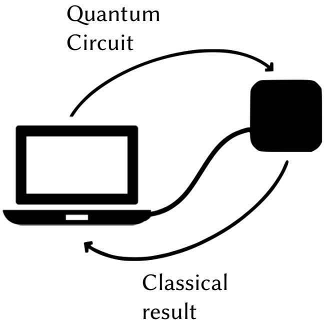
PhD Defense, 09/01/2023

Supervised by: Pablo Arrighi, Alexis Saurin, Benoît Valiron

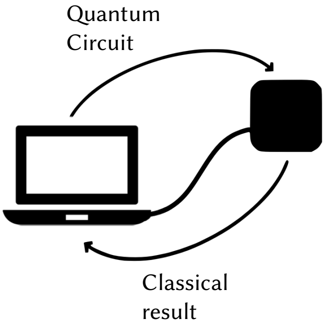
The Coprocessor Model




Quantum
Circuit

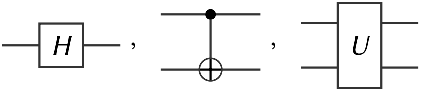

Quantum
Circuit
Classical
result

The Coprocessor Model

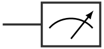


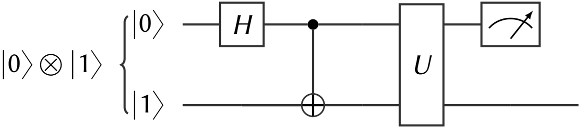
Two operations

- Unitary operations **inside** the coprocessor.

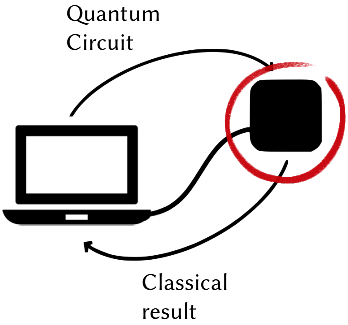


- Probabilistic operation with **measure**.



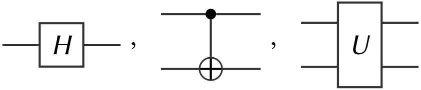


- Available data **inside coprocessor** : $\otimes^n$ qubit.

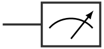


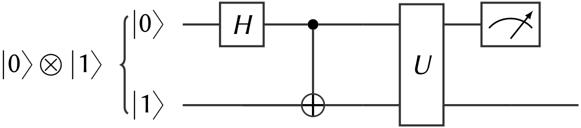
Two operations

- Unitary operations **inside** the coprocessor.



- Probabilistic operation with **measure**.





- Available data **inside coprocessor** : $\otimes^n$ qubit.

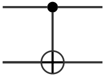
Classical	Quantum
0	$\lvert 0\rangle = \binom{1}{0}$
1	$\lvert 1\rangle = \binom{0}{1}$
$(0, 1)$	$\lvert 0\rangle \otimes \lvert 1\rangle$

$$\alpha \lvert 0\rangle + \beta \lvert 1\rangle = \binom{\alpha}{\beta}$$

Classical	Quantum
0	$\lvert 0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$
1	$\lvert 1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$
$(0,1)$	$\lvert 0\rangle \otimes \lvert 1\rangle$

$$\alpha\lvert 0\rangle + \beta\lvert 1\rangle = \left(\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right)$$

- **Unitary Operations**: can be reversed.
  - CNOT:



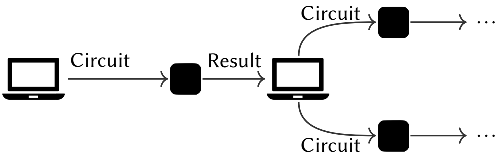
$$= \begin{cases} \lvert 0\rangle \otimes \lvert x\rangle \mapsto \lvert 0\rangle \otimes \lvert x\rangle \\ \lvert 1\rangle \otimes \lvert x\rangle \mapsto \lvert 1\rangle \otimes \lvert \neg x\rangle \end{cases}$$

  - Hadamard:

$$= \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\1 & -1\end{smallmatrix}\right) = \begin{cases} \lvert 0\rangle \mapsto \frac{\lvert 0\rangle+\lvert 1\rangle}{\sqrt{2}} \\ \lvert 1\rangle \mapsto \frac{\lvert 0\rangle-\lvert 1\rangle}{\sqrt{2}} \end{cases}$$

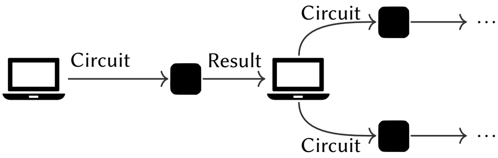
- **Non-Cloning Principle.** ~~$\lvert x\rangle \mapsto \lvert x\rangle \otimes \lvert x\rangle$~~

Classical Control Flow



From Classical to Quantum Control Flow

Classical Control Flow



Quantum Control Flow

$$\mathrm{QSwitch}(x, y, U, V) = \begin{cases} VU(y) & \text{if } x = |0\rangle \\ UV(y) & \text{if } x = |1\rangle \end{cases}$$

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |y\rangle \mapsto \alpha|0\rangle \otimes (UV|y\rangle) + \beta|1\rangle \otimes (VU|y\rangle).$$

Physically implementation but **not in co-processor**.

Classical

- Bit = $\mathbb{1} \oplus \mathbb{1}$.

QRAM

- Qubit is **opaque**.

Classical

- Bit = $\mathbb{1} \oplus \mathbb{1}$.
- Rich type system.

QRAM

- Qubit is **opaque**.
- Only **tensors**.

Classical

- Bit = $\mathbb{1} \oplus \mathbb{1}$.
- Rich type system.
- Classical control flow.

QRAM

- Qubit is **opaque**.
- Only **tensors**.
- No **quantum control flow**.

Classical

- Bit = $\mathbb{1} \oplus \mathbb{1}$.
- Rich type system.
- Classical control flow.

QRAM

- Qubit is **opaque**.
- Only **tensors**.
- No **quantum control flow**.

This thesis

Develop a new model of quantum computation featuring

- **A richer type system** (inductive);
- **with quantum control flow**.

Classical

- Bit = $\mathbb{1} \oplus \mathbb{1}$.
- Rich type system.
- Classical control flow.

QRAM

- Qubit is **opaque**.
- Only **tensors**.
- No **quantum control flow**.

This thesis

Develop a new model of quantum computation featuring

- **A richer type system** (inductive);
- **with quantum control flow**.

Approach : Curry-Howard Correspondence.

Types

- Type = Description of a data.
  product, choice, fonctions, …
- Invariant on the structure of computation.
- Ensure **safety properties**.

The Curry-Howard Correspondence

Types

- Type = Description of a data.
  product, choice, fonctions, …
- Invariant on the structure of computation.
- Ensure **safety properties**.

Logic

- Formulas = Mathematical statements
  AND, OR, IMP, …
- Study of **mathematical reasoning**.
- Focus on **propositions and their proofs**.

The Curry-Howard Correspondence

Types

- Type = Description of a data.
  product, choice, fonctions, ...
- Invariant on the structure of computation.
- Ensure **safety properties**.

Logic

- Formulas = Mathematical statements
  AND, OR, IMP, ...
- Study of **mathematical reasoning**.
- Focus on **propositions and their proofs**.

Curry-Howard

Types	$\leftrightarrow$	Propositions
Terms	$\leftrightarrow$	Proofs
Evaluation	$\leftrightarrow$	Cut-Elimination

Types

- Type = Description of a data.
  product, choice, fonctions, …
- Invariant on the structure of computation.
- Ensure **safety properties**.

Logic

- Formulas = Mathematical statements
  AND, OR, IMP, …
- Study of **mathematical reasoning**.
- Focus on **propositions and their proofs**.

Curry-Howard

Types	$\leftrightarrow$	Propositions
Terms	$\leftrightarrow$	Proofs
Evaluation	$\leftrightarrow$	Cut-Elimination

$$\frac{f : A \to B \qquad x : A}{f(x) : B}$$

Types

- Type = Description of a data.
  product, choice, fonctions, ...
- Invariant on the structure of computation.
- Ensure **safety properties**.

Logic

- Formulas = Mathematical statements
  AND, OR, IMP, ...
- Study of **mathematical reasoning**.
- Focus on **propositions and their proofs**.

Curry-Howard

Types	$\leftrightarrow$	Propositions
Terms	$\leftrightarrow$	Proofs
Evaluation	$\leftrightarrow$	Cut-Elimination

$$\frac{f : A \to B \qquad x : A}{f(x) : B}$$

$$\dfrac{\begin{matrix}\pi \\ \vdots \\ A \to B\end{matrix} \qquad \begin{matrix}\pi' \\ \vdots \\ A\end{matrix}}{B}\ \text{Modus Ponens}$$

Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1}$$

Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1}$$

$$(\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\ \parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\ \otimes}{A \vdash A}\ \text{cut}$$

Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1}$$

$$(\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\ \parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\ \otimes}{A \vdash A}\ \text{cut}$$

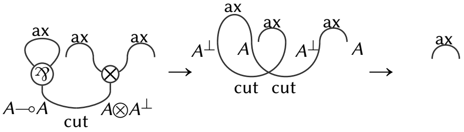
No duplication or erasure.

Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1} \qquad (\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\parr \quad \dfrac{A \vdash A \quad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\otimes}{A \vdash A}\text{cut}$$

No duplication or erasure.

Proof Nets



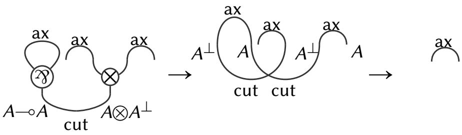
Formulas

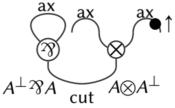
$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1}$$

$$(\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\,\parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\,\otimes}{A \vdash A}\,\text{cut}$$

No duplication or erasure.

Proof Nets



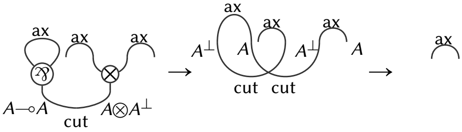


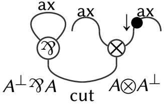
Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1} \qquad (\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\parr \quad \dfrac{A \vdash A \quad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\otimes}{A \vdash A}\,\text{cut}$$

No duplication or erasure.

Proof Nets





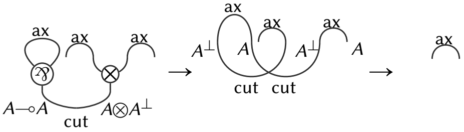
Formulas

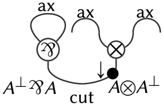
$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1}$$

$$(\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\,\parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\,\otimes}{A \vdash A}\,\text{cut}$$

No duplication or erasure.

Proof Nets



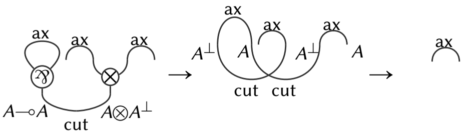


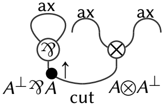
Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1} \qquad (\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\otimes}{A \vdash A}\text{cut}$$

No duplication or erasure.

Proof Nets



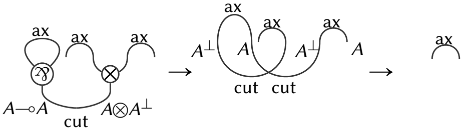


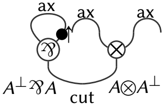
Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1} \qquad (\lambda x.x)\, y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\parr \quad \dfrac{A \vdash A \quad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\otimes}{A \vdash A}\,\text{cut}$$

No duplication or erasure.

Proof Nets



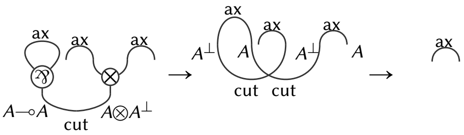


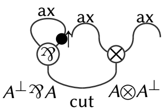
Formulas

$$A, B ::= a \mid a^{\perp} \mid A \otimes B \mid A \parr B \mid \mathbb{1} \qquad (\lambda x.x)\ y \rightsquigarrow \dfrac{\dfrac{A \vdash A}{\vdash A^{\perp} \parr A}\,\parr \qquad \dfrac{A \vdash A \qquad A \vdash A}{A \vdash A, A \otimes A^{\perp}}\,\otimes}{A \vdash A}\,\text{cut}$$

No duplication or erasure.

Proof Nets





Additives

$A, B ::= \cdots \mid A \oplus B$

$\text{Bool} = \mathbb{1} \oplus \mathbb{1}$.

$\oplus$ represent the **action of a choice**.

Two routes for quantum types.

Classical Control

- bit $= \mathbb{1} \oplus \mathbb{1}$
- Allow duplication in a controlled way.
- Quantum λ-calculus [Selinger, Valiron'04].
- Classical control.

Quantum Control

- qubit $= \mathbb{1} \oplus \mathbb{1}$
- Inductive types
  $\mathsf{list}(A) = \mu X.\mathbb{1} \oplus (A \otimes X)$.
- Quantum Switch.

Our proposal: logic μMALL, MALL + least and greatest fixed-point.

l.f.p operator
(Ch. 4, CSL'23)

Pairing
(Ch. 5, MFCS'21)

$$[A] = \mu X . \mathbb{1} \oplus (A \otimes X)$$

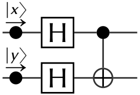
Quantum Control
(Ch. 6, Draft)

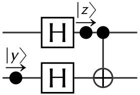
l.f.p operator
(Ch. 4, CSL'23)

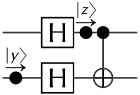
Pairing
(Ch. 5, MFCS'21)

$$[A] = \mu X. \mathbb{1} \oplus (A \otimes X)$$

Quantum Control
(Ch. 6, Draft)

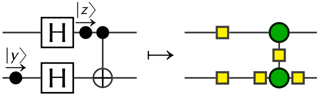

|x⟩
|y⟩
H
H


|z⟩
|y⟩
H
H



- MELL + Circuits [Dal Lago. et al'16].
- Require **synchronisation**.
- No superposition of **position**.
- Classical Control.

Token Machines for Quantum Computation



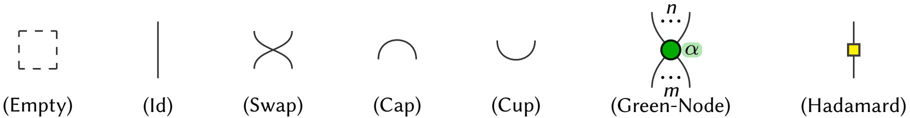
- MELL + Circuits [Dal Lago. et al'16].
- Require **synchronisation**.
- No superposition of **position**.
- Classical Control.

- Consider **Token Machine**.
- **Asynchronicity**.
- **Quantum Control**.

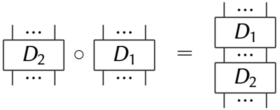
Generators

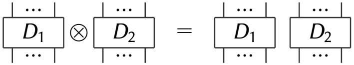
(Empty) (Id) (Swap) (Cap) (Cup) (Green-Node) (Hadamard)

Generators



Compositions



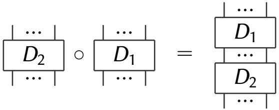


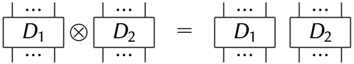
ZX-Calculus in Short

Generators

(Empty) (Id) (Swap) (Cap) (Cup) (Green-Node) (Hadamard)

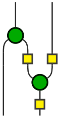
Compositions



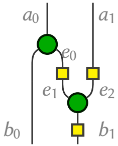


Standard Interpretation

Linear Maps : $\textbf{ZX} \to \mathcal{M}(\mathbb{C})$



$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$D =$ 

Token

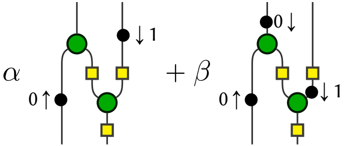
3-tuple $(e, d, b) \in \mathcal{E}(D) \times \{\uparrow, \downarrow\} \times \{0, 1\}$ where:

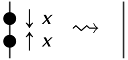
- e is an edge of the ZX-Diagram D.
- d is a direction.
- b is the state of the token.

Token State

A *token state* is a **sum** of **products** of tokens with complex coefficients.

$$\langle t \mid t' \rangle = \begin{cases} 1 & \text{if } t = t' \\ 0 & \text{if } t \neq t' \end{cases}$$



- Collisions : 

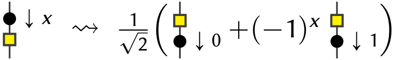
- Collisions : 

- Collisions : 

- Diffusions : 

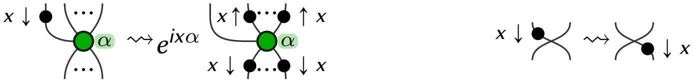
- Collisions : 

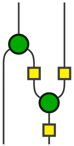
- Diffusions : 

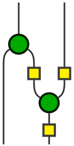


- Collisions :

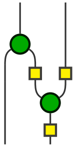
- Diffusions :



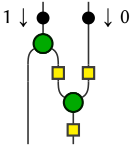
$$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$$  $$= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

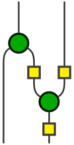
$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$

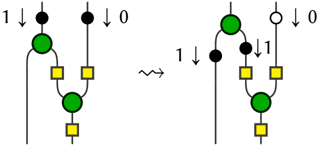
$$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$$



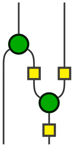
$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}}|11\rangle$$



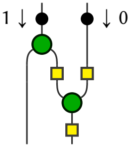
$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$  $= \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \Longrightarrow |10\rangle \mapsto \frac{1}{\sqrt{2}}\,|11\rangle$



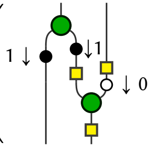
$\frac{1}{\sqrt{2}}$ CNOT =



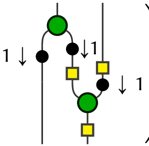
$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \Longrightarrow |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$



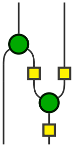
$\rightsquigarrow^* \frac{1}{\sqrt{2}} \Bigg($

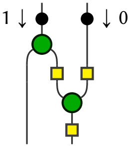


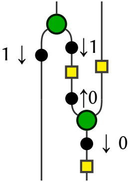
$+$

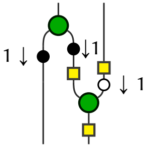


$\Bigg)$

$\frac{1}{\sqrt{2}}$ CNOT $=$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$

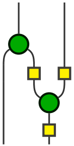


$\rightsquigarrow^{*} \frac{1}{\sqrt{2}} \Bigg($ 

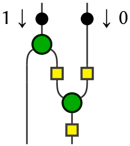
$+$ 

$\Bigg)$

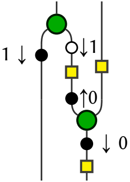
$\frac{1}{\sqrt{2}}$ CNOT =



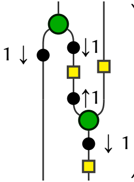
$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \Longrightarrow |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$



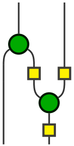
$\rightsquigarrow^{*} \frac{1}{\sqrt{2}} \Bigg($

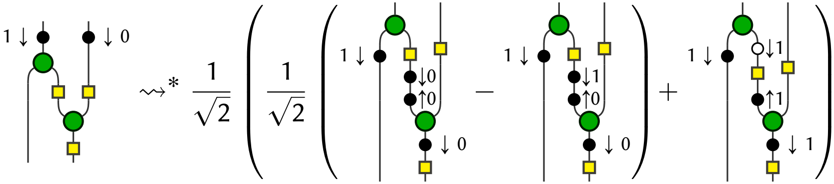


$+$

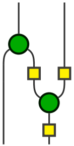


$\Bigg)$

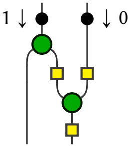
$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$



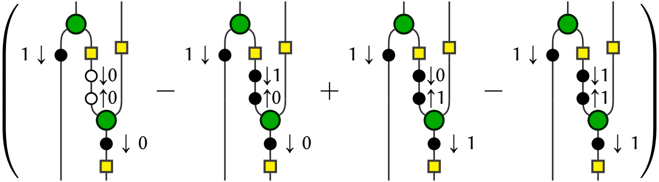
$\frac{1}{\sqrt{2}}$ CNOT =



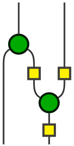
$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \Longrightarrow |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$



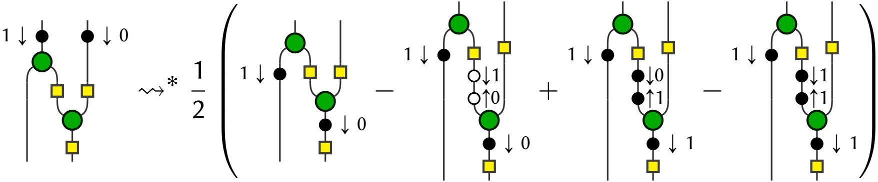
$\rightsquigarrow^* \frac{1}{2}$



$\frac{1}{\sqrt{2}}$ CNOT =

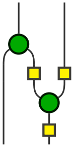


$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}}|11\rangle$$

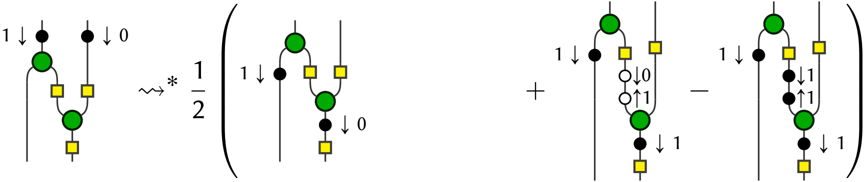


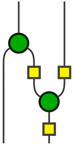
Example

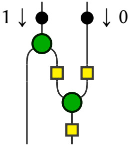
$$\frac{1}{\sqrt{2}}\,\text{CNOT} =$$

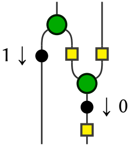


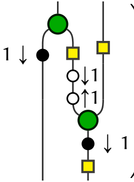
$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}}|11\rangle$$



$\frac{1}{\sqrt{2}}$ CNOT $=$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$

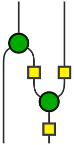


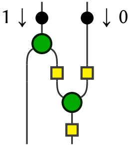
$\rightsquigarrow^* \ \frac{1}{2} \Bigg($ 

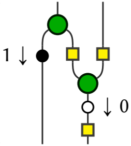
$-$ 

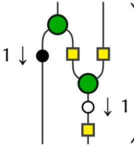
$\Bigg)$

Example

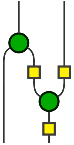
$\frac{1}{\sqrt{2}}$ CNOT $=$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$

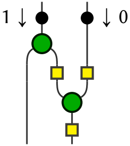


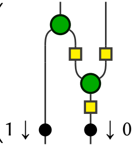
$\rightsquigarrow^* \frac{1}{2} \Bigg($ 

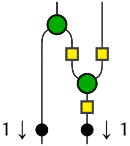
$-$ 

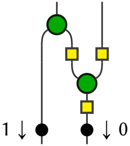
$\Bigg)$

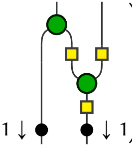
$\frac{1}{\sqrt{2}}$ CNOT $=$  $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}} |11\rangle$



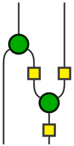
$\rightsquigarrow^* \frac{1}{2\sqrt{2}}\Bigg($ 

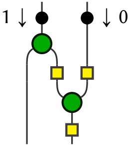
$+$ 

$-$ 

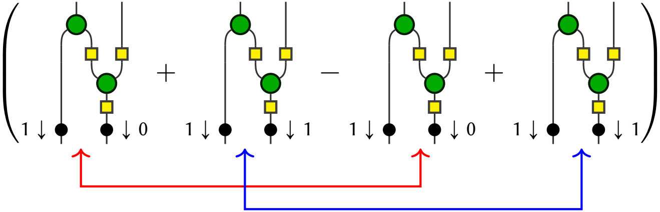
$+$ 

$\Bigg)$

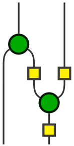
$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$  $= \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \Longrightarrow |10\rangle \mapsto \frac{1}{\sqrt{2}}|11\rangle$



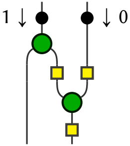
$\rightsquigarrow^* \frac{1}{2\sqrt{2}}$



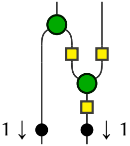
$\frac{1}{\sqrt{2}}\,\mathrm{CNOT} =$



$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies |10\rangle \mapsto \frac{1}{\sqrt{2}}\,|11\rangle$$



$\rightsquigarrow^{*} \frac{1}{\sqrt{2}}$

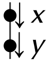


Avoiding Errors

Rewriting System

We define $\rightsquigarrow$ as *exactly* one **diffusion rule** followed by all possible **collision** rules until none applies.

Want to avoid:

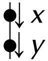
- Having multiple tokens on the same edge that don't collide: 

- Non-termination.

Rewriting System

We define $\rightsquigarrow$ as *exactly* one **diffusion rule** followed by all possible **collision** rules until none applies.

Want to avoid:

- Having multiple tokens on the same edge that don't collide: 

- Non-termination.

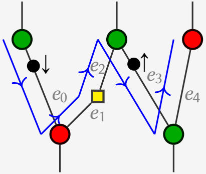
Two invariants:

- **Well-Formedness**: Avoid two tokens going in the same direction on a path.
- **Cycle-Balancedness**: Avoid tokens alone in cycles.

Polarity in a Path

$p = (e_0, e_1, e_2, e_3, e_4)$ is an oriented path.

- If a token follows the path $+1$
- If it goes against it -1
- If it is not on the path 0



Example:

- Here, polarity $P(p,(e_0 \downarrow x)(e_3 \uparrow y)) = P(p,(e_0 \downarrow x)) + P(p,(e_3 \uparrow y)) = 0$

Well-Formed Token State

Given a ZX-Diagram and a Token State, it is **Well-Formed** if for every path p its Polarity $\in \{-1, 0, 1\}$.

Well-Formed Token State

Given a ZX-Diagram and a Token State, it is **Well-Formed** if for every path p its Polarity $\in \{-1, 0, 1\}$.

- Thm 5.3.11: Well-Formedness preserved under $\rightsquigarrow$.
- Thm 5.3.12: Well-formed states cannot reach "bad configurations".

Well-Formed Token State

Given a ZX-Diagram and a Token State, it is **Well-Formed** if for every path p its Polarity $\in \{-1, 0, 1\}$.

- Thm 5.3.11: Well-Formedness preserved under $\rightsquigarrow$.
- Thm 5.3.12: Well-formed states cannot reach "bad configurations".

Cycle-Balanced Token State

Given a ZX-Diagram and a Token State, it is **Cycle-Balanced** if for every cycle c its Polarity $= 0$.

Well-Formed Token State

Given a ZX-Diagram and a Token State, it is **Well-Formed** if for every path p its Polarity $\in \{-1, 0, 1\}$.

- Thm 5.3.11: Well-Formedness preserved under $\rightsquigarrow$.
- Thm 5.3.12: Well-formed states cannot reach "bad configurations".

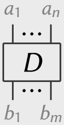
Cycle-Balanced Token State

Given a ZX-Diagram and a Token State, it is **Cycle-Balanced** if for every cycle c its Polarity $= 0$.

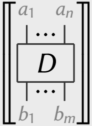
- Thm 5.3.16: Termination of well-formed, cycle-balanced token state.
- Prop 5.3.18: Local confluence of well-formed, cycle-balanced token state.

Thm 5.3.25 (Simulation of Standard Interpretation)

Let

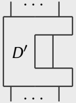


a ZX-Diagram such that

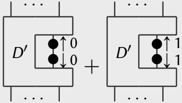


$= \sum_{q=1}^{2^{m+n}} \lambda_q \left|y_{1,q} \dots y_{m,q}\right\rangle \left\langle x_{1,q} \dots x_{n,q}\right|$

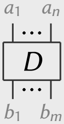
Let $D =$

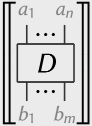


, consider $t =$

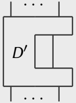


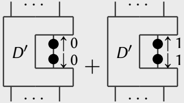
Thm 5.3.25 (Simulation of Standard Interpretation)

Let 

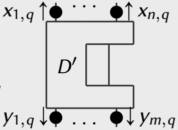
a ZX-Diagram such that 

$= \sum_{q=1}^{2^{m+n}} \lambda_q \left| y_{1,q} \dots y_{m,q} \right\rangle \left\langle x_{1,q} \dots x_{n,q} \right|$

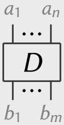
Let $D =$ 

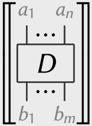
, consider $t =$ 

Then

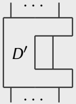
$t \rightsquigarrow^* \sum_{q=1}^{2^{m+n}} \lambda_q$ 

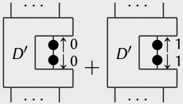
Thm 5.3.25 (Simulation of Standard Interpretation)

Let 

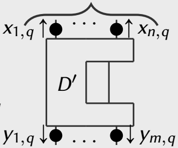
a ZX-Diagram such that 

$= \sum_{q=1}^{2^{m+n}} \lambda_q \left| y_{1,q} \dots y_{m,q} \right\rangle \left\langle x_{1,q} \dots x_{n,q} \right|$

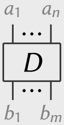
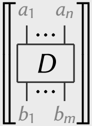
Let $D =$ 

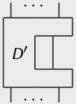
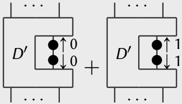
, consider $t =$ 

Then

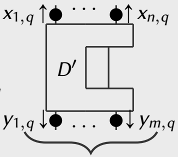
$t \rightsquigarrow^* \sum_{q=1}^{2^{m+n}} \lambda_q$ 

Thm 5.3.25 (Simulation of Standard Interpretation)

Let  a ZX-Diagram such that  $= \sum_{q=1}^{2^{m+n}} \lambda_q \left|y_{1,q} \dots y_{m,q}\right\rangle \left\langle x_{1,q} \dots x_{n,q}\right|$

Let $D =$  , consider $t =$ 

Then

$$t \rightsquigarrow^* \sum_{q=1}^{2^{m+n}} \lambda_q$$ 

l.f.p operator
(Ch. 4, CSL'23)

Pairing
(Ch. 5, MFCS'21)

$$[A] = \mu X. \mathbb{1} \oplus (A \otimes X)$$

Quantum Control
(Ch. 6, Draft)

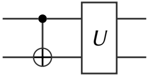
l.f.p operator
(Ch. 4, CSL'23)

Pairing
(Ch. 5, MFCS'21)

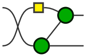
$$[A] = \mu X . \mathbb{1} \oplus (A \otimes X)$$

Quantum Control
(Ch. 6, Draft)

⊗-based languages

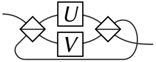


Quantum Circuits

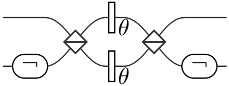


ZX-Calculus

⊕-based languages

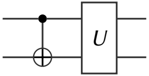


PBS-Calculus

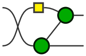


LOv-Calculus

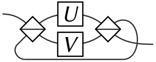
⊗-based languages **⊕-based languages**



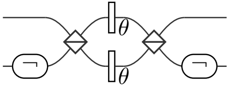
Quantum Circuits



ZX-Calculus

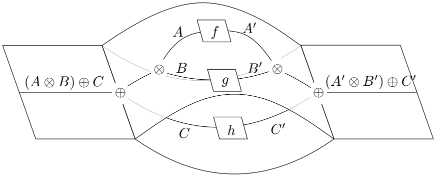


PBS-Calculus

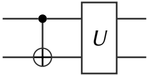


LOv-Calculus

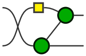
The Many-Worlds Calculus



⊗-based languages

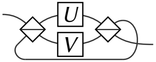


Quantum Circuits

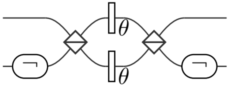


ZX-Calculus

⊕-based languages

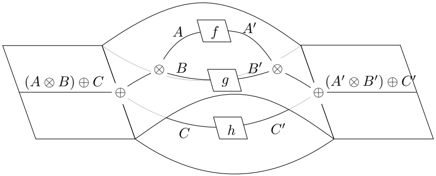


PBS-Calculus

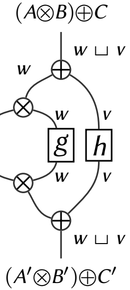


LOv-Calculus

The Many-Worlds Calculus

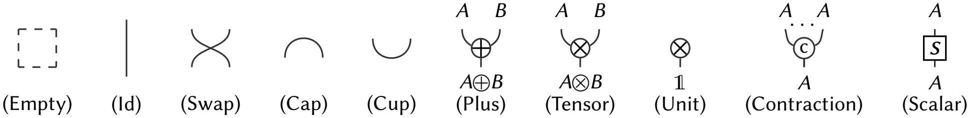


$\mapsto$

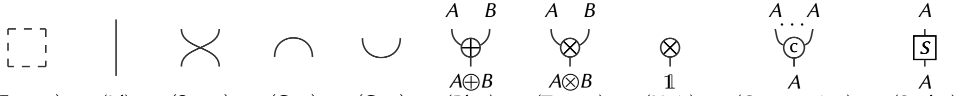


- Label **wires** with **worlds**.
- **Worlds** for naming **slices**.

Generators


(Empty)
(Id)
(Swap)
(Cap)
(Cup)
A B
A⊕B
(Plus)
A B
A⊗B
(Tensor)
𝟙
(Unit)
A . . . A
c
A
(Contraction)
A
S
A
(Scalar)

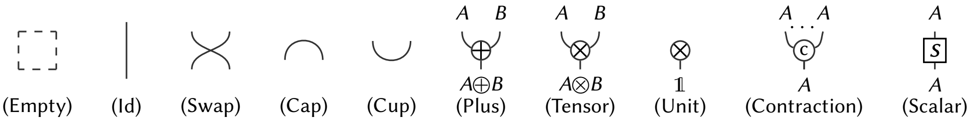
Generators



(Empty) (Id) (Swap) (Cap) (Cup) (Plus) (Tensor) (Unit) (Contraction) (Scalar)

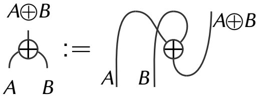
Compositions

Generators

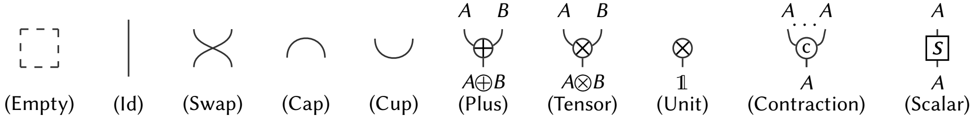


Compositions

Derived Constructors & Tokens

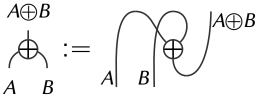


Generators



Compositions

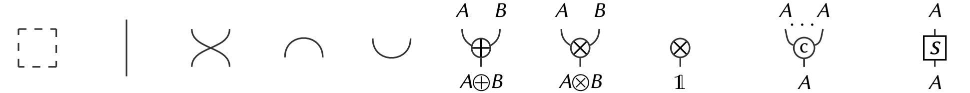
Derived Constructors & Tokens



$$v ::= () \mid \langle s_1, s_2 \rangle \mid \mathtt{inj}_\ell\ s \mid \mathtt{inj}_r\ s$$

$$s ::= v \mid ☠$$

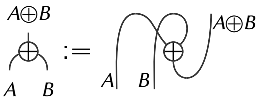
Generators



(Empty) (Id) (Swap) (Cap) (Cup) (Plus) (Tensor) (Unit) (Contraction) (Scalar)

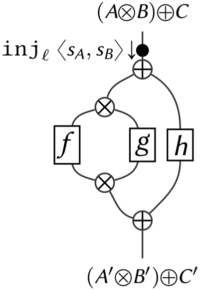
Compositions

Derived Constructors & Tokens

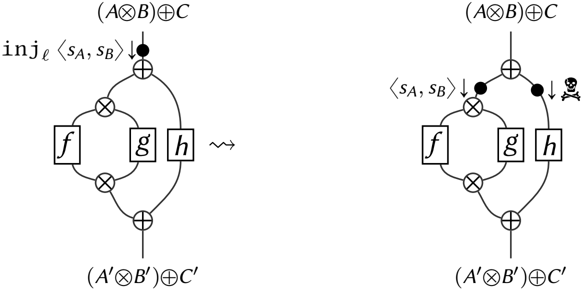


$$v ::= () \mid \langle s_1, s_2 \rangle \mid \mathtt{inj}_\ell\ s \mid \mathtt{inj}_r\ s$$
$$s ::= v \mid ☠$$
$$\text{Token} = (e, d, b) \in \mathcal{E}(D) \times \{\uparrow, \downarrow\} \times s$$

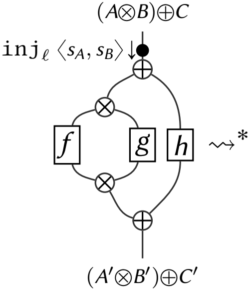
Assume s_A, s_B values of types A and B, then:

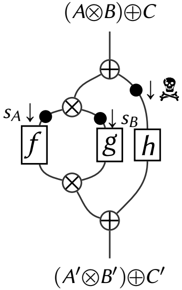


Assume s_A, s_B values of types A and B, then:

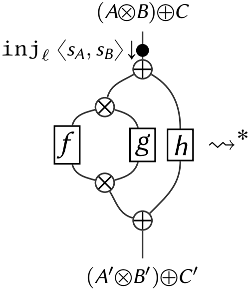


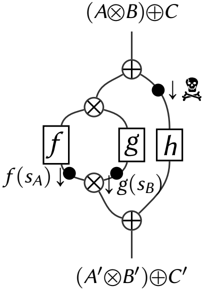
Assume s_A, s_B values of types A and B, then:



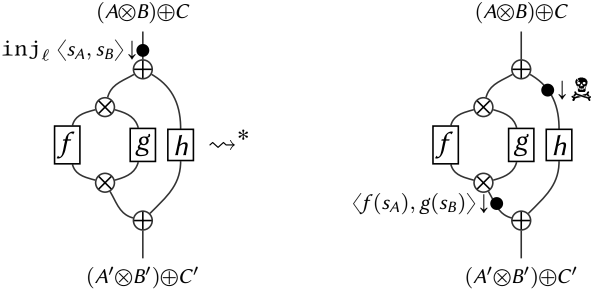


Assume s_A, s_B values of types A and B, then:

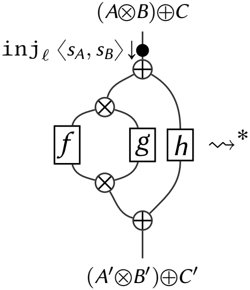


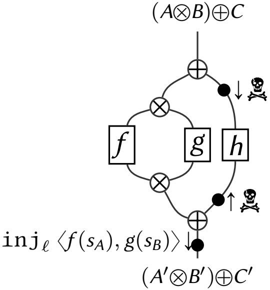


Assume s_A, s_B values of types A and B, then:

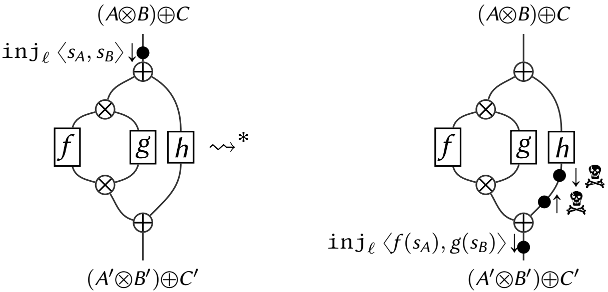


Assume s_A, s_B values of types A and B, then:

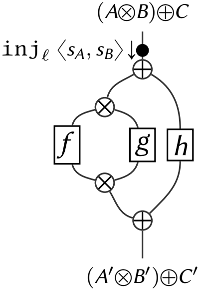




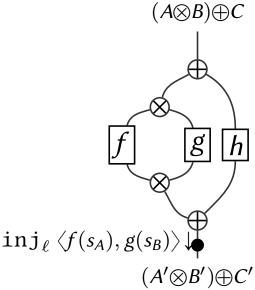
Assume s_A, s_B values of types A and B, then:



Assume s_A, s_B values of types A and B, then:

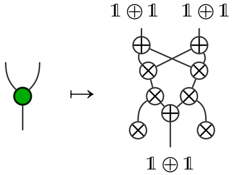


$\rightsquigarrow^*$



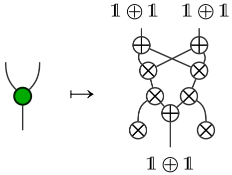
Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.

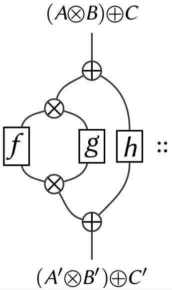


Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.

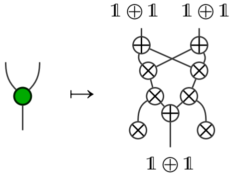


Quantum Control

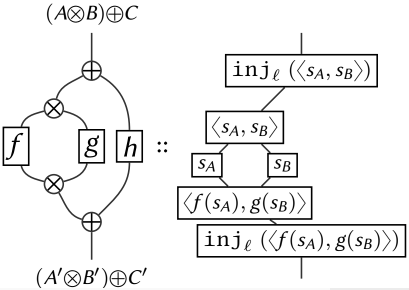


Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.

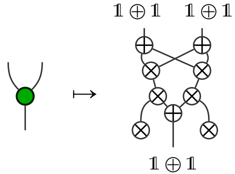


Quantum Control

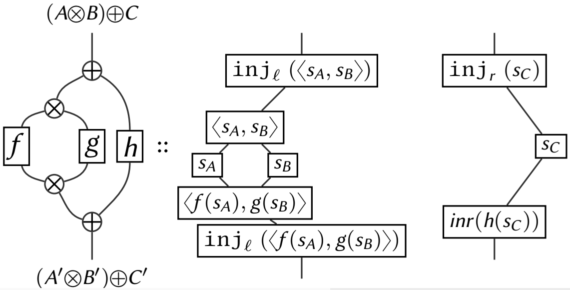


Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.

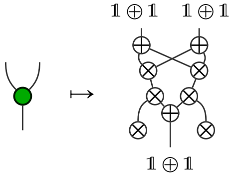


Quantum Control

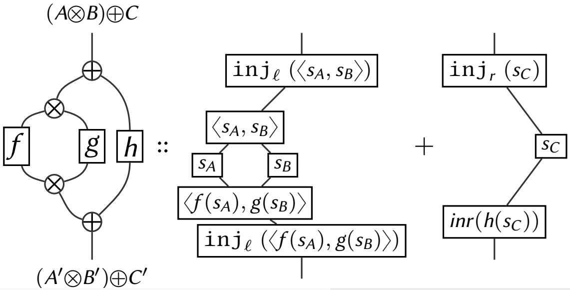


Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.

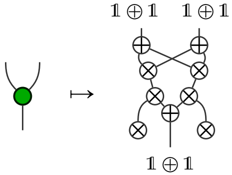


Quantum Control

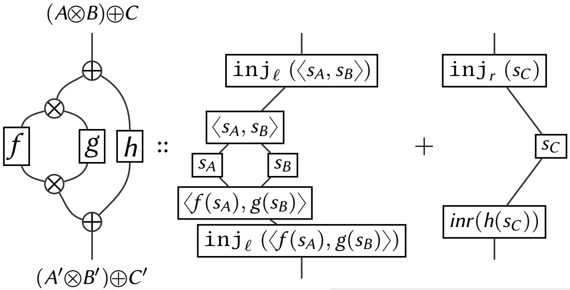


Results

Well-Formedness, **Cycle-Balancedness** still holds.
$\Rightarrow$ Confluence, Termination, Avoid bad configurations.



Quantum Control



Missing: Inductive types.

l.f.p operator
(Ch. 4, CSL'23)

Pairing
(Ch. 5, MFCS'21)

$$[A] = \mu X.\mathbb{1} \oplus (A \otimes X)$$

Quantum Control
(Ch. 6, Draft)

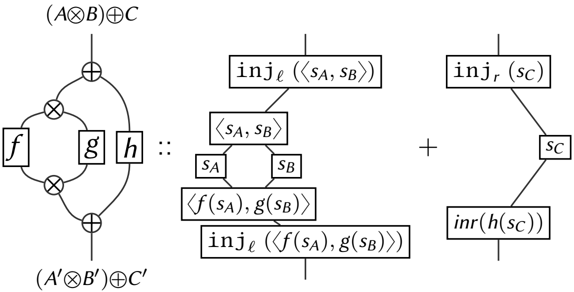
l.f.p operator
(Ch. 4, CSL'23)

Pairing
(Ch. 5, MFCS'21)

$$[A] = \mu X. \mathbb{1} \oplus (A \otimes X)$$

Quantum Control
(Ch. 6, Draft)

A Syntax Term Language for the Many-Worlds Calculus



$$\left\{ \begin{array}{lcl} \texttt{inj}_\ell\ (\langle x, y\rangle) & \leftrightarrow & \texttt{inj}_\ell\ (\langle f\ x, g\ y\rangle) \\ \texttt{inj}_r\ (z) & \leftrightarrow & \texttt{inj}_r\ (h\ z) \end{array} \right\}$$

Function from $(A \otimes B) \oplus C \leftrightarrow (A' \otimes B') \oplus C'$

(Base types)	$A, B ::= \mathbb{1} \mid A \oplus B \mid A \otimes B$
(Isos, first-order)	$T ::= A \leftrightarrow B$
(Values)	$v ::= x \mid () \mid \langle v_1, v_2 \rangle \mid \texttt{inj}_\ell\ v \mid \texttt{inj}_r\ v$
(Expressions)	$e ::= v \mid \texttt{let}\ x = \omega\ y\ \texttt{in}\ e$
(Isos)	$\omega ::= \{v_1 \leftrightarrow e_1 \mid \cdots \mid v_n \leftrightarrow e_n\}$

$$
\begin{array}{llll}
\text{(Base types)} & A, B & ::= & \mathbb{1} \mid A \oplus B \mid A \otimes B \mid \mu X.A \mid X \\
\text{(Isos, first-order)} & T & ::= & A \leftrightarrow B \\
\\
\text{(Values)} & v & ::= & x \mid () \mid \langle v_1, v_2 \rangle \mid \texttt{inj}_\ell\ v \mid \texttt{inj}_r\ v \mid \texttt{fold}\ e \\
\text{(Expressions)} & e & ::= & v \mid \texttt{let}\ x = \omega\ y\ \texttt{in}\ e \\
\text{(Isos)} & \omega & ::= & \{ v_1 \leftrightarrow e_1 \mid \cdots \mid v_n \leftrightarrow e_n \} \mid \textbf{fix}\ f.\omega \mid f
\end{array}
$$

$$
\mathrm{map}(\omega) = \textbf{fix}\ f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ \ h) :: (f\ \ t) \end{array} \right\} : [A] \leftrightarrow [B]
$$

$[\,] = \texttt{fold}\ (\texttt{inj}_\ell\ (()))$ $\quad$ $h :: t = \texttt{fold}\ (\texttt{inj}_r\ (\langle h, t \rangle))$

$\mu\mathsf{MALL}^\infty = \mathsf{MALL} + \mu.$

$$\frac{\Delta, A[X \leftarrow \mu X.A] \vdash B}{\Delta, \mu X.A \vdash B}\ \mu_L \qquad \frac{\Delta \vdash A[X \leftarrow \mu X.A]}{\Delta \vdash \mu X.A}\ \mu_R$$

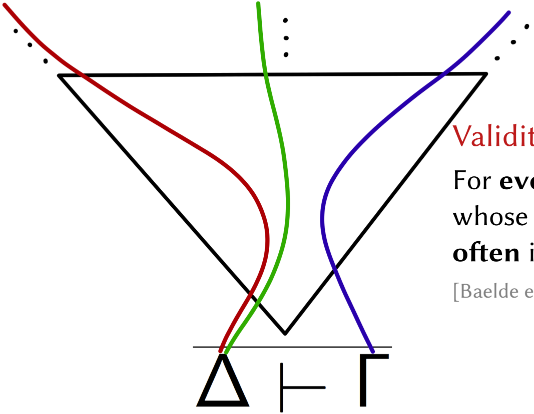
μMALL$^{\infty}$ = MALL $+\mu$.

$$\frac{\Delta, A[X \leftarrow \mu X.A] \vdash B}{\Delta, \mu X.A \vdash B}\ \mu_L \qquad \frac{\Delta \vdash A[X \leftarrow \mu X.A]}{\Delta \vdash \mu X.A}\ \mu_R$$

Non-wellfounded proofs:

$$\dfrac{\dfrac{\vdots}{\mu X.X \vdash F}\ \mu \qquad \dfrac{\vdots}{\vdash \mu X.X}\ \mu}{\vdash F}\ \text{cut}$$

There is a need for a validity criterion on derivations.



Validity Condition

For **every infinite branch**, there is a **thread** whose **smallest** formula that occurs **infinitly often** is a μ formula on the **left**.

[Baelde et al., 2016, 2022]

Let us take the $\text{map}(\omega)$ functions on lists.

$$\textbf{fix } f. \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega \;\ h) :: (f \;\ t) \end{array} \right\} : [A] \leftrightarrow [B]$$

Send it to a derivation $\text{proof}(\text{map}(\omega)) : [A] \vdash [B]$.

$$\dfrac{\dfrac{\dfrac{}{\vdash [B]}}{\mathbb{1} \vdash [B]}\ \mathbb{1}_L \qquad \dfrac{A, [A] \vdash [B]}{A \otimes [A] \vdash [B]}\ \otimes_L}{\dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\ \mu_L}\ \oplus_L$$

$$\textbf{fix}\ f.\ \left\{ \begin{array}{ll} [\,] & \leftrightarrow [\,] \\ h :: t & \leftrightarrow (\omega\ \ h) :: (f\ \ t) \end{array} \right\}$$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \mathbb{1}}\ \mathbb{1}_R}{\vdash \mathbb{1} \oplus (B \otimes [A])}\ \oplus^1_R}{\vdash [B]}\ \mu_R}{\mathbb{1} \vdash [B]}\ \mathbb{1}_L \qquad \dfrac{A, [A] \vdash [B]}{A \otimes [A] \vdash [B]}\ \otimes_L}{\dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\ \mu_L}\ \oplus_L
$$

$$
\textbf{fix } f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ \ h) :: (f\ \ t) \end{array} \right\}
$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\vdash \mathbb{1}}\ \mathbb{1}_R
}{\vdash \mathbb{1} \oplus (B \otimes [A])}\ \oplus^1_R
}{\vdash [B]}\ \mu_R
}{\mathbb{1} \vdash [B]}\ \mathbb{1}_L
\qquad
\dfrac{
\dfrac{
\dfrac{A, [A] \vdash B \otimes [B]}{A, [A] \vdash \mathbb{1} \oplus (B \otimes [B])}\ \oplus^2_R
}{A, [A] \vdash [B]}\ \mu_R
}{A \otimes [A] \vdash [B]}\ \otimes_L
}{
\dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\ \mu_L
}\ \oplus_L
$$

$$
\textbf{fix}\ f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ h) :: (f\ t) \end{array} \right\}
$$

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\dfrac{}{\vdash \mathbb{1}}\;\mathbb{1}_R}{\vdash \mathbb{1} \oplus (B \otimes [A])}\;\oplus^1_R
}{\vdash [B]}\;\mu_R
}{\mathbb{1} \vdash [B]}\;\mathbb{1}_L
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{\dfrac{\omega}{A \vdash B}}{A, [A] \vdash B \otimes [B]}\;\otimes_R
}{A, [A] \vdash \mathbb{1} \oplus (B \otimes [B])}\;\oplus^2_R
}{A, [A] \vdash [B]}\;\mu_R
}{A \otimes [A] \vdash [B]}\;\otimes_L
}{
\dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\;\mu_L
}\;\oplus_L
$$

$$
\textbf{fix } f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ h) :: (f\ \ t) \end{array} \right\}
$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{}{\vdash \mathbb{1}}\ \mathbb{1}_R
      }{\vdash \mathbb{1} \oplus (B \otimes [A])}\ \oplus^1_R
    }{\vdash [B]}\ \mu_R
  }{\mathbb{1} \vdash [B]}\ \mathbb{1}_L
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{\omega}{A \vdash B} \quad \dfrac{\vdots}{[A] \vdash [B]}
        }{A, [A] \vdash B \otimes [B]}\ \otimes_R
      }{A, [A] \vdash \mathbb{1} \oplus (B \otimes [B])}\ \oplus^2_R
    }{A, [A] \vdash [B]}\ \mu_R
  }{A \otimes [A] \vdash [B]}\ \otimes_L
}{
  \dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\ \mu_L
}\ \oplus_L
$$

$$
\mathbf{fix}\ f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ h) :: (f\ t) \end{array} \right\}
$$

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{}{\vdash \mathbb{1}}\,\mathbb{1}_R
    }{\vdash \mathbb{1} \oplus (B \otimes [A])}\,\oplus_R^1
  }{
    \dfrac{\vdash [B]}{\mathbb{1} \vdash [B]}\,\mathbb{1}_L
  }\,\mu_R
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{\omega}{A \vdash B}
          \quad
          \dfrac{\vdots}{[A] \vdash [B]}
        }{A, [A] \vdash B \otimes [B]}\,\otimes_R
      }{A, [A] \vdash \mathbb{1} \oplus (B \otimes [B])}\,\oplus_R^2
    }{A, [A] \vdash [B]}\,\mu_R
  }{A \otimes [A] \vdash [B]}\,\otimes_L
}{
  \dfrac{\mathbb{1} \oplus (A \otimes [A]) \vdash [B]}{[A] \vdash [B]}\,\mu_L
}\,\oplus_L
$$

$$
\textbf{fix } f.\ \left\{ \begin{array}{lcl} [\,] & \leftrightarrow & [\,] \\ h :: t & \leftrightarrow & (\omega\ \ h) :: (f\ \ t) \end{array} \right\}
$$

Language

Iso have an well-typed inverse. Lemma 4.2.11: $\omega : A \leftrightarrow B$ then $\omega^{-1} : B \leftrightarrow A$.

Iso are isomorphisms. Thm 4.2.13: $\omega \circ \omega^{-1} = \mathrm{Id}$.

Subject Reduction & Progress. Lemma 4.2.18 & 4.2.19.

Curry-Howard

Proof Validity. Thm 4.4.20: If $\omega : A \leftrightarrow B$ then $\mathrm{proof}(\omega) : A \vdash B$ is a proof.

Cut-Elimination Simulation. Thm 4.4.29: If $t \to t'$ then $\mathrm{proof}(t) \to \mathrm{proof}(t')$.

ZX Token Machine: MFCS'21

- **With**: Benoît Valiron, Renaud Vilmart.
- **What**: Study of Token-Based semantics for the ZX-Calculus.
- **Why**: First approach for control quantum, led to the Many-Worlds Calculus.

ZX Token Machine: MFCS'21

- **With**: Benoît Valiron, Renaud Vilmart.
- **What**: Study of Token-Based semantics for the ZX-Calculus.
- **Why**: First approach for control quantum, led to the Many-Worlds Calculus.

Many-Worlds Calculus: Draft

- **With**: Marc de Visme, Benoît Valiron, Renaud Vilmart.
- **What**: Graphical language with $\otimes$ and $\oplus$.
- **Why**: Explicit quantum control, quantum types.

ZX Token Machine: MFCS'21

- **With**: Benoît Valiron, Renaud Vilmart.
- **What**: Study of Token-Based semantics for the ZX-Calculus.
- **Why**: First approach for control quantum, led to the Many-Worlds Calculus.

Many-Worlds Calculus: Draft

- **With**: Marc de Visme, Benoît Valiron, Renaud Vilmart.
- **What**: Graphical language with $\otimes$ and $\oplus$.
- **Why**: Explicit quantum control, quantum types.

Isomorphisms & μMALL: CSL'23

- **With**: Alexis Saurin, Benoît Valiron.
- **What**: Linear, reversible programming language with inductive types.
- **Why**: First step towards quantum inductive types.

Future Work:

- Quantum Programming Language with Inductive Types.
- Many-Worlds with Inductive Types.
- Relation between the two ?

Future Work:

- Quantum Programming Language with Inductive Types.
- Many-Worlds with Inductive Types.
- Relation between the two ?

First step:

- Remove inductive types.
- Add superposition of expressions.
- Translate iso as Many-Worlds diagrams.
- Thm 6.9.14 : Soudness.